A PROJECT REPORT ON

VULNERABILITY ASSESSMENT AND PENETRATION TESTING

The partial fulfilment of the requirements for completion of internship in the domain of Cyber Security is submitted.

Submitted by

KOLLU JAHNAVI

(Student)

Under The Guidance Of

VAISHNAVU CV

(Principal Cyber Security Engineer, Mentor,
VAPT, Ethical Hacker)

YHILLS EDUTECH

Noida Uttar Pradesh

PENETRATION TESTING ON WINDOWS

Executive Summary:

The penetration testing revealed several critical vulnerabilities within the Windows environment, including misconfigurations, weak authentication mechanisms, and exploitable software weaknesses. These vulnerabilities pose significant risks to the confidentiality, integrity, and availability of the organization's assets. Recommendations are provided to address these vulnerabilities and mitigate potential security threats effectively.

Introduction:

Penetration testing, often referred to as ethical hacking, is a proactive approach to assessing the security of IT systems by simulating real-world cyberattacks. Specifically focusing on Windows systems, this form of testing involves identifying vulnerabilities and potential exploits within the Windows operating system and related services. With Windows being one of the most widely used operating systems in both corporate and personal computing environments, ensuring its security is paramount in safeguarding sensitive data and maintaining operational integrity.

The purpose of conducting penetration testing on Windows systems is twofold: to uncover weaknesses that could be exploited by malicious actors and to provide organizations with actionable insights to strengthen their security defences. By systematically probing Windows servers, workstations, and associated network infrastructure, penetration testers can identify vulnerabilities such as misconfigurations, outdated software, weak access controls, and known security flaws.

Tools Used:

- nmap – To enumerate the target host and also to get vulnerability information of that host.
- Metasploit – The exploit tool.
- john – To crack the hash of the NTLM password.
- A few very basic GNU / Linux commands.

NON-TECHNICAL REPORT

Reconnaissance:

Reconnaissance can be categorized as either active or passive depending on what methods are used to gather information. Passive reconnaissance pulls information from resources that are already publicly available whereas active reconnaissance involves directly interacting with the target system to gain information. Typically, both methods are necessary to form a full picture of the target`s vulnerabilities.

Scanning:

Once all the relevant data has been gathered in the reconnaissance phase, it`s time to move on to scanning in this penetration testing phase, the tester uses various tools to identify open ports and check network traffic on the target system. Because open ports are potential entry points for attackers, penetration testers need to identify as many open port as possible for the next penetration phase.

This steps can also be performed outside of penetration testing, in those cases, it`s referred to simply as vulnerability scanning and is usually an automated process. However, there are drawbacks to only performing a scan without a full penetration test -namely scanning can identify a potential thread but cannot determine the level at which hackers can gain access. So, while scanning is essential for cybersecurity, it also needs human intervention in the form of penetration testers to reach its full potential.

Vulnerability Assessment:

The third penetration testing phase is vulnerability assessment, in which the tester uses all the data gathered in the reconnaissance and scanning phase to identify potential vulnerability and determine whether they can be exploited. Much like scanning vulnerability assessment is a useful tool on its own but is more powerful when combined with the other penetration testing phases.

When determining the risk of discovered vulnerabilities during this stage, penetration testers have many resources to turn to. One is the National Vulnerability Database (NVD), a repository of vulnerability management data created and maintained by the U.S govt that analyses the software vulnerability published in the Common Vulnerabilities and Exposures(CVE)database. The NVO refers the diversity of known vulnerabilities using the common Vulnerability Scoring System (CVSS).

Exploitation:

Once vulnerabilities have been identified, it`s time for exploitation. In this penetration testing phase, the penetration tester attempts to access the target system and exploit the identified vulnerabilities, typically by using a tool like Metasploit to simulate real-world attacks.

This is perhaps the most delicate penetration testing phase because accessing the target system requires bypassing security restrictions. Through system crashes during penetration testing are rare, testers must still be cautious to ensure that the system isn`t compromised or damaged.

Reporting:

Once the exploitation phase is complete, the tester prepares a report documenting the penetration test`s findings. The report generated in this final penetration testing phase can be used to fix any vulnerabilities found in the system and improve the organization`s security posture.

TECHNICAL REPORT

Methodology:

The methodology used to perform penetration testing is mentioned below which includes the phases of penetration testing.

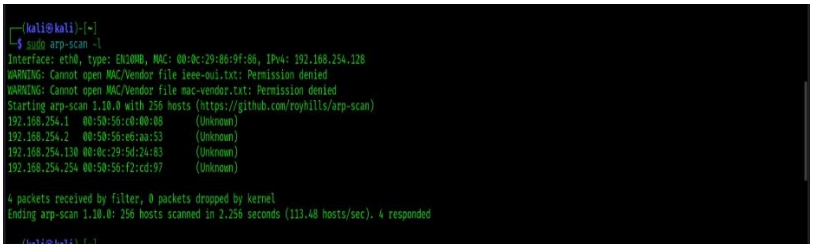
1. Reconnaissance
2. Scanning
3. Gaining access
4. Maintaining access
5. Clearing the tracks
6. Reporting

1.Reconnaissance:

Information gathering phase to understand the target environment, including network topology, operating systems, applications, and services running on the Windows systems. This phase is also named as Foot printing and information gathering phase. In this phase, hacker gathers or acquires the entire information about a target before launching an attack. These data covers important areas.

2. Scanning:

In this stage, the ethical hacker begins testing the networks and machines to identify potential attack surfaces. This involves gathering information on all machines, users, and services within the network using automated scanning tools.



Penetration testing typically undertakes three types of scans:

- Network Mapping
- Port Scanning
- Network Mapping

Network Mapping:

This involves discovering the network topology, including host information, servers, routers, and firewalls within the host network. Once mapped, white hat hackers can visualize and strategize the next steps of the ethical hacking process.

So the first thing to do is to enumerate the virtual machine to find out open and to what this machine is vulnerable. For this I used nmap with the options to scan version numbering(-sV). And an important one in this case, --script=Vuln.

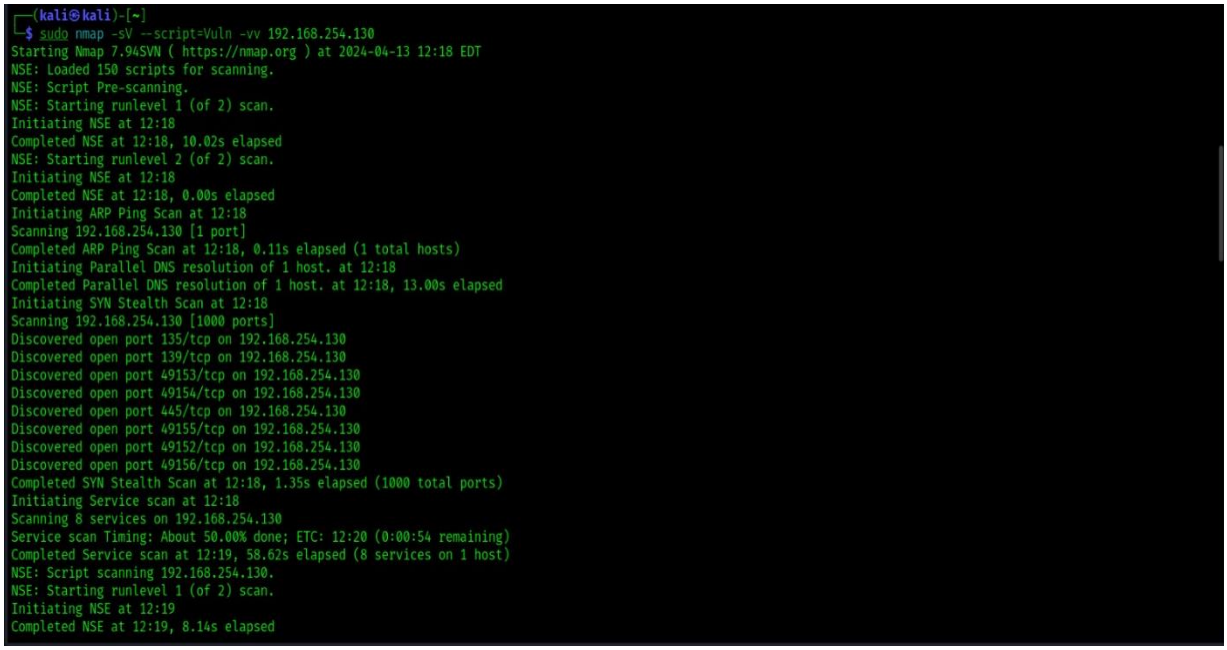
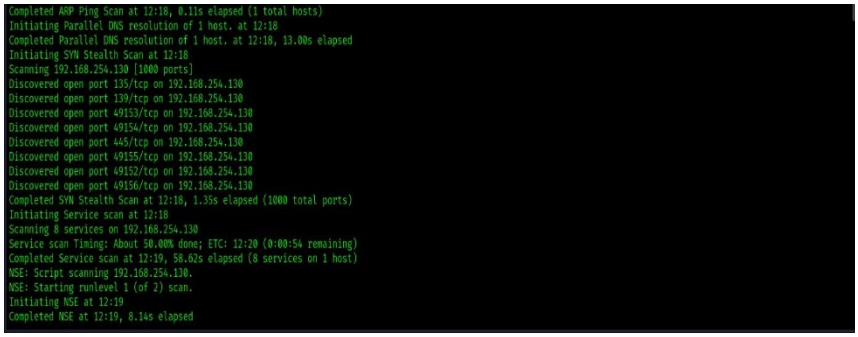


Fig: - Network Mapping

Port Scanning:

Ethical hackers use automated tools to identify any open ports on the network. This makes it an efficient mechanism to enumerate the services and live systems in a network and how to establish a connection with these components.

We see that there are few open ports. We also see that this machine is vulnerable to different exploits.



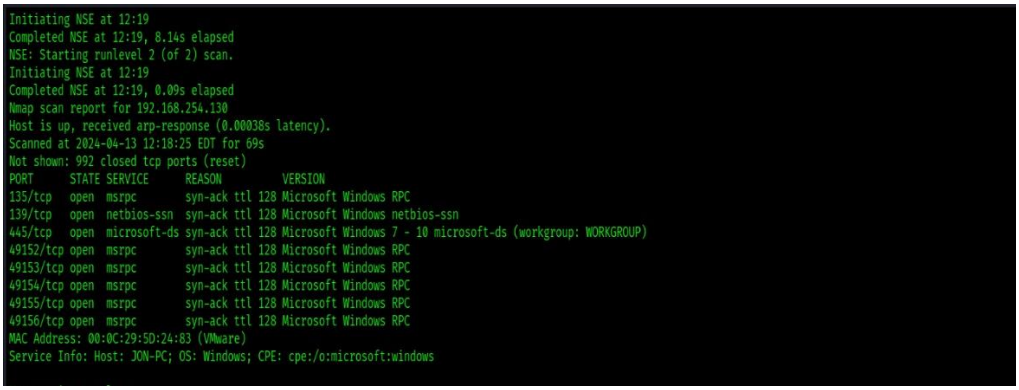


Fig: - Port Scanning

Vulnerability Scanning:

The use of automated tools to detect weaknesses that can be exploited to orchestrate attacks. While there are several tools available, here are a few popular ethical hacking tools commonly used during the scanning phase:

• SNMP Sweepers

• Ping sweeps

• Network mappers

• Vulnerability scanners

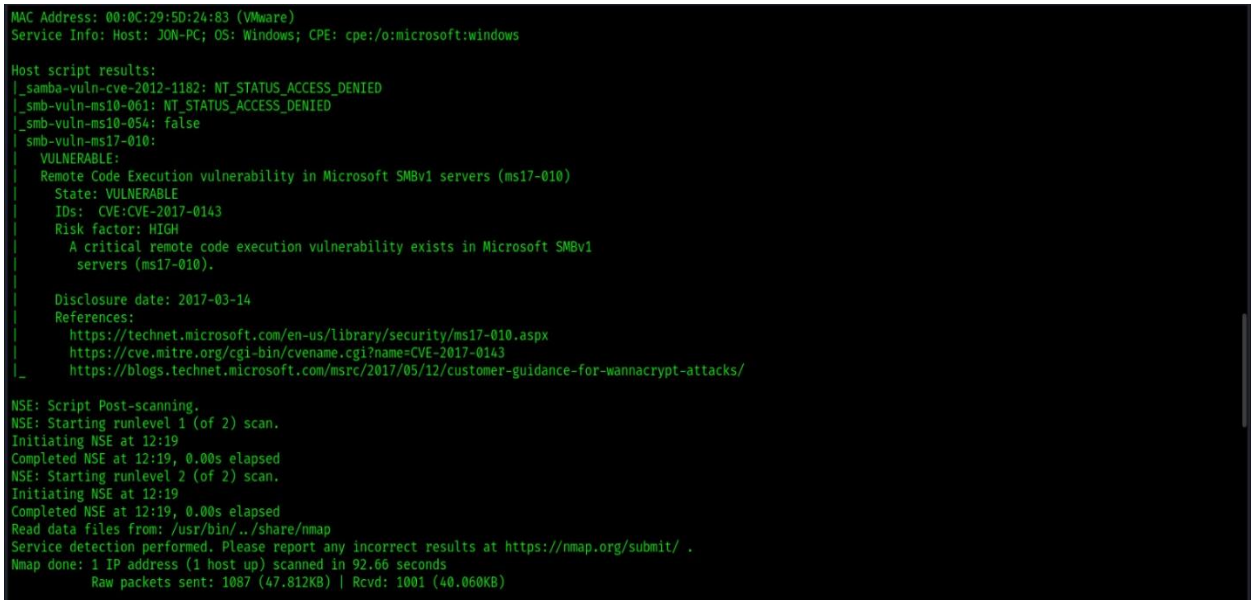


Fig: - Vulnerability Scanning

3. Gaining access:

Once ethical hackers expose vulnerabilities through the process's first and second hacking phases, they now attempt to exploit them for administrative access. The third phase involves attempting to send a malicious payload to the application through the network, an adjacent subnetwork, or physically using a connected computer. Hackers typically use many hacking tools and techniques to simulate attempted unauthorized access, including:

• Buffer overflows

• Phishing

• Injection Attacks

• XML External Entity Attacks

• Using components with known vulnerabilities

If the attacks are successful, the hacker has control of the whole or part of the system and may simulate further attacks such as data breaches and Distributed Denial of Service (DDoS).

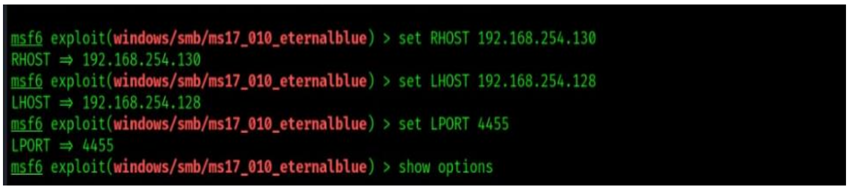
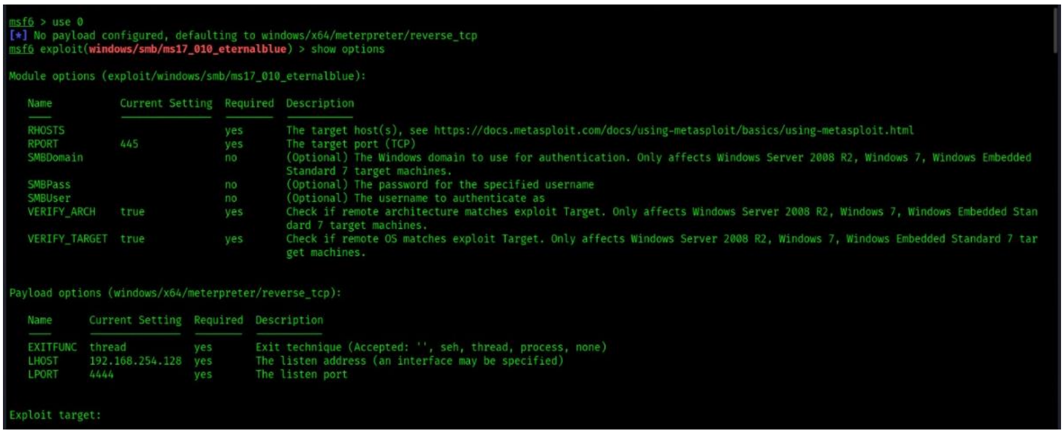


Fig: - Gaining Access

4. Maintaining access:

The fourth phase of the ethical hacking process involves processes to ensure the hacker can access the application for future use. A white-hat hacker continuously exploits the system for further vulnerabilities and escalates privileges to understand how much control attackers can gain once they pass security clearance. Some attackers may also try to hide their identity by removing the evidence of an attack and installing a backdoor for future access.



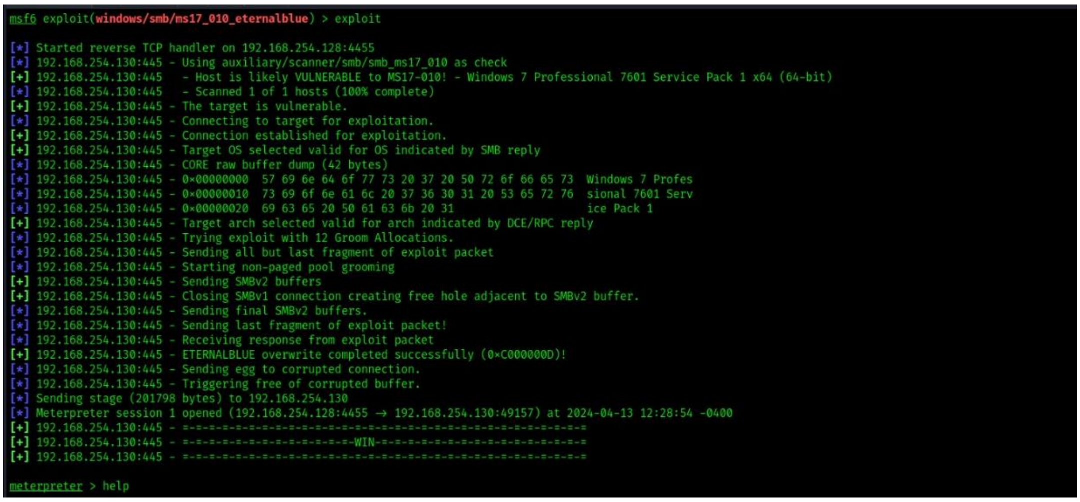


Fig:- Maintaing Access

5. Clearing the tracks:

This is the final step in order to complete the entire ethical hacking process. If this phase is completed successfully, the ethical hacker has managed to hack into a system or network. He could inflict as much damage as possible and has managed to leave the system without a trace. They need to cover their tracks throughout the process in order to avoid detection while entering and leaving the network or server.

To avoid any evidence that leads back to their malicious activity, hackers perform tasks that erase all traces of their actions. These include:

• Uninstalling scripts/applications used to carry out attacks

• Modifying registry values

• Clearing logs

• Deleting folders created during the attack

For those hackers looking to maintain undetected access, they tend to hide their identity using techniques such as:

• Tunnelling

• Stenography

Having successfully performed all the 5 steps of ethical hacking, the ethical hacker then concludes the steps of ethical hacking by documenting a report on the vulnerabilities and suggesting remediation advice.

Cracking Password:

Password cracking is a mechanism that is used in most of the parts of hacking. Exploitation uses it to exploit the applications by cracking their administrator or other account passwords, information Gathering uses it when we have to get the social media or other employees of the target organization, WIFI Hacking uses it when we have to crack the hash from the hash files, etc.

So to be a good Ethical hacker one must be aware of password cracking techniques. Though is easy to crack passwords by just using guessing techniques, it is very time consuming and less efficient so in order to automate the task, We have a lot of tools. When it comes to tools Kali Linux is the Operating System that Stands first, so here we have a list of tools in kali Linux may be used for password cracking.

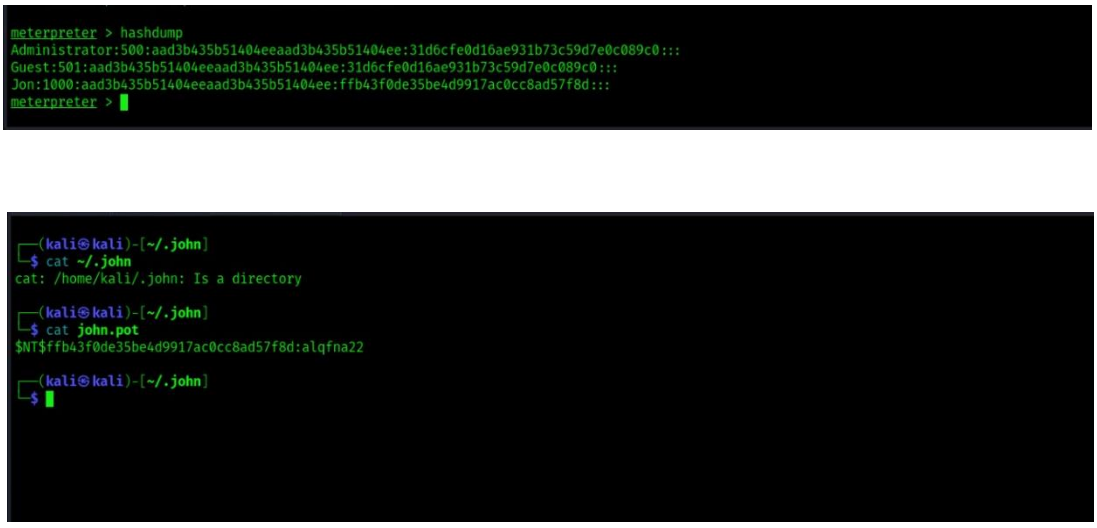


Fig: -Process Done For Cracking Password

Report:

Using Kali Linux I successfully completed the Penetrating Process and cracked the password for Windows 7.

Discussion:

Penetration testing is a comprehensive methodology, which is mostly used to identify the vulnerabilities in a system. It allows testers to exploit the systems and identify the extent of security levels in the organization. Penetration testing helps determine which vulnerabilities are exploitable and the degree of information exposure or network control that the organization could expect an attacker to achieve after successfully exploiting vulnerability.

Conclusion:

Ethical hacking is a crucial discipline in the field of cybersecurity. By leveraging ethical hacking methodologies, individuals and organizations can identify and address vulnerabilities, strengthen their defences, and protect sensitive information from malicious threats.

Recommendations:

- Obtain proper authorization
- Plan and scope your test
- Use legitimate tools and techniques
- Follow ethical guidelines
- Test password security
- Document and report findings

Acknowledgment:

I would like to express my deep and sincere gratitude to Vaishnavu CV, Principal Cyber Security Engineer, Mentor, VAPT, Ethical hacker, for giving me this opportunity to do research and providing valuable suggestions throughout my research. It was a great privilege and honour to work and study under his guidance.

(KOLLU JAHNAVI)