NETVÆRKS- OG KOMMUNIKATIONSSIKKERHED

Segmentation and NetFlow

Agenda

- Challenge
- External visit
- Netflow and packet captures
- Hand-inn exercise
- (IDS)

Challenge (decrypt)

- We obtained a cookie file possibly containing important information. Try to recover that information!!

- Download the file “cookie-secret.txt”
  - http://139.59.130.103/cookie-secret.txt

- Find the plaintext values of the content of the file.

- Scope: Only the cookie file (not the server)

Traffic capturing options

- Full Packet Capture
  - Dumping all traffic

- Session data
  - Only gathering info about the traffic

- Packet Strings
  - Dumping Application level headers

Full packet capture

- Takes huge amount of space
- Privacy issues

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

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

- Chapter 5 in the book ANSM describes different retention options (by size or by date)

Full packet capture

- netsniff-ng can also be used for FPC

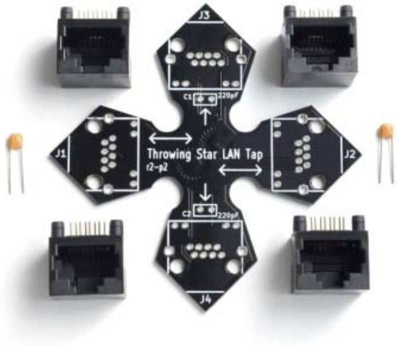
- The following uses netssniff-ng to capture the packets from eth0

```
netsniff-ng –i eth0 –o /sniffs/ -F 60
```

- -i: sniff interface
- -o: output directory
- -F: number of seconds before file rotation

How to actually collect data

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

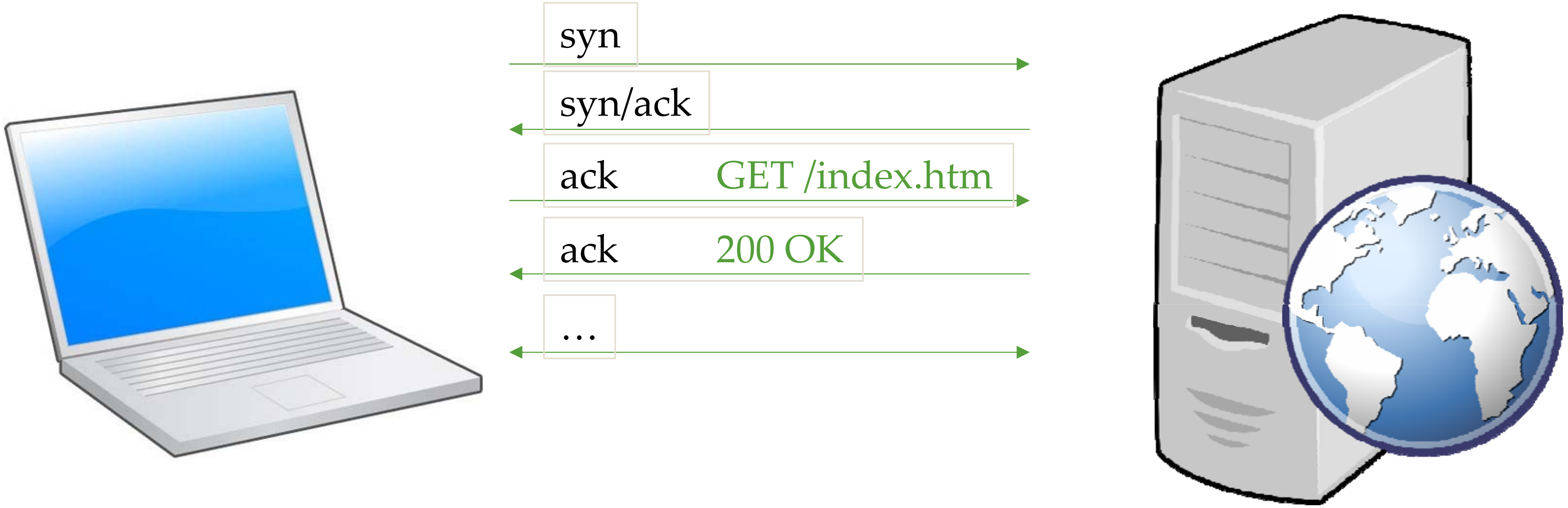


- Mirroring the port on the switch (SPAN)
  - Pros: Allready availiable if the switch supports it. No downtime
  - Cons: Can be a problem if collecting more data than the port speed

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



```
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

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.)

Hand-inn start-up

A small size 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
- 2 database servers (for each webserver)
- 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 5 servers above.
- Wifi setup for company access requiring only internet access

Hand-inn start-up

- Create a network diagram with all the components that you need (not vendor specific)
- 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

- Preferably work in groups (2-3 persons)

Further material

Netflow

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