

PROJECT : 4

DATE : 04-10-2021

TOPIC : Port scanning and vulnerability scanning.

Attacker IP:-192.168.137.55

Victim1 IP:-192.168.137.190 (Windows 7)

Victim2 IP:-192.168.137.161(Metasploitable)

Victim1:-

Nmap scan:-

```
└─(root㉿kali)-[~/home/kali]
# nmap -sC -sV 192.168.137.190
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-04 01:28 EDT
Nmap scan report for windows7-PC.mshome.net (192.168.137.190)
Host is up (0.052s latency).
Not shown: 986 closed ports
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds  Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
554/tcp    open  rtsp?
2869/tcp   open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
3389/tcp   open  ms-wbt-server?
| ssl-cert: Subject: commonName=windows7-PC
|   Not valid before: 2021-09-27T09:40:23
|   Not valid after:  2022-03-29T09:40:23
|   _ssl-date: 2021-10-04T05:30:54+00:00; -1s from scanner time.
5357/tcp   open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
10243/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
49152/tcp  open  msrpc        Microsoft Windows RPC
49153/tcp  open  msrpc        Microsoft Windows RPC
49154/tcp  open  msrpc        Microsoft Windows RPC
49155/tcp  open  msrpc        Microsoft Windows RPC
49156/tcp  open  msrpc        Microsoft Windows RPC
49157/tcp  open  msrpc        Microsoft Windows RPC
MAC Address: 08:00:27:9E:37:29 (Oracle VirtualBox virtual NIC)
Service Info: Host: WINDOWS7-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: -1s
| smb2-security-mode:
|   2.10:
|     Message signing enabled but not required
|_smb2-time: Protocol negotiation failed (SMB2)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 151.49 seconds
```

Nessus Scan:-

192.168.137.190				
CRITICAL		HIGH	MEDIUM	LOW
SEVERITY	CVSS V3.0	PLUGIN	NAME	
CRITICAL	10.0	79638	MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution (2992611) (unprivileged check)	
CRITICAL	10.0	125313	Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (unprivileged check)	
CRITICAL	10.0	108797	Unsupported Windows OS (remote)	
HIGH	9.3	58435	MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (unprivileged check)	
HIGH	9.3	97833	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNTERGY) (WannaCry) (EternalRocks) (Petya) (unprivileged check)	
MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted	
MEDIUM	6.4	57582	SSL Self-Signed Certificate	
MEDIUM	6.1	104743	TLS Version 1.0 Protocol Detection	
MEDIUM	5.8	90510	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (unprivileged check)	
MEDIUM	5.1	18405	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	
MEDIUM	5.1	18405	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	
MEDIUM	5.0	57608	SMB Signing not required	
MEDIUM	5.0	35291	SSL Certificate Signed Using Weak Hashing Algorithm	
MEDIUM	5.0	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)	
MEDIUM	4.3	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	
MEDIUM	4.3	58453	Terminal Services Doesn't Use Network Level Authentication (NLA) Only	

192.168.137.190 4

MEDIUM	4.3	57690	Terminal Services Encryption Level is Medium or Low
LOW	2.6	30218	Terminal Services Encryption Level is not FIPS-140 Compliant

Victim2:-

Nmap scan:-

```
[root@kali] [/home/kali]
# nmap -sC -sV 192.168.137.161
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-04 01:16 EDT
Stats: 0:00:58 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 95.65% done; ETC: 01:17 (0:00:02 remaining)
Nmap scan report for 192.168.137.161
Host is up (0.0047s latency).
Not shown: 977 filtered ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
|     STAT: Connected to 192.168.137.206
|       Logged in as ftp
|       TYPE: ASCII
|       No session bandwidth limit
|       Session timeout in seconds is 300
|       Control connection is plain text
|       Data connections will be plain text
|       vsFTPD 2.3.4 - secure, fast, stable
|_End of status
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:c:f:0:0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|   2048 56:56:24:0f:21:d:d:e:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet        Linux telnetd
25/tcp    open  smtp         Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN,
|   ssl-cert: Subject: commonName=Ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
|   Not valid before: 2010-03-17T14:07:45
|   Not valid after:  2010-04-16T14:07:45
|_ssl-date: 2021-10-04T05:20:02+00:00; +3s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_bind.version: 9.4.2
| dns-nsid:
| bind.version: 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp   open  rpcbind     2 (RPC #100000)
| rpcinfo:
```

```

rpcinfo:
program version    port/proto   service
 100000  2          111/tcp      rpcbind
 100000  2          111/udp      rpcbind
 100003  2,3,4      2049/tcp     nfs
 100003  2,3,4      2049/udp     nfs
 100005  1,2,3      46743/udp   mounted
 100005  1,2,3      50460/tcp    mounted
 100021  1,3,4      41719/udp   nlockmgr
 100021  1,3,4      54020/tcp    nlockmgr
 100024  1          49756/udp   status
 100024  1          52872/tcp   status
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp open  exec?
513/tcp open  login?
514/tcp open  tcpwrapped
1099/tcp open  java-rmi   GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs        2-4 (RPC #100003)
2121/tcp open  ftp       ProFTPD 1.3.1
3306/tcp open  mysql     MySQL 5.0.51a-3ubuntu5
mysql-info:
  Protocol: 10
  Version: 5.0.51a-3ubuntu5
  Thread ID: 11
  Capabilities flags: 43564
  Some Capabilities: SupportsCompression, SupportsTransactions, SwitchToSSLAfterHandshake, ConnectWithDatabase, LongColumnFlag, Speaks4IPProtocolNew, Support4IAuth
  Status: Autocommit
  Salt: peAHK!{q;pfI}Z]zm6c
5432/tcp open  postgresql PostgreSQL DB 8.3.0 - 8.3.7
ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
Not valid before: 2010-03-17T14:07:45
Not valid after: 2010-04-16T14:07:45
_ssl-date: 2021-10-04T05:20:01+00:00; +3s from scanner time.
5900/tcp open  vnc      VNC (protocol 3.3)
vnc-info:
  Protocol version: 3.3
  Security types:
    VNC Authentication (2)
6000/tcp open  X11      (access denied)
6667/tcp open  irc      UnrealIRCd
irc-info:
  users: 1
  servers: 1
  lusers: 1
  lservers: 0
  server: irc.Metasploitable.LAN
  version: Unreal3.2.8.1. irc.Metasploitable.LAN
  uptime: 0 days, 0:05:41
  source ident: nmap
  source host: 54DA3780.54E41161.FFFA6D49.IP
  error: Closing Link: poubgfcpv[192.168.137.55] (Quit: poubgfcpv)
8009/tcp open  ajp13    Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open  http    Apache Tomcat/Coyote JSP engine 1.1
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/5.5
MAC Address: 08:00:27:0E:9F:B6 (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
_clock-skew: mean: -1h56m07s, deviation: 2h18m34s, median: -3h16m08s
_nbstat: NetBIOS name: METASPOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
_smb-os-discovery:
  OS: Unix (Samba 3.0.20-Debian)
  Computer name: metasploitable
  NetBIOS computer name:
  Domain name: localdomain
  FQDN: metasploitable.localdomain
  System time: 2021-10-04T02:26:33-04:00
_smb-security-mode:
  account_used: <blank>
  authentication_level: user
  challenge_response: supported
  message_signing: disabled (dangerous, but default)
  _smb2-time: Protocol negotiation failed (SMB2)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 143.24 seconds

```

Nessus scan:-

192.168.137.161



Vulnerabilities

Total: 110

Severity	CVSS V3.0	Plugin	Name
CRITICAL	10.0	51988	Bind Shell Backdoor Detection
CRITICAL	10.0	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
CRITICAL	10.0	11356	NFS Exported Share Information Disclosure
CRITICAL	10.0	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0	46882	UnrealIRCd Backdoor Detection
CRITICAL	10.0	61708	VNC Server 'password' Password
CRITICAL	10.0	10203	rexecd Service Detection
HIGH	7.8	136808	ISC BIND Denial of Service
HIGH	7.5	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
HIGH	7.5	34460	Unsupported Web Server Detection

HIGH	7.5	34460	Unsupported Web Server Detection
HIGH	7.5	10205	rlogin Service Detection
HIGH	7.5	10245	rsh Service Detection
HIGH	7.1	20007	SSL Version 2 and 3 Protocol Detection
MEDIUM	6.8	90509	Samba Badlock Vulnerability
MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.4	57582	SSL Self-Signed Certificate
MEDIUM	6.1	104743	TLS Version 1.0 Protocol Detection

192.168.137.161

4

MEDIUM	5.8	42263	Unencrypted Telnet Server
MEDIUM	5.0	12085	Apache Tomcat Default Files
MEDIUM	5.0	12217	DNS Server Cache Snooping Remote Information Disclosure
MEDIUM	5.0	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.0	136769	ISC BIND Service Downgrade / Reflected DoS
MEDIUM	5.0	42256	NFS Shares World Readable
MEDIUM	5.0	57608	SMB Signing not required
MEDIUM	5.0	15901	SSL Certificate Expiry

MEDIUM	5.0	15901	SSL Certificate Expiry
MEDIUM	5.0	45411	SSL Certificate with Wrong Hostname
MEDIUM	5.0	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
MEDIUM	4.3	90317	SSH Weak Algorithms Supported *
MEDIUM	4.3	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
MEDIUM	4.3	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
MEDIUM	4.0	139915	ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS
LOW	2.6	70658	SSH Server CBC Mode Ciphers Enabled
LOW	2.6	71049	SSH Weak MAC Algorithms Enabled
LOW	2.6	10407	X Server Detection
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	10223	RPC portmapper Service Detection
INFO	N/A	21186	AJP Connector Detection
INFO	N/A	18261	Apache Banner Linux Distribution Disclosure
INFO	N/A	48204	Apache HTTP Server Version
INFO	N/A	39446	Apache Tomcat Detection
INFO	N/A	39519	Backported Security Patch Detection (FTP)
INFO	N/A	84574	Backported Security Patch Detection (PHP)