IT Security

INTRODUCTION

DURATION : 1’00

Summary

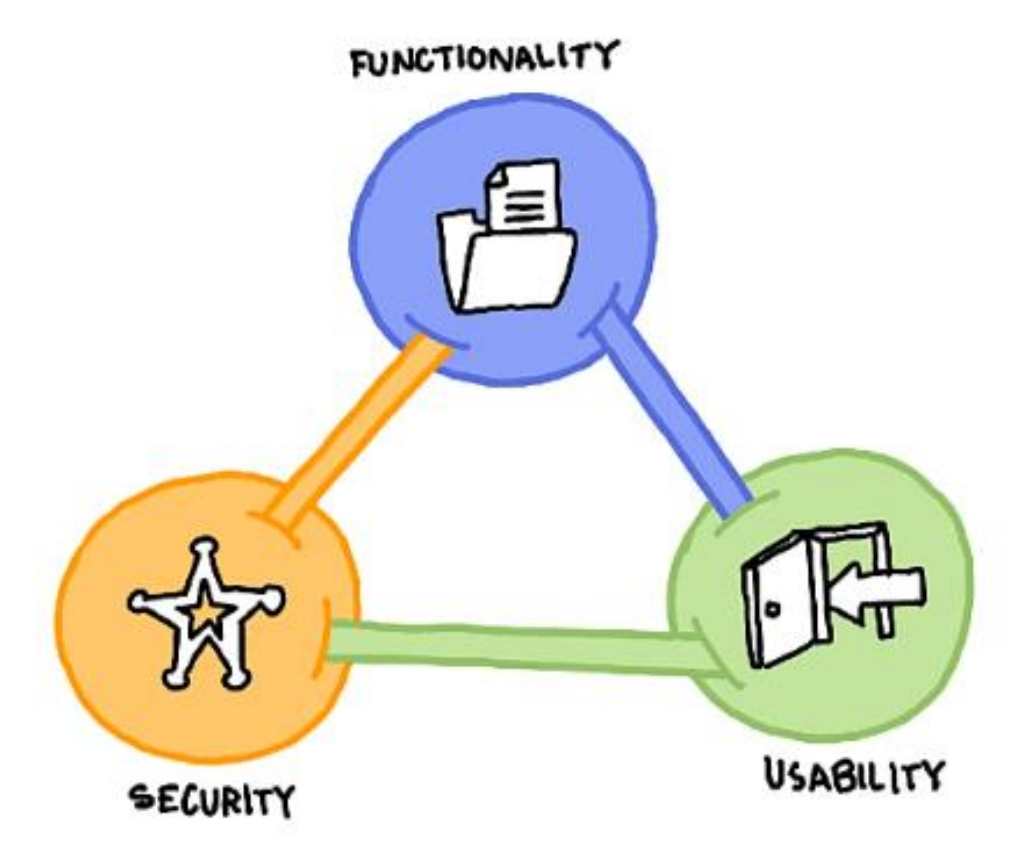
1. Introduction to cybersecurity
2. What is an ethical hacking
3. Different types of hacker
4. Hacking vocabulary
5. Other vocabulary words
6. All steps to execute a pentest & Kill chain frameworks
7. Improve your skills

Introduction to cybersecurity

- Cybersecurity / IT security prevents unauthorized access to assets (computers, servers, networks, data, etc.).
- To maintain (CIA or DICP in French)
  - **Confidentiality**:
    Cleartext or password stealing has an impact on confidentiality.
  - **Integrity**:
    Data tampering has an impact on integrity.
  - **Availability**:
    DoS attack has an impact on availability.
  - **Authenticity / Non repudiation**:
    Guarantee that the sender of a message cannot deny having sent the message and the recipient cannot deny having received it.

Security, Functionality and Usability balance

- There is an inter dependency between these three attributes.
- When security goes up, usability and functionality come down.
- Any organization should balance between these three qualities to arrive at a balanced information system.



What is an Ethical Hacking ?

- Ethical hacking involves the use of hacking tools, tricks and techniques to identify vulnerabilities and secure system security.
- If focuses on simulating the techniques used by attackers to verify the existence of exploitable vulnerabilities in a system.
- Ethical hackers perform security assessments for an organization with the permission of concerned authorities.

Different types of hacker

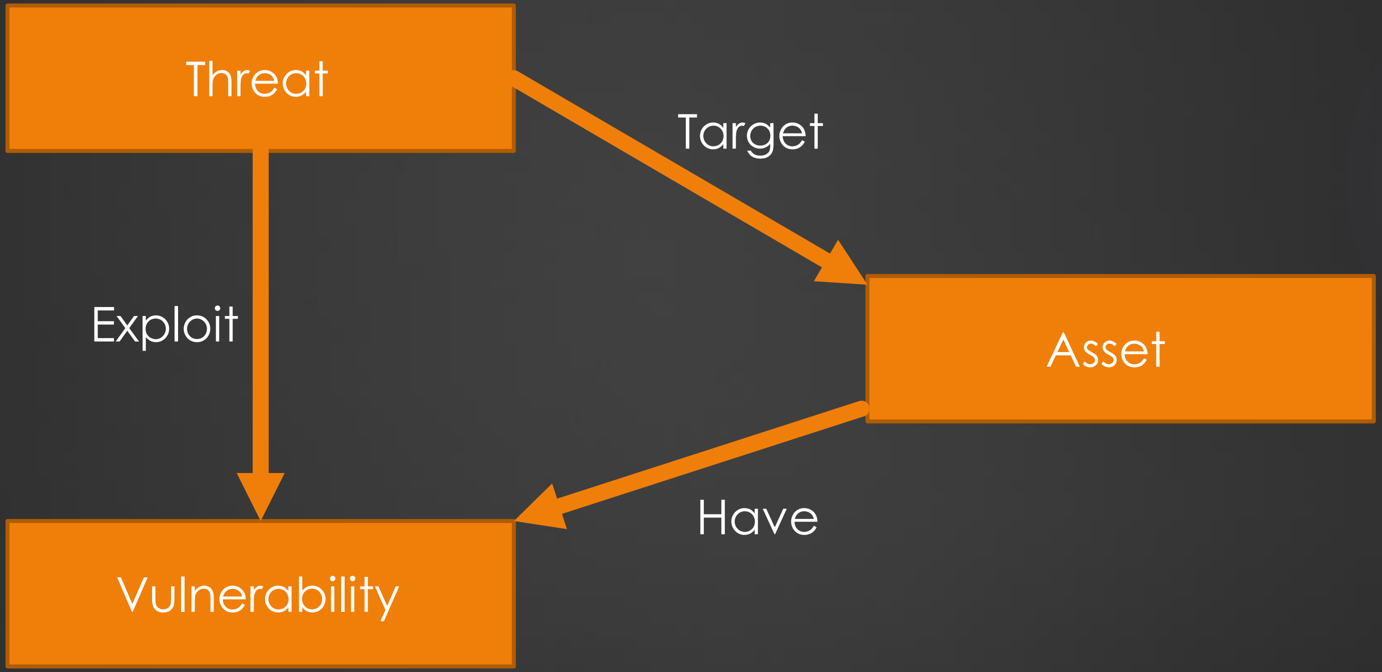
- **White Hats** is a good guys also called ethical hackers.
- **Black Hats** is a bad guys, malicious hackers.
- **Gray Hats** is a good and bad guys depends on the situation.

- **Hacktivist** is a guy who defend a political opinion.
- **Script Kiddies** is an unskilled hacker who compromises a system by running scripts, tools, or other developed by real hackers.
- **Cyber Terrorists** are guys motivated by religious or political.
- **State-sponsored Hackers** are guys employed by the government to hack another government.

Hacking vocabulary (1/2)

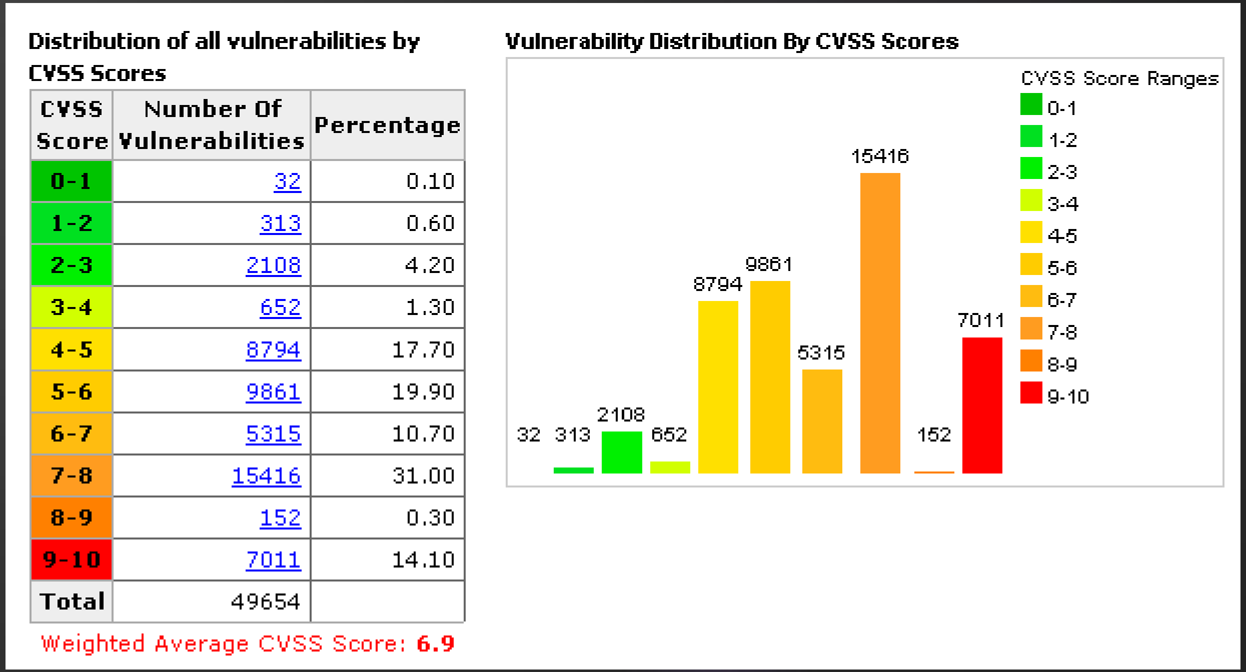
- **Threat** that could lead to a potential breach of security.
- **Exploit** takes advantage of a bug or vulnerability, leading to unauthorized access, privilege escalation, or Denial Of Service.
- **Vulnerability** is a software flaw or implementation error that can lead to an unexpected and undesirable event executing bad or damaging instructions to the system.
- **Risk analysis** aim to identify, assess and prioritize the risks associated with the activities of an organization.
- **Payload** is a component of an attack. It could also contain malware such as worms or viruses which performs the malicious action; deleting data, sending spam or encrypting data.
- **Zero-day attack** is an attack that occurs before a vendor knows or is able to patch a flaw.
- **Pivoting** involves gaining access to a network and / or computer and then using the same information to gain access to multiple networks and computers that contains desirable information.
- **Doxing** is the act of publicly providing PII (Personally Identifiable Information) about an individual or organization, usually via the Internet and without their consent.

Hacking vocabulary (2/2)



Vulnerabilities vocabulary

- **CVE** (Common Vulnerabilities and Exposures) is a list of publicly disclosed vulnerabilities and exposures that is maintained by MITRE.
- **MITRE** is an American not-for-profit organization created to improve IT security.
- **CVSS** (Common Vulnerability Scoring System) places numerical score based on severity :



Distribution of all vulnerabilities by CVSS Scores

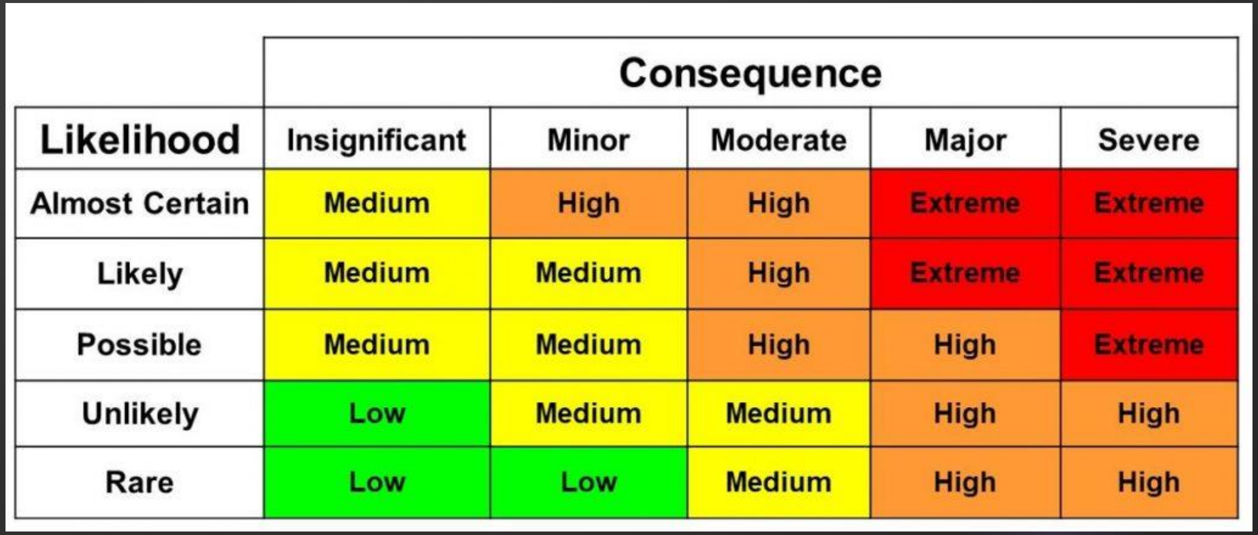
CVSS Score	Number Of Vulnerabilities	Percentage
0-1	32	0.10
1-2	313	0.60
2-3	2108	4.20
3-4	652	1.30
4-5	8794	17.70
5-6	9861	19.90
6-7	5315	10.70
7-8	15416	31.00
8-9	152	0.30
9-10	7011	14.10
Total	49654	

Weighted Average CVSS Score: **6.9**

Vulnerability Distribution By CVSS Scores

Managing the Risk (1/2)

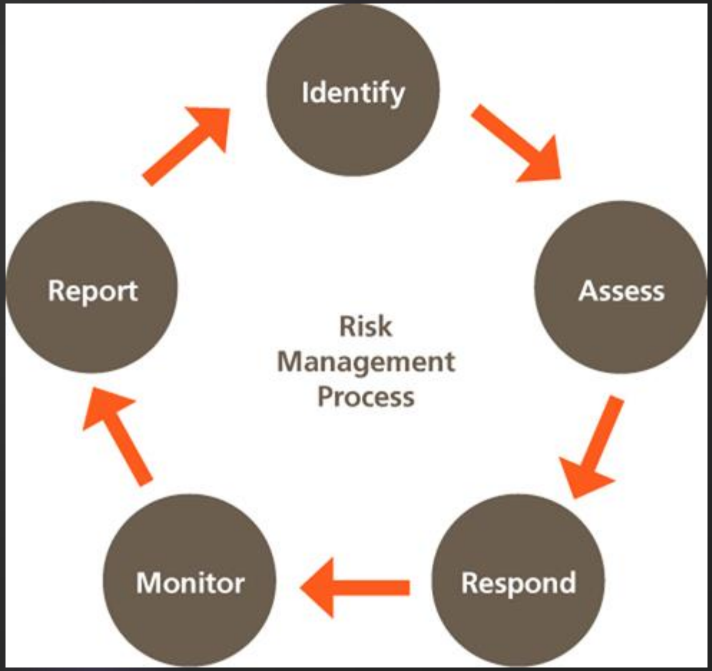
- **Risk** can be defined as a probability of the occurrence of a threat or an event that may damage, or cause loss or have other negative impact either from internal or external liabilities.
- A **risk matrix** is used during risk assessment to define the level of risk by considering the category of probability or likelihood against the category of consequence severity.



	Consequence				
Likelihood	Insignificant	Minor	Moderate	Major	Severe
Almost Certain	Medium	High	High	Extreme	Extreme
Likely	Medium	Medium	High	Extreme	Extreme
Possible	Medium	Medium	High	High	Extreme
Unlikely	Low	Medium	Medium	High	High
Rare	Low	Low	Medium	High	High

Managing the Risk (2/2)

- **Risk Management** is the identification, evaluation, and prioritization of risks.
  - **Risk Identification :** Identifies the sources, causes, consequences of the internal and external risks.
  - **Risk Assessment :** Assesses the organization risk and provides an estimate on the likelihood and impact of the risk.
  - **Risk Treatment :** Selects and implements appropriate controls on the identified risks.
  - **Risk Tracking :** Ensures appropriate control are implemented.
  - **Risk Review :** Evaluates the performance of the implemented risk management strategies.

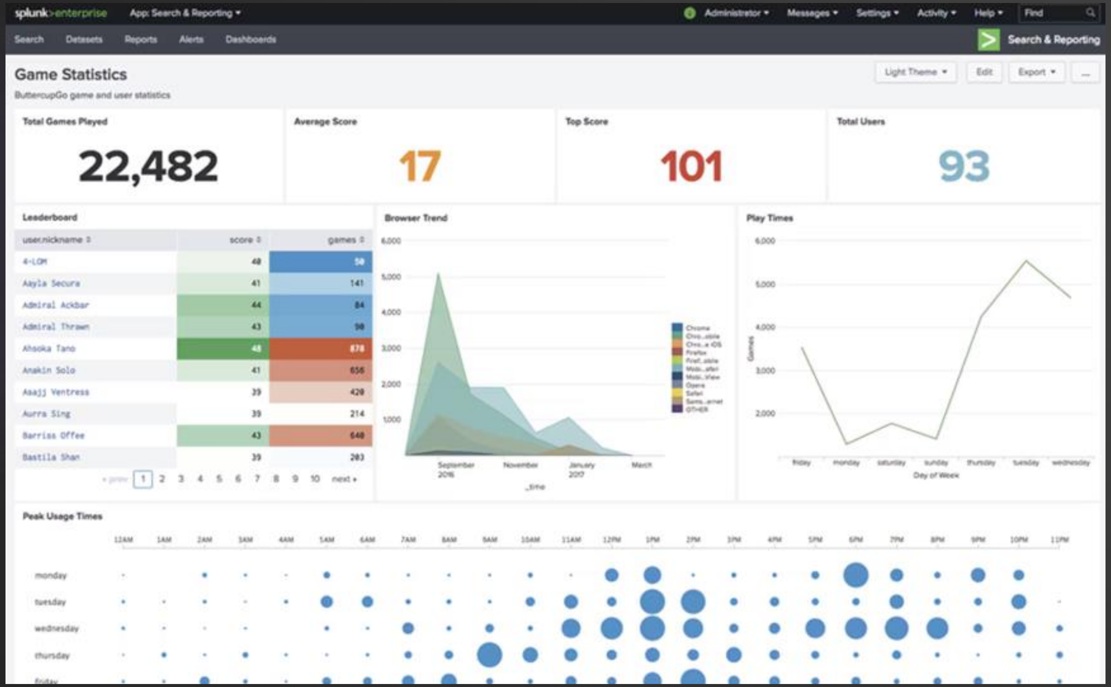


Security policies

1. **Policies :** High-level statements about protecting information. Business rules to safeguard CIA triad.
   Security Policies can be applied on Users, Systems, Partners, Networks, and Providers.
   - Security Policies examples: Password Policy
     - Meet the password complexity requirements.
     - Minimum 8 char length, upper and lower case and alphanumerical.
   - Data Retention Policy
     - Keep the data for X time.
   - Access Control Policies
     - Accessing servers; Firewalls
2. **Procedures :** Set of details steps to accomplish a goal (instructions for implementation)
3. **Guidelines :** Advice on actions given a situation (mandatory, recommended, not mandatory)

SIEM (Security Information and Event Management)

- A **SIEM** is a tool that collects, correlate, and alert (depending on the use cases created).



Game Statistics

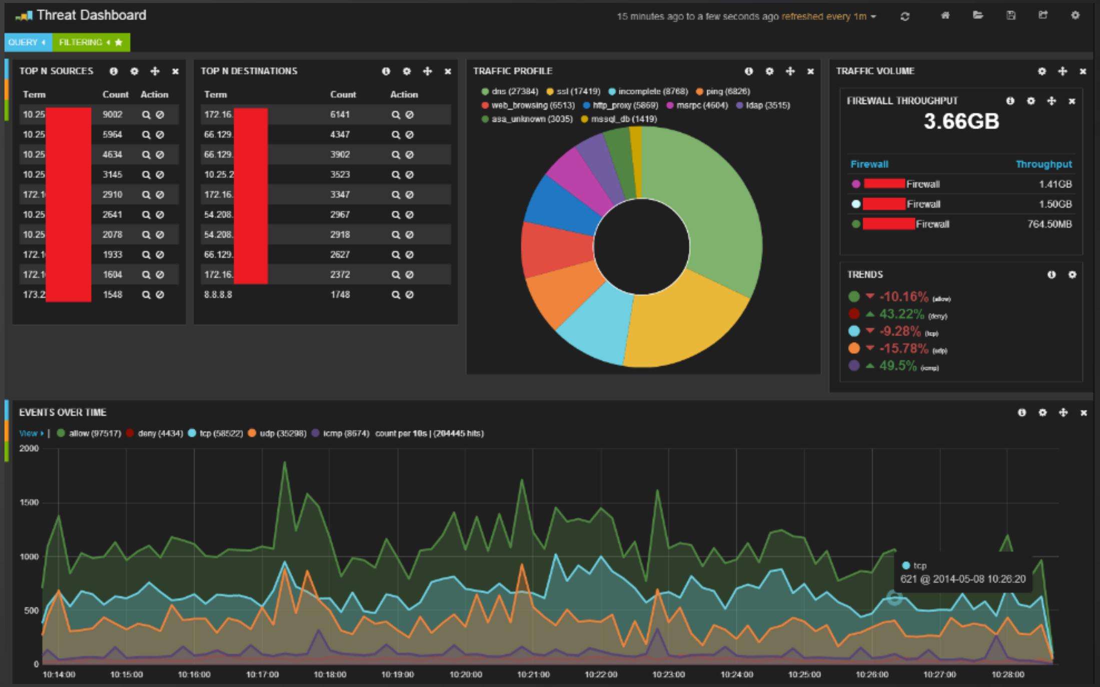
ButtercupGo game and user statistics

Total Games Played	Average Score	Top Score	Total Users
22,482	17	101	93

Leaderboard

user.nickname	score	games
4-LOM	40	50
Aayla Secura	41	141
Admiral Ackbar	44	84
Admiral Thrawn	43	90
Ahsoka Tano	48	878
Anakin Solo	41	656
Asajj Ventress	39	420
Aurra Sing	39	214
Barriss Offee	43	640
Bastila Shan	39	203

« prev 1 2 3 4 5 6 7 8 9 10 next »



TOP N SOURCES

Term	Count	Action
10.25[redacted]	9002	🔍 ⊘
10.25[redacted]	5964	🔍 ⊘
10.25[redacted]	4634	🔍 ⊘
10.25[redacted]	3145	🔍 ⊘
172.1[redacted]	2910	🔍 ⊘
10.25[redacted]	2641	🔍 ⊘
10.25[redacted]	2078	🔍 ⊘
172.1[redacted]	1933	🔍 ⊘
172.1[redacted]	1604	🔍 ⊘
173.2[redacted]	1548	🔍 ⊘

TOP N DESTINATIONS

Term	Count	Action
172.16.[redacted]	6141	🔍 ⊘
66.129.[redacted]	4347	🔍 ⊘
66.129.[redacted]	3902	🔍 ⊘
10.25.2[redacted]	3523	🔍 ⊘
172.16.[redacted]	3347	🔍 ⊘
54.208.[redacted]	2967	🔍 ⊘
54.208.[redacted]	2918	🔍 ⊘
66.129.[redacted]	2627	🔍 ⊘
172.16.[redacted]	2372	🔍 ⊘
8.8.8.8	1748	🔍 ⊘

TRAFFIC VOLUME

FIREWALL THROUGHPUT

3.66GB

Firewall	Throughput
● [redacted] Firewall	1.41GB
● [redacted] Firewall	1.50GB
● [redacted] Firewall	764.50MB

TRENDS

- ▼ -10.16% (allow)
- ▲ 43.22% (deny)
- ▼ -9.28% (tcp)
- ▼ -15.78% (udp)
- ▲ 49.5% (icmp)

Indicators Of Compromise (IOCs)

- Indicators of Compromise (IOC) are the clues and pieces of forensic data found on the network or operating system of an organization that indicate a potential intrusion or malicious activity in the organization’s infrastructure.
- Security professionals need to perform continuous monitoring of IOC to detect and respond to evolving cyber threats.

IAM (Identity and Access Management) 1/2

1. **Identification :** The information on credentials identifies the user.
    - Example: Your name, username, ID number, employee number, SSN etc.
2. **Authentication :** “Prove you are the legitimate User“ (Should always be done with Multifactor Authentication).
    - Authentication Factors:
        - Something you know (e.g. - password)
        - Something you have (e.g. - smart card)
        - Something you are (e.g. - fingerprint)
        - Something you do (e.g. - android pattern; manual signature)
        - Somewhere you are (e.g. - geolocation)

- Multi-factor authentication generally uses two of this examples (e.g. - Something you Know and Something you Have (but never on same category).

IAM (Identity and Access Management) 2/2

3. **Authorization** : What are you allowed to access.
   - Permissions:
     - Applied to resources
   - Rights / Privileges:
     - Assign at system level
   - Authorization strategies:
     - Least privileged
   - Separation of Duties
4. **Accouting :** Trace an Action to a Subjects Identity:
   - Prove who did what (non-repudiation / Logging).

DLP (Data Lost Prevention)

- A DLP is a a practice of **detecting and preventing data breaches, exfiltration, or unwanted destruction of sensitive data.** Organizations use DLP to protect and secure their data and comply with regulations.
- The DLP term refers to defending organizations against both **data loss and data leakage prevention**.
- Organizations typically use DLP to:
  - Protect Personally Identifiable Information (PII) and comply with relevant regulations;
  - Protect Intellectual Property critical for the organization;
  - Achieve data visibility in large organizations;
  - Secure data on remote cloud systems and on mobile equipments.

Testing types in pentest

- **Black box:** testing involves performing a security evaluation and testing with no prior knowledge of the infrastructure.
- **White box** testing involves performing a security evaluation and testing with complete knowledge of the infrastructure.
- **Gray box** testing involves a combination of white-box testing and black-box testing. The aim of this testing is to search for the defects if any due to improper structure or improper usage of applications.

All steps to execute a pentest

1. Talk to the client about the perimeter (IP, domain, etc.) and types of attacks that may create a risk for the customer (brute force, DoS, etc.).
2. Prepare and sign with the client the NDA (non-disclosure agreement)
3. Conduct the pentest and collect information in order to provide a report.
4. Write the report and have it proofread by a colleague.
5. Present the report findings to the client (report, documentation, etc.).

Warning : It is legally forbidden to scan / pentest / etc. if you haven't been commissioned for it or that the solution is not yours.

Hacking phase

- In general there are five phases of hacking :
  - **Reconnaissance**
  - **Scanning**
  - **Gaining Access**
  - **Maintaining Access**
  - **Clearing Tracks**

Hacking phase : Reconnaissance

- Reconnaissance refers to the preparatory phase where an attacker seeks to gather information about a target prior to launching an attack.
- The reconnaissance target range may include the target organization’s clients, employees, operations, network and systems.
  - **Passive reconnaissance** there will be no traffic generated on the target's infrastructure, it is a matter of finding public data by conventional or specialized search engines (wireshark, shodan, etc.).
  - **Active reconnaissance** it is a question of going directly to question the "target". For example, a server's ports can be scanned to see which services they are responding to.

Hacking phase : Scanning

- **Pre-attack** : Scanning refers to the pre-attack phase when the attacker scans the network for specific information based on information gathered during reconnaissance.
- **Port scanner** : Scanning can include many tools like port scanners, network mappers, ping tools, vulnerability scanners, etc.
- **Extract information** : Attackers extract information such as live machines, port, port status, OS details, device type, and system uptime to launch attack.

Hacking phase : Gaining Access

- Gaining access refers to the point where the attacker obtains access to the operating system or applications on the target computer or network.
- The attacker can gain access at the operating system, application or network levels.
- The attacker can escalate privileges to obtain complete control of the system.
- Type of gaining access:
  - password cracking,
  - buffer overflows,
  - session hijacking,
  - Etc.

Hacking phase : Maintaining Access

- Maintaining access refers to the phase when the attacker tries to retain their ownership of the system.
- Attackers may prevent the system from being owned by other attackers by securing their exclusive access with backdoors by example.
- Attackers can upload, download or manipulate data, applications and configurations on the owned system.
- Attackers use the compromised system to launch further attacks (example with pivoting).

Hacking phase : Clearing Tracks

- Clearing tracks refers to the activities carried out by an attacker to hide malicious acts.
- The attacker's intentions is to remain unnoticed by deleting evidence that might lead to their prosecution.

Kill Chain Frameworks

- Kill Chain are frameworks to prevent and identify cyber intrusions activity.
- The two main frameworks are :
  - ATT&CK : https://attack.mitre.org/
  - Cyber Kill Chain : https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html
- ATT&CK and the Cyber Kill Chain are complementary.
- I prefer ATT&CK because tactics are unordered and may not all occur in a single intrusion because adversary tactical goals change throughout an operation, whereas the Cyber Kill Chain uses ordered phases to describe high level adversary objectives.

Cyber Kill chain : Attack phases

The kill chain is a framework methodology is a component of intelligence-driven defense for the identification and prevention of malicious intrusion activities.

Pre-attack

1. **Reconnaissance**: Gather information to probe for weak points
2. **Weaponization**: Create a deliverable malicious payload using an exploit and a backdoor.

Attack

3. **Delivery**: Send weaponized bundle to the victim using email, USB, etc.
4. **Exploitation**: Exploit a vulnerability by executing code on the victim's system.
5. **Installation**: Install malware on the system target.
6. **Command and Control / Persistence**: Create a command and control to communicate and pass data back and forth.
7. **Actions on Objective**: Perform actions to achieve intended objectives or goals.

ATT&CK Tactics, Techniques and Procedures

- **Tactics** are the guidelines that describe the way of an attacker performs the attack from beginning to the end : https://attack.mitre.org/tactics/enterprise/

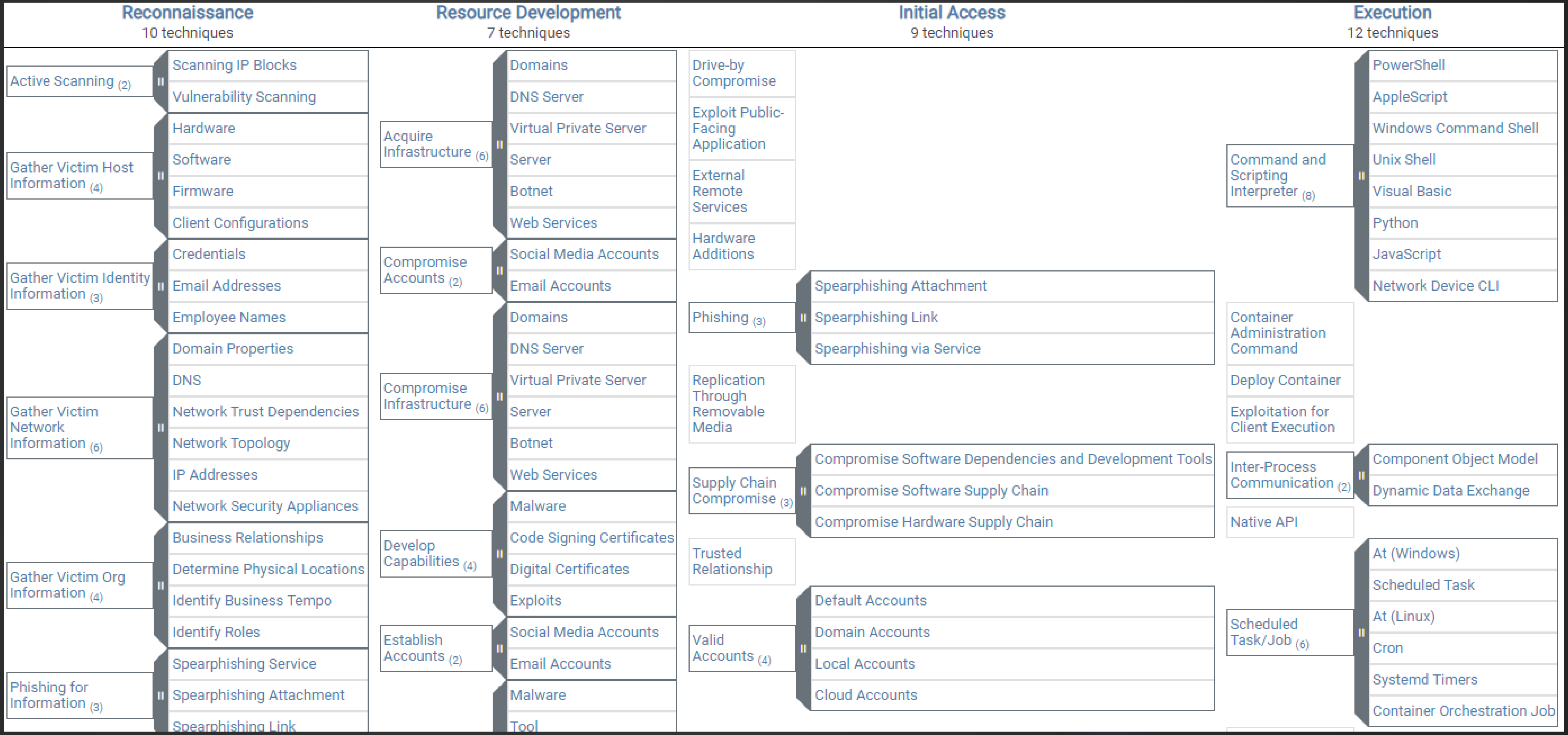
- **Techniques** are the technical methods used by an attacker to achieves his wish (exploitation , command and control, covering the tracks, etc.). https://attack.mitre.org/techniques/enterprise/

- **Procedures** are organizational approaches that threat actors follow to launch an attack.
  Example how hacker can gather informations ?

Tactics, Techniques and Procedures

Tactics

Techniques



Reconnaissance
10 techniques

- Active Scanning (2)
  - Scanning IP Blocks
  - Vulnerability Scanning
- Gather Victim Host Information (4)
  - Hardware
  - Software
  - Firmware
  - Client Configurations
- Gather Victim Identity Information (3)
  - Credentials
  - Email Addresses
  - Employee Names
- Gather Victim Network Information (6)
  - Domain Properties
  - DNS
  - Network Trust Dependencies
  - Network Topology
  - IP Addresses
  - Network Security Appliances
- Gather Victim Org Information (4)
  - Business Relationships
  - Determine Physical Locations
  - Identify Business Tempo
  - Identify Roles
- Phishing for Information (3)
  - Spearphishing Service
  - Spearphishing Attachment
  - Spearphishing Link

Resource Development
7 techniques

- Acquire Infrastructure (6)
  - Domains
  - DNS Server
  - Virtual Private Server
  - Server
  - Botnet
  - Web Services
- Compromise Accounts (2)
  - Social Media Accounts
  - Email Accounts
- Compromise Infrastructure (6)
  - Domains
  - DNS Server
  - Virtual Private Server
  - Server
  - Botnet
  - Web Services
- Develop Capabilities (4)
  - Malware
  - Code Signing Certificates
  - Digital Certificates
  - Exploits
- Establish Accounts (2)
  - Social Media Accounts
  - Email Accounts
  - Malware
  - Tool

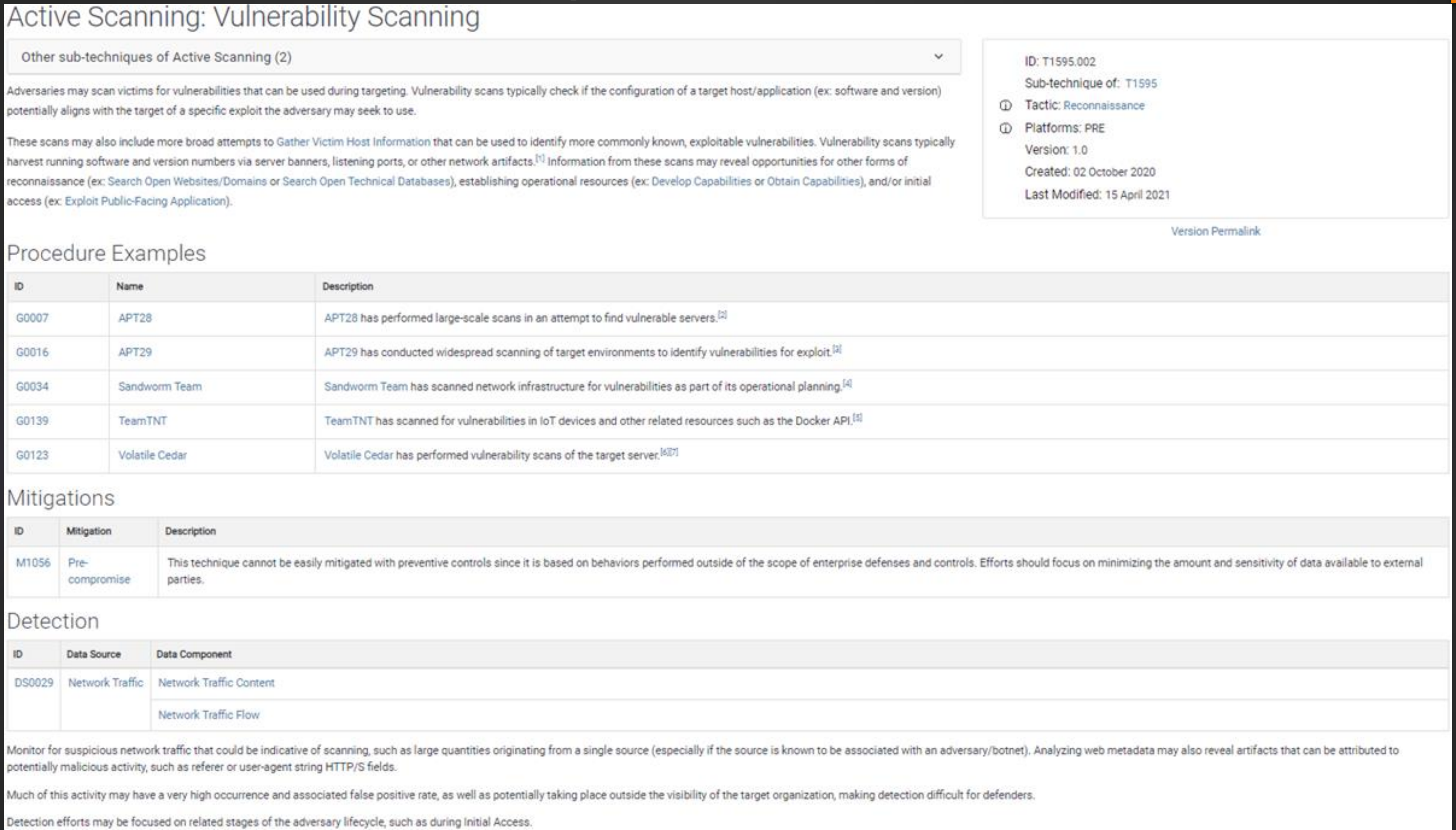
Initial Access
9 techniques

- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing (3)
  - Spearphishing Attachment
  - Spearphishing Link
  - Spearphishing via Service
- Replication Through Removable Media
- Supply Chain Compromise (3)
  - Compromise Software Dependencies and Development Tools
  - Compromise Software Supply Chain
  - Compromise Hardware Supply Chain
- Trusted Relationship
- Valid Accounts (4)
  - Default Accounts
  - Domain Accounts
  - Local Accounts
  - Cloud Accounts

Execution
12 techniques

- Command and Scripting Interpreter (8)
  - PowerShell
  - AppleScript
  - Windows Command Shell
  - Unix Shell
  - Visual Basic
  - Python
  - JavaScript
  - Network Device CLI
- Container Administration Command
- Deploy Container
- Exploitation for Client Execution
- Inter-Process Communication (2)
  - Component Object Model
  - Dynamic Data Exchange
- Native API
- Scheduled Task/Job (6)
  - At (Windows)
  - Scheduled Task
  - At (Linux)
  - Cron
  - Systemd Timers
  - Container Orchestration Job

Tactics, Techniques and Procedures



Active Scanning: Vulnerability Scanning

Adversaries may scan victims for vulnerabilities that can be used during targeting. Vulnerability scans typically check if the configuration of a target host/application (ex: software and version) potentially aligns with the target of a specific exploit the adversary may seek to use.

These scans may also include more broad attempts to Gather Victim Host Information that can be used to identify more commonly known, exploitable vulnerabilities. Vulnerability scans typically harvest running software and version numbers via server banners, listening ports, or other network artifacts.[1] Information from these scans may reveal opportunities for other forms of reconnaissance (ex: Search Open Websites/Domains or Search Open Technical Databases), establishing operational resources (ex: Develop Capabilities or Obtain Capabilities), and/or initial access (ex: Exploit Public-Facing Application).

ID: T1595.002
Sub-technique of: T1595
ⓘ Tactic: Reconnaissance
ⓘ Platforms: PRE
Version: 1.0
Created: 02 October 2020
Last Modified: 15 April 2021

Version Permalink

Procedure Examples

ID	Name	Description
G0007	APT28	APT28 has performed large-scale scans in an attempt to find vulnerable servers.[2]
G0016	APT29	APT29 has conducted widespread scanning of target environments to identify vulnerabilities for exploit.[3]
G0034	Sandworm Team	Sandworm Team has scanned network infrastructure for vulnerabilities as part of its operational planning.[4]
G0139	TeamTNT	TeamTNT has scanned for vulnerabilities in IoT devices and other related resources such as the Docker API.[5]
G0123	Volatile Cedar	Volatile Cedar has performed vulnerability scans of the target server.[6][7]

Mitigations

ID	Mitigation	Description
M1056	Pre-compromise	This technique cannot be easily mitigated with preventive controls since it is based on behaviors performed outside of the scope of enterprise defenses and controls. Efforts should focus on minimizing the amount and sensitivity of data available to external parties.

Detection

ID	Data Source	Data Component
DS0029	Network Traffic	Network Traffic Content
		Network Traffic Flow

Monitor for suspicious network traffic that could be indicative of scanning, such as large quantities originating from a single source (especially if the source is known to be associated with an adversary/botnet). Analyzing web metadata may also reveal artifacts that can be attributed to potentially malicious activity, such as referer or user-agent string HTTP/S fields.

Much of this activity may have a very high occurrence and associated false positive rate, as well as potentially taking place outside the visibility of the target organization, making detection difficult for defenders.

Detection efforts may be focused on related stages of the adversary lifecycle, such as during Initial Access.

Improve your skills

Plateform	Description	URL	Skills to begin
DVWA	Damn Vulnerable Web App is a web vulnerable application	https://dvwa.co.uk	☆☆☆
TryHackMe	Platform with interactive lessons.	https://tryhackme.com	☆☆☆
HackTheBox	Platform to test your skills in penetration testing.	https://www.hackthebox.com	★☆☆
RootMe	Plateform with many little games and CTF	https://www.root-me.org	★☆☆
VulnHub	Plateform to share vulnerable VM.	https://www.vulnhub.com	★★☆

Improve your skills ++

- A bug bounty program is a deal offered by many websites, organizations and software developers by which individuals can receive recognition and compensation for reporting bugs, especially those pertaining to security exploits and vulnerabilities.

- Bug bounty plateform:
  - https://www.hackerone.com/
  - https://www.bugcrowd.com/
  - https://www.yeswehack.com/
  - https://www.openbugbounty.org/