Penetration Tests & Ethical Hacking

Airbus Cyber Diploma

Walter Gin
Sébastien Desbordes

AIRBUS

Teacher(s) Presentation

Walter Gin

- Offensive Security consultant && Technical Advisor at Airbus Protect
- Background: Network Security, Telecoms, Cloud, and on the field operations and deployments
- Loving: Freediving, Photo and discovering new stuff

Sébastien Desbordes

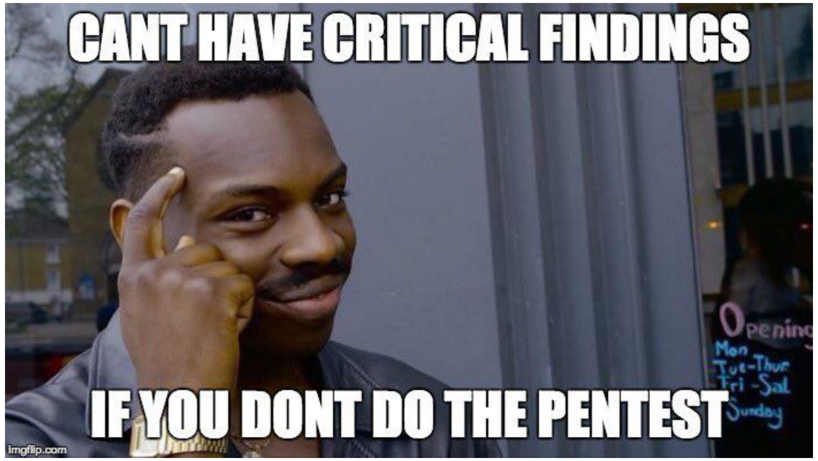
- In charge of Airbus pentest program, coordinating pentest activities through Airbus (trying at least)
- Not truly a pentester, but i’ve organised 1 or 2 exercises (or dozens…)
- I love movies, meeting new people, tekno music (in no particular order)

<game> What is ? </game>

Penetration Tests ?

Ethical Hacking ?

Red Team operations ?



Rules : Freely suggest anything you know regarding these items, errors accepted (no judgment)

Let’s build the environment ! 1/2

In order to copy/paste some commands you can find it here: https://github.com/waltergin/lab/blob/main/commands

1. Download Kali VM Image: https://cdimage.kali.org/kali-2022.4/kali-linux-2022.4-virtualbox-amd64.7z

2. Verify SHA256 checksum with powershell:

```
(Get-FileHash .\path\to\kali-linux-2022.4-virtualbox-amd64.7z).Hash -eq
"b0d4d68ed74f763c0e761e5d39350f339792c42f8e8f6da03c2fdcd33ca676ef".toUpper()
```

3. Download & install 7-Zip (https://www.7-zip.org/a/7z2201-x64.exe)

4. Unzip de 7z archive into a folder of your choice (advice: use the Virtualbox VM folder)

5. Import the VM into Virtualbox using **Machine** -> **Add** button and select the vbox file

6. Change network adapter settings to bridge (Accès par pont), in the **Advanced** settings specify the MAC Address : **00016F+ 6 last Hex number of your real network adapter** (ipconfig /all)

7. Start the Kali VM and login using kali/kali (you may want to change the password but do not forget it) -> beware of the US keyboard !

Let’s build the environment ! 2/2

1. Change the keyboard layout via Settings in Kali and replace “us” by “fr” in /etc/default/keyboard:

```
sed -i 's/XKBLAYOUT=.*$/XKBLAYOUT="fr"/g' /etc/default/keyboard
```

2. Alternatively you can edit /etc/default/keyboard manually.

3. Add the dns script provided at https://raw.githubusercontent.com/waltergin/lab/main/dns and put it here: /etc/network/if-up.d/dns, then execute `sudo chmod +x /etc/network/if-up.d/dns`

4. Override the existing network configuration file (/etc/network/interfaces) with the one provided at https://raw.githubusercontent.com/waltergin/lab/main/interfaces

5. Reboot the VM

6. Perform connectivity test:
   a. `ping 30.204.4.240`
   b. `ping 10.66.66.53`

AGENDA

[Airbus Amber]

01 **Reminder about the basics**

Description

02 **Demystifying Penetration Tests**

Description

03 **Planning, scoping, reporting, …**

Description

04 **Enumeration**

Description

05 **Exploitation**

Description

06 **Evaluation**

Yay, you know…

AIRBUS

Learning objectives & Evaluation

Learning objectives

What am i doing here ?

- Explain the different pentest methodologies
- Define a scope, know the legal impacts
- Perform active reconnaissance and master network scanning with nmap
- Identify & exploit vulnerabilities
- Obtain a shell and understand the different ones

- Break passwords
- Present and explain your findings
- Have FUN through LEARNING

Evaluation

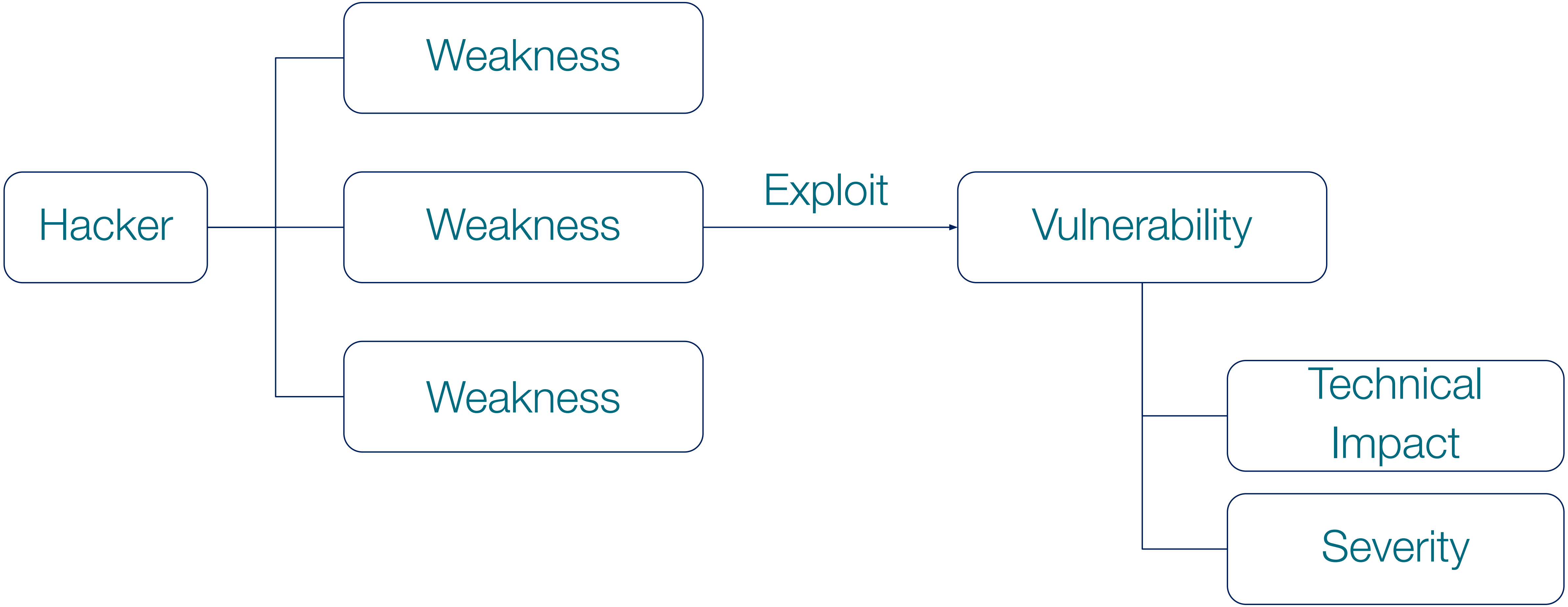
If things goes as planned, you’ll team up in pairs to perform a small penetration test on a dedicated lab. We’ll be there to assist, and we’ll let you some time to deliver a report. This report will be the evaluation’s foundation.

Reminder about the basics

Cyber Security Vocabulary

- Vulnerability
- Exploit
- Intrusion
- Severity
- Risk
- Threat

Vocabulary in context



https://youtu.be/Z6UmvkIbNrw

Story Telling Solarwinds

Demystifying Penetration Test

Goals

- Modeling real world attacks by using the same Tactics(tools)/Techniques & Procedures to compromise the target system/infrastructure/organization
- Identify/Discover vulnerabilities
- Exploit vulnerabilities
- Score/rank the vulnerabilities
- Help to better understand and reduce the risks by providing recommendations to improve the security posture

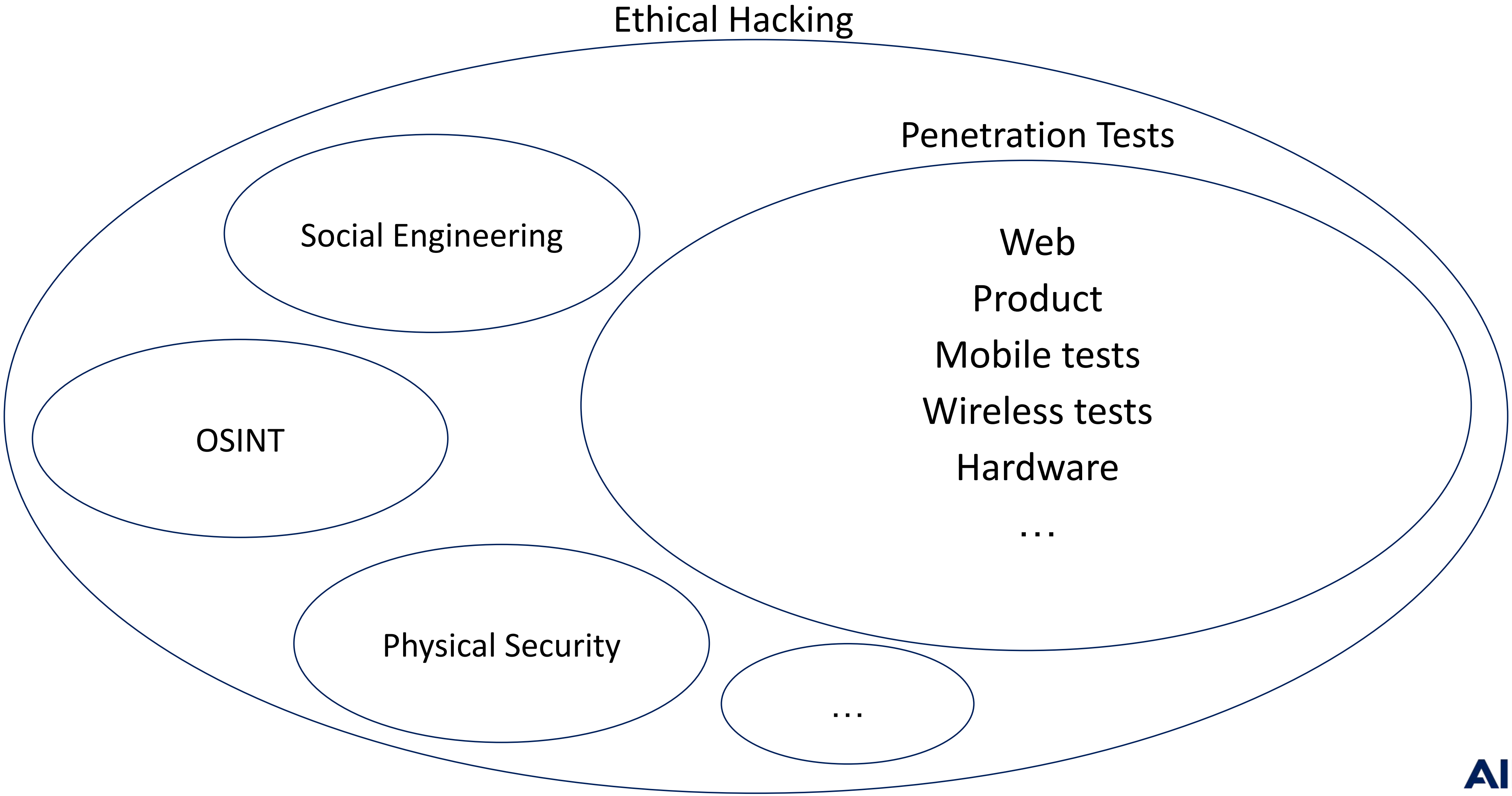
Mindset & Split-brain

Good Balance is mandatory

- Think out of the box
- Pragmatic
- Curious
- Flexible
- “RTFM”
- Deeply interested by the technical stuff

- Rigorous
- Carefull
- Methodical
- Taking notes
- Repeatable actions
- Proof and clues approach

Penetration Tests & Ethical Hacking Activities



Ethical Hacking

Penetration Tests

Web

Product

Mobile tests

Wireless tests

Hardware

…

Social Engineering

OSINT

Physical Security

…

The Attack Phases

- Recon
  - Passive Information Gathering
  - Active Information Gathering
- Scanning
  - Port Scanning
  - Vulnerability Scanning
- Exploitation
- Credentials gathering
- Privilege Escalation
- Pivoting
- Antivirus and EDR evasion Maintaining Access
- Covering Traces

Intrusion Strategy

- **Enumeration**
- Then, enumeration
- Then, enumeration,....
- **Identifying vulnerabilities**
- **Exploiting vulnerabilities**
- Enumeration
- Then, enumeration
- Then, enumeration,....
- **Pivoting**
- Then, enumeration
- Then, enumeration,....

Enumeration is the key to open the doors

Legal

- Each country has its own law regarding Intrusion in an IT system
- In France intrusion in a system is forbidden by law: *article 323-1 du code pénal*:

Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 60 000 € d'amende.

Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 100 000 € d'amende.

Lorsque les infractions prévues aux deux premiers alinéas ont été commises à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à cinq ans d'emprisonnement et à 150 000 € d'amende.

Ethics

- Operate on the defined scope and on the defined time window
- Raise issues in a timely manner
- Alert when failing
- Clean at the end

ISO 19011 : Les valeurs

- Déontologie
- Impartialité
- Conscience Professionnelle
- Confidentialité
- Indépendance
- Approche fondée sur la preuve

Pentesting Methodology

Various Pentesting framework and methodologies, many others exists

- OSTMM *Open Source Testing Methodology Manual*
- PTES *Pen Testing Execution Standard*
- PCI DSS Penetration Test Guidance
- OWASP Web Security Testing Guide
- OWASP Mobile Security Testing Guide
- OWASP Firmware Security Testing Guide
- Penetration Testing Framework
- NIST 800-115
- …

Planning, Scoping, Rules and Reporting

Security Technical Evaluation - ID card

Lead Auditor: **María MARTÍNEZ RUIZ**
Sébastien DESBORDES

SECURITY OBJECTIVES

1. eg. Identification of potential areas for improvements and risk mitigation
2. eg. Reinforce good practices observed to encourage teams and capitalize on these practices in the company

Specific focus on

1. X

RULES OF ENGAGEMENT

Scope:

Scope exclusions:

Test location:

Internal report classification: Airbus Amber

Prerequisites / status (waiting / provided)

❏ ARD | status:
❏ Access | status:
❏ X | status:
❏ X | status:

Security Technical Evaluation - ID card

PLANNING

Pentest: 10 days / 2 Evaluators / 1 Airbus Lead auditor

Report: 3 to 6 weeks after testing

Findings follow-up: shall start after report validation, or after the closing meeting for critical findings. You will be contacted by VCR to initiate the remediation action plan.

*Our evaluations aim at reducing Airbus attack surface, **we trust you to find a remediation** for each finding discovered during this exercise.*

VCR - Vulnerability Management contact : cybervulnerabilities.service@airbus.com

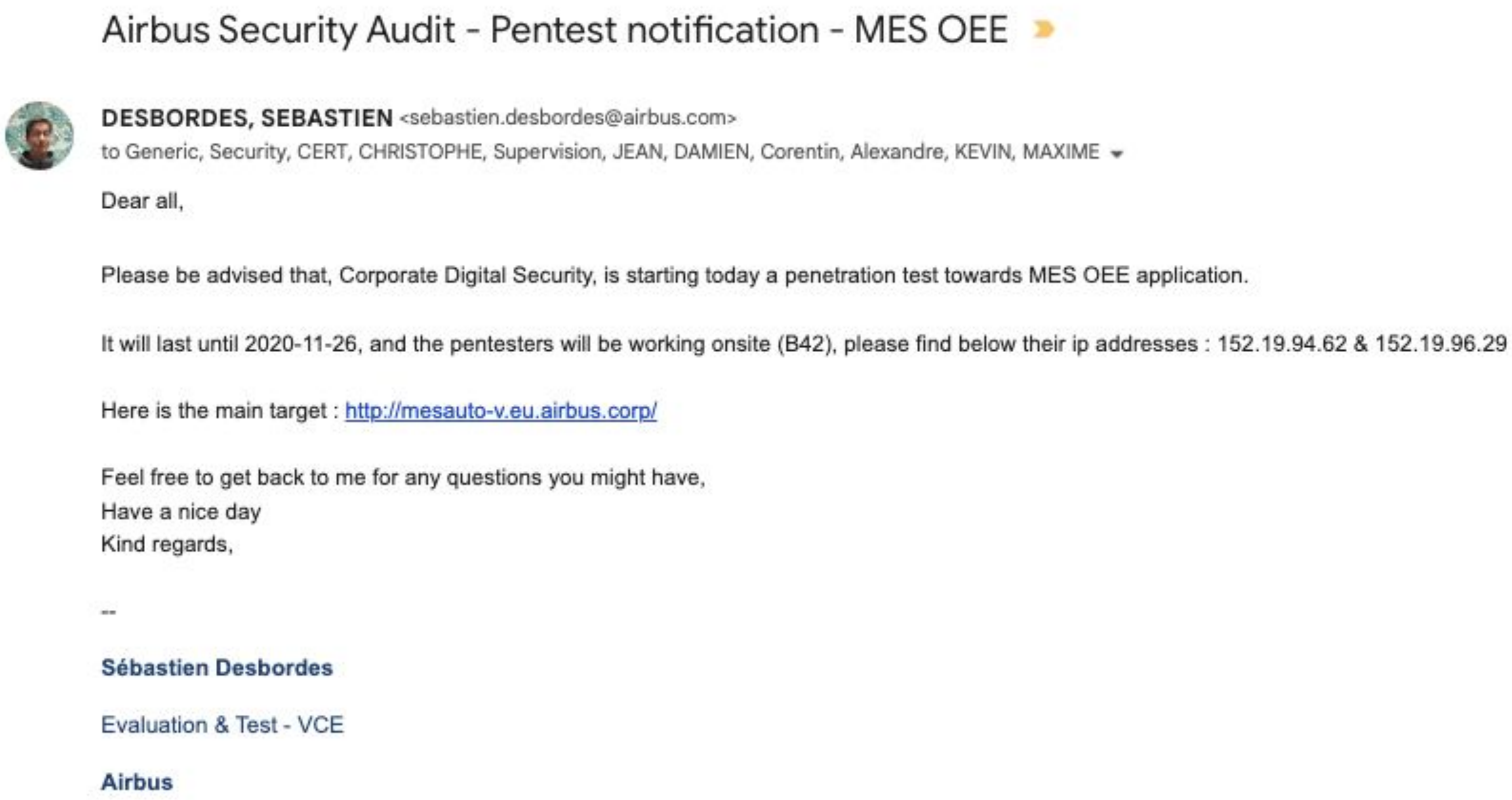
1. **Opening meeting:** 202X-MM-DD
2. **Evaluation start date:** 202X-MM-DD
3. **Closing meeting:** 202X-MM-DD

➔ Evaluator company: **XX**
➔ Sourcing restriction: X

NEXT STEPS

Actions	Owner
eg.Prerequisites to be provided	
eg.Kick-off meeting to be planned before the start of the evaluation	M.MAR / S.DES

Authorization, SOC Warning



Airbus Security Audit - Pentest notification - MES OEE

DESBORDES, SEBASTIEN <sebastien.desbordes@airbus.com>
to Generic, Security, CERT, CHRISTOPHE, Supervision, JEAN, DAMIEN, Corentin, Alexandre, KEVIN, MAXIME

Dear all,

Please be advised that, Corporate Digital Security, is starting today a penetration test towards MES OEE application.

It will last until 2020-11-26, and the pentesters will be working onsite (B42), please find below their ip addresses : 152.19.94.62 & 152.19.96.29

Here is the main target : http://mesauto-v.eu.airbus.corp/

Feel free to get back to me for any questions you might have,
Have a nice day
Kind regards,

--

Sébastien Desbordes

Evaluation & Test - VCE

Airbus

Notes, Inventory, Collaboration

- Take Notes
- Inventory of assets
- Screenshots
- Scripts
- Payloads
- …

Tools of your choice:

- Dradis
- Joplin
- Magictree
- CherryTree
- Lair
- Etherpad
- Metasploit
- …

BHP-05: No root or jailbreak detection on Android/iOS application

Severity: Informational

Description

No root or jailbreak detection is implemented in the application. This allows an attacker to modify the app on a rooted Android or jailbroken iOS device, which means the attacker can potentially induce behaviors that otherwise would not occur. Examples of the impact include accessing sensitive application data, overwriting critical functions, and an overall wider attack surface.

Impact

A malicious application with root permission can access and modify data belongs to the BHP application. Combined with the "unnecessary app permissions" issue above, a malicious third-party application can take advantage of the BHP app permissions and perform more privileged actions.

Step to Reproduce

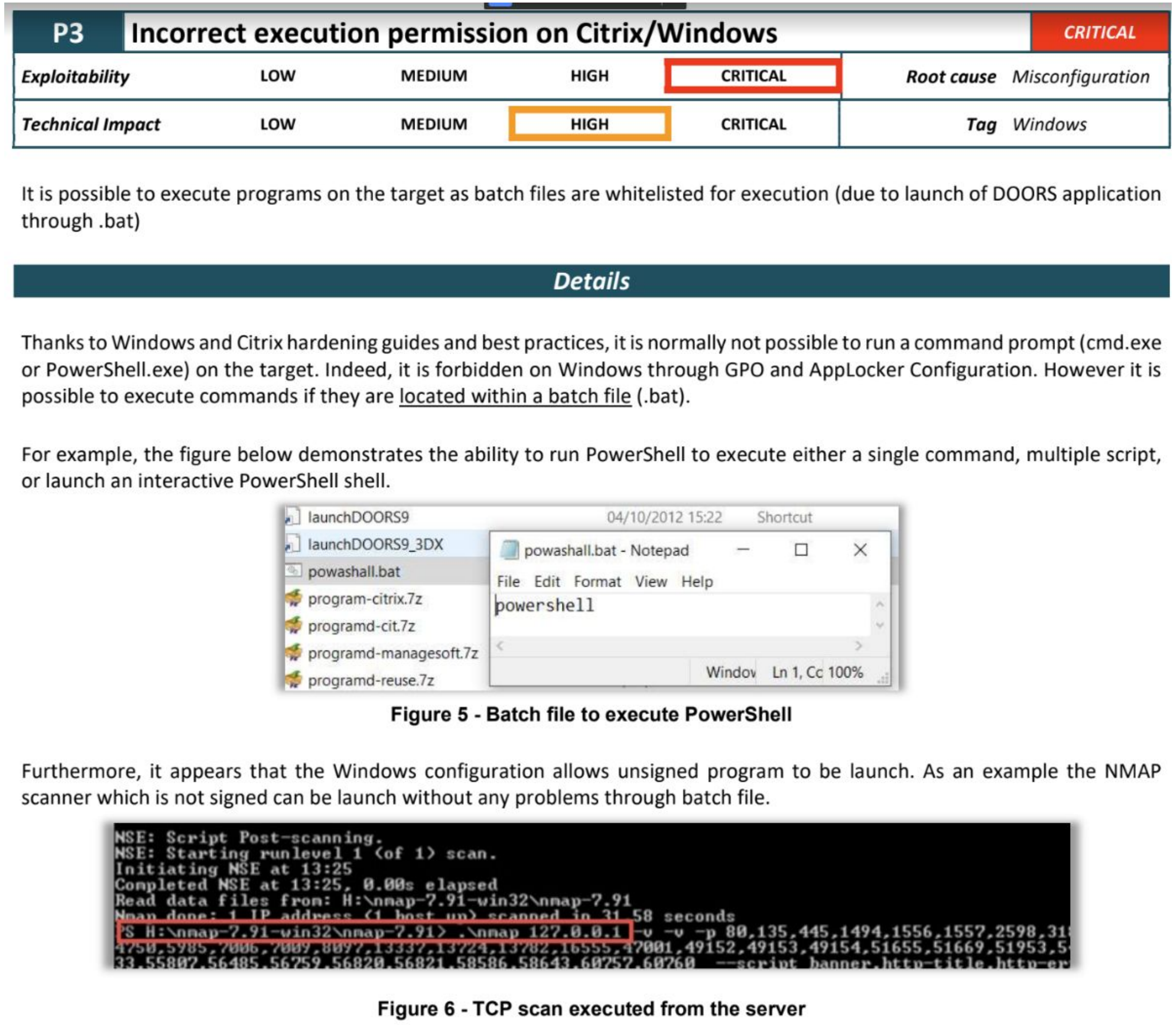
Install and run the BHP wallet on a rooted Android or jailbroken iOS device.

Recommendation

Implement root and jailbreak detection at the beginning of the runtime of your application. Shut down the application or at least display a warning message when a user attempts to use the wallet on a rooted or jailbroken device.

Some methods to check for a rooted/jailbroken device are listed below:

Android



P3 Incorrect execution permission on Citrix/Windows

CRITICAL

Exploitability	LOW	MEDIUM	HIGH	[✓ CRITICAL]	*Root cause*	*Misconfiguration*
Technical Impact	LOW	MEDIUM	[✓ HIGH]	CRITICAL	*Tag*	*Windows*

It is possible to execute programs on the target as batch files are whitelisted for execution (due to launch of DOORS application through .bat)

Details

Thanks to Windows and Citrix hardening guides and best practices, it is normally not possible to run a command prompt (cmd.exe or PowerShell.exe) on the target. Indeed, it is forbidden on Windows through GPO and AppLocker Configuration. However it is possible to execute commands if they are located within a batch file (.bat).

For example, the figure below demonstrates the ability to run PowerShell to execute either a single command, multiple script, or launch an interactive PowerShell shell.

launchDOORS9	04/10/2012 15:22	Shortcut
launchDOORS9_3DX		
powashall.bat		
program-citrix.7z		
programd-cit.7z		
programd-managesoft.7z		
programd-reuse.7z		

```
powershell
```

Figure 5 - Batch file to execute PowerShell

Furthermore, it appears that the Windows configuration allows unsigned program to be launch. As an example the NMAP scanner which is not signed can be launch without any problems through batch file.

```
NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 13:25
Completed NSE at 13:25, 0.00s elapsed
Read data files from: H:\nmap-7.91-win32\nmap-7.91
Nmap done: 1 IP address (1 host up) scanned in 31.58 seconds
PS H:\nmap-7.91-win32\nmap-7.91> .\nmap 127.0.0.1 -v -v -p 80,135,445,1494,1556,1557,2598,31
4750,5985,7006,7009,8097,13337,13724,13782,16555,47001,49152,49153,49154,51655,51669,51953,5
33,55807,56485,56759,56820,56821,58586,58643,60757,60760 --script banner,http-title,http-er
```

Figure 6 - TCP scan executed from the server

Sum Up

Enumeration

Enumeration

- Identify the widest attack surface of the target in the defined scope.
- The weakest entry point could be the one that people are unaware of.
- This allow to build a “view” of the target, this visibility on the target is the starting point of all the following activities.
- Must be performed at the beginning, but could also be redone at any time.

Passive Information Gathering aka OSINT

Reminder:

- Whois
- Dorks
- Netcraft
- Shodan
- Certificate transparency logs
- Recon-Ng
- Qualys SSL Labs
- Pastebin
- Email Harvesting
- Social Media
- Maltego
- OSINT Framework (US)
- Document Metadata (exiftool, strings, …)
- …

WARNING:

In all the following slides some tools will be presented and must only be used in the time for LABs and on the target specified in this course.

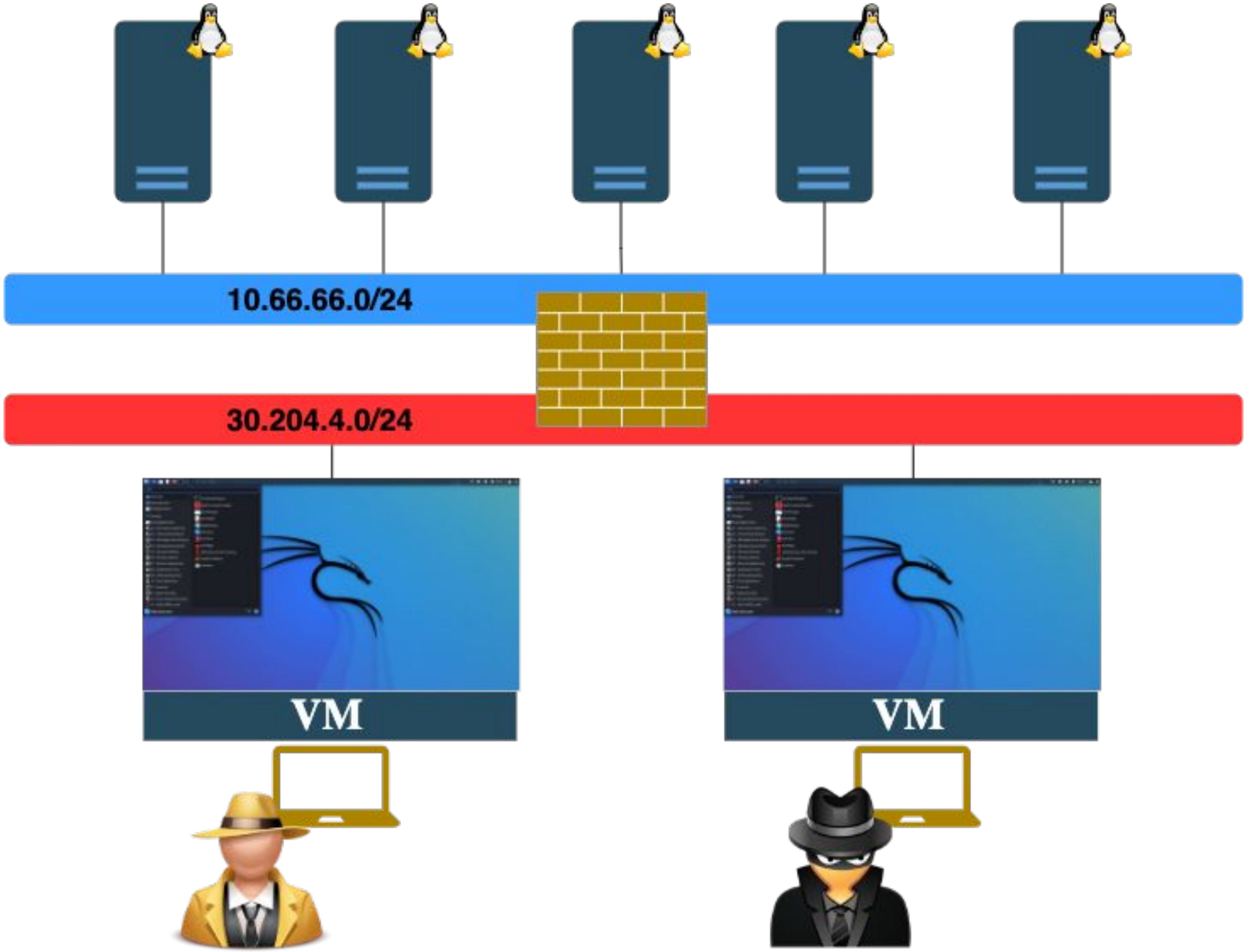
You must always have an authorization to perform offensive actions on a target. (some platforms are available for training: HackTheBox, RootMe, TryHackMe,...)

Never forget that when you use third-party services for any activity you are revealing information to them. Always consider which information you are disclosing.

SCOPE:

All the followings tests will be performed on the LAB target environment defined with the following subnet **10.66.66.0/24**

You are not allowed to perform any offensive action against IP that are out of the scope. (This include your own machines)


10.66.66.0/24
30.204.4.0/24
VM
VM

Active Information Gathering

DNS Enumeration

- Retrieving as much DNS entries as possible
- BruteForcing subdomains
- Zone Transfer
- DNS cache snooping
- From DNS entries to Hosts and the reverse

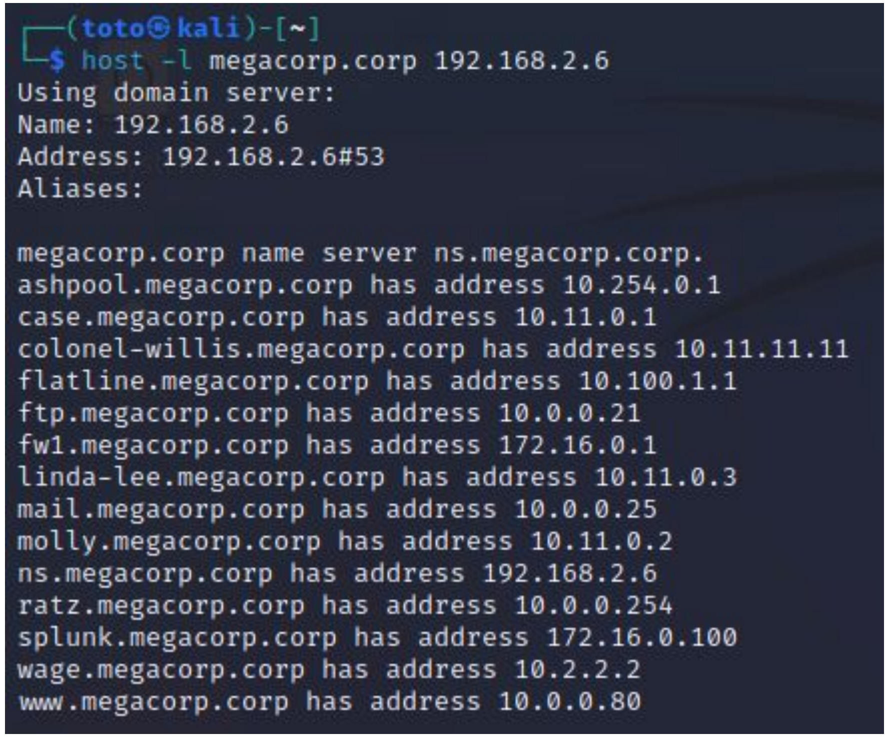
Tools:

host (Linux)
dig (Linux)
nslookup (Windows)
recon-ng

nmap (NSE Script)
dnsrecon
amass
…

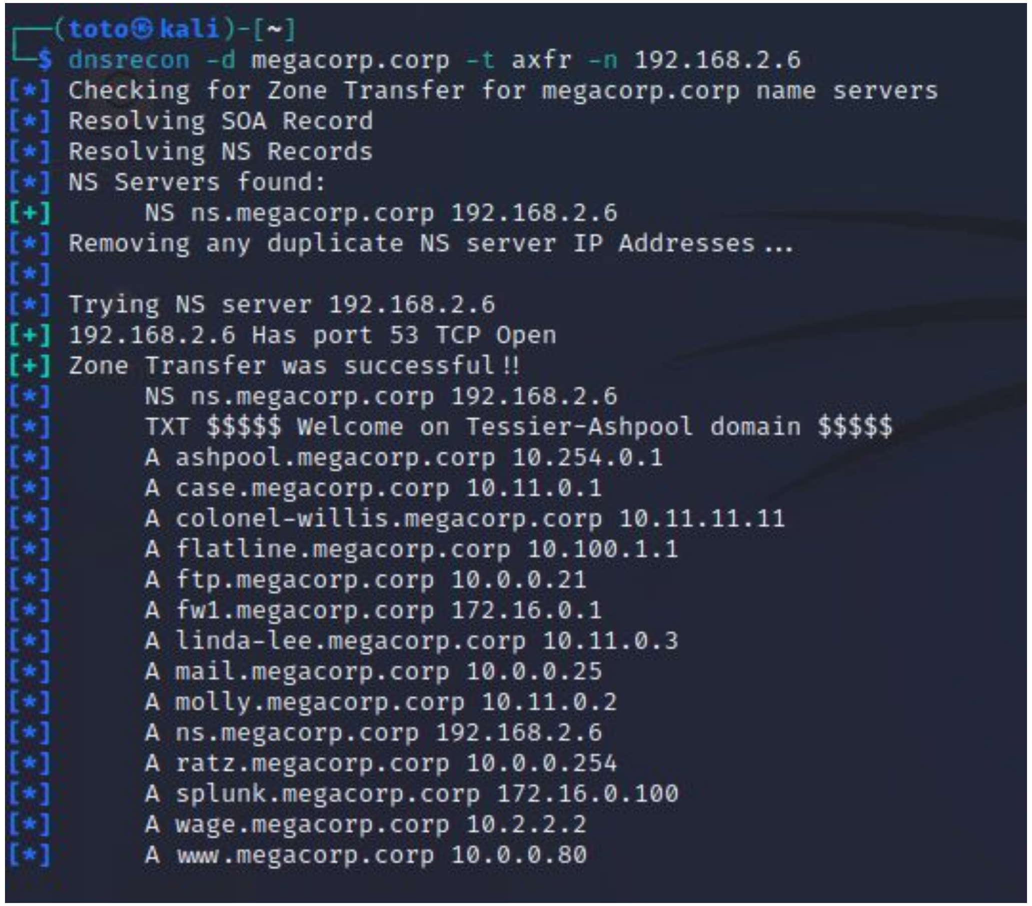
DNS Enumeration

DNS Zone Transfer



```
┌──(toto㉿kali)-[~]
└─$ host -l megacorp.corp 192.168.2.6
Using domain server:
Name: 192.168.2.6
Address: 192.168.2.6#53
Aliases:

megacorp.corp name server ns.megacorp.corp.
ashpool.megacorp.corp has address 10.254.0.1
case.megacorp.corp has address 10.11.0.1
colonel-willis.megacorp.corp has address 10.11.11.11
flatline.megacorp.corp has address 10.100.1.1
ftp.megacorp.corp has address 10.0.0.21
fw1.megacorp.corp has address 172.16.0.1
linda-lee.megacorp.corp has address 10.11.0.3
mail.megacorp.corp has address 10.0.0.25
molly.megacorp.corp has address 10.11.0.2
ns.megacorp.corp has address 192.168.2.6
ratz.megacorp.corp has address 10.0.0.254
splunk.megacorp.corp has address 172.16.0.100
wage.megacorp.corp has address 10.2.2.2
www.megacorp.corp has address 10.0.0.80
```

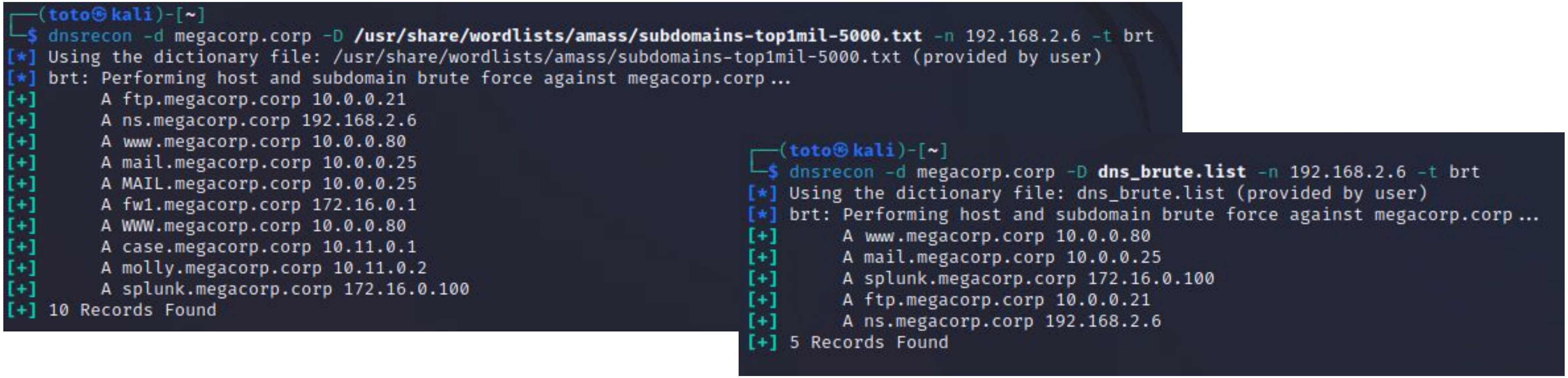


```
┌──(toto㉿kali)-[~]
└─$ dnsrecon -d megacorp.corp -t axfr -n 192.168.2.6
[*] Checking for Zone Transfer for megacorp.corp name servers
[*] Resolving SOA Record
[*] Resolving NS Records
[*] NS Servers found:
[+]     NS ns.megacorp.corp 192.168.2.6
[*] Removing any duplicate NS server IP Addresses...
[*]
[*] Trying NS server 192.168.2.6
[+] 192.168.2.6 Has port 53 TCP Open
[+] Zone Transfer was successful!!
[*]     NS ns.megacorp.corp 192.168.2.6
[*]     TXT $$$$$ Welcome on Tessier-Ashpool domain $$$$$
[*]     A ashpool.megacorp.corp 10.254.0.1
[*]     A case.megacorp.corp 10.11.0.1
[*]     A colonel-willis.megacorp.corp 10.11.11.11
[*]     A flatline.megacorp.corp 10.100.1.1
[*]     A ftp.megacorp.corp 10.0.0.21
[*]     A fw1.megacorp.corp 172.16.0.1
[*]     A linda-lee.megacorp.corp 10.11.0.3
[*]     A mail.megacorp.corp 10.0.0.25
[*]     A molly.megacorp.corp 10.11.0.2
[*]     A ns.megacorp.corp 192.168.2.6
[*]     A ratz.megacorp.corp 10.0.0.254
[*]     A splunk.megacorp.corp 172.16.0.100
[*]     A wage.megacorp.corp 10.2.2.2
[*]     A www.megacorp.corp 10.0.0.80
```

DNS Enumeration

Brute Forcing subdomains and hosts

```
# Using dnsrecon
dnsrecon -d DOMAIN -D DICTIONNARY -t TYPE -n NAMESERVER
```



```
┌──(toto㉿kali)-[~]
└─$ dnsrecon -d megacorp.corp -D /usr/share/wordlists/amass/subdomains-top1mil-5000.txt -n 192.168.2.6 -t brt
[*] Using the dictionary file: /usr/share/wordlists/amass/subdomains-top1mil-5000.txt (provided by user)
[*] brt: Performing host and subdomain brute force against megacorp.corp ...
[+]      A ftp.megacorp.corp 10.0.0.21
[+]      A ns.megacorp.corp 192.168.2.6
[+]      A www.megacorp.corp 10.0.0.80
[+]      A mail.megacorp.corp 10.0.0.25
[+]      A MAIL.megacorp.corp 10.0.0.25
[+]      A fw1.megacorp.corp 172.16.0.1
[+]      A WWW.megacorp.corp 10.0.0.80
[+]      A case.megacorp.corp 10.11.0.1
[+]      A molly.megacorp.corp 10.11.0.2
[+]      A splunk.megacorp.corp 172.16.0.100
[+] 10 Records Found
```

```
┌──(toto㉿kali)-[~]
└─$ dnsrecon -d megacorp.corp -D dns_brute.list -n 192.168.2.6 -t brt
[*] Using the dictionary file: dns_brute.list (provided by user)
[*] brt: Performing host and subdomain brute force against megacorp.corp ...
[+]      A www.megacorp.corp 10.0.0.80
[+]      A mail.megacorp.corp 10.0.0.25
[+]      A splunk.megacorp.corp 172.16.0.100
[+]      A ftp.megacorp.corp 10.0.0.21
[+]      A ns.megacorp.corp 192.168.2.6
[+] 5 Records Found
```

DNS Enumeration

Brute Forcing subdomains and hosts

Identify the DNS server in the target scope

Try to resolve ns.megacorp.corp with dig command

Kali Linux has embedded wordlists, have a look in /usr/share/wordlists.
Some tools comes with their own wordlist, in this case we use dnsrecon and you may find it in /usr/share/dnsrecon/

Perform a subdomain bruteforce attack on the DNS server to try to discover hosts on the megacorp.corp domain

DNS Enumeration

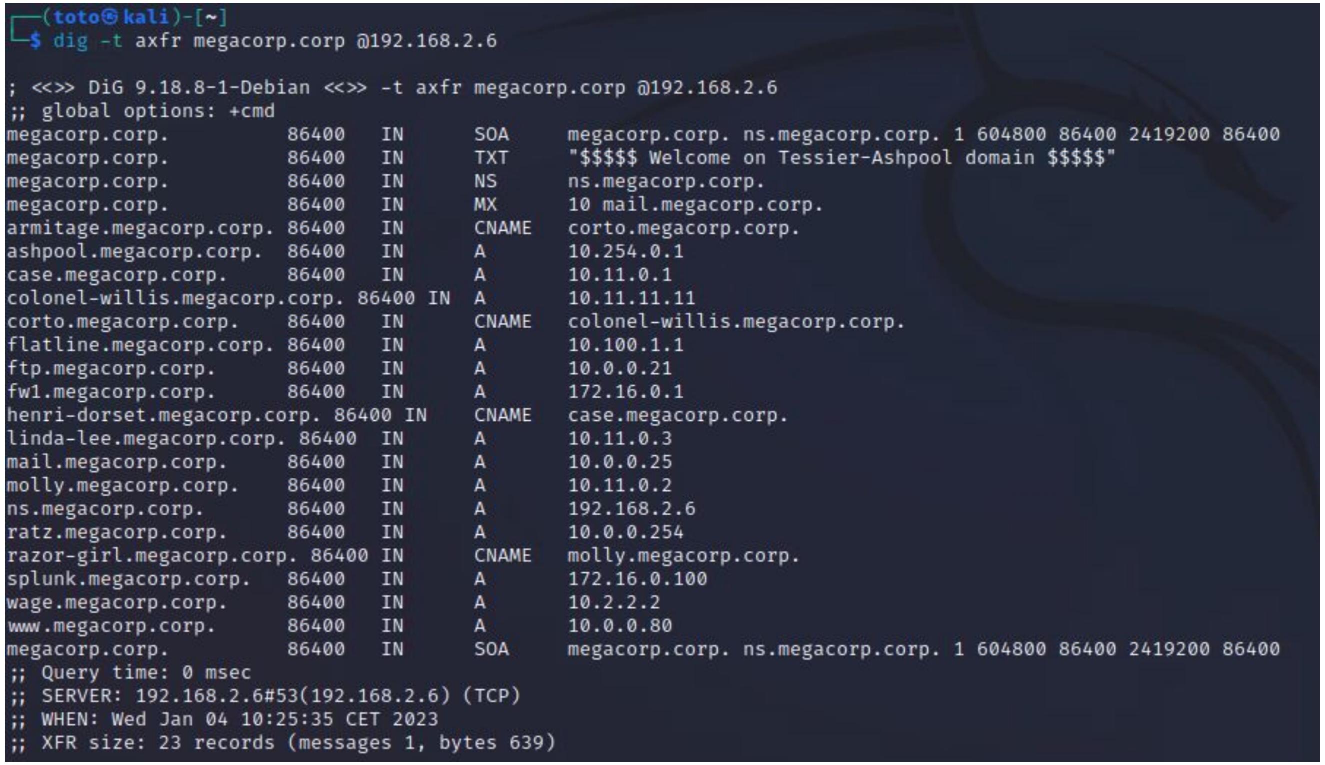
DNS Zone Transfer

- Requesting a full zone transfer with AXFR
- Requesting a full zone transfer with IXFR

```
# Using dig
dig -t TYPE DOMAIN @NameServer

# Using host
host -l DOMAIN @NameServer

# Using dnsrecon
dnsrecon -d DOMAIN -t TYPE -n NameServer
```



```
┌──(toto㉿kali)-[~]
└─$ dig -t axfr megacorp.corp @192.168.2.6

; <<>> DiG 9.18.8-1-Debian <<>> -t axfr megacorp.corp @192.168.2.6
;; global options: +cmd
megacorp.corp.          86400   IN      SOA     megacorp.corp. ns.megacorp.corp. 1 604800 86400 2419200 86400
megacorp.corp.          86400   IN      TXT     "$$$$$ Welcome on Tessier-Ashpool domain $$$$$"
megacorp.corp.          86400   IN      NS      ns.megacorp.corp.
megacorp.corp.          86400   IN      MX      10 mail.megacorp.corp.
armitage.megacorp.corp. 86400   IN      CNAME   corto.megacorp.corp.
ashpool.megacorp.corp.  86400   IN      A       10.254.0.1
case.megacorp.corp.     86400   IN      A       10.11.0.1
colonel-willis.megacorp.corp. 86400 IN  A       10.11.11.11
corto.megacorp.corp.    86400   IN      CNAME   colonel-willis.megacorp.corp.
flatline.megacorp.corp. 86400   IN      A       10.100.1.1
ftp.megacorp.corp.      86400   IN      A       10.0.0.21
fw1.megacorp.corp.      86400   IN      A       172.16.0.1
henri-dorset.megacorp.corp. 86400 IN    CNAME   case.megacorp.corp.
linda-lee.megacorp.corp. 86400  IN      A       10.11.0.3
mail.megacorp.corp.     86400   IN      A       10.0.0.25
molly.megacorp.corp.    86400   IN      A       10.11.0.2
ns.megacorp.corp.       86400   IN      A       192.168.2.6
ratz.megacorp.corp.     86400   IN      A       10.0.0.254
razor-girl.megacorp.corp. 86400 IN      CNAME   molly.megacorp.corp.
splunk.megacorp.corp.   86400   IN      A       172.16.0.100
wage.megacorp.corp.     86400   IN      A       10.2.2.2
www.megacorp.corp.      86400   IN      A       10.0.0.80
megacorp.corp.          86400   IN      SOA     megacorp.corp. ns.megacorp.corp. 1 604800 86400 2419200 86400
;; Query time: 0 msec
;; SERVER: 192.168.2.6#53(192.168.2.6) (TCP)
;; WHEN: Wed Jan 04 10:25:35 CET 2023
;; XFR size: 23 records (messages 1, bytes 639)
```

DNS Enumeration

DNS Zone Transfer

Perform a zone transfer of megacorp.corp domain with dig

Perform a zone transfer of megacorp.corp domain with dnsrecon

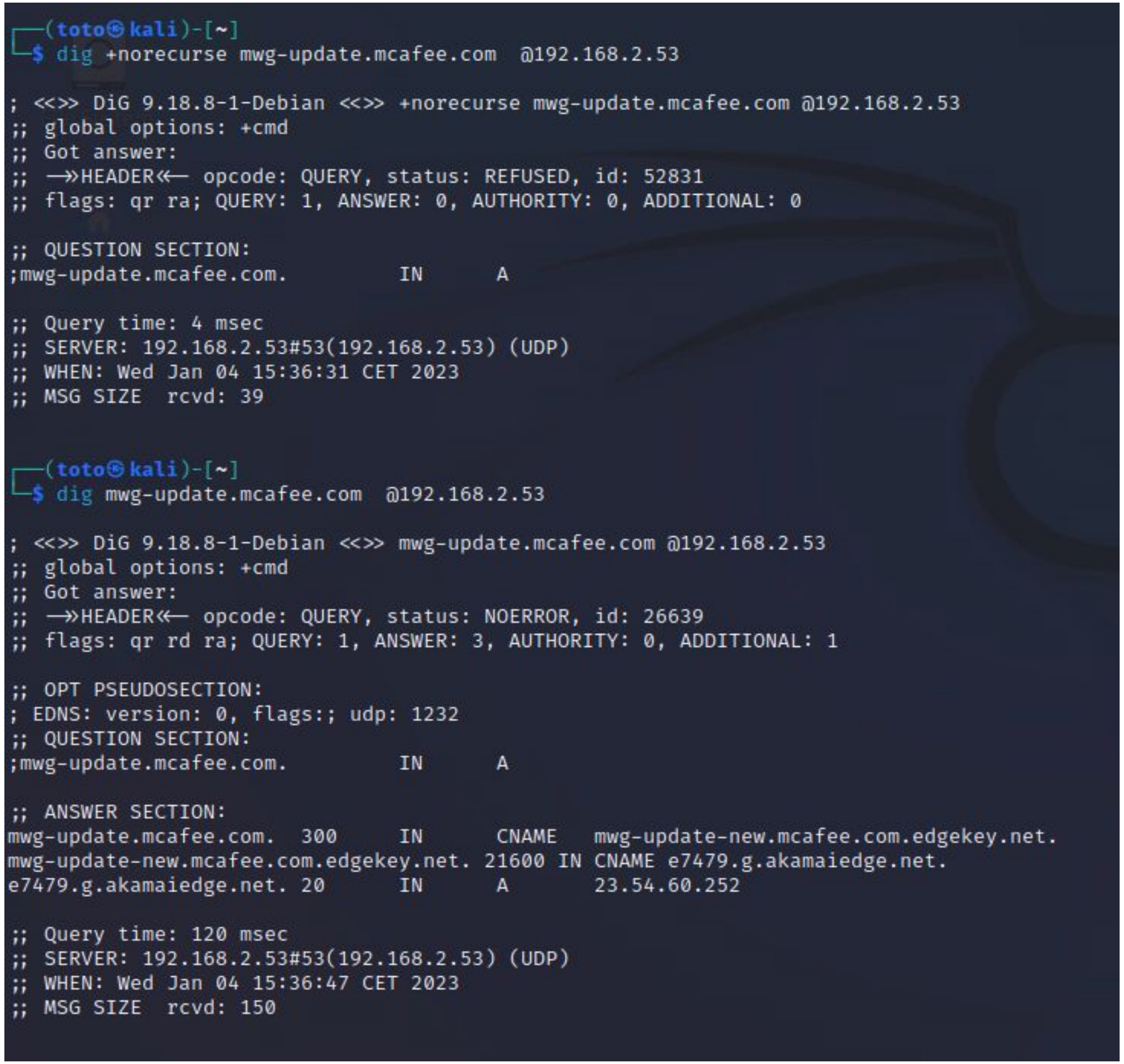
What do you notice compare to results of the bruteforce attack?

What about the wordlists ?

DNS Enumeration

DNS Cache Snooping

- Rely on the usage of the *recursion desired* bit [RD] in the DNS query and by default set to 1 in most cases.
- When setting it to 0 it is possible to discover DNS entries still in cache of the local DNS server.



```
┌──(toto㉿kali)-[~]
└─$ dig +norecurse mwg-update.mcafee.com  @192.168.2.53

; <<>> DiG 9.18.8-1-Debian <<>> +norecurse mwg-update.mcafee.com @192.168.2.53
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: REFUSED, id: 52831
;; flags: qr ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;mwg-update.mcafee.com.         IN      A

;; Query time: 4 msec
;; SERVER: 192.168.2.53#53(192.168.2.53) (UDP)
;; WHEN: Wed Jan 04 15:36:31 CET 2023
;; MSG SIZE  rcvd: 39


┌──(toto㉿kali)-[~]
└─$ dig mwg-update.mcafee.com  @192.168.2.53

; <<>> DiG 9.18.8-1-Debian <<>> mwg-update.mcafee.com @192.168.2.53
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 26639
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;mwg-update.mcafee.com.         IN      A

;; ANSWER SECTION:
mwg-update.mcafee.com.  300     IN      CNAME   mwg-update-new.mcafee.com.edgekey.net.
mwg-update-new.mcafee.com.edgekey.net. 21600 IN CNAME e7479.g.akamaiedge.net.
e7479.g.akamaiedge.net. 20      IN      A       23.54.60.252

;; Query time: 120 msec
;; SERVER: 192.168.2.53#53(192.168.2.53) (UDP)
;; WHEN: Wed Jan 04 15:36:47 CET 2023
;; MSG SIZE  rcvd: 150
```

- Example &/or demo & exercise at the same time of the course

- Recon-ng + dnsrecon -t crt

Scanning

Goals:

- Build a network topology of the target
- Identify IP addresses of live hosts
- Build an exhaustive list of open ports on the live hosts as well as their operating systems
- Identify potential vulnerabilities
- Do not disturb in production systems, especially in industrial environments

Scanning

Types:

1. Network sweeping: Attempt to identify a maximum of live hosts
2. Network tracing: attempt to build the network topology
3. Port scanning: discover the TCP and UDP open ports of live hosts
4. Service versions identification: attempt to grab technical information related to the services running on the discovered open ports
5. OS fingerprinting: attempt to identify the OS of the target host
6. Vulnerability scanning: attempt to find known vulnerabilities on services

Scanning caveats

Load Balancing:

- When scanning or attacking a target domain name, DNS load balancing may be configured to spread the load across multiple server. Use the target IP address instead of the domain name.
- A same IP can be shared across multiple servers for load balancing or redundancy purposes.
- When scanning or attacking a web server **use** the domain name in order to access the right content, especially if it’s a shared web server instance.

Scanning limitations

What may impact scanning performances ?

- Latency
- Bandwidth / Throughput
- Silent Drop, TCP reset, ICMP unreachable

Scanning limitations

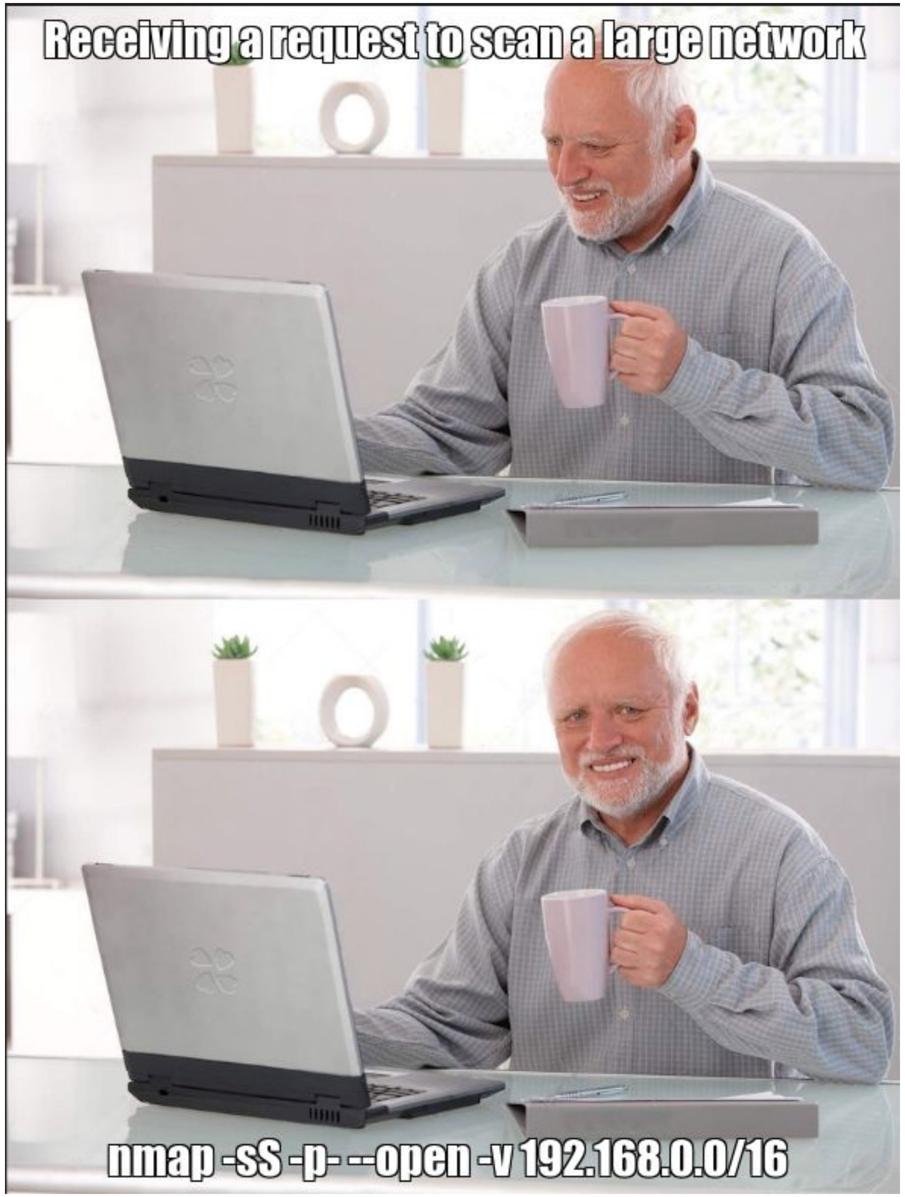
Scanning large networks

- 65536 TCP ports
- 65536 UDP ports
- 2000 hosts
- Baseline 1 sec / port

Do the math …

- Parallelization of port scanning 100 ports / sec

Do the math …


Receiving a request to scan a large network
nmap -sS -p- --open -v 192.168.0.0/16

Scanning limitations

Scanning large networks

As the time might not be reduce, the scope does:

- Reduce the number of ports to scan

OR/AND

- Reduce the number of hosts to scan

OR/AND

- Review firewall rules and adapt the scan (this might hide misconfiguration of firewalls)

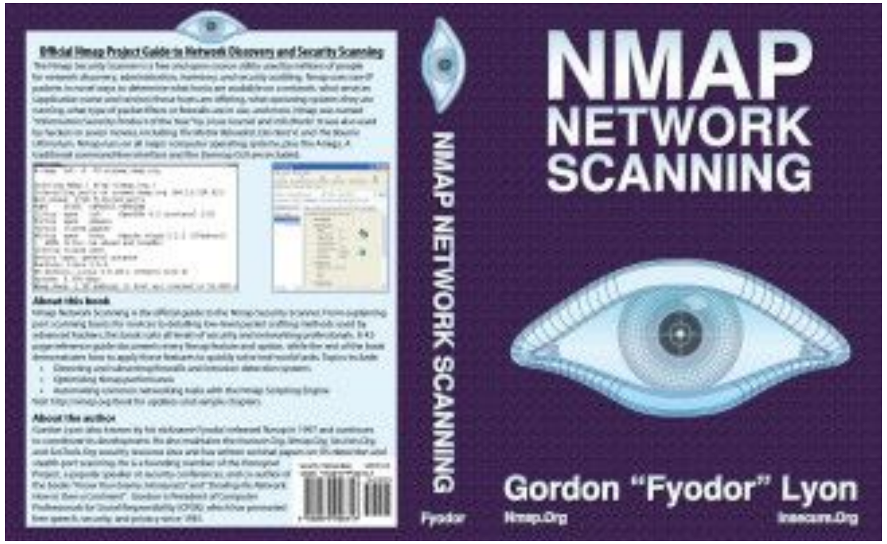
Use specific tools, with custom setup for speeding the port scanning:

- scanrand
- masscan
- …

Nmap has bench of options to optimize scanning time

NMAP (nmap.org)

- Network Scanner but not only….
- Vulnerability Scanner with NSE: Nmap Scripting Engine)
- a huge amount of options in the man pages, and on the site.
- A bible written by the author of Nmap:

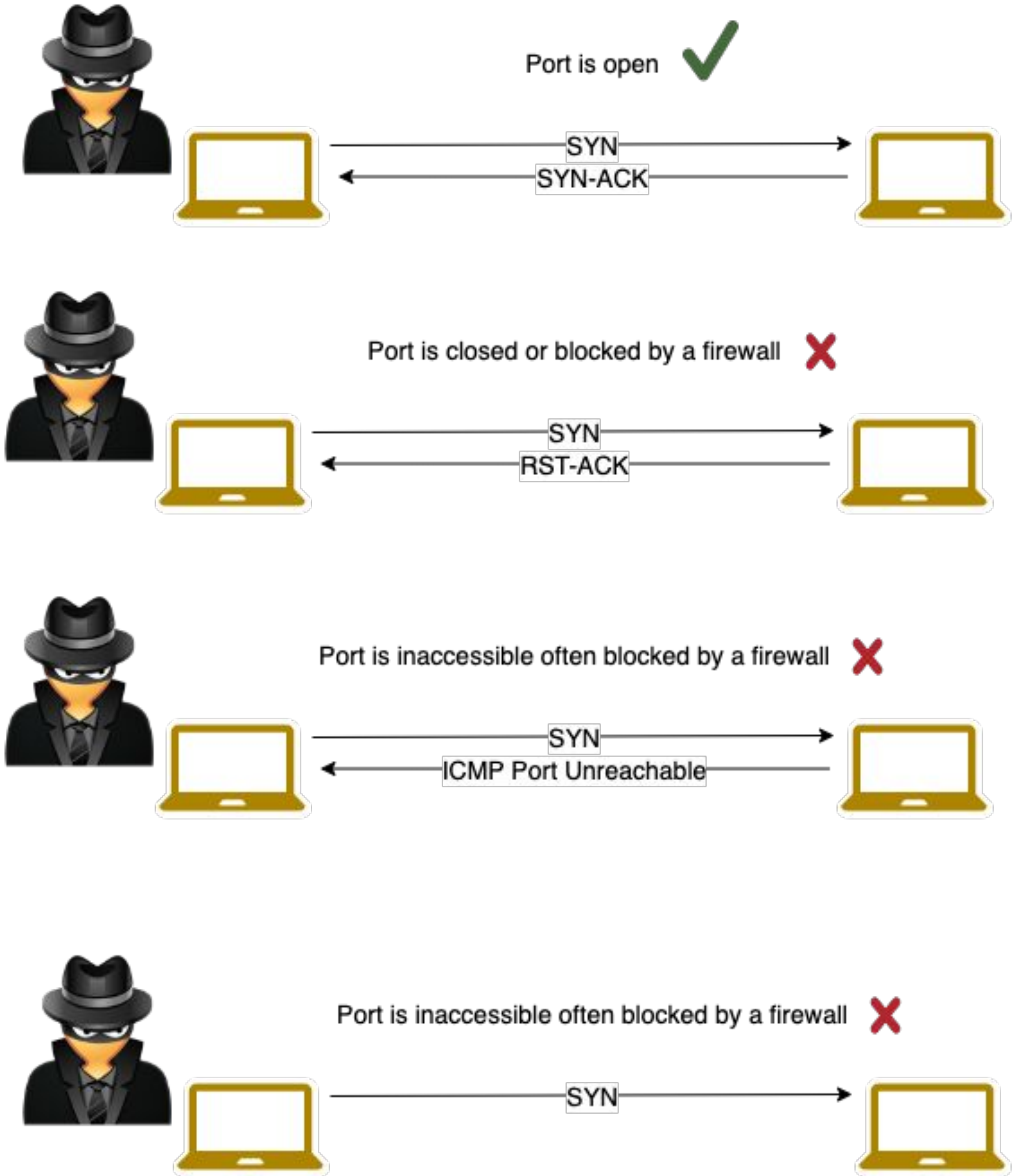


Before Scanning few reminders

TCP behavior illustrated with the TCP half-open scanning

- NMAP port status:
  - Open
  - Close
  - Filtered

- NMAP scanning strongly depends if there is an answer or not.


Port is open ✓
SYN
SYN-ACK
Port is closed or blocked by a firewall ✗
SYN
RST-ACK
Port is inaccessible often blocked by a firewall ✗
SYN
ICMP Port Unreachable
Port is inaccessible often blocked by a firewall ✗
SYN

Before Scanning few reminders

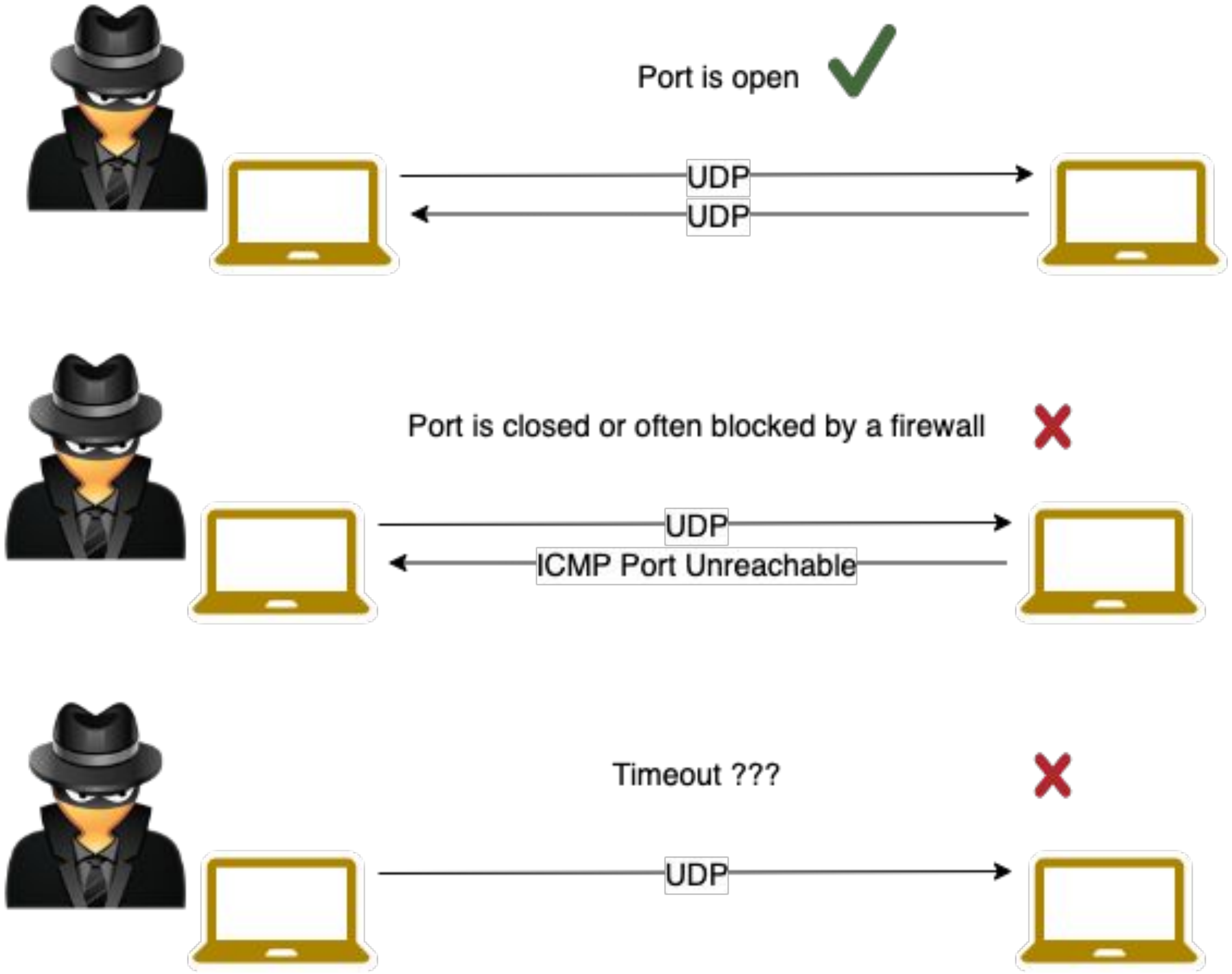
- Other ICMP messages types might be send back.
- A TCP full handshake scan is also possible.

Before Scanning few reminders

UDP behavior illustrated

- Depending on the target system the ICMP messages sent might be throttled

- Other ICMP type messages can be sent back changing NMAP port status to filtered

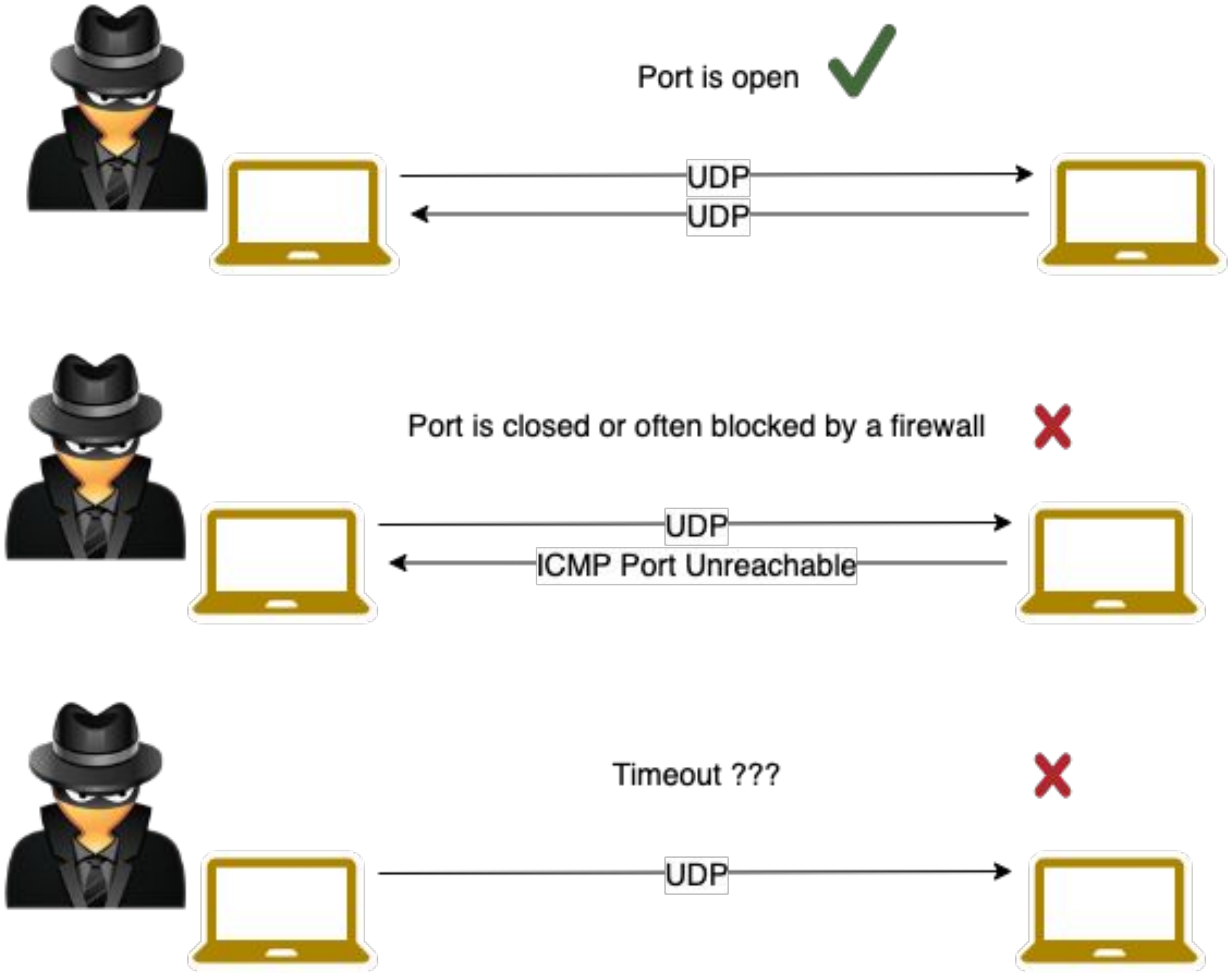


Before Scanning few reminders

UDP behavior illustrated

- If nothing comes back … timeout:
  - Firewall block inbound request?
  - Firewall block outbound request?
  - Port is closed
  - A service is open but waiting for a specific payload to answer.

- For few common UDP ports NMAP send a valid payload (dns, snmp,...)



Let’s start using NMAP

Network Sweeping

Objective: Mapping potential target by sending probes

- Bench of probes are possible with NMAP (manual page)
- When performing a network sweep on the same subnet:
  - -PR: use ARP to collect alive hosts (implicitly done by nmap when scanning the same network as the scanner)
- When performing a network sweep on another network:
  - Different options are possible, the classic one is: -sP
- If you don’t want to probe the targets and start the scan:
  - -Pn: do not Probe (hosts are considered alive)

Network Sweeping

Objective: Mapping potential target by sending probes

- Perform a Network Sweep of the target network (10.66.66.0/24)

```
nmap -sP 10.66.66.0/24
```

Network Sweeping

Objective: Mapping potential target by sending probes

Result:

- Not really interesting in this context, but might be useful to quickly identify targets on a large network.
- Enumeration must continue….

Port Scanning

Objective: Finding Open Ports

TCP Scan:

- Specify TCP scan type, numerous are available
  - Connect Scan (sT)
  - SYN Stealth Scan (sS)
  - ACK Scan (sA)
  - FIN Scan (sF)
  - NULL Scan (sN)
  - And others
  - TCP flags can also be adjusted as desired

UDP Scan just use (sU)

Port Scanning

Objective: Finding Open Ports

TCP Scan:

- Specify the list of ports to scan, numerous options are available (man page), but the syntax is simple:
  - -p 0-65535 (scan all the port range)
  - -p 22,445,80 (scan a list of port)
  - …
- Using:
  - -F (scan top 100 ports most used)
  - –top-ports 1000 (scan top 1000 ports most used)
- Nmap use a file with port and service mapping, find it !

nmap-services file path:

Port Scanning

Objective: Finding Open Ports

Timing Options:

- By default NMAP has an adaptive scanning model, but options are available to force a behavior:
  - -T 0: Paranoid mode very slow (scan in serial)
  - -T1: Sneaky (scan in serial)
  - -T2: Polite (scan in serial)
  - -T3: Default (scan in parallel)
  - -T4: Aggressive (scan in parallel short timeout for probe responses)
  - -T5: Insane (scan in parallel,short timeout and maximum 15min/host)

Port Scanning

Saving the outputs:

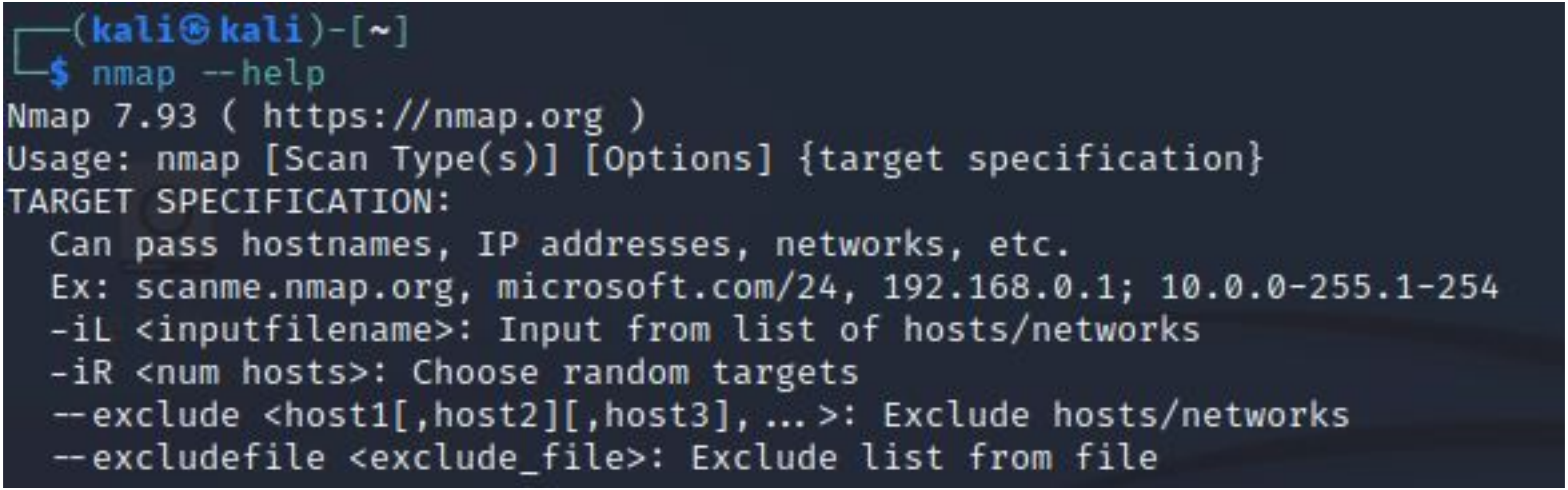
Nmap offers different options to filter the output and to save it:

- Storing results
  - -oX FILENAME: save with XML format
  - -oG FILENAME: save with Greppable format
  - -oN: FILENAME: save with Nmap output
  - -oA: FILENAME: save with All the previous format

- Filtering results:
  - TIPS: add –open to only show open ports.

Port Scanning

Let’s Scan the target



```
┌──(kali㉿kali)-[~]
└─$ nmap --help
Nmap 7.93 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
```

Port Scanning

Let’s Scan the target

Propose a basic nmap command to scan the target network (10.66.66.0/24).

Propose an enhanced nmap command to scan the target network (10.66.66.0/24).

When nmap is running try pressing these key strokes: p, Shift+p, d, Shift+d

What does it do ?

```
p
Shift+p
d
Shift+d
V
Shift+v
```

Service and Version Identification

NMAP is build with probes to try to find services and versions on open ports

- -sV: Version scan

Propose a new enhanced nmap command to scan the target network with the Service and Version identification attempt, display only open ports and save the results into various formats:

What is very important to notice compare to the previous results?

OS Fingerprinting and

NMAP is build with methods to try to detect OS of the target

- -O: perform OS fingerprinting

NMAP is also a vulnerability scanner (details in the coming slides)

- -sC: run nmap scripting engine in the default category

NMAP provide a all in one argument

- -A: run nmap with -O -sV -sV –traceroute

Try a new nmap command to scan the target (vple.megacorp.corp) with the all in one argument:

Have a look at the results, did some information ring a bell ?

Vulnerability Scanning and Exploitation

Thank you

AIRBUS