PTW ASSIGNMENT 1

Penetration Testing Workshop (CSE 3157)

Programme: B.Tech. (CSE - CYBERSECURITY) **Semester: 6th**
Last Date: 20/02/2025

Course Outcomes/ Subject Learning Outcomes	*Taxonomy Level	Question Number	Marks
Remember (kali) Linux Basic Commands, Understand Basic Concepts of Pen Test, Scripting (Python, Shell, Power shell, Ruby, Java)			
Develop Proficiency on exploitation tools Measploit, netcraft, Information gathering, DNS Reconnaissance, Searching EMail Address, Maltego, Port Scanning	L3.L4,L4	2,3	
Investigate Vulnerabilities: Nmap Scripting Engine, Web Application Scanning, Manual Analysis	L3.L4,L4	1	
Perform Pen Test on Vulnerable Machines (DC7, Kioptrix, Digital World.local, HackinOS, Sunset:Nightfall, Mumbai:1), Network traffic Capture, Burp Suite, Bypass Antivirus			
Perform and Evaluate Attacks: ARP Cache Poisoning, DNS Cache Poisoning, SSL Attack, Exploiting phpMyAdmin, Buffer Overflow, Password Attacks, SQL Injection, wireless attacks, social engineering toolkits			
Analysis Post Exploitation situation: Meterpreter, Create post Exploitation report, structure, objectives Export to Word, Client Side Exploitation			

*Bloom's taxonomy levels: Knowledge (L1), Comprehension (L2), Application (L3), Analysis (L4), Evaluation (L5), Creation (L6)

1. Run nmap with Metasploit to find target machines: Run nmap in your subnet with Metasploit environments. Use hosts and services commands. Find the ip addresses along with port addresses of the samba, smb, netbios applications.
2. Investigate with a domain and a person name with maltego. Domain Investigation: 1)Use Maltego CE to investigate "example.com". 2)Identify associated subdomains, email addresses, and related IPs. 3)Summarize your findings and create a report.
3. Name Investigation: 1)Use Maltego CE to investigate "Elon Musk". 2)Identify related social media accounts, companies, and email addresses. 3)Summarize your findings and create a report

PTW ASSIGNMENT 2

Penetration Testing Workshop (CSE 3157)

Programme: B.Tech. (CSE - CYBERSECURITY) **Semester: 6th**
Last Date: 28/02/2025

Course Outcomes/ Subject Learning Outcomes	*Taxonomy Level	Question Number	Marks
Remember (kali) Linux Basic Commands, Understand Basic Concepts of Pen Test, Scripting (Python, Shell, Power shell, Ruby, Java)			
Develop Proficiency on exploitation tools Measploit, netcraft, Information gathering, DNS Reconnaissance, Searching EMail Address, Maltego, Port Scanning	L3,L4,L5	1,2,3	
Investigate Vulnerabilities: Nmap Scripting Engine, Web Application Scanning, Manual Analysis			
Perform Pen Test on Vulnerable Machines (DC7, Kioptrix, Digital World.local, HackinOS, Sunset:Nightfall, Mumbai:1), Network traffic Capture, Burp Suite, Bypass Antivirus	L2,L3	4,5	
Perform and Evaluate Attacks: ARP Cache Poisoning, DNS Cache Poisoning, SSL Attack, Exploiting phpMyAdmin, Buffer Overflow, Password Attacks, SQL Injection, wireless attacks, social engineering toolkits			
Analysis Post Exploitation situation: Meterpreter, Create post Exploitation report, structure, objectives Export to Word, Client Side Exploitation			

*Bloom's taxonomy levels: Knowledge (L1), Comprehension (L2), Application (L3), Analysis (L4), Evaluation (L5), Creation (L6)

1. You have a website at http://172.30.16.191/dfw/.
   - Apply nikto to find the vulnerabilities of this website.
   - Find all image files (if available) in this website using nikto.
   - Find the versions of apache, php, and mod_perl of this website. Check any metasploit script available which can breach any specific versions of apache, php, and mod_perl
   - Find the applications running on any open ports in this website.
   - Use netcat to find strange ports in this website if available.
   - Find valid username if available using VRFY and netcat
   - Write a detail opinion about the vulnerabilities of this website.
2. Using ettercap demonstrate dns cache poisoning and arpspoofing.
3. misdirect your window system browsing to a different site.
4. Poison dns cache for www.facebook.com to different IP. Clear browsing history and cache before testing Explain step by step process and take screenshot from your window systems.
5. Write your IP, your window IP, and gateway IP. On your wireshark, show traffic from your window systems.

PTW ASSIGNMENT 3

Penetration Testing Workshop (CSE 3157)

Programme: B.Tech. (CSE - CYBERSECURITY) **Semester: 6th**
Last Date: 07/03/2025

Course Outcomes/ Subject Learning Outcomes	*Taxonomy Level	Question Number	Marks
Remember (kali) Linux Basic Commands, Understand Basic Concepts of Pen Test, Scripting (Python, Shell, Power shell, Ruby, Java)			
Develop Proficiency on exploitation tools Measploit, netcraft, Information gathering, DNS Reconnaissance, Searching EMail Address, Maltego, Port Scanning	L3-L6	1-5	
Investigate Vulnerabilities: Nmap Scripting Engine, Web Application Scanning, Manual Analysis			
Perform Pen Test on Vulnerable Machines (DC7, Kioptrix, Digital World.local, HackinOS, Sunset:Nightfall, Mumbai:1), Network traffic Capture, Burp Suite, Bypass Antivirus			
Perform and Evaluate Attacks: ARP Cache Poisoning, DNS Cache Poisoning, SSL Attack, Exploiting phpMyAdmin, Buffer Overflow, Password Attacks, SQL Injection, wireless attacks, social engineering toolkits			
Analysis Post Exploitation situation: Meterpreter, Create post Exploitation report, structure, objectives Export to Word, Client Side Exploitation			

*Bloom's taxonomy levels: Knowledge (L1), Comprehension (L2), Application (L3), Analysis (L4), Evaluation (L5), Creation (L6)

1. **Metasploit Basics** Explain the difference between a bind shell and a reverse shell in Metasploit. Provide an example of when you would use each.
2. **Searching for Exploits** Use Metasploit to search for vulnerabilities related to Ubuntu. Write the command you used and list any two exploits you found.
3. **Exploit Module Configuration** You have identified `ms08_067_netapi` as an exploit for a Windows XP target. Write the Metasploit commands to:
   - Use the exploit
   - Show the available options
   - Set the target IP to `192.168.1.100`
   - Set the payload to `windows/shell_reverse_tcp`
4. **Msfcli Execution** Using Msfcli, write a single command to exploit a Windows XP machine at `192.168.1.100` using `ms08_067_netapi` with a bind shell payload.
5. **Understanding Exploit Execution** After executing an exploit in Metasploit, explain what happens step by step when a reverse shell is used. Include:
   - What Metasploit does when you run `exploit`
   - How the target machine responds
   - How the attacker gains access

PTW ASSIGNMENT 4

Penetration Testing Workshop (CSE 3157)

Programme: B.Tech. (CSE - CYBERSECURITY) **Semester: 6th**
Last Date: 14/03/2025

Course Outcomes/ Subject Learning Outcomes	*Taxonomy Level	Question Number	Marks
Remember (kali) Linux Basic Commands, Understand Basic Concepts of Pen Test, Scripting (Python, Shell, Power shell, Ruby, Java)			
Develop Proficiency on exploitation tools Measploit, netcraft, Information gathering, DNS Reconnaissance, Searching EMail Address, Maltego, Port Scanning	L3-L5	1	
Investigate Vulnerabilities: Nmap Scripting Engine, Web Application Scanning, Manual Analysis	L3-L5	1	
Perform Pen Test on Vulnerable Machines (DC7, Kioptrix, Digital World.local, HackinOS, Sunset:Nightfall, Mumbai:1), Network traffic Capture, Burp Suite, Bypass Antivirus			
Perform and Evaluate Attacks: ARP Cache Poisoning, DNS Cache Poisoning, SSL Attack, Exploiting phpMyAdmin, Buffer Overflow, Password Attacks, SQL Injection, wireless attacks, social engineering toolkits	L3-L6	2-3	
Analysis Post Exploitation situation: Meterpreter, Create post Exploitation report, structure, objectives Export to Word, Client Side Exploitation			

*Bloom's taxonomy levels: Knowledge (L1), Comprehension (L2), Application (L3), Analysis (L4), Evaluation (L5), Creation (L6)

1. Scenario: You are part of the internal red team for XYZ Corp, assigned to test the security of their internal network. Your task is to simulate a penetration test that evaluates host discovery, service enumeration, and basic exploitation.
    - Perform a ping sweep to identify live hosts within the 192.168.10.0/24 subnet. Submit a script and brief findings.
    - Use Nmap to perform both SYN and UDP scans on one live host. Compare the results and discuss the usefulness of each method.
    - Identify all open ports on the live host using a stealth scan. Explain the stealth techniques used to avoid detection.
    - Attempt to identify running services and versions. Based on the findings, comment on potentially exploitable services.
    - For one service with a known vulnerability, write a Metasploit module configuration (not full exploit) using use, set, and show options to simulate the exploitation planning.
2. You've successfully compromised a user workstation inside a company. Now, you need to maintain access and pivot further. This assignment tests post-exploitation, MITM, and command/control skills.
    - Set up a Netcat listener on port 4444 to simulate receiving a reverse shell. Explain how this can be used in a real engagement.
    - Create a custom reverse shell payload using msfvenom and explain each parameter used. Include potential antivirus evasion tactics.
    - Perform an ARP spoofing attack to intercept traffic between the compromised host and the gateway. Document tools used and steps taken.

- Simulate a DNS tunneling setup. Explain how data could be exfiltrated through DNS and propose three defense mechanisms.
- Discuss how Metasploit's payloads differ (staged vs non-staged) and which one would be ideal in this scenario.

3. You're hired by a client to assess the security of their internal web application and remote login services.

   - Simulate a Blind SQL Injection against a login page. Demonstrate how you would infer information without seeing output directly. Include payloads used and expected behavior.
   - [1] Compare standard SQLi and blind SQLi with an example each. Explain why blind SQLi is harder to detect and exploit.
   - Use Hydra to perform a brute-force attack on SSH for a given IP address. Try at least two usernames with a wordlist and include command used and outcome.
   - Research and explain how altering the Windows hosts file could redirect all browser traffic from one domain to another. Demonstrate it using www.google.com as an example.

     Nessus (or simulate with reports if tool isn't available) to scan a system and identify at least three vulnerabilities. Explain what they are and how an attacker might exploit them.

---

[1] This is an additional task which is not covered in class. You may need to explore online resources.