2 MARK ANSWERS – ETHICAL HACKING

1. **Outline penetration testing phases.**

Penetration testing (pen testing) involves simulating cyberattacks to identify security vulnerabilities in a system, network, or application.

1. **what are common types of malware, and how can organizations protect against malware attacks?**

* Virus
* Worms
* Trojan horse

Protection against Malware attacks

* Use Antivirus & Anti-Malware
* **Keep Software Updated**
* **Enable Firewalls**

**3.Difference between Ethical Hacking and Cybersecurity**

|  |  |
| --- | --- |
| **Ethical Hacking** | **Cybersecurity** |
| * The practice of legally breaking into computers and networks to identify security vulnerabilities before malicious hackers can exploit them. * Identify and exploit security flaws ethically. * Penetration testing, social engineering, vulnerability assessments. | * The process of protecting systems, networks, and data from cyber threats, unauthorized access, and attacks. * Prevent, detect, and respond to attacks. * Firewalls, antivirus, risk management, incident response. |

**4.State the different types of Hackers.**

1. White Hat Hackers
2. Black Hat Hackers
3. Grey Hat Hackers

**5.Compare vulnerability versus penetration test.**

|  |  |
| --- | --- |
| **Vulnerability** | **Penetration test** |
| * A security process that identifies, analyzes, and prioritizes weaknesses in a system without exploiting them. * Detect and prioritize vulnerabilities. * Eg. Running a vulnerability scanner like Nessus. | * A simulated cyberattack where ethical hackers exploit vulnerabilities to evaluate the security of a system. * Test security defenses and assess real risk. * Eg. Using Metasploit to exploit a detected vulnerability |

**6.List the various HTTP methods with description.**

1. GET
2. POST
3. PATCH
4. PUT
5. DELETE

**7.How foot printing is carried out using social engineering techniques?**

Footprinting is the process of gathering information about a target system, and social engineering techniques can be used to extract sensitive details from individuals.

Methods of Social Engineering for Footprinting:

* **Phishing**
* **Pretexting**

**8.List the types of scans that can be used for port scanning.**

* TCP Connect Scan
* SYN Scan (Half-Open Scan)
* UDP Scan
* ACK Scan
* FIN Scan
* **NULL Scan**
* XMAS Scan
* Idle Scan

**9.Define Enumeration.**

**Enumeration** is the process of actively gathering detailed information about a target system, such as usernames, shared resources, network services, and system vulnerabilities. It is a crucial step in ethical hacking and penetration testing.

**10.List the tools used for NTP enumeration.**

* Nmap
* **Ntpq**
* Ntpdate
* ntpdump