Ethical Hacking

UNIT I INTRODUCTION TO HACKING

Introduction to Hacking – Importance of Security – Elements of Security – Phases of an Attack – Types of Hacker Attacks– Vulnerability Research – Introduction to Foot printing – Information Gathering Methodology – Foot printing Tools – DNS Information Tools – Locating the Network Range

HACKING

Hacking has been a part of computing for almost five decades and it is a very broad discipline, which covers a wide range of topics. The first known event of hacking had taken place in 1960 at MIT and at the same time, the term "Hacker" was originated.

Hacking is the act of finding the possible entry points that exist in a computer system or a computer network and finally entering into them. Hacking is usually done to gain unauthorized access to a computer system or a computer network, either to harm the systems or to steal sensitive information available on the computer.

Hacking is usually legal as long as it is being done to find weaknesses in a computer or network system for testing purpose. This sort of hacking is what we call **Ethical Hacking**.

A computer expert who does the act of hacking is called a "Hacker". Hackers are those who seek knowledge, to understand how systems operate, how they are designed, and then attempt to play with these systems.

Types of Hacking

We can segregate hacking into different categories, based on what is being hacked. Here is a set of examples −

- **Website Hacking** − Hacking a website means taking unauthorized control over a web server and its associated software such as databases and other interfaces.
- **Network Hacking** − Hacking a network means gathering information about a network by using tools like Telnet, NS lookup, Ping, Tracert, Netstat, etc. with the intent to harm the network system and hamper its operation.
- **Email Hacking** − It includes getting unauthorized access on an Email account and using it without taking the consent of its owner.
- **Ethical Hacking** − Ethical hacking involves finding weaknesses in a computer or network system for testing purpose and finally getting them fixed.
- **Password Hacking** − This is the process of recovering secret passwords from data that has been stored in or transmitted by a computer system.
- **Computer Hacking** − This is the process of stealing computer ID and password by applying hacking methods and getting unauthorized access to a computer system.

Advantages of Hacking

Hacking is quite useful in the following scenarios −

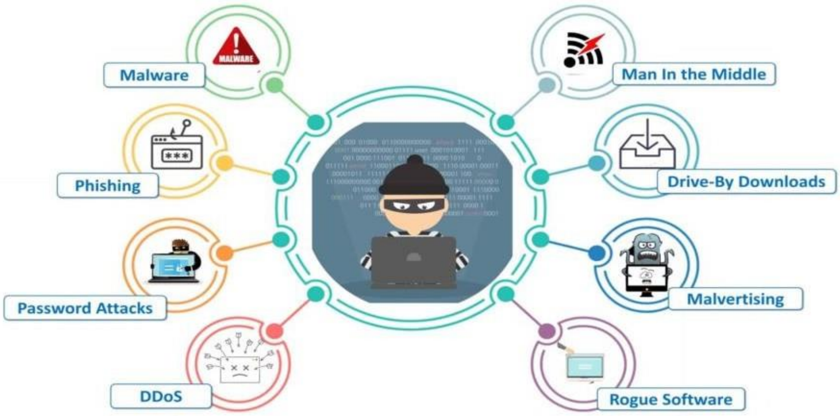
- To recover lost information, especially in case you lost your password.
- To perform penetration testing to strengthen computer and network security.
- To put adequate preventative measures in place to prevent security breaches.
- To have a computer system that prevents malicious hackers from gaining access.

Disadvantages of Hacking

Hacking is quite dangerous if it is done with harmful intent. It can cause −

- Massive security breach.
- Unauthorized system access on private information.
- Privacy violation.
- Hampering system operation.
- Denial of service attacks.
- Malicious attack on the system.

Importance of Security



Malware

It is a form of malicious software in which any file or program can be used to harm a computer user. This includes worms, viruses, Trojans and spyware.

Phishing

Is a form of social engineering where fraudulent email or text messages that resemble those from reputable or known sources are sent. Often random attacks, the intent of these messages is to steal sensitive data, such as credit card or login information.

Password Attacks

A password attack refers to any of the various methods used to maliciously authenticate into password-protected accounts. These attacks are typically facilitated through the use of software that expedites cracking or guessing passwords. The most common attack methods include brute forcing, dictionary attacks, password spraying, and credential stuffing.

DDOS

Distributed denial-of-service (DDoS) attacks are those in which multiple systems disrupt the traffic of a targeted system, such as a server, website or other network resource. By flooding the target with messages, connection requests or packets, the attackers can slow the system or crash it, preventing legitimate traffic from using it.

Man in middle

They are eavesdropping attacks that involve an attacker intercepting and relaying messages between two parties who believe they are communicating with each other.

Drive by Downloads

Drive by download attacks specifically refer to malicious programs that install to your devices — without your consent. This also includes unintentional downloads of any files or bundled software onto a computer device.

Malvertising

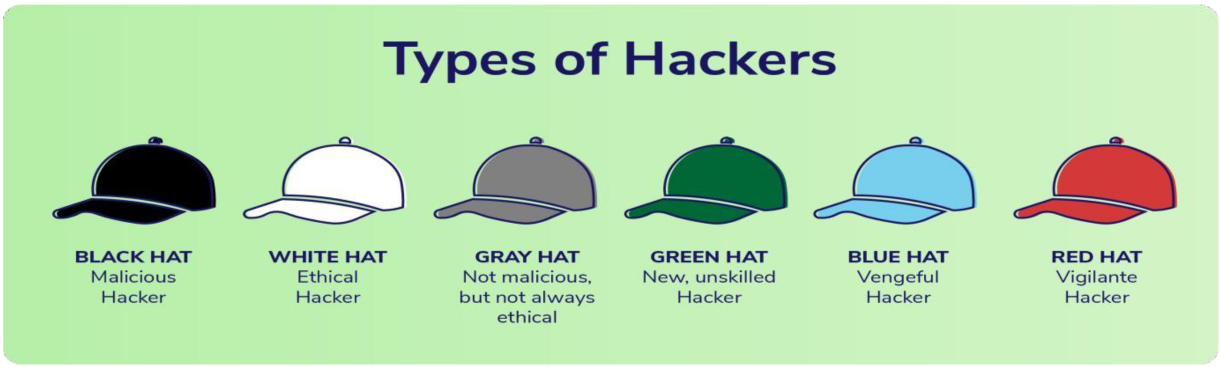
It is a malicious cyber tactic that attempts to distribute malware through online advertisements. Online advertising is a vital source of income to many websites and internet properties. With demand higher than ever, online networks have become expansive and complex in order to effectively reach large online audiences.

Rogue Software

Rogue security software is a **form of malicious software and internet fraud that misleads users into believing** there is a virus on their computer and aims to convince them to pay for a fake malware removal tool that actually installs malware on their computer.This kind of software is designed to show fake security alerts, update notifications to attempt users into doing fraud

Hacker Types

Hackers can be classified into different categories such as white hat, black hat, and grey hat, based on their intent of hacking a system. These different terms come from old Spaghetti Westerns, where the bad guy wears a black cowboy hat and the good guy wears a white hat.



White Hat Hackers

White Hat hackers are also known as **Ethical Hackers**. They never intent to harm a system, rather they try to find out weaknesses in a computer or a network system as a part of penetration testing and vulnerability assessments.

Ethical hacking is not illegal and it is one of the demanding jobs available in the IT industry. There are numerous companies that hire ethical hackers for penetration testing and vulnerability assessments.

Black Hat Hackers

Black Hat hackers, also known as **crackers**, are those who hack in order to gain unauthorized access to a system and harm its operations or steal sensitive information.

Black Hat hacking is always illegal because of its bad intent which includes stealing corporate data, violating privacy, damaging the system, blocking network communication, etc.

Grey Hat Hackers

Grey hat hackers are a blend of both black hat and white hat hackers. They act without malicious intent but for their fun, they exploit a security weakness in a computer system or network without the owner’s permission or knowledge.

Their intent is to bring the weakness to the attention of the owners and getting appreciation or a little bounty from the owners.

Miscellaneous Hacker

Apart from the above well-known classes of hackers, we have the following categories of hackers based on what they hack and how they do it.

Red Hat Hackers

Red hat hackers are again a blend of both black hat and white hat hackers. They are usually on the level of hacking government agencies, top-secret information hubs, and generally anything that falls under the category of sensitive information.

Blue Hat Hackers

A blue hat hacker is someone outside computer security consulting firms who is used to bug-test a system prior to its launch. They look for loopholes that can be exploited and try to close these gaps. Microsoft also uses the term **BlueHat** to represent a series of security briefing events.

Green Hat Hacker

Newbie hacker who are learning to hack .They are not aware of consequences of their action and cause unintentional damage without knowing how to fix it. A neophyte, "n00b", or "newbie" or "Green Hat Hacker"

Elite Hackers

This is a social status among hackers, which is used to describe the most skilled. Newly discovered exploits will circulate among these hackers.

ScriptKiddie

A script kiddie is a non-expert who breaks into computer systems by using pre-packaged automated tools written by others, usually with little understanding of the underlying concept, hence the term **Kiddie**.

Hacktivist

A hacktivist is a hacker who utilizes technology to announce a social, ideological, religious, or political message. In general, most hacktivism involves website defacement or denial of-service attacks.

Elements of security

APPLICATION SECURITY
END USER COMPILANCE
DISASTER RECOVERY
NETWORK SECURITY
INFORMATION SECURITY
ELEMENTS OF CYBER SECURITY

For fulfilling all the security-related constraints and requirements, researchers and security analysts have come up with some unique concepts that, when preserved, can help in keeping the system safe and secure. If anyone of the elements gets compromised, there is a potential risk for the information and the system. These six elements are

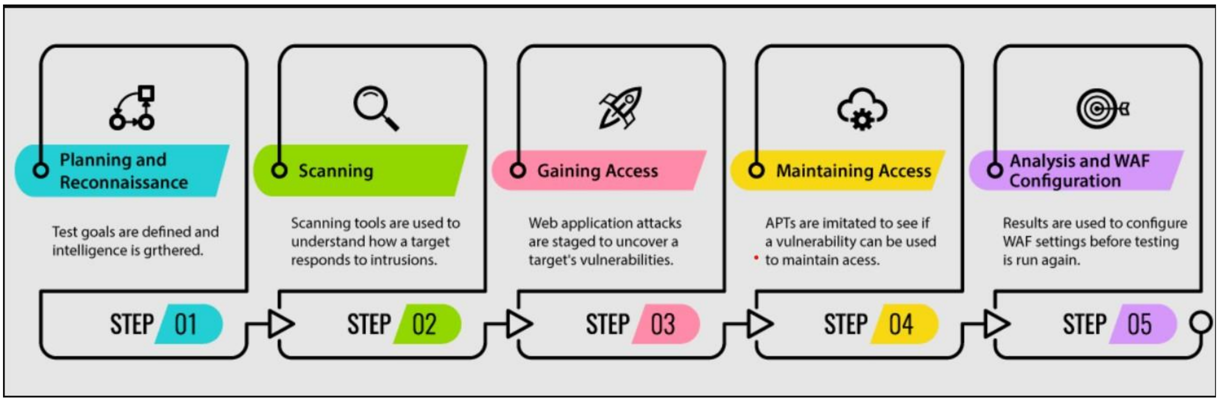
1. **Availability:** As the name suggests, availability specifies whether the data or resource is available when required or requested by the client. The information that has been requested will possess the actual value only when legitimate users can access those resources at the right time. Cybercriminals seize those data so that the request to access those resources gets denied (leads to downtime of a working server), which is a conventional attack.
2. **Integrity:** This refers to the techniques to ensure that all the data or resources that can be accessed in real-time are legitimate, correct, and protected from unlawful user (hackers) modification. Data integrity has become a primary and essential component or element of information security because users have to trust online information to use them. Data integrity is verified through techniques like checksums, change in hash values, and data comparison.
3. **Authenticity:** It is another essential element, and authentication can be defined as the process of ensuring and confirming that the identity of the user is genuine and legitimate. This authentication process takes place when the user tries to gain access to any data or information (commonly done by login or biometric access). However, cybercriminals use more sophisticated tools and techniques to gain such access using social engineering, password guessing, brute force techniques, or cracking ciphers.
4. **Confidentiality**: It can be defined as permitting approved users for accessing all sensitive as well as protected information. Confidentiality can be made certain by using role-based security techniques for ensuring user or viewer's authorization and access controls on any particular data.
5. **Non-repudiation:** can be defined as the way of assurance that message transmitted among two or more users via digital signature or through encryption is accurate, and no one can deny the authentication of the digital signature on any document. Authentic data and its origination can be acquired with the help of a data hash.

6. **Utility:** as the name suggests is used for any purpose or reason and is accessed and then used by users. Cryptography is used to preserve the efficiency of any resource sent over the internet. Various encryption mechanisms are used for securing the message or data sent over the internet so that it is not altered during the transmission; otherwise, the utility of that resource will not prevail.

Phases of an Attack

Like all good projects, ethical hacking too has a set of distinct phases. It helps hackers to make a structured ethical hacking attack.

Different security training manuals explain the process of ethical hacking in different ways, but for me as a Certified Ethical Hacker, the entire process can be categorized into the following six phases.



Test goals are defined and intelligence is grthered.

Scanning tools are used to understand how a target responds to intrusions.

Web application attacks are staged to uncover a target's vulnerabilities.

APTs are imitated to see if a vulnerability can be used to maintain acess.

Results are used to configure WAF settings before testing is run again.

Reconnaissance

Reconnaissance is the phase where the attacker gathers information about a target using active or passive means. The tools that are widely used in this process are NMAP, Hping, Maltego , and Google Dorks.

Scanning

In this process, the attacker begins to actively probe a target machine or network for vulnerabilities that can be exploited. The tools used in this process are Nessus, Nexpose, and NMAP.

Gaining Access

In this process, the vulnerability is located and you attempt to exploit it in order to enter into the system. The primary tool that is used in this process is Metasploit.

Maintaining Access

It is the process where the hacker has already gained access into a system. After gaining access, the hacker installs some backdoors in order to enter into the system when he needs access in this owned system in future. Metasploit is the preferred tool in this process.

Clearing Tracks

This process is actually an unethical activity. It has to do with the deletion of logs of all the activities that take place during the hacking process.

Reporting

Reporting is the last step of finishing the ethical hacking process. Here the Ethical Hacker compiles a report with his findings and the job that was done such as the tools used, the success rate, vulnerabilities found, and the exploit processes.

Quick Tip

The processes are not standard. You can adopt a set of different processes and tools according to your techniques that you are comfortable with. The process is of least significance as long as you are able to get the desired results.

Reconnaissance

Information Gathering and getting to know the target systems is the first process in ethical hacking. Reconnaissance is a set of processes and techniques (Footprinting, Scanning & Enumeration) used to covertly discover and collect information about a target system.

During reconnaissance, an ethical hacker attempts to gather as much information about a target system as possible, following the seven steps listed below −

- Gather initial information
- Determine the network range
- Identify active machines
- Discover open ports and access points
- Fingerprint the operating system
- Uncover services on ports
- Map the network

We will discuss in detail all these steps in the subsequent chapters of this tutorial. Reconnaissance takes place in two parts − **Active Reconnaissance** and **Passive Reconnaissance**.

Active Reconnaissance

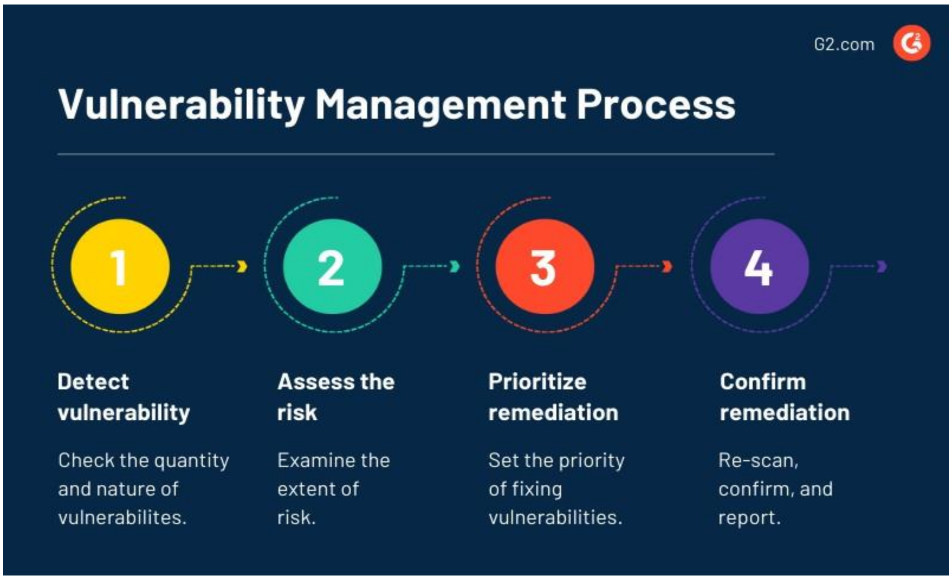
In this process, you will directly interact with the computer system to gain information. This information can be relevant and accurate. But there is a risk of getting detected if you are planning active reconnaissance without permission. If you are detected, then system admin can take severe action against you and trail your subsequent activities.

Passive Reconnaissance

In this process, you will not be directly connected to a computer system. This process is used to gather essential information without ever interacting with the target systems.

Vulnerability Research

- In the current threat environment, vulnerability research is incredibly important.
- These findings can serve to better protect users and make software developers and vendors aware of flaws that could put sensitive information at risk of exposure.
- Cyber-attacks becoming more prevalent, one would think the industry would welcome any opportunity to mitigate the chances of hackers breaking into commonly-used programs



G2.com

Vulnerability Management Process

1 Detect vulnerability
Check the quantity and nature of vulnerabilites.

2 Assess the risk
Examine the extent of risk.

3 Prioritize remediation
Set the priority of fixing vulnerabilities.

4 Confirm remediation
Re-scan, confirm, and report.

What are vulnerability lists?

It is a documented listing of common vulnerabilities.

- They are usually assigned an identification number, a description and public references.
- These vulnerabilities have been found to occur commonly and often lead to the exploitation of systems on the internet.

- **Databases**: These databases include various information on vulnerabilities. For instance, information might include security checklist references, security-related software flaws, misconfigurations , product names and impact metrics.

The following are some examples:

- NVD by NIST: This is a repository managed by the U.S. government
- CVE: This is managed by the MITRE Corporation and sponsored by the U.S. DHS
- OWASP: OWASP manages a list of vulnerabilities in a project known as the OWASP Top 10. Here, vulnerabilities are classified based on their frequency of attack. The list is updated only as OWASP decides it is necessary, with several years often passing between updates
- Exploit Database: This database of exploits is managed by Offensive Security
- **Vendor advisories**: Software vendors may issue advisories on how to deal with security vulnerabilities by applying patches that fix these security issues.
- The following are common vendors that take this approach to make security issues known:
- **Microsoft**: Microsoft Security Response Center manages a comprehensive library of security documents that discusses security issues affecting Microsoft products
- **Adobe**: Adobe manages a security advisory list where security issues are addressed and patches suggested
- **VMware**: Security issues related to VMware's virtualization are published here

Footprinting

Footprinting is a part of reconnaissance process which is used for gathering possible information about a target computer system or network. Footprinting could be both **passive** and **active**. Reviewing a company's website is an example of passive footprinting, whereas attempting to gain access to sensitive information through social engineering is an example of active information gathering.

Footprinting is basically the first step where hacker gathers as much information as possible to find ways to intrude into a target system or at least decide what type of attacks will be more suitable for the target.

During this phase, a hacker can collect the following information −

- Domain name
- IP Addresses
- Namespaces
- Employee information
- Phone numbers
- E-mails
- Job Information

In the following section, we will discuss how to extract the basic and easily accessible information about any computer system or network that is linked to the Internet.

Domain Name Information

You can use http://www.whois.com/whois website to get detailed information about a domain name information including its owner, its registrar, date of registration, expiry, name server, owner's contact information, etc.

Finding IP Address

You can use **ping** command at your prompt. This command is available on Windows as well as on Linux OS. Following is the example to find out the IP address of tutorialspoint.com

```
$ping tutorialspoint.com
```

It will produce the following result −

```
PING tutorialspoint.com (66.135.33.172) 56(84) bytes of data.
64 bytes from 66.135.33.172: icmp_seq = 1 ttl = 64 time = 0.028 ms
64 bytes from 66.135.33.172: icmp_seq = 2 ttl = 64 time = 0.021 ms
64 bytes from 66.135.33.172: icmp_seq = 3 ttl = 64 time = 0.021 ms
64 bytes from 66.135.33.172: icmp_seq = 4 ttl = 64 time = 0.021 ms
```

Finding Hosting Company

Once you have the website address, you can get further detail by using ip2location.com website. Following is the example to find out the details of an IP address −

Different steps for Footprinting

- EC-Council has divided Footprinting into seven steps.

1. Information Gathering
2. Determining the network
3. Identify active machines
4. Finding open ports and access points
5. OS fingerprinting
6. Fingerprinting services
7. Mapping the network

Methods of footprinting

- Who is lookup
- Port Scanning
- Traceroutes
- Extract Website information from Wayback machine
- Collecting information from Google Header
- Ping Sweep

1. **Who is lookup** : This method can be used to collect basic database queries like domain name, IP Address block, location, and much more information bout the organization.
2. **Port Scanning** :

- Port scanners are used to determine live hosts on the internet and find out which Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) ports are listening on each system
- Port scanners are also find out which operating system is installed on the host.

3. **Traceroutes** : To identify the relationship of each host and potential security mechanisms between the attacker and targets, they use traceroutes.

Tools:

NSLookup - to perorm DNS queries and zone transfers

Tracert - to create network maps of the target.

Once port scanning and trace routing are done, attackers will create a network map that represents the target's internet footprinting.

4. **Extract Website information from Wayback machine** : It is very easy to get complete history of any website using www.archieve.org

5. Collecting information from Google Header :

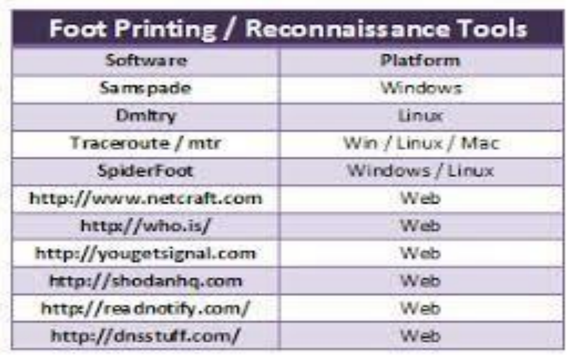
- This method does not involve hacking Google! This means by which you can collect information from the Google search engine in a smart way.

Search engines have many features using which you can get uncommon, but very specific search results from the internet. Using these techniques, hackers and attackers perform a search using advanced operators

Footprinting tools

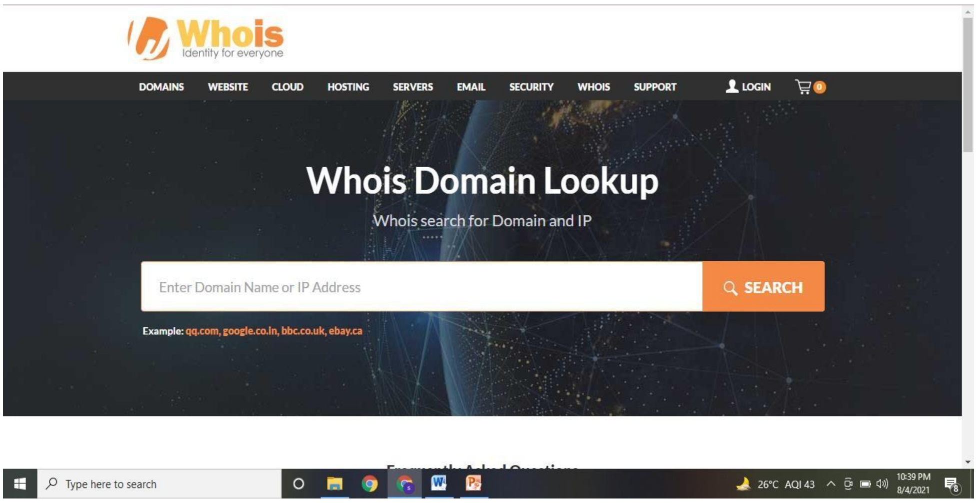
Some of the common tools used for footprinting and information gathering are as follows:

- Whois
- NSlookup
- Sam Spade
- SuperScan
- Nmap
- TcpView
- My ip Suite
- Dns enumerator
- Spider Foot
- Nessus
- Zone Transfer
- Port Scan
- HTTP Header Grabber



Foot Printing / Reconnaissance Tools	
Software	Platform
Samspade	Windows
Dmitry	Linux
Traceroute / mtr	Win / Linux / Mac
SpiderFoot	Windows / Linux
http://www.netcraft.com	Web
http://who.is/	Web
http://yougetsignal.com	Web
http://shodanhq.com	Web
http://readnotify.com/	Web
http://dnsstuff.com/	Web

1) https://www.whois.com/whois/



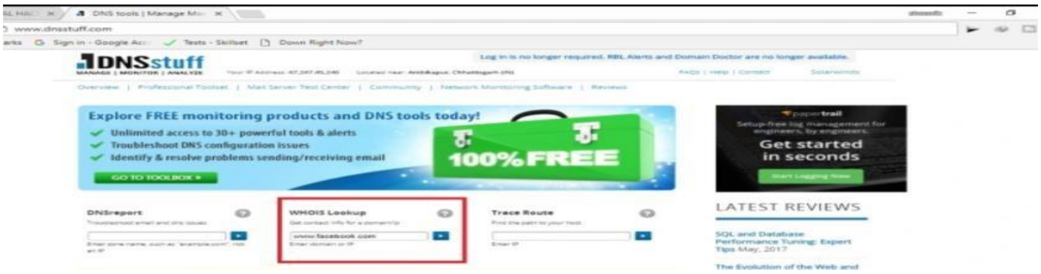
Whois Domain Lookup

Whois search for Domain and IP

Enter Domain Name or IP Address

Example: qq.com, google.co.in, bbc.co.uk, ebay.ca

3. www.dnsstuff.com



Log in is no longer required. RBL Alerts and Domain Doctor are no longer available.

Explore FREE monitoring products and DNS tools today!

- Unlimited access to 30+ powerful tools & alerts
- Troubleshoot DNS configuration issues
- Identify & resolve problems sending/receiving email

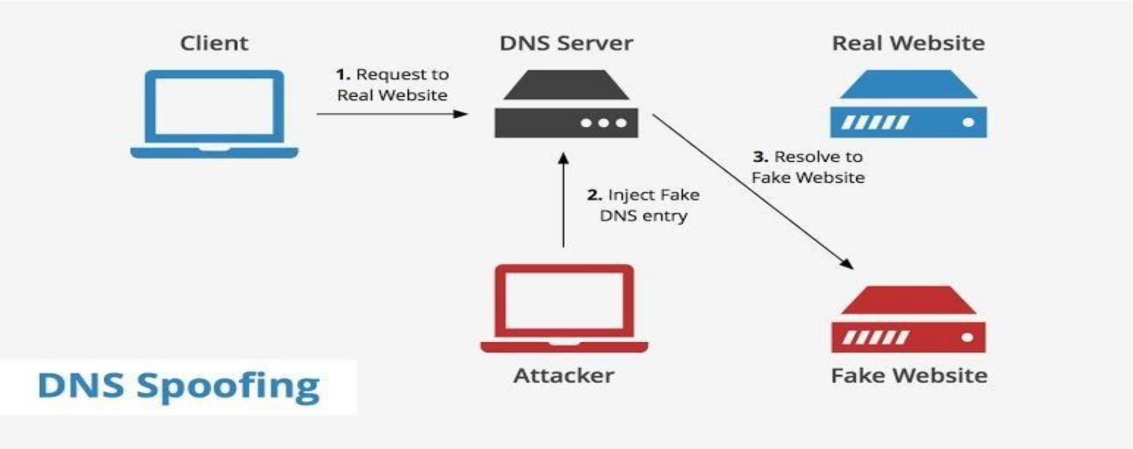
SQL and Database Performance Tuning: Expert Tips May, 2017

The Evolution of the Web and

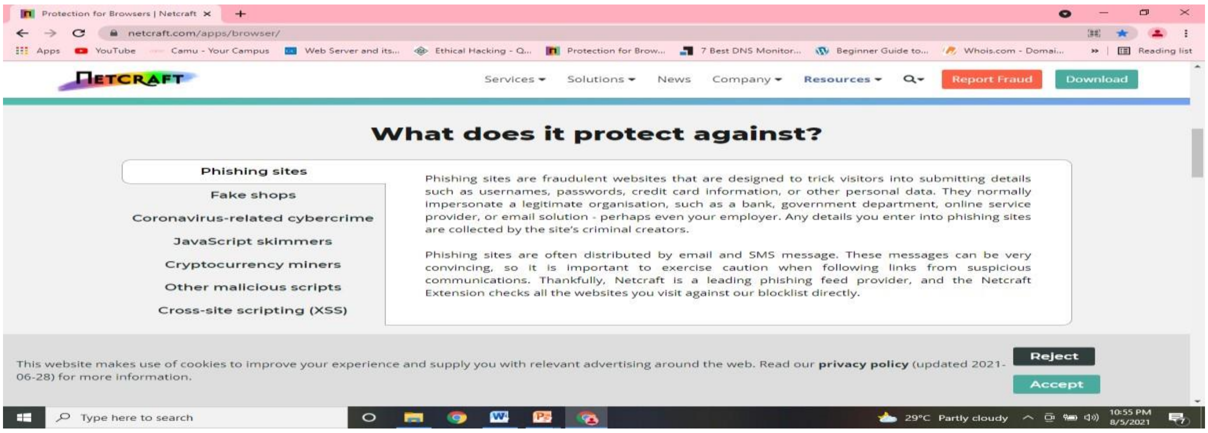
DNS Information Tools

What is DNS?

- The Domain Name System (DNS) maps human-readable domain names (in URLs or in email address) to IP addresses.
- For example, DNS translates and maps the domain freecodecamp.org to the IP address 104.26.2.33



- https://www.netcraft.com/apps/browser/



What does it protect against?

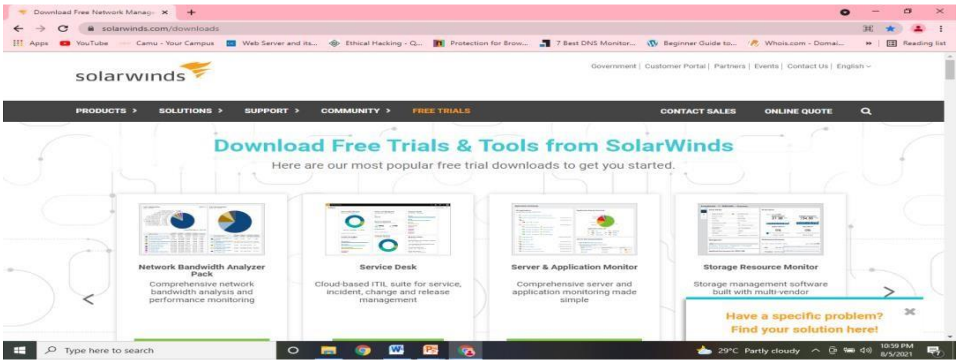
- Phishing sites
- Fake shops
- Coronavirus-related cybercrime
- JavaScript skimmers
- Cryptocurrency miners
- Other malicious scripts
- Cross-site scripting (XSS)

Phishing sites are fraudulent websites that are designed to trick visitors into submitting details such as usernames, passwords, credit card information, or other personal data. They normally impersonate a legitimate organisation, such as a bank, government department, online service provider, or email solution - perhaps even your employer. Any details you enter into phishing sites are collected by the site's criminal creators.

Phishing sites are often distributed by email and SMS message. These messages can be very convincing, so it is important to exercise caution when following links from suspicious communications. Thankfully, Netcraft is a leading phishing feed provider, and the Netcraft Extension checks all the websites you visit against our blocklist directly.

This website makes use of cookies to improve your experience and supply you with relevant advertising around the web. Read our **privacy policy** (updated 2021-06-28) for more information.

- https://www.solarwinds.com/downloads



Download Free Trials & Tools from SolarWinds

Here are our most popular free trial downloads to get you started.

Network Bandwidth Analyzer Pack: Comprehensive network bandwidth analysis and performance monitoring

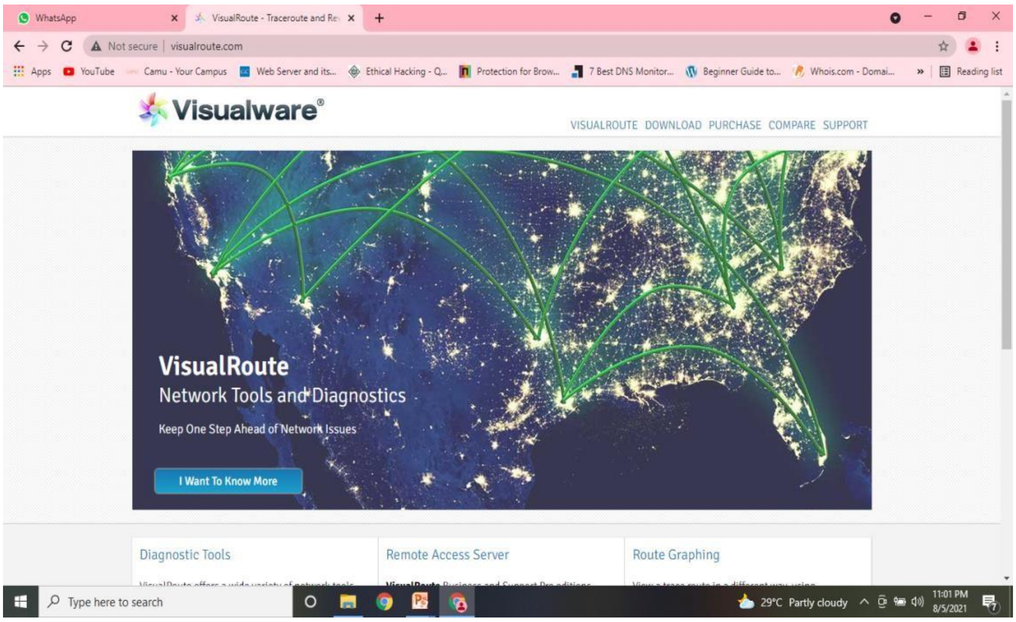
Service Desk: Cloud-based ITIL suite for service, incident, change and release management

Server & Application Monitor: Comprehensive server and application monitoring made simple

Storage Resource Monitor: Storage management software built with multi-vendor

Have a specific problem? Find your solution here!

Locating the Network Range



VisualRoute

Network Tools and Diagnostics

Keep One Step Ahead of Network Issues

Traceroute is the name of a tool used to determine the path of communication between two computers. Traceroute works by displaying each **hop**, the act of traveling from one point to the next on a network path, as a data packet travels to its destination.

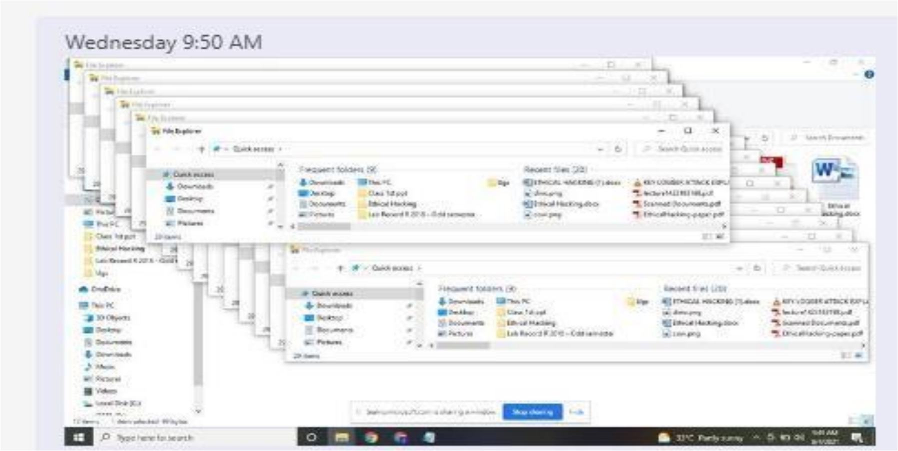
Example: Batch file

```
@echo off
:start
set /a var = var+1
explorer
if %var% EQU 20 goto end
goto start
:end
exit
```

---------------- save as - slow.bat

Output:

It Show multiple file look like malware attack


Wednesday 9:50 AM
File Explorer
Quick access
Frequent folders
Recent files