10.10.10.40

Enumeration

```
autorecon 10.10.10.40
```

```
[*] [10.10.10.40/all-tcp-ports] Discovered open port tcp/139 on 10.10.10.40
[*] [10.10.10.40/all-tcp-ports] Discovered open port tcp/135 on 10.10.10.40
[*] [10.10.10.40/all-tcp-ports] Discovered open port tcp/445 on 10.10.10.40
[*] [10.10.10.40/all-tcp-ports] Discovered open port tcp/49156 on 10.10.10.40
[*] [10.10.10.40/all-tcp-ports] Discovered open port tcp/49155 on 10.10.10.40
[*] [10.10.10.40/all-tcp-ports] Discovered open port tcp/49152 on 10.10.10.40
[*] [10.10.10.40/all-tcp-ports] Discovered open port tcp/49154 on 10.10.10.40
[*] [10.10.10.40/all-tcp-ports] Discovered open port tcp/49153 on 10.10.10.40
```

TCP

UDP

Web Services

Nikto

Dirb|DirBuster

WebDav

CMS

Other Services

SMB

SNMP

DB

Other

Exploitation

Service Exploited: SMB
Vulnerability Type: RCE
Exploit POC:
Description:

Discovery of Vulnerability

```
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
```

Exploit Code Used

msfconsole ms17-010 exploit

Proof\Local.txt File

- ☐ Screenshot with ifconfig\ipconfig
- ☐ Submit too OSCP Exam Panel

Post Exploitation

Script Results

Host Information

Operating System

Architecture

Domain

Installed Updates

File System

Writeable Files\Directories

Directory List

Running Processes

Process List

Installed Applications

Installed Applications

Users & Groups

Users

Groups

Network

IPConfig\IFConfig

Network Processes

ARP

DNS

Route

Scheduled Jobs

Scheduled Tasks

Priv Escalation

Service Exploited:
Vulnerability Type:
Exploit POC:
Description:

Discovery of Vulnerability

Exploit Code Used

Proof\Local.txt File

- ☐ Screenshot with ifconfig\ipconfig
- ☐ Submit too OSCP Exam Panel

Goodies

Hashes

Passwords

Proof|Flags|Other

root.txt: ff548eb71e920ff6c08843ce9df4e717
user.txt: 4c546aea7dbee75cbd71de245c8deea9

Software Versions

Software Versions

Potential Exploits

Methodology

Network Scanning

- ☐ nmap -sn 10.11.1.*
- ☐ nmap -sL 10.11.1.*
- ☐ nbtscan -r 10.11.1.0/24
- ☐ smbtree

Individual Host Scanning

- ☐ nmap --top-ports 20 --open -iL iplist.txt
- ☐ nmap -sS -A -sV -O -p- ipaddress
- ☐ nmap -sU ipaddress

Service Scanning

WebApp

- ☐ Nikto
- ☐ dirb
- ☐ dirbuster
- ☐ wpscan
- ☐ dotdotpwn
- ☐ view source
- ☐ davtest\cadevar
- ☐ droopscan
- ☐ joomscan
- ☐ LFI\RFI Test

Linux\Windows

- ☐ snmpwalk -c public -v1 *ipaddress* 1
- ☐ smbclient -L //ipaddress
- ☐ showmount -e ipaddress port
- ☐ rpcinfo
- ☐ Enum4Linux

Anything Else

- ☐ nmap scripts (locate *nse* | grep servicename)
- ☐ hydra
- ☐ MSF Aux Modules
- ☐ Download the softward

Exploitation

- ☐ Gather Version Numbes
- ☐ Searchsploit
- ☐ Default Creds
- ☐ Creds Previously Gathered
- ☐ Download the software

Post Exploitation

Linux

- ☐ linux-local-enum.sh
- ☐ linuxprivchecker.py
- ☐ linux-exploit-suggestor.sh
- ☐ unix-privesc-check.py

Windows

- ☐ wpc.exe
- ☐ windows-exploit-suggestor.py
- ☐ windows_privesc_check.py
- ☐ windows-privesc-check2.exe

Priv Escalation

- ☐ acesss internal services (portfwd)
- ☐ add account

Windows

- ☐ List of exploits

Linux

- ☐ sudo su
- ☐ KernelDB
- ☐ Searchsploit

Final

- ☐ Screenshot of IPConfig\WhoamI
- ☐ Copy proof.txt
- ☐ Dump hashes
- ☐ Dump SSH Keys
- ☐ Delete files

Log Book