ABC Pte Ltd is running a financial institute. They had reports that financial institute were being targeted recently by hackers. Hence ABC bank had engaged us to do a vulnerability test ensure that their system is reasonably safe and secured.

**Engagement plans**

**Objectives:**

1. Identify system misconfigurations and network weaknesses
2. Determine the effectiveness of endpoint detection and response systems
3. Evaluate the impact of data exposure and exfiltration

**Scope:**

1. System downtime is not permitted under any circumstances.
   1. Any form of DDoS or DoS is prohibited.
   2. Any ransomware and other variations is prohibited.
2. Any form of social engineering is prohibited.
3. Attacks against systems within 192.168.199.0/24 are permitted.

**Mission Plan:**

1. Script to install all tools/software needed
2. Script to automate item 3 and 4
3. Nmap scans to determine
   1. Which Ip address are online
   2. Which ports are openf
   3. If there were outdated services
4. Nmap scripts to identify vulnerability
5. Metasploit to identify
   1. exploitable service/ports
   2. If password hash is extractable
   3. If Usernames are extractable
6. Hydra to identify weak password

**Remediation Plan**

1. Detailed result with explanation would be provided
2. Consultation would be provided

**Resource Plan**

Execution plan: 16 October ~ 22 October 2022

Reconnaissance: 19 October 2022

Initial Access: 20 October 2022

Post-Exploitation and Persistence: 20 October ~ 21 October 2022

Remediation: TBD

Personal Needed: Rayden Leong

Tools To Use: Nmap, Masscan, Hydra, Vulnscript, Msfconsole

**RESULT SUMMARY**

Online IPs Discovered:  
192.168.199.2  
192.168.199.136  
192.168.199.137  
192.168.199.143

**Scan Results:**

**192.168.199.2 –** Vmware rounter  
Discovered 1 open port   
Port 53/tcp domain service, version Cloudflare Public DNS  
  
**Summary** - Safe  
Port 53 is only listening on your LAN it's likely you have some computer sharing the internet  
  
**Recommendation**  
No Recommendation  
  
  
**192.168.199.136 – Vulnerable** – Microsoft Windows 10   
Discovered 6 open port   
135/tcp msrpc Microsoft Windows RPC

139/tcp netbios-ssn Microsoft Windows netbios-ssn

137/udp netbios-ns

445/tcp microsoft-ds?

5040/tcp unknown

7680/tcp pando-pub?

49664/tcp msrpc Microsoft Windows RPC

**Summary** - **Vulnerable**   
System is up-to-date, but services are exploitable  
We are able to find domain names on port 137/udp  
Although unable to login, we are able to brute force and find usernames and password on port 445 Administrator:Passw0rd!  
  
**Recommendation**  
Close off unused ports and only to open when needed..  
Port 139/445 are exploitable, by correct guess/dictionary, attackers are able to login and infiltrate the system  
Use stronger passwords

**192.168.199.136 – Exploitable** – linux:linux\_kernel:2.6

53/tcp domain ISC BIND 9.4.2

139/tcp netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

445/tcp netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

2049/tcp nfs 2-4 (RPC #100003)

6667/tcp irc UnrealIRCd

8180/tcp http Apache Tomcat/Coyote JSP engine 1.1

8787/tcp drb Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)

37440/tcp java-rmi GNU Classpath grmiregistry

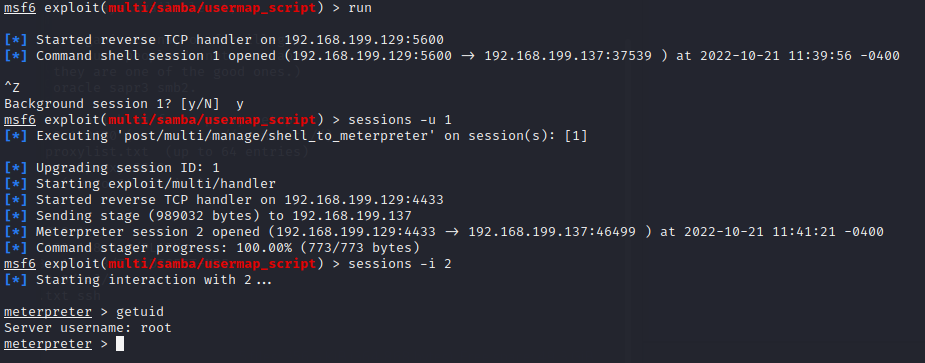
41453/tcp status 1 (RPC #100024)

41880/tcp mountd 1-3 (RPC #100005)

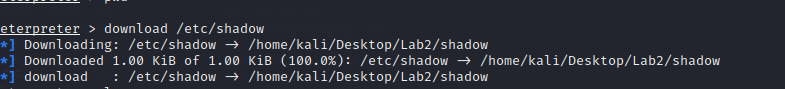
46045/tcp nlockmgr 1-4 (RPC #100021)

**Summary** - **Vulnerable**   
System services are out of date  
Port 139, 445, 6667, 8180, 37440 are easily exploitable to gain root access  
  
**Recommendation**  
Close off unused ports and only to open when needed..  
Update all services and ports urgently  
  
A screen shot on how port 139 is being exploited

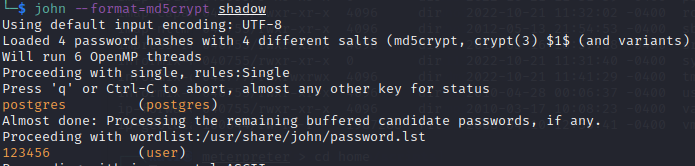
Easily gain root accessed



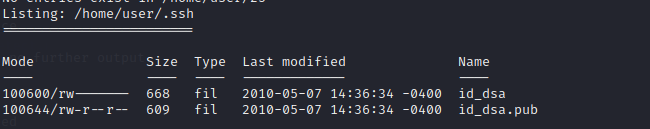
Able to create new user or crack the hash in the shadow file to get admin usernames and password for future login



Weak passwords being cracked within 1 min using default wordlist provided by John the ripper



Found dsa keys



Reference

<https://null-byte.wonderhowto.com/how-to/easily-detect-cves-with-nmap-scripts-0181925/>