KPMG

Hacker Fundamentals

Presented by: Yusef Ward, Jagjit SIngh

—

Date 29|.05.2023

About the Course

This course will give you the fundamentals to do the following:

- Gain an understanding of ethical hacking concepts and principles.
- Learn about different types of cyber threats and attacks.
- Explore common vulnerabilities in computer systems and how to identify them.
- Learn about tools and techniques used by hackers and how to defend against them.
- Obtain practical knowledge and skills that can be applied in real-world scenarios to enhance cybersecurity posture.

About the Course

It is a **practical course**. Even though there is a slide deck, we will hack systems together which requires active communication and hands-on. So, don't hesitate to ask questions! ☺

This course will not make you a "master hacker". The purpose of this course is to learn the fundamentals. To be a capable hacker, it requires a lot of (self) work.

Introductions

```
[~]$ whoami
```

ARSLAN MASOOD
Course Instructor
Cybersecurity Expert
CRTO, OSCP

J leads the Red Team and Network Testing teams in KPMG. His main areas of expertise:

- Red Teaming
- Network Security
- Web security
- Exploit development

YUSEF WARD
Course Instructor
Cybersecurity Expert
GPEN, eWAPT

Yusef joined KPMG in 2021. His main areas of expertise:

- Web Security
- Network Security

Course Schedule

DAY 1

- 9:00 - 9:30 Introduction to course
- 9:30 - 10:30 Introduction to Hacking
- 10:30 - 10:45 Coffee Break
- 10:45 - 12:00 Information Gathering
- 12:00 - 13:00 Lunch Break
- 13:00 - 14:30 Scanning and Enumeration
- 14:30 - 14:45 Coffee Break
- 14:45 - 15:30 Vulnerability Assessments
- 15:30 – 17:00 Lab Exercise: Vulnerability Assessments

DAY 2

- 9:00 - 9:30 Recap of Day 1
- 9:30 - 10:30 Exploitation
- 10:30 - 10:45 Coffee Break
- 10:45 - 12:00 Lab exercise: Exploiting Vulnerable Systems
- 12:00 - 13:00 Lunch Break
- 13:00 - 14:30 Post Exploitation
- 14:30 - 14:45 Coffee Break
- 14:45 - 15:30 Lab Exercise: Escalating Privileges
- 15:30 - 16:00 Maintaining Access/Covering Tracks
- 16:00 – 17:00 Hacking Trivia

Getting Started

We will need the following to get started:

- Kali VM provided by KPMG
- VPN configuration files
- Course cheatsheets (Optional)

01

Introduction to Hacking

What is hacking?

Hacking defined

“The act of attempting to gain unauthorized access to computer systems or networks, usually with the intent to steal, modify, or destroy data or to disrupt the normal functioning of the system or network.”

- It involves using technical skills and creativity to identify and exploit vulnerabilities in various in scope targets.

Fundamentals of Hacking

There is always a target.

- Sometimes the target is known and at times it needs to be discovered.
- The target can be of various types including computer systems, networks, websites, applications, IoT devices, clouds and can also include humans and organizations.

Fundamentals of Hacking

- The targets we look for can be **vulnerable** in some form.
- Hacking involves identifying those **vulnerabilities** in computer systems and networks.
- This involves **understanding** how computer systems and networks work and using tools and techniques to find weaknesses in them.

Fundamentals of Hacking

Vulnerabilities can be exploited.

- Once vulnerabilities have been identified, hackers use various tools and techniques to exploit them.
- This involves taking advantage of the vulnerability to gain unauthorized access to the system or network, steal data, modify data, or disrupt the normal functioning of the target.

Fundamentals of Hacking

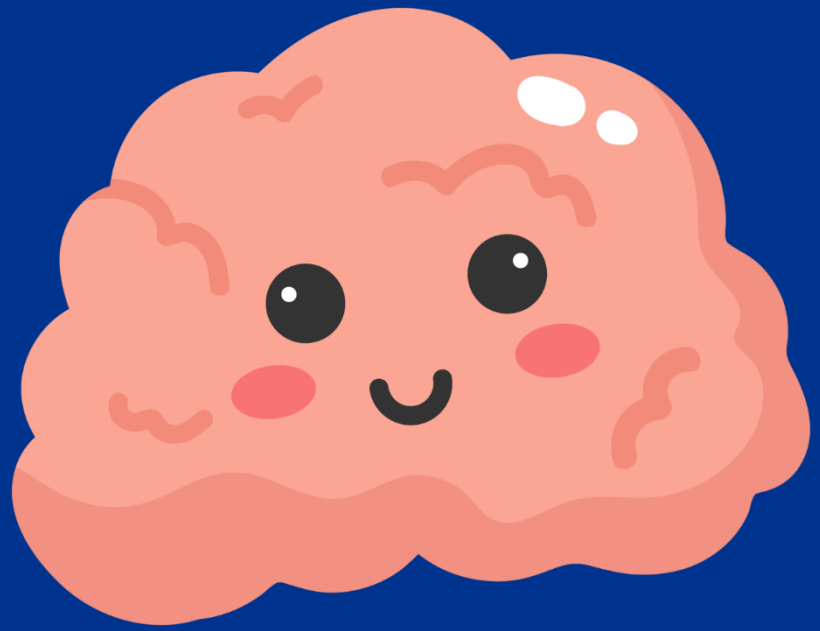
Technical skills are used for hacking.

- Hackers need to understand how the target works, how they can be vulnerable and how to use their tools and techniques to exploit them.
- Different targets need different skills. For example, a social engineer hacking a company employee will need a different skillset than an application penetration tester.
- Similar to the above point, different skills have different tools – hackers need to properly understand how their tools work to not cause any adverse effects.

Fundamentals of Hacking

Creativity plays a role

- Hacking involves the ability to think outside the box and come up with innovative ways to exploit vulnerabilities.
- Creativity is often required to identify new attack vectors or develop custom exploits that are not covered by existing tools and techniques.



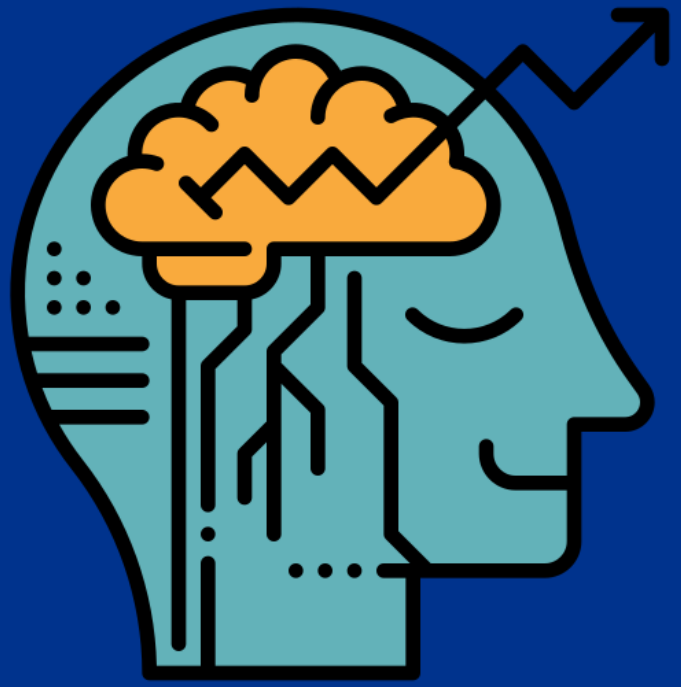
Fundamentals of Hacking

Record keeping is essential.

- Accurate note taking has proven itself to be valuable time after time.
- Need to keep track of commands, tricks, payloads used throughout the engagement.
- Timestamps make for accurate reporting.

Fundamentals of Hacking

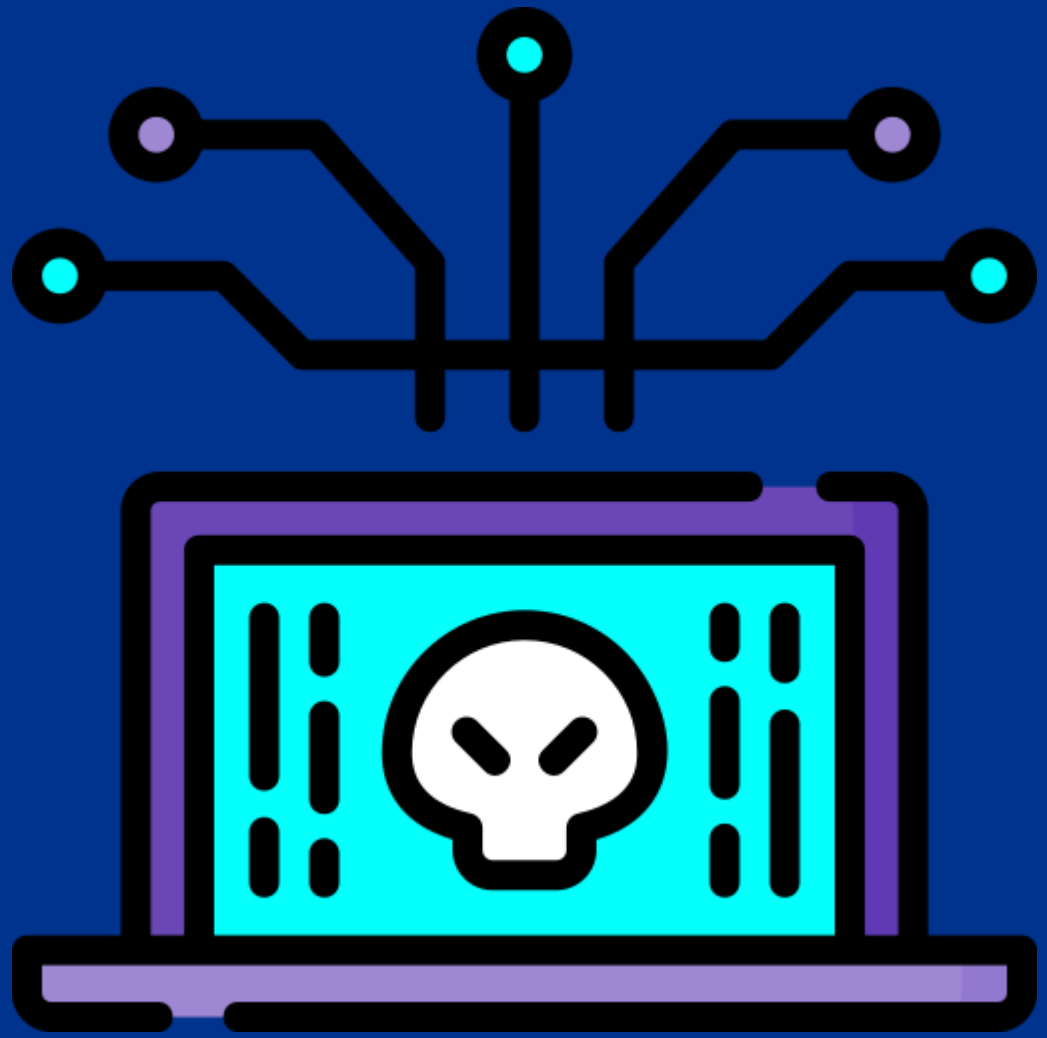
To become a successful hacker, it's important to constantly learn and stay up-to-date with the latest technologies, techniques, and vulnerabilities. Hacking requires persistence, creativity, and a deep curiosity about how things work. This is also known as **the hacker mindset**.



Fundamentals of Hacking - Steps

Hacking usually consists of these steps:

1. Identify the target
2. Communicate with the target
3. Find vulnerabilities in the target
4. Exploit vulnerabilities
5. Post exploitation



In this course, we will have a target that we will:

1. Discover
2. Enumerate (communicate with)
3. Identify their vulnerabilities
4. Exploit vulnerabilities to gain access
5. Post exploitation actions

Types of hacking

Legal and Ethical Considerations

- **Obtain permission**: Ethical hackers must obtain proper permissions and authorizations before conducting any testing.
- **Respect privacy and confidentiality**: Ethical hackers should access only necessary information and avoid disclosing sensitive information.
- **Follow laws and regulations**: Ethical hackers must comply with applicable laws and regulations.
- **Avoid harm and damage**: Ethical hackers must take steps to prevent causing harm to the systems they are testing or any other individuals or organizations.
- **Disclose vulnerabilities**: Ethical hackers must promptly disclose any vulnerabilities they discover and provide clear and detailed recommendations for remediation.
- **Continuously learn and improve**: Ethical hackers should stay up-to-date with the latest techniques and engage in ongoing learning and improvement.

Types of hackers

- White Hat Hackers
- Black Hat Hackers
- Gray Hat Hackers
- Script Kiddies
- State-sponsored Hackers
- Hacktivists
- Phreakers
- Malware Developers
- Professional Hackers

Professional hacking forms

- Penetration Testing
  - Web applications
  - Networks
  - Devices
  - Wireless
  - Cloud
- Red Teaming
- Social Engineering
- Physical Security

CYBER FRAMEWORKS

Frameworks help guide professional ethical hacking engagements. Sometimes, customers require (or request) specific frameworks.

As an ethical hacker, it is important to have knowledge of popular exploit and vulnerability frameworks,

Some examples of frameworks are:

- **OWASP**
- **PTES**
- **MITRE ATT&CK**

Introduction to MITRE ATT&CK Framework

The **MITRE ATT&CK Framework** is a comprehensive knowledge base of adversary **tactics**, **techniques**, and **procedures** (**TTPs**).

It is a globally-accessible, structured framework that is used by cybersecurity professionals to describe, analyze, and understand cyber threats.

The matrix is organized into 12 tactics:

- The tactics are broken down into 100+ techniques that describe specific methods used by attackers to achieve their goals.
- Each technique is assigned a unique identifier, a description, and links to relevant examples and detection methods.

Lets see the different asset types we could see, the skills we will need to hack them and what we can do after we hack them...

Computer Systems

Computer Systems

Information that is important to know about a computer as a target:

1. Operating system: Windows, Linux, MacOS
2. Hardware specifications: CPU, memory, storage
3. Network connections: IP address, firewall settings, open ports

Computer Systems

Some of the ways how computer systems can be vulnerable to exploitation are:

- Unpatched software or operating systems
- Misconfigured settings or weaknesses
- Social engineering attacks such as phishing or pretexting
- Malware infections or backdoors

Computer Systems

The skills needed to identify vulnerabilities and hack a target:

- Knowledge of operating systems, software, and protocols
- Familiarity with common attack vectors and exploit techniques
- Proficiency in using vulnerability scanners, penetration testing tools, and debugging utilities
- Understanding of defensive measures and how to bypass them
- Expertise in coding and scripting to create custom attack tools

Computer Systems

What can we do when we successfully hack a computer system?

- Escalating privileges to gain administrative access
- Installing backdoors or trojans for persistent access
- Stealing or manipulating data
- Covering tracks to avoid detection

Applications and Services

Applications and Services

Information that is important to know about applications & services as a target:

1. Type of application or service: web application, mobile app, database, email server, etc.
2. Common programming languages: Java, Python, PHP, .NET, etc.
3. Frameworks and libraries used: Django, Flask, Ruby on Rails, etc.

Fact: **Web applications are one of the most commonly targeted assets by hackers due to their prevalence and importance in organizations.**

Applications and Services

Some of the ways how applications & services can be vulnerable to exploitation are:

- Input validation errors or injection attacks (e.g. SQL injection, XSS)
- Insecure configurations or weak authentication mechanisms
- Vulnerable software components or dependencies
- Insufficient encryption or hashing mechanisms

OWASP

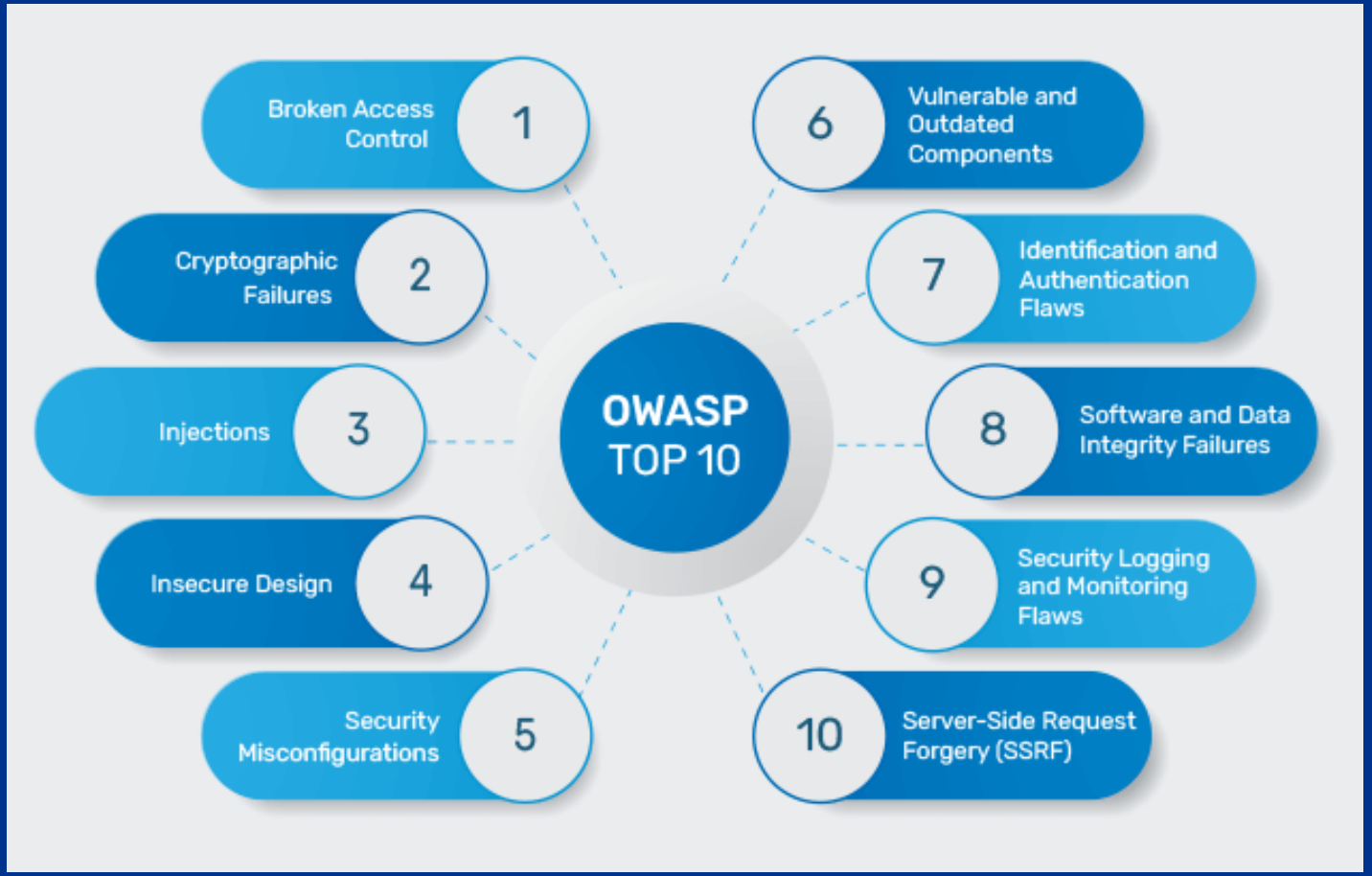
OWASP (**The Open Web Application Security Project**) is an online community that produces freely-available articles, methodologies, documentation, tools, and technologies in the field of web application security.

The methodologies they have published are:

- **Web Security Testing Guide** (**WSTG**)
- **Mobile Security Testing Guide** (**MSTG**)
- **Firmware Security Testing Methodology**
- **Application Security Verification Standard (ASVS)**

Web Application Security Basics

OWASP Top 10 vulnerability categories (**OWASP Top 10 2021**):



Applications and Services

The skills needed to identify vulnerabilities and hack a target:

- Knowledge of programming languages, web frameworks, and database systems
- Familiarity with common web application vulnerabilities and attack vectors
- Proficiency in using automated vulnerability scanners and manual testing techniques
- Understanding of defensive measures and how to bypass them
- Expertise in coding and scripting to create custom attack tools

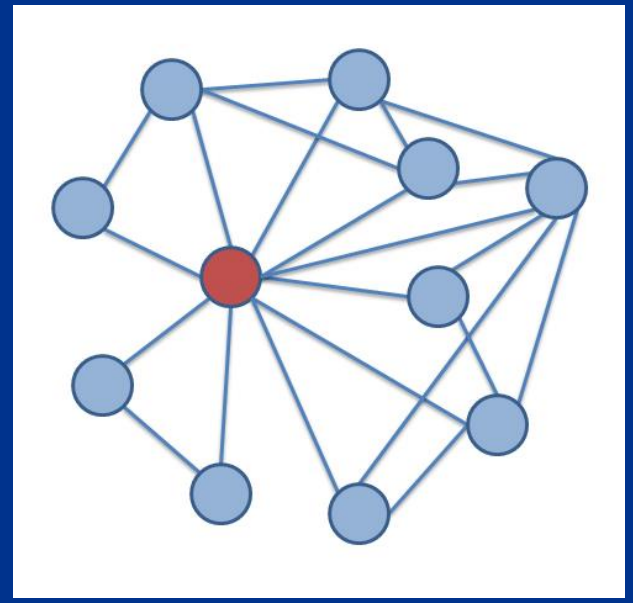
Applications and Services

What can we do when we successfully hack an application or service?

- Escalating privileges to gain administrative access
- Stealing or manipulating data
- Covering tracks to avoid detection

Networks

Networks



Information that is important to know about networks as a target:

1. Network topology and devices
2. Ports and services in use
3. Security controls and policies in place
4. Network traffic and communication patterns

Fact: **Networks are often vulnerable as organizations focus on outside perimeters (applications, services etc.) more than internal networks.**

Networks

Some of the ways how networks can be vulnerable to exploitation are:

- Misconfigured network devices
- Poorly configured firewalls and other security controls
- Inadequate segmentation between networks
- Weak passwords or authentication methods
- Social engineering attacks, such as phishing or spear-phishing

Networks

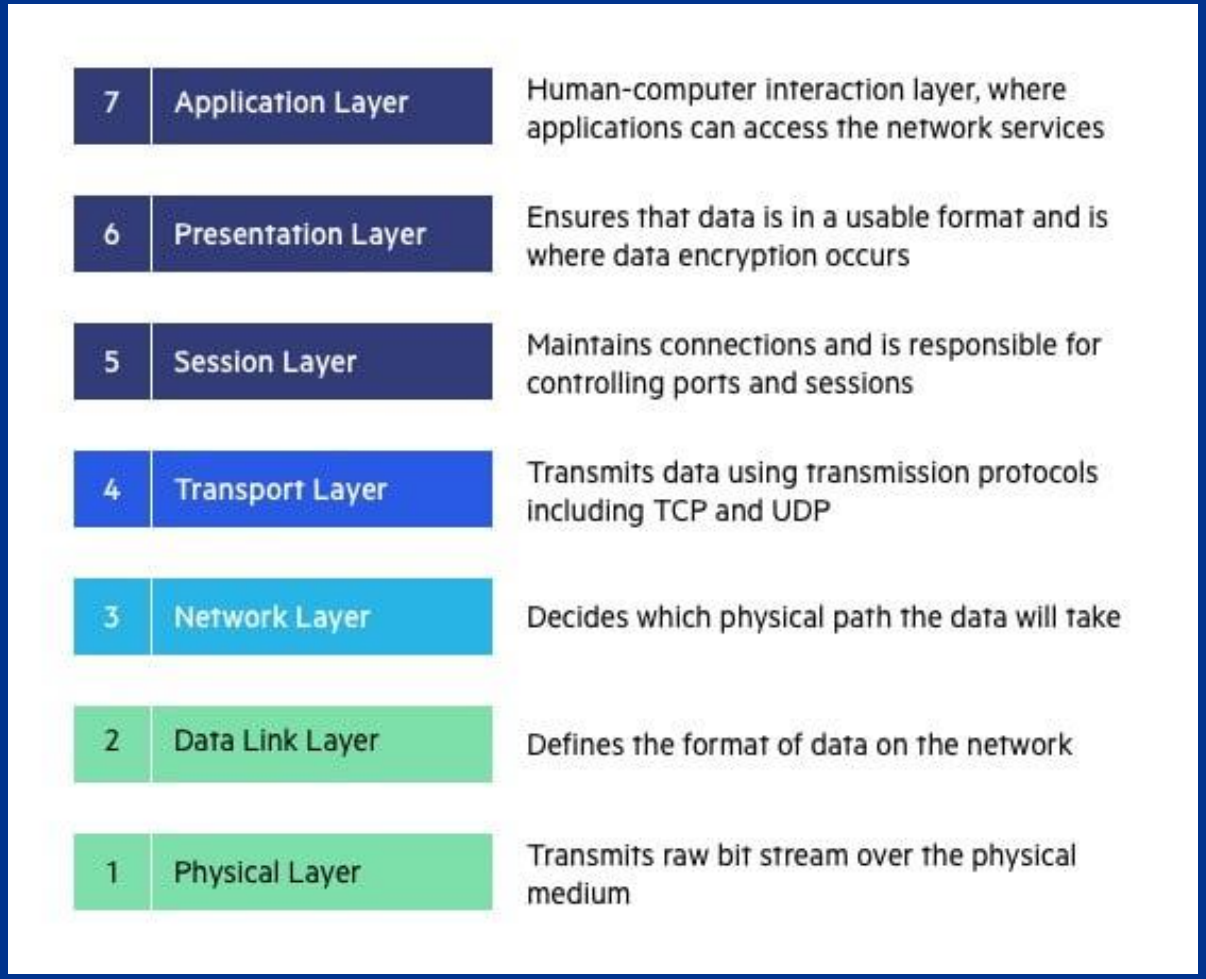
Skills needed to identify vulnerabilities and hack target:

- Network scanning and reconnaissance
- Exploitation of open ports and services
- Sniffing and analysis of network traffic
- Use of network-level exploits and attacks

Introduction to Networking Concepts

Understanding of the **Open Systems Interconnection** (**OSI**) model:

- The OSI model is a conceptual framework that describes the different layers involved in networking and communication.
- Hackers need to have a basic understanding of the OSI model in order to identify and exploit vulnerabilities at different layers.



Introduction to Networking Concepts

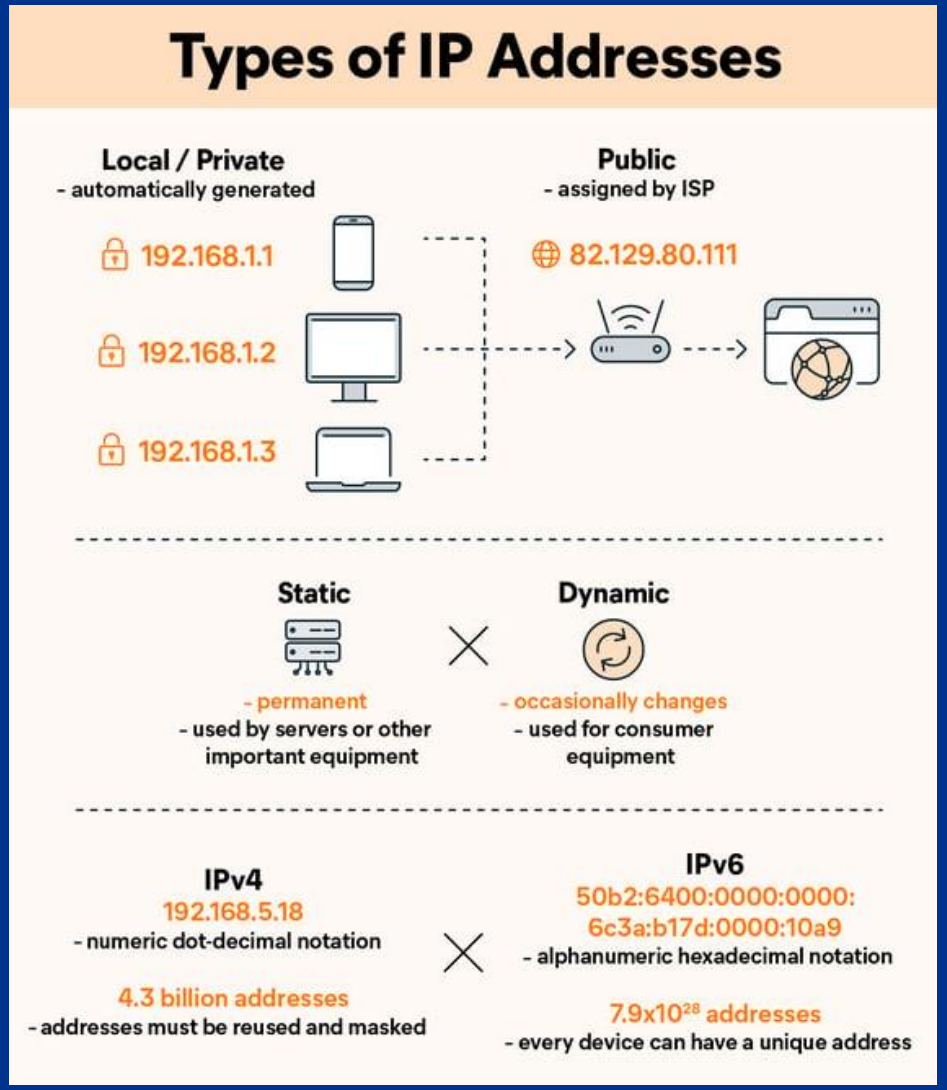
Knowledge of **TCP/IP** protocols:

- TCP/IP is the suite of protocols that is used for communication on the Internet and most computer networks.
- Hackers need to be familiar with the different TCP/IP protocols, such as **TCP**, **UDP**, **IP**, **ICMP**, and others, in order to identify and exploit vulnerabilities.

Introduction to Networking Concepts

IP addressing and subnetting:

- IP addressing is a fundamental concept in networking that involves assigning unique addresses to devices on a network.
- Hackers need to be able to understand IP addressing and subnetting in order to identify and target specific devices on a network.



Private vs Public IPs

172.16.1.1

10.10.23.1

194.100.12.194

192.168.1.9

Introduction to Networking Concepts

Network protocols and services:

- Hackers need to be familiar with common network protocols and services, such as **DNS**, **DHCP**, **HTTP**, **FTP**, **SSH**, and others, in order to identify vulnerabilities and exploit them.

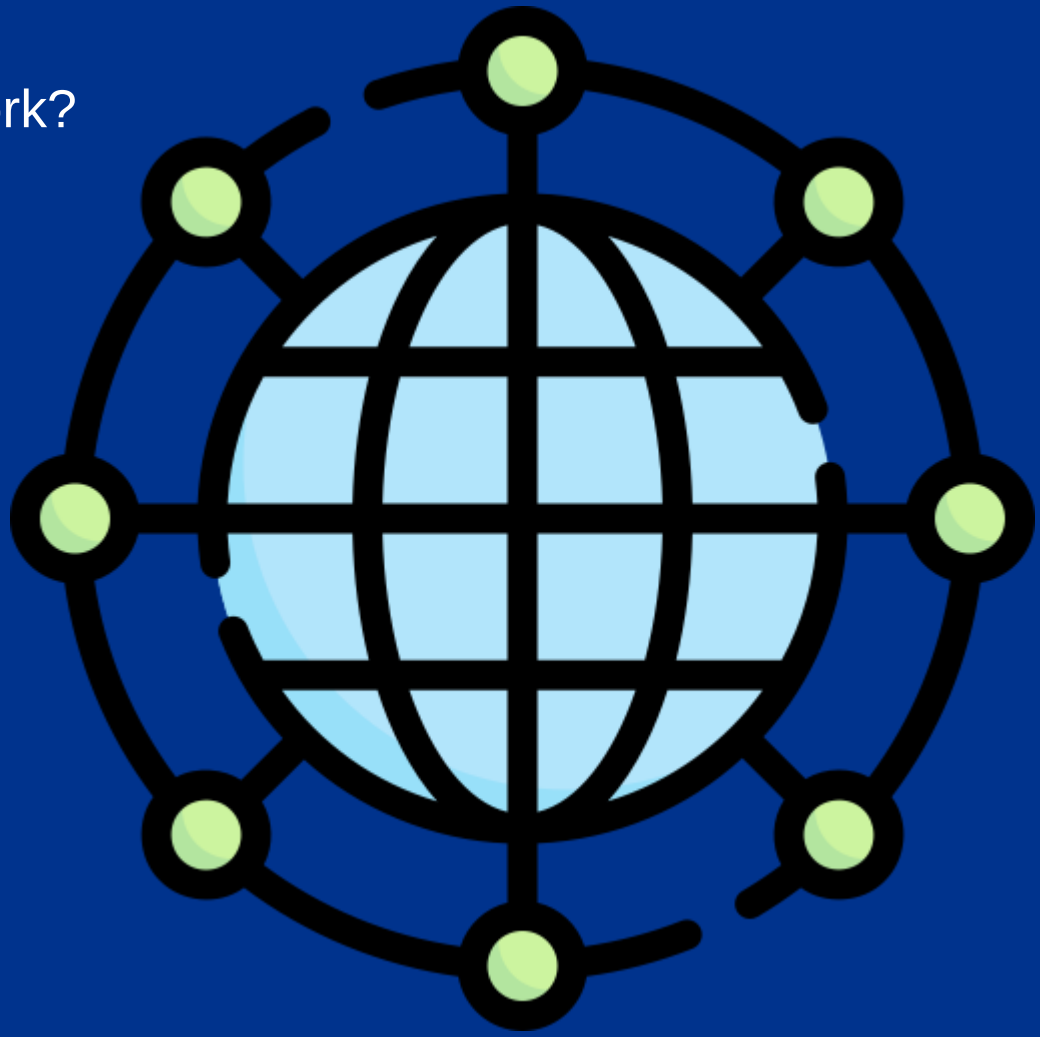
Well-Known Ports

Service	Port	Function
HTTP	80	Web traffic
HTTPS	443	Secure web traffic
FTP	20, 21	File transfer
DNS	53	Name resolution
SMTP	25	Internet mail
POP3	110	Post Office Protocol (POP) mailbox
IMAP	143	Internet Message Access Protocol (IMAP) Mailbox
Telnet	23	Remote login
SSH	22	Secure remote logn

Networks

What can we do when we successfully hack a network?

- Network infiltration and persistence
- Traffic interception and redirection
- Data exfiltration



Humans

Humans

Information that is important to know about humans as a target:

- Humans are often the weakest link in security
- Phishing attacks are a common way to target individuals
- Password reuse and weak passwords are common

Humans

Some of the ways how humans can be vulnerable to exploitation are:

- Social engineering attacks, such as phishing or spear-phishing
- Malicious attachments or links in emails
- Unsecured personal devices, such as mobile phones or laptops

Humans

Skills needed to identify vulnerabilities and hack target:

- Social engineering tactics and manipulation techniques
- Phishing campaign creation
- Malware analysis and reverse engineering
- OSINT (Open Source Intelligence Gathering)

Humans

What can we do when we successfully hack a human?

- Installing malware on personal devices
- Stealing personal data
- Gaining access to work-related accounts or systems

Organizations

Organizations

Information that is important to know about organizations as a target:

1. Organizations present a combination of various computer systems, applications, and networks that they may own.
2. Sensitive data, such as customer data or financial information, is often stored on their systems.

Organizations

Some of the ways how networks can be vulnerable to exploitation are:

- Poorly secured systems or networks
- Insider threats from employees or contractors
- Social engineering attacks, such as phishing or spear-phishing

Organizations

Skills needed to identify vulnerabilities and hack target:

- Social engineering tactics and manipulation techniques
- Network and system penetration testing
- Threat intelligence gathering
- Incident response and forensic analysis

Organizations

What can we do when we successfully hack an organization?

- Installing backdoors or rootkits
- Elevating privileges
- Stealing sensitive data

COURSE SCENARIO

Captain Crunch Industries, a fictional company, has requested our team to conduct a penetration test.

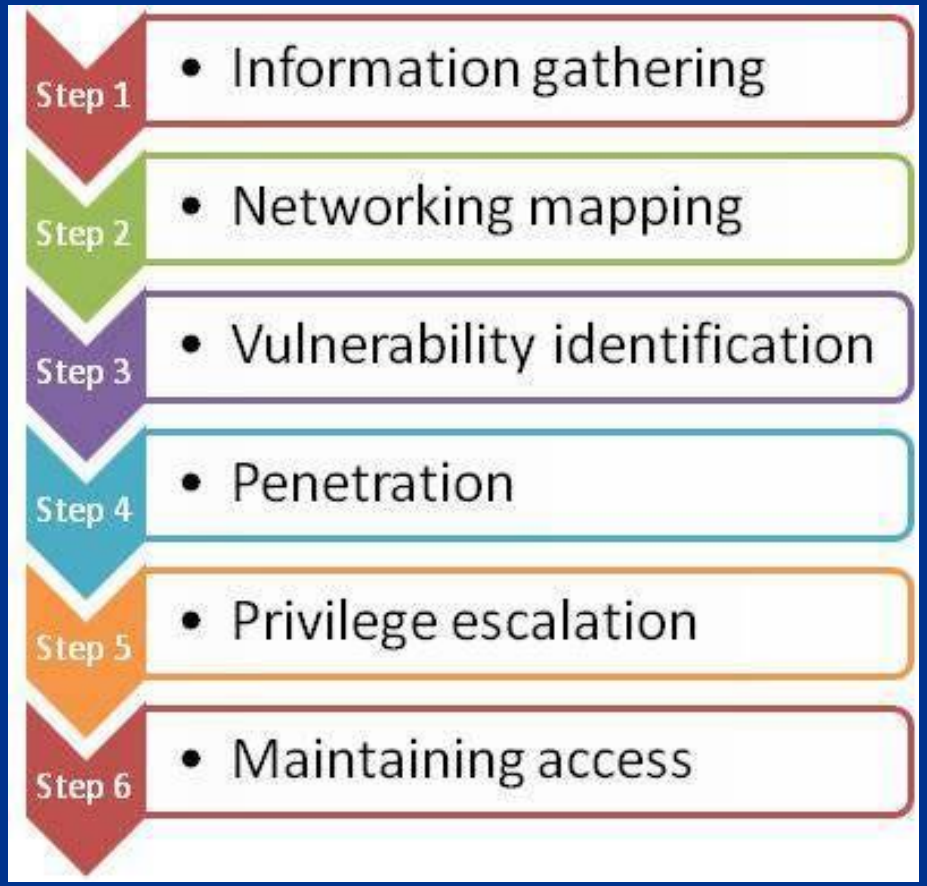
Objective: Simulate real-world ethical hacking techniques, starting with external reconnaissance (OSINT) and moving on to internal scanning, exploiting vulnerabilities, and post-exploitation activities.

Captain Crunch Industries Domain: **captaincrunch.co**

IP Range of Captain Crunch Industries: **10.10.10.0/24, 10.10.30.0/24**

Hands-on Training: You will gain practical skills through supervised, controlled, and authorized activities in a simulated environment.

Disclaimer: *This course is for educational purposes only and is aimed at developing ethical hacking skills within legal and ethical boundaries. Unauthorized activities outside of this course are strictly prohibited.*



15 minute Break

02

Information Gathering

General Information Gathering

The first step includes getting information on the target, the function(s) they perform, how they do things to gain general knowledge on them.

Publicly available information can be widely used to create an impression of the target. Also call open-source intelligence.

Start out by Googling them, finding clues on their website, enumerate search engines for information on them.

Open Source Intelligence (OSINT)

How **OSINT** (**Open-Source Intelligence**) is used in hacking:

1. **General Enumeration**
2. **DNS Enumeration**
3. **Network Mapping and Discovery**
4. **Social Engineering**
5. **Social Media**

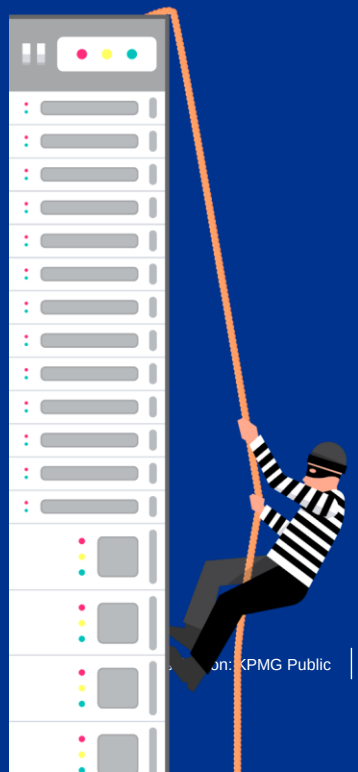
Hacker's Motivation

During the **reconnaissance phase** an attacker tries to gain as much information as possible before launching more serious attacks.

An attacker focuses often on **privileged individuals** and **confidential information/data within the target's network**. Here you can draw parallels with how a thief prepares to steal valuables from his victim's house – he studies when the victim is not home, where are the doors located, what locks are being used, where the valuable items might be stores etc.

Reconnaissance helps the attacker to make **better decisions** in the next cyber attack stages.

- ✓ Username/e-mail format of the target organization?
- ✓ Information about specific users to be used in phishing?
- ✓ Hardware or software used in the organization?



DNS Enumeration

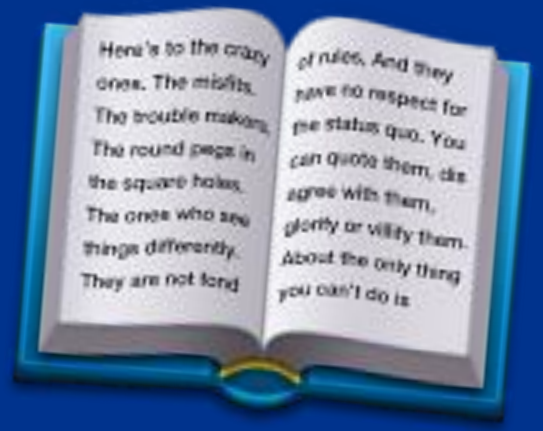
- OSINT can be used to discover the target's domain names, subdomains, and IP addresses, as well as mail servers and other DNS records.
- This information can be used to map out the target's infrastructure, identify potential targets for attacks, and gather email addresses or other contact information for social engineering or spear-phishing attacks.

We have target’s domain: What information can we find with that?

DNS Record Types

There are different DNS records:

- ✓ **NS**: Nameserver record
- ✓ **A**: Address record for IPv4
- ✓ **AAAA**: Address record for IPv6
- ✓ **HINFO**: Host information
- ✓ **MX**: Mail Exchange
- ✓ **TXT**: Text record
- ✓ **CNAME**: Canonical Name
- ✓ **RP**: Responsible person
- ✓ **SRV**: Service location
- ✓ **SOA**: Start of Authority
- ✓ **PTR**: Pointer for inverse lookups



Network Mapping and Discovery

- OSINT can be used to identify IP addresses and network ranges associated with a target, as well as discover open ports, services, and operating systems running on those systems.
- This information can be used to build a map of the target network, identify potential attack vectors, and plan more targeted attacks.

Social Engineering

- OSINT can be used to gather personal information about the target, such as name, phone number, email address, job title, and interests, which can be used to craft targeted social engineering attacks.
- Social engineering attacks may involve techniques like phishing, pretexting, baiting, or tailgating, and can be used to gain access to sensitive information or systems.

Social Media

- OSINT can be used to gather information about the target's social media presence, including profiles, posts, and interactions with others.
- This information can be used to identify weaknesses or vulnerabilities to exploit, such as posting sensitive information, oversharing personal details, or using weak passwords.
- It can also be used to build a profile of the target's interests and behaviors, which can inform social engineering attacks or be used to craft more convincing phishing messages.

Techniques and Tools for Information Gathering

Google Hacking (often referred to as **Google Dorking**) – is a technique, which uses Google Search engine capabilities to find relevant OSINT information on the target.

You can't actually hack sites directly using Google, but as it has tremendous web-crawling capabilities, it can index almost anything within your website, including sensitive information.*

The **Google Hacking Database** (**GHDB**) is a set of Google Hacking search terms which have been found to reveal sensitive data exposed by vulnerable servers and web applications.

https://en.wikipedia.org/wiki/Google_hacking

https://www.exploit-db.com/google-hacking-database

Techniques and Tools for Information Gathering

whois – is a TCP-based transaction-oriented query/response protocol that is used for querying databases that store the registered users or assignees of an Internet resource (domain name, IP address block). It is also used for a wider range of other information.

https://whois.icann.org/en/technical-overview

whois (command) – with the **whois** lookup command you can get the details about both the ownership of domains and the owners.

EXAMPLE COMMAND(S)

$ whois delfi.ee

$ whois 185.20.100.194

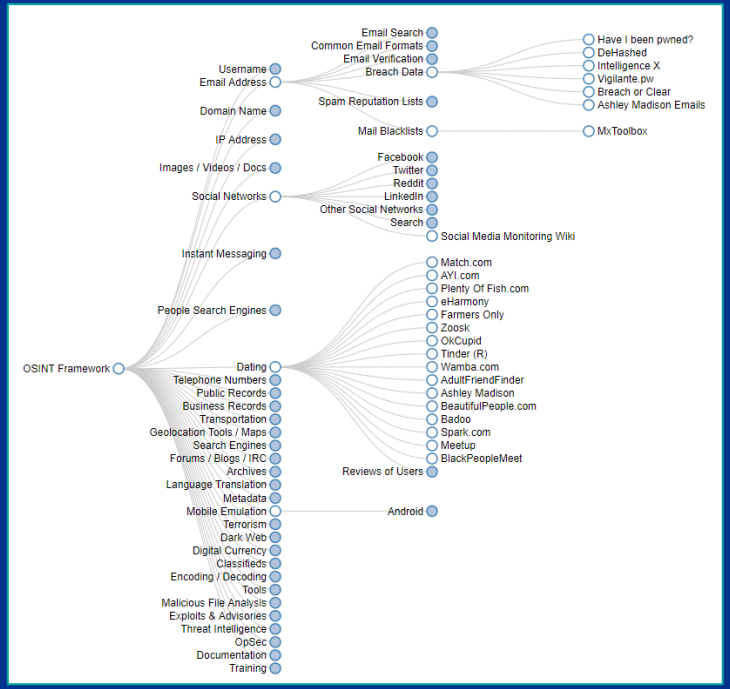
```
kali@kali:~$ whois delfi.ee
Search results may not be used for commercial, advertising, recompilatio
repackaging, redistribution, reuse, obscuring or other similar activitie

Estonia .ee Top Level Domain WHOIS server

Domain:
name:       delfi.ee
status:     ok (paid and in zone)
registered: 2010-07-04 03:59:01 +03:00
changed:    2019-11-10 00:42:51 +02:00
expire:     2020-11-17
outzone:
delete:

Registrant:
name:       AS EKSPRESS MEEDIA
org id:     10586863
country:    EE
email:      Not Disclosed - Visit www.internet.ee for webbased WHOIS
changed:    2019-11-10 00:42:51 +02:00

Administrative contact:
name:       Not Disclosed - Visit www.internet.ee for webbased WHOIS
email:      Not Disclosed - Visit www.internet.ee for webbased WHOIS
changed:    Not Disclosed - Visit www.internet.ee for webbased WHOIS

Technical contact:
name:       Not Disclosed - Visit www.internet.ee for webbased WHOIS
email:      Not Disclosed - Visit www.internet.ee for webbased WHOIS
changed:    Not Disclosed - Visit www.internet.ee for webbased WHOIS

Registrar:
name:       Telia Eesti AS
url:        http://www.telia.ee
phone:      +372 655 9188
changed:    2019-12-04 13:26:47 +02:00

Name servers:
nserver:    ns-1018.awsdns-63.net
nserver:    ns-1049.awsdns-03.org
nserver:    ns-1864.awsdns-41.co.uk
nserver:    ns2.delfi.ee
nserver:    ns-350.awsdns-43.com
nserver:    ns.delfi.ee
changed:    2018-09-18 12:17:11 +03:00
```

Techniques and Tools for Information Gathering

Social media scraping tools:

- Using tools like **Social-Searcher** or **OSINT Framework** to scrape social media profiles, posts, and interactions for information about the target.
- This can be used to identify potential vulnerabilities, such as weak passwords or oversharing of personal details, or to gain insight into the target's interests and behaviors.

OSINT Framework - https://osintframework.com/



Techniques and Tools for Information Gathering

OSINT frameworks:

- Utilizing OSINT frameworks like **Maltego** or **SpiderFoot** to automate the process of gathering and analyzing information about the target.
- These frameworks can help identify relationships between different pieces of information, build a profile of the target, and highlight potential vulnerabilities or attack vectors.

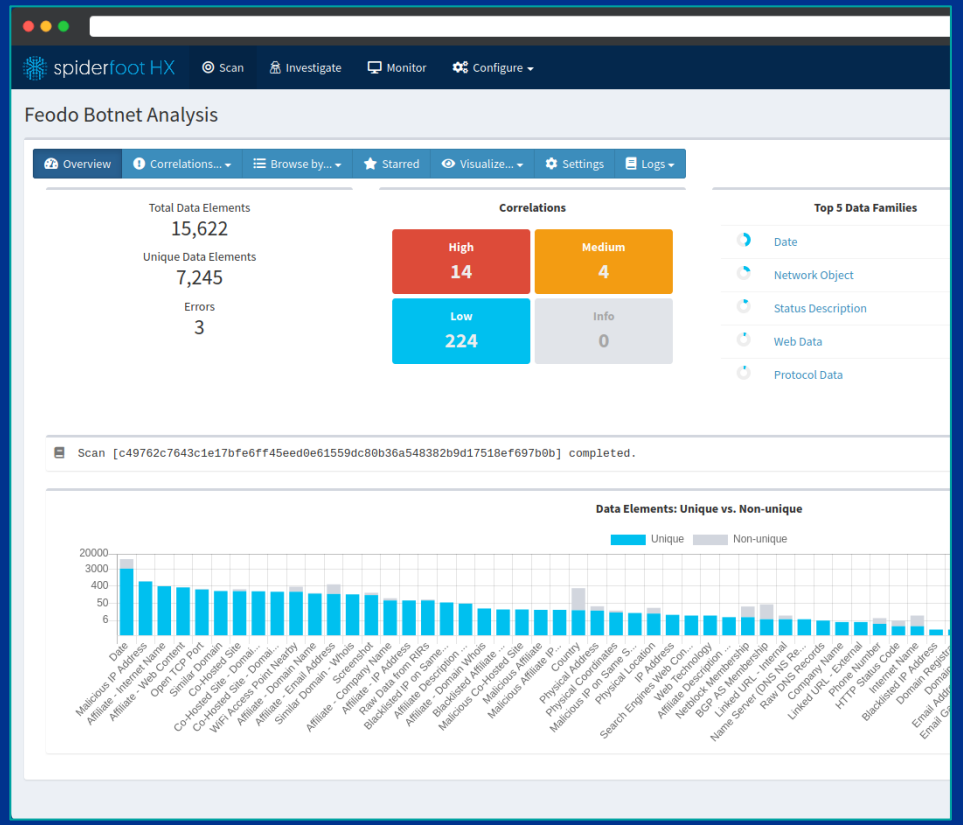
SpiderFoot

SpiderFoot – is a attack surface mapping tool, which scans the entire public Internet, creates real-time threat intelligence streams and creates reports that show the exposure of what is connected to the Internet.

https://www.spiderfoot.net/

Continuously collects and correlates data from internet accessible devices, allowing organizations to see what is their attack surface and what they are exposing to attackers.

- ✓ Ports and Services Exposure
- ✓ Possible Vulnerabilities
- ✓ Accessible Remote Desktops
- ✓ Invalid SSL Certificates
- ✓ Misconfigured Network Shares
- ✓ Databases



Maltego

Maltego – is a open-source intelligence and forensics tool for graphical link analyses that offers real-time data mining and information gathering.

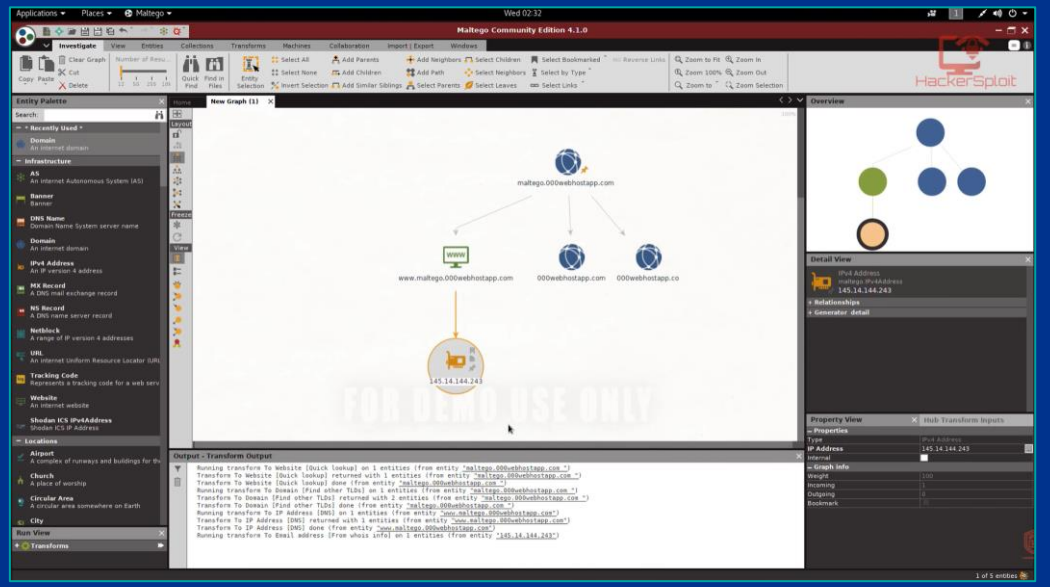
https://www.maltego.com/

Maltego is able to represent the collected information on a node-based graph, making patterns and multiple order connections between said information easily identifiable.*

There are three versions:

- Community (Free)
- Pro (Paid version)
- Enterprise (Paid version)

https://www.maltego.com/pricing-plans/



Course Lab - Information Gathering for Captain Crunch

- **Objective**: Gather external information on Captain Crunch Industries using publicly available sources.
- What open source information can we find for our target?

Lunch Break

03

Scanning and Enumeration

Introduction to Scanning and Enumeration

Scanning and enumeration are crucial stages in the hacking process that involve gathering information about the target system or network in order to identify potential vulnerabilities and attack vectors.

Scanning involves using various tools and techniques to probe the target system or network for open ports, services, and vulnerabilities. Some common scanning techniques include:

- **Ping Sweep**: Used to identify active hosts on a network by sending ICMP packets.
- **TCP/UDP Port Scanning**: Used to identify open ports on a target host or network.
- **Service Scanning**: Used to identify running services and their versions on open ports.
- **Vulnerability Scanning**: Used to identify known vulnerabilities and security weaknesses in the target system or network.

However, it's important to use these tools responsibly and only on systems and networks that you have permission to scan and enumerate. Unethical or unauthorized scanning can lead to serious legal and ethical consequences.

Scanning Steps

Network Sweep	Send probe packets to identify alive hosts on network
Port Scan	Determine open TCP and UDP ports
OS Fingerprinting	Determine target OS type based on network behavior
Version Scan	Determine the version of services and protocols
Vulnerability Scan	Determine a list of potential vulnerabilities

Port Scanning & Banner Grabbing

Port scanning is the process of identifying open ports on a target system or network. This can be useful for identifying potential vulnerabilities and attack vectors.

A port is a communication endpoint on a network device that can be used to send and receive data. There are 65,535 ports available on a typical network device, but only a few of them are commonly used for specific purposes.

Banner grabbing is the process of collecting information about a service or application running on an open port by analyzing its response to network requests.

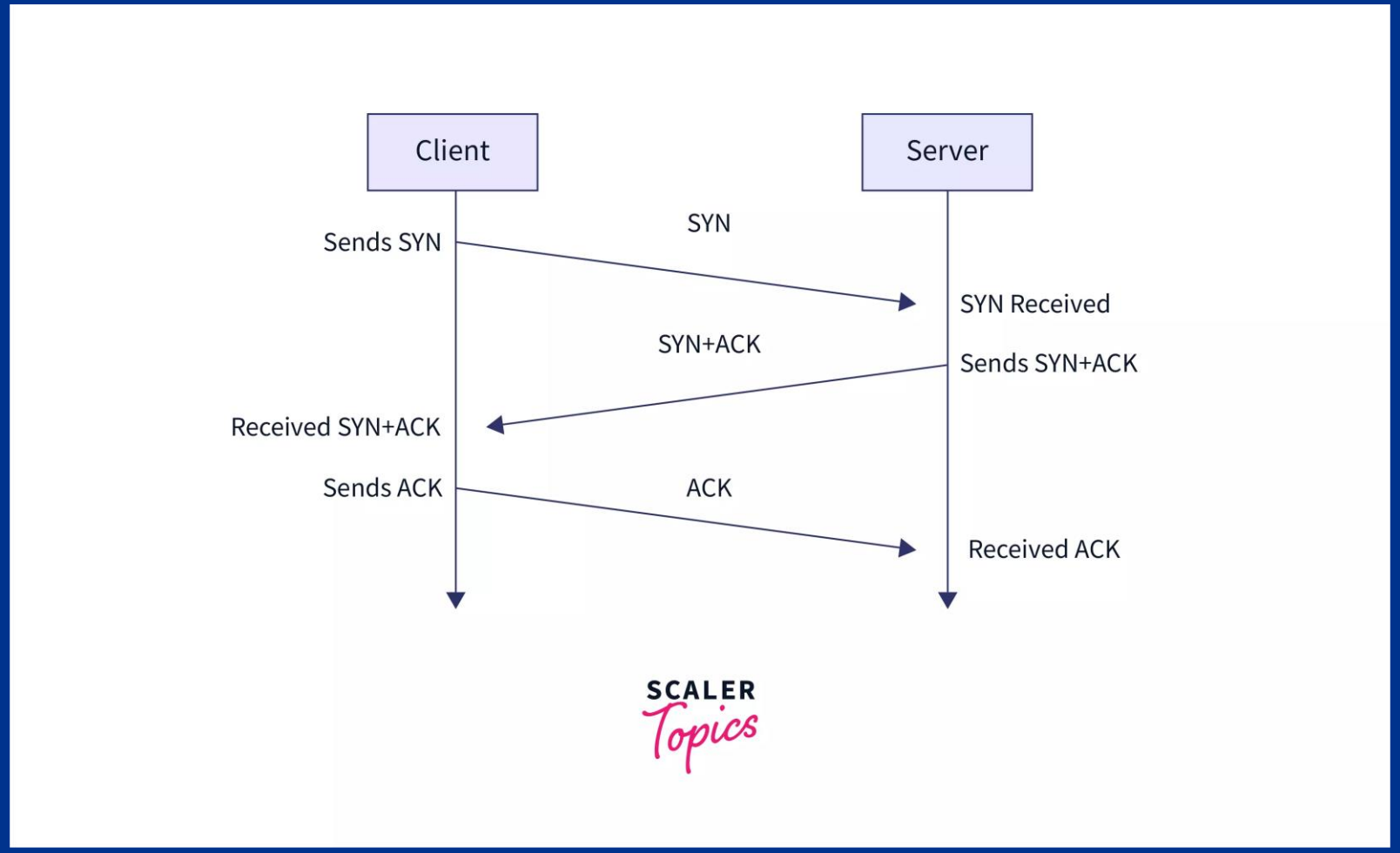
Many services and applications include a banner or header that reveals information about the software version, operating system, or other configuration details.

Port Scanning & Banner Grabbing

Scanning specific services:

- Many services and applications use specific ports to communicate with other devices on a network. Some common services and their associated ports include:
  - **HTTP** (**80**, **8080**): Used for web browsing and hosting web pages.
  - **FTP** (**20**, **21**): Used for file transfers between devices.
  - **SSH** (**22**): Used for secure remote access and control.
  - **Telnet** (**23**): Used for remote access and control, but without encryption.
  - **SMTP** (**25**): Used for sending and receiving email messages.
  - **DNS** (**53**): Used for resolving domain names to IP addresses.
  - **SNMP** (**161**): Used for monitoring and managing network devices.
- Once you identify the specific service and its associated port, you can use port scanning and banner grabbing techniques to gather more information about the service and potentially identify vulnerabilities or weaknesses.

TCP Handshake



Nessus Scanning

- There are two main types of Nessus scanning types:
  - Discovery scanning
  - Assessment scanning

Web Application Scanning

Web applications are a common target for attackers, and it's important to scan them for vulnerabilities and weaknesses to protect them from potential attacks.

Web application scanning involves using specialized tools and techniques to identify vulnerabilities and misconfigurations in web applications, such as SQL injection, cross-site scripting, and insecure file uploads.

Common web application scanning tools include:

- **Burp Suite:** A web application security testing framework that includes a scanner for identifying vulnerabilities and an intercepting proxy for modifying and analyzing web traffic.
- **OWASP ZAP:** An open-source web application scanner that can be used to identify vulnerabilities and security weaknesses.
- **nikto:** A web server scanner that includes a plugin for checking for web application vulnerabilities.

Web application scanning can also involve manual techniques, such as reviewing source code, analyzing server logs, and testing for known vulnerabilities.

Burp Suite

- One of the most utilized tools related to web application testing
- Has multiple features,
  - Most importantly can scan and audit security issues.
  - Provides vulnerability scans

nikto

- Also a vulnerability scanner for web applications

EXAMPLE COMMAND(S)

```
$ nikto –host <hostname> -port <port_number>
```

WPScan

WPScan – is a WordPress vulnerability scanner.

WPScan CLI tool is a free, for non-commercial use, black box WordPress security scanner written for security professionals and blog maintainers to test the security of their sites. https://wpscan.com/wordpress-security-scanner

WordPress is a open-source website builder and a content management system (CMS) written in PHP and paired with a MySQL or MariaDB database.

https://wordpress.com/

Why WPScan?

Why is WPScan important? Here are WordPress statistics:

WordPress powers about 39% of the Internet's webpages. What makes WordPress sites insecure is if site owners don't install relevant security patches, and if they install plugins or themes that are themselves insecure. The same can be said of other content management systems (CMAs) like Drupal. Both WordPress and Drupal are used by government agencies.

	% All Websites
WordPress	38
Joomla	2.6
Drupal	1.7
Squarespace	1.5
Wix	1.3

Here are some examples of the US embassy websites running on WordPress:

- United Kingdom: uk.usembassy.gov.
- Mexico: mx.usembassy.gov.
- France: fr.usembassy.gov.
- Germany: de.usembassy.gov.
- Australia: au.usembassy.gov.
- Japan: jp.usembassy.gov.
- China: cn.usembassy.gov.

nmap and Other Scanning Tools

- Scanning and enumeration are crucial steps in the hacking process, as they allow you to identify potential attack vectors and vulnerabilities on a target network.
- **nmap** is a popular tool for network scanning and host discovery. It can be used to scan for open ports and services, detect operating systems, and even perform vulnerability scanning.
- Other scanning and enumeration tools include:
  - **netcat**: A versatile network tool that can be used for port scanning, banner grabbing, and more.
  - **enum4linux**: A tool for enumerating SMB shares and domains, as well as NetBIOS and LDAP information.
  - **snmp-check**: A tool for enumerating information from SNMP-enabled devices, such as routers and switches.
  - **nikto**: A web server scanner that can identify potential vulnerabilities and misconfigurations.
- It's important to use these tools responsibly and with permission, and to follow best practices for minimizing disruptions and protecting yourself.
- By using these tools effectively, you can gather valuable information about a target network and identify potential attack vectors and vulnerabilities that can be exploited to gain unauthorized access or cause disruption.

nmap

Target Specification

Switch	Example	Description
	nmap 192.168.1.1	Scan a single IP
	nmap 192.168.1.1 192.168.2.1	Scan specific IPs
	nmap 192.168.1.1-254	Scan a range
	nmap scanme.nmap.org	Scan a domain
	nmap 192.168.1.0/24	Scan using CIDR notation
-iL	nmap -iL targets.txt	Scan targets from a file
-iR	nmap -iR 100	Scan 100 random hosts
--exclude	nmap --exclude 192.168.1.1	Exclude listed hosts

Scan Techniques

Switch	Example	Description
-sS	nmap 192.168.1.1 -sS	TCP SYN port scan (Default)
-sT	nmap 192.168.1.1 -sT	TCP connect port scan (Default without root privilege)
-sU	nmap 192.168.1.1 -sU	UDP port scan
-sA	nmap 192.168.1.1 -sA	TCP ACK port scan
-sW	nmap 192.168.1.1 -sW	TCP Window port scan
-sM	nmap 192.168.1.1 -sM	TCP Maimon port scan

Host Discovery

Switch	Example	Description
-sL	nmap 192.168.1.1-3 -sL	No Scan. List targets only
-sn	nmap 192.168.1.1/24 -sn	Disable port scanning
-Pn	nmap 192.168.1.1-5 -Pn	Disable host discovery
-PS	nmap 192.168.1.1-5 -PS22-25,80	TCP SYN discovery on port x. Port 80 by default
-PA	nmap 192.168.1.1-5 -PA22-25,80	TCP ACK discovery on port x. Port 80 by default
-PU	nmap 192.168.1.1-5 -PU53	UDP discovery on port x. Port 40125 by default
-PR	nmap 192.168.1.1-1/24 -PR	ARP discovery on local network
-n	nmap 192.168.1.1 -n	Never do DNS resolution

Port Specification

Switch	Example	Description
-p	nmap 192.168.1.1 -p 21	Port scan for port x
-p	nmap 192.168.1.1 -p 21-100	Port range
-p	nmap 192.168.1.1 -p U:53,T:21-25,80	Port scan multiple TCP and UDP ports
-p-	nmap 192.168.1.1 -p-	Port scan all ports
-p	nmap 192.168.1.1 -p http,https	Port scan from service name
-F	nmap 192.168.1.1 -F	Fast port scan (100 ports)
--top-ports	nmap 192.168.1.1 --top-ports 2000	Port scan the top x ports
-p-65535	nmap 192.168.1.1 -p-65535	Leaving off initial port in range makes the scan start at port 1
-p0-	nmap 192.168.1.1 -p0-	Leaving off end port in range makes the scan go through to port 65535

www.stationx.net/nmap-cheat-sheet/

nmap Scripting Engine (NSE)

nmap is more than a port scanner.

It can also be used to scan for vulnerabilities:

```
root@kali:~# nmap --script  vuln -p139,445 192.168.0.18
Starting Nmap 7.70 ( https://nmap.org ) at 2019-04-25 20:58 CDT
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for 192.168.0.18
Host is up (0.0017s latency).

PORT    STATE SERVICE
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143

Nmap done: 1 IP address (1 host up) scanned in 39.49 seconds
root@kali:~#
```

15 minute Break

04

Vulnerability Assessments

Introduction to Vulnerability Scanning and Analysis

The next step in hacking is to analyze the results of the scans to identify vulnerabilities that could be exploited by attackers.

Allows for the identification of specific vulnerabilities that can be leveraged for unauthorized access or exploitation.

Vulnerabilities are typically prioritized based on severity, potential impact, and exploitability to determine their relative risk and prioritize them for remediation.

Once vulnerabilities are identified and prioritized, they can be exploited using appropriate techniques to gain unauthorized access, escalate privileges, or perform other malicious activities.

Vulnerability analysis and assessment also play a critical role in proactive defense, as they allow organizations to identify and remediate vulnerabilities before they are exploited by malicious actors.

Introduction to Vulnerability Scanning and Analysis

Scanning with tools like **nmap**, **nikto**, etc. is the first step in identifying potential vulnerabilities, and vulnerability analysis and assessment are the subsequent steps in leveraging those vulnerabilities for offensive security purposes

Vulnerability Assessment Tools

Open Source (available on your Kali VMs and course cheatsheets):

1. **Nikto** – Web applications
2. **Nmap** (Scripting Engine) – Networks
3. **Burp Suite** – Web applications

Enterprise-grade solutions:

1. **Qualys**
2. **Tenable.io**
3. **Rapid7 InsightVM**
4. **Nessus Professional**

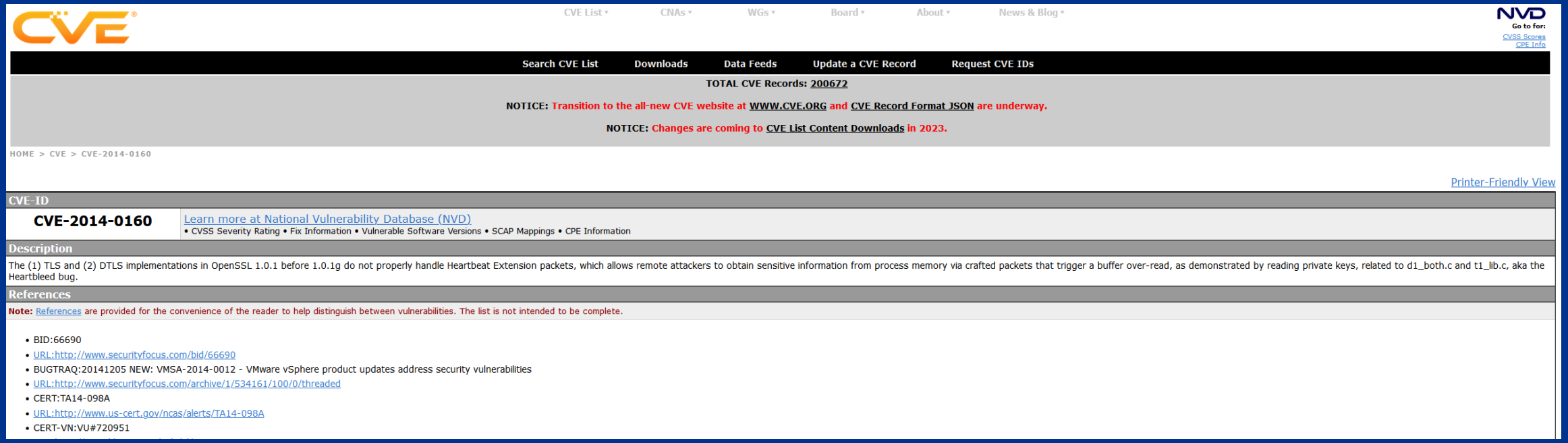
Vulnerability Scoring Systems

- **Common Vulnerabilities and Exposures** (**CVE**): A standardized list of common vulnerabilities and exposures maintained by the MITRE Corporation. Each vulnerability is assigned a unique identifier (**CVE ID**) to facilitate communication and tracking of vulnerabilities across different systems and organizations.

- **Common Vulnerability Scoring System** (**CVSS**): A framework for assessing the severity and impact of vulnerabilities, developed by the Forum of Incident Response and Security Teams (**FIRST**). CVSS provides a numeric score (ranging from 0 to 10) to quantify the severity of a vulnerability based on its characteristics such as exploitability, impact, and complexity.

- **Common Weakness Enumeration** (**CWE**): A community-developed list of software weaknesses and vulnerabilities maintained by the MITRE Corporation. CWE provides a standardized taxonomy for identifying and categorizing common software vulnerabilities, making it easier to understand and address software weaknesses.

CVE (MITRE)



CVE List ▾ CNAs ▾ WGs ▾ Board ▾ About ▾ News & Blog ▾

NVD
Go to for:
CVSS Scores
CPE Info

Search CVE List | Downloads | Data Feeds | Update a CVE Record | Request CVE IDs

TOTAL CVE Records: 200672

NOTICE: Transition to the all-new CVE website at WWW.CVE.ORG and CVE Record Format JSON are underway.

NOTICE: Changes are coming to CVE List Content Downloads in 2023.

HOME > CVE > CVE-2014-0160

Printer-Friendly View

CVE-ID

CVE-2014-0160

Learn more at National Vulnerability Database (NVD)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

The (1) TLS and (2) DTLS implementations in OpenSSL 1.0.1 before 1.0.1g do not properly handle Heartbeat Extension packets, which allows remote attackers to obtain sensitive information from process memory via crafted packets that trigger a buffer over-read, as demonstrated by reading private keys, related to d1_both.c and t1_lib.c, aka the Heartbleed bug.

References

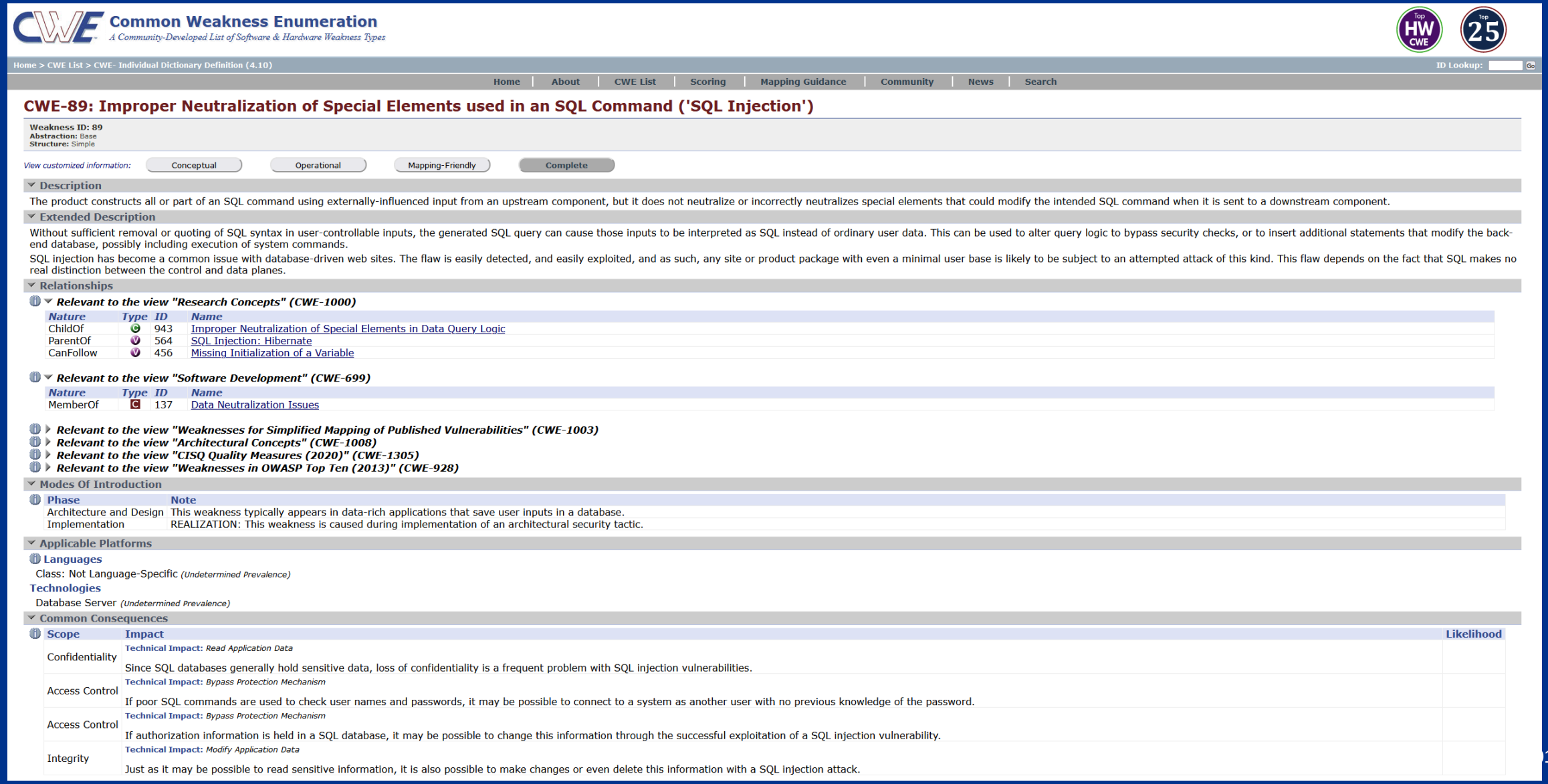
Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- BID:66690
- URL:http://www.securityfocus.com/bid/66690
- BUGTRAQ:20141205 NEW: VMSA-2014-0012 - VMware vSphere product updates address security vulnerabilities
- URL:http://www.securityfocus.com/archive/1/534161/100/0/threaded
- CERT:TA14-098A
- URL:http://www.us-cert.gov/ncas/alerts/TA14-098A
- CERT-VN:VU#720951

CVSS

Let’s have a look

CWE (MITRE… Again)



Common Weakness Enumeration
A Community-Developed List of Software & Hardware Weakness Types

Home > CWE List > CWE- Individual Dictionary Definition (4.10) ID Lookup: Go

Home | About | CWE List | Scoring | Mapping Guidance | Community | News | Search

CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Weakness ID: 89
Abstraction: Base
Structure: Simple

View customized information: Conceptual | Operational | Mapping-Friendly | Complete

Description

The product constructs all or part of an SQL command using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the intended SQL command when it is sent to a downstream component.

Extended Description

Without sufficient removal or quoting of SQL syntax in user-controllable inputs, the generated SQL query can cause those inputs to be interpreted as SQL instead of ordinary user data. This can be used to alter query logic to bypass security checks, or to insert additional statements that modify the back-end database, possibly including execution of system commands.

SQL injection has become a common issue with database-driven web sites. The flaw is easily detected, and easily exploited, and as such, any site or product package with even a minimal user base is likely to be subject to an attempted attack of this kind. This flaw depends on the fact that SQL makes no real distinction between the control and data planes.

Relationships

Relevant to the view "Research Concepts" (CWE-1000)

Nature	Type	ID	Name
ChildOf	C	943	Improper Neutralization of Special Elements in Data Query Logic
ParentOf	V	564	SQL Injection: Hibernate
CanFollow	V	456	Missing Initialization of a Variable

Relevant to the view "Software Development" (CWE-699)

Nature	Type	ID	Name
MemberOf	C	137	Data Neutralization Issues

Relevant to the view "Weaknesses for Simplified Mapping of Published Vulnerabilities" (CWE-1003)
Relevant to the view "Architectural Concepts" (CWE-1008)
Relevant to the view "CISQ Quality Measures (2020)" (CWE-1305)
Relevant to the view "Weaknesses in OWASP Top Ten (2013)" (CWE-928)

Modes Of Introduction

Phase	Note
Architecture and Design	This weakness typically appears in data-rich applications that save user inputs in a database.
Implementation	REALIZATION: This weakness is caused during implementation of an architectural security tactic.

Applicable Platforms

Languages
Class: Not Language-Specific *(Undetermined Prevalence)*

Technologies
Database Server *(Undetermined Prevalence)*

Common Consequences

Scope	Impact	Likelihood
Confidentiality	**Technical Impact:** *Read Application Data* Since SQL databases generally hold sensitive data, loss of confidentiality is a frequent problem with SQL injection vulnerabilities.	
Access Control	**Technical Impact:** *Bypass Protection Mechanism* If poor SQL commands are used to check user names and passwords, it may be possible to connect to a system as another user with no previous knowledge of the password.	
Access Control	**Technical Impact:** *Bypass Protection Mechanism* If authorization information is held in a SQL database, it may be possible to change this information through the successful exploitation of a SQL injection vulnerability.	
Integrity	**Technical Impact:** *Modify Application Data* Just as it may be possible to read sensitive information, it is also possible to make changes or even delete this information with a SQL injection attack.	

Vulnerability Assessment Lab

KPMG

Hacker Fundamentals

Day 2

Presented by: Yusef Ward, Jagjit Singh

—

Date: 11.05.2023

Recap of Day 1

- Information Gathering
- Scanning and Enumeration
- Vulnerability Assessments

05

Exploitation

Exploitation Essentials

Needs proper target enumeration first

Exploits written for specific versions

Can be found on web and also written manually

Requires advanced understanding of tools and exploit code

Exploitation Techniques

After conducting vulnerability scans using tools like **nmap**, **nikto**, etc., identified vulnerabilities can be exploited to gain unauthorized access or execute malicious code on the target system.

Below is a list of exploitation techniques:

1. **Exploit Databases**: Leveraging publicly available exploit databases and repositories, such as Exploit-DB, Metasploit Framework, GitHub, etc., to find and utilize existing exploits for known vulnerabilities.
2. **Metasploit-like Frameworks**: Using comprehensive exploitation frameworks like Metasploit, Cobalt Strike, and other similar tools that provide a wide range of pre-built exploits and modules for various vulnerabilities and attack vectors.
3. **Writing Custom Exploits**: Developing custom exploits or modifying existing ones to target specific vulnerabilities that may not have publicly available exploits, tailored to the target system or application.
4. **Zero-day Exploits**: Exploiting previously unknown vulnerabilities, also known as zero-day exploits, which are not yet patched by vendors and may provide a significant advantage to attackers.

Exploit Database (ExploitDB)

Public exploit databases like **exploitdb.com** can be a valuable resource for penetration testers, security researchers, and ethical hackers like the following:

- Publicly available repositories of exploits and vulnerabilities
- Contain a large collection of exploits for known vulnerabilities
- Provide a searchable database of exploits for various platforms and applications
- Can be used to find and download pre-built exploits for testing and validation
- Often include details such as exploit code, vulnerability information, and references
- Require careful usage and adherence to legal and ethical guidelines
- Regularly updated with new exploits and vulnerabilities
- Should be used responsibly and legally, with proper authorization and permission from the target systems or applications

Introduction to the Metasploit Framework

Metasploit is a powerful, user-friendly exploitation framework with pre-built exploits, customization options, and extensive documentation for responsible and ethical use in security testing.

- Comprehensive exploitation framework with a wide range of pre-built exploits and modules
- Provides a user-friendly interface for managing and executing exploits
- Supports a variety of platforms and applications for targeted exploitation
- Allows for customization and modification of existing exploits or creation of custom exploits
- Offers features for payload generation, post-exploitation, and pivoting
- Includes extensive documentation and community support for learning and troubleshooting
- Can be used for both manual exploitation and automated exploitation using auxiliary modules
- Requires proper authorization and adherence to ethical and legal guidelines for responsible use

Metasploit

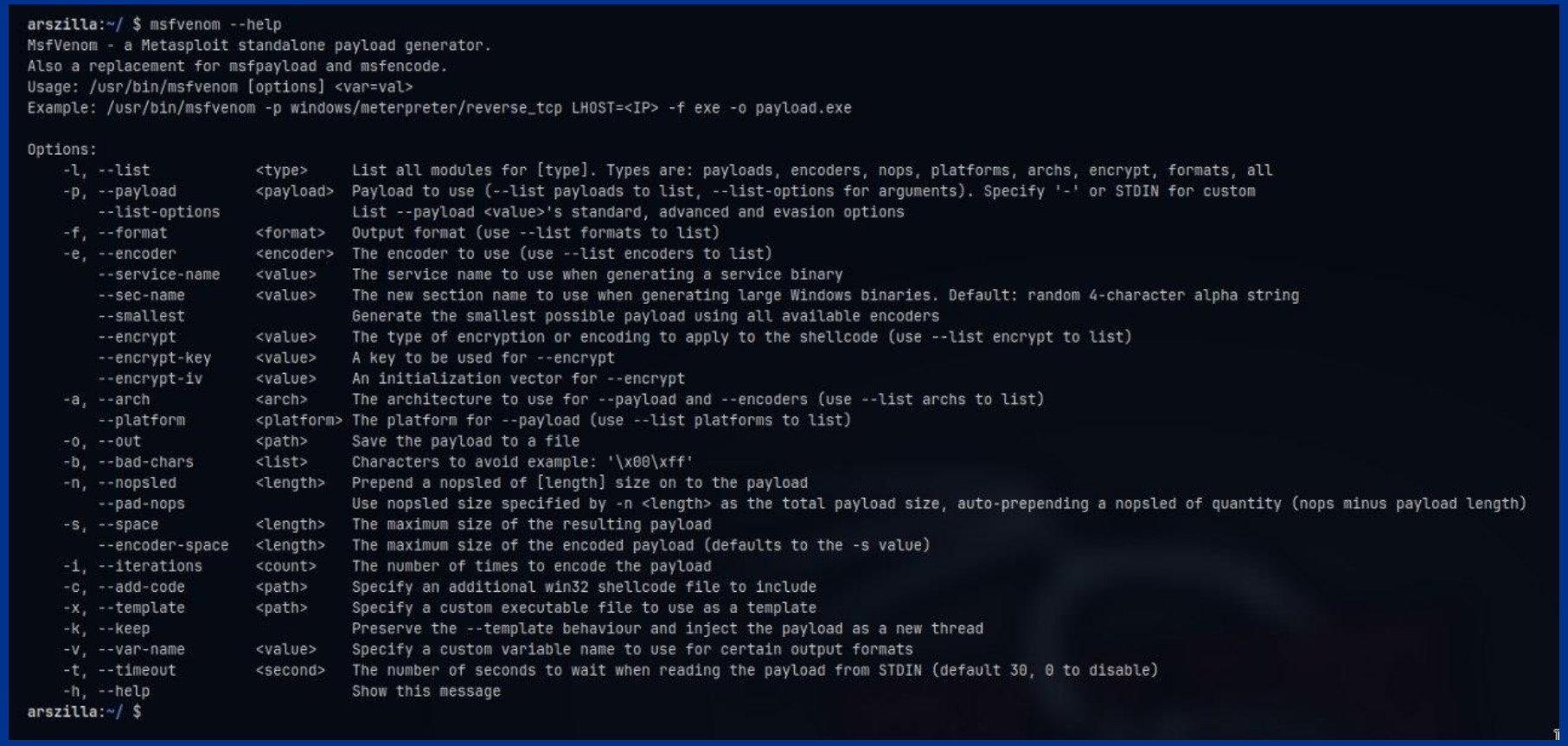
Metasploit is split into 3 different parts:

- **Exploit** – Takes advantage of a vulnerability.
- **Payload** – Makes the target do something the attacker wants.
- **Post** – Used in post-exploitation.

msfvenom

msfvenom is a “component” of Metasploit, generating payloads (i.e. shells). The generated can be connected to Metasploit or other tools and software, such as (but not limited to):

- netcat
- Cobalt Strike
- PowerShell Empire



15 minute Break

Exploiting Vulnerable Systems Lab

Lunch Break

06

Post Exploitation

What is the objective of Post Exploitation?

- Move laterally
- Escalate privileges
- Steal or access sensitive data
- Download and execute ransomware
- Erase data
- Code execution
- Cover tracks

Command and control frameworks like Meterpreter, Cobalt Strike, Empire, and others are vastly used for post-exploitation activities. It’s one of their main benefits.

Command and Control (C&C)

Command and Control (C2) frameworks are powerful tools used by attackers in post-exploitation to maintain stealthy, persistent control over compromised systems.

C2 frameworks allow attackers to remotely manage compromised systems, exfiltrate data, pivot to other systems, and launch further attacks. Additionally, they allow an attacker to manage their backdoors, rootkits, and other post-exploitation tools on compromised systems.

Popular C2 frameworks are (but not limited to):

- Cobalt Strike
- Powershell-Empire
- Metasploit

C2 frameworks provide a wide range of capabilities for post-exploitation activities and can used to establish covert communication channels, blend in with legitimate traffic, and evade detection by security controls.

Understanding the capabilities and usage of C2 frameworks is essential for both offensive security (penetration testing) and defensive security (incident response) perspectives.

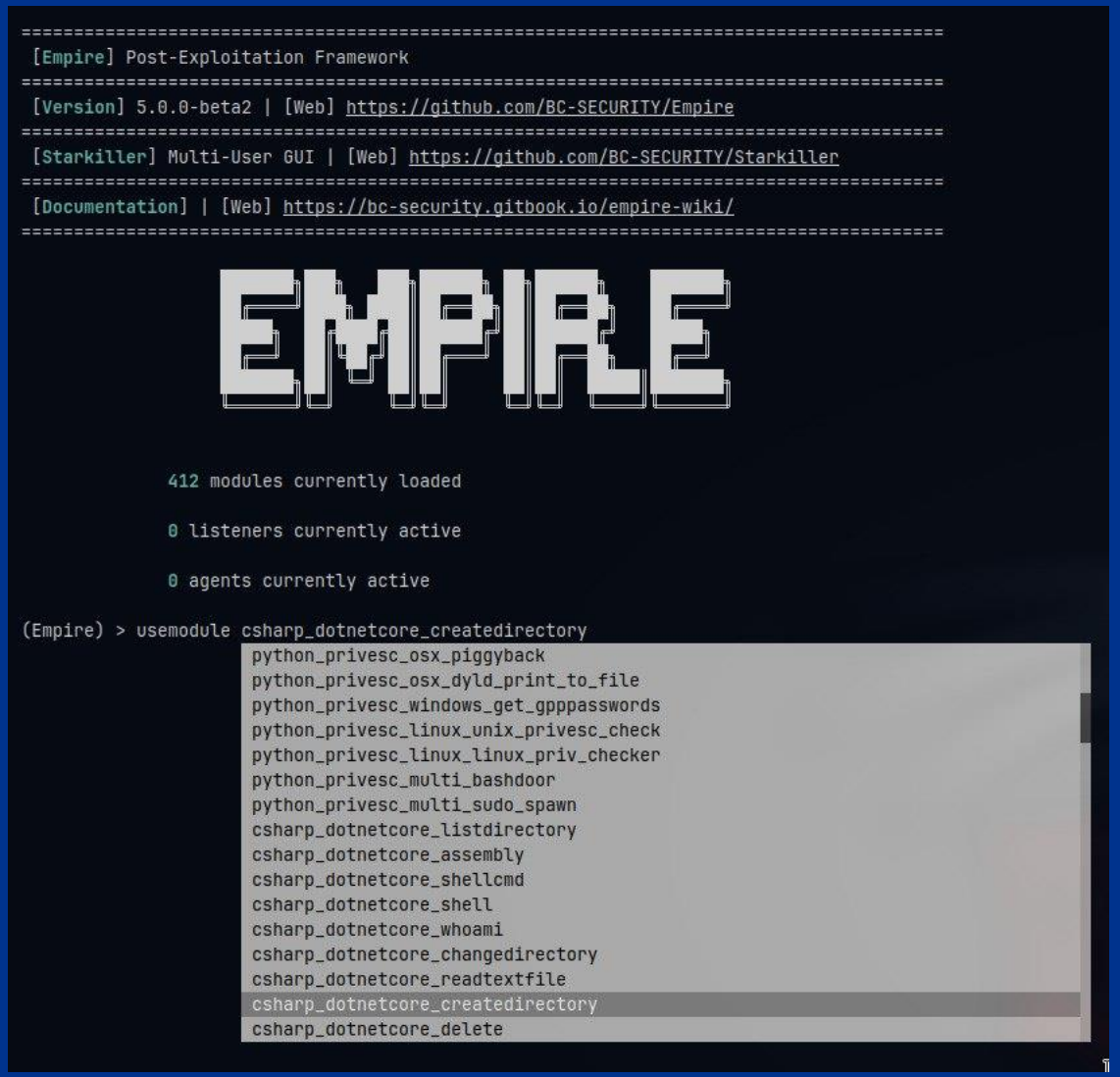
https://www.thec2matrix.com/

PowerShell Empire

PowerShell-Empire is a post-exploitation framework, just like **Metasploit**. However, while Metasploit can be used for exploitation, PowerShell-Empire is specifically for post-exploitation. However, unlike Metasploit, it's more or so similar to Cobalt Strike, where it's meant to be a collaborative post-exploitation framework.

While it's intended use case is over the terminal (CLI), it has a GUI client (**starkiller**).

https://github.com/BC-SECURITY/Empire



Privilege Escalation

After a successful exploitation, gaining elevated privileges is the next step for further access. This is achieved by performing privilege escalation, whether by exploiting a vulnerable service, kernel, etc. These techniques vary depending on the target system, operating system, and application configurations.

The most common privilege escalation techniques include (but not limited to):

- Exploiting misconfigurations,
- Weak permissions,
- Unpatched vulnerabilities.

Privilege escalation is a fundamental concept in cybersecurity and an important skill for penetration testers and ethical hackers.

Privilege Escalation

- **Collect**: Enumeration, more enumeration and some more enumeration.
- **Process**: Sort through data, analyze and prioritization.
- **Search**: Know what to search for and where to find the exploit code.
- **Adapt**: Customize the exploit, so it fits. Not every exploit work for every system "out of the box".
- **Try:** Get ready for (lots of) trial and error.

Privilege Escalation tools

Privilege escalation is often OS centric –

Some popular Linux tools for privilege escalation are:

- Linpeas
- Linenum
- BeRoot

https://book.hacktricks.xyz/linux-hardening/linux-privilege-escalation-checklist

Some popular Windows tools for privilege escalation are:

- Winpeas
- SharpUp
- SeatBelt
- PowerUp

https://book.hacktricks.xyz/windows-hardening/checklist-windows-privilege-escalation

Linenum output example

```
#########################################################
-e # Local Linux Enumeration & Privilege Escalation Script #
-e #########################################################
-e # www.rebootuser.com
-e # version 0.982

[-] Debug Info
-e [+] Thorough tests = Disabled
-e

-e Scan started at:
Sun May 28 14:35:52 UTC 2023
-e

-e ### SYSTEM ##############################################
-e [-] Kernel information:
Linux studenthub 5.19.0-23-generic #24-Ubuntu SMP PREEMPT_DYNAMIC Fri Oct 14 15:39:57 UTC 2022 x86_64 x86_64 x86_64 GNU/Linux
-e

-e [-] Kernel information (continued):
Linux version 5.19.0-23-generic (buildd@lcy02-amd64-076) (x86_64-linux-gnu-gcc-12 (Ubuntu 12.2.0-3ubuntu1) 12.2.0, GNU ld (GNU Binutils for Ubuntu) 2.39) #24
-Ubuntu SMP PREEMPT_DYNAMIC Fri Oct 14 15:39:57 UTC 2022
-e

-e [-] Specific release information:
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=22.10
DISTRIB_CODENAME=kinetic
DISTRIB_DESCRIPTION="Ubuntu 22.10"
PRETTY_NAME="Ubuntu 22.10"
NAME="Ubuntu"
VERSION_ID="22.10"
VERSION="22.10 (Kinetic Kudu)"
VERSION_CODENAME=kinetic
ID=ubuntu
ID_LIKE=debian
HOME_URL="https://www.ubuntu.com/"
SUPPORT_URL="https://help.ubuntu.com/"
BUG_REPORT_URL="https://bugs.launchpad.net/ubuntu/"
```

PowerUp

```
ServiceName                     : lpasvc
Path                            : "C:\Program Files\Microsoft Policy Platform\policyHost.exe" /serv
                                  ice
ModifiableFile                  : C:\
ModifiableFilePermissions       : {Delete, GenericWrite, GenericExecute, GenericRead}
ModifiableFileIdentityReference : NT AUTHORITY\Authenticated Users
StartName                       : LocalSystem
AbuseFunction                   : Install-ServiceBinary -Name 'lpasvc'
CanRestart                      : False
Name                            : lpasvc
Check                           : Modifiable Service Files
```

crackmapexec

- CME is a great tool for Active Directory related post-exploitation attacks

EXAMPLE COMMAND(S)

```
$ crackmapexec smb <IP> -u users.txt –p passwords.txt
```

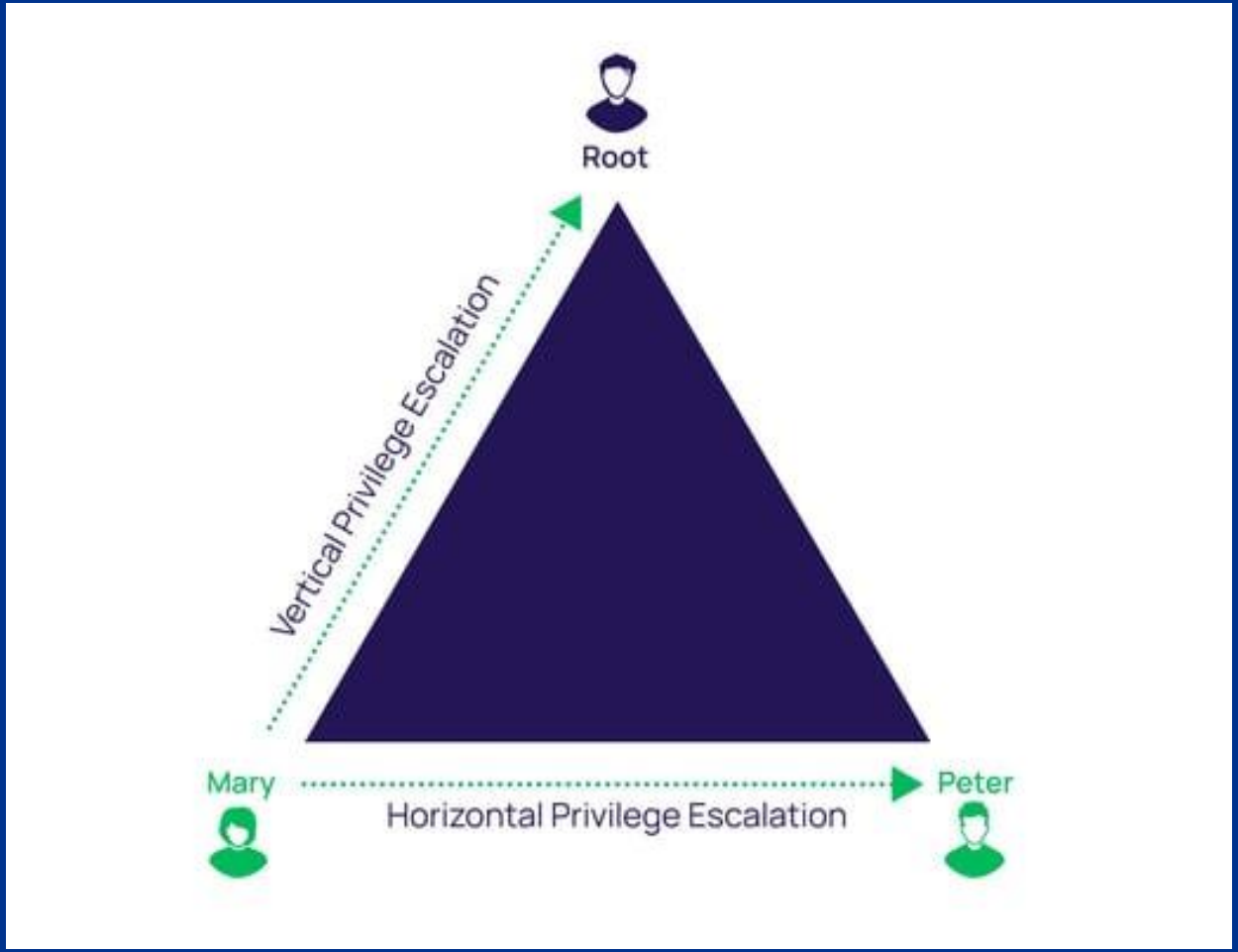
Sniffing hashes with crackmapexec

```
┌──(mpgn㉿kali)-[~/CrackMapExec]
└─$ poetry run crackmapexec ldap poudlard.wizard -u tom -p October2021 -M laps
SMB         192.168.133.148 445    poudlard.wizard  [*] Windows 10.0 Build 17763 x64 (name:DC01) (domain:poudlard.wizard) (signing:True) (SMBv1:
LDAP        192.168.133.148 389    poudlard.wizard  [+] poudlard.wizard\tom:October2021
LAPS        192.168.133.148 389    DC01             [*] Getting LAPS Passwords
LAPS        192.168.133.148 389    DC01             Computer: DC01$              Password: DN/9[pl65HNO9@
LAPS        192.168.133.148 389    DC01             Computer: ADCS$              Password: A3)[qo4CS6#I$t
LAPS        192.168.133.148 389    DC01             Computer: SQL01$             Password: k9nzH@cBcFBv!-

┌──(mpgn㉿kali)-[~/CrackMapExec]
└─$ poetry run crackmapexec smb /tmp/hosts -u tom -p October2021 --laps
SMB         192.168.133.138 445    192.168.133.138  [*] Windows 10.0 Build 17763 x64 (name:ADCS) (domain:poudlard.wizard) (signing:False) (SMBv1
SMB         192.168.133.167 445    192.168.133.167  [*] Windows Server 2016 Datacenter Evaluation 14393 x64 (name:SQL01) (domain:poudlard.wizard
SMB         192.168.133.138 445    192.168.133.138  [+] ADCS\administrator:A3)[qo4CS6#I$t (Pwn3d!)
SMB         192.168.133.167 445    192.168.133.167  [+] SQL01\administrator:k9nzH@cBcFBv!- (Pwn3d!)

┌──(mpgn㉿kali)-[~/CrackMapExec]
└─$ poetry run crackmapexec smb /tmp/hosts -u tom -p October2021 --laps --sam
SMB         192.168.133.167 445    192.168.133.167  [*] Windows Server 2016 Datacenter Evaluation 14393 x64 (name:SQL01) (domain:poudlard.wizard
SMB         192.168.133.138 445    192.168.133.138  [*] Windows 10.0 Build 17763 x64 (name:ADCS) (domain:poudlard.wizard) (signing:False) (SMBv1
SMB         192.168.133.167 445    192.168.133.167  [+] SQL01\administrator:k9nzH@cBcFBv!- (Pwn3d!)
SMB         192.168.133.138 445    192.168.133.138  [+] ADCS\administrator:A3)[qo4CS6#I$t (Pwn3d!)
SMB         192.168.133.167 445    192.168.133.167  [+] Dumping SAM hashes
SMB         192.168.133.167 445    192.168.133.167  Administrator:500:aad3b435b51404eeaad3b435b51404ee:4590d90c80f5cdb8cbcfc3e937b4aa84:::
SMB         192.168.133.167 445    192.168.133.167  Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB         192.168.133.167 445    192.168.133.167  DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB         192.168.133.167 445    192.168.133.167  [+] Added 3 SAM hashes to the database
SMB         192.168.133.138 445    192.168.133.138  [+] Dumping SAM hashes
SMB         192.168.133.138 445    192.168.133.138  Administrator:500:aad3b435b51404eeaad3b435b51404ee:24cf58cd48500170a0e3e244571b531c:::
SMB         192.168.133.138 445    192.168.133.138  Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB         192.168.133.138 445    192.168.133.138  DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB         192.168.133.138 445    192.168.133.138  WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:cddc831ea5e7359b8c5fe18d9d2318ca:::
SMB         192.168.133.138 445    192.168.133.138  toto:1000:aad3b435b51404eeaad3b435b51404ee:999e1c2a032ada29d812361249fb3c58:::
SMB         192.168.133.138 445    192.168.133.138  test2:1001:aad3b435b51404eeaad3b435b51404ee:0210e43570d22539c0bc588587d2a7e6:::
SMB         192.168.133.138 445    192.168.133.138  adminlocal:1002:aad3b435b51404eeaad3b435b51404ee:999e1c2a032ada29d812361249fb3c58:::
SMB         192.168.133.138 445    192.168.133.138  [+] Added 7 SAM hashes to the database
```

Mimikatz

```
Authentication Id : 0 ; 2594251 (00000000:002795cb)
Session           : Service from 0
User Name         : svc-SQLAnalysis
Domain            : ADSECLAB
SID               : S-1-5-21-1473643419-774954089-2222329127-1608
        msv :
         [00000003] Primary
         * Username : svc-SQLAnalysis
         * Domain   : ADSECLAB
         * NTLM     : 3c917b61c58c4cba165396aad7d140a2
         * SHA1     : f089edb437e1f455ac1ab65886ed51959df7dc30
        tspkg :
         * Username : svc-SQLAnalysis
         * Domain   : ADSECLAB
         * Password : ThisIsAnOKPassword99!
        wdigest :
         * Username : svc-SQLAnalysis
         * Domain   : ADSECLAB
         * Password : ThisIsAnOKPassword99!
        kerberos :
         * Username : svc-SQLAnalysis
         * Domain   : LAB.ADSECURITY.ORG
         * Password : ThisIsAnOKPassword99!
        ssp :
        credman :
```

Vertical vs Horizontal Privilege Escalation



Lateral Movement

After gaining initial access, attackers often attempt to move laterally within a network to expand their control. Lateral movement involves moving from one compromised system to another to gain broader access and privileges.

Attackers use various techniques like pivoting, remote desktop, password reuse, and other means to move laterally.

Lateral movement allows attackers to explore and compromise additional systems, potentially gaining access to sensitive data or critical resources. Understanding lateral movement techniques is vital for identifying and mitigating potential attack paths in a network.

Lateral movement techniques depend on the network architecture, security controls, and the target environment. It should be noted that lateral movement itself is a complex and evolving aspect of offensive security assessments that requires continuous learning and updates.

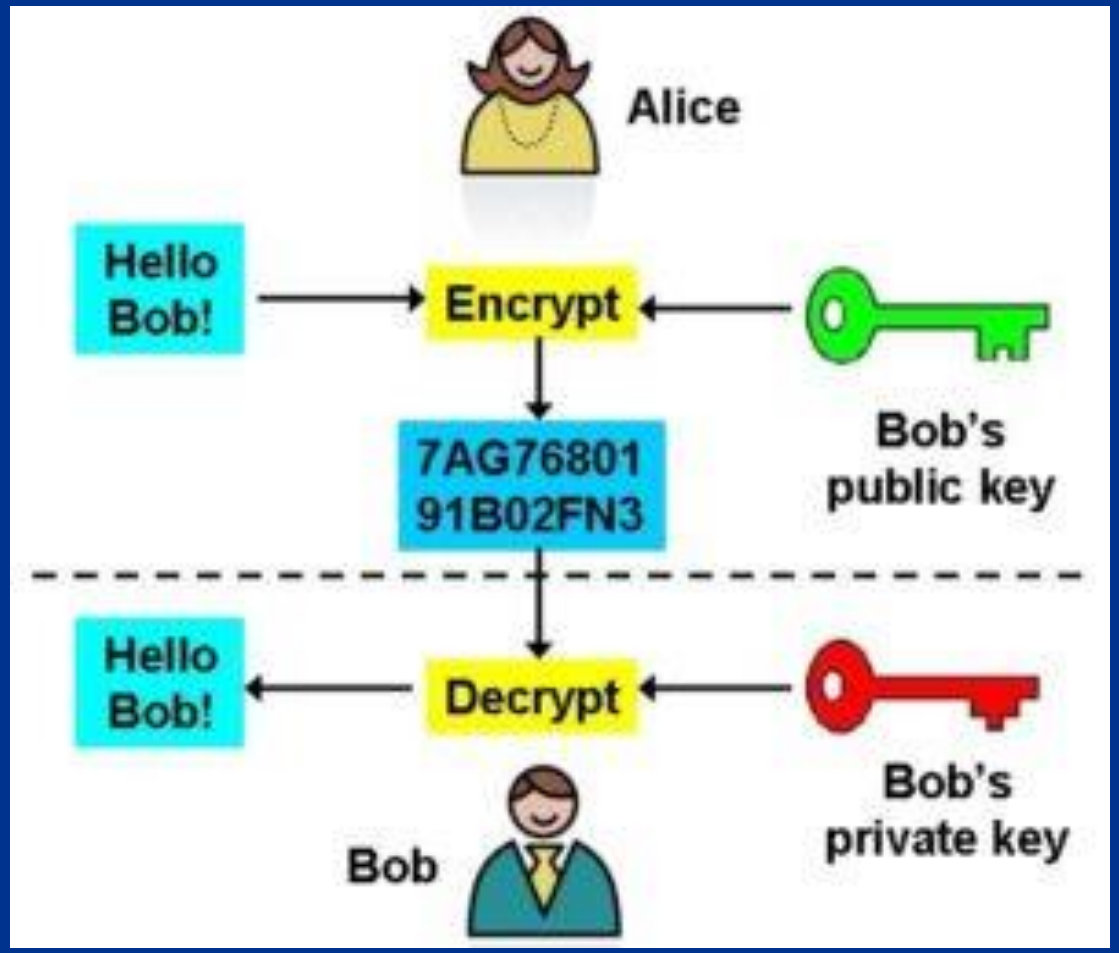
SSH – Secure Shell

- SSH creates a fast and easy way to execute commands, make changes, and configure services remotely.
- SSH gives a user two options to authenticate to a machine
  - Password based authentication (not recommended, we will see why in the lab)
  - Using SSH key pairs (Key-based authentication)

EXAMPLE COMMAND(S)

```
$ ssh username@ip_address
```

How key-pairs work



How SSH Key based authentication works

Generating ssh keys

```
PS C:\Users\ploshin> ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (C:\Users\ploshin/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in C:\Users\ploshin/.ssh/id_rsa.
Your public key has been saved in C:\Users\ploshin/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:wLk1KNLR/6ez9s5cfWIFByJtsbc2pYH7prbaQlCGJ0A office\ploshin@TTGT-I6UWJeZU2u
The key's randomart image is:
+---[RSA 3072]----+
|     .oE. ...o..  |
|    . o.oo +.o+ . |
|   . o =.o= .o + o|
|    . . +o.    o B |
|       . So   . = .|
|           o .o + |
|          . o  * o|
|           =+.= ..|
|          .oOO.   |
+----[SHA256]-----+
```

Some SSH misconfiguration issues

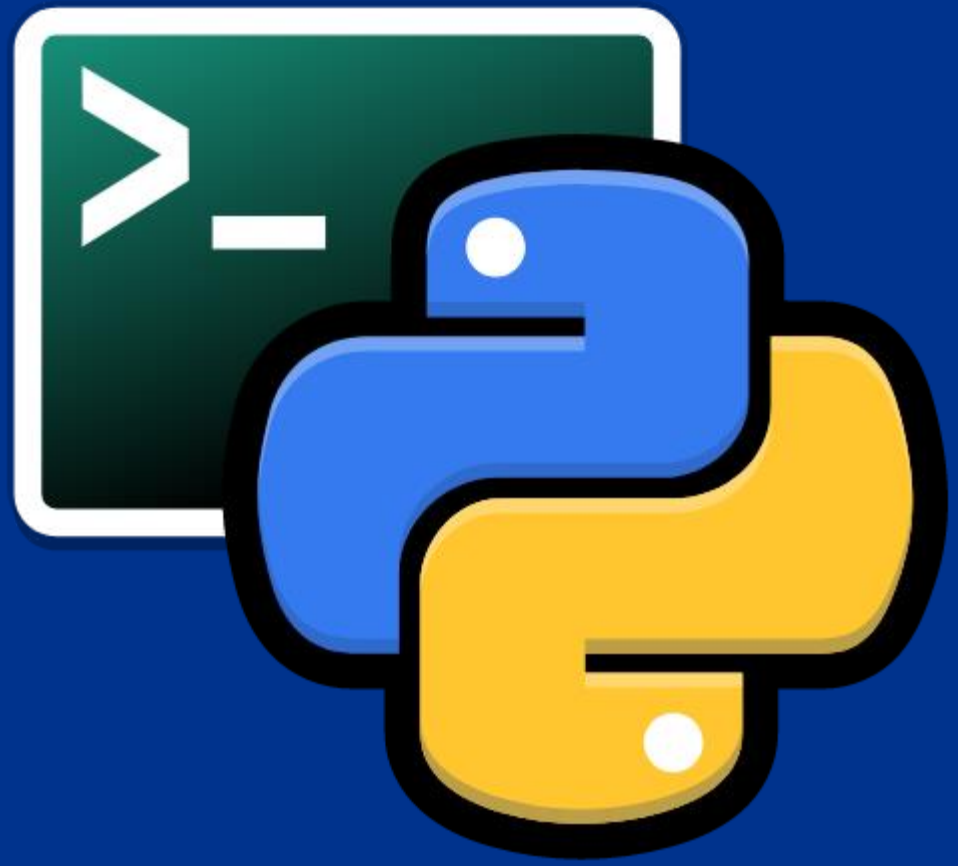
- Readable private keys
- Writable public keys
- Credentials in files accessible by others
- Mistakenly uploading ssh private keys to Github

How AD Misconfigurations can lead to Lateral Movement and Privilege Escalation

1. Loose Administrative Privileges
2. Open Network Shares
3. Service Accounts with Weak Passwords
4. Services Running on Hosts with Multiple Admins
5. Aged accounts with no password expiration

Impacket

- Impacket is a collection of Python classes for working with network protocols
- Impacket can communicate with:
  - SMB
  - Kerberos
  - NTLM



Popular impacket modules

EXAMPLE COMMAND(S)

```
# This script will gather data about the domain's users and their corresponding email addresses.
$ GetADUsers.py domain/user:password@IP

# A generic SMB client that will let you list shares and files, rename,
# upload and download files and create and delete directories
smbclient.py domain/user:password@IP
smbclient.py -dc-ip 10.10.2.1 -target-ip 10.10.2.3 domain/user:password
```

Impacket Demo

15 minute Break

Escalating Privileges Lab

07
Maintaining Access & Covering Tracks

Maintaining Access & Covering Tracks

After gaining initial access to a system, attackers often take steps to maintain persistence and continue their activities without being detected. This may involve creating additional user accounts, installing backdoors, modifying system configurations, or setting up scheduled tasks

To avoid detection and hide their activities, attackers often attempt to cover their tracks by deleting logs, modifying timestamps, clearing event logs, obfuscating their presence, and erasing evidence of their activities. This may also include using anti-forensic technique

Attackers may use various techniques to evade forensic analysis, such as encrypting communication, obfuscating data, deleting logs, and using anti-forensic tools or techniques to remove traces of their activities, such as file wiping, steganography, or encryption

As part of maintaining access and covering tracks, attackers may employ countermeasures to bypass security controls, disable or evade antivirus software, firewall rules, intrusion detection systems (IDS), and other security mechanisms

Persistance on Windows

Check if we have access to the Startup folder. This can be used to run malicious executables. However, this is commonly used for persistence.

EXAMPLE COMMAND(S)

```
$ icacls.exe “C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup
```

Alternatively:

- An attacker can use Task Scheduler (with the aide of **SharPersist**)
- An attacker can use COM Hijacks

to establish persistence as well

https://github.com/mandiant/SharPersist

08
Hacking Trivia

Question 1

Which of the following is not a type of hacking?

a) Black hat hacking
b) White hat hacking
c) Grey hat hacking
d) Red hat hacking

Question 2

Which type of hacking attack involves sending a large number of requests to a web server in order to overload it and cause it to crash?

A) DDoS attack

B) Man-in-the-middle attack

C) Brute force attack

D) SQL injection attack

Question 3

What is the term for a type of hacking attack in which an attacker intercepts and alters communication between two parties in order to eavesdrop or steal data?

A) SQL injection attack

B) Man-in-the-middle attack

C) Cross Site Scripting (XSS)

D) Social engineering attack

Question 4

Which of the following is a type of malware that spreads by copying itself onto other files or programs on a victim's computer?

A) Trojan horse

B) Worm

C) Rootkit

D) Botnet

Question 5

Which of the following is not a type of password attack?

a) Brute force attack
b) Dictionary attack
c) Social engineering attack
d) Rainbow table attack

Question 6

Which of the following is not a popular C2 (command-and-control) framework used by hackers?

a) Cobalt Strike

b) Empire

c) Metasploit

d) FinFisher

Question 7

Which of the following is a technique used to discover vulnerabilities in a network or system by testing it for known exploits?

A) Penetration testing

B) Social engineering

C) Rootkit installation

D) DNS poisoning

Question 8

Which of the following is not a component of the Metasploit Framework?

a) Exploit database
b) Payload generator
c) SQL injection scanner
d) Post-exploitation modules

Question 9

What is the term for a type of hacking attack that exploits a weakness in a software program or system in order to gain unauthorized access or control?

A) Exploit

B) Vulnerability

C) Malware

D) Rootkit

Question 10

Which of the following is not a common tool used for vulnerability assessments?

a) Nessus
b) Metasploit
c) Wireshark
d) OpenVAS

Question 11

What is Mimikatz?

a) A tool used for password cracking

b) A technique for exploiting vulnerabilities in software

c) A type of backdoor Trojan

d) A tool used to extract credentials from Windows systems

Question 12

Which of the following is a technique used to hide the identity of a hacker or attacker by routing their internet traffic through a series of servers and computers around the world?

A) Spoofing

B) VPN

C) TOR

D) Proxy server

Question 13

Which of the following is not a way to protect against password attacks?

a) Using a strong password policy
b) Limiting login attempts
c) Disabling password complexity requirements
d) Using multi-factor authentication

Question 14

Which of the following is a type of malware that is designed to monitor a user's activity and capture sensitive information like login credentials and credit card numbers?

A) Adware

B) Spyware

C) Ransomware

D) Botnet

Question 15

What is a honeypot?

a) A decoy system designed to attract and deceive attackers

b) A type of firewall used to filter incoming traffic

c) A tool used for scanning and identifying vulnerabilities in a system or network

d) A type of antivirus software

Thank you!

CTF Time

Resource List

- Google Dorking (https://www.exploit-db.com/google-hacking-database)
- Whois
- https://osintframework.com/
- Spiderfoot (https://www.spiderfoot.net/)
- Maltego (https://www.maltego.com/)
- Nessus (https://www.tenable.com/products/nessus)
- Nmap (https://nmap.org/)
- Nikto
- Burpsuite (https://portswigger.net/burp)
- Wpscan
- https://owasp.org/www-project-top-ten/
- https://book.hacktricks.xyz/linux-hardening/privilege-escalation
- https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation
- Metasploit (https://www.offsec.com/metasploit-unleashed/msfconsole/)
- Impacket (https://github.com/fortra/impacket)
- Empire
- Cobalt Strike (https://www.cobaltstrike.com/)
- Linenum (https://github.com/rebootuser/LinEnum)
- Linpeas (https://github.com/carlospolop/PEASS-ng/tree/master/linPEAS)
- Crackmapexec (https://wiki.porchetta.industries/)
- Powerup
- Mimikatz (https://www.sentinelone.com/cybersecurity-101/mimikatz/)
- ssh-keygen
- Netcat
- Enum4linux
- Snmp-check
- Beroot
- Sharpup (https://github.com/GhostPack/SharpUp)
- Seatbelt
- Powerup

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.ee

Document Classification: KPMG Public