

What is Cyber Security



SoftUni Team
Technical Trainers



SoftUni



Software University

<https://softuni.bg>

sli.do

#Cyber-Security

1. Cyber Security in a Nutshell
2. Cyber Security Fundamentals
 - What is Exploit, Vulnerability, Payload, Attack, Firewall, IDS/IPS
3. How to Stay Safe Online?





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

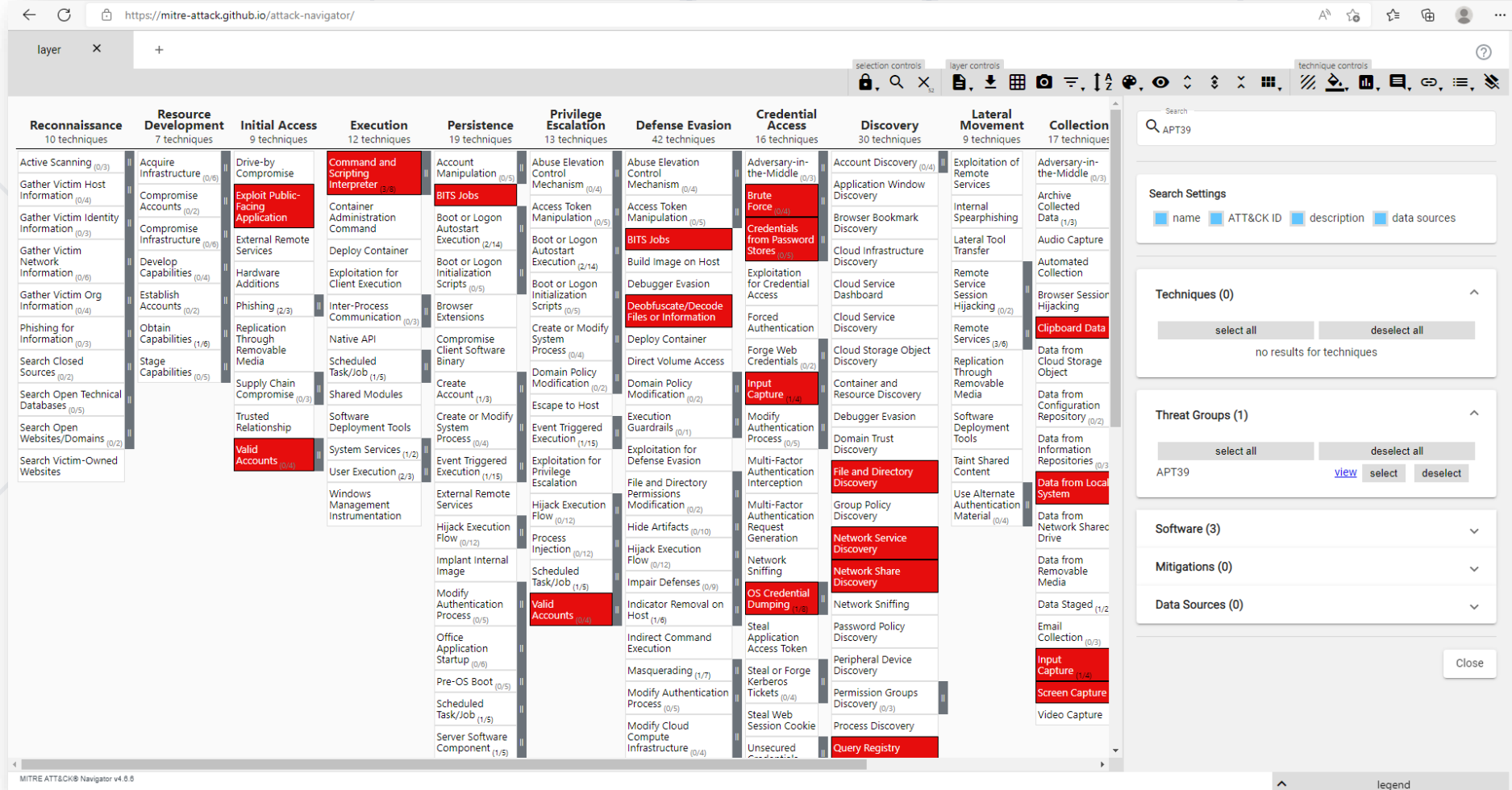
What is a Threat Actor?

- Threat actor is someone with malicious intentions, ready to inflict real harm
- These are the bad guys, a.k.a. "Black Hats"
- Threat actors are recorded as Advanced Persistent Threats (APT)



There are Frameworks for Recording Threat Actions!

■ ATT&CK (<https://attack.mitre.org/>)



The screenshot displays the MITRE ATT&CK Navigator v4.6.0 interface. The main area is a grid of attack techniques, organized into columns representing different phases of an attack. The phases and their counts are: Reconnaissance (10 techniques), Resource Development (7 techniques), Initial Access (9 techniques), Execution (12 techniques), Persistence (19 techniques), Privilege Escalation (13 techniques), Defense Evasion (42 techniques), Credential Access (16 techniques), Discovery (30 techniques), Lateral Movement (9 techniques), and Collection (17 techniques). The techniques are listed in rows, with some highlighted in red. The interface includes a search bar at the top right, search settings, and a list of threat groups and software.

Phase	Count	Techniques
Reconnaissance	10	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	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	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	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	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), Domain Policy Modification (0/2), Escape to Host, Event Triggered Execution (1/15), Exploitation for Privilege Escalation, 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	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, Execution Guardrails (0/1), Exploitation for Defense Evasion, File and Directory Permissions Modification (0/2), Hide Artifacts (0/10), Hijack Execution Flow (0/12), Scheduled Task/Job (1/5), 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)
Defense Evasion	42	Abuse Elevation Control Mechanism (0/4), Access Token Manipulation (0/5), 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	Adversary-in-the-Middle (0/3), Brute Force (0/0), Credentials from Password Stores (0/3), 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 (1/2), Steal Application Access Token, Steal or Forge Kerberos Tickets (0/4), Steal Web Session Cookie, Unsecured Credentials
Discovery	30	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	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	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 Share Drive, Data from Removable Media, Data Staged (1/2), Email Collection (0/3), Input Capture (1/4), Screen Capture, Video Capture

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. Try not giving it to them...
- **Black Hats** – Complete Cyber Criminals



What is a Breach?

- **Breach** is when the threat successfully executes its 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 happens, 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
 - And many, many, many, more ...



What is Vulnerability?

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



Quiz for you!

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

YES!!!

- But **WHY?**



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
 - More, more, and more yet to come ...



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 security related tasks without written permission.

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 task
[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)

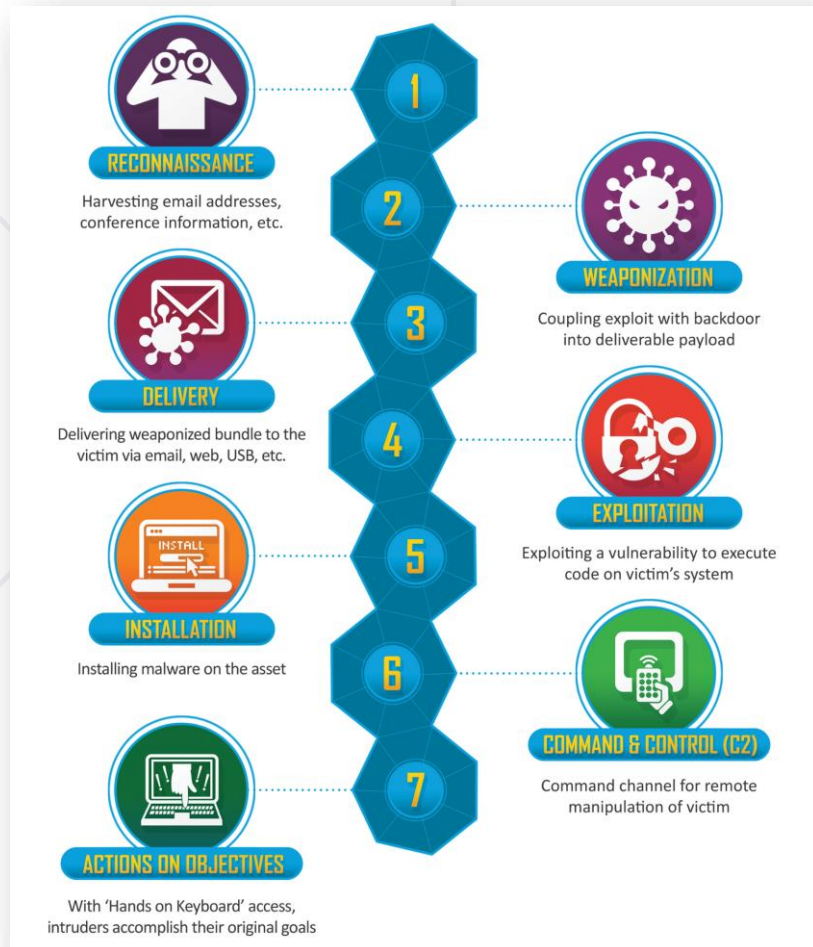
What is Payload?

- **Payload** is 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



- 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
- Example in the next slide ...

■ Lockheed Martin kill chain:



Before we Dive Into More Terms

- Why not take a little break?



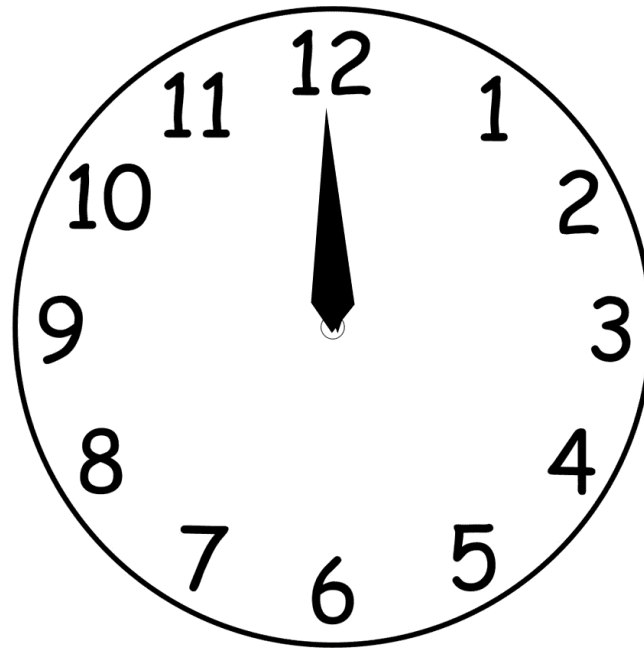
What is Phishing?

- **Phishing** is a 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
 - SMSishing
 - Voice Phishing and many, many, many, many, more ...



Another Quiz, do not Chill Here!

- Is a phishing attack a vulnerability or an exploit?
- Take your time!



Phishing Attack is an Exploit

- Why?
- 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

Waaaaait a Minute... Kaboom, Another Quiz!

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



- 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 (web link or .exe program)
 - The human itself. We cannot count entirely on systems, since we built them after all. The last vulnerability is the human clicking and following phishing's instructions. Be self aware!

What is a Firewall?

- **Firewall** is a security mechanism to filter traffic, based on predefined rules
- It can be software / hardware
- Firewall is a MUST in every company
- Do you wonder how the hardware firewall is looking? Here:



How does a Firewall Rule Looks Like?

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

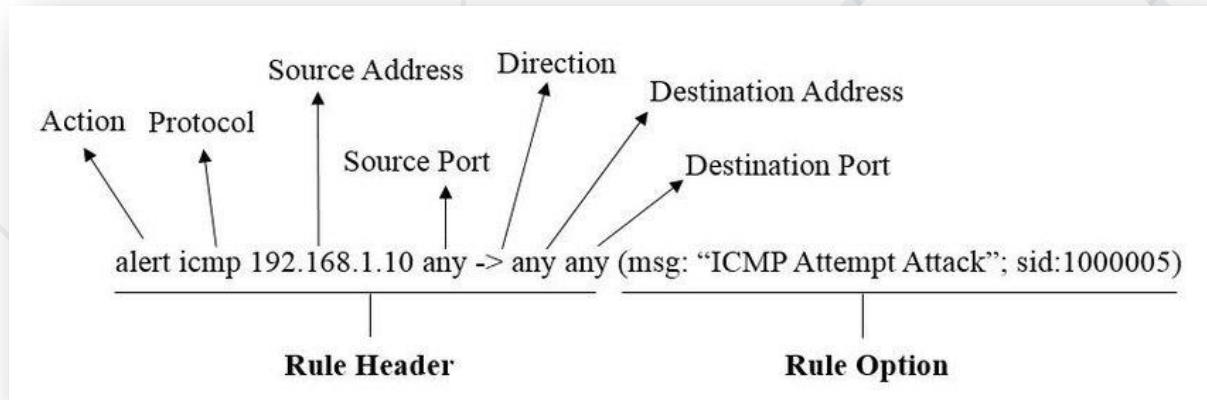


What is IPS?

- **Intrusion Prevention System (IPS)** is 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



- Snort (<https://www.snort.org/>)



```
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 [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.1.23:64399 -> 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} 192.168.1.23:64399 -> 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 [**] [Classification: 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 [**] [Classification: 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:

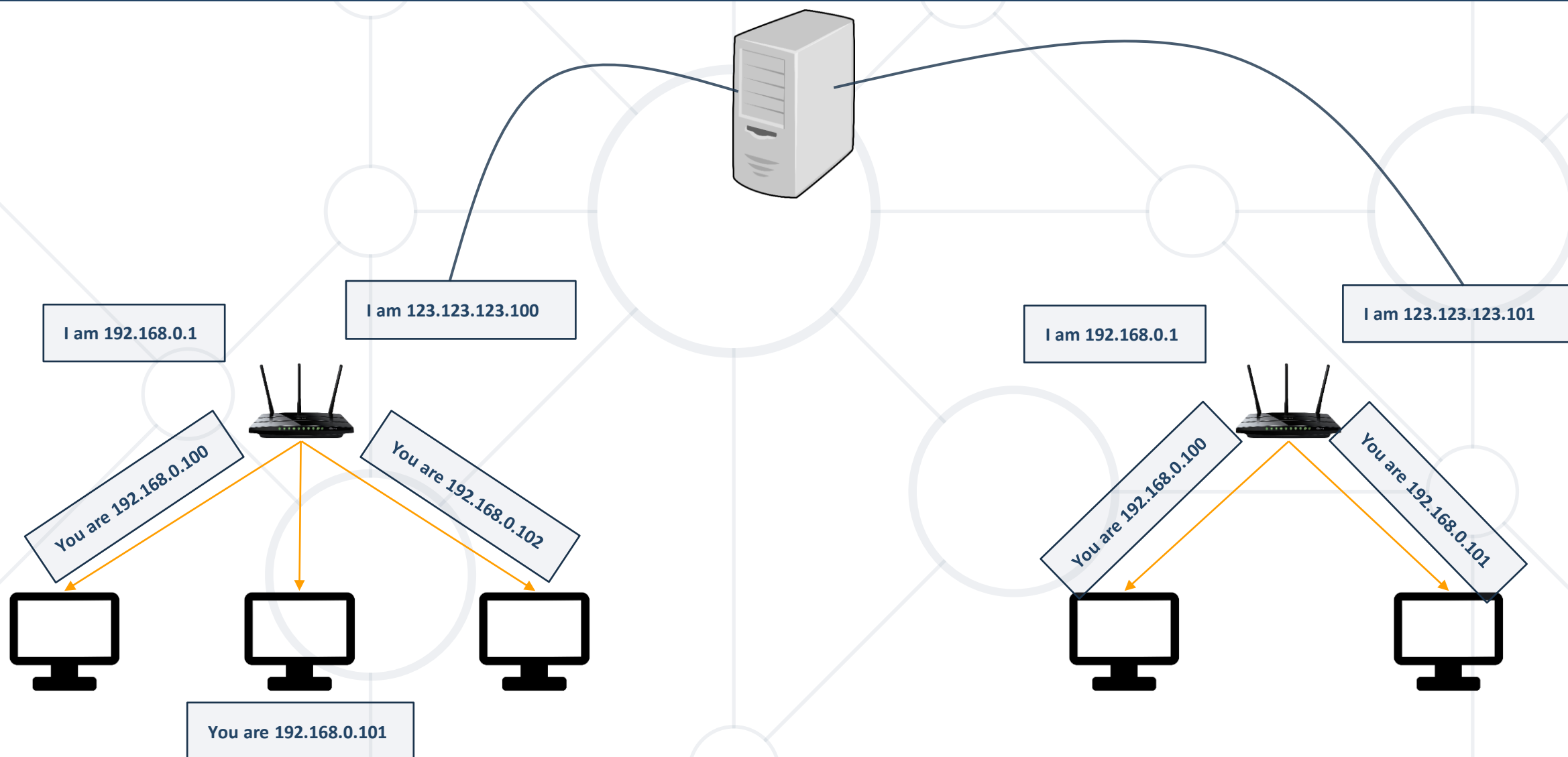
- 192.168.0.1 / 45.33.32.156 (IPv4)
- 2001:0db8:85a3:0000:0000:8a2e:0370:7334 (IPv6)



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
- Hope the next slide clears the picture a little bit more:

External vs Internal IP Address Visual Representation



What is Port?

- **Port** is 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
 - And 65,531 more 😊



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`

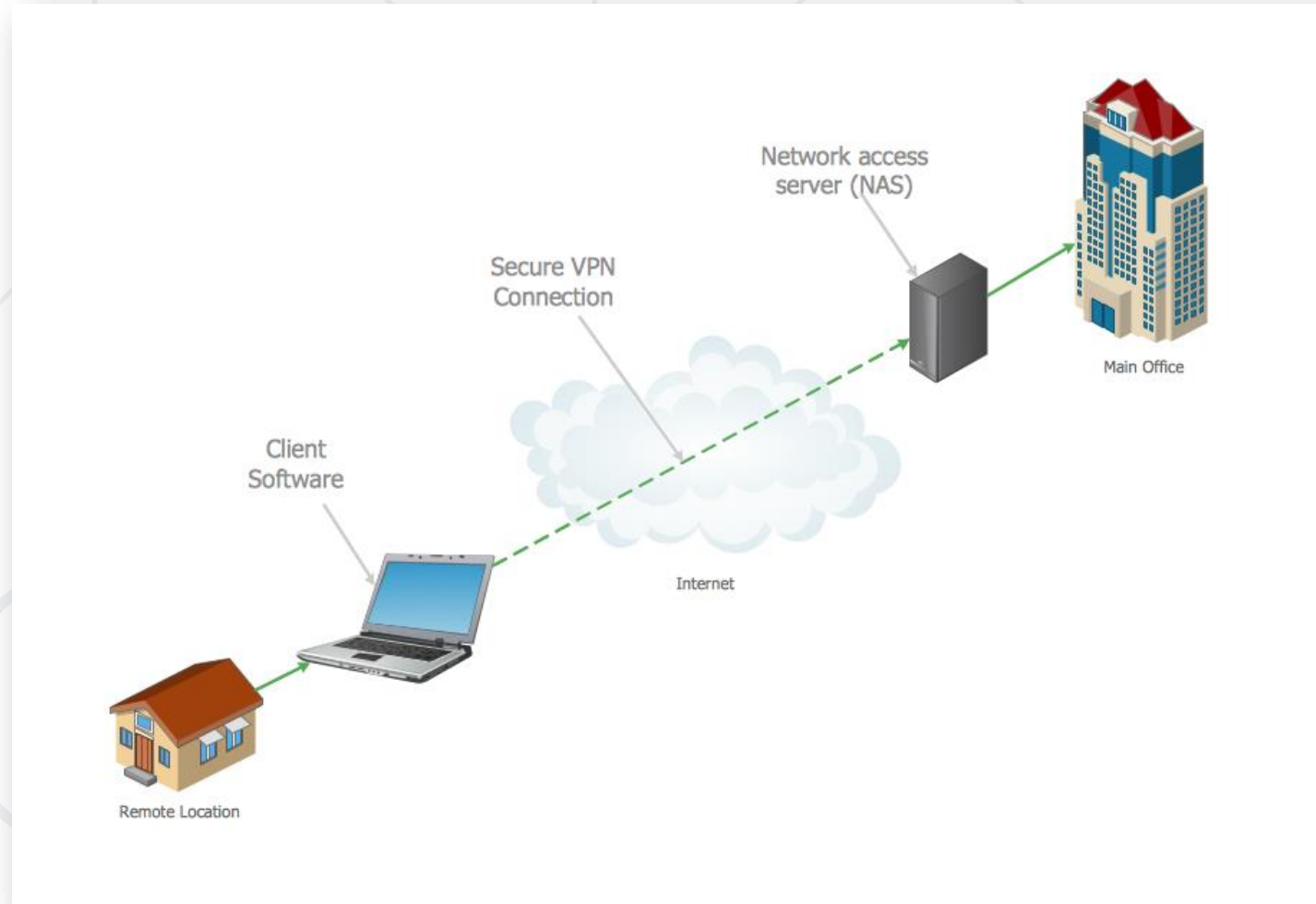
```
lsec@lsec-Precision-7710:~$ ss -nltp
State      Recv-Q      Send-Q      Local Address:Port      Peer Address:Port      Process
LISTEN     0            4096        127.0.0.53%lo:53        0.0.0.0:*
LISTEN     0            128         127.0.0.1:631          0.0.0.0:*
LISTEN     0            50          *:1716                 *:.*
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** is a 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 ... Of course, but not recommended

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?

```
1 client
2 dev tun
3 proto udp
4 remote edge-eu-free-2.hackthebox.eu 1337
5 resolv-retry infinite
6 nobind
7 persist-key
8 persist-tun
9 remote-cert-tls server
10 comp-lzo
11 verb 3
12 cipher AES-128-CBC
13 auth SHA256
14 key-direction 1
15 <ca>
16 -----BEGIN CERTIFICATE-----
17 MIIEjzCCA3egAwIBAgIJAMSH/ERKV569MA0GCSqGSIb3DQEBBQUAMIGLMQswCQYD
18 VQQGEwJVSzENMA5GA1UECBMEQ2l0eTEPMA0GA1UEBxMGTG9uZG9uMRMwEQYDVQK
19 EwpIYWNRVGhlQm94MRYwFAYDVQQDEw1IYWNRVGhlQm94IENBMQwwCgYDVQQpEwNo
20 dGIxITAFBgkqhkiG9w0BCQEWEmluZm9AaGFja3RoZWJveC5ldTAeFw0yMDAzMTIx
21 MTQ1MDVaFw0zMDAzMTAxMTQ1MDVaMIGLMQswCQYDVQQGEwJVSzENMA5GA1UECBME
22 Q2l0eTEPMA0GA1UEBxMGTG9uZG9uMRMwEQYDVQKQEWpIYWNRVGhlQm94MRYwFAYD
23 VQQDEw1IYWNRVGhlQm94IENBMQwwCgYDVQQpEwNodGIxITAFBgkqhkiG9w0BCQEW
24 EmluZm9AaGFja3RoZWJveC5ldTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoC
25 ggEBANxs/DZXeXKDIBo4DPKgKw+8k70G6WN/sF0mLiJ1hF4hPbmR7byjyIgi+uki
```

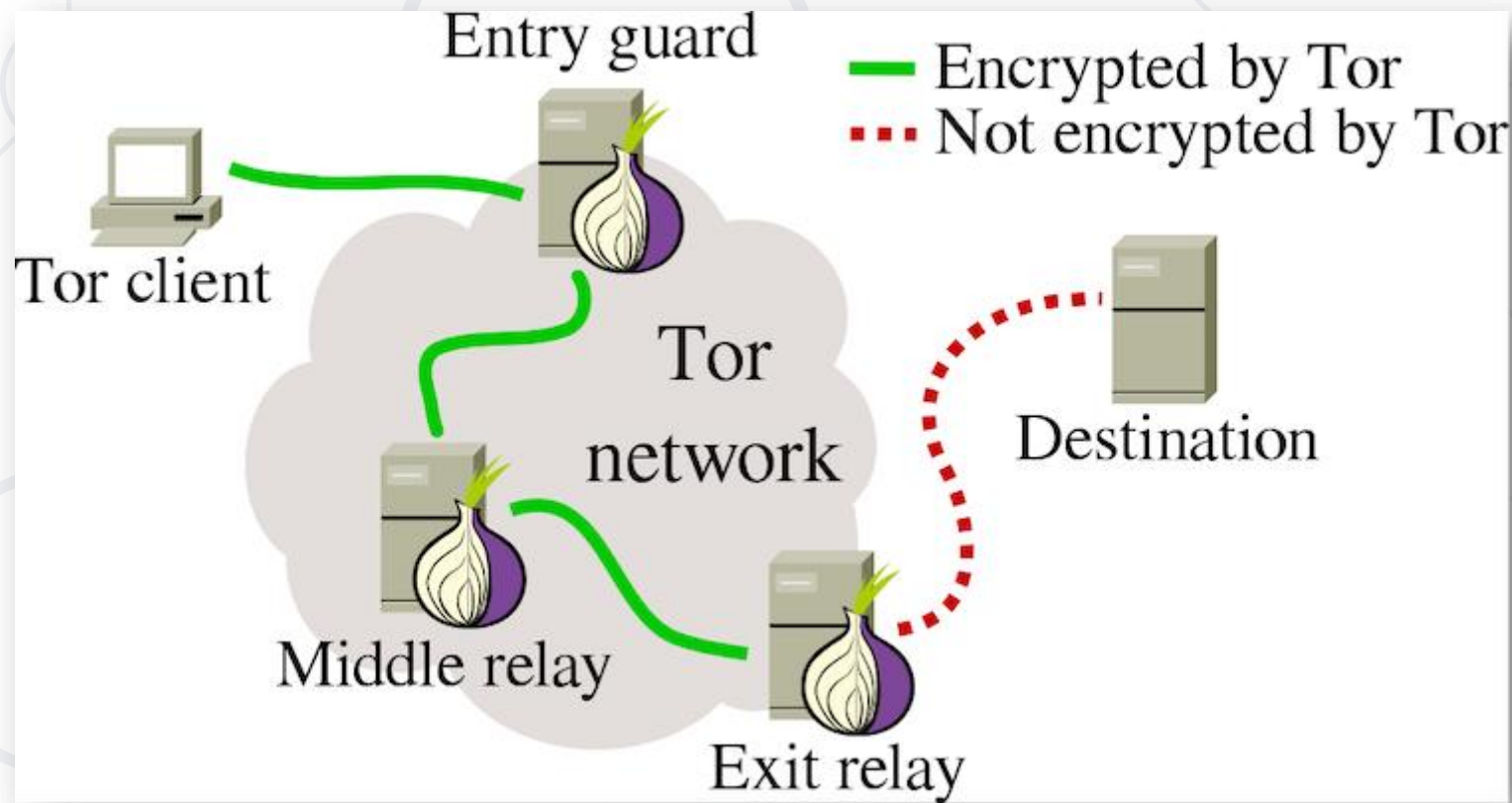
What is TOR?



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

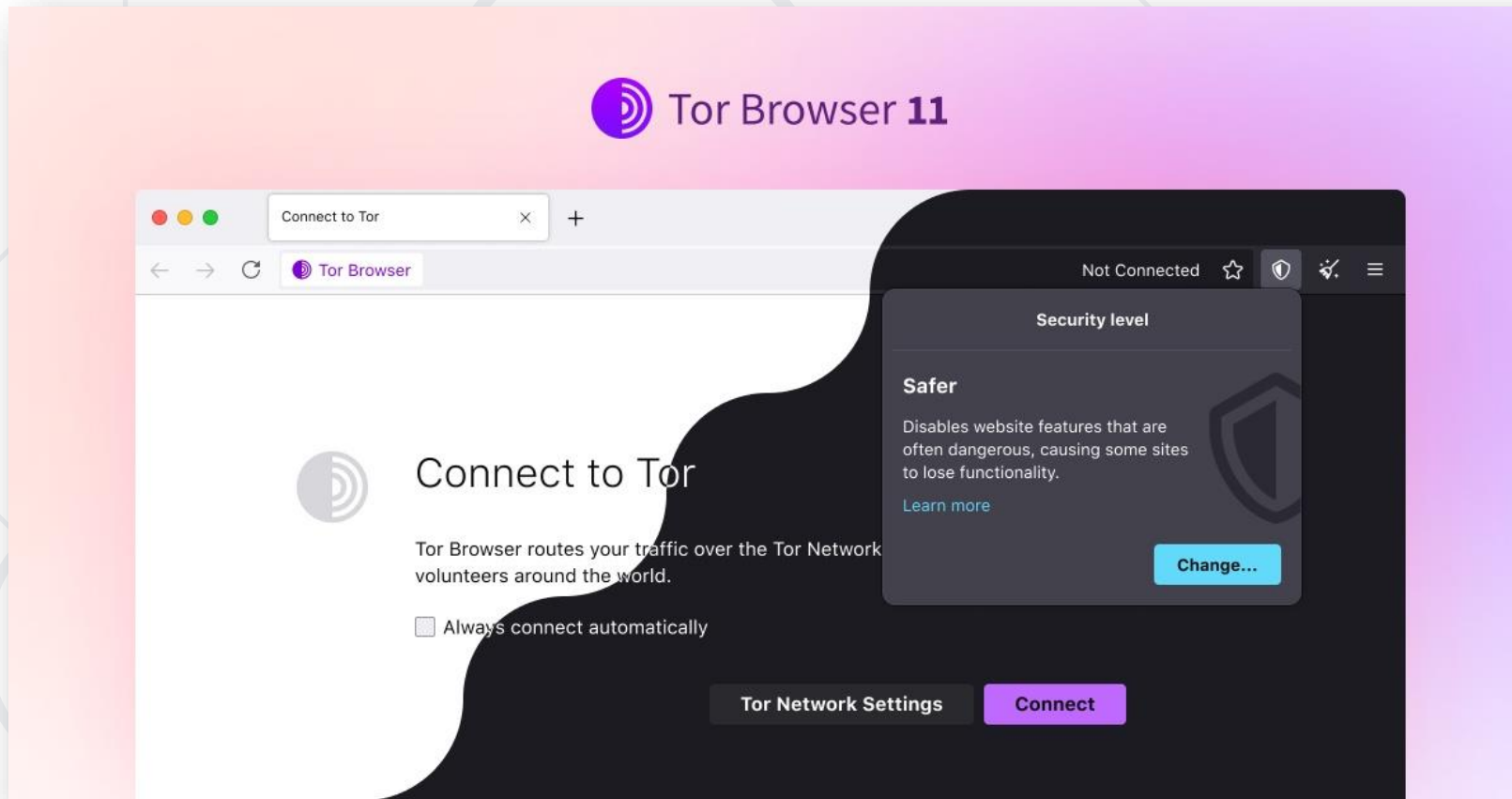
What Does TOR Looks Like?

- Tor Network



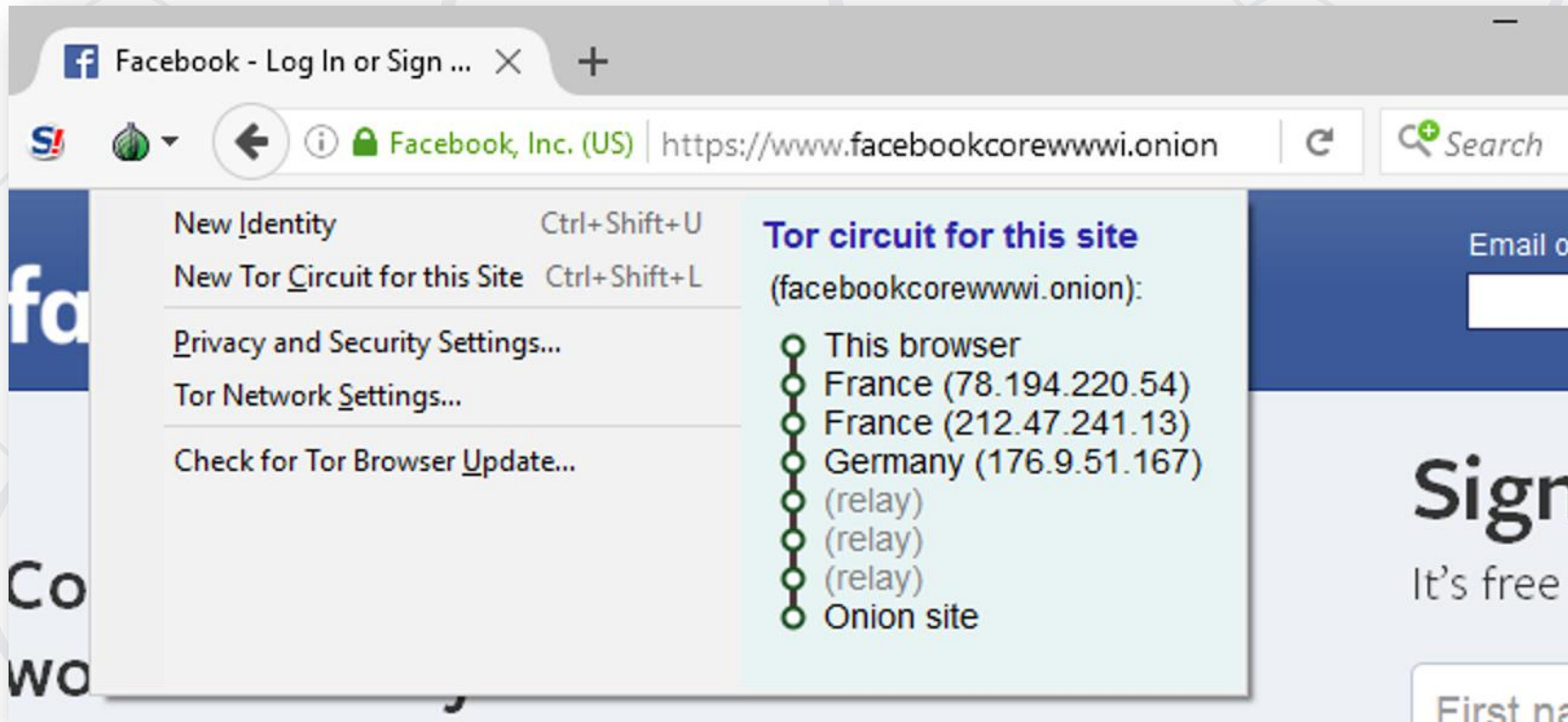
What Does TOR Looks Like?

- Tor Browser



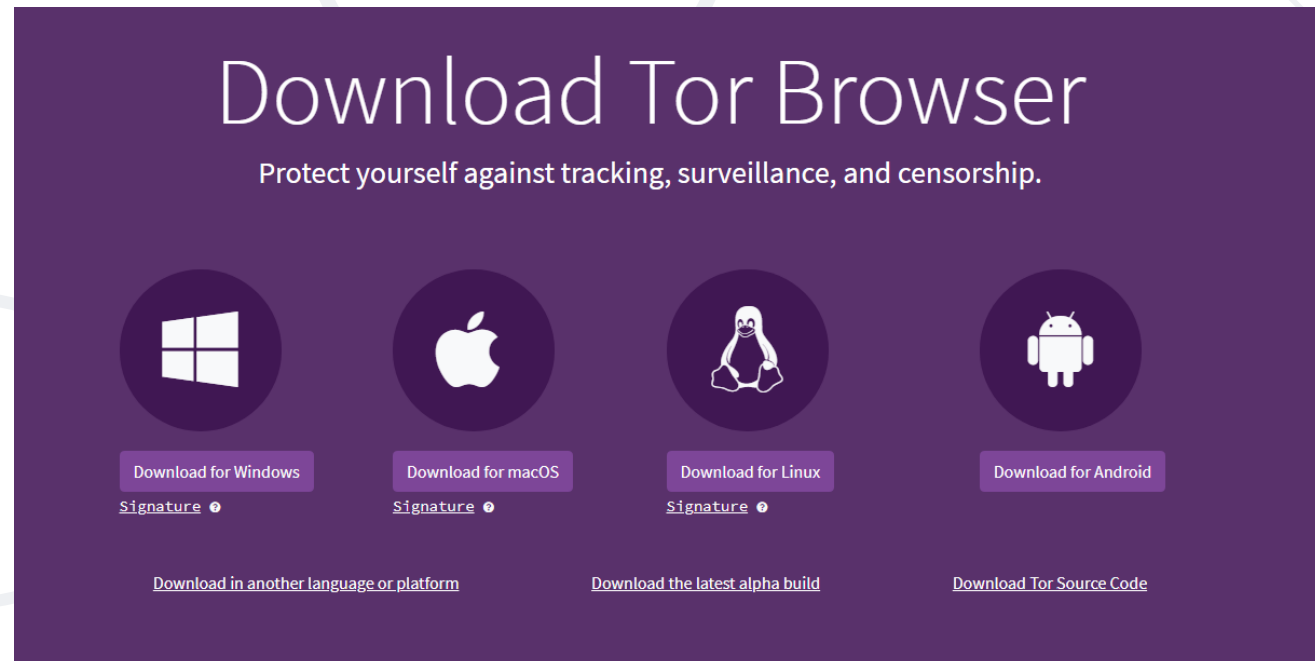
What Does TOR Looks Like?

■ Tor Domain



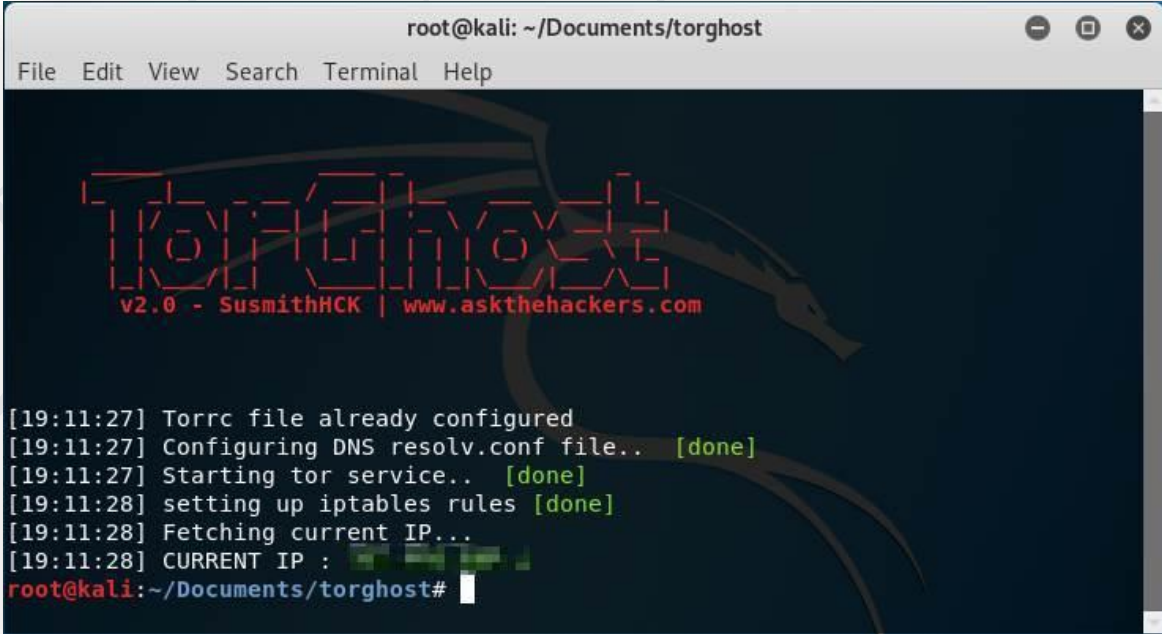
How to Connect on Windows?

- Simply download and run Tor Browser
(<https://www.torproject.org/download/>)



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>)



```
root@kali: ~/Documents/torghost
File Edit View Search Terminal Help

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 : 192.168.1.100
root@kali:~/Documents/torghost#
```



How to Stay Safe Online?

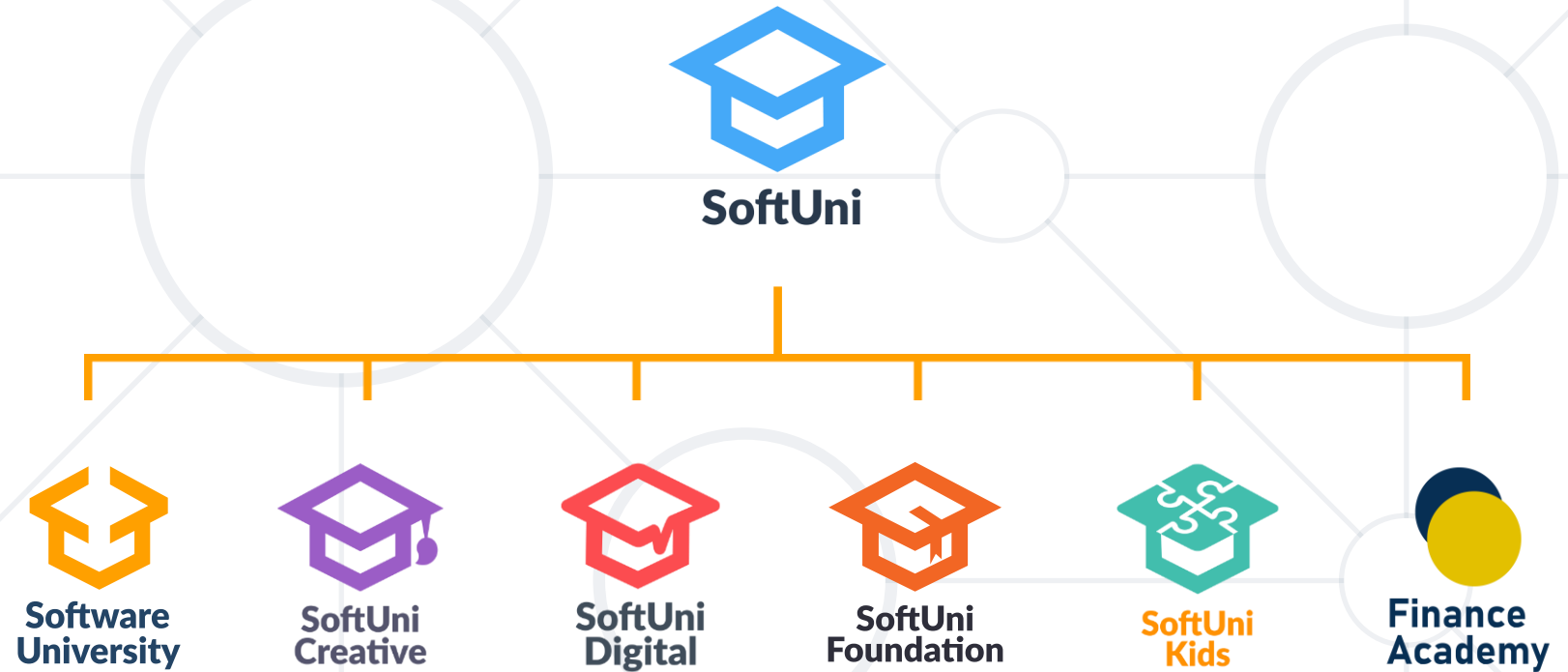
How to Stay Safe Online?

- **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

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



Questions?



SoftUni Diamond Partners



- 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



- This course (slides, examples, demos, exercises, homework, documents, videos and other assets) is **copyrighted content**
- Unauthorized copy, reproduction or use is illegal
- © SoftUni – <https://softuni.org>
- © Software University – <https://softuni.bg>

