Assesment of OS Vulnerabilities Using Armitage

[1]Dr.Kolhe Prakash R., [2]Shivpuje Prakash R.,[3]Dr.Deshmukh Nilesh K, [4]Dr.Parag Bhalchandra, [5]Rudrawar S.S.
[1]Associate Professor
[1]DR.BALASAHEB SAWANT KONKAN KRISHI VIDYAPEETH, DAPOLI, DIST. RATNAGIRI

***Abstract*— Armitage is a graphical cyber attack management tool for Metasploit project that visualizes target and recommends exploits. It is a free and open source network security tool. It is GUI front end for the Metasploit Framework developed by Raphael Mudge with the goal of helping security professionals better understand hacking and to help them realize the power of Metasploit. It was developed for cyber defense exercise. It is a free and open source security tool. It is built on top of Metasploit framework. Using Armitage user may launch scan and exploits, get exploit recommendations and use advanced feature of Metasploit framework.**

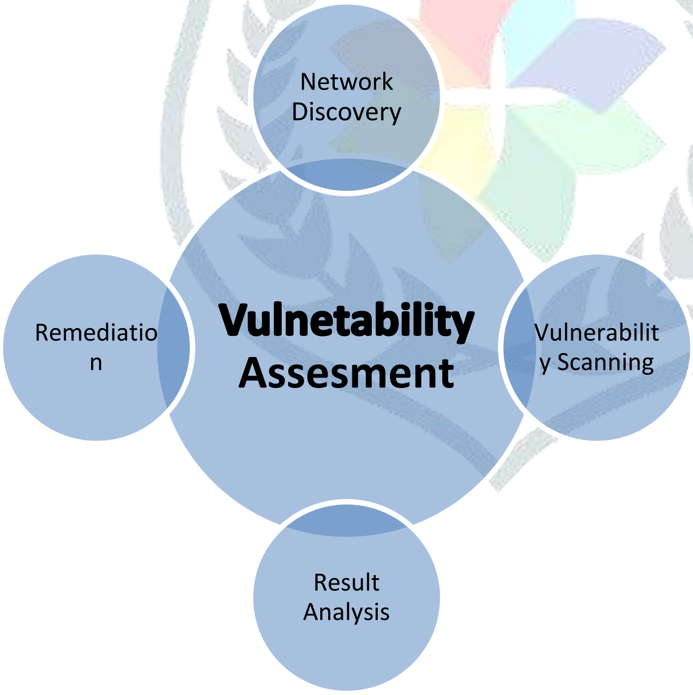
Keywords: *Armitage,Vulnerability,Exploit,Metasploit*

I. Introduction

Vulnerability assessment is also termed as vulnerability analysis. The method of recognizing, categorizing and characterizing the security holes among the network infrastructure, computers, hardware system and software etc is known as vulnerability analysis. Few examples of such vulnerabilities are like a misconfiguration of components in a network infrastructure, a defect or error in an operating system, any ambiguity in a marketable product. If vulnerabilities are found as a part of any vulnerability assessment then there is a need for vulnerability disclosure.

II. What is Vulnerability Assessment

Vulnerability assessment is the technique of identifying (discovery) and measuring security vulnerabilities (scanning) in a given environment. It is a comprehensive assessment of the information security position (result analysis). Further, it identifies the potential weaknesses and provides the proper mitigation measures (remediation) to either remove those weaknesses or reduce. Below diagram shows that how vulnerability assessment is done



III. Steps for Assessment of Security

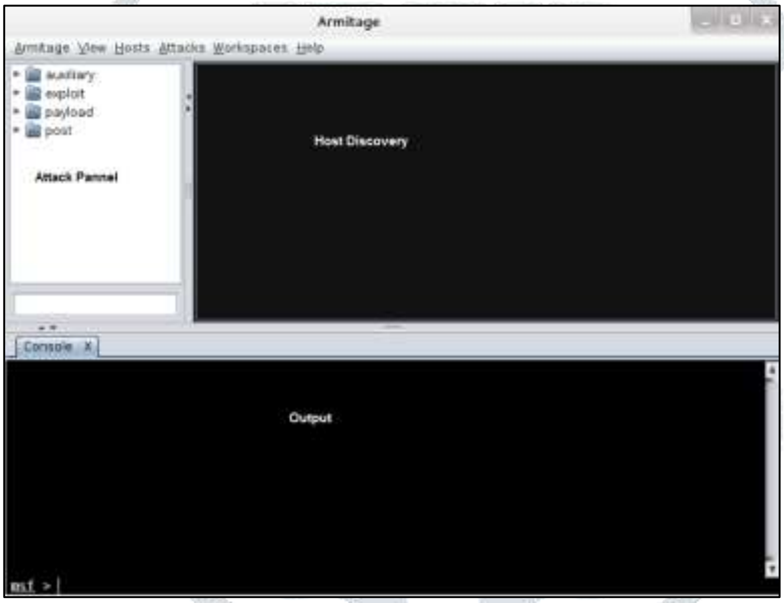
1) Spot and realize the approach of your industry.
2) Trace the systems, data, and applications that are exercised throughout the practice of the business.
3) Investigate the unseen data sources which can permit simple entry to the protected information.
4) Classify both the physical and virtual servers that run the necessary business applications.
5) Tracking all the existing security measures which are already implemented.
6) Inspect the network for any vulnerability.

IV. Vulnetability Assesment Tools

- NMAP
- **Armitage**
- Netsparker
- Secunia Personal Software Inspector
- Microsoft Baseline Security Analyzer
- Nexpose Community
- Tripwire IP360
- Wireshark
- Aircrack
- OpenVAS
- Retina CS Community
- Nessus Professional
- Nikto

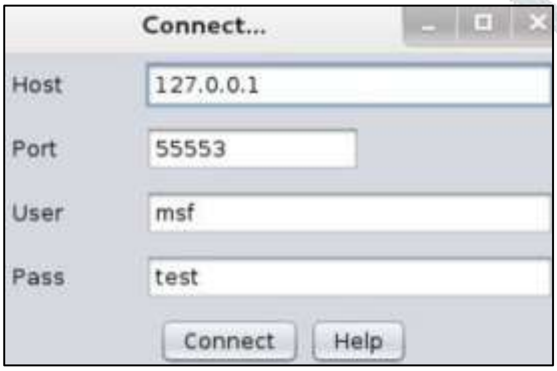
V. Launching of Armitage & Scanning

```
# service postgresql start
# armitage
```



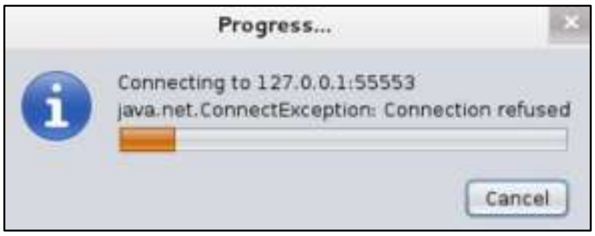
```
msf >
```

Figure1. Launching of Armitage



Host 127.0.0.1
Port 55553
User msf
Pass test

Figure2. Connecting Armitage

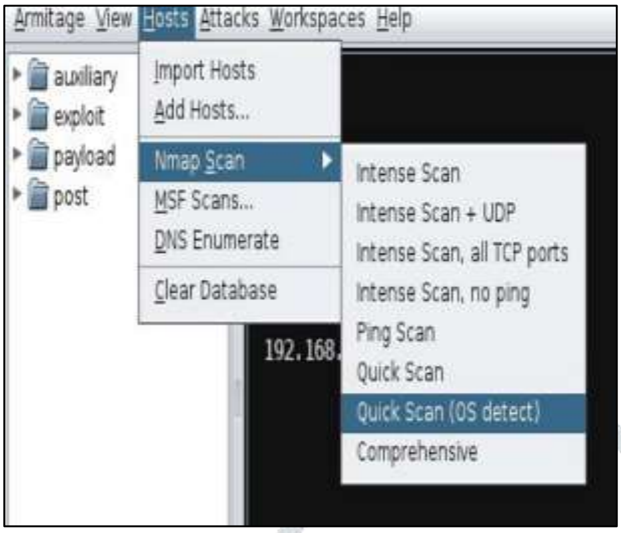


Connecting to 127.0.0.1:55553
java.net.ConnectException: Connection refused

Figure3. Progress

SCANNING OR HOST DISCOVERY

Click Hosts > Nmap Scan > Quick Scan (OS detect)



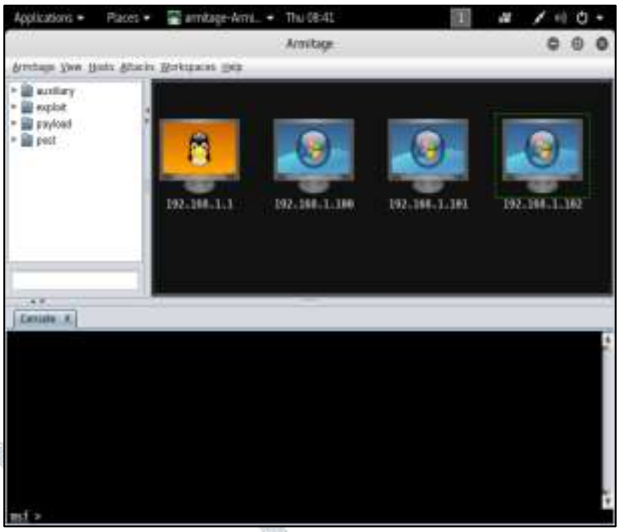
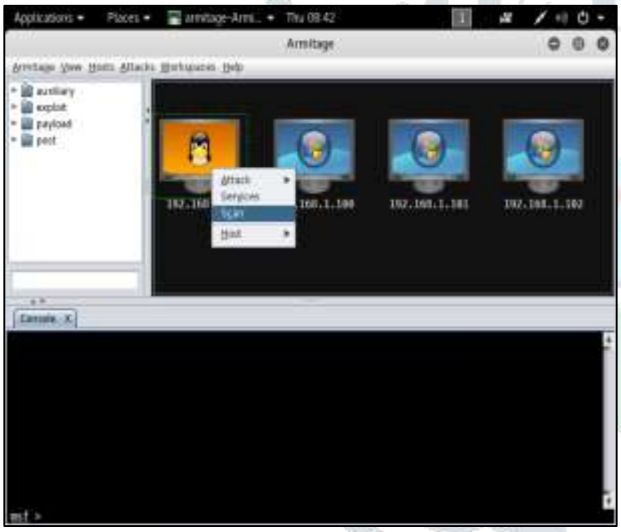
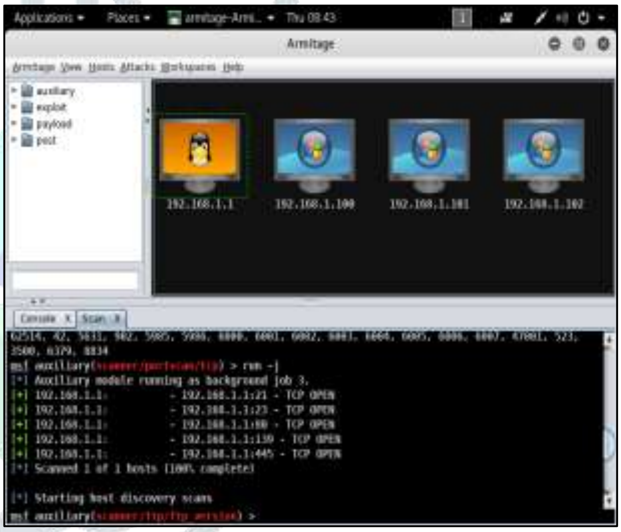


Figure4.Scanning or Host Discovery **Figure5. Scanning Result**





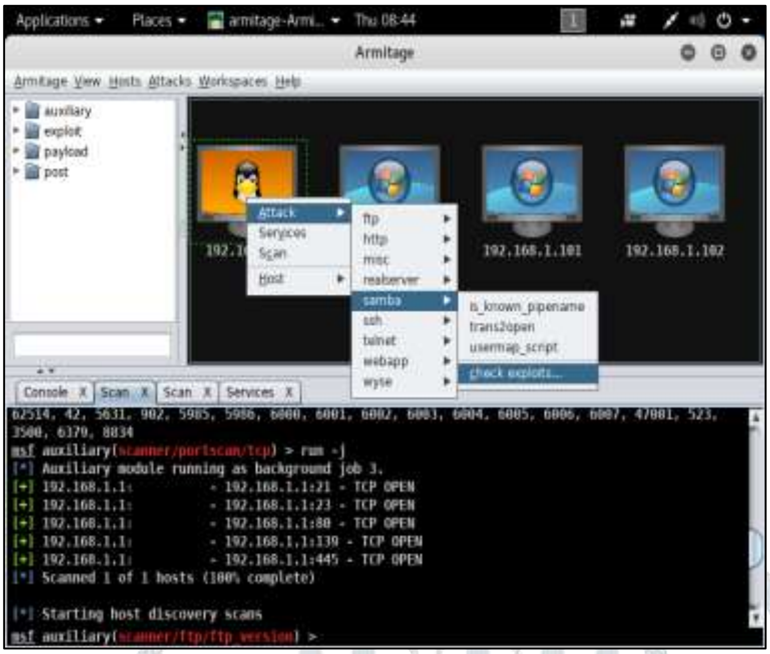
```
62514, 42, 5631, 902, 5985, 5900, 6000, 6001, 6002, 6003, 6004, 6005, 6006, 6007, 47001, 523,
3500, 6379, 8834
msf auxiliary(scanner/portscan/tcp) > run -j
[*] Auxiliary module running as background job 3.
[+] 192.168.1.1:          - 192.168.1.1:21 - TCP OPEN
[+] 192.168.1.1:          - 192.168.1.1:23 - TCP OPEN
[+] 192.168.1.1:          - 192.168.1.1:80 - TCP OPEN
[+] 192.168.1.1:          - 192.168.1.1:139 - TCP OPEN
[+] 192.168.1.1:          - 192.168.1.1:445 - TCP OPEN
[*] Scanned 1 of 1 hosts (100% complete)

[*] Starting host discovery scans
msf auxiliary(scanner/ftp/ftp_version) >
```

Figure6. Scanning Port **Figure7. Scanning Port Result**

From the above diagram we come to know that computer 192.168.1.1 comes with some open port numbers
21: FTP
23: Telnet
80: HTTP
139: NetBIOS
445: SMB

Below diagram shows that how to check for exploits whether our computer is vulnerable for particular exploit or not if vulnerable session will get opened else no session will be displayed.



```
62514, 42, 5631, 902, 5985, 5986, 6000, 6001, 6002, 6003, 6004, 6005, 6006, 6007, 47001, 523,
3500, 6379, 8834
msf auxiliary(scanner/portscan/tcp) > run -j
[*] Auxiliary module running as background job 3.
[+] 192.168.1.1:          - 192.168.1.1:21 - TCP OPEN
[+] 192.168.1.1:          - 192.168.1.1:23 - TCP OPEN
[+] 192.168.1.1:          - 192.168.1.1:80 - TCP OPEN
[+] 192.168.1.1:          - 192.168.1.1:139 - TCP OPEN
[+] 192.168.1.1:          - 192.168.1.1:445 - TCP OPEN
[*] Scanned 1 of 1 hosts (100% complete)

[*] Starting host discovery scans
msf auxiliary(scanner/ftp/ftp_version) >
```

Figure8. Check Exploits

VI. Conclusion

Here we come to know that if OS is vulnerable we can update as soon as possible. It is simplest and easiest way to check OS weakness and patching becomes easy if vulnerability found.

VII. References

[1] https://www.offensive-security.com

[2] https://ntrs.nasa.gov

[3] https://dl.packetstormsecurity.net

[4] https://www.kali.org

[5] https://www.metasploit.com

[6] https://www.rapid7.com/