Tishk International University
Faculty of Applied Science
Cybersecurity Department

Lecture 8 : Ethical Hacking

CBS221/A : Ethics and Legal Issues in Cybersecurity

Week 9 : 30/11-04/12/2025

Instructor: Prof. Dr. Qaysar Salih Mahdi

Tishk International University
Faculty of Applied Science
Cybersecurity Department

What is Ethical Hacking?

Ethical Hacking

The Certified Ethical Hacker (CEH) credentialing and provided by EC-Council is a respected and trusted ethical hacking course in the industry. Since the inception of Certified Ethical Hacker in 2003, the credential has become one of the best options for industries and companies across the world. The CEH exam is ANSI 17024 compliant, adding value and credibility to credential members. It is also listed as a baseline certification in the US Department of Defense (DoD) Directive 8570 and is a NSCS Certified Training.

Today, you can find Certified Ethical Hackers working with some of the finest and largest companies across industries like healthcare, financial, government, energy, and much more!

Tishk International University
Faculty of Applied Science
Cybersecurity Department

What Does an Ethical Hacker Do?

An ethical hacker is a cybersecurity professional trained to identify and fix vulnerabilities in systems before malicious hackers can exploit them. They simulate real-world cyberattacks to assess risk and strengthen security posture.

- **Ethical Hackers help organizations answer critical cybersecurity questions:**
- **What vulnerabilities could an attacker exploit?**
- **What systems or data are most at risk?**
- **What damage could an attacker cause with the compromised information?**
- **How many security layers detect or log the intrusion?**

Ethical hackers learn and perform hacking in a professional manner, based on the direction of the client, and later, present a maturity scorecard highlighting their overall risk and vulnerabilities and suggestions to improve.

- **What are the best ways to mitigate these vulnerabilities?**

They operate under strict authorization, document their findings, and deliver a comprehensive risk and vulnerability scorecard along with actionable recommendations.

Exercise: Identify ethical issues in the Equifax breach.

Solution: Internal disclosure aligns with utilitarian ethics; external disclosure aligns with deontology but may violate law.

Tishk International University
Faculty of Applied Science
Cybersecurity Department

Hacktivism

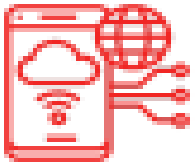
Motivations, Tactics, and Threats

Where are we and how did we get here?

- Technology makes it easier to disseminate a wide variety of ideologies
  - — Some have caught on:
    - Freedom of information
    - Government and organizational distrust
- Anonymity of the Internet
- Disparity between resources required to attack

Types of Ethical Hacking?

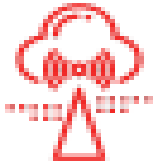
It is no big secret that any system, process, website, device, etc., can be hacked. In order to understand how the hack might happen and what the damage could be, ethical hackers must know how to think like malicious hackers and know the tools and techniques they are likely to use.



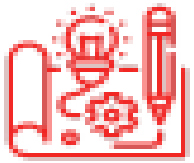
Web Application Hacking

System Hacking

Web Server Hacking



Hacking Wireless Network



Social Engineering

Hacktivism defined

- Hacking to promote a political agenda, religious belief or social ideology.
  - Political
  - Religious
  - Social ideology
    - Human rights
    - Free speech
    - Freedom of information
- Hacking "clothed" in moral attire
- The morality is subjective

LulzSec (Lulz Security)

- Infragard
- US Senate
- CIA
- FBI Cybercrime conference call
- Group retired in 2011
- Some members arrested

Anonymous

- International network of hacktivists
- Originated in 2003
- No Leadership
- Released names of supposed KKK members to pastebin yesterday

Edward Snowden

- Published NSA files on phone record collection in 2013
- Charged with espionage

Who is your Snowden?

Tishk International University
Faculty of Applied Science
Cybersecurity Department

Wikileaks

- Site that publishes secret information, classified files, and news leaks from anonymous sources

Latest Releases

CIA Director John Brennan emails

2015-10-21

Today, 21 October 2015 and over the coming days WikiLeaks is releasing documents from one of CIA chief John Brennan's non-government email accounts. Brennan used the account occasionally for several intelligence related projects.

Updated TPP Treaty: Intellectual Property Rights Chapter

2015-10-09

Today, 9 October, 2015 WikiLeaks releases the final negotiated text for the TPP (Trans-Pacific Partnership) Intellectual Property Rights Chapter. The TPP encompasses 12 nations representing more than 40 per cent of global GDP. Despite a final agreement, the text is still being withheld from the public, notably until after the Canadian election on October 19.

Target Tokyo

2015-07-31

Today, Friday 31 July 2015, 9am CEST, WikiLeaks publishes "Target Tokyo", 35 Top Secret NSA targets in Japan including the Japanese cabinet and Japanese companies such as Mitsubishi, together with intercepts relating to US-Japan

WikiLeaks Archives

U.K. (2009) Publication of the UK Royal Mail's PostZon postcode database

WikiLeaks released the UK government database of all 1,841,177 UK post codes together with latitude and longitude, grid references, county, district, ward, NHS codes and regions, Ordnance Survey reference, and date of introduction. The database was last updated on July 8, 2009 and is over 100,000 pages in size.

U.K. (2009) Barclays Bank

On Monday 16th March 2009, The Guardian newspaper in the United Kingdom published a series of leaked memos from the banking giant Barclays. The next day, these documents were removed from The Guardian web archive, as a result of a court injunction obtained in the middle of the night.

WikiLeaks obtained the documents from an anonymous source and published them the next day. The documents are copies of alleged internal memos from within Barclays Bank. They were sent by an anonymous whistleblower to Vince Cable, Liberal-Democrat shadow chancellor. The documents reveal a number of elaborate international tax avoidance schemes by the SCM (Structured Capital Markets) division of Barclays. According to these documents, Barclays has been systematically assisting clients to avoid huge amounts of tax they should be liable for across multiple jurisdictions.

Pastebin

- Public data repository
- Anonymous posting allowed
- Commonly find hacker loot and malicious code or copyright infringement source code

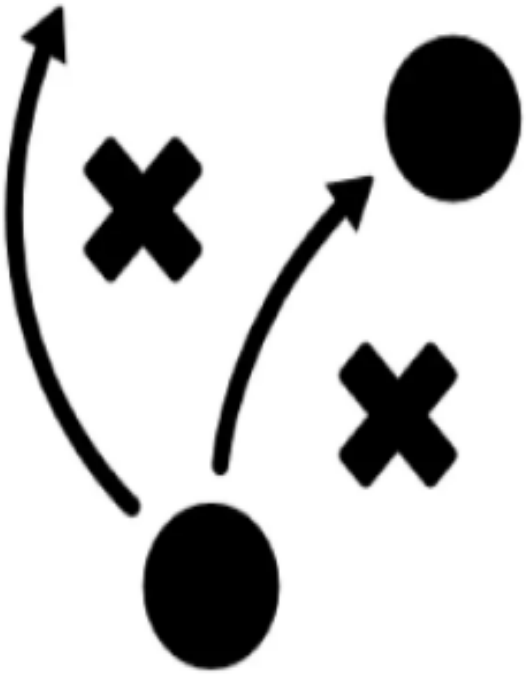
NAME / TITLE	ADDED	HITS	USER
Official OpKKK HoodsOff 2015 Data Release	12 hours ago	329,062	WestFlorissantAvenue
#OpKKK	1 day ago	2,119	a guest
SharedSec Official #OpKKK Release	12 hours ago	32,392	Operation_KKK_
Operation KKK NOV 4 TweetStorm	2 days ago	11,734	a guest
#OpKKK Phone members KKK (#4)- Anonymous	3 days ago	212,254	a guest
Internals of the NHS pay calculator 04/11/2015	1 day ago	1,756	a guest
#OpKKK	11 hours ago	1,155	a guest

Stratfor

- "Freedom of Information" hack
- Hacktivists upset that makes some information public but other information available only to specific clients
- Published emails on wikileaks
- Result to Stratfor:
  - PR cost and effort
  - Rebuild customer relationships

Tactics

- DDoS
- Most common hacking methods
- Negative SEO
  - Google bombing – associate negative keywords with your name
  - Utilize penalized SEO tactics on your sites / social media
- Email flooding
- Fax spam
- Phishing, Spam and SPIM



Action items

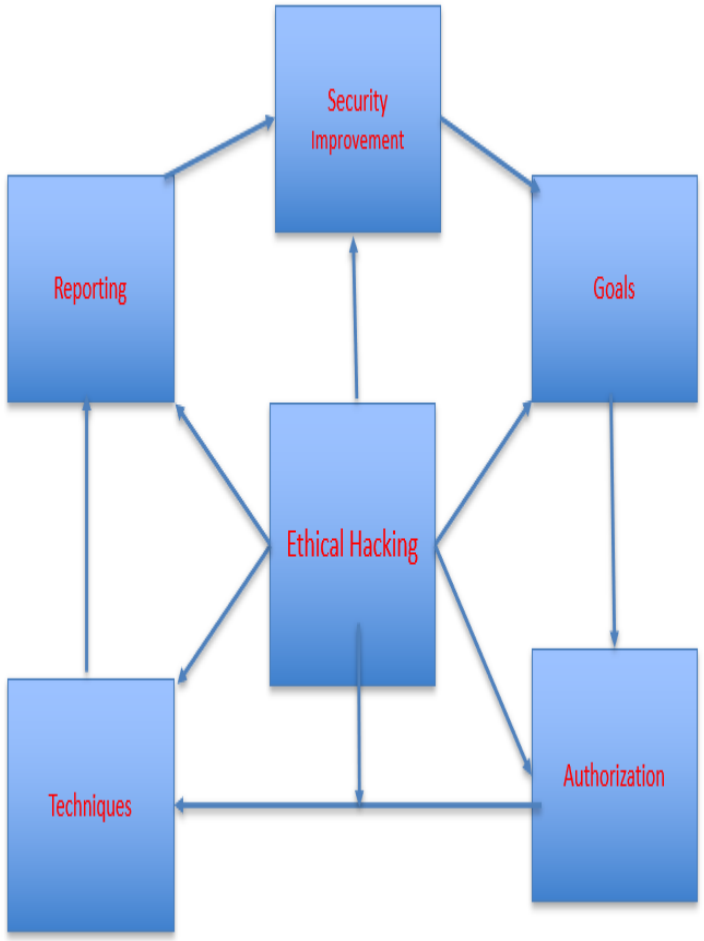
- Assess PR statements for hacktivism risk
- FBI warns law enforcement to limit social media use
- You can't throw money at this problem -- it requires cultural change
  - Assess your culture
- Background checks and personality profiling
- Pen test including social engineering

Tishk International University
Faculty of Applied Science
Cybersecurity Department

Key Theory Points:
Ethical hacking = authorized testing of systems to find vulnerabilities.
Also called 'white-hat hacking'.
Goal: improve security, not exploit.

Problem & Solution:
Q: A hacker tests a company system with permission. What type of hacker is this?
A: White-hat (ethical hacker).

Homework (HW):
HW:
1. Research one famous ethical hacking case.
2. Summarize the findings and impact.



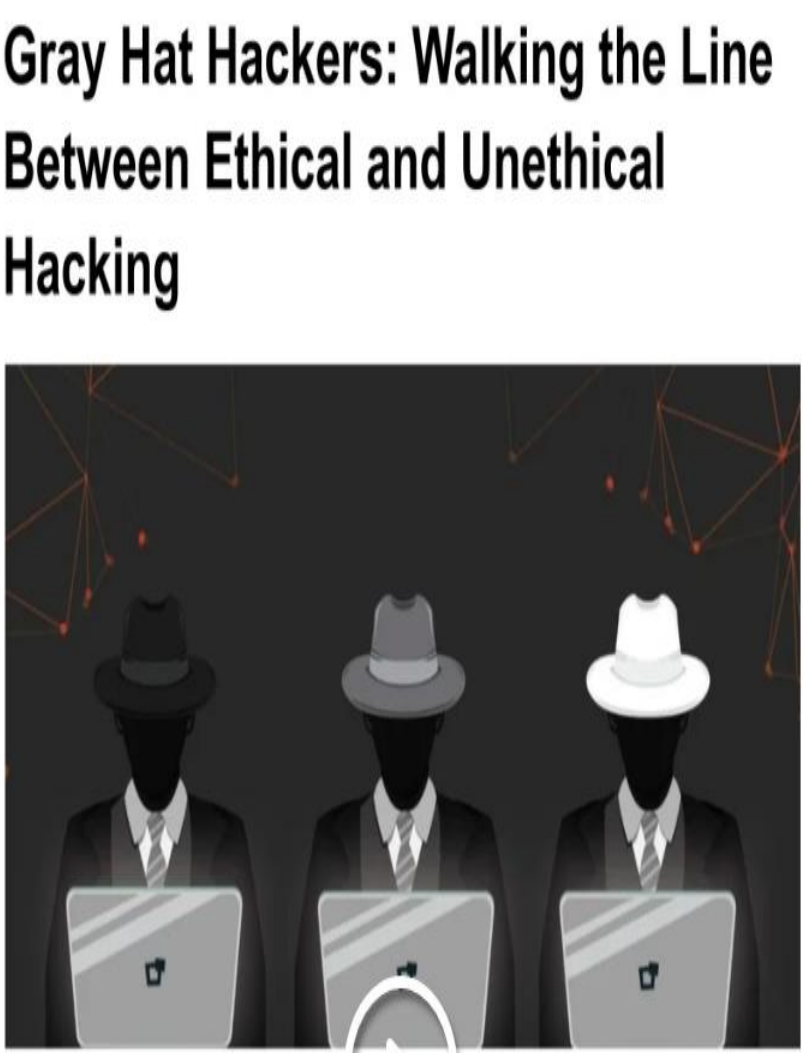
Tishk International University
Faculty of Applied Science
Cybersecurity Department

Types of Hackers

Key Theory Points:
Types of hackers:
- White-hat = authorized, improves security
- Black-hat = unauthorized, malicious
- Grey-hat = unauthorized but may report issues

Problem & Solution:
Q: Which hacker type hacks illegally but may inform the company afterwards?
A: Grey-hat.

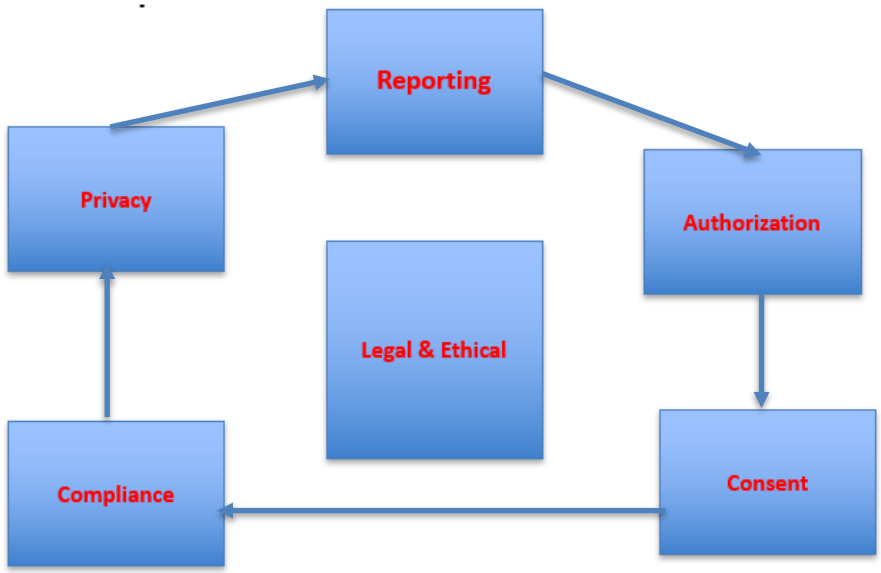
Homework (HW):
HW:
1. List 2 ethical differences between white-hat and black-hat hackers.
2. Discuss a grey-hat scenario ethically.



Tishk International University
Faculty of Applied Science
Cybersecurity Department

Legal and Ethical Considerations

Key Theory Points:
Legal/ethical rules:
- Must have explicit authorization
- Avoid privacy violations
- Comply with laws (CFAA, GDPR)



Problem & Solution:
Q: What law in the USA regulates unauthorized
A: Computer Fraud & Abuse Act (CFAA).

Homework (HW):
HW:
1. Summarize one court case involving ethical hacking.
2. Explain ethical lessons learned.

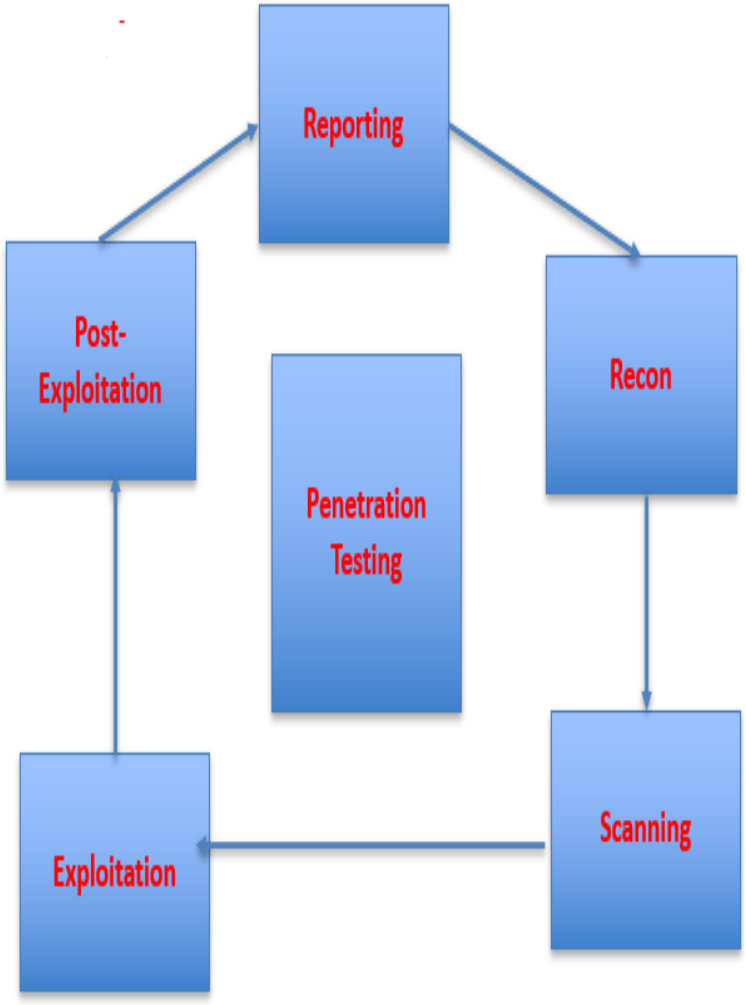
Tishk International University
Faculty of Applied Science
Cybersecurity Department

Penetration Testing Overview

Key Theory Points:
Penetration testing = simulated cyber attack to find vulnerabilities.
Phases: Reconnaissance, Scanning, Exploitation, Post-Exploitation, Reporting.

Problem & Solution:
Q: Which phase gathers information about target systems?
A: Reconnaissance.

Homework (HW):
HW:
1. Create a flow diagram of the 5 pen-testing phases.
2. Explain the importance of reporting vulnerabilities.



Penetration Testing

- **Penetration testing is the process of identifying the security vulnerabilities in a system or network and trying to exploit them. The results of penetration tests play a vital role in finding and patching security flaws.**
- **In this article, we'll discuss the responsibilities of a penetration tester and outline the five penetration testing phases, in addition to looking at some popular penetration testing tools that can be used to examine systems for vulnerabilities.**
- **Responsibilities of a Penetration Tester (Pen Testing)**
- **A penetration tester is responsible for finding security vulnerabilities, including determining which penetration testing method (Gupta, 2021) is best suited to the situation. This is a challenging task that requires advanced skills and knowledge.**
- **A penetration tester needs to be familiar with different hacking techniques and have in-depth network security knowledge. They must also know how to use various tools to assess the target system's security posture.**

The Five Phases of Penetration Testing

There are five penetration testing phases: reconnaissance, scanning, vulnerability assessment, exploitation, and reporting. Let's take a closer look at the 5 Penetration Testing phases.

1. Reconnaissance

The first penetration testing phase is reconnaissance. In this phase, the tester gathers as much information about the target system as they can, including information about the network topology, operating systems and applications, user accounts, and other relevant information. The goal is to gather as much data as possible so that the tester can plan an effective attack strategy.

Reconnaissance can be categorized as either active or passive depending on what methods are used to gather information (Braithwaite, 2022). Passive reconnaissance pulls information from resources that are already publicly available, whereas active reconnaissance involves directly interacting with the target system to gain information. Typically, both methods are necessary to form a full picture of the target's vulnerabilities.

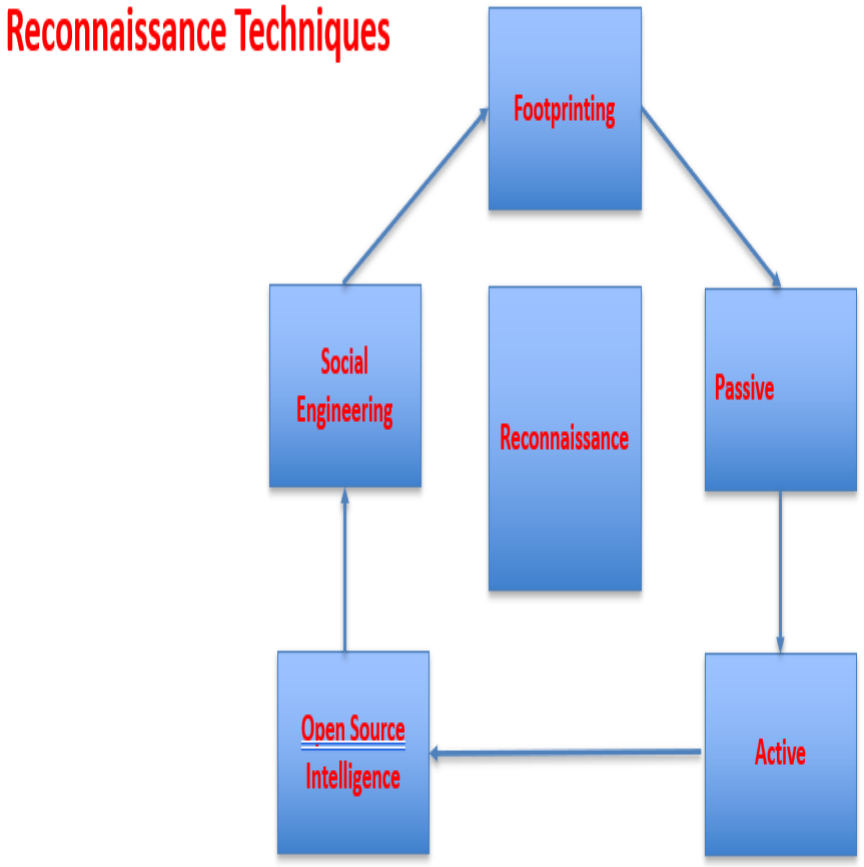
Tishk International University
Faculty of Applied Science
Cybersecurity Department

Reconnaissance Techniques

Key Theory Points:
Reconnaissance techniques:
- Passive: gather info without touching systems
- Active: directly probe systems

Problem & Solution:
Q: Using LinkedIn to collect company info: active or passive?
A: Passive.

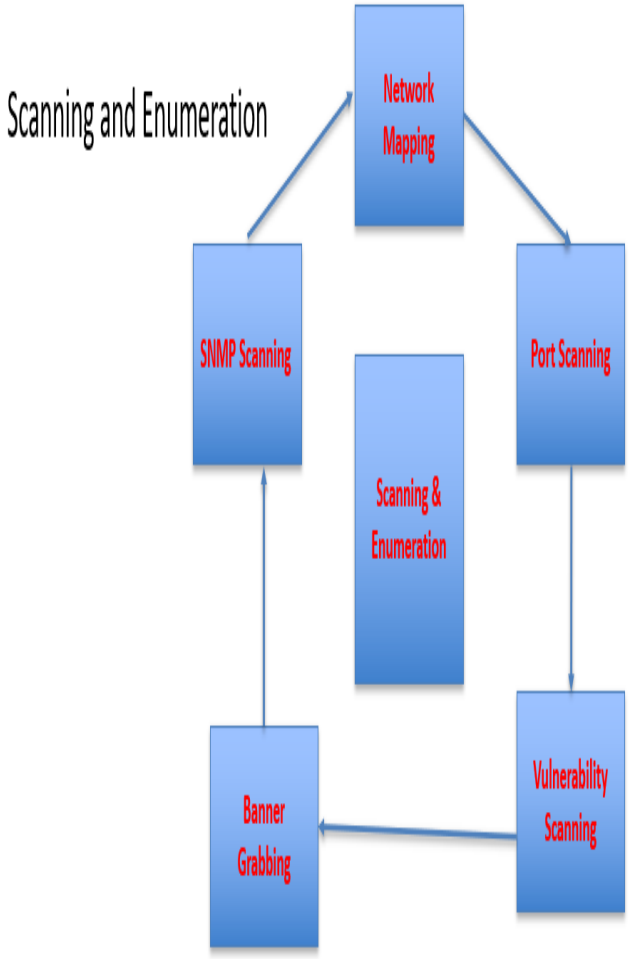
Homework (HW):
HW:
1. List 3 passive recon tools.
2. Explain one active recon tool and its ethical use.



2. Scanning

Once all the relevant data has been gathered in the reconnaissance phase, it's time to move on to scanning. In this penetration testing phase, the tester uses various tools to identify open ports and check network traffic on the target system. Because open ports are potential entry points for attackers, penetration testers need to identify as many open ports as possible for the next penetration testing phase.

This step can also be performed outside of penetration testing; in those cases, it's referred to simply as vulnerability scanning and is usually an automated process. However, there are drawbacks to only performing a scan without a full penetration test—namely, scanning can identify a potential threat but cannot determine the level at which hackers can gain access (Agio, 2022). So, while scanning is essential for cybersecurity, it also needs human intervention in the form of penetration testers to reach its full potential.



3. Vulnerability Assessment

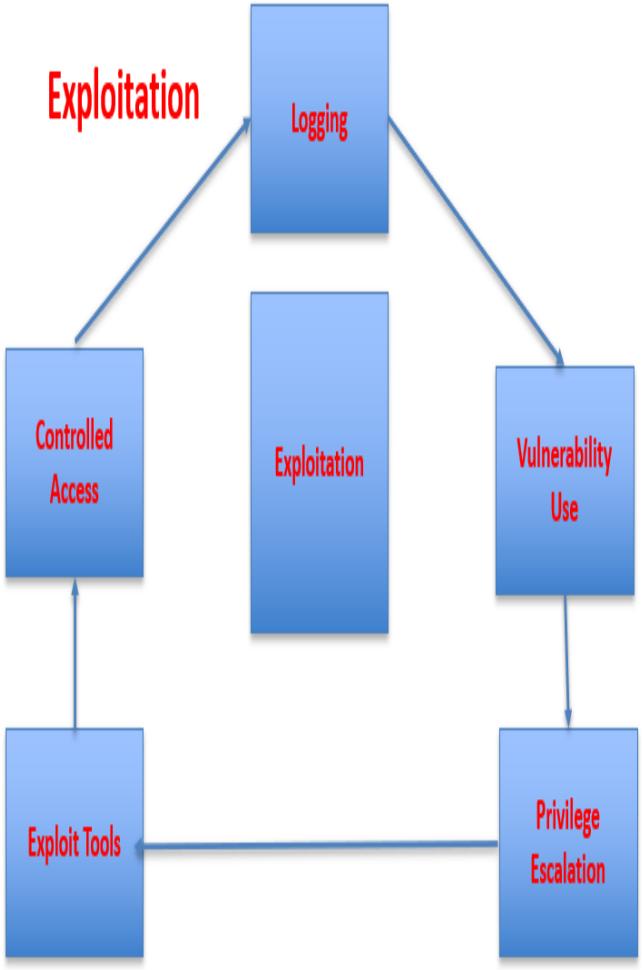
The third penetration testing phase is vulnerability assessment, in which the tester uses all the data gathered in the reconnaissance and scanning phases to identify potential vulnerabilities and determine whether they can be exploited. Much like scanning, vulnerability assessment is a useful tool on its own but is more powerful when combined with the other penetration testing phases.

When determining the risk of discovered vulnerabilities during this stage, penetration testers have many resources to turn to. One is the National Vulnerability Database (NVD), a repository of vulnerability management data created and maintained by the U.S. government that analyzes the software vulnerabilities published in the Common Vulnerabilities and Exposures (CVE) database. The NVD rates the severity of known vulnerabilities using the Common Vulnerability Scoring System (CVSS).

4. Exploitation

Once vulnerabilities have been identified, it's time for exploitation. In this penetration testing phase, the penetration tester attempts to access the target system and exploit the identified vulnerabilities, typically by using a tool like Metasploit to simulate real-world attacks.

This is perhaps the most delicate penetration testing phase because accessing the target system requires bypassing security restrictions. Though system crashes during penetration testing are rare, testers must still be cautious to ensure that the system isn't compromised or damaged (Basu, 2022).



5. Reporting

Once the exploitation phase is complete, the tester prepares a report documenting the penetration test's findings. The report generated in this final penetration testing phase can be used to fix any vulnerabilities found in the system and improve the organization's security posture.

Building a penetration testing report requires clearly documenting vulnerabilities and putting them into context so that the organization can remediate its security risks. The most useful reports include sections for a detailed outline of uncovered vulnerabilities (including CVSS scores), a business impact assessment, an explanation of the exploitation phase's difficulty, a technical risk briefing, remediation advice, and strategic recommendations (Sharma, 2022).

Popular Penetration Testing Tools

There are many different penetration testing tools available, and each has its strengths and weaknesses. Some of the most popular include:

- **Nmap.** Nmap is a powerful network scanning tool that can scan for open ports and services. It also includes features for identifying vulnerable applications.
- **Metasploit.** Metasploit is a vulnerability exploitation tool. It includes a library of exploits for a variety of programs and operating systems, as well as a wizard that can assist penetration testers in capitalizing on known vulnerabilities.
- **Wireshark.** Wireshark is a network analysis tool that can capture packet data from a network and decode it into a readable form. This can be useful for identifying malicious traffic or sensitive information being transmitted over a network.
- **Burp Suite.** Burp Suite is an all-in-one web application security testing tool. It can scan websites for vulnerabilities, manipulate requests and responses, and intercept traffic between the client and server.

These are just a few of the many penetration testing tools available (Aboagye, 2021). As a penetration tester, it's essential to be familiar with as many of them as possible so that you can choose the right tool for each penetration testing phase.

Tishk International University
Faculty of Applied Science
Cybersecurity Department

1. Quick overview Penetration testing: a *controlled, simulated attack* on an information system to discover, validate, and quantify vulnerabilities and their business impact, then report prioritized fixes.

2. Phases — function, methods, outputs

Phase A — Reconnaissance (Passive & Active)

Function: collect information about the target (organization, IP ranges, domains, email addresses, public code, employee names) to find likely attack vectors.

Typical activities & tools: OSINT queries, WHOIS, DNS enumeration, search engines, social media, job postings, public code repos, Shodan, passive DNS, email harvesting.

Outputs: asset list, domain/IP map, likely services, public-facing app endpoints, user lists, attack hypotheses.

Role in sequence: defines scope and vectors for Scanning & Exploitation.

Phase B — Scanning (Active discovery & enumeration)

Function: probe assets to discover open ports, services, versions, misconfigurations, and initial vulnerabilities.

Typical activities & tools: Nmap (port/service scan), banner grabbing, vulnerability scanners (Nessus, OpenVAS), application fingerprinting, web crawlers, and directory brute force.

Outputs: host/service inventory, vulnerability candidates, prioritized targets for exploitation.

Role in sequence: converts Recon hypotheses into concrete technical targets with measurable risk.

Phase D — Post-Exploitation (Pivoting & persistence)

Function: investigate how far an attacker can go: lateral movement, data exfiltration proof, persistence, privilege escalation, and cleanup.

Typical activities: credential harvesting, pivoting (proxying through compromised hosts), mapping internal networks, exfiltration simulation, persistence tests (but not permanent changes), data access demonstration.

Outputs: attack paths from initial foothold to critical assets, list of accessed sensitive data (sample), attack graph.

Role in sequence: quantifies business impact and supports remediation prioritization.

Phase E — Reporting (Deliverables & remediation)

Function: produce an actionable report: executive summary, technical details, evidence, risk ratings, remediation steps, retest recommendations.

Typical contents: executive summary, scope/timeline, methodology, full findings (vuln descriptions, PoC), risk prioritization, suggested fixes, verification plan.

Role in sequence: communicates results to stakeholders and drives remediation; may trigger retest.

3. Sequence process (flow + loops)

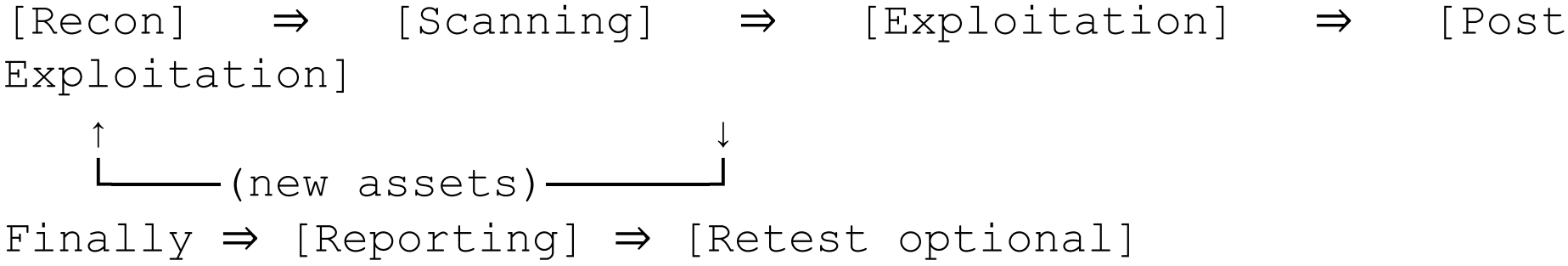
Canonical linear flow:

Reconnaissance → Scanning → Exploitation → Post-Exploitation → Reporting

But in practice it's iterative:

- Recon informs Scanning; Scanning produces new Recon items (e.g., a discovered subdomain).
- Exploitation may reveal new internal assets that require fresh Recon/Scanning (pivoting).
- Post-Exploitation can update the attack graph and re-prioritize other targets.
- Reporting may request retest cycles.

Graphically (text):



Tishk International University
Faculty of Applied Science
Cybersecurity Department

4. Mathematical models you can use (and why)

Below are practical formal models used to reason about pen tests: discovery probability, scanner throughput, exploit success probability, risk scoring, and a simple Markov chain for process transitions.

4.1 Probability of discovering a vulnerability (effort model)

A common model: assume scanning/testing attempts are Poisson in time/effort. The probability P_d of discovering at least one vulnerability as a function of testing **effort** E (e.g., hours, number of probes) can be modeled as:

$$P_d(E) = 1 - e^{-kE}$$

where $k > 0$ is the *discovery rate* (per unit effort) — depends on skill, tooling, and asset complexity.

Interpretation: diminishing returns — more effort increases discovery probability but with decreasing marginal gains.

Example (step-by-step arithmetic): let $k = 0.20$ per hour and effort $E = 10$ hours.

1.Compute exponent: $-kE = -0.20 \times 10 = -2.0$.

2.Compute $e^{-2.0}$ .Using standard value $e^{2.0} \approx 7.389056098$,so $e^{-2.0} = 1/7.389056098 \approx 0.135335283$.

3.Compute $P_d = 1 - 0.135335283 = 0.864664717$.

So $P_d \approx 0.8647$ (%86.47 ≈)after 10 hours.

4.2 Scanning throughput and estimated time to full coverage

If you have Nassets and each asset requires on average $t$hours to scan thoroughly, total scanning time $T$is:

$$T = N \times t$$

If scans can be parallelized across m workers/tools:

$$T_{\text{parallel}} = \frac{N \times t}{m}$$

Example: $N = 120$hosts, $t = 0.5$hours/host, $m = 4$parallel scanners.
Compute $N \times t = 120 \times 0.5 = 60.0$hours.
Then $T_{parallel} = 60.0/4 = 15.0$hours.

4.3 Probability of successful exploitation (logistic / sigmoid model)

Exploit success often depends on several continuous factors (exploitability, required privileges, network conditions). A convenient model is logistic:

$$P_s = \frac{1}{1 + e^{-(\alpha X + \beta Y + \gamma)}}$$

where:

- X = exploitability score (0..1),
- Y = privilege requirement factor (higher = harder; you can use $1 - \text{priv\_req}$ to represent ease),
- α, β, γ are fitted constants.

Simple numeric example: choose $\alpha = 4, \beta = 3, \gamma = -2$. Let $X = 0.7$ (highly exploitable), $Y = 0.6$ (moderate privilege requirement but converted to ease).

Tishk International University
Faculty of Applied Science
Cybersecurity Department

Simple numeric example: choose $\alpha = 4$, $\beta = 3$, $\gamma = -2$. Let $X = 0.7$(highly exploitable), $Y = 0.6$(moderate privilege requirement but converted to ease).

Compute the linear term:

1.$\alpha X = 4 \times 0.7 = 2.8.$

2.$\beta Y = 3 \times 0.6 = 1.8.$

3.Sum with γ: $2.8 + 1.8 - 2 = 2.6.$

4.Compute $e^{-2.6}$ .First 2.6exponent: $e^{2.6} \approx 13.46373804$so $e^{-2.6} = 1/13.46373804 \approx 0.074270.$

5.Then $P_s = 1/(1 + 0.074270) = 1/1.074270 \approx 0.931$(%93.1 ≈)

So high exploitability and moderate privilege requirement yield a high success probability in this parameterization.

4.4 Risk scoring (expected loss model)

A standard approach: **Risk = Likelihood × Impact**.

Let:

•L= likelihood that a vulnerability is exploited (use $P_s$or other estimate).

•I= impact (monetary loss, or normalized 0..1).

Then expected loss $EL$is:

$$EL = L \times I$$

If you measure Impact in monetary terms ($), $EL$is $ expected loss.

Example: Suppose $L = 0.4$and $I = \$250{,}000$.

Compute $EL = 0.4 \times 250{,}000 = 100{,}000$. So expected loss $100,000.

Prioritization: rank findings by ELor normalized score.

4.5 Vulnerability prioritization using a weighted score

You can compute a composite priority score S:

$$S = w_1 \cdot Exploitability + w_2 \cdot Impact + w_3 \cdot Exposure$$

where weights $w_i$sum to 1 and each component is normalized to [0,1].

Example weights: $w_1 = 0.5, w_2 = 0.3, w_3 = 0.2$ .If Exploitability=0.8, Impact=0.7, Exposure=0.6:

$1.0.5 \times 0.8 = 0.40.$

$2.0.3 \times 0.7 = 0.21.$

$3.0.2 \times 0.6 = 0.12.$

4.Sum $S = 0.40 + 0.21 + 0.12 = 0.73.$

Priority score 0.73 (on 0–1 scale).

Tishk International University
Faculty of Applied Science
Cybersecurity Department

4.6 Simple Markov chain for phase transitions (process reliability)

Model phases as states: Recon (R), Scan (S), Exploit (E), Post (P), Report (T — terminal). Some transitions might fail and return to earlier states (e.g., exploitation fails → more scanning or recon). Let the non-terminal states be R,S,E,P and terminal T. Define a transition matrix P(rows sum to 1). Example qualitative matrix:

$$P = \begin{array}{c|ccccc} & R & S & E & P & T \\ \hline R & 0.1 & 0.8 & 0.0 & 0.0 & 0.1 \\ S & 0.0 & 0.1 & 0.7 & 0.0 & 0.2 \\ E & 0.0 & 0.2 & 0.1 & 0.6 & 0.1 \\ P & 0.0 & 0.0 & 0.0 & 0.2 & 0.8 \\ T & 0.0 & 0.0 & 0.0 & 0.0 & 1.0 \end{array}$$

You can analyze this chain to find expected number of steps to termination, absorption probabilities, or steady-state behavior. (Computation uses linear algebra — compute fundamental matrix $N = (I - Q)^{-1}$ where Q is transitions among transient states R,S,E,P.)

5. Practical metrics to collect during a pen test

- **Time per phase:** hours in Recon, Scanning, Exploitation, Post.
- **Coverage:** % of assets scanned vs. scope.
- **Discovery probability estimate:** $P_d(E)$ using effort model.
- **Exploit success rate:** fraction of vulnerabilities validated (PoC) divided by total candidates.
- **Mean Time to Compromise (MTTC):** average time until initial compromise.
- **Attack path depth:** hops from perimeter to crown-jewel asset.
- **Expected Loss (EL)** per finding.
- **Remediation ETA & verification status** after fixes.

Tishk International University
Faculty of Applied Science
Cybersecurity Department

6. Example end-to-end numeric scenario (compact)

Scope: 50 externally facing hosts. Team: 2 testers. Avg scan time per host $t = 0.4$h. Discovery rate $k = 0.15$per hour. You spend 16 hours total.

1. Scanning parallel time:
   1. $N \times t = 50 \times 0.4 = 20.0$hours.
   2. With $m = 2$parallel workers: $T_{parallel} = 20.0/2 = 10.0$hours.
2. Discovery probability after total effort $E = 16$h and $k = 0.15$:
   1. $-kE = -0.15 \times 16 = -2.4$.
   2. $e^{-2.4}$ .Compute $e^{2.4} \approx 11.02317638$,so $e^{-2.4} = 1/11.02317638 \approx 0.090717953$.
   3. $P_d = 1 - 0.090717953 = 0.909282047.\%90.93 \approx \rightarrow$
3. Suppose you find 20 candidate vulns and successfully exploit 12:
   1. Exploit success rate = $12/20 = 0.6 = 60\%$.
4. For one important vuln, exploitability score 0.9, impact $500,000, using logistic model with simple mapping $L = P_s \approx 0.9$,
   1. $EL = 0.9 \times 500{,}000 = 450{,}000$expected loss — high priority.

7. Good practices / operational rules

- **Keep scope and rules of engagement (RoE) documented.**
- **Evidence safety:** collect screenshots, logs, timestamps, and avoid destructive actions.
- **Credential handling:** never leave persistent credentials or backdoors.
- **Communication:** daily standups for long tests; immediate reporting for critical findings (out-of-band).
- **Retesting:** after fixes, do a focused retest to validate remediation.
- **Threat model alignment:** map pen test findings to existing threat models and business assets.

8. What to put in the report (and a short template)

1. **Executive summary:** scope, top 3 risks, overall risk posture.
2. **Scope & methodology:** rules of engagement, timeframe, tools, limitations.
3. **Findings (for each):**
    1. Title, CVE/reference (if any)
    2. Technical description & PoC (screenshots/logs)
    3. Exploitability score and computed P_s
    4. Impact estimate I
    5. Expected loss $EL = P_s \times I$
    6. Priority (using composite score S)
    7. Remediation steps (detailed, code/config)
    8. Suggested verification steps
4. **Attack graph:** a map from perimeter to critical assets (include path lengths).
5. **Metrics & time accounting:** per-phase hours, coverage, success rates.
6. **Appendices:** raw scanner output, command logs, responsible disclosures.

9. Final tips (concise)

- Use the $P_d(E) = 1 - e^{-kE}$ model to plan testing effort vs. coverage.
- Convert technical findings into **expected monetary impact** to help decision makers prioritize.
- Treat pen tests as *continuous* security activity — each test increases knowledge (and thus reduces some k uncertainty).
- Automate scanning for broad coverage; use manual, expert work for exploitation and post-exploitation.

Tishk International University
Faculty of Applied Science
Cybersecurity Department

Phase B — Scanning (Active discovery & enumeration)

Function: probe assets to discover open ports, services, versions, misconfigurations, and initial vulnerabilities.

Typical activities & tools: Nmap (port/service scan), banner grabbing, vulnerability scanners (Nessus, OpenVAS), application fingerprinting, web crawlers, directory brute force.

Outputs: host/service inventory, vulnerability candidates, prioritized targets for exploitation.

Role in sequence: converts Recon hypotheses into concrete technical targets with measurable risk.

Phase C — Exploitation

Function: attempt to abuse identified vulnerabilities to gain unauthorized access or escalate privileges (proof of concept).

Typical activities & tools: exploit frameworks (Metasploit), manual exploit chaining, SQL injection, XSS, RCE, config misuse, credential reuse.

Outputs: proof of compromise (screenshots, shells), exploited vulnerability details, root/privilege level reached, timestamps.

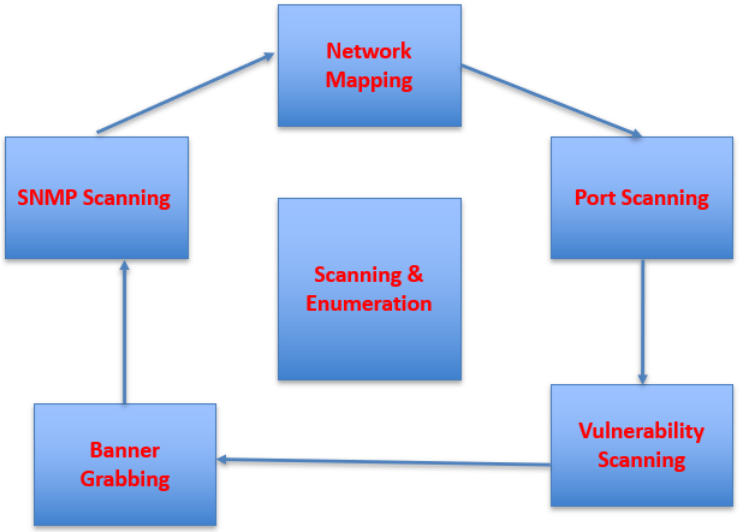
Role in sequence: validates vulnerabilities and shows real business impact.

Tishk International University
Faculty of Applied Science
Cybersecurity Department

Scanning and Enumeration

Key Theory Points:
Scanning: detect open ports/services.
Enumeration: extract detailed info (usernames, shares)

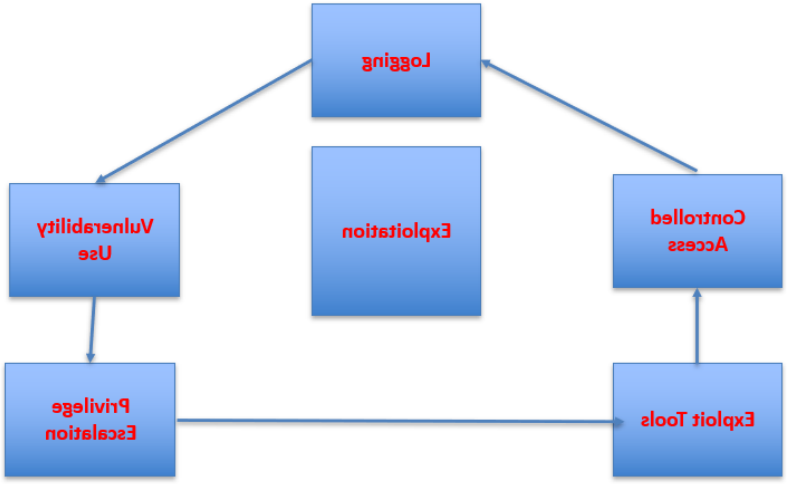
Problem & Solution:
Q: Extracting usernames from a server is which step?
A: Enumeration.



Homework (HW):
HW:
1. Explain difference between scanning and enumeration.
2. List 2 common scanning tools.

Tishk International University
Faculty of Applied Science
Cybersecurity Department

Exploitation



Key Theory Points:
Exploitation: using vulnerabilities to gain access.
Must have authorization and document carefully.

Problem & Solution:
Q: Gaining admin privileges after finding a bug is called?
A: Privilege Escalation.

Homework (HW):
HW:
1. Describe one controlled exploit scenario.
2. Discuss ethical reporting steps.

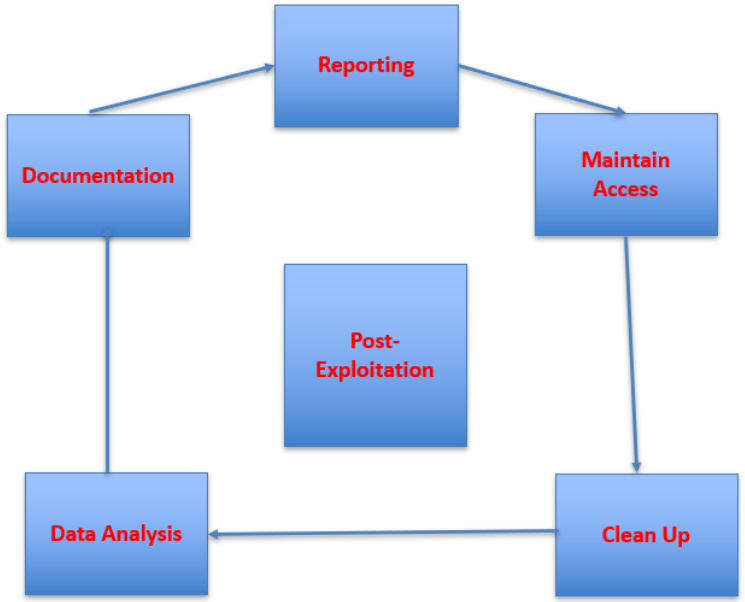
Tishk International University
Faculty of Applied Science
Cybersecurity Department

Post-Exploitation

Key Theory Points:
Post-Exploitation: maintain access for testing, clean trac

Problem & Solution:
Q: Why is clean-up important?
A: Prevent leaving vulnerabilities behind.

Homework (HW):
HW:
1. Explain why post-exploitation phase is critical ethicall
2. Suggest one reporting template item.



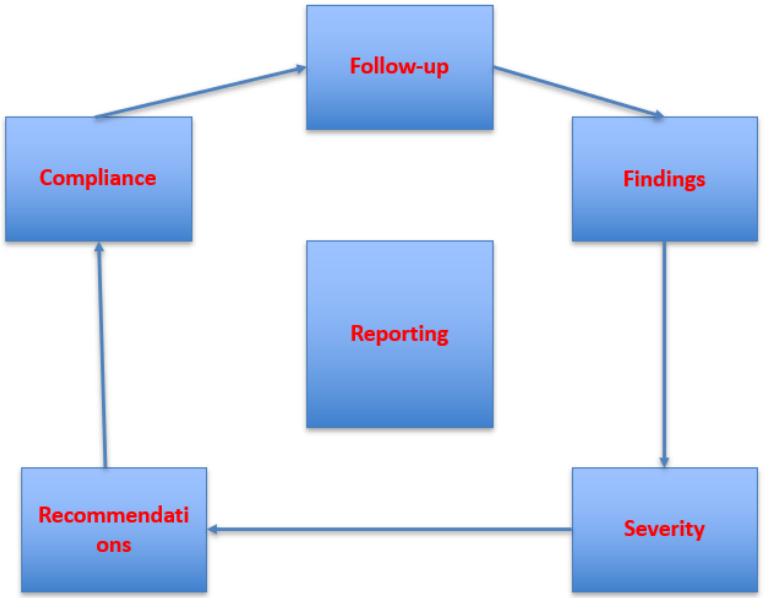
Tishk International University
Faculty of Applied Science
Cybersecurity Department

Reporting & Remediation

Key Theory Points:
Reporting: report all findings to authorized parties and provide remediation steps.

Problem & Solution:
Q: What is main purpose of pen-test reports?
A: Help organization remediate vulnerabilities.

Homework (HW):
HW:
1. Create a mini-report template with 3 key sections.
2. Explain why severity ratings are important.



Tishk International University
Faculty of Applied Science
Cybersecurity Department

Tools for Ethical Hacking

Key Theory Points:
Common tools: Nmap, Metasploit, Wireshark, Burp Suite, Nessus.
Choose tools legally and ethically.

Problem & Solution:
Q: Which tool is used for network scanning?
A: Nmap.

Homework (HW):
HW:
1. Pick 2 tools and describe an ethical use-case.
2. Explain legal considerations for each.

Tishk International University
Faculty of Applied Science
Cybersecurity Department

Challenges & Best Practices

Key Theory Points:
Challenges: legal limits, system complexity, evolving threats.
Best practices: authorization, documentation, skill updates, ethical code.

Problem & Solution:
Q: Name one common challenge ethical hackers face?
A: Evolving threats.

Homework (HW):
HW:
1. List 3 best practices for ethical hackers.
2. Explain how following a code of ethics reduces risks.

References

- Books: Ethical Hacking and Penetration Testing (Rehman), Hacking: The Art of Exploitation (Erickson)
- Laws: CFAA (USA), GDPR (EU)
- Tools: Nmap, Metasploit, Wireshark official docs

References

Aboagye, M. (2021, February 17). 13 online pentest tools for reconnaissance and exploit search. Geekflare. *https://geekflare.com/reconnaissance-exploit-search-tools/*

Agio. (2022, June 8). Vulnerability scanning vs. penetration testing. *https://agio.com/vulnerability-scanning-vs-penetration-testing/*

Basu, S. (2022, June 29). 7 penetration testing phases for web applications: A detailed account. Astra. *https://www.getastra.com/blog/security-audit/penetration-testing-phases/*

Brathwaite, S. (2022, January 6). Active vs passive cyber reconnaissance in information security. Security Made Simple. *https://www.securitymadesimple.org/cybersecurity-blog/active-vs-passive-cyber-reconnaissance-in-information-security*

Graham, K. (2021, June 28). What is cybersecurity compliance? An industry guide. BitSight. *https://www.bitsight.com/blog/what-is-cybersecurity-compliance*

Gupta, A. (2022, February 3). Determining the appropriate penetration testing method. Forbes. *https://www.forbes.com/sites/forbestechcouncil/2022/02/03/determining-the-appropriate-penetration-testing-method/*

Sharma, S. (2022, July 13). Penetration testing report or VAPT report by Astra Security. Astra. *https://www.getastra.com/blog/security-audit/penetration-testing-report/*