EH ASSIGNMENT 2

Q.1 What are the types of hacker?

ANS. Script Kiddies

Black hat hackers

White hat hackers

Gray hat hackers

Green hat hackers

Blue hat hackers

Red hat hackers

Q.2 Explain in brief - Ethical hacking and cyber security.

ANS. EHTHICAL HACKING

Ethical hacking involves an authorized attempt to gain unauthorized access to a computer system, application, or data. Carrying out an ethical hack involves duplicating strategies and actions of malicious attackers. This practice helps to identify security vulnerabilities which can then be resolved before a malicious attacker has the opportunity to exploit them.

KEY CONCPETS

1. Stay legal. Obtain proper approval before accessing and performing a security assessment.

2. Define the scope. Determine the scope of the assessment so that the ethical hacker's work remains legal and within the organization's approved boundaries.
3. Report vulnerabilities. Notify the organization of all vulnerabilities discovered during the assessment. Provide remediation advice for resolving these vulnerabilities.
4. Respect data sensitivity. Depending on the data sensitivity, ethical hackers may have to agree to a non-disclosure agreement, in addition to other terms and conditions required by the assessed organization.

CYBER SECURITY

Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as information technology security or electronic information security. The term applies in a variety of contexts, from business to mobile computing, and can be divided into a few common categories.

· Network security is the practice of securing a computer network from intruders, whether targeted attackers or opportunistic malware.

· Application security focuses on keeping software and devices free of threats. A compromised application could provide access to the data its designed to protect. Successful security begins in the design stage, well before a program or device is deployed.

· Information security protects the integrity and privacy of data, both in storage and in transit.

· Operational security includes the processes and decisions for handling and protecting data assets. The permissions users have when accessing a network and the procedures that determine how and where data may be stored or shared all fall under this umbrella.

· Disaster recovery and business continuity define how an organization responds to a cyber-security incident or any other event that causes the loss of operations or data. Disaster recovery policies dictate how the organization restores its operations and information to return to the same operating capacity as before the event. Business continuity is the plan the organization falls back on while trying to operate without certain resources.

· End-user education addresses the most unpredictable cyber-security factor: people. Anyone can accidentally introduce a virus to an otherwise secure system by failing to follow good security practices. Teaching users to delete suspicious email attachments, not plug in unidentified USB drives, and various other important lessons is vital for the security of any organization.

Q.3 Explain Foot printing Methodology

ANS. This is a passive information gathering process where we gather information about the target from social media, search engines, various websites etc. Information gathered includes name, personal details, geographical location detrails, login pages, intranet portals etc. Even some target specific information like Operating system details, IP details, Netblock information, technologies behind web application etc can be gathered by searching through search engines.

Q.4 Find basic information using Google advance search operator and Pipl search

ANS. **"search term"** Use this to do an exact-match search.

- **OR** Search for this OR that. This will return results related to the two terms or both.
- **AND** Search for this AND that. This will only return results related to the two terms
- **–** Exclude a term or search phrase.
- ***** Acts as a wildcard and will match any word or phrase.
- **( )** Groups multiple terms or operators to control how the search is shown.
- **$** Search for prices.
- **define**: Displays the meaning of a word in a card-like result.

- **Cache:** Returns the most recent cached version of a web page (as long as the page is indexed).
- **filetype:** Shows results of a certain filetype (PDF, DOCX, TXT, PPT, etc.)
- **site:** Limit results to a specific website.
- **related:** Find sites related to another site.
- **intitle:** Find pages that contain a specific word in the title.
- **allintitle:** Like “intitle,” this finds web pages containing all of the specific words in the page title.
- **inurl:** Finds pages with a certain word in the URL.
- **allinurl:** Similar to “inurl,” this finds web pages containing all of the URL’s specific words.
- **intext:** Finds pages containing a specific word in the content.
- **allintext:** Finds results containing all of the specific words somewhere on the page.
- **AROUND(X)** This proximity search finds pages containing two words (or phrases) within X words of each other.
- **weather:** Finds the weather for a specific location.
- **stocks:** See stock information
- **map:** View map results for a location search.
- **movie:** Finds information about a specific movie.
- **in** Convert one unit into another (like currencies, weights, temperatures, etc.)

- **source:** Find news results from a certain source within Google News.

Q.5 Find vulnerability tool and check open port and service.

ANS. 1. Acunetix

2. beSECURE

3. Burp Suite

4. GFI Languard

5. Frontline

6. Nessus

7. Nexpose

8. Nmap

9. OpenVAS

10. Qualys Guard

11. Qualys Web Application Scanner

12. SAINT

13.Tenable

Open ports

1.Nmap

2.Wireshark

3.Angry IP Scanner

4.NetCat

5.Advanced IP Scanner