T1 Examination Solutions Key (ODD 2023: Ethical Hacking and Prevention)

1. **[CO1: Understanding – Level 2: 4 Marks]** Describe the ethical guidelines that a penetration tester should adhere to when conducting security assessments on targets with reference to EC-Council standards and Indian laws.
   [At least 6 points from both may be provided by student]

Code of Ethics by EC-Council

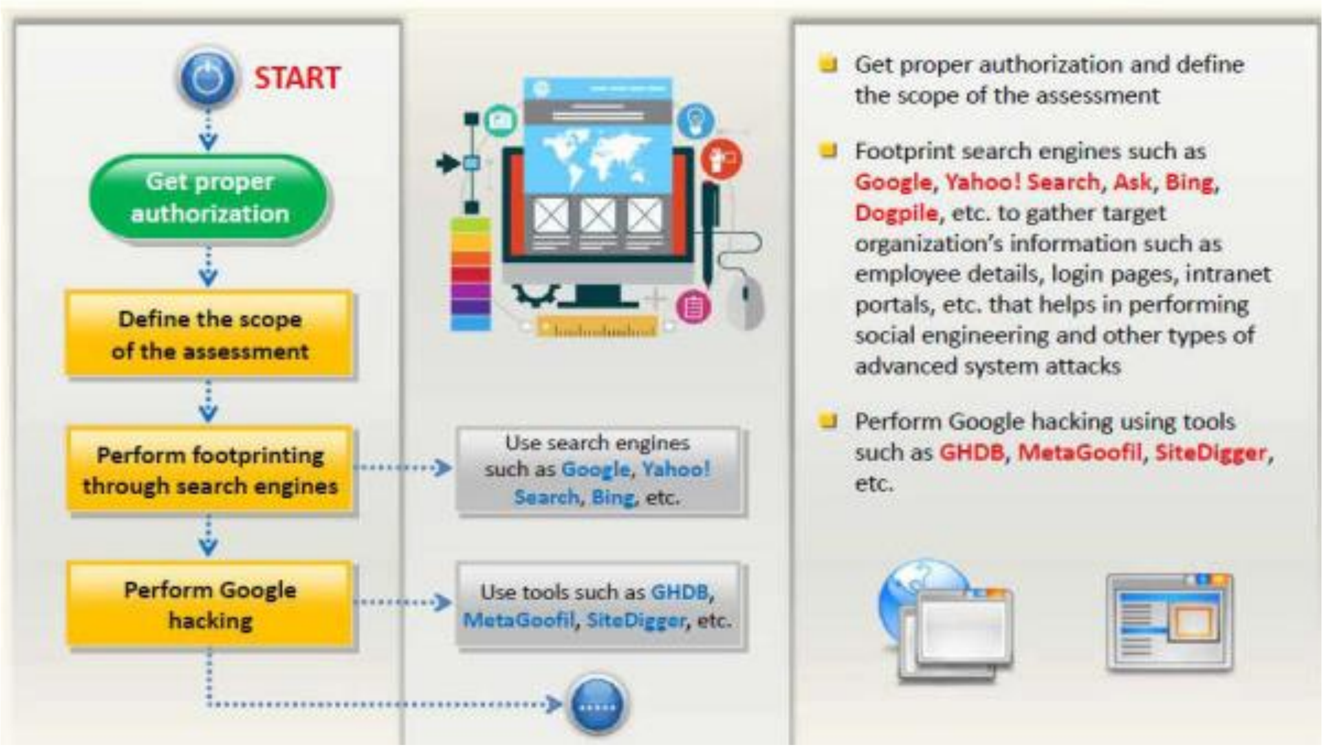
- Keep private and confidential information gained in your professional work, (in particular as it pertains to client lists and client personal information). Not collect, give, sell, or transfer any personal information (such as name, e-mail address, Social Security number, or other unique identifier) to a third party without client prior consent.
- Protect the intellectual property of others by relying on your own innovation and efforts, thus ensuring that all benefits vest with its originator.
- Disclose to appropriate persons or authorities' potential dangers to any ecommerce clients, the Internet community, or the public, that you reasonably believe to be associated with a particular set or type of electronic transactions or related software or hardware.
- Provide service in your areas of competence, being honest and forthright about any limitations of your experience and education. Ensure that you are qualified for any project on which you work or propose to work by an appropriate combination of education, training, and experience.
- Never knowingly use software or process that is obtained or retained either illegally or unethically.
- Not to engage in deceptive financial practices such as bribery, double billing, or other improper financial practices.
- Use the property of a client or employer only in ways properly authorized, and with the owner's knowledge and consent.
- Disclose to all concerned parties those conflicts of interest that cannot reasonably be avoided or escaped.
- Ensure good management for any project you lead, including effective procedures for promotion of quality and full disclosure of risk.
- Add to the knowledge of the e-commerce profession by constant study, share the lessons of your experience with fellow EC-Council members, and promote public awareness of benefits of electronic commerce.
- Conduct oneself in the most ethical and competent manner when soliciting professional service or seeking employment, thus meriting confidence in your knowledge and integrity.
- Ensure ethical conduct and professional care at all times on all professional assignments without prejudice.
- Not to neither associate with malicious hackers nor engage in any malicious activities.
- Not to purposefully compromise or allow the client organization's systems to be compromised in the course of your professional dealings.
- Ensure all penetration testing activities are authorized and within legal limits.
- Not to take part in any black hat activity or be associated with any black hat community that serves to endanger networks.
- Not to be part of any underground hacking community for purposes of preaching and expanding black hat activities.
- Not to make inappropriate reference to the certification or misleading use of certificates, marks or logos in publications, catalogues, documents or speeches.
- Not convicted in any felony, or violated any law of the land.

IT Act 200

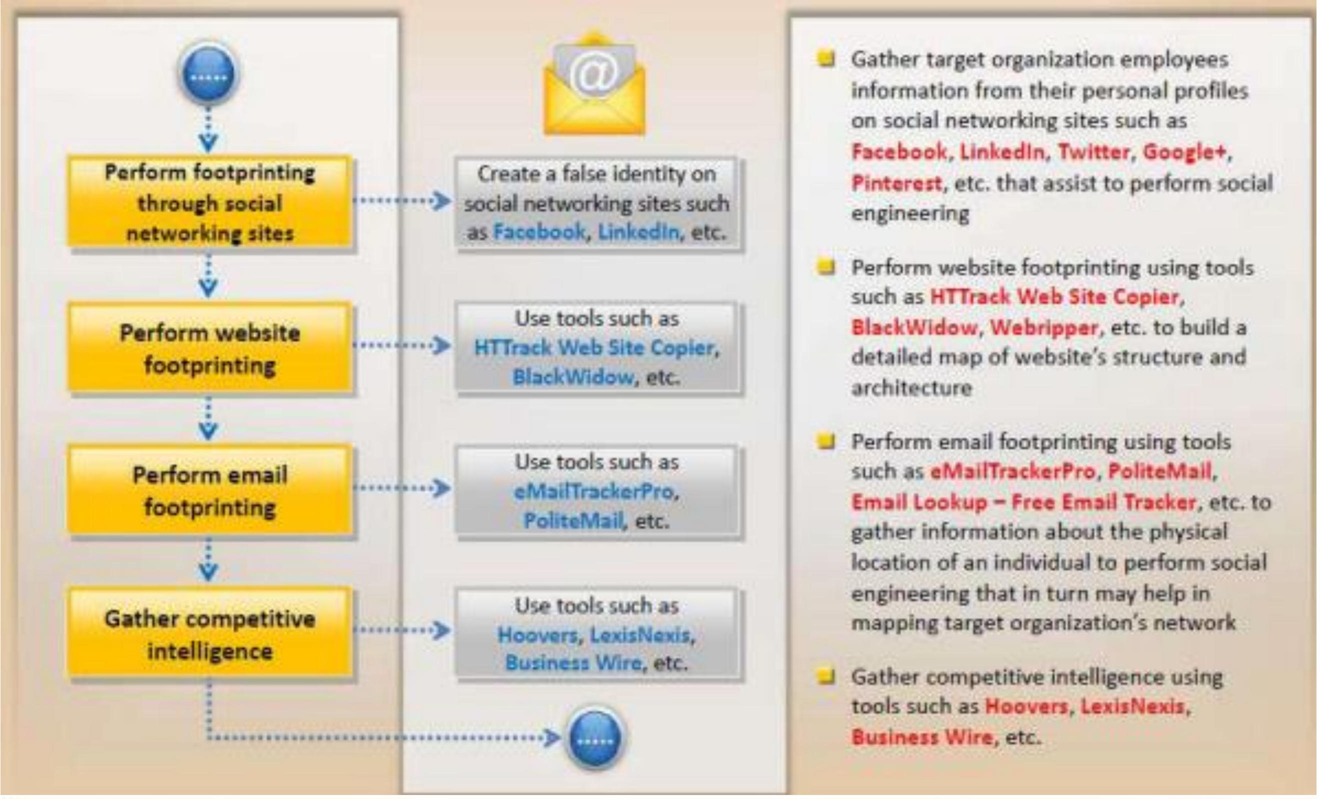
- The Information Technology Act came into effect in the year 2000.
- The act came into force with the object to provide legality to electronic data exchange
- and such other e-transactions (particularly E-Commerce)

- Sec 43 of the IT Act, 2000, in case a person tends to damage, modify, destroy or extract any information that can be harmful if used in an ill-manner by entering into the computer or network of any person without prior permission of such person would be liable to be penalised for any damage caused.
- Sec 43 A of the same Act in case an ethical hacker or any person having authorised access to vital information shall be penalized in case he is not successful in protecting such data/information.
- Sec 66 of the Information Technology Act, 2000 includes fraud and dishonest people indulging in acts mentioned as offences above under the provision of Sec 43 of the said Act to be punished with 3 years of imprisonment.
- In India, the Information Technology Law puts into question and penalizes people hacking through a network or computer system without proper permission/authorisation.
- However, the obvious flaw is that the law only provides safeguards ethical hacking only if he is appointed by the government and not those others who have authorised access to hacking but are not government-appointed [as mentioned under Sec 84].

2. <u>**[CO1: Understanding – Level 2: 4 Marks]** List and outline the flow of foot-printing methodology by highlighting the tools and process followed at each level.</u>


START
Get proper authorization
Define the scope of the assessment
Perform footprinting through search engines
Perform Google hacking
Use search engines such as Google, Yahoo! Search, Bing, etc.
Use tools such as GHDB, MetaGoofil, SiteDigger, etc.

- Get proper authorization and define the scope of the assessment
- Footprint search engines such as Google, Yahoo! Search, Ask, Bing, Dogpile, etc. to gather target organization's information such as employee details, login pages, intranet portals, etc. that helps in performing social engineering and other types of advanced system attacks
- Perform Google hacking using tools such as GHDB, MetaGoofil, SiteDigger, etc.



Perform footprinting through social networking sites

Create a false identity on social networking sites such as Facebook, LinkedIn, etc.

Perform website footprinting

Use tools such as HTTrack Web Site Copier, BlackWidow, etc.

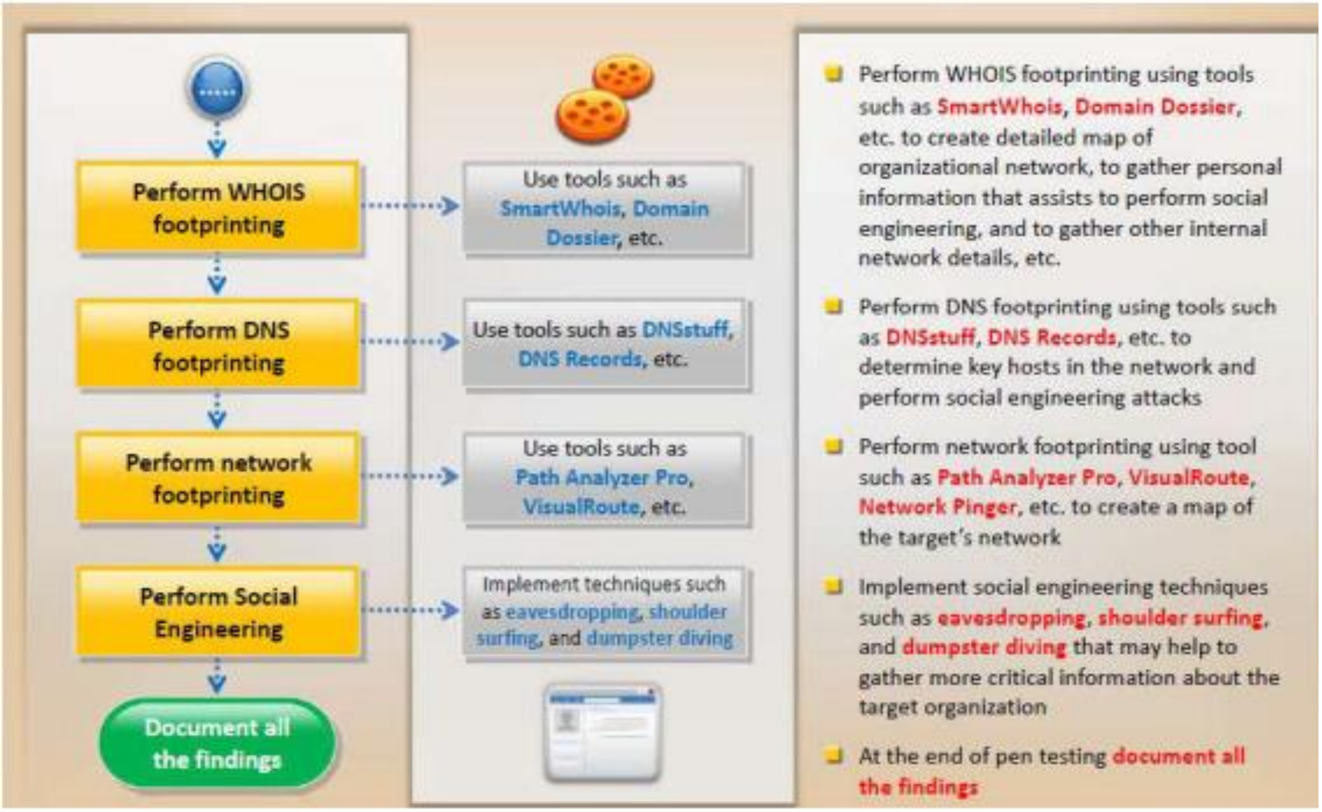
Perform email footprinting

Use tools such as eMailTrackerPro, PoliteMail, etc.

Gather competitive intelligence

Use tools such as Hoovers, LexisNexis, Business Wire, etc.

- Gather target organization employees information from their personal profiles on social networking sites such as Facebook, LinkedIn, Twitter, Google+, Pinterest, etc. that assist to perform social engineering
- Perform website footprinting using tools such as HTTrack Web Site Copier, BlackWidow, Webripper, etc. to build a detailed map of website's structure and architecture
- Perform email footprinting using tools such as eMailTrackerPro, PoliteMail, Email Lookup – Free Email Tracker, etc. to gather information about the physical location of an individual to perform social engineering that in turn may help in mapping target organization's network
- Gather competitive intelligence using tools such as Hoovers, LexisNexis, Business Wire, etc.



Perform WHOIS footprinting

Use tools such as SmartWhois, Domain Dossier, etc.

Perform DNS footprinting

Use tools such as DNSstuff, DNS Records, etc.

Perform network footprinting

Use tools such as Path Analyzer Pro, VisualRoute, etc.

Perform Social Engineering

Implement techniques such as eavesdropping, shoulder surfing, and dumpster diving

Document all the findings

- Perform WHOIS footprinting using tools such as SmartWhois, Domain Dossier, etc. to create detailed map of organizational network, to gather personal information that assists to perform social engineering, and to gather other internal network details, etc.
- Perform DNS footprinting using tools such as DNSstuff, DNS Records, etc. to determine key hosts in the network and perform social engineering attacks
- Perform network footprinting using tool such as Path Analyzer Pro, VisualRoute, Network Pinger, etc. to create a map of the target's network
- Implement social engineering techniques such as eavesdropping, shoulder surfing, and dumpster diving that may help to gather more critical information about the target organization
- At the end of pen testing document all the findings

3. **[CO2: Apply – Level 3: 3 x 4 = 12 Marks]** Assume that you are a network security administrator for a large organization, and

3a) you suspected that someone is conducting stealthy and XMAS scan on your network. Explain the concept of stealth and XMAS scana in network security, and describe how in general it will be conducted using **NMAP** tool and how you can detect and respond to such scans.
Stealth Scan: [1 Mark]

A stealth scan, also known as a "stealthy scan" or "half-open scan," is a network reconnaissance technique used by attackers to gather information about a target network without triggering intrusive alerts or raising suspicions. The primary goal of a stealth scan is to identify open ports on a target system and potentially identify services running on those ports. Its working procedure is as follows:

- The attacker sends TCP SYN packets to target ports on the victim system.
- If the port is closed, the victim responds with a TCP RST packet, indicating that the port is not open.
- If the port is open, the victim does not respond with an RST packet, allowing the attacker to infer that the port is open without completing the TCP handshake.

XMAS Scan: [1 Mark]

An XMAS scan is a variation of the stealth scan. In an XMAS scan, the attacker sends a TCP packet with specific TCP flags set in a unique pattern. The flags set are the FIN, URG, and PUSH flags, which are typically not used together in legitimate network traffic. Its working procedure is as follows:

- The attacker sends TCP packets with the FIN, URG, and PUSH flags set to target ports.
- If the port is closed, the victim should respond with an RST packet.
- If the port is open, the victim may not respond, allowing the attacker to identify open ports.

Using NMAP for Stealth and XMAS Scans: [1 Mark]

NMAP is a widely used network scanning tool that can be configured to perform stealthy and XMAS scans. Attackers often use NMAP due to its flexibility and extensive feature set. To perform these scans with NMAP, an attacker might use command-line options like "-sS" for a SYN scan (stealth scan) or "--scanflags" to set specific TCP flags for an XMAS scan.

Detecting and Responding to Stealth and XMAS Scans: [1 Mark]

The following are some steps to detect and respond to stealth and XMAS scans:

1. Network Monitoring: Implement robust network monitoring solutions that can detect unusual traffic patterns, including a high number of SYN packets without corresponding ACK packets or packets with unusual flag combinations like those in an XMAS scan.
2. Firewall Rules: Configure firewall rules to block or limit incoming packets with unusual flag combinations. For example, drop incoming packets with the FIN, URG, and PUSH flags set.
3. Intrusion Detection Systems (IDS): Deploy an IDS to detect and alert on suspicious scanning activities. IDS systems can analyze traffic patterns and flag potential attacks.
4. Logging and Analysis: Maintain detailed logs of network traffic and regularly analyze them for signs of scanning activities. Look for patterns such as a large number of connection attempts from a single IP address.
5. Incident Response: If a stealth or XMAS scan is detected then investigate it promptly to determine the source IP address and take appropriate action, such as blocking the attacker’s IP address, updating firewall rules, and reporting the incident to relevant authorities if necessary.
6. Patch and Update: Ensure that the organization systems are up-to-date with security patches to minimize vulnerabilities that attackers might attempt to exploit.
7. Education and Training: Train the staff to recognize and report suspicious network activities. User awareness is a crucial component of network security.

3b) you received reports of excessive network traffic and suspected a Distributed Denial of Service (DDoS) attack. Illustrate how you can use **Hping3** to conduct a simple DdoS simulation test on your own network, and discuss the countermeasures you should take when performing such tests.

A DDoS attack can be conducted by an individual or group of individuals — attackers — write some virus(es)/ malwares/ trojans etc. and distribute such software and propagate worldwide using various media like e-mails, torrents, warez, cracked software, key generators, malicious websites etc.

The hping3 tool allows one to send manipulated packets including size, quantity, and fragmentation of packets in order to overload the target and bypass or attack firewalls. Hping3 can be useful for security or capability testing purposes. By using it, one can test firewalls effectiveness and if a server can handle a big amount of connections. The following illustrate the use of hping3 for network security testing.

Step 1: Install hping3 in linux

```
$ sudo apt install hping3 -y
```

Step 2: start conducting DDoS on webserver

```
$ sudo hping3 -S --flood -V -p <target IP Address>
```

where

sudo: gives needed privileges to run hping3.
hping3: calls hping3 program.
-S: specifies SYN packets.
–flood: replies will be ignored and packets will be sent as fast as possible.
-V: Verbosity.
-p 80: port 80, one can replace this number for the service one want to attack.
target IP (some IP address ex. 192.168.1.10).

Flood Using SYN Packets Against Port 80

SYN packets include the connection synchronization confirmation request.
The following example shows a SYN attack against lacampora.org:

```
$ sudo hping3 lacampora.org -q -n -d 120 -S -p 80 --flood --rand-source
```

Flood from a Fake IP Address With hping3

With hping3 one can also attack oner targets with a fake IP. In order to bypass a firewall, one can even clone oner target IP itself, or any allowed address one may know (one can achieve it for example with Nmap or a sniffer to listen to established connections).

The syntax is the following:

```
$sudo hping3 -a <FAKE IP> <target> -S -q -p 80
```

In the example below, I replaced my real IP address with the IP 190.0.174.10.

```
$ sudo hping3 -a 190.0.174.10 190.0.175.100 -S -q -p 80
```

3c) you have accessed a password dump consisting of LM and NTLM hashes. Explain the difference between LM and NTLM hashes. Illustrate how to recognize the type of hash available in a dump using **hashcat** tool, and command using the **John** the Ripper tool for conducting dictionary attacks for password cracking.

LM (LAN Manager) and NTLM (NT LAN Manager) are two different password hashing algorithms used primarily in Windows operating systems for authentication purposes. the primary differences between LM and NTLM hashes are their security, character set support, and usage. NTLM is considered more secure and is widely used in modern Windows environments, while LM is deprecated due to its significant security weaknesses. It's important to note that both LM and NTLM hashes have limitations and should be replaced with more secure authentication methods whenever possible. The following are the details of the differences: [2 Marks]

1. Hashing Algorithm:
   - LM Hash: LM hash is an older, less secure password hashing algorithm. It splits the user's password into two 7-character halves, converts them to uppercase, and then hashes each half separately.
   - NTLM Hash: NTLM hash is a more secure and modern password hashing algorithm. It uses a more complex process to hash the user's password.
2. Security:
   - LM Hash: LM hashes are considerably less secure compared to NTLM hashes. They have several vulnerabilities, including vulnerability to brute-force and precomputed attacks due to their fixed length and limited character set.

- NTLM Hash: NTLM hashes are more secure than LM hashes and are resistant to many of the attacks that affect LM hashes. However, NTLM hashes are still vulnerable to certain types of attacks, such as dictionary attacks.

3. Character Set:
   - LM Hash: LM hashes only support uppercase alphanumeric characters (A-Z, 0-9) and some special characters, such as !@#$%^&*()_-+=|{}[]:";'<>?,./\.
   - NTLM Hash: NTLM hashes support a wider character set, including uppercase and lowercase letters, numbers, and a broader range of special characters.
4. Compatibility:
   - LM Hash: LM hashes are still supported for backward compatibility in some Windows systems, but their use is deprecated due to security concerns.
   - NTLM Hash: NTLM hashes are widely used in modern Windows systems for authentication.
5. Length:
   - LM Hash: LM hashes are always 16 characters in length.
   - NTLM Hash: NTLM hashes can vary in length but are typically 32 characters in length.
6. Usage:
   - LM Hash: Historically used in older versions of Windows (Windows 95, 98, and NT) and in some legacy systems.
   - NTLM Hash: Used in modern Windows systems for various authentication protocols, including NTLM and NTLMv2.

Hashcat to identify hash type [1 mark]

Step 1: Create a text file (let's call it `hashes.txt`) and paste the hash you want to identify into this file.
Step 2: Open a terminal or command prompt and navigate to the directory where Hashcat is installed.
Step 3: Identify the Hash type by running the following command to identify the hash type:

```
hashcat -m 0 -a 0 --example-hashes
```

- The `-m` option specifies the hash type mode, and in this case, `-m 0` means Hashcat will display a list of supported hash types.
- The `-a` option specifies the attack mode, and `-a 0` specifies "Straight."

Hashcat will display a list of supported hash types along with their numerical identifiers. Look for the identifier that corresponds to the hash type one wants to identify. Once the numerical identifier is identified then one can use it to recognize the hash type. For example, if one can see the identifier 1000 corresponds to LM has, then one can conclude that the hash is of type LM hash.

John the ripper to crack passwords [1 Mark]

John’s single crack mode:

```
$ john --single --format=raw-sha1 crack.txt
```

Here is the command to run John in dictionary mode using the wordlist.

```
$ john --wordlist=/usr/share/wordlists/rockyou.txt --format=raw-sha1 crack.txt
```