NETVÆRKS- OG KOMMUNIKATIONSSIKKERHED

Segmentation and NetFlow

Agenda

- Follow up from challenge
- Follow up from last time
- Netflow and packet captures
- Segmenting a network

Practicalities

- WPA2 hack
- Skoleprotokol
- Challenge fra sidst
- Besøg af representant fra Rådet for digital sikkerhed d. 10. November
    - Jesper B. Hansen, Siscon

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
```

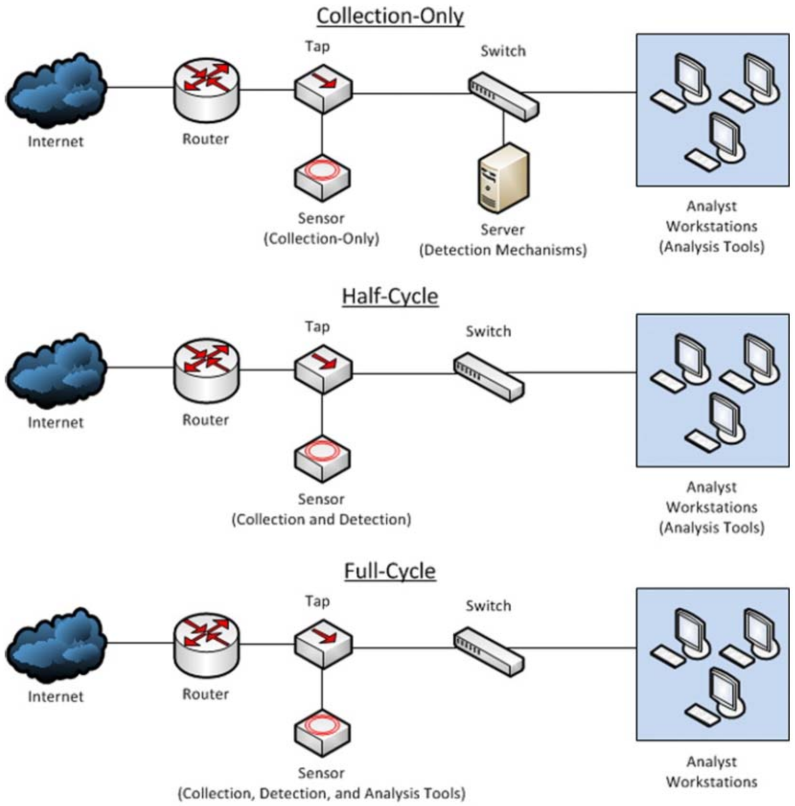
Traffic capturing options

- Full Packet Capture
  - Dumping all traffic

- Session data
  - Only gathering info about the traffic

- Packet Strings
  - Dumping Application level headers

Sensor types



Full Packet capture

- Takes huge amount of space
- Privacy issues

- Basically this is what wireshark does for us. In linux we can also use tcpdump for capturing the traffic

```
tcpdump -i eth0 -w dmp.pcap
```

How to actually collect data

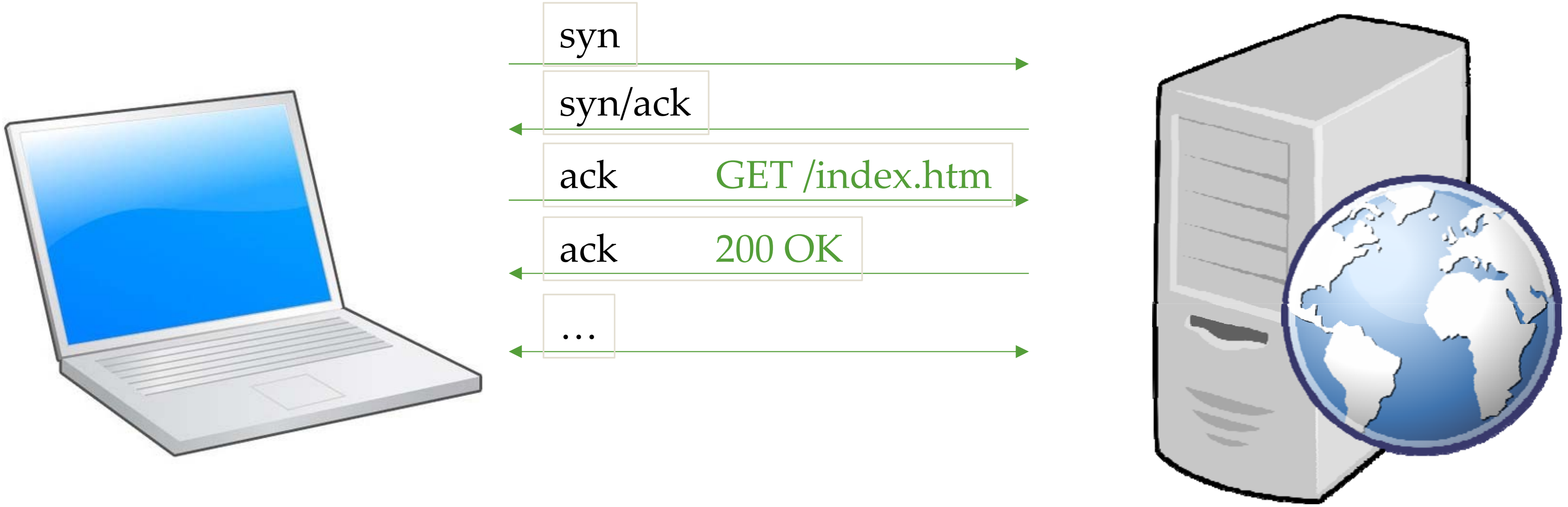
- Hardware Taps
  - Pros: Can be scaled for need
  - Cons: can be very expensive for high speed

- Mirroring the port on the switch (SPAN)
  - Pros: Allready availiable if the switch supports it. No downtime
  - Cons: Can be a problem if collecting more data than the port speed

What is netflow?

- Unidirectional
- 2 flows
- Aggregated metadata
- Pros
  - Very fast
  - Takes up about 0,01% of traffic capture
  - Encrypted traffic looks like the unencrypted
  - Very efficient for detecting anomalies in traffic patterns
- Cons
  - Does not provide content of the traffic

One tcp connection -> 2 flows



syn

syn/ack

ack GET /index.htm

ack 200 OK

…

```
Date first seen         Duration    Proto       Src IP Addr:Port Dst IP Addr:Port               Flags       Tos         Packets     Bytes       Flows
2013-10-20 13:07:08.618 15.465      TCP         192.168.169.2:59579 -> 2.17.221.15:80           .AP.SF      0           11          4783        1
2013-10-20 13:07:08.664 15.419      TCP         2.17.221.15:80 -> 192.168.169.2:59579           .AP.SF      0           13          10768       1

Date first seen         Duration    Proto       Src IP Addr:Port Dst IP Addr:Port               Flags       Tos         Out Pkt In Pkt Out Byte In Byte Flows
2013-10-20 13:07:08.618 15.465      TCP         192.168.169.2:59579 <-> 2.17.221.15:80          .AP.SF      0           13      11     10768    4783    2
```

Full capture vs. netflow compromise

- Combining full packet captures with netflow data can be considered a optimal solution

- F.ex. Rotating Full packet capture after 1 week and netflow data after 365 days

- Setting up netflow sensors on all routers, but only full packet capture on critical segments

Components needed

- fprobe
  - This is the **exporter** that generates the netflow updates
- nfcapd
  - This is the **collector** that, accepts the updates from the exporter
- nfdump
  - This is the **analysis** tool, that enables up to query the netflow data

Setting up Netflow

- Install fprobe and nfdump

```
apt-get update
apt-get install fprobe
apt-get install nfdump
```

- Make fprobe export all traffic on eth0 as netflow to collector (running localy on port 555)

```
fprobe -i eth0 localhost:555
```

- Collect the netflow data on port 555 and write it to the disk

```
Mkdir netflow
nfcapd -D -p 555 -S 1 -z -I Linux-Host-1-eth0 -l /root/netflow/
```

Netflow from pcap

- Netflow traffic can be extracted from full packet capture using nfpcapd

```
nfpcapd –r dmp.pcap –S 1 –z –l /root/netflow/
```

Looking into Netflow

- To read the content of a specific nfdump file:

```
nfdump -r nfcapd.xxxxxxxxxx
```

- Or you could have nfdump read a whole directory

```
nfdump -R /root/netflow/*
```

- You can apply filters on the netflow output

```
nfdump -R /root/netflow/* 'host 192.168.65.133'
```

Looking into Netflow

- You can have netflow combine the unidirectional flow

```
nfdump -R netflow/* -B
```

- You can also have netflow provide you with statistical aggregation
- The following will for example give the ip address consuming most traffic in the flow

```
nfdump -R netflow/* -s ip/bytes
```

- The following will aggregate the flows by source ip, order by bytes and limit the flows displayed to 10

```
nfdump -R netflow/* -A srcip -O bytes -c 10
```

Segmentation and network devices

Core network equipment

- Switch, Router

End systems

- Servers
- Clients

Other hardware

- Firewall
- VPN concentrator
- Netflow collector
- Sensors (IDS, full packet capture etc.)

Mandatory start-up

A midsize company requires a redesign of their network

Start with a clean slate, and create a network consisting of the following:

- 1 web server facing the www
- 1 web server for internal tools
- 1 database server
- 1 file server
- 1 sales team (~50 hosts) requiring internet access and access to local file server
- 1 technical support team (~10 hosts) requiring access to internal tools and web
- 1 development team (~10 hosts) they should have access to all systems, and have their own dev environment, consisting of a clone of the 4 servers above.
- Wifi setup for company access requiring only internet access

Mandatory start-up

- Create a network diagram with all the components that you need (not vendor specifik)
- Define the IPs for the subnets and devices
- Add the security devices you find necessary (firewalls, sensors, vpns)
- Write about your considerations (~ 1 page)

- Consider limited resources, and that we do not have all the storage in the world for storing full packet capture

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

Netflow

- https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/ios-netflow/prod_white_paper0900aecd80406232.html

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