Introduction to Ethical Hacking

MODULE TOPICS

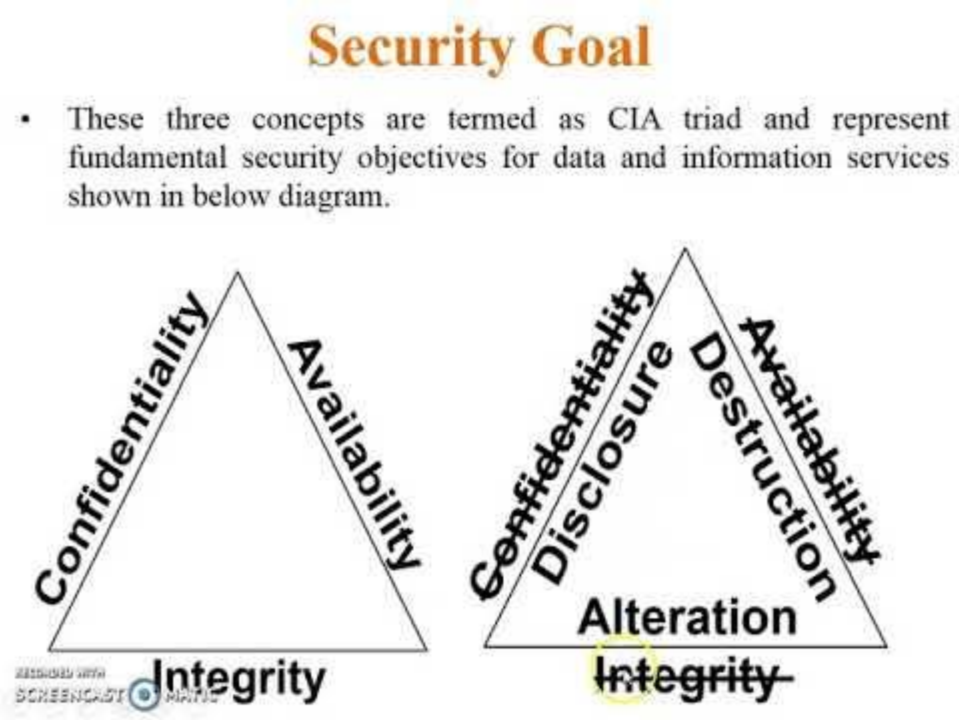
- Fundamental Security Concepts
- Threat Report 2023
- Hacking and hackers
- Ethical Hacking

WHAT IS INFORMATION?

- Is an asset which, like other important business assets, has value to an organization and consequently needs to be suitably protected
- Exists in many forms
  - ➢can be printed or written on paper
  - ➢stored electronically
  - ➢transmitted by post or using electronic means
  - ➢shown on films
  - ➢spoken in conversation

FUNDAMENTAL SECURITY CONCEPTS

- The whole principle is to avoid Theft, Tampering and Disruption of the systems through CIA Triad (Confidentiality, Integrity and Availability).



Security Goal

- These three concepts are termed as CIA triad and represent fundamental security objectives for data and information services shown in below diagram.

Confidentiality

Availability

Integrity

~~Confidentiality~~ Disclosure

~~Availability~~ Destruction

Alteration

~~Integrity~~

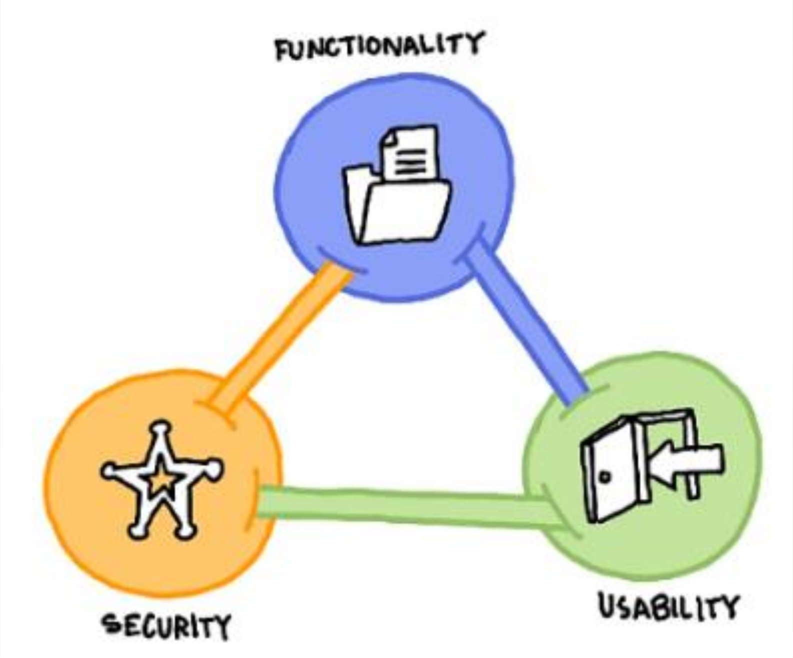
RECORDED WITH SCREENCAST-O-MATIC

FUNDAMENTAL SECURITY CONCEPTS

- **Confidentiality** Keeping systems and data from being accessed, seen, read to anyone who is not authorized to do so. Information is accessible only to the authorized personnel.
- **Integrity** TRUSTWORTHINESS OF DATA OR RESOURCES: Protect the data from modification or deletion by unauthorized parties and ensuring that when authorized people make changes that shouldn't have been made the damage can be undone.
- **Availability** - ACCESSIBLE WHEN REQUIRED BY AUTHORIZED USERS: Systems, access channels, and authentication mechanisms must all be working properly for the information they provide and protect to be available when needed.

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.



ATTACK VECTORS

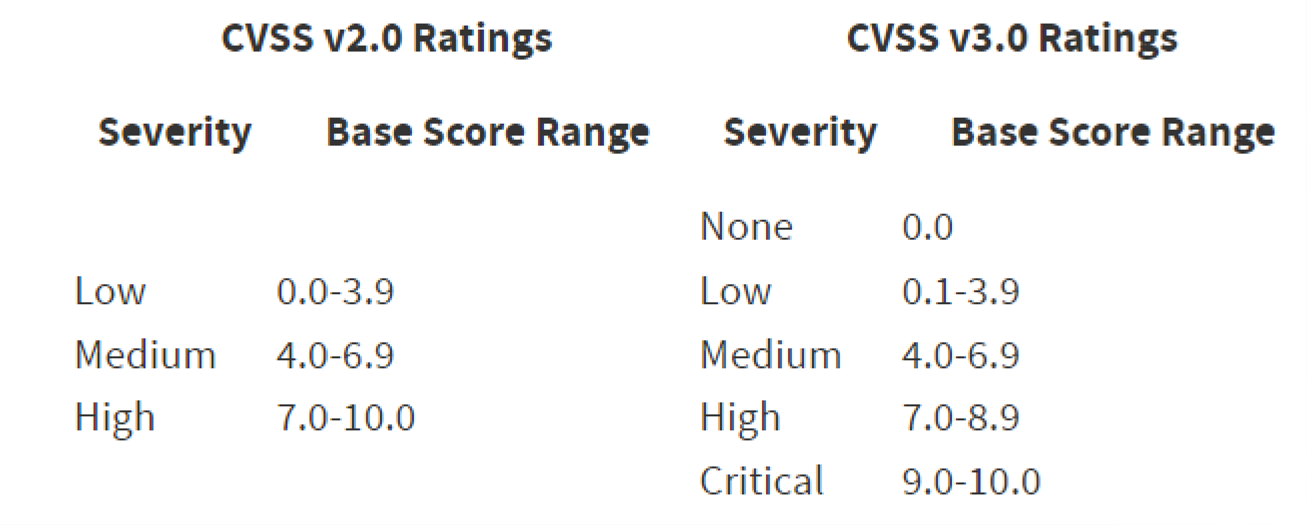
-path by which a hacker can gain access to a host in order to deliver a payload or malicious outcome

- **APT - Advanced Persistent Threats**
- **Cloud computing / Cloud based technologies**
- **Viruses, worms, and malware**
- **Ransomware**
- **Mobile Device threats**
- **Botnets**
- **Insider attacks**
- **Phishing attacks**
- **Web Application Threats**
- **IoT Threats**

VULNERABILITIES

CVSS - Common Vulnerability Scoring System

is an open framework for communicating the characteristics and severity of software vulnerabilities. CVSS consists of three metric groups: Base, Temporal, and Environmental

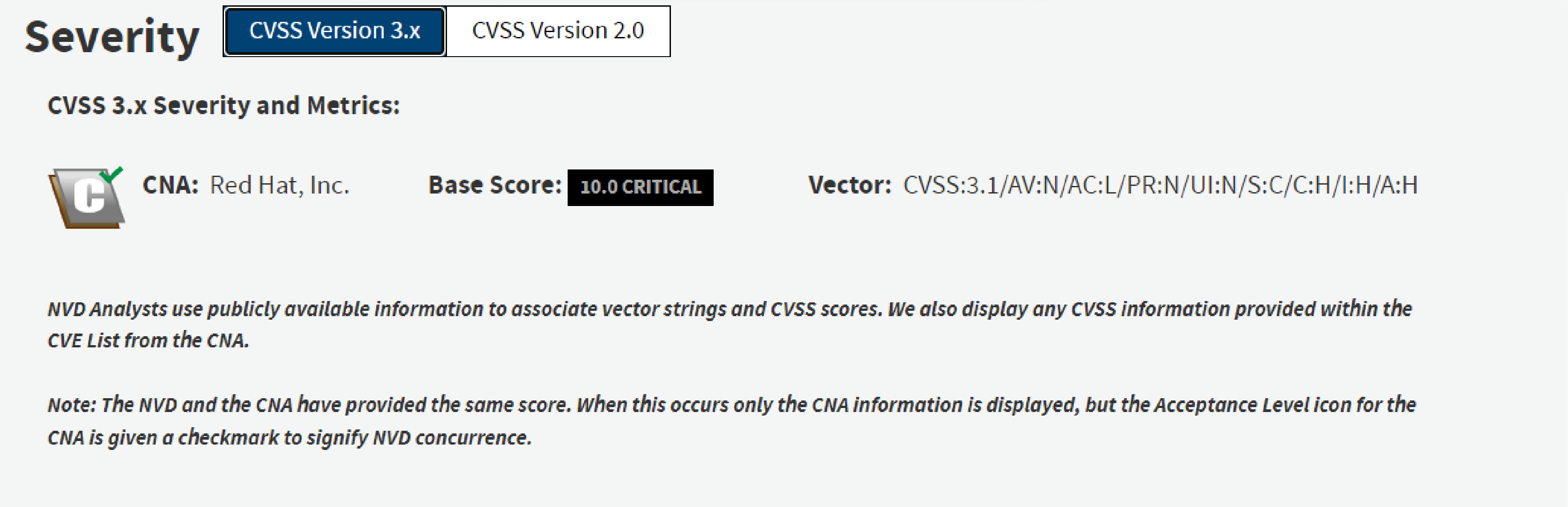


CVSS v2.0 Ratings		CVSS v3.0 Ratings	
Severity	**Base Score Range**	**Severity**	**Base Score Range**
		None	0.0
Low	0.0-3.9	Low	0.1-3.9
Medium	4.0-6.9	Medium	4.0-6.9
High	7.0-10.0	High	7.0-8.9
		Critical	9.0-10.0

VULNERABILITIES

CVSS - Common Vulnerability Scoring System

CVSS 3.X Severity for CVE-2024-3094 - XZ Upstream Supply Chain Attack



CVSS 3.x Severity and Metrics:

CNA: Red Hat, Inc. **Base Score:** 10.0 CRITICAL **Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

Note: The NVD and the CNA have provided the same score. When this occurs only the CNA information is displayed, but the Acceptance Level icon for the CNA is given a checkmark to signify NVD concurrence.

VULNERABILITIES

CVE – Common Vulnerabilities and Exposures

Is a list of publicly disclosed vulnerabilities and exposures that is maintained by MITRE

https://cve.mitre.org/

https://www.cve.org/

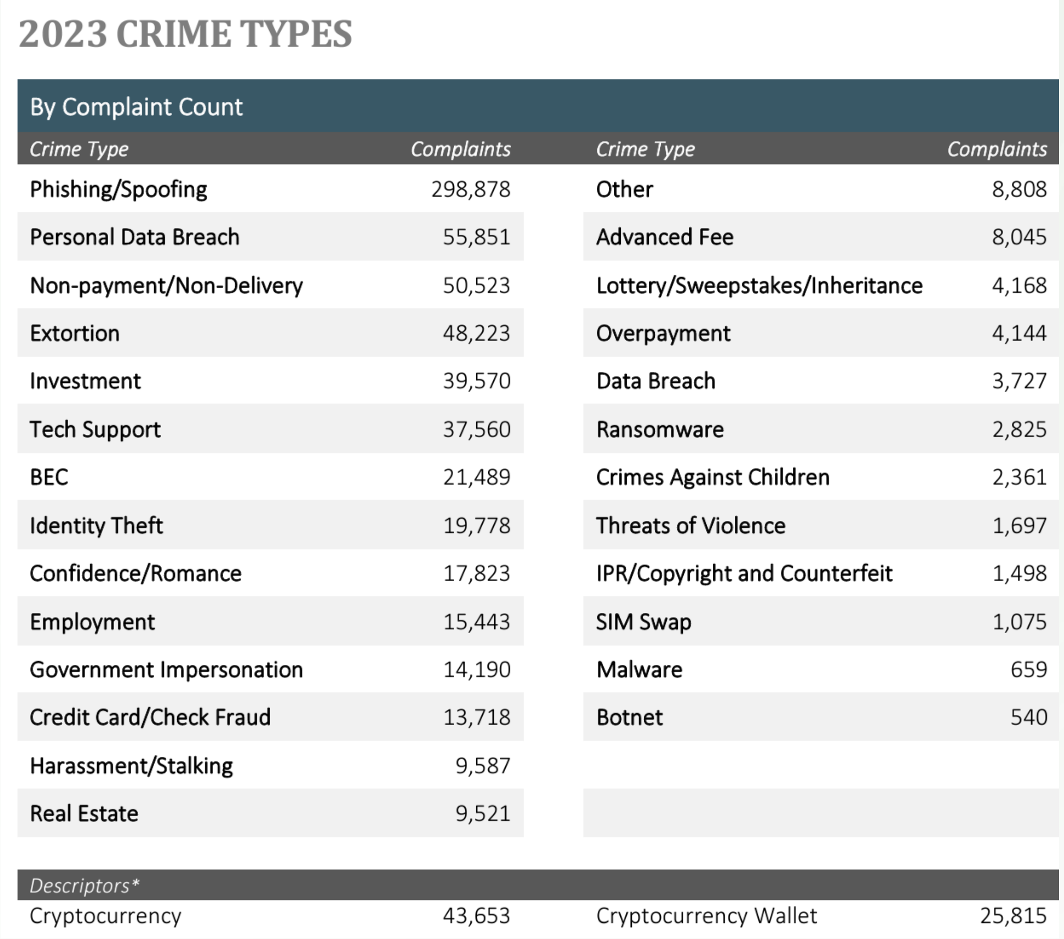
- Once made public, a CVE entry includes the CVE ID (in the format "CVE-2019-1234567"), a brief description of the security vulnerability or exposure, and references, which can include links to vulnerability reports and advisories.

2022 TOP ROUTINELY EXPLOITED VULNERABILITIES

CVE	Vendor	Product	Type
CVE-2018-13379	Fortinet	FortiOS and FortiProxy	SSL VPN credential exposure
CVE-2021-34473 / (Proxy Shell)	Microsoft	Exchange Server	RCE
CVE-2021-31207 / (Proxy Shell)	Microsoft	Exchange Server	Security Feature Bypass
CVE-2021-34523 / (Proxy Shell)	Microsoft	Exchange Server	Elevation of Privilege
CVE-2021-40539	Zoho ManageEngine	ADSelfService Plus	RCE/ Authentication Bypass
CVE-2021-26084	Atlassian	Confluence Server and Data Center	Arbitrary code execution
CVE-2021- 44228 / (Log4Shell)	Apache	Log4j2	RCE
CVE-2022-22954	VMware	Workspace ONE Access and Identity Manager	RCE
CVE-2022-22960	VMware	Workspace ONE Access, Identity Manager, and vRealize Automation	Improper Privilege Management
CVE-2022-1388	F5 Networks	BIG-IP	Missing Authentication Vulnerability
CVE-2022-30190	Microsoft	Multiple Products	RCE
CVE-2022-26134	Atlassian	Confluence Server and Data Center	RCE

Source: Cybersecurity and Infrastructure Security Agency

TOP CYBERCRIME FOR 2023



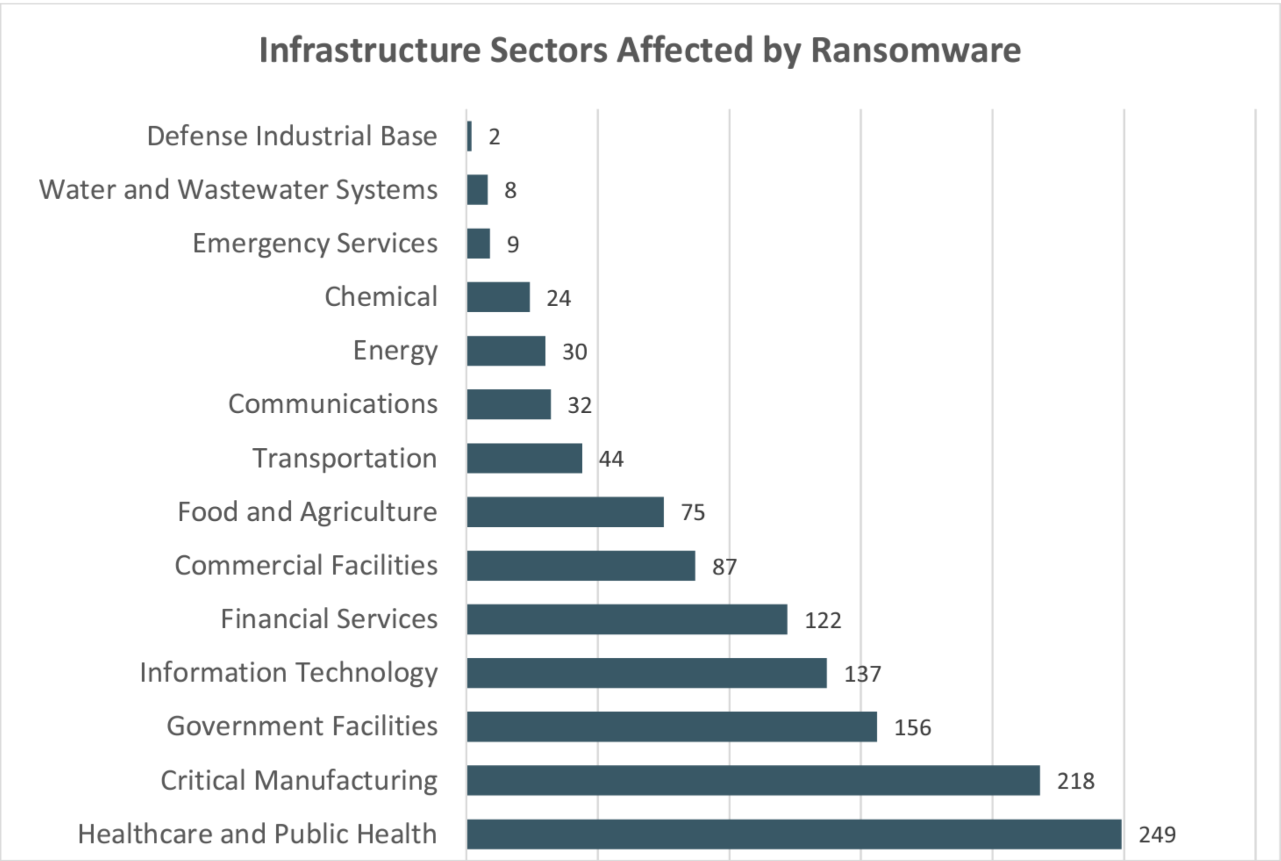
2023 CRIME TYPES

By Complaint Count

Crime Type	*Complaints*	*Crime Type*	*Complaints*
Phishing/Spoofing	298,878	Other	8,808
Personal Data Breach	55,851	Advanced Fee	8,045
Non-payment/Non-Delivery	50,523	Lottery/Sweepstakes/Inheritance	4,168
Extortion	48,223	Overpayment	4,144
Investment	39,570	Data Breach	3,727
Tech Support	37,560	Ransomware	2,825
BEC	21,489	Crimes Against Children	2,361
Identity Theft	19,778	Threats of Violence	1,697
Confidence/Romance	17,823	IPR/Copyright and Counterfeit	1,498
Employment	15,443	SIM Swap	1,075
Government Impersonation	14,190	Malware	659
Credit Card/Check Fraud	13,718	Botnet	540
Harassment/Stalking	9,587		
Real Estate	9,521		
*Descriptors**			
Cryptocurrency	43,653	Cryptocurrency Wallet	25,815

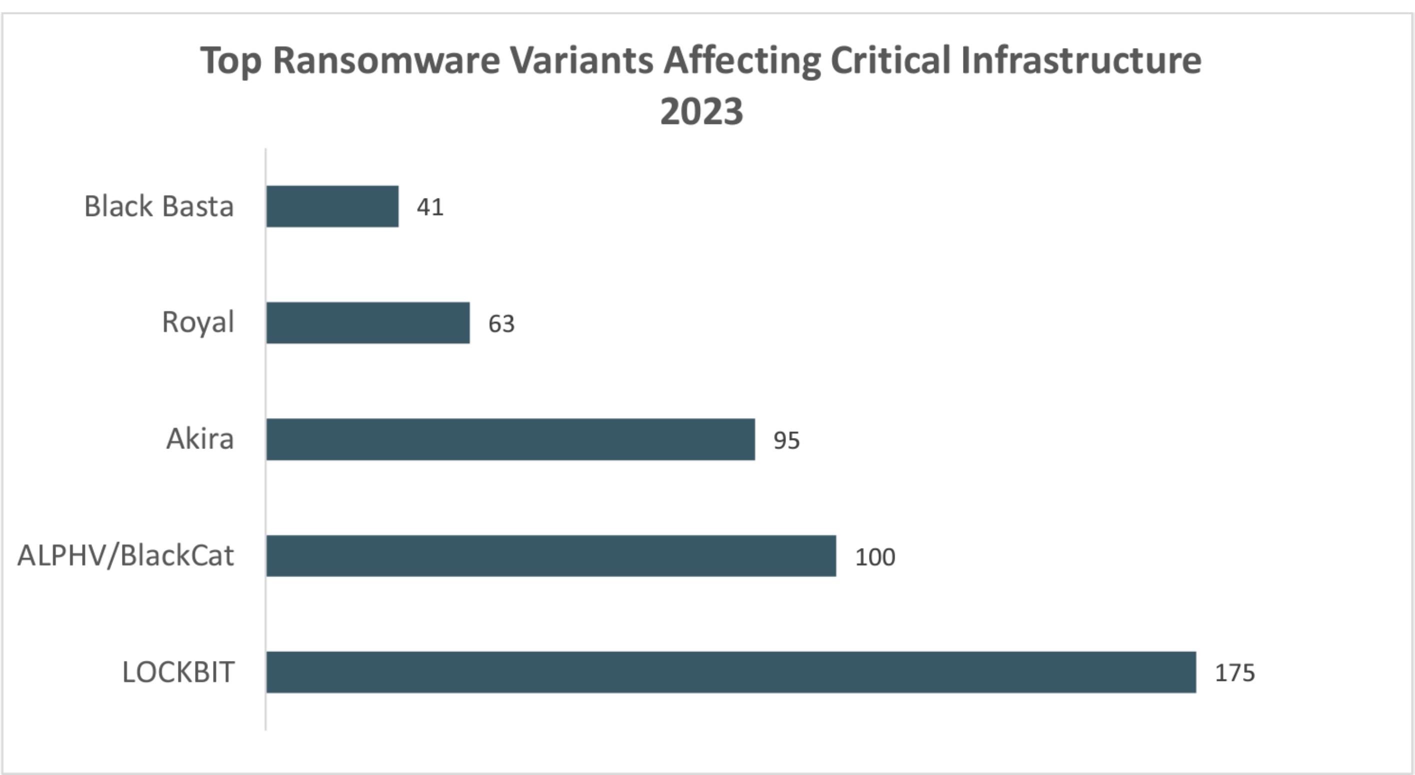
Source: FBI Internet Crime Report 2023

VICTIMS OF RANSOMWARE



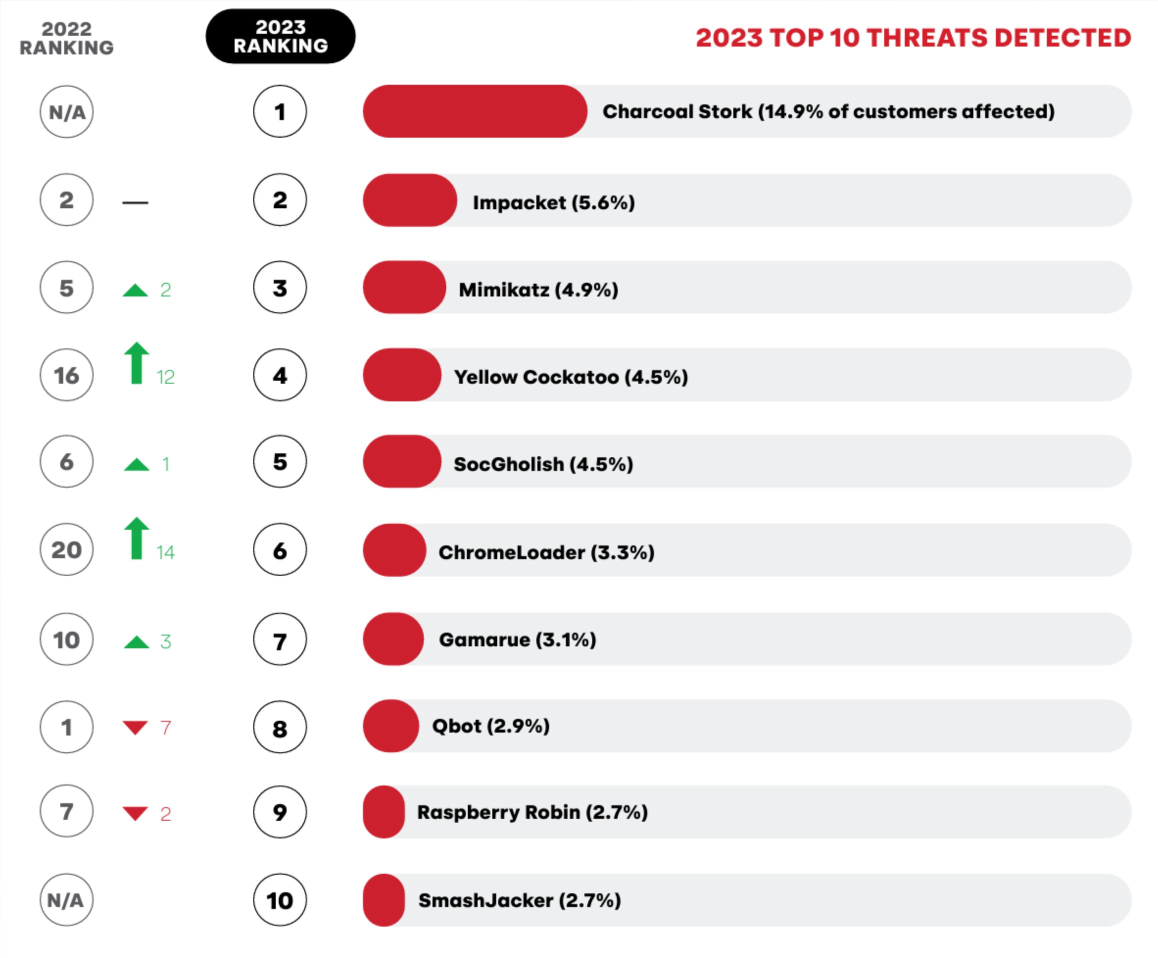
Source: FBI Internet Crime Report 2023

TOP RANSOMWARE VARIANTS



Source: FBI Internet Crime Report 2023

TOP 10 THREATS OF 2023

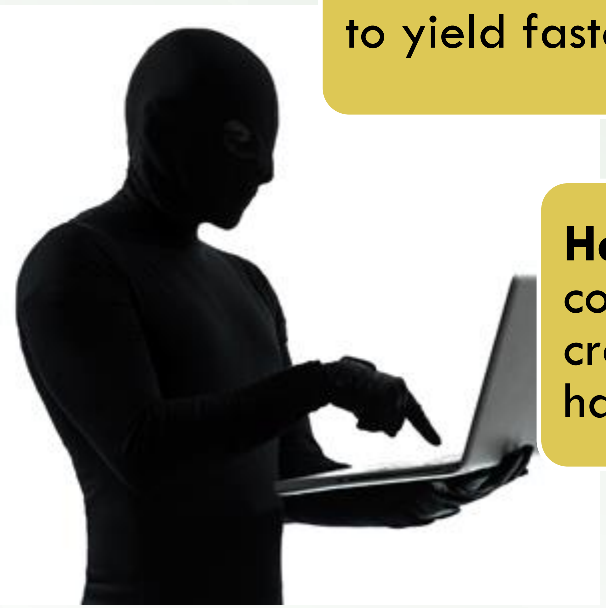


2023 TOP 10 THREATS DETECTED

2022 RANKING		2023 RANKING	
N/A		1	Charcoal Stork (14.9% of customers affected)
2	—	2	Impacket (5.6%)
5	▲ 2	3	Mimikatz (4.9%)
16	↑ 12	4	Yellow Cockatoo (4.5%)
6	▲ 1	5	SocGholish (4.5%)
20	↑ 14	6	ChromeLoader (3.3%)
10	▲ 3	7	Gamarue (3.1%)
1	▼ 7	8	Qbot (2.9%)
7	▼ 2	9	Raspberry Robin (2.7%)
N/A		10	SmashJacker (2.7%)

Source: Red Canary's 2023 Threat Detection Report

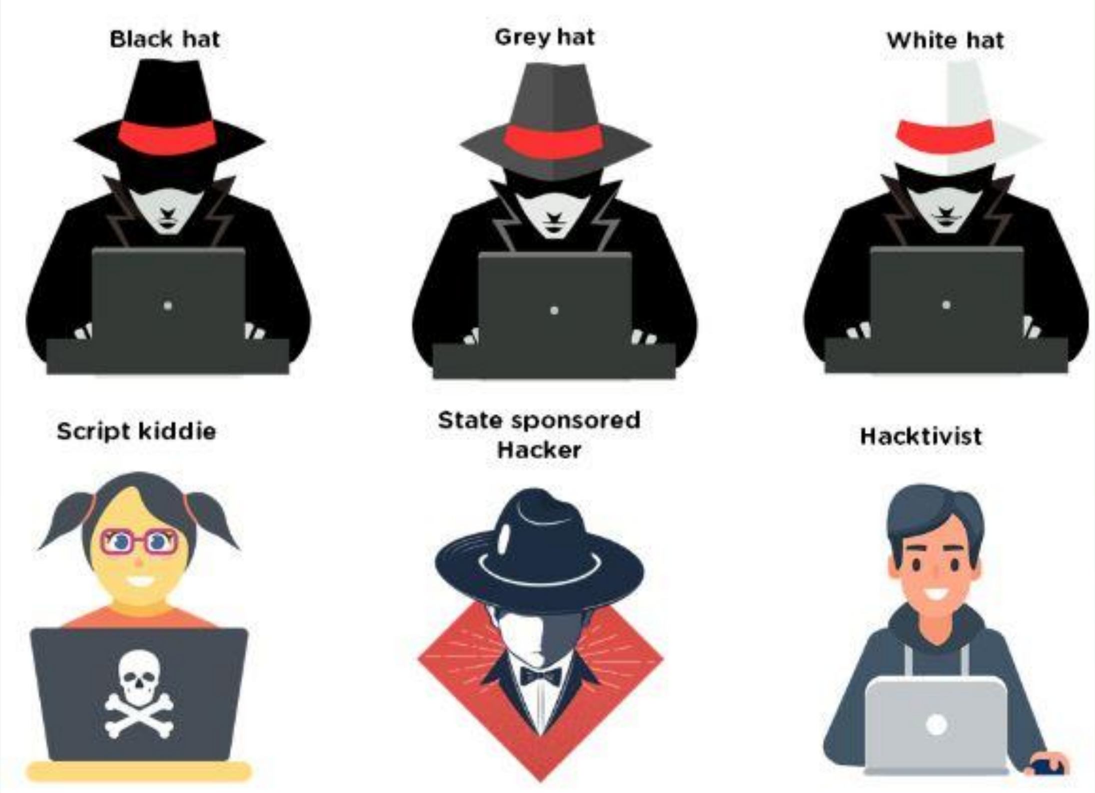
WHAT IS A HACKER?



Hack: a fast work around, or shortcut that was undertaken to improve a program or to yield faster results.

Hackers: Individuals with excellent computer skills and the ability to create and explore computer hardware / software

TYPES OF HACKERS



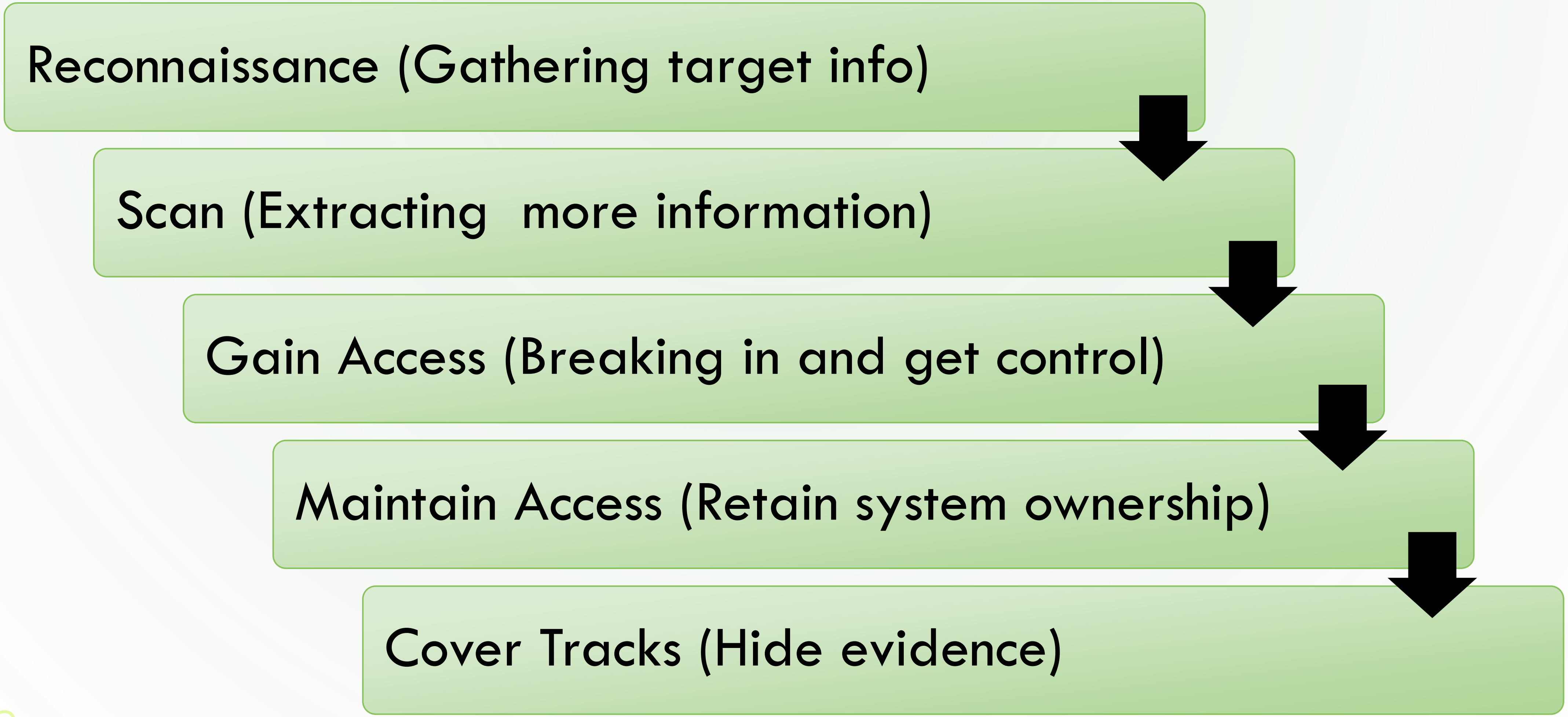
TYPES OF HACKERS

- **Black Hat** - Hackers that seek to perform malicious activities.
- **Gray Hat** - Hackers that perform good or bad activities but do not have the permission of the organization they are hacking against.
- **White Hat** - Ethical hackers; They use their skills to improve security by exposing vulnerabilities before malicious hackers.
- **Script Kiddie / Skiddies** - Unskilled individual who uses malicious scripts or programs, such as a web shell, developed by others to attack computer systems and networks and deface websites.
- **State-Sponsored Hacker** - Hacker that is hired by a government or entity related.
- **Hacktivist** - Someone who hacks for a cause; political agenda.
- **Suicide Hackers** - Are hackers that are not afraid of going jail or facing any sort of punishment; hack to get the job done.
- **Cyberterrorist** - Motivated by religious or political beliefs to create fear or disruption

TERMS TO REMEMBER

- **Hack value** - Perceived value or worth of a target as seen by the attacker.
- **Vulnerability** - A system flaw, weakness on the system (on design, implementation etc).
- **Threat** - Exploits a vulnerability.
- **Exploit** - Exploits are a way of gaining access to a system through a security flaw and taking advantage of the flaw for their benefit.
- **Payload** - Component of an attack; is the part of the private user text which could also contain malware such as worms or viruses which performs the malicious action; deleting data, sending spam or encrypting data.
- **Zero-day attack** - Attack that occurs before a vendor knows or is able to patch a flaw.
- **Daisy Chaining / Pivotting** - It 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.
- **Doxxing** - Publishing PII about an individual usually with a malicious intent.

WHAT DOES A HACKER DO?



Reconnaissance (Gathering target info)

Scan (Extracting more information)

Gain Access (Breaking in and get control)

Maintain Access (Retain system ownership)

Cover Tracks (Hide evidence)

WHAT DOES A HACKER DO?

Reconnaissance

Gathering evidence about targets; There are two types of Recon:

- **Passive Reconnaissance**: Gain information about targeted computers and networks **without direct interaction with the systems**.
  - e.g: Google Search, Public records, New releases, Social Media, Wardrive scanning networks around.
- **Active Reconnaissance**: Envolves direct interaction with the target.
  - e.g: Make a phone call to the target, Job interview; tools like Nmap, Nessus, OpenVAS, Nikto and Metasploit can be considered as Active Recon.

WHAT DOES A HACKER DO?

Scanning & Enumeration

Obtaining more in-depth information about targets.

- e.g: Network Scanning, Port Scanning, Which versions of services are running.

Gaining Access

Attacks are leveled in order to gain access to a system.

- e.g: Can be done locally (offline), over a LAN or over the internet.
  - e.g(2): Spoofing to exploit the system by pretending to be a legitimate user or different systems, they can send a data packet containing a bug to the target system in order to exploit a vulnerability.
  - Can be done using many techniques like command injection, buffer overflow, DoS, brute forcing credentials, social engineering, misconfigurations etc.

WHAT DOES A HACKER DO?

Maintaining Access

Items put in place to ensure future access.

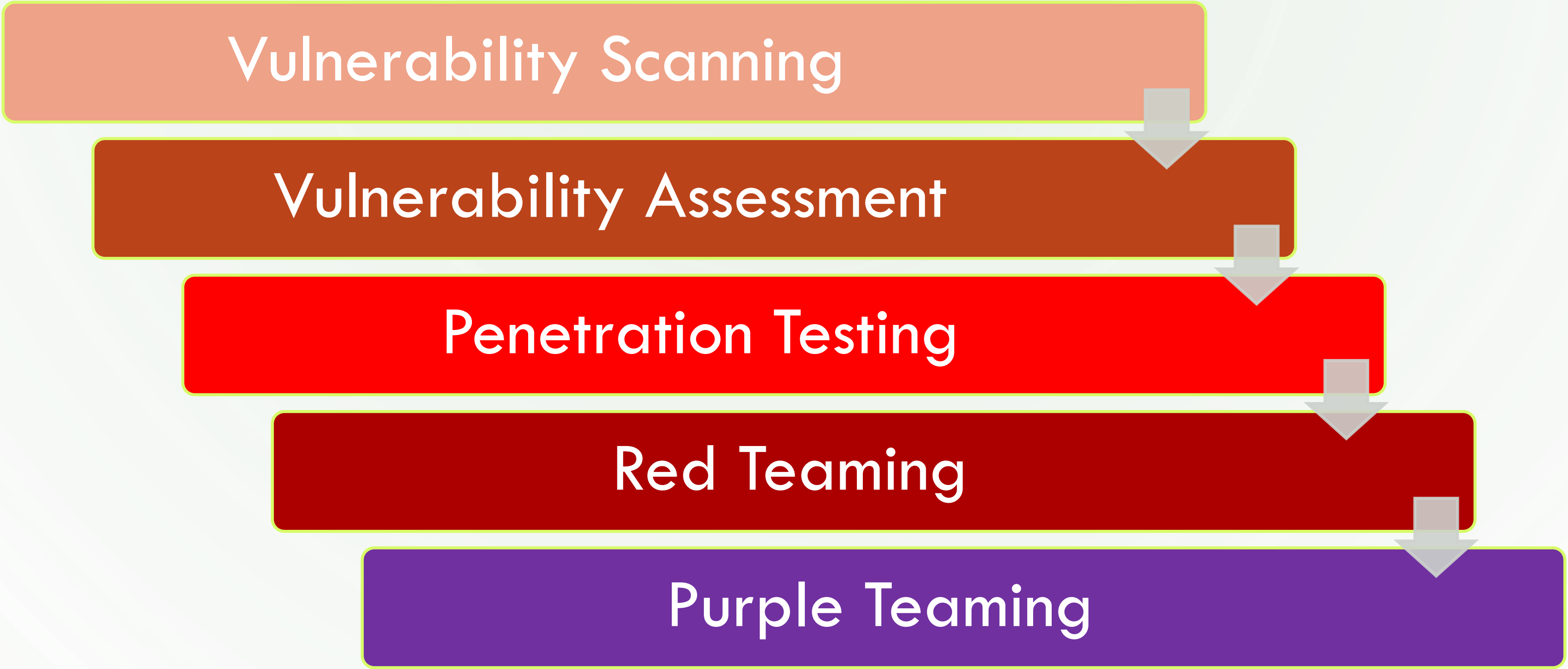
- e.g: Rookit, Trojan, Backdoor can be used.

Covering Tracks

Steps taken to conceal success and intrusion; Not be noticed.

- e.g: Clear the logs; Obfuscate trojans or malicious backdoors programs.

CYBER MATURITY MODEL



Vulnerability Scanning

Vulnerability Assessment

Penetration Testing

Red Teaming

Purple Teaming

WHAT'S NOT INCLUDED IN NSSECU2?

- Mobile Pentesting
- Active Directory Pentesting
- EDR/AV Evasion
- Exploit Development
- Code Review

WHY IS ETHICAL HACKING NECESSARY?

- Hacking involves creative thinking - vulnerability testing and security audits are not enough
- Allows countering attacks from malicious hackers by anticipating methods they can use to break into the system
- Used to identify vulnerabilities and possible remedial actions to resolve them

WHAT DO ETHICAL HACKERS DO?

- Ethical hackers try to answer the following questions:
  - What can an intruder see on the target system?
  - What can an intruder do with that information?
  - Does anyone at the target notice the intrusion?

> *"If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle."*
>
> -Sun Tzu, Art of War

WHAT DO ETHICAL HACKERS DO?

- Are hired by an organization to do penetration testing on information systems and networks
  - Attack systems to test if security measures are functioning correctly
  - Discover and document vulnerabilities found
  - Provide advice on how to fix vulnerabilities found

WHAT YOU CANNOT DO LEGALLY – PHILIPPINE CYBERCRIME PREVENTION ACT OF 2012

- Accessing a computer without permission
- Intentional interception of data
- Alteration or deletion of data without permission
- Hindering the function of a system
- Possession of others' passwords can be a crime
- Information theft

ETHICAL HACKING RULES

- DO be sure you have permission (if possible written) to probe the target to identify security issues
- DO respect the privacy of the individual or company
- DO disclose all vulnerabilities found in software or hardware
- DON'T leave anything open for you or others to exploit
- DON'T do anything irreversible

ETHICAL HACKING / PENTESTING CERTIFICATION BODIES

- Offensive Security
- eLearnSecurity
- EC-Council
- SANS
- Pentester Academy
- Zeropoint Security
- CompTIA

ETHICAL HACKING CAREER

- Vulnerability Manager
- Penetration Tester
- Web Application Penetration Tester
- Mobile Application Penetration Tester
- Red Team / Adversary Simulation
- Security Researcher / Bug Bounty Hunter