What is Cyber Security

SoftUni Team

Technical Trainers

Software University

SoftUni

Software University

https://softuni.bg

Have a Question?

Software University

sli.do

#Cyber_Security

Table of Contents

1. Cyber Security in a Nutshell
2. Cyber Security Fundamentals
   - Exploit
   - Vulnerability
   - Payload
   - Attack
   - FirewallIDS / IPS
3. How to Stay Safe Online?

Cyber Security in a Nutshell

Cyber Security in a Nutshell

- **Protection**
  - Of informational or infrastructural assets
- **Dedication**
  - It is a hard job being a protector, no matter which skill path you pick
- **Professionalism**
  - It is a responsible job and must be executed with high level of professionalism
- **Embrace yourself** for a LOT of terminology

Why Cyber Security is IMPORTANT?

- We live in a digital world where:
  - **Your money is digital**
  - **Your personal data is digital**
  - **Your almost everything else is digital**
- Someone must look after these kind of things, the industry is hungry for **new joiners**
- We have a lot to cover so let's start with some terms

Cyber Security Fundamentals

What is Asset?

- An **asset** is any data, device or other component of an organization's systems that is valuable – often because it contains sensitive data or can be used to access such information
- For example, an employee's desktop computer, laptop or company phone would be considered an asset, as would **applications on those devices**
- Likewise, critical infrastructure, such as **servers** and **support systems**, are assets

What is Asset?

- An organization's most common assets are **information assets**
- These are things such as **databases** and **physical files** – i.e. the sensitive data that you store
- A related concept is the "**information asset container**", which is where that information is kept
- In the case of databases, this would be the application that was **used to create the database**
- For physical files, it would be the filing cabinet where the **information resides**

What is a Threat?

- A **threat** is any incident that could **negatively affect an asset**
- For example, if it's lost, knocked offline or accessed by an unauthorized party
- Threats can be categorized as circumstances that compromise the **confidentiality**, **integrity** or **availability** of an asset, and can either be intentional or accidental

What is a Threat?

- Intentional threats include things such as **criminal hacking** or a **malicious** insider stealing information, whereas accidental threats generally involve **employee error**, a **technical malfunction** or an **event** that causes physical damage, such as a fire or natural disaster

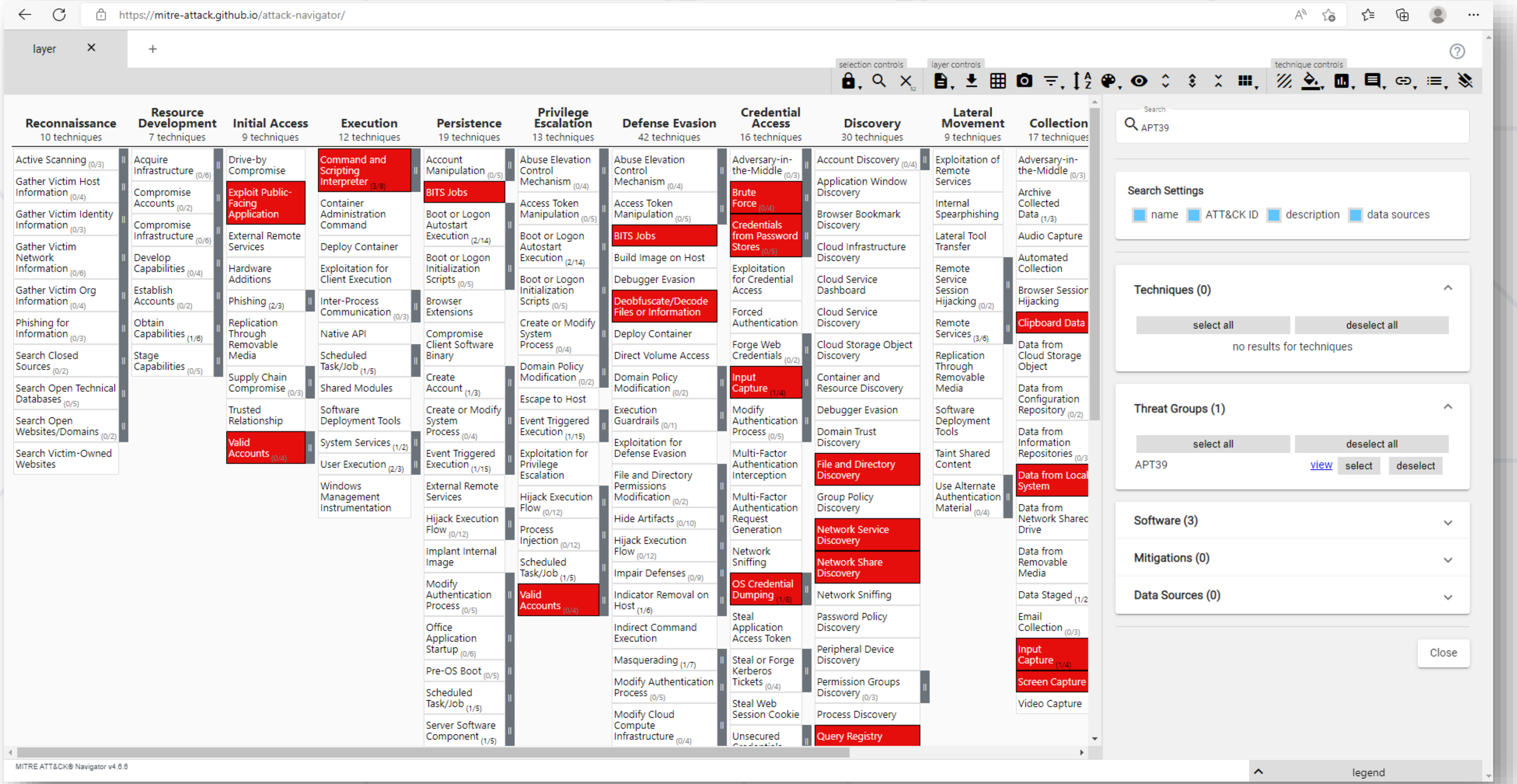
What is a Threat Actor?

- Someone with **malicious intentions**, ready to inflict **real harm**
- These are the bad guys, as known as "**Black Hats**"
- Threat actors are recorded as **Advanced Persistent Threats** (APT)

There are Frameworks for Recording Threat Actions!

Software University

- ATT & CK (https://attack.mitre.org/)



https://mitre-attack.github.io/attack-navigator/

layer

Reconnaissance
10 techniques

- Active Scanning (0/3)
- Gather Victim Host Information (0/4)
- Gather Victim Identity Information (0/3)
- Gather Victim Network Information (0/6)
- Gather Victim Org Information (0/4)
- Phishing for Information (0/3)
- Search Closed Sources (0/2)
- Search Open Technical Databases (0/5)
- Search Open Websites/Domains (0/2)
- Search Victim-Owned Websites

Resource Development
7 techniques

- Acquire Infrastructure (0/6)
- Compromise Accounts (0/2)
- Compromise Infrastructure (0/6)
- Develop Capabilities (0/4)
- Establish Accounts (0/2)
- Obtain Capabilities (1/6)
- Stage Capabilities (0/5)

Initial Access
9 techniques

- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing (2/3)
- Replication Through Removable Media
- Supply Chain Compromise (0/3)
- Trusted Relationship
- Valid Accounts (0/4)

Execution
12 techniques

- Command and Scripting Interpreter (3/8)
- Container Administration Command
- Deploy Container
- Exploitation for Client Execution
- Inter-Process Communication (0/3)
- Native API
- Scheduled Task/Job (1/5)
- Shared Modules
- Software Deployment Tools
- System Services (1/2)
- User Execution (2/3)
- Windows Management Instrumentation

Persistence
19 techniques

- Account Manipulation (0/5)
- BITS Jobs
- Boot or Logon Autostart Execution (2/14)
- Boot or Logon Initialization Scripts (0/5)
- Browser Extensions
- Compromise Client Software Binary
- Create Account (1/3)
- Create or Modify System Process (0/4)
- Event Triggered Execution (1/15)
- External Remote Services
- Hijack Execution Flow (0/12)
- Implant Internal Image
- Modify Authentication Process (0/5)
- Office Application Startup (0/6)
- Pre-OS Boot (0/5)
- Scheduled Task/Job (1/5)
- Server Software Component (1/5)

Privilege Escalation
13 techniques

- Abuse Elevation Control Mechanism (0/4)
- Access Token Manipulation (0/5)
- Boot or Logon Autostart Execution (2/14)
- Boot or Logon Initialization Scripts (0/5)
- Create or Modify System Process (0/4)
- Domain Policy Modification (0/2)
- Escape to Host
- Event Triggered Execution (1/15)
- Exploitation for Privilege Escalation
- Hijack Execution Flow (0/12)
- Process Injection (0/12)
- Scheduled Task/Job (1/5)
- Valid Accounts (0/4)

Defense Evasion
42 techniques

- Abuse Elevation Control Mechanism (0/4)
- Access Token Manipulation (0/5)
- BITS Jobs
- Build Image on Host
- Debugger Evasion
- Deobfuscate/Decode Files or Information
- Deploy Container
- Direct Volume Access
- Domain Policy Modification (0/2)
- Execution Guardrails (0/1)
- Exploitation for Defense Evasion
- File and Directory Permissions Modification (0/2)
- Hide Artifacts (0/10)
- Hijack Execution Flow (0/12)
- Impair Defenses (0/9)
- Indicator Removal on Host (1/6)
- Indirect Command Execution
- Masquerading (1/7)
- Modify Authentication Process (0/5)
- Modify Cloud Compute Infrastructure (0/4)

Credential Access
16 techniques

- Adversary-in-the-Middle (0/3)
- Brute Force (0/4)
- Credentials from Password Stores (0/5)
- Exploitation for Credential Access
- Forced Authentication
- Forge Web Credentials (0/2)
- Input Capture (1/4)
- Modify Authentication Process (0/5)
- Multi-Factor Authentication Interception
- Multi-Factor Authentication Request Generation
- Network Sniffing
- OS Credential Dumping (1/8)
- Steal Application Access Token
- Steal or Forge Kerberos Tickets (0/4)
- Steal Web Session Cookie
- Unsecured

Discovery
30 techniques

- Account Discovery (0/4)
- Application Window Discovery
- Browser Bookmark Discovery
- Cloud Infrastructure Discovery
- Cloud Service Dashboard
- Cloud Service Discovery
- Cloud Storage Object Discovery
- Container and Resource Discovery
- Debugger Evasion
- Domain Trust Discovery
- File and Directory Discovery
- Group Policy Discovery
- Network Service Discovery
- Network Share Discovery
- Network Sniffing
- Password Policy Discovery
- Peripheral Device Discovery
- Permission Groups Discovery (0/3)
- Process Discovery
- Query Registry

Lateral Movement
9 techniques

- Exploitation of Remote Services
- Internal Spearphishing
- Lateral Tool Transfer
- Remote Service Session Hijacking (0/2)
- Remote Services (3/6)
- Replication Through Removable Media
- Software Deployment Tools
- Taint Shared Content
- Use Alternate Authentication Material (0/4)

Collection
17 techniques

- Adversary-in-the-Middle (0/3)
- Archive Collected Data (1/3)
- Audio Capture
- Automated Collection
- Browser Session Hijacking
- Clipboard Data
- Data from Cloud Storage Object
- Data from Configuration Repository (0/2)
- Data from Information Repositories (0/3
- Data from Local System
- Data from Network Shared Drive
- Data from Removable Media
- Data Staged (1/2
- Email Collection (0/3)
- Input Capture (1/4)
- Screen Capture
- Video Capture

Search
APT39

Search Settings
☑ name ☑ ATT&CK ID ☑ description ☑ data sources

Techniques (0)
select all | deselect all
no results for techniques

Threat Groups (1)
select all | deselect all
APT39 view select deselect

Software (3)

Mitigations (0)

Data Sources (0)

Close

MITRE ATT&CK® Navigator v4.6.6

legend

What Types of Hackers we Have?

- **White Hats** – Ethical Hackers
  - They hack only with agreement and report every security issue
- **Grey Hats** – Bug Bounty hunters
  - They hack illegal but do not compromise or breach a company, instead they ask for a bounty
- **Black Hats** – Complete Cyber Criminals

What is a Breach?

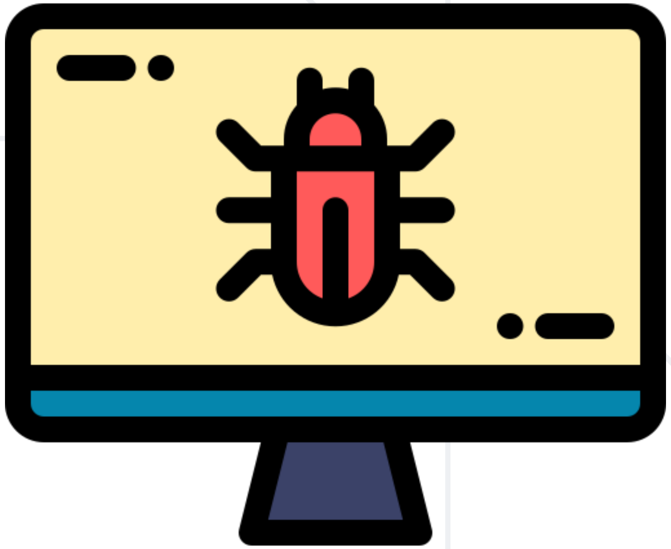
- **Breach** is when the threat successfully executes it's malicious activities
- Every breach is **devastating for the company** (reputation and money are lost in almost all of the cases)
- Cyber Security is about **reducing the risk of breach**, and even if one happen, to **deflect it as soon as possible**

What is Malware?

- **Malware** stands for Malicious Software
- Malwares are having many types, some of which are:
  - Ransomware
  - Adware
  - Trojans

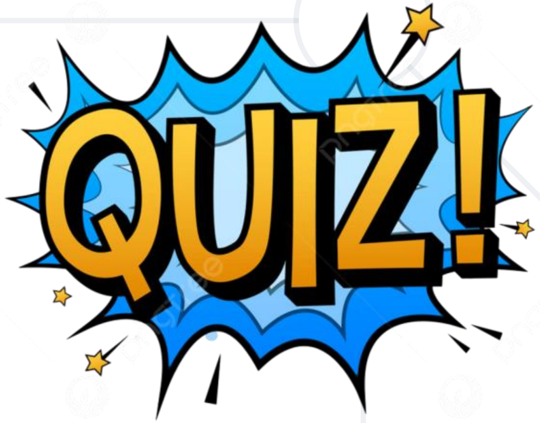
What is Vulnerability?

- **Vulnerability** is context condition, making the targeted application / infrastructure vulnerable to cyber attacks
- Vulnerability = Weakness
- More about vulnerabilities next week ☺



Quiz

Is having a password like "123456" or "Qwerty123" a vulnerability?

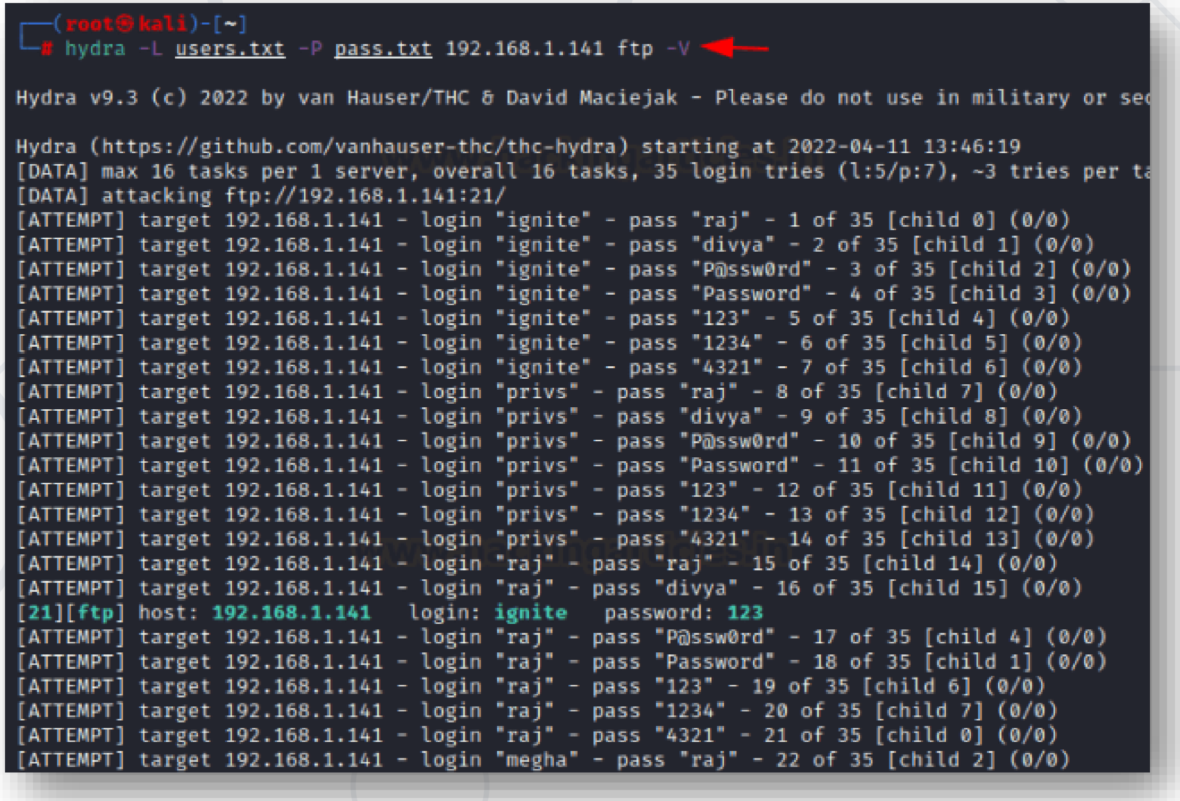


What is Exploit?

- **Exploit** is the action that a threat is utilizing to attack or "exploit" the vulnerability
- In most of the cases, exploitation is focused for:
  - **Getting access**
  - **Escalating privileges**
  - **Stealing data**
  - **Attack Pivoting**

Example Exploit

- Vulnerability is you **having a weak password**
- Exploitation is someone **brute-forcing it with hydra**



```
┌──(root㉿kali)-[~]
└─# hydra -L users.txt -P pass.txt 192.168.1.141 ftp -V

Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or sec

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-04-11 13:46:19
[DATA] max 16 tasks per 1 server, overall 16 tasks, 35 login tries (l:5/p:7), ~3 tries per ta
[DATA] attacking ftp://192.168.1.141:21/
[ATTEMPT] target 192.168.1.141 - login "ignite" - pass "raj" - 1 of 35 [child 0] (0/0)
[ATTEMPT] target 192.168.1.141 - login "ignite" - pass "divya" - 2 of 35 [child 1] (0/0)
[ATTEMPT] target 192.168.1.141 - login "ignite" - pass "P@ssw0rd" - 3 of 35 [child 2] (0/0)
[ATTEMPT] target 192.168.1.141 - login "ignite" - pass "Password" - 4 of 35 [child 3] (0/0)
[ATTEMPT] target 192.168.1.141 - login "ignite" - pass "123" - 5 of 35 [child 4] (0/0)
[ATTEMPT] target 192.168.1.141 - login "ignite" - pass "1234" - 6 of 35 [child 5] (0/0)
[ATTEMPT] target 192.168.1.141 - login "ignite" - pass "4321" - 7 of 35 [child 6] (0/0)
[ATTEMPT] target 192.168.1.141 - login "privs" - pass "raj" - 8 of 35 [child 7] (0/0)
[ATTEMPT] target 192.168.1.141 - login "privs" - pass "divya" - 9 of 35 [child 8] (0/0)
[ATTEMPT] target 192.168.1.141 - login "privs" - pass "P@ssw0rd" - 10 of 35 [child 9] (0/0)
[ATTEMPT] target 192.168.1.141 - login "privs" - pass "Password" - 11 of 35 [child 10] (0/0)
[ATTEMPT] target 192.168.1.141 - login "privs" - pass "123" - 12 of 35 [child 11] (0/0)
[ATTEMPT] target 192.168.1.141 - login "privs" - pass "1234" - 13 of 35 [child 12] (0/0)
[ATTEMPT] target 192.168.1.141 - login "privs" - pass "4321" - 14 of 35 [child 13] (0/0)
[ATTEMPT] target 192.168.1.141 - login "raj" - pass "raj" - 15 of 35 [child 14] (0/0)
[ATTEMPT] target 192.168.1.141 - login "raj" - pass "divya" - 16 of 35 [child 15] (0/0)
[21][ftp] host: 192.168.1.141   login: ignite   password: 123
[ATTEMPT] target 192.168.1.141 - login "raj" - pass "P@ssw0rd" - 17 of 35 [child 4] (0/0)
[ATTEMPT] target 192.168.1.141 - login "raj" - pass "Password" - 18 of 35 [child 1] (0/0)
[ATTEMPT] target 192.168.1.141 - login "raj" - pass "123" - 19 of 35 [child 6] (0/0)
[ATTEMPT] target 192.168.1.141 - login "raj" - pass "1234" - 20 of 35 [child 7] (0/0)
[ATTEMPT] target 192.168.1.141 - login "raj" - pass "4321" - 21 of 35 [child 0] (0/0)
[ATTEMPT] target 192.168.1.141 - login "megha" - pass "raj" - 22 of 35 [child 2] (0/0)
```

What is Payload?

- The actions that **comes after the exploitation**
- Usually this is the **malicious code for C2** (Command and Control)
- It is obfuscated in 99% of the time in order to evade **anti-virus** and **other security measurements**

Attack Chain

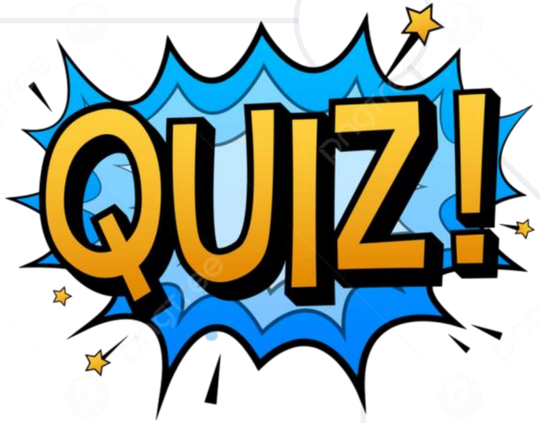
- It is also called "**kill chain**"
- The usual attack chain is the following:
  - **Find a vulnerability**
  - **Develop / Find an exploit for that vulnerability**
  - **Modify the exploit with custom payload**
  - **Exploit the vulnerability**

What is Phishing?

- Malicious act for **stealing personal data**
- Phishing is dangerous, since it attacks the weakest part of the cyber security – people!
- Phishing attacks are **massive** and can be performed with various of ways, such as:
  - **Phishing e-mails**
  - **SMSishng**
  - **Voice Phishing**

Quiz

Is a phishing attack a vulnerability or an exploit?

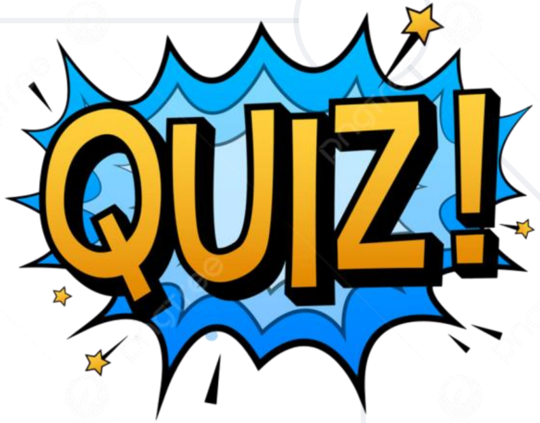


Phishing Attack is an Exploit

- Vulnerability by **itself is not dangerous**, a vulnerability can sit **unexploited for years**!
- The danger is **when a vulnerability is Exploited**, that is where the problems starts
- Since phishing attacks are **actually stealing data**, it can be considered exploit

Quiz

If phishing attack is an exploit act, what is the vulnerability?



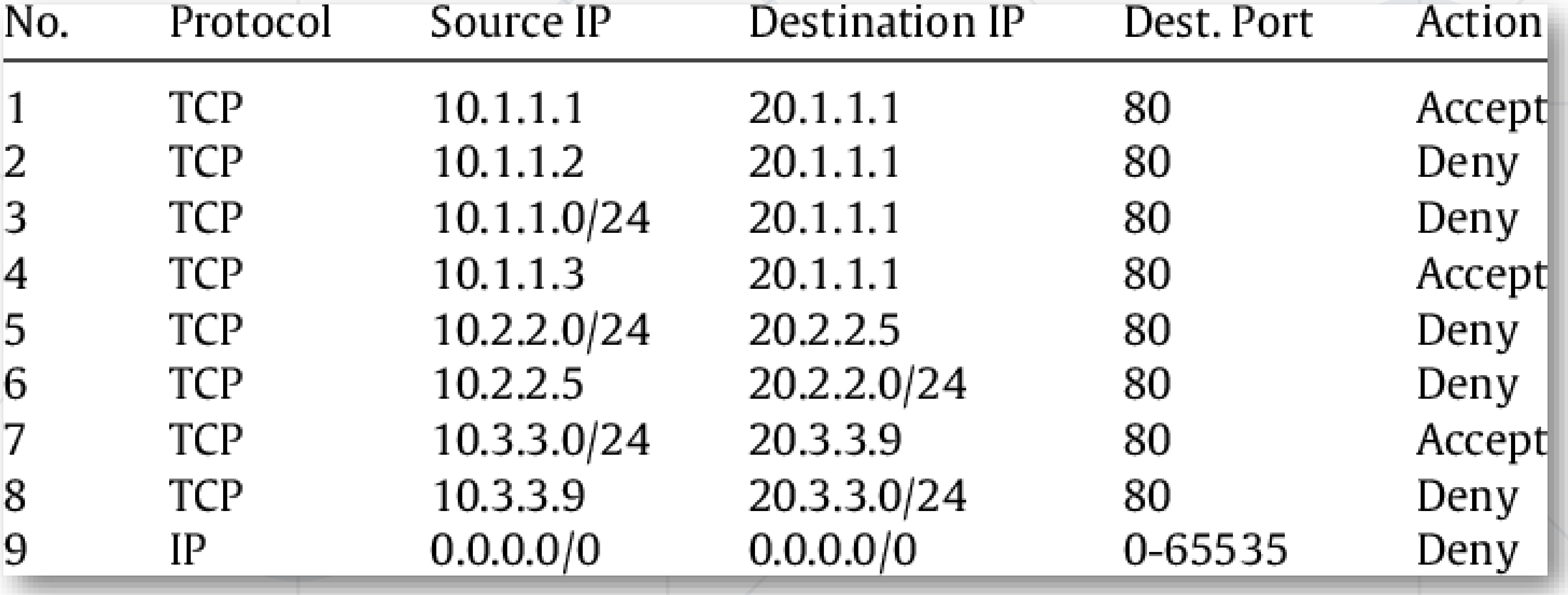
Maybe we Are not so Perfect

- The vulnerability here is **not just one**, but let's point them out:
  - The systems that allowed the **phishing mail to successfully come into the person's inbox**
  - The security mechanisms that did not stop you whenever you **opened up the phishing email's content**
  - We cannot count **entirely on systems**, since we built them after all
  - The last vulnerability is the human **clicking and following phishing's instructions**

What is a Firewall?

- Security mechanism to **filter traffic**, based on **predefined rules**
- It can be **software** / **hardware**
- Firewall is a **must in every company**

Firewall Rule Visualization



No.	Protocol	Source IP	Destination IP	Dest. Port	Action
1	TCP	10.1.1.1	20.1.1.1	80	Accept
2	TCP	10.1.1.2	20.1.1.1	80	Deny
3	TCP	10.1.1.0/24	20.1.1.1	80	Deny
4	TCP	10.1.1.3	20.1.1.1	80	Accept
5	TCP	10.2.2.0/24	20.2.2.5	80	Deny
6	TCP	10.2.2.5	20.2.2.0/24	80	Deny
7	TCP	10.3.3.0/24	20.3.3.9	80	Accept
8	TCP	10.3.3.9	20.3.3.0/24	80	Deny
9	IP	0.0.0.0/0	0.0.0.0/0	0-65535	Deny

What is IDS?

Intrusion Detection System

- An **alert system**, upon a security event is triggered
- It works on **predefined security rules**
- It does **not provide protection**, just **alert** on trigger

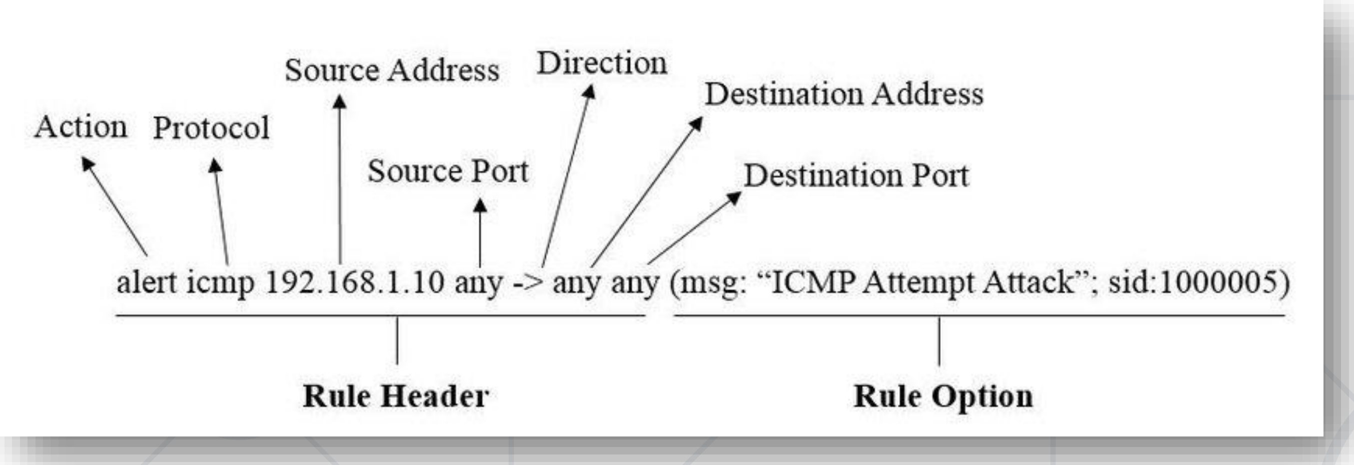
What is IPS?

Intrusion Prevention System

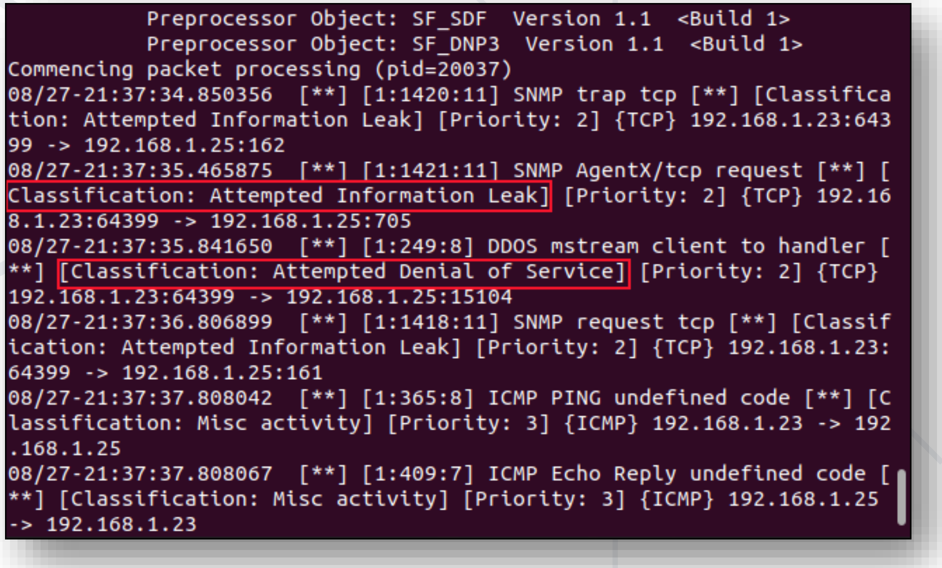
- Security system for **catching** and **preventing security threats**
- It works on **predefined security rules**, just like IPS
- Instead of only alerting, it performs **auto-mitigation actions** such as:
  - **Blocking IP**
  - **Closing local ports**
  - **Redirecting traffic and more**

IDS / IPS Example

- Snort: https://www.snort.org/



alert icmp 192.168.1.10 any -> any any (msg: “ICMP Attempt Attack”; sid:1000005)



```
           Preprocessor Object: SF_SDF  Version 1.1  <Build 1>
           Preprocessor Object: SF_DNP3  Version 1.1  <Build 1>
Commencing packet processing (pid=20037)
08/27-21:37:34.850356  [**] [1:1420:11] SNMP trap tcp [**] [Classifica
tion: Attempted Information Leak] [Priority: 2] {TCP} 192.168.1.23:643
99 -> 192.168.1.25:162
08/27-21:37:35.465875  [**] [1:1421:11] SNMP AgentX/tcp request [**] [
Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.16
8.1.23:64399 -> 192.168.1.25:705
08/27-21:37:35.841650  [**] [1:249:8] DDOS mstream client to handler [
**] [Classification: Attempted Denial of Service] [Priority: 2] {TCP}
192.168.1.23:64399 -> 192.168.1.25:15104
08/27-21:37:36.806899  [**] [1:1418:11] SNMP request tcp [**] [Classif
ication: Attempted Information Leak] [Priority: 2] {TCP} 192.168.1.23:
64399 -> 192.168.1.25:161
08/27-21:37:37.808042  [**] [1:365:8] ICMP PING undefined code [**] [C
lassification: Misc activity] [Priority: 3] {ICMP} 192.168.1.23 -> 192
.168.1.25
08/27-21:37:37.808067  [**] [1:409:7] ICMP Echo Reply undefined code [
**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.1.25
-> 192.168.1.23
```

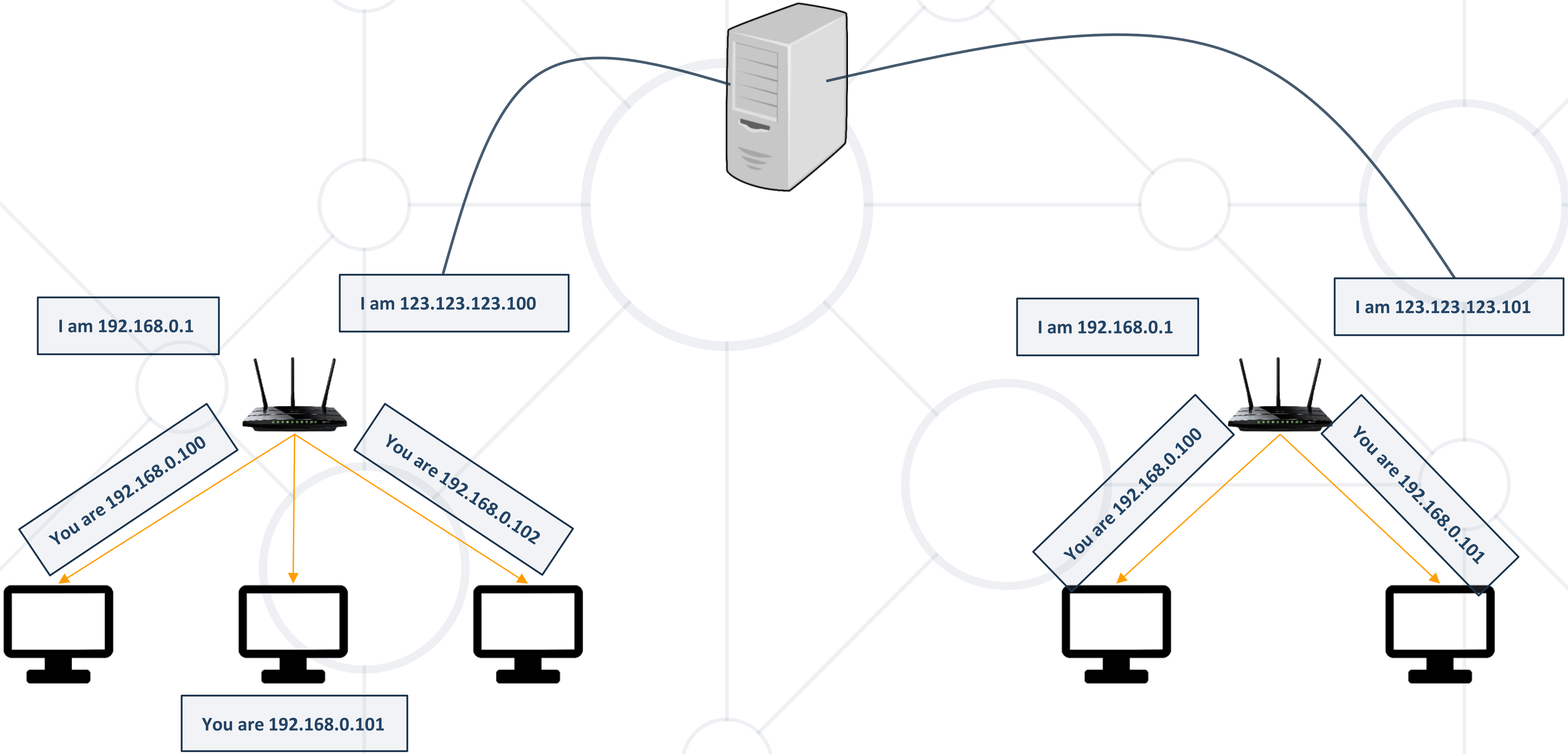
What is IP Address?

- IP address is like a **real address**, but in the **internet space**
- It consist of **4x (IPv4)** or **6x (IPv6)** characters
- Examples:
  - **192.168.0.1 / 45.33.32.156 (IPv4)**
  - **2001:0db8:85a3:0000:0000:8a2e:0370:7334 (IPv6)**

External vs Internal IP Address

- **External address** is the IP that exits the router (gateway)
- **Internal addresses** are inside your local network, containers or virtualizations

External vs Internal IP Address Visual Representation



I am 192.168.0.1

I am 123.123.123.100

You are 192.168.0.100

You are 192.168.0.102

You are 192.168.0.101

I am 192.168.0.1

I am 123.123.123.101

You are 192.168.0.100

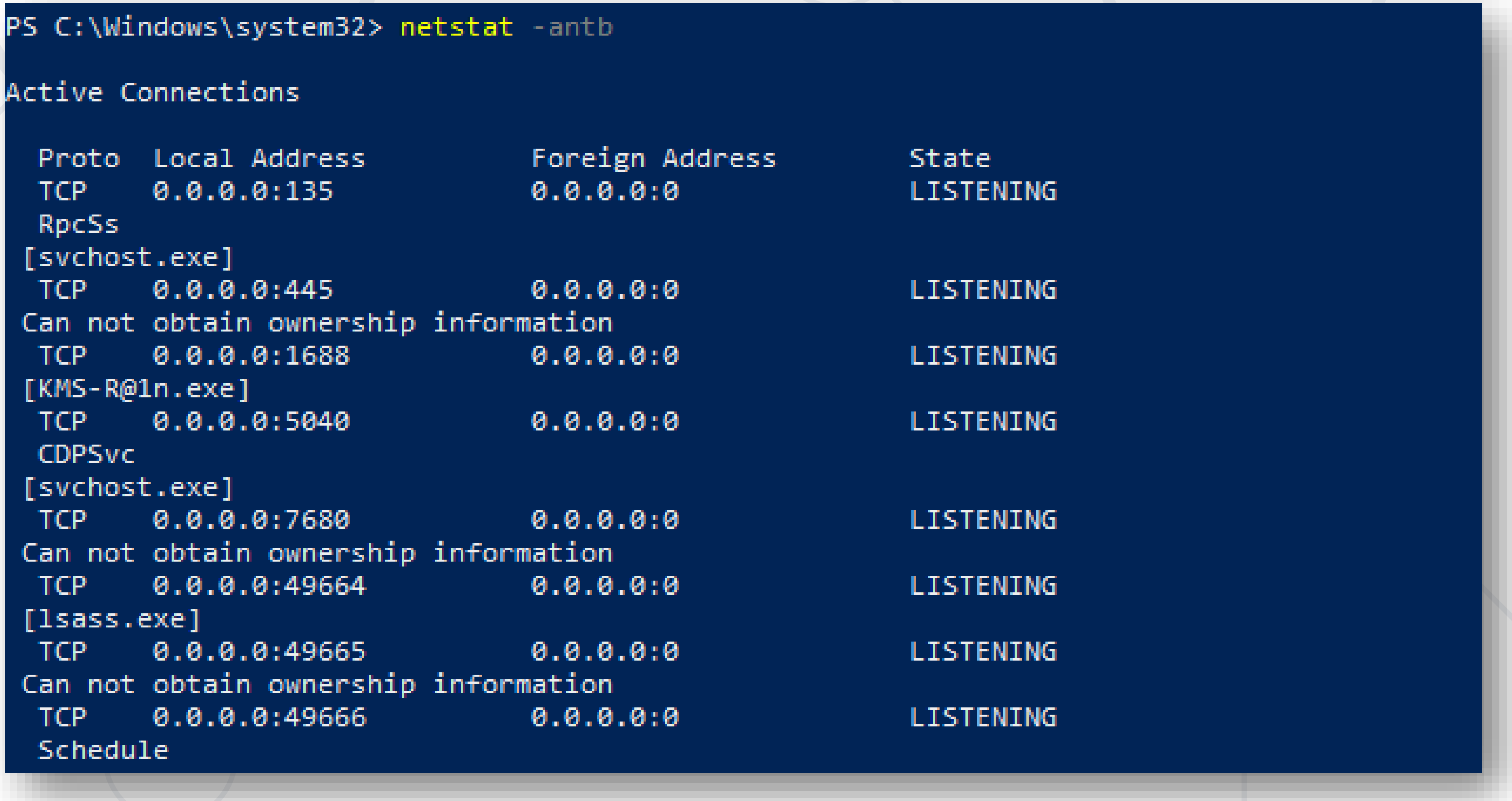
You are 192.168.0.101

What is Port?

- Where the **packet is actually being received**
- The IP is the **house**, the port is the **door**
- Example ports / service:
  - **22 / SSH**
  - **80 / HTTP**
  - **443 / HTTPS**
  - **389 / LDAP**

How to Check What Ports are Opened on Your PC?

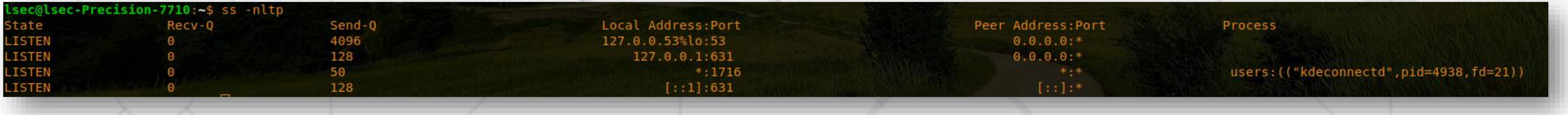
- Windows:
  - **netstat –an**
  - **netstat –antb**



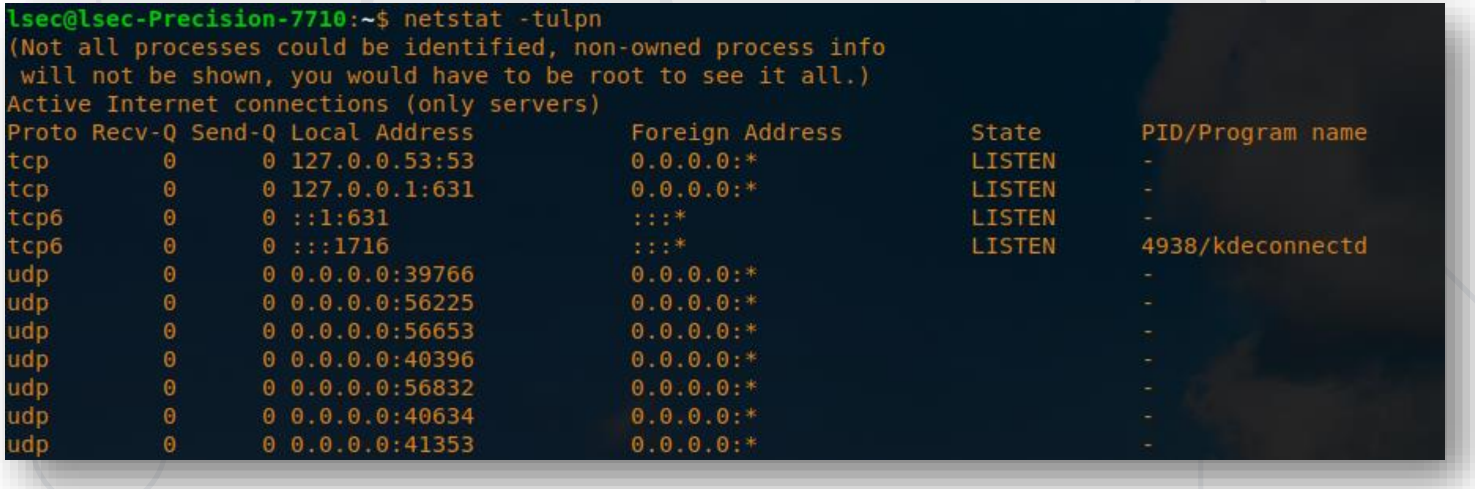
```
PS C:\Windows\system32> netstat -antb

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  RpcSs
 [svchost.exe]
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
 Can not obtain ownership information
  TCP    0.0.0.0:1688           0.0.0.0:0              LISTENING
 [KMS-R@1n.exe]
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING
  CDPSvc
 [svchost.exe]
  TCP    0.0.0.0:7680           0.0.0.0:0              LISTENING
 Can not obtain ownership information
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING
 [lsass.exe]
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING
 Can not obtain ownership information
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING
  Schedule
```

How to Check What Ports are Opened on Your PC?

- Unix:
  - **ss –nltp**
  - **netstat –tulpn**



```
lsec@lsec-Precision-7710:~$ ss -nltp
State                Recv-Q               Send-Q                             Local Address:Port                              Peer Address:Port              Process
LISTEN               0                    4096                               127.0.0.53%lo:53                                     0.0.0.0:*
LISTEN               0                    128                                    127.0.0.1:631                                    0.0.0.0:*
LISTEN               0                    50                                             *:1716                                       *:*                   users:(("kdeconnectd",pid=4938,fd=21))
LISTEN               0                    128                                        [::1]:631                                     [::]:*
```



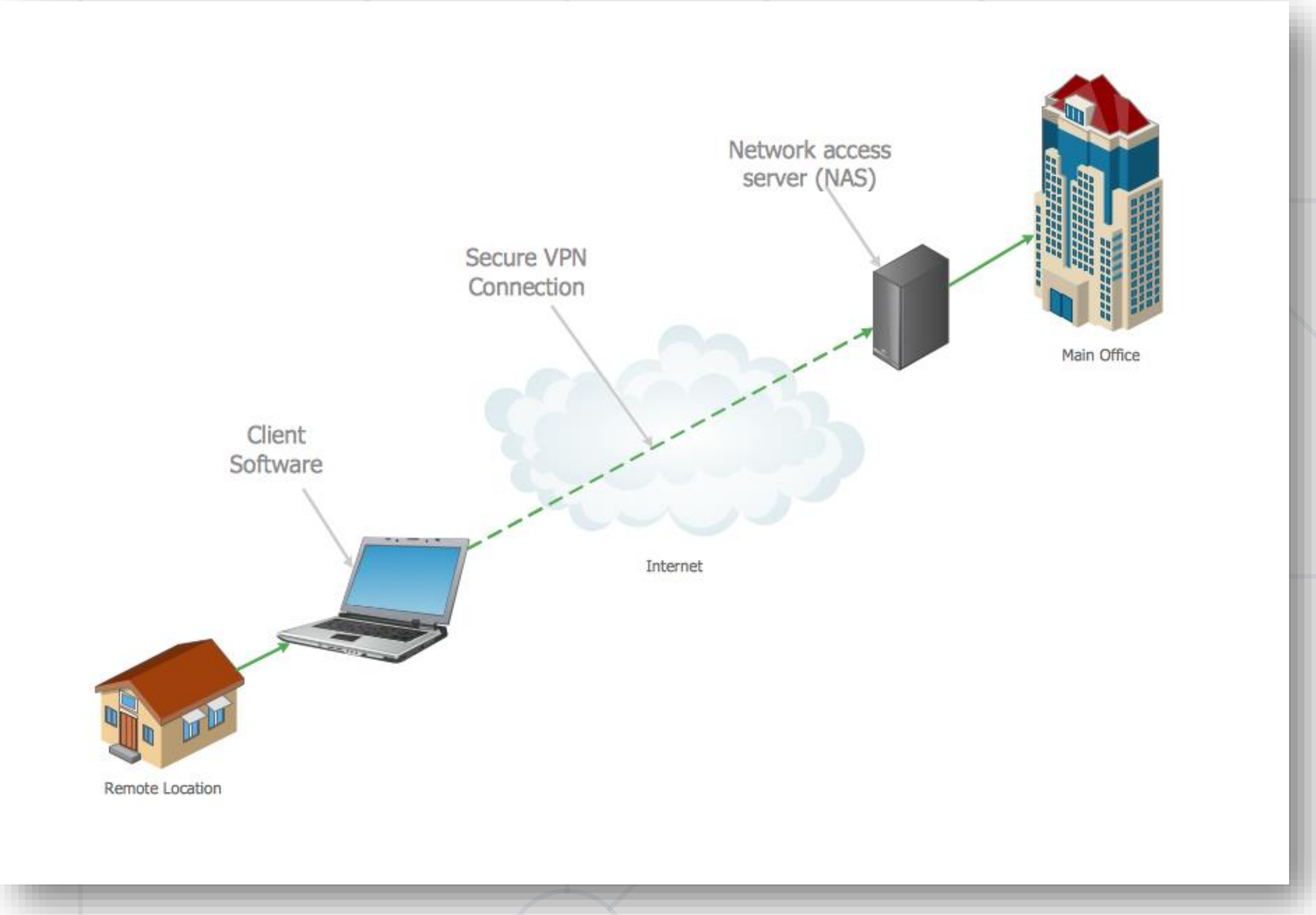
```
lsec@lsec-Precision-7710:~$ netstat -tulpn
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN      -
tcp6       0      0 ::1:631                 :::*                    LISTEN      -
tcp6       0      0 :::1716                 :::*                    LISTEN      4938/kdeconnectd
udp        0      0 0.0.0.0:39766           0.0.0.0:*                           -
udp        0      0 0.0.0.0:56225           0.0.0.0:*                           -
udp        0      0 0.0.0.0:56653           0.0.0.0:*                           -
udp        0      0 0.0.0.0:40396           0.0.0.0:*                           -
udp        0      0 0.0.0.0:56832           0.0.0.0:*                           -
udp        0      0 0.0.0.0:40634           0.0.0.0:*                           -
udp        0      0 0.0.0.0:41353           0.0.0.0:*                           -
```

What is VPN?

Virtual Private Network

- Infrastructure that **allows machines to connect to each other** in a secure way
- VPN can be used for:
  - **Accessing distant servers securely**
  - **Staying safe online**
  - **Hack**

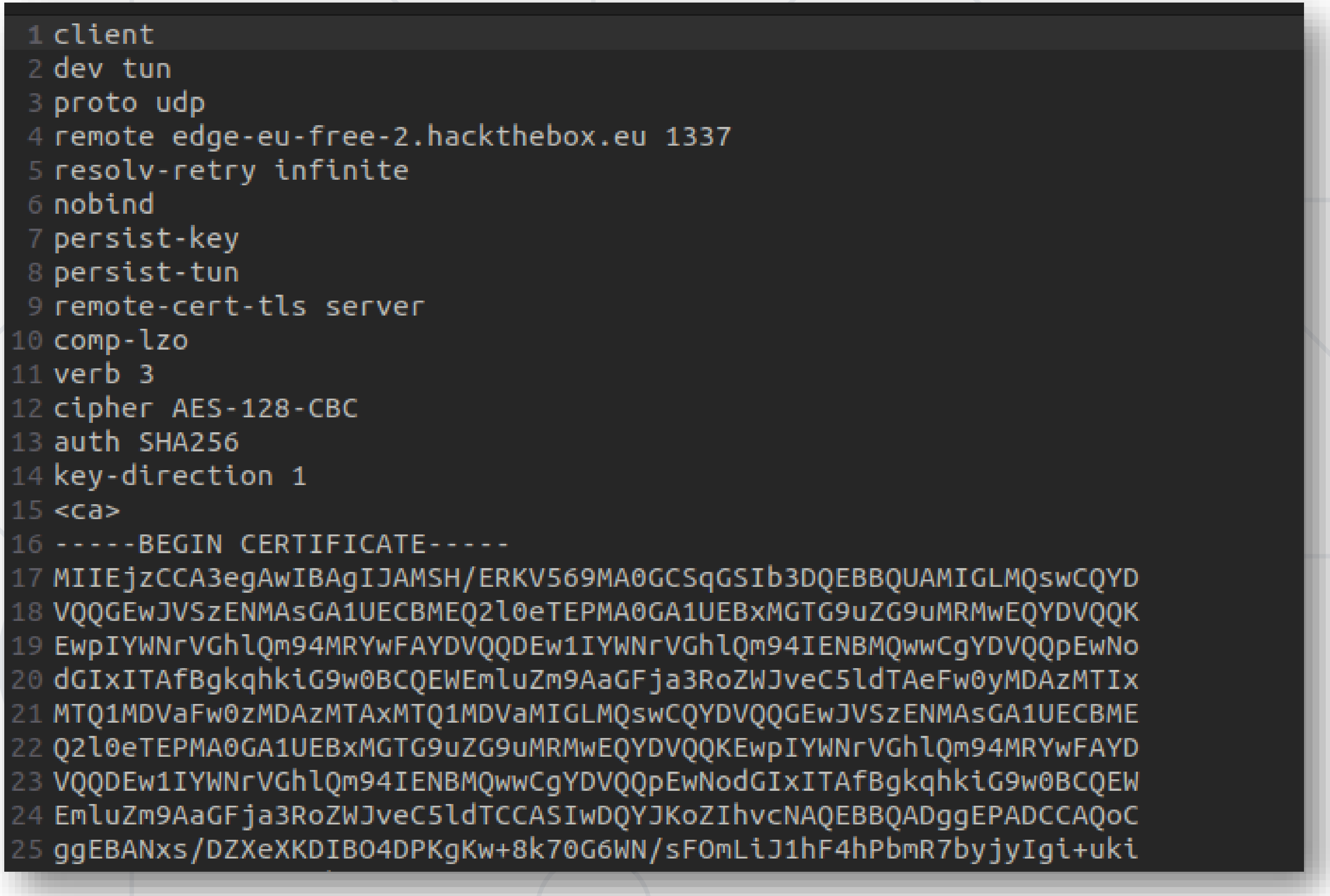
How Remote Work is Possible?



Everyone Can Setup VPN

- **OpenVPN** is the open source way and everyone can implement it
- Technical knowledge is **required**
- It works with **.ovpn files**
- Infrastructure is **required**
  - Link: *https://openvpn.net/*

What Does .ovpn File Look Like?

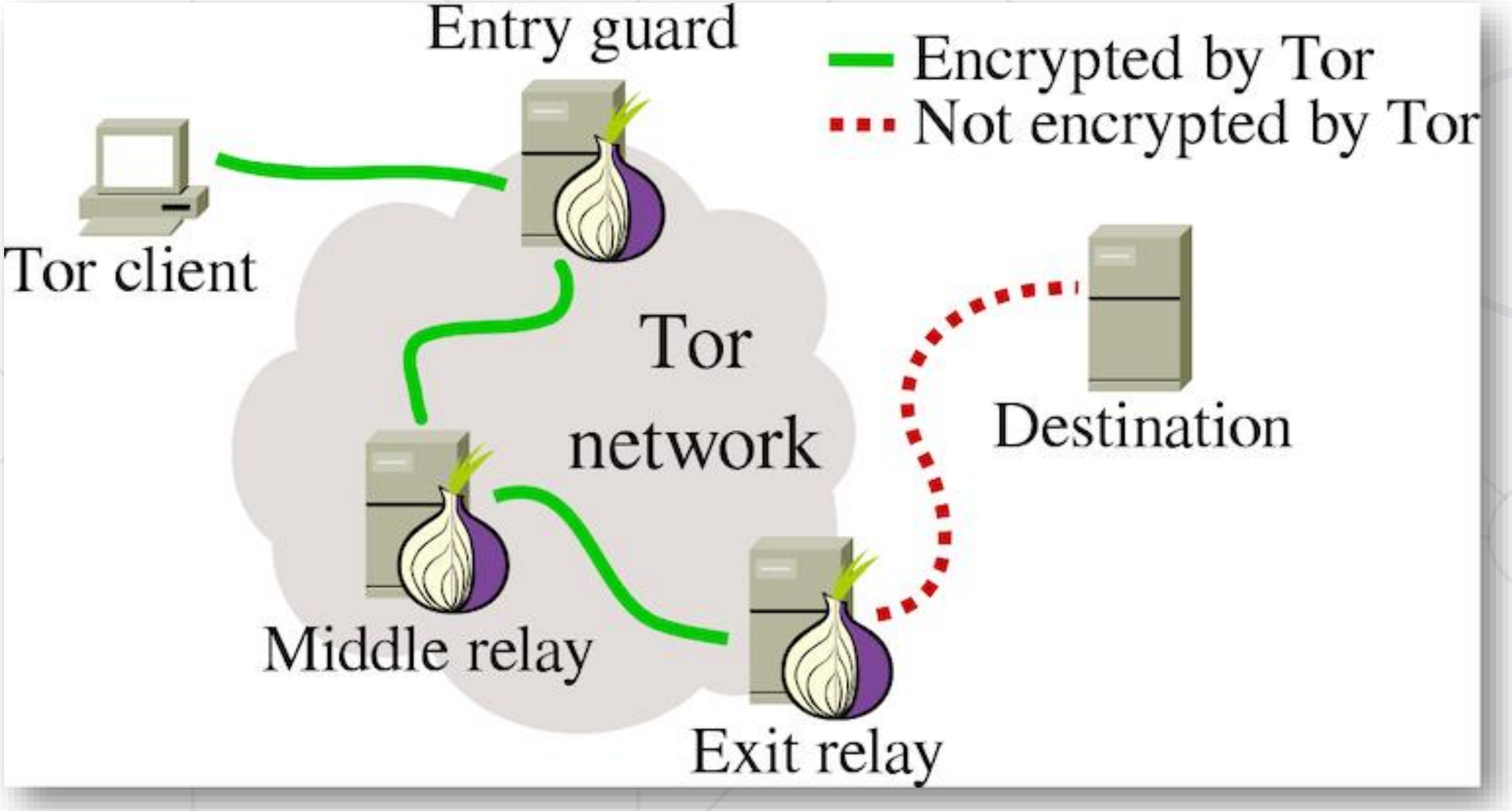


```
client
dev tun
proto udp
remote edge-eu-free-2.hackthebox.eu 1337
resolv-retry infinite
nobind
persist-key
persist-tun
remote-cert-tls server
comp-lzo
verb 3
cipher AES-128-CBC
auth SHA256
key-direction 1
<ca>
-----BEGIN CERTIFICATE-----
MIIEjzCCA3egAwIBAgIJAMSH/ERKV569MA0GCSqGSIb3DQEBBQUAMIGLMQswCQYD
VQQGEwJVSzENMAsGA1UECBMEQ2l0eTEPMA0GA1UEBxMGTG9uZG9uMRMwEQYDVQQK
EwpIYWNrVGhlQm94MRYwFAYDVQQDEw1IYWNrVGhlQm94IENBMQwwCgYDVQQpEwNo
dGIxITAfBgkqhkiG9w0BCQEWEmluZm9AaGFja3RoZWJveC5ldTAeFw0yMDAzMTIx
MTQ1MDVaFw0zMDAzMTAxMTQ1MDVaMIGLMQswCQYDVQQGEwJVSzENMAsGA1UECBME
Q2l0eTEPMA0GA1UEBxMGTG9uZG9uMRMwEQYDVQQKEwpIYWNrVGhlQm94MRYwFAYD
VQQDEw1IYWNrVGhlQm94IENBMQwwCgYDVQQpEwNodGIxITAfBgkqhkiG9w0BCQEW
EmluZm9AaGFja3RoZWJveC5ldTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoC
ggEBANxs/DZXeXKDIBO4DPKgKw+8k70G6WN/sFOmLiJ1hF4hPbmR7byjyIgi+uki
```

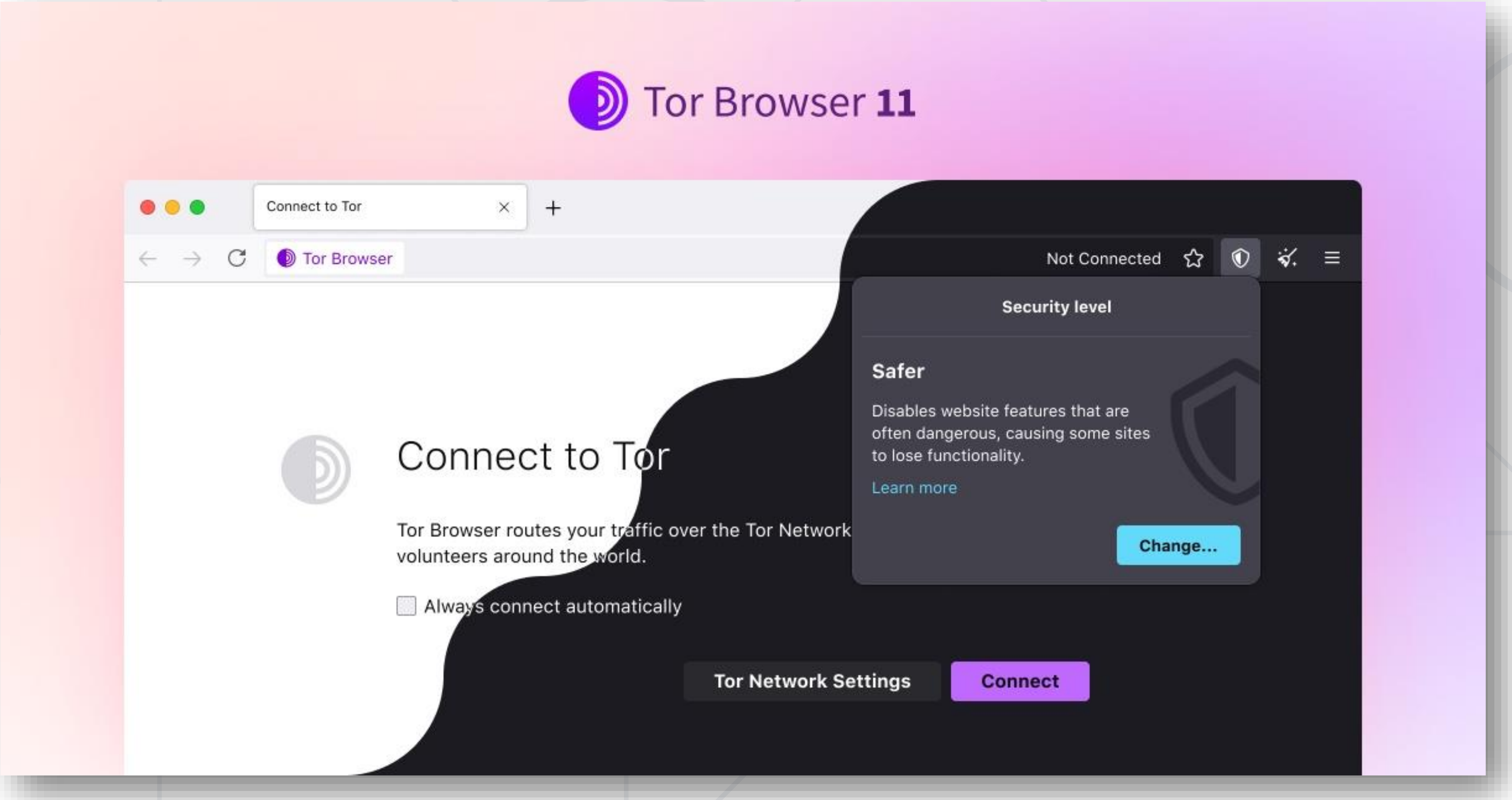
What is TOR?

- **Free** and **open source** network of computers and servers, all running a specific service called
- Open source means that **everyone can contribute to the project**
- This network is used for **anonymity online** and for many more **illegal activities**
- Tor can be used for **hosting websites** or **just browsing** "completely" anonymous

What Does TOR Network Looks Like?



What Does TOR Browser Looks Like?



Tor Browser 11

Connect to Tor

Tor Browser routes your traffic over the Tor Network run by thousands of volunteers around the world.

□ Always connect automatically

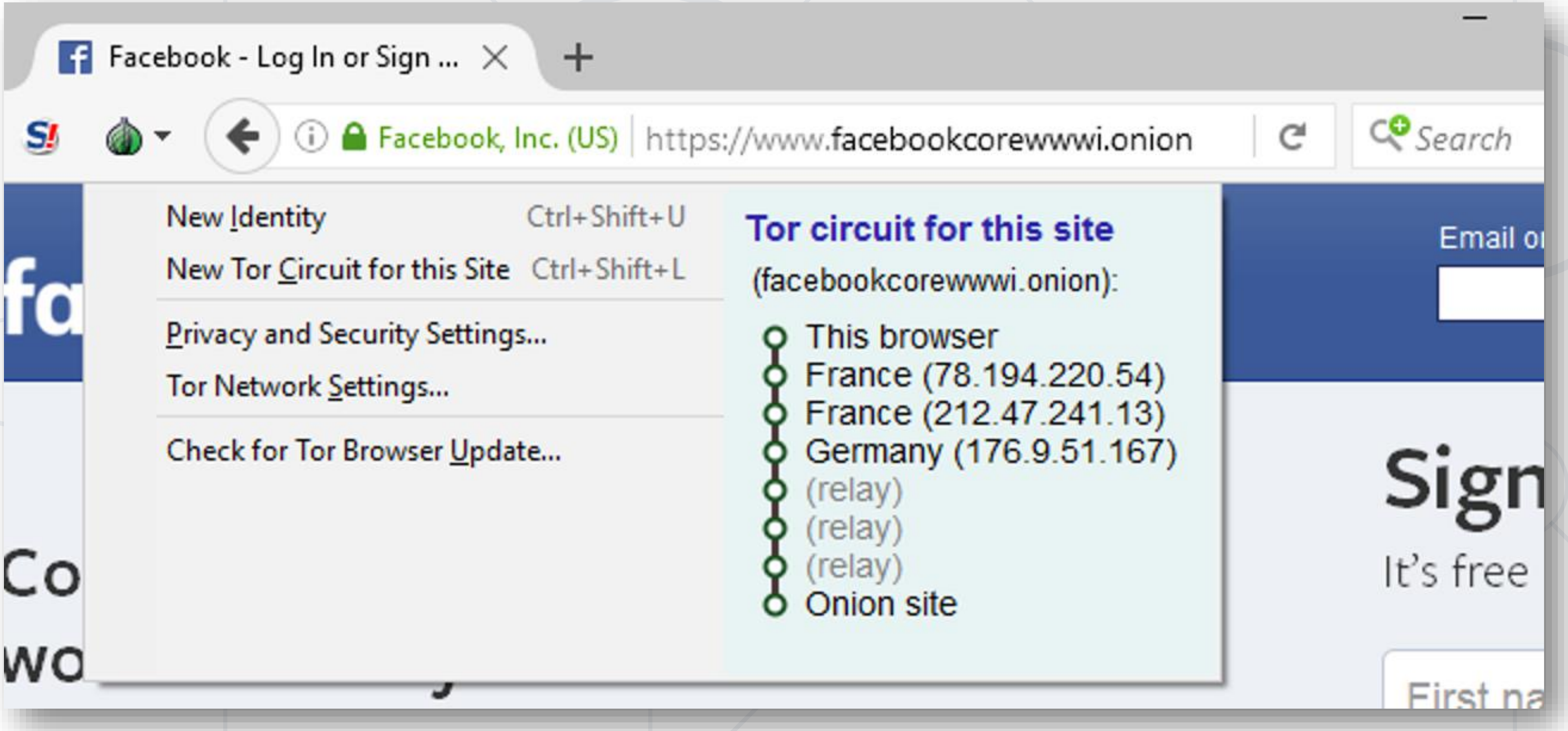
Security level

Safer

Disables website features that are often dangerous, causing some sites to lose functionality.

Learn more

What Does TOR Domain Looks Like?



Facebook - Log In or Sign ...
Facebook, Inc. (US)
https://www.facebookcorewwwi.onion
Search
New Identity Ctrl+Shift+U
New Tor Circuit for this Site Ctrl+Shift+L
Privacy and Security Settings...
Tor Network Settings...
Check for Tor Browser Update...
Email or
Sign
It's free
First na

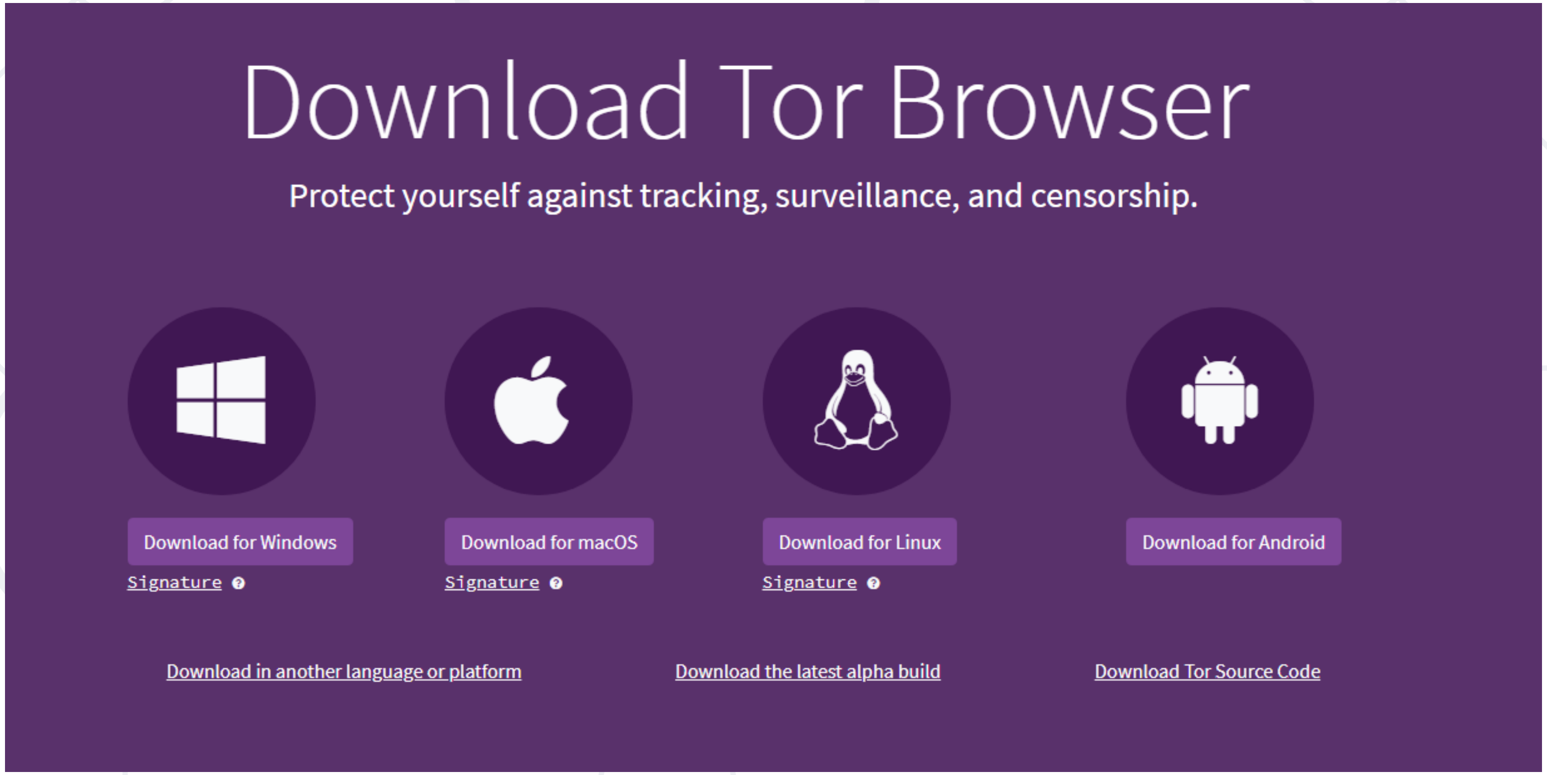
Tor circuit for this site

(facebookcorewwwi.onion):

- This browser
- France (78.194.220.54)
- France (212.47.241.13)
- Germany (176.9.51.167)
- (relay)
- (relay)
- (relay)
- Onion site

How to Connect on Windows?

- Simply download and run Tor Browser: *https://www.torproject.org/download/*

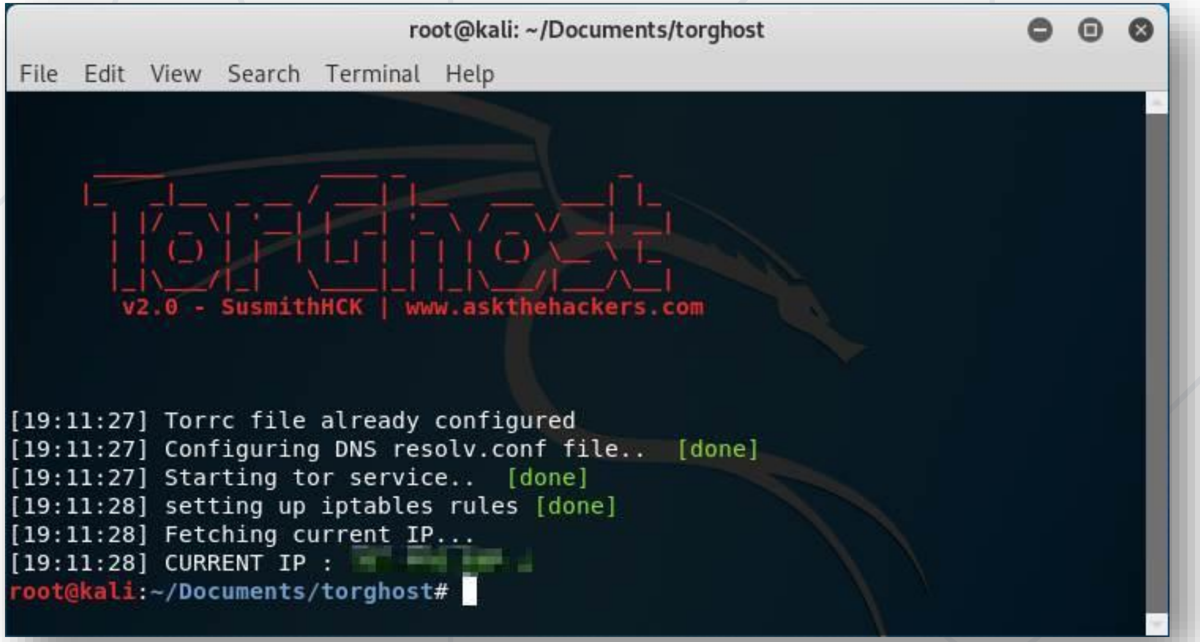


Download Tor Browser

Protect yourself against tracking, surveillance, and censorship.

How to Connect on Linux?

- You can follow the Windows step: https://www.torproject.org/download/
- Or use tools like TorGhost: https://github.com/SusmithKrishnan/torghost



```
 v2.0 - SusmithHCK | www.askthehackers.com

[19:11:27] Torrc file already configured
[19:11:27] Configuring DNS resolv.conf file..  [done]
[19:11:27] Starting tor service..  [done]
[19:11:28] setting up iptables rules [done]
[19:11:28] Fetching current IP...
[19:11:28] CURRENT IP : [redacted]
root@kali:~/Documents/torghost#
```

How to Stay Safe Online?

How to Stay Safe Online?

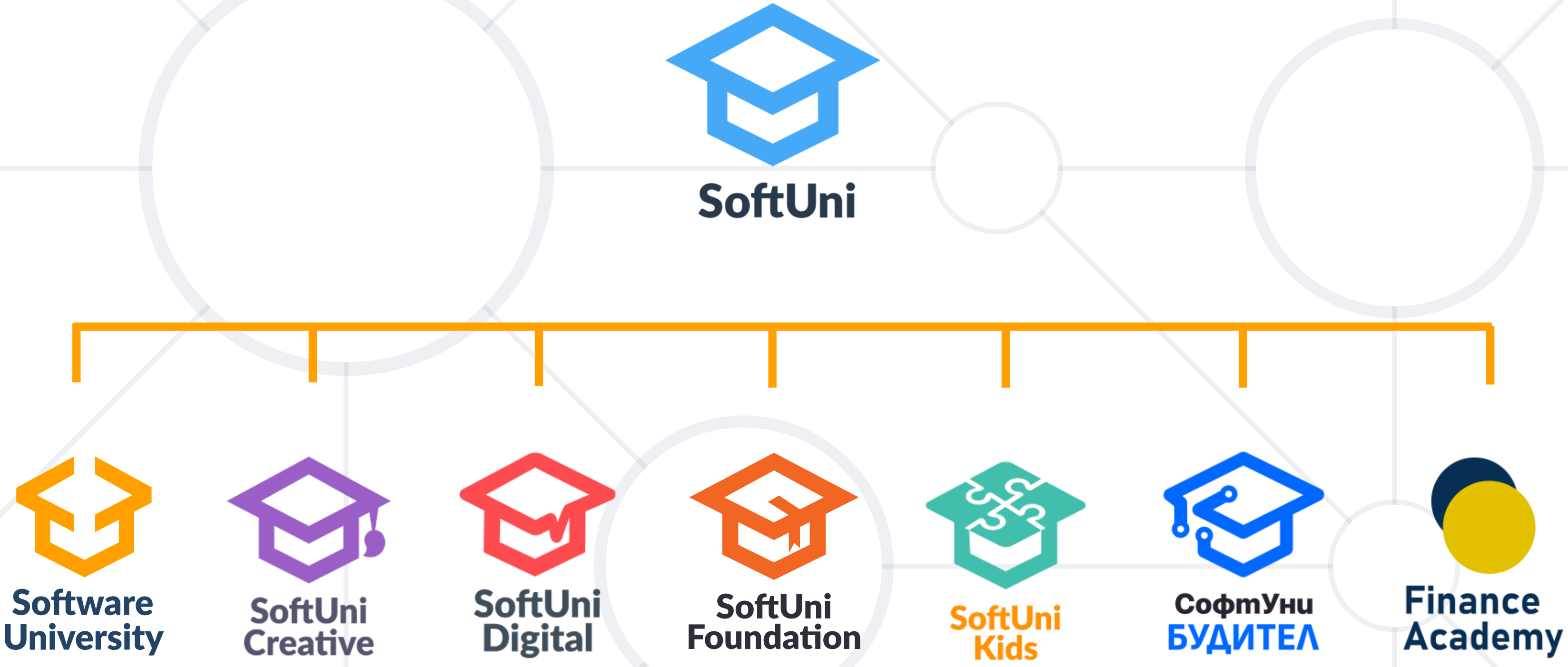
- **DO NOT FALL FOR PHISHING ATTACKS !!!**
- Do **not download** and **run** unverified executables
- Always take note of the URL address bar
  - **Does it contain HTTPS?**
  - **Is the website legit or official?**
- Disable JavaScript with plugins like **adblocker** or be careful on **what you click** if you do not use adblocker
- **VPN** / **TOR** is optional

Summary

- Cyber Security is important since everything is digital nowadays
- Cyber security jobs are harder and it takes a lot of dedication
- A breach can come from all angles
- Be cyber smart and follow basic security principles to stay safe online

Software University

Questions?



SoftUni Diamond Partners

SmartIT

createX

VIVACOM

INDEAVR
Serving the high achievers

Coca-Cola HBC
Bulgaria

Postbank
Решения за твоето утре

AMBITIONED

SUPER
HOSTING
.BG

DRAFT
KINGS
THE CROWN IS YOURS

PHAR
VISION

Trainings @ Software University (SoftUni)

- Software University – High-Quality Education, Profession and Job for Software Developers
  - softuni.bg, softuni.org
- Software University Foundation
  - softuni.foundation
- Software University @ Facebook
  - facebook.com/SoftwareUniversity

License