Communication and Network Security exercises

Henrik Kramselund
xhek@kea.dk

May 6, 2024

Note: exercises marked with ⚠ are considered important. These contain subjects that are essential for the course and curriculum. Even if you don't work through the exercise, you are expected to know the subjects covered by these.

Exercises marked with ℹ are considered optional. These contain subjects that are related to the course and curriculum. You may want to browse these and if interested work through them. They may require more time than we have available during the course.

Contents

Preface

This material is prepared for use in Communication and Network Security workshop and was prepared by Henrik Kramselund , http://www.zencurity.com . It describes the networking setup and applications for trainings and workshops where hands-on exercises are needed.

Further a presentation is used which is available as PDF from kramse@Github
Look for communication-and-network-security-exercisesin the repo security-courses.

These exercises are expected to be performed in a training setting with network connected systems. The exercises use a number of tools which can be copied and reused after training. A lot is described about setting up your workstation in the repo

https://github.com/kramse/kramse-labs

Prerequisites

This material expect that participants have a working knowledge of TCP/IP from a user perspective. Basic concepts such as web site addresses and email should be known as well as IP-addresses and common protocols like DHCP.

Have fun and learn

Introduction to networking

IP - Internet protocol suite

It is extremely important to have a working knowledge about IP to implement secure and robust infrastructures. Knowing about the alternatives while doing implementation will allow the selection of the best features.

ISO/OSI reference model

A very famous model used for describing networking is the ISO/OSI model of networking which describes layering of network protocols in stacks.

This model divides the problem of communicating into layers which can then solve the problem as smaller individual problems and the solution later combined to provide networking.

Having layering has proven also in real life to be helpful, for instance replacing older hardware technologies with new and more efficient technologies without changing the upper layers.

In the picture the OSI reference model is shown along side with the Internet Protocol suite model which can also be considered to have different layers.

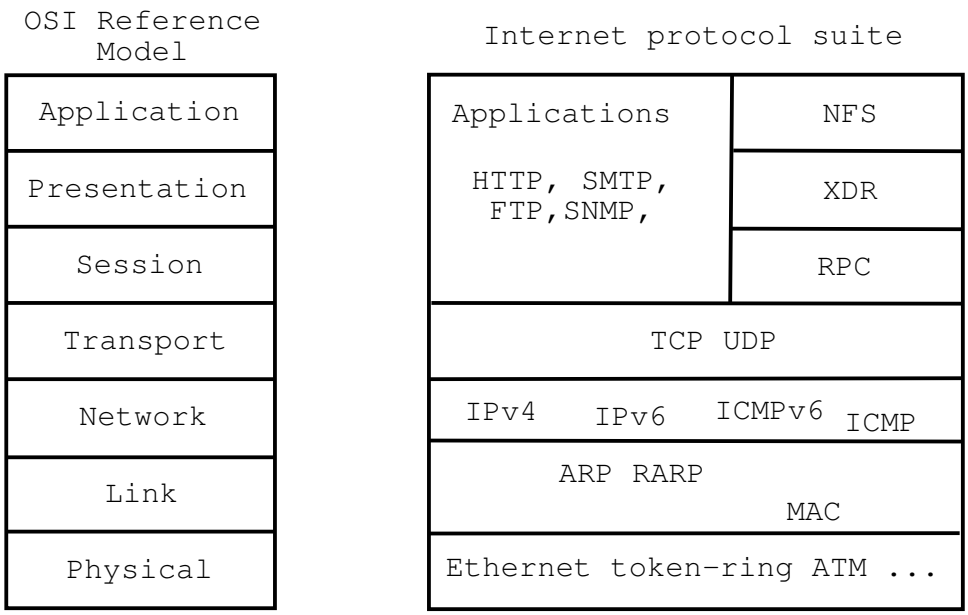


Figure 1: OSI og Internet Protocol suite

Exercise content

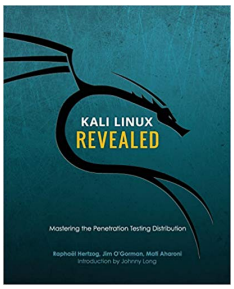
Most exercises follow the same procedure and has the following content:

- **Objective:** What is the exercise about, the objective
- **Purpose:** What is to be the expected outcome and goal of doing this exercise
- **Suggested method:** suggest a way to get started
- **Hints:** one or more hints and tips or even description how to do the actual exercises
- **Solution:** one possible solution is specified
- **Discussion:** Further things to note about the exercises, things to remember and discuss

Please note that the method and contents are similar to real life scenarios and does not detail every step of doing the exercises. Entering commands directly from a book only teaches typing, while the exercises are designed to help you become able to learn and actually research solutions.

Exercise 1

⚠ Download Kali Linux Revealed (KLR) Book 10 min



Kali Linux Revealed Mastering the Penetration Testing Distribution

Objective:
We need a Kali Linux for running tools during the course. This is open source, and the developers have released a whole book about running Kali Linux.

This is named Kali Linux Revealed (KLR)

Purpose:
We need to install Kali Linux in a few moments, so better have the instructions ready.

Suggested method:
Create folders for educational materials. Download PDF from: https://kali.training/

Direct link to PDF: https://kali.training/downloads/Kali-Linux-Revealed-1st-edition.pdf

Solution:
When you have a directory structure for download for this course, and the book KLR in PDF you are done.

Discussion:
Linux is free and everywhere. The tools we will run in this course are made for Unix, so they run great on Linux.

Kali Linux is a free pentesting platform, and probably worth more than $10.000

The book KLR is free, but you can buy/donate, and I recommend it.

Exercise 2

⚠ Check your Kali VM, run Kali Linux 30 min

Objective:
Make sure your virtual machine is in working order.

We need a Kali Linux for running tools during the course.

Purpose:
If your VM is not installed and updated we will run into trouble later.

Suggested method:
Go to https://github.com/kramse/kramse-labs/

Read the instructions for the setup of a Kali VM.

Hints:
If you allocate enough memory and disk you wont have problems.

Solution:
When you have a updated virtualisation software and Kali Linux, then we are good.

Discussion:
Linux is free and everywhere. The tools we will run in this course are made for Unix, so they run great on Linux.

Kali Linux includes many hacker tools and should be known by anyone working in infosec.

Exercise 3

ℹ Download Debian Administrators Handbook (DEB) Book 10 min

Objective:
We need a Linux for running some tools during the course. I have chosen Debian Linux as this is open source, and the developers have released a whole book about running it.

This book is named The Debian Administrators Handbook, - shortened DEB

Purpose:
We need to install Debian Linux in a few moments, so better have the instructions ready.

Suggested method:
Create folders for educational materials. Go to download from the link `https://debian-handbook.info/` Read and follow the instructions for downloading the book.

Solution:
When you have a directory structure for download for this course, and the book DEB in PDF you are done.

Discussion:
Linux is free and everywhere. The tools we will run in this course are made for Unix, so they run great on Linux.

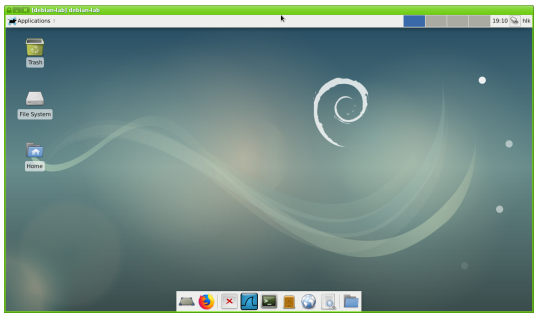
Debian Linux is a free operating system platform.

The book DEB is free, but you can buy/donate to Debian, and I recommend it.

Not curriculum but explains how to use Debian Linux

Exercise 4

ℹ Check your Debian VM 10 min



Objective:
Make sure your virtual machine is in working order.

We need a Debian Linux for running tools during the course.

Purpose:
If your VM is not installed and updated we will run into trouble later.

Suggested method:
Go to https://github.com/kramse/kramse-labs/

Read the instructions for the setup of a Debian VM.

This is a bonus exercise - only one Debian is needed per team.

Hints:
If you allocate enough memory and disk you wont have problems.

I suggest 50G disk, 2CPU cores and 6Gb memory for this course, if you have this.

Solution:
When you have a updated virtualisation software and a running VM, then we are good.

Discussion:
Linux is free and everywhere. The tools we will run in this course are made for Unix, so they run great on Linux.

Debian Linux allows us to run Ansible and provision a whole SIEM in very few minutes.

Exercise 5

❶ Investigate /etc 10 min

Objective:
We will investigate the /etc directory on Linux. We need a Debian Linux

Purpose:
Start seeing example configuration files, including:

- User database `/etc/passwd` and `/etc/group`
- The password database `/etc/shadow`

Suggested method:
Boot your Linux VMs, log in

Investigate permissions for the user database files `passwd` and `shadow`

Hints:
Linux has many tools for viewing files, the most efficient would be less.

```
user@debian:~$ cd /etc
user@debian:/etc$ ls -l shadow passwd
-rw-r--r-- 1 root root   2203 Mar 26 17:27 passwd
-rw-r----- 1 root shadow 1250 Mar 26 17:27 shadow
user@debian:/etc$ ls
... all files and directories shown, investigate more if you like
```

Showing a single file: `less /etc/passwd` and press q to quit

Showing multiple files: `less /etc/*` then :n for next and q for quit

```
Trying reading the shadow file as your regular user:
user@debian:/etc$ cat /etc/shadow
cat: /etc/shadow: Permission denied
```

Why is that? Try switching to root, using su or sudo, and redo the command.

Solution:
When you have seen the most basic files you are done.

Also note the difference between running as root and normal user. Usually books and instructions will use a prompt of hash mark `#` when the root user is assumed and dollar sign `$` when a normal user prompt.

Discussion:
Linux is free and everywhere. The tools we will run in this course are made for Unix, so they run great on Linux.

Sudo is a tool often used for allowing users to perform certain tasks as the super user. The tool is named from superuser do! https://en.wikipedia.org/wiki/Sudo

Exercise 6

⚠ Enable firewall - 15min

Objective:
Turn on a firewall and configure a few simple rules.

Purpose:
See how easy it is to restrict incoming connections to a server.

Suggested method:
Install a utility for firewall configuration.

You should also perform Nmap port scan with the firewall enabled and disabled.

Hints:
Using the ufw package it is very easy to configure the firewall on Linux.

Install and configuration can be done using these commands.

```
root@debian01:~# apt install ufw
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  ufw
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 164 kB of archives.
After this operation, 848 kB of additional disk space will be used.
Get:1 http://mirrors.dotsrc.org/debian stretch/main amd64 ufw all 0.35-4 [164 kB]
Fetched 164 kB in 2s (60.2 kB/s)
...
root@debian01:~# ufw allow 22/tcp
Rules updated
Rules updated (v6)
root@debian01:~# ufw enable
Command may disrupt existing ssh connections. Proceed with operation (y|n)? y
Firewall is active and enabled on system startup
root@debian01:~# ufw status numbered
Status: active

     To                         Action      From
     --                         ------      ----
[ 1] 22/tcp                     ALLOW IN    Anywhere
[ 2] 22/tcp (v6)                ALLOW IN    Anywhere (v6)
```

Also allow port 80/tcp and port 443/tcp - and install a web server. Recommend Nginx `apt-get install nginx`

Solution:
When firewall is enabled and you can still connect to Secure Shell (SSH) and web service, you are done.

Discussion:
Further configuration would often require adding source prefixes which are allowed to connect to specific services. If this was a database server the database service should probably not be reachable from all of the Internet.

Web interfaces also exist, but are more suited for a centralized firewall.

Configuration of this firewall can be done using ansible, see the documentation and examples at `https://docs.ansible.com/ansible/latest/modules/ufw_module.html`

Should you have both a centralized firewall in front of servers, and local firewall on each server? Discuss within your team.

Exercise 7

⚠ Git tutorials - 15min

Objective:
Try the program Git locally on your workstation

Purpose:
Running Git will allow you to clone repositories from others easily. This is a great way to get new software packages, and share your own.

Git is the name of the tool, and Github is a popular site for hosting git repositories.

Suggested method:
Run the program from your Linux VM. You can also clone from your Windows or Mac OS X computer. Multiple graphical front-end programs exist too.

Most important are Git clone and pull:

```
user@Projects:tt$ git clone https://github.com/kramse/kramse-labs.git
Cloning into 'kramse-labs'...
remote: Enumerating objects: 283, done.
remote: Total 283 (delta 0), reused 0 (delta 0), pack-reused 283
Receiving objects: 100% (283/283), 215.04 KiB | 898.00 KiB/s, done.
Resolving deltas: 100% (145/145), done.

user@Projects:tt$ cd kramse-labs/

user@Projects:kramse-labs$ ls
LICENSE  README.md  core-net-lab  lab-network  suricatazeek  work-station
user@Projects:kramse-labs$ git pull
Already up to date.
```

Hints:
Browse the Git tutorials on https://git-scm.com/docs/gittutorial
and https://guides.github.com/activities/hello-world/

We will not do the whole tutorials within 15 minutes, but get an idea of the command line, and see examples. Refer back to these tutorials when needed or do them at home.

Note: you don't need an account on Github to download/clone repositories, but having an acccount allows you to save repositories yourself and is recommended.

Solution:
When you have tried the tool and seen the tutorials you are done.

Discussion:
Before Git there has been a range of version control systems,
see https://en.wikipedia.org/wiki/Version_control for more details.

Exercise 8

ℹ Use Ansible to install Elastic Stack

Objective:
Install and run Elasticsearch with additional programs – the elastic stack. Previously named ELK stack after Elasticsearch, Logstash and Kibana.

Warning: This may become a bit long and we have other options.
If you are not prepared to do a lot of work. On the other hand, this could be used as the basis for a production setup. YMMV.

Purpose:
See an example tool used for many projects, Elasticsearch from the Elastic Stack

Suggested method:
We will run Elasticsearch, either using the method from:
`https://www.elastic.co/guide/en/elastic-stack-get-started/current/get-started-elastic-stack.html`

or by the method described below using Ansible - your choice.

Ansible used below is a configuration management tool `https://www.ansible.com/` and you can adjust them for production use!

I try to test my playbooks using both Ubuntu and Debian Linux, but Debian is the main target for this training.

First make sure your system is updated, as root run:

```
apt-get update && apt-get -y upgrade && apt-get -y dist-upgrade
```

You should reboot if the kernel is upgraded :-)

Second make sure your system has ansible and my playbooks: (as root run)

```
apt -y install ansible git python
git clone https://github.com/kramse/kramse-labs
```

We will run the playbooks locally, while a normal Ansible setup would use SSH to connect to the remote node.

Then it should be easy to run Ansible playbooks, like this: (again as root, most packet sniffing things will need root too later)

```
cd kramse-labs/suricatazeek
ansible-playbook -v 1-dependencies.yml 2-suricatazeek.yml 3-elasticstack.yml 4-configuration.yml
```

Note: I keep these playbooks flat and simple, but you should investigate Ansible roles for real deployments.

If I update these, it might be necessary to update your copy of the playbooks. Run this while you are in the cloned repository:

```
git pull
```

Note: usually I would recommend running git clone as your personal user, and then use sudo command to run some commands as root. In a training environment it is OK if you want to run everything as root. Just beware.

Note: these instructions are originally from the course
Go to `https://github.com/kramse/kramse-labs/tree/master/suricatazeek`

Hints:

Ansible is great for automating stuff, so by running the playbooks we can get a whole lot of programs installed, files modified - avoiding the Vi editor ☺

Example playbook content, installing software using APT:

```
apt:
    name: "{{ packages }}"
    vars:
      packages:
        - nmap
        - curl
        - iperf
        ...
```

Solution:

When you have a updated VM and Ansible running, then we are good.

Discussion:

Linux is free and everywhere. The tools we will run in this course are made for Unix, so they run great on Linux.

Exercise 9

❶ Configure Elasticsearch Security

Objective:
Configure the security settings for Elastic stack – mainly Kibana and Elasticsearch communication.

Purpose:
Getting access to dashboards and logging data should only be allowed for security administrators.

Suggested method:
When starting Kibana there is a small popup which guide you to the minimal setup. There are multiple steps and require some Linux/unix knowledge to perform them all. There is no requirement to perform this, if you are new to Unix and Elasticsearch, but make a mental note that it is available.

Currently:
https://www.elastic.co/guide/en/elasticsearch/reference/7.17/security-minimal-setup.html

Two settings are needed for elasticsearch
On every node in your cluster, add the xpack.security.enabled setting to the `/etc/elasticsearch/elasticsearch.y` file and set the value to true, change from false to true:

```
xpack.security.enabled: true
```

and at the bottom add:

```
discovery.type: single-node
```

Then restart the elasticsearch service using `service elasticsearch restart`

Afterwards generate random passwords using:

```
/usr/share/elasticsearch/bin/elasticsearch-setup-passwords auto
```

This will print a number of passwords, which should be saved in a text file!

Two actions are needed for kibana
Add the elasticsearch.username setting to the file `/etc/kibana/kibana.yml` and set the value to the `kibana_system` user:

```
elasticsearch.username: "kibana_system"
```

Add the password for the `kibana_system` user to the Kibana keystore:

```
# /usr/share/kibana/bin/kibana-keystore create
# /usr/share/kibana/bin/kibana-keystore add elasticsearch.password
```

Then restart the kibana service using `service kibana restart`

Log in to Kibana as the elastic user.

Congratulate yourself if this works, good job.
You enabled password protection for your local cluster to prevent unauthorized access. You can log in to Kibana securely as the elastic user and create additional users and roles.

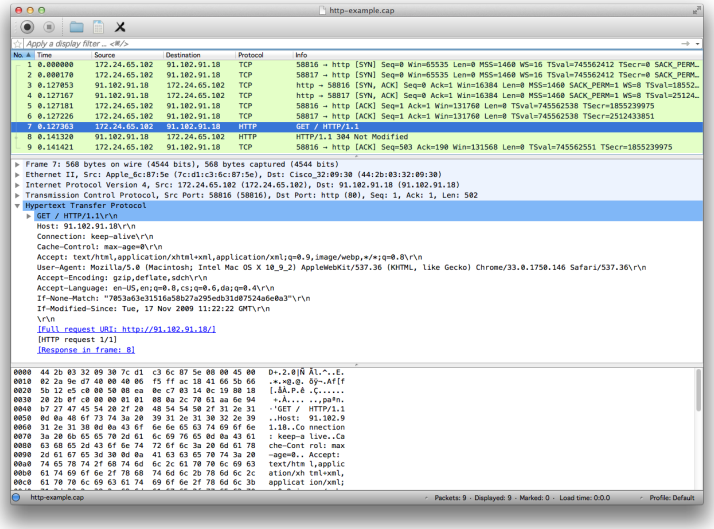
Hints:
You should be able to change a few lines of configuration using an editor, but for production use it is recommended to use Ansible or some other configuration management.

Solution:
When you have read the instructions, and understood that Elastic stack includes some security settings, available and highly recommended for production use, you are done.

Discussion:
We could have added these settings and commands to Ansible playbooks, but since it is something that must be done differently in production clusters I considered it a good exercise.

Exercise 10

⚠ Wireshark and Tcpdump 15 min



Objective:
Try the program Wireshark locally your workstation, or tcpdump

You can run Wireshark on your host too, if you want.

Purpose:
Installing Wireshark will allow you to analyse packets and protocols

Tcpdump is a feature included in many operating systems and devices to allow packet capture and saving network traffic into files.

Suggested method:
Run Wireshark or tcpdump from your Kali Linux

The PPA book page 41 describes Your First Packet Capture.

Hints:
PCAP is a packet capture library allowing you to read packets from the network. Tcpdump uses libpcap library to read packet from the network cards and save them. Wireshark is a graphical application to allow you to browse through traffic, packets and protocols.

Both tools are already on your Kali Linux, or do: `apt-get install tcpdump wireshark`

Solution:
When Wireshark is installed sniff some packets. We will be working with both live traffic and saved packets from files in this course.

If you want to capture packets as a non-root user on Debian, then use the command to add a Wireshark group:

```
sudo dpkg-reconfigure wireshark-common
```


and add your user to this:

```
sudo gpasswd -a $USER wireshark
```

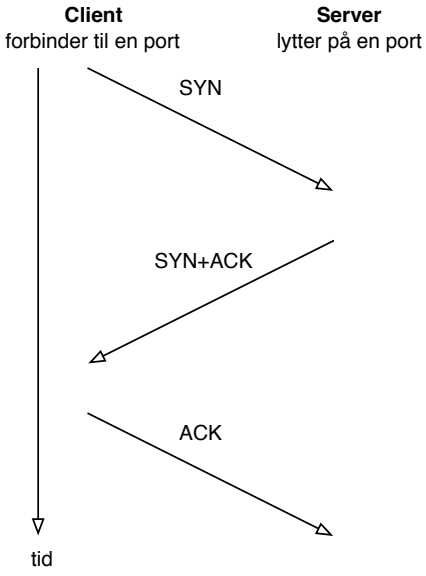
Dont forget to logout/login to pick up this new group.

Discussion:
Wireshark is just an example other packet analyzers exist, some commercial and some open source like Wireshark

We can download a lot of packet traces from around the internet, we might use examples from https://old.zeek.org/community/traces.html

Exercise 11

⚠ Capturing TCP Session packets 10 min



Objective:
Sniff TCP packets and dissect them using Wireshark

Purpose:
See real network traffic, also know that a lot of information is available and not encrypted.

Note the three way handshake between hosts running TCP. You can either use a browser or command line tools like cURL while capturing

```
curl http://www.zencurity.com
```

Suggested method:
Open Wireshark and start a capture
Then in another window execute the ping program while sniffing

or perform a Telnet connection while capturing data

Hints:
When running on Linux the network cards are usually named eth0 for the first Ethernet and wlan0 for the first Wireless network card. In Windows the names of the network cards are long and if you cannot see which cards to use then try them one by one.

Solution:
When you have collected some TCP sessions you are done.

Discussion: Is it ethical to collect packets from an open wireless network?

Also note the TTL values in packets from different operating systems

Exercise 12

⚠ Whois databases 15 min

Objective:
Learn to lookup data in the global Whois databases

Purpose:
We often need to see where traffic is coming from, or who is responsible for the IP addresses sending attacks.

Suggested method:
Use a built-in command line, like: `host www.zencurity.dk` to look up an IP address and then `whois` with the IP address.

Hints:
Another option is to use web sites for doing Whois lookups https://apps.db.ripe.net/db-web-ui/#/query or their RIPEStat web site which can give even more information https://stat.ripe.net/

Solution:
When you can find our external address and look it up, you are done.

Discussion:
Whois databases are global and used for multiple purposes, the ones run by the Regional Internet Registries ARIN, RIPE, AfriNIC, LACNIC og APNIC have information about IP addresses and AS numbers allocated.

Exercise 13

⚠ IP address research 30 min

Objective:
Work with IP addresses

Purpose:
What is an IP address?

Investigate the following IP addresses

- 192.168.1.1
- 192.0.2.0/24
- 172.25.0.1
- 182.129.62.63
- 185.129.62.63

Write down everything you can about them!

Suggested method:
Search for the addresses, look for web sites that may help.

Hints:
Download the fun guide from Julia Evans (b0rk) `https://jvns.ca/networking-zine.pdf`

Pay attention to Notation Time page

Lookup `ripe.net` they may have a service called stats or stat – something like that.

What is the Torproject? good, bad, neutral?

Solution:
When you have found some information about each of the above, say 2-3 facts about each you are done.

Discussion:
IP addresses are much more than an integer used for addressing system interfaces and routing packets.

We will later talk more about IP reputation

Exercise 14

⚠ Using ping and traceroute 10 min

Objective:
Be able to do initial debugging of network problems using commands ping and traceroute

Purpose:
Being able to verify connectivity is a basic skill.

Suggested method:
Use `ping` and `traceroute` to test your network connection - can be done one Windows and UNIX.

Hints:

```
$ ping 10.0.42.1
PING 10.0.42.1 (10.0.42.1) 56(84) bytes of data.
64 bytes from 10.0.42.1: icmp_seq=1 ttl=62 time=1.02 ms
64 bytes from 10.0.42.1: icmp_seq=2 ttl=62 time=0.998 ms
^C
--- 10.0.42.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 0.998/1.012/1.027/0.034 ms
```

Dont forget that UNIX ping continues by default, press ctrl-c to break.

Do the same with traceroute.

Solution:
Run both programs to local gateway and some internet address by your own choice.

Discussion:
Note the tool is called tracert on Windows, shortened for some reason.

ICMP is the Internet Control Message Protocol, usually used for errors like host unreachable. The ECHO request ICMP message is the only ICMP message that generates another.

The traceroute programs send packets with low Time To Live (TTL) and receives ICMP messages, unless there is a problem or a firewall/filter. Also used for mapping networks.

ℹ

Whats the difference between:

- **traceroute** and **traceroute -I**
- NB: traceroute -I is found on UNIX - traceroute using ICMP pakker
- Windows tracert by default uses ICMP
- Unix by default uses UDP, but can use ICMP instead.
- Lots of traceroute-like programs exist for tracing with TCP or other protocols

Exercise 15

⚠ DNS and Name Lookups 10 min

Objective:
Be able to do DNS lookups from specific DNS server

Purpose:
Try doing DNS lookup using different programs

Suggested method:
Try the following programs:

- nslookup - UNIX and Windows, but not recommended
  `nslookup -q=txt -class=CHAOS version.bind. 0`
- dig - syntax @server domain query-type query-class
  `dig @8.8.8.8 www.example.com`
- host - syntaks host [-l] [-v] [-w] [-r] [-d] [-t querytype] [-a] host [server]
  `host www.example.com 8.8.8.8`

Hints:
Dig is the one used by most DNS admins, I often prefer the host command for the short output.

Solution:
Shown inline, above.

Discussion:
The nslookup program does not use the same method for lookup as the standard lookup libraries, results may differ from what applications see.

What is a zone transfer, can you get one using the host command?

Explain forward and reverse DNS lookup.

Exercise 16

⚠ Nping check ports 10 min

Objective:
Show the use of Nping tool for checking ports through a network

Purpose:
Nping can check if probes can reach through a network, reporting success of failure. Allows very specific packets to be sent. It is part of the Nmap package.

Suggested method:
Run the command using a common port like Web HTTP:

```
root@KaliVM:~# nping --tcp -p 80 www.zencurity.com

Starting Nping 0.7.70 ( https://nmap.org/nping ) at 2018-09-07 19:06 CEST
SENT (0.0300s) TCP 10.137.0.24:3805 > 185.129.60.130:80 S ttl=64 id=18933 iplen=40  seq=2984847972 win=1480
RCVD (0.0353s) TCP 185.129.60.130:80 > 10.137.0.24:3805 SA ttl=56 id=49674 iplen=44  seq=3654597698 win=16384 <mss
SENT (1.0305s) TCP 10.137.0.24:3805 > 185.129.60.130:80 S ttl=64 id=18933 iplen=40  seq=2984847972 win=1480
RCVD (1.0391s) TCP 185.129.60.130:80 > 10.137.0.24:3805 SA ttl=56 id=50237 iplen=44  seq=2347926491 win=16384 <mss
SENT (2.0325s) TCP 10.137.0.24:3805 > 185.129.60.130:80 S ttl=64 id=18933 iplen=40  seq=2984847972 win=1480
RCVD (2.0724s) TCP 185.129.60.130:80 > 10.137.0.24:3805 SA ttl=56 id=9842 iplen=44  seq=2355974413 win=16384 <mss 1
SENT (3.0340s) TCP 10.137.0.24:3805 > 185.129.60.130:80 S ttl=64 id=18933 iplen=40  seq=2984847972 win=1480
RCVD (3.0387s) TCP 185.129.60.130:80 > 10.137.0.24:3805 SA ttl=56 id=1836 iplen=44  seq=3230085295 win=16384 <mss 1
SENT (4.0362s) TCP 10.137.0.24:3805 > 185.129.60.130:80 S ttl=64 id=18933 iplen=40  seq=2984847972 win=1480
RCVD (4.0549s) TCP 185.129.60.130:80 > 10.137.0.24:3805 SA ttl=56 id=62226 iplen=44  seq=3033492220 win=16384 <mss

Max rtt: 40.044ms | Min rtt: 4.677ms | Avg rtt: 15.398ms
Raw packets sent: 5 (200B) | Rcvd: 5 (220B) | Lost: 0 (0.00%)
Nping done: 1 IP address pinged in 4.07 seconds
```

Hints:
A lot of options are similar to Nmap

Solution:
When you have tried it towards an open port, a closed port and an IP/port that is filtered you are done.

Discussion:
A colleague of ours had problems sending specific IPsec packets through a provider. Using a tool like Nping it is possible to show what happens, or where things are blocked.

Things like changing the TTL may provoke ICMP messages, like this:

```
root@KaliVM:~# nping --tcp -p 80 --ttl 3 www.zencurity.com

Starting Nping 0.7.70 ( https://nmap.org/nping ) at 2018-09-07 19:08 CEST
SENT (0.0303s) TCP 10.137.0.24:37244 > 185.129.60.130:80 S ttl=3 id=60780 iplen=40  seq=1997801125 win=1480
RCVD (0.0331s) ICMP [10.50.43.225 > 10.137.0.24 TTL=0 during transit (type=11/code=0) ] IP [ttl=62 id=28456 iplen=
SENT (1.0314s) TCP 10.137.0.24:37244 > 185.129.60.130:80 S ttl=3 id=60780 iplen=40  seq=1997801125 win=1480
RCVD (1.0337s) ICMP [10.50.43.225 > 10.137.0.24 TTL=0 during transit (type=11/code=0) ] IP [ttl=62 id=28550 iplen=
SENT (2.0330s) TCP 10.137.0.24:37244 > 185.129.60.130:80 S ttl=3 id=60780 iplen=40  seq=1997801125 win=1480
RCVD (2.0364s) ICMP [10.50.43.225 > 10.137.0.24 TTL=0 during transit (type=11/code=0) ] IP [ttl=62 id=28589 iplen=
SENT (3.0346s) TCP 10.137.0.24:37244 > 185.129.60.130:80 S ttl=3 id=60780 iplen=40  seq=1997801125 win=1480
RCVD (3.0733s) ICMP [10.50.43.225 > 10.137.0.24 TTL=0 during transit (type=11/code=0) ] IP [ttl=62 id=29403 iplen=
SENT (4.0366s) TCP 10.137.0.24:37244 > 185.129.60.130:80 S ttl=3 id=60780 iplen=40  seq=1997801125 win=1480
RCVD (4.0558s) ICMP [10.50.43.225 > 10.137.0.24 TTL=0 during transit (type=11/code=0) ] IP [ttl=62 id=30235 iplen=

Max rtt: 38.574ms | Min rtt: 2.248ms | Avg rtt: 13.143ms
Raw packets sent: 5 (200B) | Rcvd: 5 (360B) | Lost: 0 (0.00%)
Nping done: 1 IP address pinged in 4.07 seconds
```

Exercise 17

❶ Try pcap-diff 15 min

Objective:
Try both getting an utility tool from Github and running an actual useful tool for comparing packet captures.

Purpose:
Being able to get tools and scripts from Github makes you more effective.

The tool we need today is https://github.com/isginf/pcap-diff

Suggested method:
Git clone the repository, follow instructions for running a packet diff.

Try saving a few packets in a packet capture, then using tcpdump read and write a subset - so you end up with two packet captures:

```
sudo tcpdump -w icmp-dump.cap
// run ping in another window, which probably creates ARP packets
// Check using tcpdump
sudo tcpdump -r icmp-dump.cap arp
reading from file icmp-dump.cap, link-type EN10MB (Ethernet)
10:06:18.077055 ARP, Request who-has 10.137.0.22 tell 10.137.0.6, length 28
10:06:18.077064 ARP, Reply 10.137.0.22 is-at 00:16:3e:5e:6c:00 (oui Unknown), length 28
10:06:24.776987 ARP, Request who-has 10.137.0.6 tell 10.137.0.22, length 28
10:06:24.777107 ARP, Reply 10.137.0.6 is-at fe:ff:ff:ff:ff:ff (oui Unknown), length 28
// Write the dump - but without the ARP packets:
sudo tcpdump -r icmp-dump.cap -w icmp-dump-no-arp.cap not arp
```

With these pcaps you should be able to do:

```
sudo pip install scapy
git clone https://github.com/isginf/pcap-diff.git
cd pcap-diff/

$ python pcap_diff.py -i ../icmp-dump.cap -i ../icmp-dump-no-arp.cap -o diff.cap
Reading file ../icmp-dump.cap:
Found 23 packets

Reading file ../icmp-dump-no-arp.cap:
Found 19 packets

Diffing packets:

Found 2 different packets

Writing diff.cap
// Try reading the output packet diff:

$ sudo tcpdump -r diff.cap
reading from file diff.cap, link-type EN10MB (Ethernet)
10:06:24.777107 ARP, Reply 10.137.0.6 is-at fe:ff:ff:ff:ff:ff (oui Unknown), length 28
10:06:24.776987 ARP, Request who-has 10.137.0.6 tell 10.137.0.22, length 28
```

Note: I ran these on a Debian, so I needed the sudo, if you run this on Kali there is no need to use

sudo.

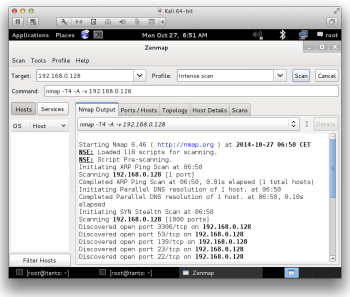
Hints:
Git is one of the most popular software development tools, and Github is a very popular site for sharing open source tools.

Solution:
When you or your team mate has a running pcap-diff then you are done

Discussion:
I often find that 90% of my tasks can be done using existing open source tools.

Exercise 18

⚠ Discover active systems ping sweep 10 min



Objective:
Use nmap to discover active systems

Purpose:
Know how to use nmap to scan networks for active systems.

Suggested method:

Due to python version 2 being deprecated there are some missing files for running the tool Zenmap. This can be fixed by using the Kali Kaboxer `apt install zenmap-kbx`

Process is described in various posts around the internet. https://www.kali.org/blog/introducing-kaboxer/

The command to run Zenmap becomes: `zenmap-kbx`
As always try typing zen and press TAB twice, will show all commands starting with these letters.

Try different scans,

- Ping sweep to find active systems
- Port sweeps to find active systems with specific ports

Hints:
Try nmap in sweep mode - and you may run this from Zenmap

Solution:
Use the command below as examples:

- Ping sweep `nmap -sP 10.0.45.*`
- Port sweeps `nmap -p 80 10.0.45.*`

Discussion:
Quick scans quickly reveal interesting hosts, ports and services

Also now make sure you understand difference between single host scan 10.0.45.123/32, a whole subnet /24 250 hosts 10.0.45.0/24 and other more advanced targeteting like 10.0.45.0/25 and 10.0.45.1-10

Exercise 19

⚠ Execute nmap TCP and UDP port scan 20 min

Objective:
Use nmap to discover important open ports on active systems

Purpose:
Finding open ports will allow you to find vulnerabilities on these ports.

Suggested method:
Use `nmap -p 1-1024 server` to scan the first 1024 TCP ports and use Nmap without ports. What is scanned then?

Try to use `nmap -sU` to scan using UDP ports, not really possible if a firewall is in place.

If a firewall blocks ICMP you might need to add `-Pn` to make nmap scan even if there are no Ping responses

Hints:
Sample command: `nmap -Pn -sU -p1-1024 server` UDP port scanning 1024 ports without doing a Ping first

Solution:
Discover some active systems and most interesting ports, which are 1-1024 and the built-in list of popular ports.

Discussion:
There is a lot of documentation about the nmap portscanner, even a book by the author of nmap. Make sure to visit http://www.nmap.org

TCP and UDP is very different when scanning. TCP is connection/flow oriented and requires a handshake which is very easy to identify. UDP does not have a handshake and most applications will not respond to probes from nmap. If there is no firewall the operating system will respond to UDP probes on closed ports - and the ones that do not respond must be open.

When doing UDP scan on the internet you will almost never get a response, so you cannot tell open (not responding services) from blocked ports (firewall drop packets). Instead try using specific service programs for the services, sample program could be `nsping` which sends DNS packets, and will often get a response from a DNS server running on UDP port 53.

Exercise 20

⚠ Perform nmap OS detection 10 min

Objective:
Use nmap OS detection and see if you can guess the brand of devices on the network

Purpose:
Getting the operating system of a system will allow you to focus your next attacks.

Suggested method:
Look at the list of active systems, or do a ping sweep.

Then add the OS detection using the option `-O`

Hints:
The nmap tool can send a lot of packets that will get different responses, depending on the operating system. TCP/IP is implemented using various constants chosen by the implementors, they have chosen different standard packet TTL etc.

Solution:
Use a command like `nmap -O -p1-100 10.0.45.45` or `nmap -A -p1-100 10.0.45.45`

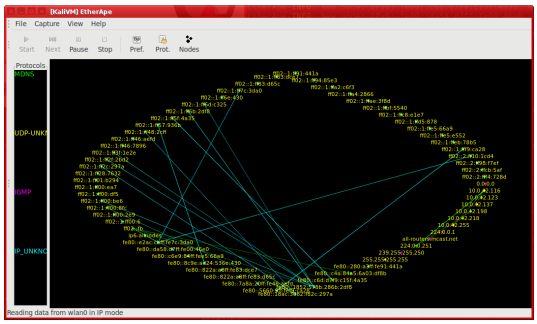
Discussion:
Nmap OS detection is not a full proof way of knowing the actual operating system, but in most cases in can detect the family and in some cases it can identify the exact patch level of the system.

Better to use `-A` all the time, includes even more scripts and advanced stuff You can also save prefixes to scan in a text file, I usually name it `targets`

I also recommend adding `-oA` for writing output files. So a regular Nmap command might be: `nmap -p 1-65535 -A -oA full-tcp-scan -iL targets`

Exercise 21

ℹ EtherApe 10 min



> EtherApe is a graphical network monitor for Unix modeled after etherman. Featuring link layer, IP and TCP modes, it displays network activity graphically. Hosts and links change in size with traffic. Color coded protocols display. Node statistics can be exported.

Objective:
Use a tool to see more about network traffic, whats going on in a network.

Purpose:
Get to know the concept of a node by seeing nodes communicate in a graphical environment.

Suggested method:
Use the tool from Kali

The main page for the tool is: https://etherape.sourceforge.io/

Hints:
Your built-in Wi-Fi network card may not be the best for sniffing in promiscious and monitor mode.

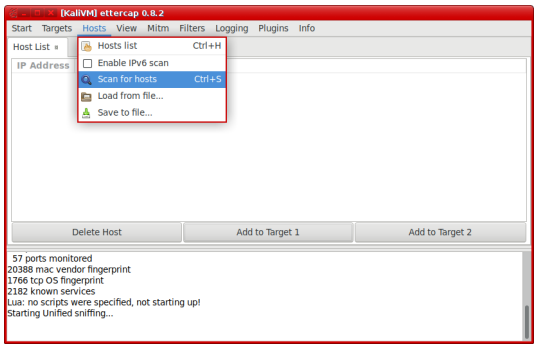
Put your network card for the virtual system into bridging mode, and produce some data using Nmap ping scanning. Something like this for your local network `nmap -sP 192.168.0.0/24`

Solution:
When you have the tool running and showing data, you are done.

Discussion:

Exercise 22

❶ ARP spoofing and ettercap 20min



Objective:
Use a tool to see more about network traffic, whats going on in a network.

Purpose:
Start the tool, do a scan and start sniffing between your laptop and the router.

Suggested method:

1. Start the tool using `ettercap --gtk` to get the graphical version.
2. Select menu Info, Help - and read about unified and bridged sniffing.
3. Start Unified sniffing from Sniff, Unified sniffing - select your network card.
4. Select Hosts - Scan

You should be able to see some hosts. Then the next step would be to initiate attacks - which are menu-driven and easy to perform.

You might ruin the network temporarily for others when playing with this, so be cautious.

Hints:
We might be messing to much with the traffic, so attacks wont succeed. Some coordination is needed.

Solution:
When you can scan for hosts and realize how easy that was, you are done.

Discussion:
How many admins know about ARP spoofing, ARP poisoning?

Exercise 23

❶ TCP SYN flooding 30min

Objective:
Start a webserver attack using SYN flooding tool hping3.

Purpose:
See how easy it is to produce packets on a network using hacker programs.

The tool we will use is very flexible and can produce ICMP, UDP and TCP using very few options. This tool is my primary one for doing professsional DDoS testing.

```
-1 --icmp
       ICMP  mode,  by  default  hping3  will  send  ICMP echo-request, you can set other ICMP
       type/code using --icmptype --icmpcode options.

-2 --udp
       UDP mode, by default hping3 will send udp to target host's port 0.  UDP header  tunable
       options are the following: --baseport, --destport, --keep.
```

TCP mode is default, so no option needed.

Suggested method:
Connect to the LAB network using Ethernet! Borrow a USB network card if you dont have one.

Start your Kali VM in bridged mode, try a basic TCP flooding attack against the server provided by the instructor, or your own Debian server.

Try doing the most common attacks TCP SYN flood using hping3:

```
hping3 --flood -p 80 -S 10.0.45.12
```

You should see something like this:

```
HPING 10.0.45.12: NO FLAGS are set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 10.0.45.12 hping statistic ---
352339 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

You can try different ports with TCP flooding, try port 22/tcp or HTTP(S) port 80/tcp and 443/tcp

Hints:
The tool we use can do a lot of different things, and you can control the speed. You can measure at the server being attacked or what you are sending, commonly using ifpps or such programs can help.

By changing the speed we can find out how much traffic is needed to bring down a service. This measurement can then be re-checked later and see if improvements really worked.

This allows you to use the tool to test devices and find the breaking point, which is more interesting than if you can overload, because you always can.


```
-i --interval
       Wait  the  specified  number  of  seconds or micro seconds between sending each packet.
       --interval X set wait to X seconds, --interval uX set wait to X micro seconds.  The de
       fault  is  to  wait one second between each packet. Using hping3 to transfer files tune
       this option is really important in order to increase transfer rate. Even  using  hping3
       to  perform  idle/spoofing  scanning  you should tune this option, see HPING3-HOWTO for
       more information.

--fast Alias for -i u10000. Hping will send 10 packets for second.

--faster
       Alias for -i u1. Faster then --fast ;) (but not as fast as your computer can send pack
       ets due to the signal-driven design).

--flood
       Sent  packets  as fast as possible, without taking care to show incoming replies.  This
       is ways faster than to specify the -i u0 option.
```

Solution:

When your team has sent +1 million packets per second into the network, from one or two laptops - you are done.

Discussion:

Gigabit Ethernet can send up to 1.4 million packets per second, pps.

There is a presentation about DDoS protection with low level technical measures to implement at https://github.com/kramse/security-courses/tree/master/presentations/network/introduction-ddos-testing

Receiving systems, and those en route to the service, should be checked for resources like CPU load, bandwidth, logging. Logging can also overload the logging infrastructure, so take care when configuring this in your own networks.

Exercise 24

ℹ TCP other flooding 15min

Objective:
Start a webserver attack using TCP flooding tool hping3.

Purpose:
Run various other common attacks

TCP mode is default, so no option needed.

Suggested method:
Connect to the LAB network using Ethernet! Borrow a USB network card if you dont have one.

Start your Kali VM in bridged mode, try a basic TCP flooding attack against the server provided by the instructor, or your own Debian server.

```
hping3 --flood -p 80 -R 10.0.45.12
```

You should see something like this:

```
HPING 10.0.45.12: NO FLAGS are set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 10.0.45.12 hping statistic ---
352339 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Hints:
Common attacks use the SYN, as shown in previous exercise, but other popular TCP attacks are RST, PUSH, URG, FIN, ACK attacks - setting one or more flags in the packets.

```
-L  --setack     set TCP ack
-F  --fin        set FIN flag
-S  --syn        set SYN flag
-R  --rst        set RST flag
-P  --push       set PUSH flag
-A  --ack        set ACK flag
-U  --urg        set URG flag
-X  --xmas       set X unused flag (0x40)
-Y  --ymas       set Y unused flag (0x80)
```

Solution:
When your team has sent +1 million packets per second into the network, from one or two laptops - you are done.

Discussion:
If an attacker varies the packets they can be harder to filter out, and the attacks succeed.

Exercise 25

❶ UDP flooding NTP, etc. 15min

Objective:
Start a webserver attack using UDP flooding tool hping3.

Purpose:
See how easy it is to produce packets on a network using hacker programs.

The tool we will use is very flexible and can produce ICMP, UDP and TCP using very few options. This tool is my primary one for doing professsional DDoS testing.

This time we will select UDP mode:

```
-2 --udp
       UDP mode, by default hping3 will send udp to target host's port 0.  UDP header  tunable
       options are the following: --baseport, --destport, --keep.
```

Suggested method:
Connect to the LAB network using Ethernet! Borrow a USB network card if you dont have one.

Start your Kali VM in bridged mode, try a basic TCP flooding attack against the server provided by the instructor, or your own Debian server.

```
hping3 --flood -2 -p 53 10.0.45.12
```

Hints:

Try doing the most common attacks:

- UDP flooding, try port 53/udp DNS, 123/udp NTP and port 161/udp SNMP

Solution:
When your team has sent +1 million packets per second into the network, from one or two laptops - you are done.

Discussion:
Many networks don't send and receive a lot of UDP traffic. If you measure a baseline of the protocols needed on a daily basis you might be able to configure a profile for normal usage, and filter out bad traffic in case of attacks.

A starting point might be to allow full bandwidth for TCP, 10% UDP and 1% ICMP. This will ensure that even if an attacker is sending more than 1% ICMP only a fraction reaches your network and systems.

This is especially effective for protocols like ICMP which is not used for large data transfers.

Exercise 26

❶ ICMP flooding 15min

Objective:
Start a webserver attack using ICMP flooding tool hping3.

Purpose:
See how easy it is to produce packets on a network using hacker programs.

The tool we will use is very flexible and can produce ICMP, UDP and TCP using very few options. This tool is my primary one for doing professsional DDoS testing.

This time we will select UDP mode:

```
-1 --icmp
       ICMP  mode,  by  default  hping3  will  send  ICMP echo-request, you can set other ICMP
       type/code using --icmptype --icmpcode options.
```

Suggested method:
Connect to the LAB network using Ethernet! Borrow a USB network card if you dont have one.

Start your Kali VM in bridged mode, try a basic TCP flooding attack against the server provided by the instructor, or your own Debian server.

Try doing the most common attack:

- ICMP flooding with echo

```
hping3 --flood -1 10.0.45.12
```

Hints:
Common attacks use ICMP ECHO, but other types can be sent in the packets.

```
ICMP
  -C  --icmptype   icmp type (default echo request)
  -K  --icmpcode   icmp code (default 0)
      --force-icmp send all icmp types (default send only supported types)
      --icmp-gw    set gateway address for ICMP redirect (default 0.0.0.0)
      --icmp-ts    Alias for --icmp --icmptype 13 (ICMP timestamp)
      --icmp-addr  Alias for --icmp --icmptype 17 (ICMP address subnet mask)
      --icmp-help  display help for others icmp options
```

Solution:
When your team has sent +1 million packets per second into the network, from one or two laptops - you are done.

Discussion:
If you have a 10G network connection, do you REALLY need 10Gbps of ICMP traffic?

Probably not, and routers can often filter this in wirespeed.

Routers have extensive Class-of-Service (CoS) tools today and a starting point might be as shown in Juniper Junos policer config:

```
term limit-icmp {
    from {
        protocol icmp;
    }
    then {
        policer ICMP-100M;
        accept;
    }
}
term limit-udp {
    from {
        protocol udp;
    }
    then {
        policer UDP-1000M;
        accept;
    }
}
```

This effectively limit the damage an attacker can do. Your firewall and IDS devices will be free to spend more processing on the remaining protocols.

Exercise 27

❶ Misc - stranger attacks 15min

Various other attacks are possible, sending illegal combinations of flags etc.

Objective:
Start a webserver attack using the packet generator and flooding tool t50.

Purpose:
See how easy it is to produce packets on a network using hacker programs.

The tool we will use is very flexible and can produce ICMP, UDP and TCP using very few options. This tool is another primary one for doing professsional DDoS testing.

Apart from TCP,UDP and ICMP this tool can also produce packets for dynamic routing testting, OSPF, EIGRP and other esoteric RSVP, IPSEC, RIP and GRE.

```
  $ t50 -help
  T50 Experimental Mixed Packet Injector Tool v5.8.3
  Originally created by Nelson Brito <nbrito@sekure.org>
  Previously maintained by Fernando Mercês <fernando@mentebinaria.com.br>
  Maintained by Frederico Lamberti Pissarra <fredericopissarra@gmail.com>

  Usage: t50 <host[/cidr]> [options]
  Common Options:
      --threshold NUM           Threshold of packets to send     (default 1000)
      --flood                   This option supersedes the 'threshold'
      --encapsulated            Encapsulated protocol (GRE)      (default OFF)
   -B,--bogus-csum              Bogus checksum                   (default OFF)
      --shuffle                 Shuffling for T50 protocol       (default OFF)
   -q,--quiet                   Disable INFOs
      --turbo                   Extend the performance           (default OFF)
   -l,--list-protocols          List all available protocols
   -v,--version                 Print version and exit
   -h,--help                    Display this help and exit
...
   Some considerations while running this program:
    1. There is no limitation of using as many options as possible.
    2. Report t50 bugs at https://gitlab.com/fredericopissarra/t50.git.
    3. Some header fields with default values MUST be set to '0' for RANDOM.
    4. Mandatory arguments to long options are mandatory for short options too.
    5. Be nice when using t50, the author DENIES its use for DoS/DDoS purposes.
    6. Running t50 with '--protocol T50' option sends ALL protocols sequentially.
```

Suggested method:
Connect to the LAB network using Ethernet! Borrow a USB network card if you dont have one.

Start your Kali VM in bridged mode, try a basic TCP flooding attack against the server provided by the instructor, or your own Debian server.

Run the help page, and browse options.

```
t50 -h
```

Hints:

The tools we use can do a lot of different things and using the command line options can produce high speed packet attacks without having to program in C ourselves.

Try doing a special attack:

- t50 with '–protocol T50' option sends ALL protocols, so try:
  `t50 --protocol T50 10.0.45.12`

Solution:
When your team has sent +1 million packets per second into the network, from one or two laptops - you are done.

Discussion:
Gigabit Ethernet can send up to 1.4 million packets per second, pps.

There is a presentation about DDoS protection with low level technical measures to implement at
https://github.com/kramse/security-courses/tree/master/presentations/network/introduction-ddos-testing

Receiving systems, and those en route to the service, should be checked for resources like CPU load, bandwidth, logging. Logging can also overload the logging infrastructure, so take care when configuring this in your own networks.

Exercise 28

⚠ Perform nmap service scan 10 min

Objective:
Use more advanced features in Nmap to discover services.

Purpose:
Getting more intimate with the system will allow more precise discovery of the vulnerabilities and also allow you to select the next tools to run.

Suggested method:
Use `nmap -A` option for enabling service detection and scripts

Hints:
Look into the manual page of nmap or the web site book about nmap scanning

Solution:
Run nmap and get results.

Notice how the output changes if you enable/disable the firewall on the system under test. Nmap tries to report open, filtered and closed in a sensible way. So if most ports are filtered and scanning 100 ports it might say 98 filtered, 1 open and 1 close for instance.

Discussion:
Some services will show software versions allowing an attacker easy lookup at web sites to known vulnerabilities and often exploits that will have a high probability of success.

Make sure you know the difference between a vulnerability which is discovered, but not really there, a false positive, and a vulnerability not found due to limitations in the testing tool/method, a false negative.

A sample false positive might be reporting that a Windows server has a vulnerability that you know only to exist in Unix systems.

Exercise 29

⚠ SSH scanners - 15min

Objective:
Try ssh scanners, similar to sslscan and Nmap sshscan

Purpose:
We often need to find older systems with old settings.

Suggested method:
Use Nmap with built-in scripts for getting the authentication settings from SSH servers

Hints:
Nmap includes lots of scripts, look into the directory on Kali:

```
$ ls /usr/share/nmap/scripts/*ssh*
/usr/share/nmap/scripts/ssh2-enum-algos.nse   /usr/share/nmap/scripts/ssh-publickey-acceptance.nse
/usr/share/nmap/scripts/ssh-auth-methods.nse  /usr/share/nmap/scripts/ssh-run.nse
/usr/share/nmap/scripts/ssh-brute.nse       /usr/share/nmap/scripts/sshv1.nse
/usr/share/nmap/scripts/ssh-hostkey.nse

$ sudo nmap -A -p 22 --script "ssh2-enum-algos,ssh-auth-methods" 10.0.45.2
Starting Nmap 7.80 ( https://nmap.org ) at 2020-02-20 08:46 CET
Nmap scan report for 10.0.42.6
Host is up (0.0038s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     Cisco/3com IPSSHd 6.6.0 (protocol 2.0)
| ssh-auth-methods:
|   Supported authentication methods:
|     publickey
|_    password
| ssh2-enum-algos:
|   kex_algorithms: (1)
|       diffie-hellman-group1-sha1
|   server_host_key_algorithms: (1)
|       ssh-dss
|   encryption_algorithms: (6)
|       aes128-cbc
|       aes192-cbc
|       aes256-cbc
|       blowfish-cbc
|       cast128-cbc
|       3des-cbc
|   mac_algorithms: (4)
|       hmac-sha1
|       hmac-sha1-96
|       hmac-md5
|       hmac-md5-96
|   compression_algorithms: (1)
|_      none
```

Solution:
When you have tried running against one or two SSH servers, you are done.

Discussion:
I recommend disabling password login on systems connected to the internet.

Having only public key authentication reduces or even removes the possibility for brute force attacks succeeding.

I also move the service to a random high port, which then requires an attacker must perform port scan to find it - more work.

Thus a better and more modern OpenSSH would look like this:

```
PORT      STATE SERVICE VERSION
4xxxx/tcp open  ssh     OpenSSH 7.9 (protocol 2.0)
| ssh-auth-methods:
|   Supported authentication methods:
|     publickey
| ssh2-enum-algos:
|   kex_algorithms: (4)
|       curve25519-sha256@libssh.org
|       diffie-hellman-group16-sha512
|       diffie-hellman-group18-sha512
|       diffie-hellman-group14-sha256
|   server_host_key_algorithms: (4)
|       rsa-sha2-512
|       rsa-sha2-256
|       ssh-rsa
|       ssh-ed25519
|   encryption_algorithms: (6)
|       chacha20-poly1305@openssh.com
|       aes128-ctr
|       aes192-ctr
|       aes256-ctr
|       aes128-gcm@openssh.com
|       aes256-gcm@openssh.com
|   mac_algorithms: (3)
|       umac-128-etm@openssh.com
|       hmac-sha2-256-etm@openssh.com
|       hmac-sha2-512-etm@openssh.com
|   compression_algorithms: (2)
|       none
|_      zlib@openssh.com
```


Exercise 30

❶ Configure SSH keys for more secure access

Objective:
See how SSH keys can be used.

Purpose:
Secure Shell is a very powerful administration tool. Administrators use this for managing systems. If an attacker gains access they can perform the same tasks.

Using SSH keys for access and disabling password based logins effectively prevents brute-force login attacks from succeeding.

Suggested method:
First generate a SSH key, use:

```
$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Created directory '/root/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/hlk/.ssh/id_rsa.
Your public key has been saved in /home/hlk/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:15esp66lQArFOlXqOoHnxpg8zRS6shK8nx9KGf+oSp4 root@debian01
The key's randomart image is:
+---[RSA 2048]----+
|      .          |
|   . o           |
|   .=            |
| ..=.      o .   |
|o.*o. . S o +    |
|oB==+o   . o     |
|+*B=.o.   o .    |
|=++.o +. o o     |
|oEo=oo .ooo      |
+----[SHA256]-----+
```

Then use the utility tool `ssh-copy-id` for copying the public key to the server. Install tool if not available using `apt` :

```
hlk@kunoichi:hlk$ ssh-copy-id -i /home/hlk/.ssh/id_rsa hlk@10.0.42.147
/usr/local/bin/ssh-copy-id: INFO: Source of key(s) to be installed: ".ssh/kramse.pub"
The authenticity of host '10.0.42.147 (10.0.42.147)' can't be established.
ECDSA key fingerprint is SHA256:DP6jqadDWEJW/3FYPY84cpTKmEW7XoQ4zDNf/RdTu6M.
Are you sure you want to continue connecting (yes/no)? yes
/usr/local/bin/ssh-copy-id: INFO: attempting to log in with the new key(s),
to filter out any that are already installed
```

```
/usr/local/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you
are prompted now it is to install the new keys
hlk@10.0.42.147's password:

Number of key(s) added:        1

Now try logging into the machine, with:   "ssh -o 'IdentitiesOnly yes' 'hlk@10.0.42.147'"
and check to make sure that only the key(s) you wanted were added.
```

This is the best tool for the job!

The public must exist in the `authorized_keys` file, in the right directory, with the correct permissions ... use `ssh-copy-id`

Hints:
You can publish the public part of your SSH keys in places such as Github and Ubuntu installation can fetch this during install, making the use of SSH keys extremely easy.

Solution:
When you can login using key you are done.

Discussion:
We have not discussed using passphrase on the key, neither how to turn off password based logins by reconfiguring the SSH daemon. This is left as an exercise for the reader.

Exercise 31

⚠ Nmap full scan - strategy 15 min

Objective:
Write down your Nmap strategy, and if needed create your own Nmap profile in Zenmap.

Purpose:
Doing a port scan often requires you to run multiple Nmap scans.

Suggested method:
Use Zenmap to do:

1. A few quick scans, to get web servers and start web scanners/crawlers
2. Full scan of all TCP ports, -p 1-65535
3. Full or limited UDP scan, `nmap -sU --top-ports 100`
4. Specialized scans, like specific source ports

Hints:
Using a specific source ports using -g/–source-port <portnum>: Use given port number with ports like FTP 20, DNS 53 can sometimes get around router filters and other stateless Access Control Lists

Solution:
Run nmap and get results.

Discussion:
Recommendation it is highly recommended to always use:

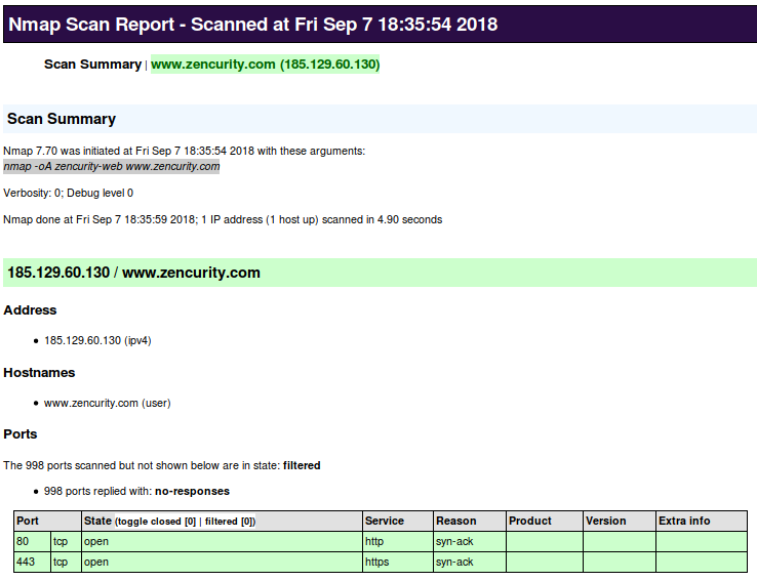
```
-iL <inputfilename>: Input from list of hosts/networks
-oA outputbasename: output in all formats, see later
```

Some examples of real life Nmaps I have run recently:

```
dns-scan: nmap -sU -p 53 --script=dns-recursion -iL targets -oA dns-recursive
bgpscan: nmap -A -p 179 -oA bgpscan -iL targets
dns-recursive: nmap -sU -p 53 --script=dns-recursion -iL targets -oA dns-recursive
php-scan: nmap -sV --script=http-php-version -p80,443 -oA php-scan -iL targets
scan-vtep-tcp: nmap -A -p 1-65535 -oA scan-vtep-tcp 185.129.60.77 185.129.60.78
snmp-10.x.y.0.gnmap: nmap -sV -A -p 161 -sU --script=snmp-info -oA snmp-10xy 10.x.y.0/19
snmpscan: nmap -sU -p 161 -oA snmpscan --script=snmp-interfaces -iL targets
sshscan: nmap -A -p 22 -oA sshscan -iL targets
vncscan: nmap -A -p 5900-5905 -oA vncscan -iL targets
```

Exercise 32

❶ Reporting HTML 15 min



Nmap Scan Report - Scanned at Fri Sep 7 18:35:54 2018

Scan Summary | www.zencurity.com (185.129.60.130)

Scan Summary

Nmap 7.70 was initiated at Fri Sep 7 18:35:54 2018 with these arguments:
nmap -oA zencurity-web www.zencurity.com

Verbosity: 0; Debug level 0

Nmap done at Fri Sep 7 18:35:59 2018; 1 IP address (1 host up) scanned in 4.90 seconds

185.129.60.130 / www.zencurity.com

Address

- 185.129.60.130 (ipv4)

Hostnames

- www.zencurity.com (user)

Ports

The 998 ports scanned but not shown below are in state: **filtered**

- 998 ports replied with: **no-responses**

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
80	tcp	open	http	syn-ack			
443	tcp	open	https	syn-ack			

Objective:
Show the use of XML output and convert to HTML

Purpose:
Reporting data is very important. Using the oA option Nmap can export data in three formats easily, each have their use. They are normal, XML, and grepable formats at once.

Suggested method:
First run Nmap, with output, then process it

```
sudo nmap -oA zencurity-web www.zencurity.com
xsltproc zencurity-web.xml > zencurity-web.html
```

Hints:
Nmap includes the stylesheet in XML and makes it very easy to create HTML.

If the tool `xsltproc` is not installed, then install it: `apt-get install xsltproc`

Solution:
Run XML through xsltproc, command line XSLT processor, or another tool

Discussion:
Options you can use to change defaults:

```
--stylesheet <path/URL>: XSL stylesheet to transform XML output to HTML
--webxml: Reference stylesheet from Nmap.Org for more portable XML
```

Also check out the Ndiff tool

```
hlk@cornerstone03:~$ ndiff zencurity-web.xml zencurity-web-2.xml
-Nmap 7.70 scan initiated Fri Sep 07 18:35:54 2018 as: nmap -oA zencurity-web www.zencurity.com
+Nmap 7.70 scan initiated Fri Sep 07 18:46:01 2018 as: nmap -oA zencurity-web-2 www.zencurity.com

 www.zencurity.com (185.129.60.130):
 PORT    STATE SERVICE VERSION
+443/tcp open  https
```

(I ran a scan, removed a port from the first XML file and re-scanned)

Exercise 33

⚠ SSL/TLS scanners 15 min

Objective:
Try the Online Qualys SSLLabs scanner https://www.ssllabs.com/ Try the command line tool sslscan checking servers - can check both HTTPS and non-HTTPS protocols!

Purpose:
Learn how to efficiently check TLS settings on remote services.

Suggested method:
Run the tool against a couple of sites of your choice.

```
root@kali:~# sslscan --ssl2 www.kramse.dk
Version: 1.10.5-static
OpenSSL 1.0.2e-dev xx XXX xxxx

Testing SSL server www.kramse.dk on port 443
...
  SSL Certificate:
Signature Algorithm: sha256WithRSAEncryption
RSA Key Strength:    2048

Subject:  *.kramse.dk
Altnames: DNS:*.kramse.dk, DNS:kramse.dk
Issuer:   AlphaSSL CA - SHA256 - G2
```

Also run it without `--ssl2` and against SMTPTLS if possible.

Hints:
Originally sslscan is from http://www.titania.co.uk but use the version on Kali, install with apt if not installed.

Solution:
When you can run and understand what the tool does, you are done.

Discussion:
SSLscan can check your own sites, while Qualys SSLLabs only can test from hostname

Exercise 34

⚠ Internet scanners 15 min

Objective:
Try the Online scanners https://internet.nl/ and a few more.

Purpose:
Learn how to efficiently check settings on remote services.

Suggested method:
There are multiple portals and testing services which allow you to checck a domain, mail settings or web site.

Run tools against a couple of sites of your choice.

- `https://internet.nl/` Generic checker
- `https://www.hardenize.com/` Generic checker
- `https://www.wormly.com/test_ssl` Test TLS
- `https://observatory.mozilla.org/` Web site headers check
- `https://dnsviz.net/` DNS zone check
- `https://rpki.cloudflare.com/` Check RPKI - route validator enter IP address
  More information about this: `https://labs.ripe.net/author/nathalie_nathalie/rpki-test/`

Others exist, feel free to suggest some.

Hints:

Solution:
When you can run and understand what at least one tool does, you are done.

Discussion:
Which settings are most important, which settings are your responsebility?

Exercise 35

ℹ Nginx as a Transport Layer Security (TLS) endpoint 40 min

Objective:
Read how to configure Nginx with TLS locally on your workstation This is a longer exercise. Feel free to complete this exercise at home.

Purpose:
Web services with TLS is a requirement in many circumstances. Unfortunately having TLS enabled requires both certificates, settings and large software packages like OpenSSL. A lot of vulnerabilities have been found in these and updating them may prove hard.

Having a centralized entry where TLS is served to the internet may help you.

Suggested method:
Run the programs from your Debian Linux VM, use `apt install nginx` if not already installed.

Follow a guide like the one from Nginx:
`http://nginx.org/en/docs/http/configuring_https_servers.html`

Check using sslscan if your site is working, and configured according to best current practice.

Hints:
Note: above link does NOT show how to generate certificates and keys, so you need to find this yourself. A good place would be at certificate providers, search for Nginx CSR Certificate Signing Request – just dont order certificates.

A full blown tutorial from Digital Ocean:
https://www.digitalocean.com/community/tutorials/how-to-create-a-self-signed-ssl-certificate-for-nginx-on-debian-10

My kramse-labs also includes some example configs, check with `git pull`

Solution:
When you have configured an instance of Nginx you are done.

Discussion:
A great document about Transport Layer Security (TLS) is available from the web site of NCSC in the Netherlands:
`https://english.ncsc.nl/publications/publications/2021/january/19/it-security-guidelines-for-transport-layer-security-2.1`

Dont forget to add the recommended HTTP Strict Transport Security header to your configuration, if your site is in production.

`https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html`

A regular production site could also benefit from Lets Encrypt certificates updated automatically using one of the many clients available. Try searching for Lets Encrypt and Nginx.

Exercise 36

⚠ Nginx logging 20 min

Objective:
See the common log format used by web servers.

`https://en.wikipedia.org/wiki/Common_Log_Format`

Purpose:
Knowing that a common format exist, allow you to choose between multiple log processors.

Suggested method:
Run Nginx on your Debian Linux VM and then check the logs.

```
# cd /var/log/nginx
# ls
# less access.log
# less error.log
```

Produce some bad logs using Nikto or using a browser, and check `error.log`

Hints:
A lot of scanning acctivities would result in error logs, so if you observe a rise in 404 not found or similar, then maybe you are being targetted.

Solution:
When you have tried the tool and seen some data you are done.

Discussion:
I commonly recommend tools like Packetbeat and other tools from Elastic to process logs, see https://www.elastic.co/beats/packetbeat

Another popular one is Matomo formerly known as Piwik
https://matomo.org/.

Exercise 37

⚠ Nginx filtering 40 min

Objective:
See how Nginx can filter a request easily.

Purpose:
Running Nginx with a filtering configuration can protect some resource, or part of a web site from attacks.

Example configuration:

```
server {
    listen       80;
    server_name  service.dev;
    access_log   /var/log/nginx/access.log;
    error_log    /var/log/nginx/error.log debug;
    # Proxy settings
    proxy_set_header   Host $http_host;
    proxy_redirect     off;
    location / {
        # Catch all
        proxy_pass     http://127.0.0.1:81/;
    }
    location /admin/ {
        # /admin/ only
        allow 192.168.5.0/24;
        deny  all;
        proxy_pass     http://127.0.0.1:81/;
    }
}
```

Note; this does a proxy pass to another service locally, you may need to change it. Perhaps you can use another Nginx example running on port 3000.

If you use the JuiceShop running in Docker, and as a directory to disallow, perhaps the `/ftp/` one.

Suggested method:
Run the configuration from your Debian Linux VM

Hints:
My kramse-labs also includes some example configs, check with `git pull`

Having a negative list is bad, better to have a positive list of allowed requests.

Solution:
When you have tried above and seen Nginx block your request, you are done.

Discussion:
Multiple modules exist for Nginx, Apache, PHP etc. for blocking bad requests. Which one is right for your setup, you must research for yourselves.

Exercise 38

❶ Burp app and proxy - up to 30min

Objective:
Run Burp proxy.

Add a web proxy in-between your browser and the internet. We will use Burp suite which is a commercial product, in the community edition.

Purpose:
We will learn more about web applications as they are a huge part of the applications used in enterprises and on the internet. Most mobile apps are also web applications in disguise.

By inserting a web proxy we can inspect the data being sent between browsers and the application.

Suggested method:
You need to have browsers and a proxy, plus a basic knowledge of HTTP.

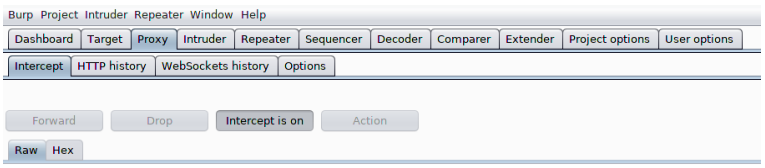
If you could install Firefox it would be great, and we will use the free version of Burp Suite, so please make sure you can run Java and download the free version plain JAR file from Portswigger from:

https://portswigger.net/burp/communitydownload

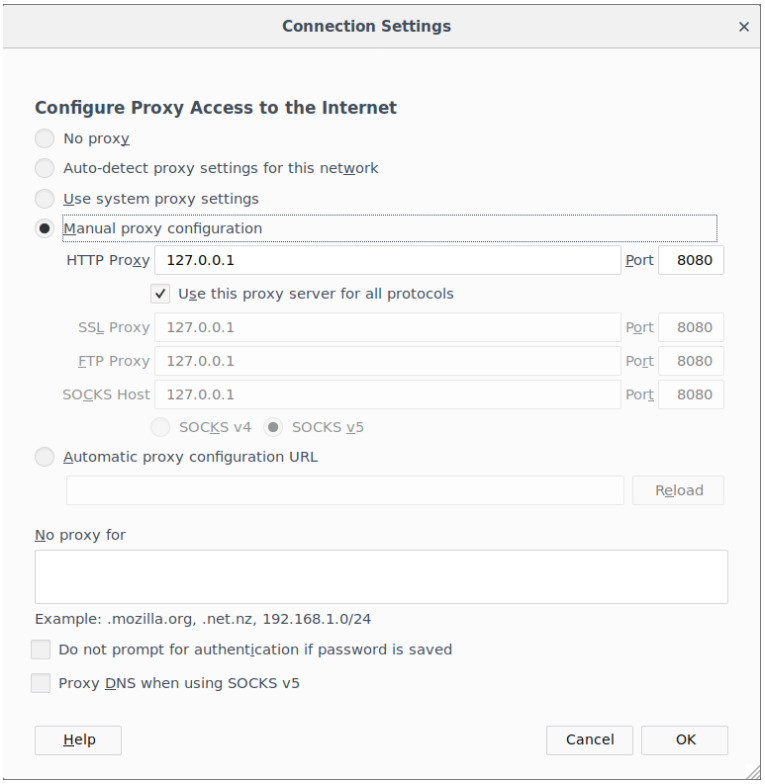
follow the Getting Started instructions at:
https://support.portswigger.net/customer/portal/articles/1816883-getting-started-with-burp-suite

Hints:
Recommend running Burp on the default address and port 127.0.0.1 port 8080.

Note: Burp by default has `intercept is on` in the Proxy tab, press the button to allow data to flow.



Then setting it as proxy in Firefox:



Solution:
When web sites and servers start popping up in the Target tab, showing the requests and responses - you are done.

Your browser will alert you when visiting TLS enabled sites, HTTPS certificates do not match, as Burp is doing a person-in-the-middle. You need to select advanced and allow this to continue.

Discussion:
Since Burp is often updated I use a small script for starting Burp which I save in `~/bin/burp` - dont forget to add to PATH and `chmod` x bin/burp+.

```
#! /bin/sh
DIRNAME=`dirname $0`
BURP=`ls -1tra $DIRNAME/burp*.jar | tail -1`
java -jar -Xmx6g $BURP &
```

Exercise 39

ℹ Burp intercept TLS - 15min

Objective:
Use Burp with HTTPS, possibly Strict Transport HSTS

Purpose:
Read about the tool burp, and lets try to run it.

Knowing how to test and debug HTTP and HTTPS is very important.

Suggested method:
Run Burp with some HTTP site, see how we can intercept.

Then move to a HTTPS site, and see how it breaks. One option is to go to burp/ download the CA certificate and then import it into your browser.

Hints:
If the site uses HSTS strict transport, your browser might already have a certificate - and it needs to be removed!

Depending on the browser Manage Certificates is the place.

Solution:
When you have intercepted some HTTPS / TLS traffic you are done

Discussion:

Exercise 40

ℹ sslstrip 15 min

Objective:
sslstrip https://moxie.org/software/sslstrip/

Purpose:
Read about the tool, and lets try to run it - on a single VM.

> This tool provides a demonstration of the HTTPS stripping attacks that I presented at Black Hat DC 2009. It will transparently hijack HTTP traffic on a network, watch for HTTPS links and redirects, then map those links into either look-alike HTTP links or homograph-similar HTTPS links. It also supports modes for supplying a favicon which looks like a lock icon, selective logging, and session denial. For more information on the attack, see the video from the presentation below.

Suggested method:
Make sure tool is installed, Then run it and intercept your own traffic from the same system.

You may run this on the wireless and try intercepting others.

Hints:
IF you are using wireless - most likely, then make sure to run on the same channel/AP/frequency. Either switch everything to 2.4GHz and have only one AP or just do the mitm on a single host - run browser and mitmproxy on the same VM.

Solution:
When you have intercepted some traffic you are done, we will spend at least 30-45 minutes doing various mitm related stuff.

Discussion:

Exercise 41

ℹ mitmproxy 30 min

Objective:
mitmproxy https://mitmproxy.org/

mitmproxy is a free and open source interactive HTTPS proxy

Purpose:
Try running a mitm attack on your phone or another laptop.

Suggested method:
Make sure tool is installed

Then use the command line interface to verify it is working, then switch to the Web interface for playing with the tool.

Hints:
IF you are using wireless - most likely, then make sure to run on the same channel/AP/frequency. Either switch everything to 2.4GHz and have only one AP or just do the mitm on a single host - run browser and mitmproxy on the same VM.

Solution:
When you have intercepted some traffic you are done, we will spend at least 30-45 minutes doing various mitm related stuff.

Discussion:

Exercise 42

ℹ sslsplit 10 min

Objective:
Read about sslsplit https://www.roe.ch/SSLsplit - transparent SSL/TLS interception system

Purpose:
This tool has a lot of features described on the home page.

> Overview
> SSLsplit is a tool for man-in-the-middle attacks against SSL/TLS encrypted network connections. It is intended to be useful for network forensics, application security analysis and penetration testing.
>
> SSLsplit is designed to transparently terminate connections that are redirected to it using a network address translation engine. SSLsplit then terminates SSL/TLS and initiates a new SSL/TLS connection to the original destination address, while logging all data transmitted. Besides NAT based operation, SSLsplit also supports static destinations and using the server name indicated by SNI as upstream destination. SSLsplit is purely a transparent proxy and cannot act as a HTTP or SOCKS proxy configured in a browser.

Suggested method:
If we were to use this tool, we would redirect traffic using "firewalls"/routers

- SSLsplit currently supports the following operating systems and NAT engines:
- FreeBSD: pf rdr and divert-to, ipfw fwd, ipfilter rdr
- OpenBSD: pf rdr-to and divert-to
- Linux: netfilter REDIRECT and TPROXY
- Mac OS X: ipfw fwd and pf rdr

We wont run this tool, but beware such tools exist

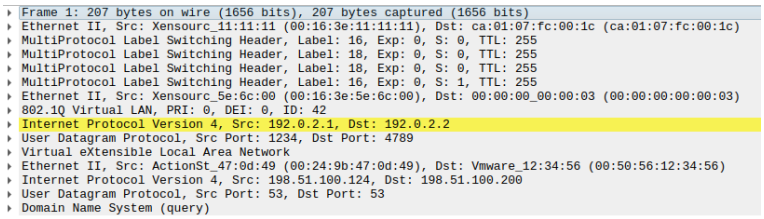
Hints:
Specifically read the section SSLsplit implements a number of defences against mechanisms - and think about the consequences to a regular user.

Solution:
When you feel you have a idea about what this tool can do then you are done.

Discussion:
Should tools like this even exist?

Exercise 43

❶ Frankenpacket - 20 min



Objective:
See an example of a tunneled and encapsulated packet

Purpose:
Show that Virtual Private Network technologies can obscure data, even if not encrypted.

Suggested method:
Look into the Github repository
https://github.com/kramse/frankenpacket

Download the repository/clone it using git

```
$ git clone https://github.com/kramse/frankenpacket.git
```

Then open the capture files in Wireshark

Hints:
These are syntetic packets, produced by Scapy - Packet crafting for Python2 and Python3
https://scapy.net/

Solution:
When you have seen that packets can be very complex, and decoding them might be hard, you are done.

Discussion:
Would all Intrusion Detection Systems be able to decode this packet?

I know Suricata can handle Virtual Extensible LAN (VXLAN), since I helped create that code.

Exercise 44

❶ Creating Frankenpackets - 15 min

Objective:
See how to craft packets using Scapy

Purpose:
Often it can help when you want to test network security to produce traffic.

Scapy is a popular tool for this.
https://scapy.net/

Suggested method:
Look into the Github repository
https://github.com/kramse/frankenpacket

Download the repository/clone it using git
`$ git clone https://github.com/kramse/frankenpacket.git`

Then run the python programs, which uses Scapy. They all start like this:

```
#!/usr/bin/python
#
###[ Loading modules ]###
import sys
import getopt
#from scapy.all import PcapReader, wrpcap, Packet, NoPayload, or just:
from scapy.all import *
```

Hints:
Scapy is a module for Python and can be installed using Pip, if not already available.

Solution:
When you have read some of the Python code you are done.

Discussion:
Scapy is not very fast, but very flexible. If you want to send fast, you can write a packet capture file and replay it.

Exercise 45

ℹ Wireguard - 60 min

Objective:
Test wireguard between two Linux servers

Purpose:
Know there is alternative to connect servers securely.

Wireguard is very easy to setup, as it requires very little configuration.

Suggested method:
Use two servers with Debian and install wireguard according to the setup on the web page.

https://www.wireguard.com/quickstart/

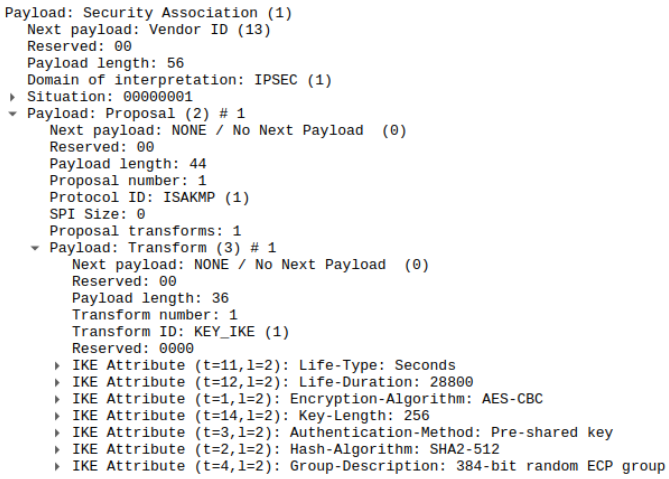
Hints:
They have a Demo Server which allows you to try out Wireguard

Solution:
When you have a working connection between them, you are done.

Discussion:
We wont do this in class, but I have a lot of friends that use Wireguard in production for complex setups.

Exercise 46

ℹ IPsec negotiation - 30-60 min



Objective:
Research how IPsec is keyed, using the Internet Key Exchange (IKE) protocol.

Purpose:
See how each end has a proposal, and they must match - completely!

Suggested method:
Download packet captures from: https://weberblog.net/ikev1-ikev2-capture/

Open them in Wireshark, and look into IKE packets.

Hints:
Johannes Weber wrote blog posts about each of these, which are linked on the web page. He is also a really nice person. In this he describes how to configure using Palo Alto and FortiGate firewall products.

Solution:
When you have found the packet shown in the picture above, you are done.

Discussion:
A common problem in IPsec is the negotiation not succeeding. The best way to debug is to have people sitting and watching the logs in each end of the tunnel. Then using a simple PSK debug each phase.

You can find a lot of packet captures from the Wireshark Wiki:
https://wiki.wireshark.org/SampleCaptures

Exercise 47

ℹ Wardriving Up to 60min

Objective:
Try putting a network card in monitor mode and sniff wireless networks.

Purpose:
See that wireless networks dont encrypt MACs addresses and other characteristics - what can be found just by turning on the radio.

Suggested method:
Insert USB wireless card, make sure your VM has USB 2.0 Hub and allow VM to control the card.

Start monitor mode - maybe card is not wlan0!:
`airmon-ng start wlan0`

Start airodump-ng:
`airodump-ng wlan0mon`

See the data

Hints:
Selecting a specific channel can be done using –channel and writing captured packets can be done using -w

Solution:
When you have an overview of nearby networks you are done.

Discussion:

Lots of information is available on the internet. One recommended site is:
http://www.aircrack-ng.org

Exercise 48

⚠ Aircrack-ng 30 min

Objective:
See the program aircrack-ng being used for cracking WEP and WPA-PSK keys.

Purpose:
Some methods previously used to protect wireless networks should not be used anymore.

Suggested method:
Get access to a WEP encrypted dump of wireless network traffic and break encryption. Get access to a WPA handshake and try cracking it.

Hints:
Kali includes the aircrack-ng program and some test data in
`/pentest/wireless/aircrack-ng/test`

Solution:
When you have cracked a network from either testdata or real nearby - our lab network.

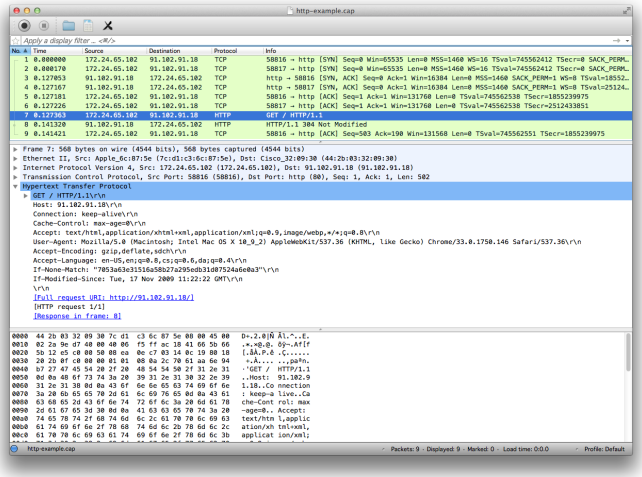
Discussion:
There is a lot of information available about aircrack-ng at the web site:
http://www.aircrack-ng.org/

Another tool available is pyrit and cpyrit which can break WPA-PSK using CUDA enabled graphic cards - instead of 100s of keys/second this may allow 10000s keys/second.

Hashcat also is able to crack WPA https://hashcat.net/hashcat/

Exercise 49

❶ PPA Chapter 10 ESPN pcap - 20min



Objective:
Open packet capture using Wireshark

Purpose:
See how a problem can be diagnosed using packets, Specifically the example Missing Web Content from page 200 in the PPA book.

Suggested method:
Using chapter 10 from the book PPA, open packet capture and go through the steps.

Note the DNS and the TCP layers, are the most interesting now.

Practical Packet Analysis - Using Wireshark to Solve Real-World Network Problems, 3rd edition 2017, Chris Sanders ISBN: 9781593278021 - shortened PPA

Hints:
The book has a web page:
https://nostarch.com/packetanalysis3/

There is a link to the packet captures:
https://nostarch.com/download/ppa3ecaptures_updated.zip

Wireshark can also show times for packets, delays - who is the slow one.

Solution:
When you have downloaded, opened and investigated the packet capture you are done.

Discussion:
Lots of different packet captures can be found on the internet. Easier than having to setup something complex first.

Exercise 50

❶ SNMP walk 15min

Objective:
Run SNMP walk on a switch, `snmpwalk` see information from device.

Lots of basic information helps defenders - AND attackers.

Purpose:
SNMP is a default management protocol used in almost any network.

Suggested method:
Run snmpwalk using community string public. Command is: `snmpwalk -v 2c -c public system`

Hints:
Community strings private and public used to be default for network devices. Today professionel devices have no SNMP configured by default, but lots of networks install the community "public" anyway.

Solution:
When you have done snmpwalk for at least one device.

Discussion:
Which part of the information is most relevant to defenders, and attackers.

Also remember on internal LAN segments, use Nmap:

```
snmp-10.x.y.0.gnmap: nmap -sV -A -p 161 -sU --script=snmp-info -oA snmp-10xy 10.x.y.0/19
snmpscan: nmap -sU -p 161 -oA snmpscan --script=snmp-interfaces -iL targets
```

Exercise 51

❶ Try Hydra brute force 30min

Objective:
Try a brute force program named hydra/Xhydra.

You decide which service to attack, SSH or SNMP are good examples.

Purpose:
Learn that some protocols allow brute forcing.

Suggested method:
Make a short list of usernames and a short list of passwords and use hydra to brute force your way into a system. Use the editor `kate`, using `kate users.txt` and `kate pass.txt` followed by a command similar to this:

```
$ hydra -V -t 1 -L users.txt -P pass.txt 10.0.45.2 ssh
```

If you want to attack SNMP try with a small list of community names: public, private, kramse, etc.

Hints:
When learning tools create a nice environment and check that things are working before trying to hack. So with brute forcing an account, create and test it!

Solution:
When you have found working credentials for at least one service, like SNMP and done SNMPwalk

Discussion:
The hydra program can brute force a lot of different protocols and also allow a lot of tuning.

The hydra program does an online brute force attack, in some cases you can get access to data like password databases, or hash values that can be cracked in off-line brute force attacks.

Exercise 52

⚠ Zeek on the web 10min

Objective:
Try Zeek Network Security Monitor - without installing it.

Purpose:
Show a couple of examples of Zeek scripting, the built-in language found in Zeek Network Security Monitor

Suggested method:
Go to `http://try.zeek.org/#/?example=hello` and try a few of the examples.

Hints:
The exercise The Summary Statistics Framework can be run with a specifc PCAP.

```
192.168.1.201 did 402 total and 2 unique DNS requests in the last 6 hours.
```

Solution:
You should read the example Raising a Notice. Getting output for certain events may be interesting to you.

Discussion:
Zeek Network Security Monitor is an old/mature tool, but can still be hard to get started using. I would suggest that you always start out using the packages available in your Ubuntu/Debian package repositories. They work, and will give a first impression of Zeek. If you later want specific features not configured into the binary packages, then install from source.

The tool was renamed in 2018 from Bro to Zeek. Some commands and files still reference the old names.

Also Zeek uses a zeekctl program to start/stop the tool, and a few config files which we should look at. From a Debian system they can be found in `/opt/zeek/etc` :

This is from the Debian 11 package, checked May 2022

`/opt/zeek/etc`:

```
root@debian-lab-11:/opt/zeek/etc# ls -la
total 24
drwxrwsr-x  3 root zeek 4096 Apr 16 20:03 .
drwxr-xr-x 10 root root 4096 Apr 16 20:03 ..
-rw-rw-r--  1 root zeek  262 Jan 28  2015 networks.cfg
-rw-rw-r--  1 root zeek  651 Jan 28  2015 node.cfg
-rw-rw-r--  1 root zeek 3052 Jan 28  2015 zeekctl.cfg
drwxr-xr-x  2 root zeek 4096 Apr 16 20:03 zkg
```

Exercise 53

⚠ Zeek DNS capturing domain names 10min

Objective:
We will now start using Zeek on our systems.

Purpose:
Try Zeek with example traffic, and see what happens.

Suggested method packet capture file:
Use Nitroba.pcap can be found in various places around the internet

Note: a dollar sign is the Linux prompt, showing the command after

```
$ bro
Error: Use of 'bro' is no longer supported. Please use 'zeek' instead.
$ cd
$ wget http://downloads.digitalcorpora.org/corpora/scenarios/2008-nitroba/nitroba.pcap
$ mkdir $HOME/zeek;cd $HOME/zeek; zeek -r ../nitroba.pcap
... Zeek reads the packets
~/zeek$ ls
conn.log  dns.log  dpd.log  files.log  http.log  packet_filter.log
sip.log  ssl.log  weird.log  x509.log
~/zeek$ less *
```

Use :n to jump to the next file in less, go through all of them.

Suggested method Live traffic:
Make sure Zeek is configured as a standalone probe and configured for the right interface. Linux used to use eth0 as the first ethernet interface, but now can use others, like ens192 or enx00249b1b2991.

```
root@debian-lab-11:/opt/zeek/etc# cat node.cfg
# Example ZeekControl node configuration.
#
# This example has a standalone node ready to go except for possibly changing
# the sniffing interface.

# This is a complete standalone configuration.  Most likely you will
# only need to change the interface.
[zeek]
type=standalone
host=localhost
interface=eth0
...
```

The interface may need to be configured differently for your installation!

Hints:
There are multiple commands for showing the interfaces and IP addresses on Linux. The old way is using `ifconfig -a` newer systems would use `ip a`

Note: if your system has a dedicated interface for capturing, you need to turn it on, make it available. This can be done manually using `ifconfig eth0 up` **Solution:**
When you either run Zeek using a packet capture or using live traffic

Running with a capture can be done using a command line such as: `zeek -r traffic.pcap`

Using zeekctl to start it would be like this:

```
// install Zeek files first
kunoichi:~ root# zeekctl
Hint: Run the zeekctl "deploy" command to get started.

Welcome to ZeekControl 1.5
Type "help" for help.

[ZeekControl] > install
removing old policies in /opt/zeek/spool/installed-scripts-do-not-touch/site ...
removing old policies in /opt/zeek/spool/installed-scripts-do-not-touch/auto ...
creating policy directories ...
installing site policies ...
generating standalone-layout.zeek ...
generating local-networks.zeek ...
generating zeekctl-config.zeek ...
generating zeekctl-config.sh ...
...

// back to zeekctl and start it
[ZeekControl] > start
starting zeek
// and then go find the logs ... one is called dns.log

root@debian-lab-11:/opt/zeek/spool/zeek# ls -l
total 100
-rw-r--r-- 1 root zeek   106 May 16 10:53 capture_loss.log
-rw-r--r-- 1 root zeek  7281 May 16 10:58 conn.log
-rw-r--r-- 1 root zeek  4998 May 16 10:54 dns.log
-rw-r--r-- 1 root zeek   491 May 16 10:54 files.log
-rw-r--r-- 1 root zeek   625 May 16 10:58 http.log
-rw-r--r-- 1 root zeek    96 May 16 10:52 known_services.log
-rw-r--r-- 1 root zeek 35370 May 16 10:52 loaded_scripts.log
-rw-r--r-- 1 root zeek   200 May 16 10:53 notice.log
-rw-r--r-- 1 root zeek    90 May 16 10:52 packet_filter.log
-rw-r--r-- 1 root zeek   541 May 16 10:52 reporter.log
-rw-r--r-- 1 root zeek   269 May 16 10:58 ssl.log
-rw-r--r-- 1 root zeek   968 May 16 10:57 stats.log
-rw-r--r-- 1 root zeek    19 May 16 10:52 stderr.log
-rw-r--r-- 1 root zeek   204 May 16 10:52 stdout.log
-rw-r--r-- 1 root zeek  1270 May 16 10:58 weird.log
root@debian-lab-11:/opt/zeek/spool/zeek#
```

You should be able to spot entries like this in the file `dns.log`:

```
#fields ts      uid     id.orig_h       id.orig_p       id.resp_h       id.resp_p       proto   trans_i
     query   qclass  qclass_name     qtype   qtype_name      rcode   rcode_name      AA      TC      RD
1538982372.416180 CD12Dc1SpQm42QW4G3 10.xxx.0.145 57476 10.x.y.141 53 udp 20383 0.045021 www.dr.dk 1 C_
v1.edgekey.net,e16198.b.akamaiedge.net,2.17.212.93 60.000000,20409.000000,20.000000 F
```

Note: this show ALL the fields captured and dissected by Zeek, there is a nice utility program zeek-cut which can select specific fields:


```
root@debian-lab-11:/opt/zeek/spool/zeek# cat dns.log | zeek-cut -d ts query answers | grep dr.dk
2018-10-08T09:06:12+0200 www.dr.dk www.dr.dk-v1.edgekey.net,e16198.b.akamaiedge.net,2.17.212.93
```

Discussion:
Why is DNS interesting?

If your Zeek installation is configured to use JSON, your output will be in JSON. What are the benefits of the original format, compared to JSON?

Exercise 54

⚠ Zeek TLS capturing certificates 10min

Objective:
Run more traffic through Zeek, see the various files.

Purpose:
See that even though HTTPS and TLS traffic is encrypted it often show names and other values from the certificates and servers.

Suggested method:
Run Zeek capturing live traffic, start https towards some sites. A lot of common sites today has shifted to HTTPS/TLS.

Hints:
use zeekctl start and watch the output directory

```
root@debian-lab-11:/opt/zeek/spool/zeek# ls *.log
communication.log  dhcp.log files.log known_services.log packet_filter.log  stats.log
stdout.log x509.log conn.log dns.log known_hosts.log loaded_scripts.log  ssl.log
stderr.log weird.log
```

We already looked at `dns.log`, now check `ssl.log` and `x509.log`

```
root@debian-lab-11:/opt/zeek/spool/zeek# grep dr.dk ssl.log
1538983060.546122 CtKYZ625cq3m3jUz9k 10.xxx.0.145 49932 2.17.212.93 443 TLSv12 TLS_ECDHE_RSA_WITH_AES_2
sa,C=BE - - ok
1538983060.674217 CLjZo51fzuTcvPT0lg 200xxxxb:89b0:5cbf 49933 2a02:26f0:2400:2a1::3f46 443 TLSv12 TLS_E
sa,C=BE - - ok
```

Solution:
When you have multiple log files with data from Zeek, and have looked into some of them. You are welcome to ask questions and look into more files.

Discussion:
How can you hide that you are going to HTTPS sites?

Hint: VPN

Exercise 55

⚠ Suricata Basic Operation 15min

Objective:
Start using Suricata IDS engine with some traffic.

Purpose:
Show how to get started, meet some obstacles - missing files etc.

Discuss how to solve problems, why do we miss them, how to fix

Suggested method packet capture file:
Note: a dollar sign is the Linux prompt, showing the command after

```
$ cd
$ wget http://downloads.digitalcorpora.org/corpora/network-packet-dumps/2008-nitroba/nitroba.pcap
$ mkdir $HOME/suricata;cd $HOME/suricata;  suricata -r ../nitroba.pcap -c /etc/suricata/suricata.yaml -
l .
... Suricata reads the packets
~/suricata$ ls
eve.json  fast.log  stats.log
$ less *
```

Suggested method live capture:
Make sure the config file `/etc/suricata/suricata.yaml` has the right interface eth0 - or maybe ens192?. Check using `ifconfig -a`

Try starting the service

```
hlk@debian:~$ sudo service suricata start
hlk@debian:~$ cd /var/log/suricata/
hlk@debian:/var/log/suricata$ ls
eve.json  fast.log  stats.log  suricata.log
hlk@debian:/var/log/suricata$

hlk@debian:/var/log/suricata$ tail -3 suricata.log
8/10/2018 -- 17:15:58 - <Warning> - [ERRCODE: SC_ERR_AFP_CREATE(190)] - Can not open iface 'eth0'
8/10/2018 -- 17:15:58 - <Warning> - [ERRCODE: SC_ERR_AFP_CREATE(190)] - Can not open iface 'eth0'
8/10/2018 -- 17:16:19 - <Warning> - [ERRCODE: SC_ERR_AFP_CREATE(190)] - Can not open iface 'eth0'
```

Yeah my network card is called `ens33`, and I should replace eth0 with ens33 in the config file.

```
perl -pi -e "s/eth0/ens33/g" /etc/suricata/suricata.yaml
```

```
hlk@debian:/var/log/suricata$ sudo service suricata stop
hlk@debian:/var/log/suricata$ sudo service suricata start
hlk@debian:/var/log/suricata$ tail -3 suricata.log
8/10/2018 -- 17:23:20 - <Warning> - [ERRCODE: SC_ERR_NO_RULES(42)] - No rule files match the pattern /e
worm.rules
8/10/2018 -- 17:23:20 - <Warning> - [ERRCODE: SC_ERR_NO_RULES(42)] - No rule files match the pattern /e
8/10/2018 -- 17:23:20 - <Notice> - all 2 packet processing threads, 4 management threads initialized, e
```

Hints:
`https://redmine.openinfosecfoundation.org/projects/suricata/wiki/Quick_Start_Guide` and `https://redmine.openinfosecfoundation.org/projects/suricata/wiki/Basic_Setup`

Solution:
When you can start and stop suricata, and it only complains about missing rules, you are done with this exercise.

Discussion:
What was the main problems in this exercise?

Exercise 56

⚠ Basic Suricata rule configuration 15min

Objective:
See the Suricata configuration files, and get some rules.

The best IDS is nothing without good rules.

Purpose:
The rules make Suricata useful, and we will learn how to get a ruleset installed, and to keep it updated.

Suggested method:
Check the file `/etc/suricata/suricata-oinkmaster.conf`

It contains this:

```
hlk@debian:/etc/suricata$ cat suricata-oinkmaster.conf
# This is a Debian specific config file for oinkmaster crafted for suricata,
# you should read oinkmaster documentation to modify this file.
# This config is loaded by default from the suricata-oinkmaster-updater binary
# which is called daily from a cronjob by default

skipfile local.rules
skipfile deleted.rules
skipfile snort.conf
use_external_bins = 0

url = https://rules.emergingthreats.net/open/suricata-3.0/emerging.rules.tar.gz
```

Then try running the oinkmaster program in "dry run" with -c

```
root@debian:~# oinkmaster -i -c -C /etc/suricata/suricata-oinkmaster.conf -o /etc/suricata/rules/
Loading /etc/suricata/suricata-oinkmaster.conf
Downloading file from https://rules.emergingthreats.net/open/suricata-3.0/emerging.rules.tar.gz... done
Archive successfully downloaded, unpacking... done.
Setting up rules structures... done.
Processing downloaded rules... disablesid 0, enablesid 0, modifysid 0, localsid 0, total rules 26212
```

If the output looks OK, then re-run without -c and let it update files.

```
root@debian:~# oinkmaster -i -C /etc/suricata/suricata-oinkmaster.conf -o /etc/suricata/rules/
...
[+] Added files (consider updating your snort.conf to include them if needed):
    -> botcc.portgrouped.rules
    -> botcc.rules
    -> BSD-License.txt
    -> ciarmy.rules
...
    -> emerging-chat.rules
    -> emerging-current_events.rules
    -> emerging-deleted.rules
    -> emerging-dns.rules
```

```
    -> emerging-dos.rules
    -> emerging-exploit.rules
    -> emerging-ftp.rules
Do you approve these changes? [Yn]
```

Hints:

You need to restart Suricata for the rules to be found. In the example below I remove the long log with errors, and restart:

```
root@debian:~# service suricata stop
root@debian:~# rm /var/log/suricata/suricata.log
root@debian:~# service suricata start
root@debian:~# cat /var/log/suricata/suricata.log
8/10/2018 -- 17:45:19 - <Notice> - This is Suricata version 3.2.1 RELEASE
```

Solution:

When you have the ruleset downloaded and Suricata is happy when starting you are done with this exercise.

In a real deployment it is advised to automate the update of rules, and also some rules are probably not needed in you environments, YMMV. We will not go through all the rules provided.

Discussion:

Emerging Threats is a well-known ruleset provider, with commercial support.

Whenever there is a new internet wide security incident there are people providing IDS rules in Snort or Suricata format. Since Suricata can read snort rules, this is a good way to add up-to-date rules to your installation.

Note: we haven't mentioned it, but the config files for both Zeek and Suricata allows one to specify your home network.

Checkout the files: Zeek configuration in `/opt/zeek/etc/networks.cfg` and Suricata main config `/etc/suricata/suricata.yaml`

```
vars:
  # more specifc is better for alert accuracy and performance
  address-groups:
    HOME_NET: "[192.168.0.0/16,10.0.0.0/8,172.16.0.0/12]"
    #HOME_NET: "[192.168.0.0/16]"
```


Exercise 57

⚠ Configure Mirror Port 10min

Objective:
Mirror ports are a way to copy traffic to Suricata and other devices - for analyzing it. We will go through the steps on a Juniper switch to show how. Most switches which are configurable have this possibility.

Purpose:
We want to capture traffic for multiple systems, so we select an appropriate port and copy the traffic. In our setup, we select the uplink port to the internet/router.

It is also possible to buy passive taps, like a fiber splitter, which then takes part of the signal, and is only observable if you look for signal strength on the physical layer.

Suggested method:
We will configure a mirror port on a Juniper EX2200-C running Junos.

```
root@ex2200-c# show ethernet-switching-options | display set
set ethernet-switching-options analyzer mirror01 input ingress interface ge-0/1/1.0
set ethernet-switching-options analyzer mirror01 input egress interface ge-0/1/1.0
set ethernet-switching-options analyzer mirror01 output interface ge-0/1/0.0
set ethernet-switching-options storm-control interface all
```

Hints:
When checking your own devices this is often called SPAN ports, Mirror ports or similar.

`https://en.wikipedia.org/wiki/Port_mirroring`

Cisco has called this Switched Port Analyzer (SPAN) or Remote Switched Port Analyzer (RSPAN), so many will refer to them as SPAN-ports.

Solution:
When we can see the traffic from the network, we have the port configured - and can run any tool we like. Note: specialized capture cards can often be configured to spread the load of incoming packets onto separate CPU cores for performance. Capturing 100G and more can also be done using switches like the example found on the Zeek web site using an Arista switch 7150.

Discussion:
When is it ethical to capture traffic?

Exercise 58

ℹ Suricata Netflow 10min

Objective:
Configure Suricata to do netflow logging

Purpose:
In some cases we dont know what traffic we need to analyze, but if we collect netflow data - summary data about every connection. We can go back and check for specific types of traffic, based on ports, length etc.

Suggested method:

uncomment netflow in the config file `/etc/suricata/suricata.yaml` by removing the "#" in front of this line:

```
#- netflow
```

and restart Suricata.

Hints:
Netflow logging allows efficient logging of summary data, which can be very useful.

Solution:
When you have configured Suricata for netflow, you are done.

Discussion:
Specialized tools exist for collecting and visualizing netflow data. If you have nothing, then Suricata may be a good start.

Exercise 59

❶ Extending Zeek and Suricata 10min

Objective:
Sometimes Zeek and Suricata by themselves will not be enough.

Investigate how to extend Zeek and Suricata, by some examples.

Purpose:
See examples of scripts and rules, evaluate the complexity.

Suggested method:
VXLAN support was added recently in Suricata. The VXLAN patch does not need to be installed, but how big is it, how complex is it, could you or your organisation to something similar?

Go to github and find the VXLAN patch, and see the files changed.

Zeek scripts extend the basic engine, and are a big part of the eco-system. Some 1000s of script lines are already included. Do you have a specific need to analyze in your network which could be implemented in this?

Hints:
Earlier it was quite hard to write C programs for creating and analyzing network traffic. Today we can use the Zeek scripting and Suricata rules to analyze traffic using highly efficient engines.

Solution:
When you have seen the VXLAN patch you are done.

Discussion:
Note that making a small change to Suricata, and getting it imported into the source code – is not hard.

Which tool is easiest to expand, what are you missing from them?

To repeat something I often say:
Whenever there is a new internet wide security incident there are people providing IDS rules in Snort or Suricata format. Since Suricata can read snort rules, this is a good way to add up-to-date rules to your installation.

Would you be able to write a rule for something attacking your network?

Exercise 60

❶ VXLAN Detection

Objective:
One recent addition to many networks are cloud environments using tunneling and encapsulation to connect islands of containers and virtual systems.

One such protocol named VXLAN can be used without the network people being involved, which can be bad for security. Also it would be easy for an attacker which have compromised a system to use this for exfiltration of data.

So, do you have any VXLAN traffic in your network?

Purpose:
The main idea of this exercise is to talk about unknown traffic, that which you dont even know exist in your network. Some networks have tunnels and IPv6, but the network and security might not be fully aware of this.

Suggested method:
VXLAN traffic will most likely use the default port 4789, which is not used by much other traffic.

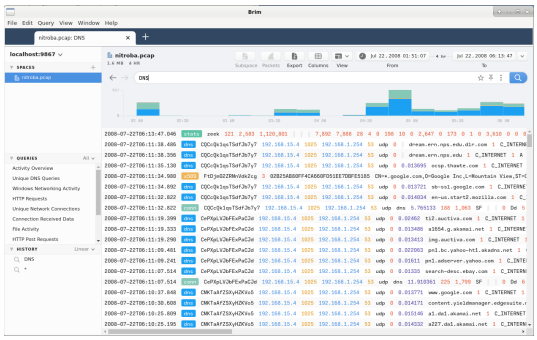
VXLAN is also UDP packets, so analysing if a few endpoints use a LOT of UDP might reveal interesting stuff.

Hints:
The conn.log might show you interesting things about such traffic.

Solution:
We dont have a VXLAN tunnel, but it is very easy to add a VXLAN interface to a Linux server, and start sending data out.

Exercise 61

ℹ Zui desktop app 20 min



Objective:
Try running Zeek through a desktop app which re-uses concepts from Zeek. Zeek is an advanced open source network security monitoring tool that can decode network packets, either live or using packet capture files. `https://zeek.org/`

The tool Zui (Brim desktop app) allows us to import larger packet captures into a GUI tool.

Purpose:
You might be presented with a packet capture file, that must be analyzed. Zui is packaged as a desktop app, built with Electron just like many other applications. Once installed, you can open a pcap with Zui and it will transform the pcap into Zeek logs in the ZNG format.

Suggested method:
Use either your normal operating system or the Debian VM. Then download the Zui desktop application from: `https://www.brimdata.io/download/` I choose the one for Ubuntu/Debian named: `zui_1.4.1_amd64.deb`

Download a sample packet capture:
`http://downloads.digitalcorpora.org/corpora/scenarios/2008-nitroba/nitroba.pcap`

Hints:
Download the .deb file for your Debian and install using: `$ sudo dpkg -i zui_1.4.1_amd64.deb`

Then open a packet capture, nitroba.pcap is a common example used.

Solution:
When you have browsed the Brim web site you are done, better if you managed to run it.

Discussion:
We often need a combination of tools, like Wireshark with GUI and Tcpdump with command line.

Here we have Zui with GUI and Zeek for command line and production use. These are much more advanced and can decode complex packet captures quickly.

Use the tool you like best for the task at hand.

Exercise 62

⚠ Indicators of Compromise 30min

Objective:
Indicators of Compromise is a term used for artifacts observed in networks or systems which indicate that a system was compromised.

This could be a known DNS domain where a specifc malware is downloaded from, a specific file name downloaded, a TCP connection to a malware control and command server.

`https://en.wikipedia.org/wiki/Indicator_of_compromise`

Purpose:
The purpose of this exercise is to look at the data gathered and to start planning how one could use this with IOCs to perform after-the-fact analysis of your network. Goal is to answer how an attack got in, when was the first device compromised etc.

Suggested method:
Look at the data provided by Zeek and Suricata, list the files again. Which parts will be of greatest interest in your networks? Could some of these facts have helped prevent, restrict, limit or otherwise improve your security stance?

We have some logs by now, or find examples from their web page.

Suricata and Zeek can include data from other sources, check the intel module

- Zeek documentation Intel framework
  https://docs.zeek.org/en/stable/frameworks/intel.html

- Suricata reputation support
  https://suricata.readthedocs.io/en/latest/reputation/index.html

Go to the web version of the exercise, and it is OK to only read it:
https://old.zeek.org/current/exercises/intel/index.html

Hints:
We don't need to find these ourselves. A lot of sources exist. I often recommend looking at Maltrail, since they incorporate a lot of different sources into their tool.

> Maltrail is a malicious traffic detection system, utilizing publicly available (black)lists containing malicious and/or generally suspicious trails, along with static trails compiled from various AV reports and custom user defined lists, where trail can be anything from domain name (e.g. zvpprsensinaix.com for Banjori malware), URL (e.g. hXXp://109.162.38.120/harsh02.exe for known malicious executable), IP address (e.g. 185.130.5.231 for known attacker) or HTTP User-Agent header value (e.g. sqlmap for automatic SQL injection and database takeover tool). Also, it uses (optional) advanced heuristic mechanisms that can help in discovery of unknown threats (e.g. new malware).

https://github.com/stamparm/maltrail

Solution:
Done, when you have seen the exercise on the web, not performed it, only looked: https://old.zeek.org/current/exercises/intel/index.html

Discussion:
Would this need to be updated every day to have value? How do we demonstrate return on investment and benefit from looking at traffic?

Discussion:
Which protocols are the most dangerous, and why?

Exercise 63

❶ Logning med syslogd og syslog.conf 10min

Objective:
See how server syslog is configured on regular Unix/Linux

Purpose:
The main idea of this exercise is to understand how easy network connected systems can send log data.

Suggested method:
Log into your local Linux systems or network devices, see how syslog is configured.

Hints:
Look in the config file, may be in /etc/syslog or /etc/syslog-ng/syslog-ng.conf

Sample output from old-skool syslogd

```
*.err;kern.debug;auth.notice;authpriv.none;mail.crit    /dev/console
*.notice;auth,authpriv,cron,ftp,kern,lpr,mail,user.none /var/log/messages
kern.debug;user.info;syslog.info                        /var/log/messages
auth.info                                               /var/log/authlog
authpriv.debug                                          /var/log/secure
...
# Uncomment to log to a central host named "loghost".
#*.notice;auth,authpriv,cron,ftp,kern,lpr,mail,user.none        @loghost
#kern.debug,user.info,syslog.info                               @loghost
#auth.info,authpriv.debug,daemon.info                           @loghost
```

Solution:
When you understand how to configure syslog from a couple of devices and has looked up which protocol and port it uses. (default is 514/udp)

Discussion:
There are syslog senders for Windows too.

Note: syslog is almost always there, available, but often better and more modern alternatives exist – like Filebeat.

https://www.elastic.co/beats/filebeat

Exercise 64

❶ Create Kibana Dashboard 15min

Objective:
See Kibana and understand how it is configured.

Purpose:
Kibana is a very popular system for creating dashboards from data in elasticsearch.

Learning how to create and import dashboards is a good exercise.

Suggested method:
Revisit exercise **??** and make sure you have Elasticsearch and Kibana running.

Kibana should be available on port 5601 on localhost (127.0.0.1) only though!

Using Firefox visit Kibana on http://127.0.0.1:5601 first time you need to select `logstash-*` as a default index. Note: Kibana is an advanced and powerful tool in itself.

Try loading the ones from: https://github.com/StamusNetworks/KTS7

The commands are similar to

```
git clone https://github.com/StamusNetworks/KTS7.git
cd KTS7
```

Then use the commands listed in the README.rst file.

Hints:
Logstash and Elastic stack are a great way to get started with dashboarding.

However, running a big installation is harder than it looks. Make sure to have multiple servers and good monitoring.

Solution: When you have either loaded existing dashboards into your Kibana, OR made a change, just a small one, to an existing dashboard – you are done.

Discussion:
Making dashboard are an art form. We will NOT start creating beautiful dashboards.

If you want, there is a SELKS LiveCD dedicated to suricata which also includes more tools for administration of rules and getting alerts:
https://www.stamus-networks.com/open-source/