Sniffing is the process of monitoring and capturing all the packets passing through a given network using sniffing tools. It is a form of “tapping phone wires” and get to know about the conversation. It is also called **wiretapping**applied to the computer networks.

There is so much possibility that if a set of enterprise switch ports is open, then one of their employees can sniff the whole traffic of the network. Anyone in the same physical location can plug into the network using Ethernet cable or connect wirelessly to that network and sniff the total traffic.

In other words, Sniffing allows you to see all sorts of traffic, both protected and unprotected. In the right conditions and with the right protocols in place, an attacking party may be able to gather information that can be used for further attacks or to cause other issues for the network or system owner.

What can be sniffed?

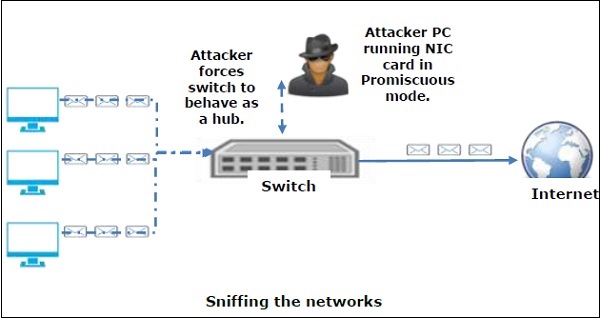
One can sniff the following sensitive information from a network −

* Email traffic
* FTP passwords
* Web traffics
* Telnet passwords
* Router configuration
* Chat sessions
* DNS traffic

How it works

A sniffer normally turns the NIC of the system to the **promiscuous mode** so that it listens to all the data transmitted on its segment.

Promiscuous mode refers to the unique way of Ethernet hardware, in particular, network interface cards (NICs), that allows an NIC to receive all traffic on the network, even if it is not addressed to this NIC. By default, a NIC ignores all traffic that is not addressed to it, which is done by comparing the destination address of the Ethernet packet with the hardware address (a.k.a. MAC) of the device. While this makes perfect sense for networking, non-promiscuous mode makes it difficult to use network monitoring and analysis software for diagnosing connectivity issues or traffic accounting.



A sniffer can continuously monitor all the traffic to a computer through the NIC by decoding the information encapsulated in the data packets.

Types of Sniffing

Sniffing can be either Active or Passive in nature.

Passive Sniffing

In passive sniffing, the traffic is locked but it is not altered in any way. Passive sniffing allows listening only. It works with Hub devices. On a hub device, the traffic is sent to all the ports. In a network that uses hubs to connect systems, all hosts on the network can see the traffic. Therefore, an attacker can easily capture traffic going through.

The good news is that hubs are almost obsolete nowadays. Most modern networks use switches. Hence, passive sniffing is no more effective.

Active Sniffing

In active sniffing, the traffic is not only locked and monitored, but it may also be altered in some way as determined by the attack. Active sniffing is used to sniff a switch-based network. It involves injecting **address resolution packets** (ARP) into a target network to flood on the switch **content addressable memory** (CAM) table. CAM keeps track of which host is connected to which port.

Following are the Active Sniffing Techniques −

* MAC Flooding
* DHCP Attacks
* DNS Poisoning
* Spoofing Attacks
* ARP Poisoning

Protocols which are affected

Protocols such as the tried and true TCP/IP were never designed with security in mind and therefore do not offer much resistance to potential intruders. Several rules lend themselves to easy sniffing −

* **HTTP** − It is used to send information in the clear text without any encryption and thus a real target.
* **SMTP** (Simple Mail Transfer Protocol) − SMTP is basically utilized in the transfer of emails. This protocol is efficient, but it does not include any protection against sniffing.
* **NNTP** (Network News Transfer Protocol)− It is used for all types of communications, but its main drawback is that data and even passwords are sent over the network as clear text.
* **POP** (Post Office Protocol) − POP is strictly used to receive emails from the servers. This protocol does not include protection against sniffing because it can be trapped.
* **FTP** (File Transfer Protocol) − FTP is used to send and receive files, but it does not offer any security features. All the data is sent as clear text that can be easily sniffed.
* **IMAP** (Internet Message Access Protocol) − IMAP is same as SMTP in its functions, but it is highly vulnerable to sniffing.
* **Telnet** − Telnet sends everything (usernames, passwords, keystrokes) over the network as clear text and hence, it can be easily sniffed.

Sniffers are not the dumb utilities that allow you to view only live traffic. If you really want to analyze each packet, save the capture and review it whenever time allows.

Hardware Protocol Analyzers

Before we go into further details of sniffers, it is important that we discuss about **hardware protocol analyzers**. These devices plug into the network at the hardware level and can monitor traffic without manipulating it.

* Hardware protocol analyzers are used to monitor and identify malicious network traffic generated by hacking software installed in the system.
* They capture a data packet, decode it, and analyze its content according to certain rules.
* Hardware protocol analyzers allow attackers to see individual data bytes of each packet passing through the cable.

These hardware devices are not readily available to most ethical hackers due to their enormous cost in many cases.

Lawful Interception

Lawful Interception (LI) is defined as legally sanctioned access to communications network data such as telephone calls or email messages. LI must always be in pursuance of a lawful authority for the purpose of analysis or evidence. Therefore, LI is a security process in which a network operator or service provider gives law enforcement officials permission to access private communications of individuals or organizations.

Almost all countries have drafted and enacted legislation to regulate lawful interception procedures; standardization groups are creating LI technology specifications. Usually, LI activities are taken for the purpose of infrastructure protection and cyber security. However, operators of private network infrastructures can maintain LI capabilities within their own networks as an inherent right, unless otherwise prohibited.

LI was formerly known as **wiretapping** and has existed since the inception of electronic communications.

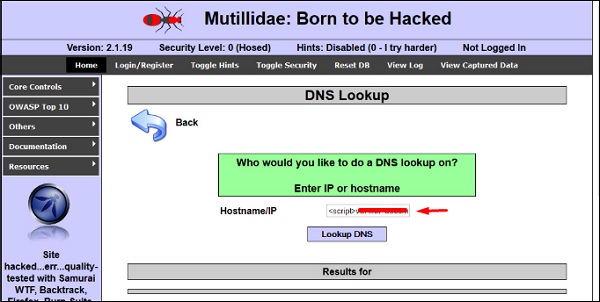
Cross-site scripting (XSS) is a code injection attack that allows an attacker to execute malicious JavaScript in another user's browser.

The attacker does not directly target his victim. Instead, he exploits a vulnerability in a website that the victim visits, in order to get the website to deliver the malicious JavaScript for him. To the victim's browser, the malicious JavaScript appears to be a legitimate part of the website, and the website has thus acted as an unintentional accomplice to the attacker. These attacks can be carried out using HTML, JavaScript, VBScript, ActiveX, Flash, but the most used XSS is malicious JavaScript.

These attacks also can gather data from account hijacking, changing of user settings, cookie theft/poisoning, or false advertising and create DoS attacks.

Example

Let’s take an example to understand how it works. We have a vulnerable webpage that we got by the **metasploitable** machine. Now we will test the field that is highlighted in red arrow for XSS.



First of all, we make a simple alert script

<script>

alert(‘I am Vulnerable’)

</script>

It will produce the following output −



Types of XSS Attacks

XSS attacks are often divided into three types −

* **Persistent XSS,** where the malicious string originates from the website's database.
* **Reflected XSS,** where the malicious string originates from the victim's request.
* **DOM-based XSS,** where the vulnerability is in the client-side code rather than the server-side code.

Generally, cross-site scripting is found by **vulnerability scanners** so that you don’t have to do all the manual job by putting a JavaScript on it like

<script>

alert('XSS')

</script>

**Burp Suite** and **acunetix** are considered as the best vulnerability scanners.

# Ethical Hacking - SQL Injection

SQL injection is a set of SQL commands that are placed in a URL string or in data structures in order to retrieve a response that we want from the databases that are connected with the web applications. This type of attacks generally takes place on webpages developed using PHP or ASP.NET.

An SQL injection attack can be done with the following intentions −

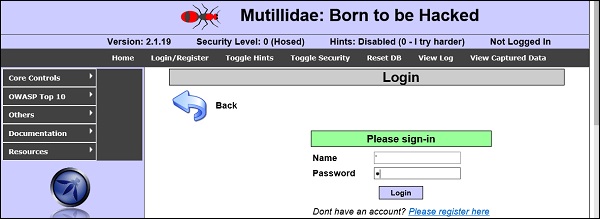
* To dump the whole database of a system,
* To modify the content of the databases, or
* To perform different queries that are not allowed by the application.

This type of attack works when the applications don’t validate the inputs properly, before passing them to an SQL statement. Injections are normally placed put in address bars, search fields, or data fields.

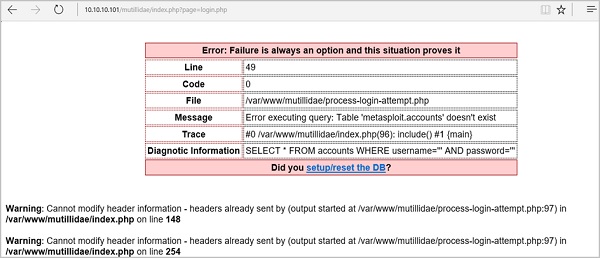
The easiest way to detect if a web application is vulnerable to an SQL injection attack is to use the " ‘ " character in a string and see if you get any error.

Example 1

Let’s try to understand this concept using a few examples. As shown in the following screenshot, we have used a " ‘ " character in the Name field.



Now, click the **Login** button. It should produce the following response −



It means that the “Name” field is vulnerable to SQL injection.

Example 2

We have this URL − **http://10.10.10.101/mutillidae/index.php?page=site-footer-xssdiscussion.php**

And we want to test the variable “page” but observe how we have injected a " ‘ " character in the string URL.



When we press Enter, it will produce the following result which is with errors.



SQLMAP

SQLMAP is one of the best tools available to detect SQL injections. It can be downloaded from <http://sqlmap.org/>

It comes pre-compiled in the Kali distribution. You can locate it at − Applications → Database Assessment → Sqlmap.

After opening SQLMAP, we go to the page that we have the SQL injection and then get the header request. From the header, we run the following command in SQL −

./sqlmap.py --headers="User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:25.0)

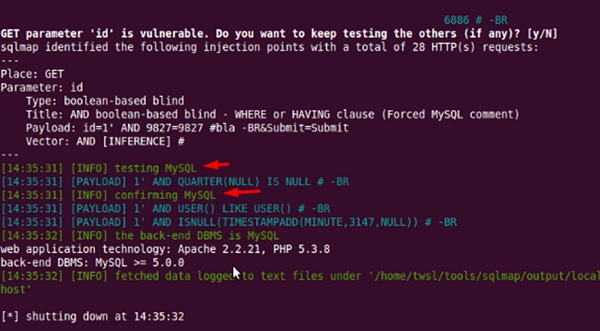
Gecko/20100101 Firefox/25.0" --cookie="security=low;

PHPSESSID=oikbs8qcic2omf5gnd09kihsm7" -u '

http://localhost/dvwa/vulnerabilities/sqli\_blind/?id=1&Submit=Submit#' -

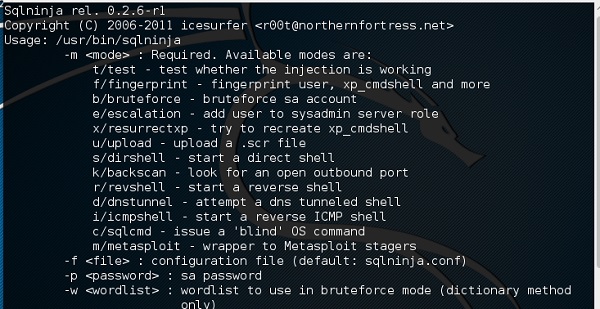
level=5 risk=3 -p id --suffix="-BR" -v3

The SQLMAP will test all the variables and the result will show that the parameter “id” is vulnerable, as shown in the following screenshot.



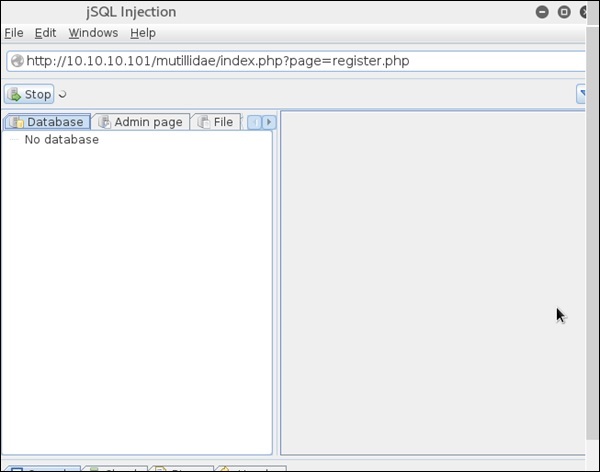
SQLNinja

SQLNinja is another SQL injection tool that is available in Kali distribution.



JSQL Injection

JSQL Injection is in Java and it makes automated SQL injections.



# Ethical Hacking - Metasploit

Metasploit is one of the most powerful exploit tools. Most of its resources can be found at: [https://www.metasploit.com](https://www.metasploit.com/). It comes in two versions − **commercial** and **free edition**. There are no major differences in the two versions, so in this tutorial, we will be mostly using the Community version (free) of Metasploit.

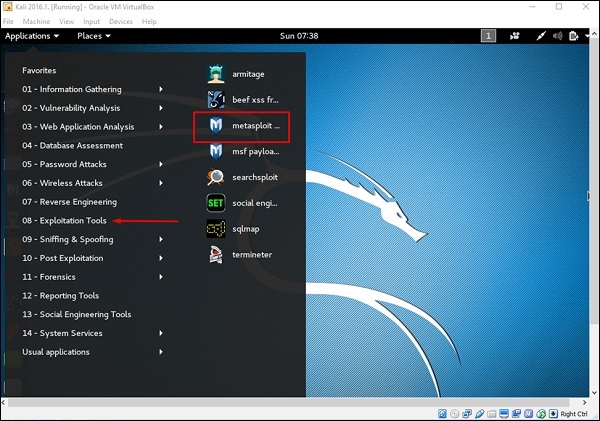
As an Ethical Hacker, you will be using “Kali Distribution” which has the Metasploit community version embedded in it along with other ethical hacking tools. But if you want to install Metasploit as a separate tool, you can easily do so on systems that run on Linux, Windows, or Mac OS X.

The hardware requirements to install Metasploit are −

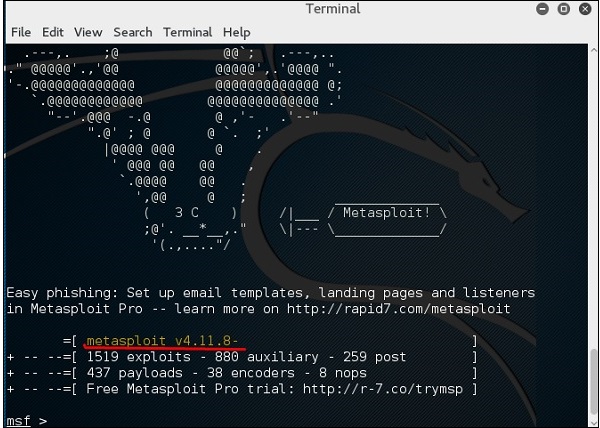
* 2 GHz+ processor
* 1 GB RAM available
* 1 GB+ available disk space

Matasploit can be used either with command prompt or with Web UI.

To open in Kali, go to Applications → Exploitation Tools → metasploit.



After Metasploit starts, you will see the following screen. Highlighted in red underline is the version of Metasploit.

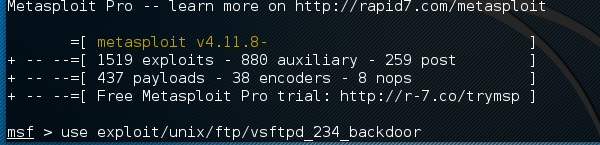


Exploits of Metasploit

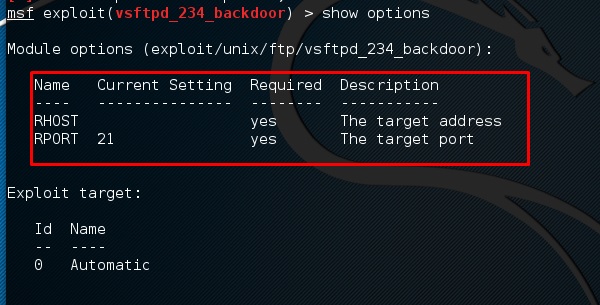
From Vulnerability Scanner, we found that the Linux machine that we have for test is vulnerable to FTP service. Now, we will use the exploit that can work for us. The command is −

use “exploit path”

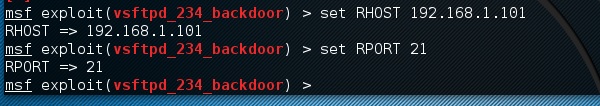
The screen will appear as follows −



Then type **mfs> show options** in order to see what parameters you have to set in order to make it functional. As shown in the following screenshot, we have to set RHOST as the “target IP”.



We type **msf> set RHOST 192.168.1.101 and msf>set RPORT 21**



Then, type **mfs>run**. If the exploit is successful, then it will open one session that you can interact with, as shown in the following screenshot.



Metasploit Payloads

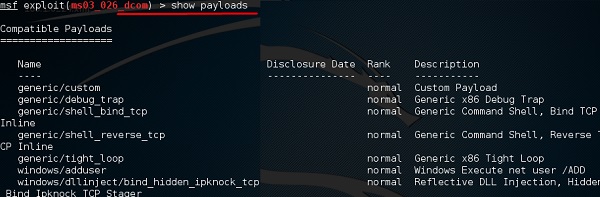
Payload, in simple terms, are simple scripts that the hackers utilize to interact with a hacked system. Using payloads, they can transfer data to a victim system.

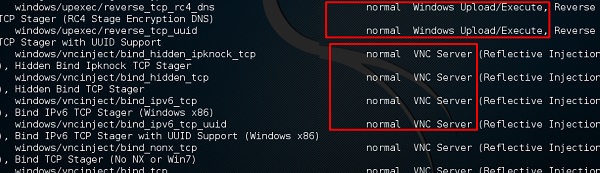
Metasploit payloads can be of three types −

* **Singles** − Singles are very small and designed to create some kind of communication, then move to the next stage. For example, just creating a user.
* **Staged** − It is a payload that an attacker can use to upload a bigger file onto a victim system.
* **Stages** − Stages are payload components that are downloaded by Stagers modules. The various payload stages provide advanced features with no size limits such as Meterpreter and VNC Injection.

Payload Usage − Example

We use the command **show payloads**. With this exploit, we can see the payloads that we can use, and it will also show the payloads that will help us upload /execute files onto a victim system.

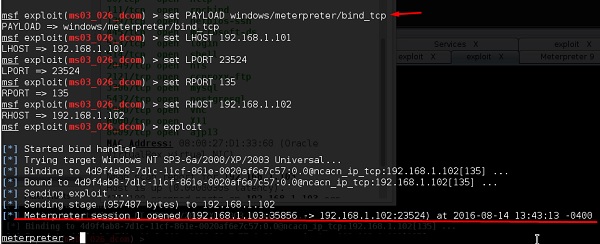




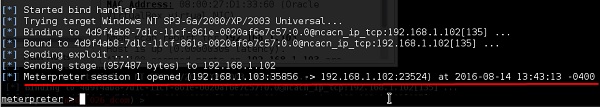
To set the payload that we want, we will use the following command −

set PAYLOAD payload/path

Set the listen host and listen port (LHOST, LPORT) which are the **attacker IP**and **port**. Then set remote host and port (RPORT, LHOST) which are the **victim IP** and **port**.



Type “exploit”. It will create a session as shown below −



Now we can play with the system according to the settings that this payload offers.

# Sniffing Tools

There are so many tools available to perform sniffing over a network, and they all have their own features to help a hacker analyze traffic and dissect the information. Sniffing tools are extremely common applications. We have listed here some of the interesting ones −

* **BetterCAP** − BetterCAP is a powerful, flexible and portable tool created to perform various types of MITM attacks against a network, manipulate HTTP, HTTPS and TCP traffic in real-time, sniff for credentials, and much more.
* **Ettercap** − Ettercap is a comprehensive suite for man-in-the-middle attacks. It features sniffing of live connections, content filtering on the fly and many other interesting tricks. It supports active and passive dissection of many protocols and includes many features for network and host analysis.
* **Wireshark** − It is one of the most widely known and used packet sniffers. It offers a tremendous number of features designed to assist in the dissection and analysis of traffic.
* **Tcpdump** − It is a well-known command-line packet analyzer. It provides the ability to intercept and observe TCP/IP and other packets during transmission over the network. Available at www.tcpdump.org.
* **WinDump** − A Windows port of the popular Linux packet sniffer tcpdump, which is a command-line tool that is perfect for displaying header information.
* **OmniPeek** − Manufactured by WildPackets, OmniPeek is a commercial product that is the evolution of the product EtherPeek.
* **Dsniff** − A suite of tools designed to perform sniffing with different protocols with the intent of intercepting and revealing passwords. Dsniff is designed for Unix and Linux platforms and does not have a full equivalent on the Windows platform.
* **EtherApe** − It is a Linux/Unix tool designed to display graphically a system's incoming and outgoing connections.
* **MSN Sniffer** − It is a sniffing utility specifically designed for sniffing traffic generated by the MSN Messenger application.
* **NetWitness NextGen** − It includes a hardware-based sniffer, along with other features, designed to monitor and analyze all traffic on a network. This tool is used by the FBI and other law enforcement agencies.

A potential hacker can use any of these sniffing tools to analyze traffic on a network and dissect information.

# Trojan Attacks

Trojans are non-replication programs; they don’t reproduce their own codes by attaching themselves to other executable codes. They operate without the permissions or knowledge of the computer users.

Trojans hide themselves in healthy processes. However we should underline that Trojans infect outside machines only with the assistance of a computer user, like clicking a file that comes attached with email from an unknown person, plugging USB without scanning, opening unsafe URLs.

Trojans have several malicious functions −

* They create backdoors to a system. Hackers can use these backdoors to access a victim system and its files. A hacker can use Trojans to edit and delete the files present on a victim system, or to observe the activities of the victim.
* Trojans can steal all your financial data like bank accounts, transaction details, PayPal related information, etc. These are called **Trojan-Banker**.
* Trojans can use the victim computer to attack other systems using Denial of Services.
* Trojans can encrypt all your files and the hacker may thereafter demand money to decrypt them. These are **Ransomware Trojans**.
* They can use your phones to send SMS to third parties. These are called **SMS Trojans**.

## Trojan Information

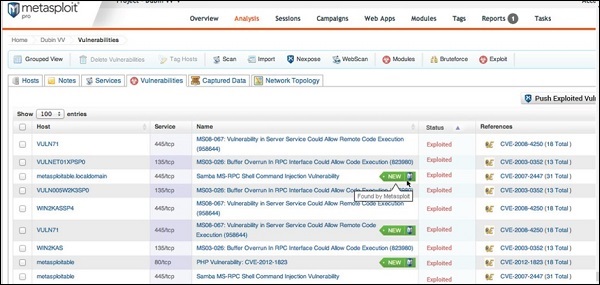
If you have found a virus and want to investigate further regarding its function, then we will recommend that you have a look at the following virus databases, which are offered generally by antivirus vendors.

* **Kaspersky Virus database** − [https://www.kaspersky.com](https://www.kaspersky.com/viruswatchlite?hour_offset=-1)
* **F-secure** − [https://www.f-secure.com](https://www.f-secure.com/en/web/labs_global/threat-descriptions)
* **Symantec – Virus Encyclopedia** − [https://www.symantec.com](https://www.symantec.com/security_response/landing/azlisting.jsp)

# Exploitation

Exploitation is a piece of programmed software or script which can allow hackers to take control over a system, exploiting its vulnerabilities. Hackers normally use vulnerability scanners like Nessus, Nexpose, OpenVAS, etc. to find these vulnerabilities.

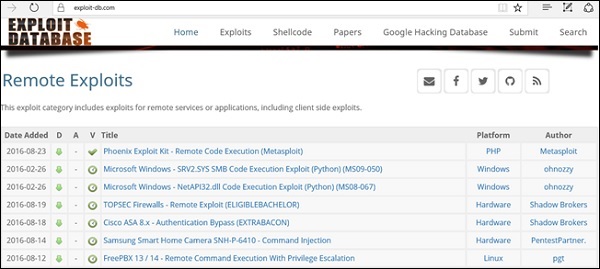
Metasploit is a powerful tool to locate vulnerabilities in a system.



Based on the vulnerabilities, we find exploits. Here, we will discuss some of the best vulnerability search engines that you can use.

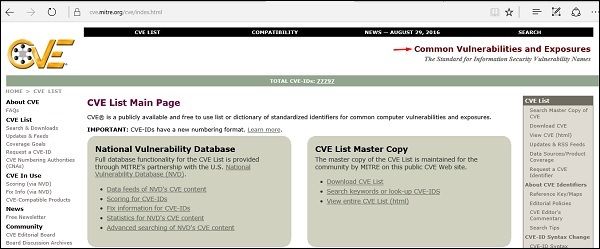
Exploit Database

[www.exploit-db.com](https://www.exploit-db.com/) is the place where you can find all the exploits related to a vulnerability.



Common Vulnerabilities and Exposures

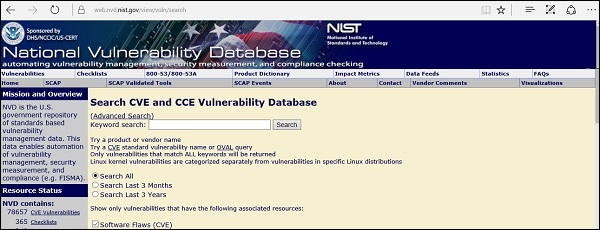
Common Vulnerabilities and Exposures (CVE) is the standard for information security vulnerability names. CVE is a dictionary of publicly known information security vulnerabilities and exposures. It’s free for public use. [https://cve.mitre.org](https://cve.mitre.org/)



National Vulnerability Database

National Vulnerability Database (NVD) is the U.S. government repository of standards based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance. You can locate this database at − [https://nvd.nist.gov](https://nvd.nist.gov/)

NVD includes databases of security checklists, security-related software flaws, misconfigurations, product names, and impact metrics.



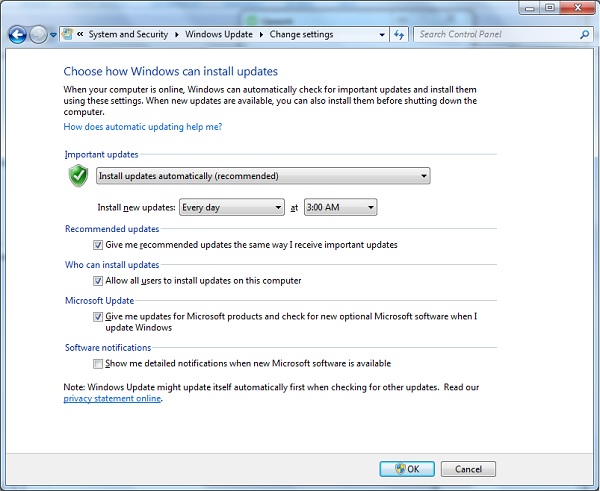
In general, you will see that there are two types of exploits −

* **Remote Exploits** − These are the type of exploits where you don’t have access to a remote system or network. Hackers use remote exploits to gain access to systems that are located at remote places.
* **Local Exploits** − Local exploits are generally used by a system user having access to a local system, but who wants to overpass his rights.

Quick Fix

Vulnerabilities generally arise due to missing updates, so it is recommended that you update your system on a regular basis, for example, once a week.

In Windows environment, you can activate automatic updates by using the options available in the Control Panel → System and Security → Windows Updates.



In Linux Centos, you can use the following command to install automatic update package.

yum -y install yum-cron

# Ethical Hacking - Tools

## NMAP

Nmap stands for Network Mapper. It is an open source tool that is used widely for network discovery and security auditing. Nmap was originally designed to scan large networks, but it can work equally well for single hosts. Network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime.

Nmap uses raw IP packets to determine −

* what hosts are available on the network,
* what services those hosts are offering,
* what operating systems they are running on,
* what type of firewalls are in use, and other such characteristics.

Nmap runs on all major computer operating systems such as Windows, Mac OS X, and Linux.

## Metasploit

Metasploit is one of the most powerful exploit tools. It’s a product of Rapid7 and most of its resources can be found at: www.metasploit.com. It comes in two versions − **commercial** and **free edition**. Matasploit can be used with command prompt or with Web UI.

With Metasploit, you can perform the following operations −

* Conduct basic penetration tests on small networks
* Run spot checks on the exploitability of vulnerabilities
* Discover the network or import scan data
* Browse exploit modules and run individual exploits on hosts

## Burp Suit

Burp Suite is a popular platform that is widely used for performing security testing of web applications. It has various tools that work in collaboration to support the entire testing process, from initial mapping and analysis of an application's attack surface, through to finding and exploiting security vulnerabilities.

Burp is easy to use and provides the administrators full control to combine advanced manual techniques with automation for efficient testing. Burp can be easily configured and it contains features to assist even the most experienced testers with their work.

## Angry IP Scanner

Angry IP scanner is a lightweight, cross-platform IP address and port scanner. It can scan IP addresses in any range. It can be freely copied and used anywhere. In order to increase the scanning speed, it uses multithreaded approach, wherein a separate scanning thread is created for each scanned IP address.

Angry IP Scanner simply pings each IP address to check if it’s alive, and then, it resolves its hostname, determines the MAC address, scans ports, etc. The amount of gathered data about each host can be saved to TXT, XML, CSV, or IP-Port list files. With help of plugins, Angry IP Scanner can gather any information about scanned IPs.

## Cain & Abel

Cain & Abel is a password recovery tool for Microsoft Operating Systems. It helps in easy recovery of various kinds of passwords by employing any of the following methods −

* sniffing the network,
* cracking encrypted passwords using Dictionary, Brute-Force and Cryptanalysis attacks,
* recording VoIP conversations,
* decoding scrambled passwords,
* recovering wireless network keys,
* revealing password boxes,
* uncovering cached passwords and analyzing routing protocols.

Cain & Abel is a useful tool for security consultants, professional penetration testers and everyone else who plans to use it for ethical reasons.

## Ettercap

Ettercap stands for Ethernet Capture. It is a network security tool for Man-in-the-Middle attacks. It features sniffing of live connections, content filtering on the fly and many other interesting tricks. Ettercap has inbuilt features for network and host analysis. It supports active and passive dissection of many protocols.

You can run Ettercap on all the popular operating systems such as Windows, Linux, and Mac OS X.

## EtherPeek

EtherPeek is a wonderful tool that simplifies network analysis in a multiprotocol heterogeneous network environment. EtherPeek is a small tool (less than 2 MB) that can be easily installed in a matter of few minutes.

EtherPeek proactively sniffs traffic packets on a network. By default, EtherPeek supports protocols such as AppleTalk, IP, IP Address Resolution Protocol (ARP), NetWare, TCP, UDP, NetBEUI, and NBT packets.

## SuperScan

SuperScan is a powerful tool for network administrators to scan TCP ports and resolve hostnames. It has a user friendly interface that you can use to −

* Perform ping scans and port scans using any IP range.
* Scan any port range from a built-in list or any given range.
* View responses from connected hosts.
* Modify the port list and port descriptions using the built in editor.
* Merge port lists to build new ones.
* Connect to any discovered open port.
* Assign a custom helper application to any port.

## QualysGuard

QualysGuard is an integrated suite of tools that can be utilized to simplify security operations and lower the cost of compliance. It delivers critical security intelligence on demand and automates the full spectrum of auditing, compliance and protection for IT systems and web applications.

QualysGuard includes a set of tools that can monitor, detect, and protect your global network.

## WebInspect

WebInspect is a web application security assessment tool that helps identify known and unknown vulnerabilities within the Web application layer.

It can also help check that a Web server is configured properly, and attempts common web attacks such as parameter injection, cross-site scripting, directory traversal, and more.

## LC4

LC4 was formerly known as **L0phtCrack**. It is a password auditing and recovery application. It is used to test password strength and sometimes to recover lost Microsoft Windows passwords, by using dictionary, brute-force, and hybrid attacks.

LC4 recovers Windows user account passwords to streamline migration of users to another authentication system or to access accounts whose passwords are lost.

## LANguard Network Security Scanner

LANguard Network Scanner monitors a network by scanning connected machines and providing information about each node. You can obtain information about each individual operating system.

It can also detect registry issues and have a report set up in HTML format. For each computer, you can list the **netbios** name table, current logged-on user, and Mac address.

## Network Stumbler

Network stumbler is a WiFi scanner and monitoring tool for Windows. It allows network professionals to detect WLANs. It is widely used by networking enthusiasts and hackers because it helps you find non-broadcasting wireless networks.

Network Stumbler can be used to verify if a network is well configured, its signal strength or coverage, and detect interference between one or more wireless networks. It can also be used to non-authorized connections.

## ToneLoc

ToneLoc stands for Tone Locator. It was a popular war dialling computer program written for MS-DOS in the early 90’s. War dialling is a technique of using a modem to automatically scan a list of telephone numbers, usually dialling every number in a local area code.

Malicious hackers use the resulting lists in breaching computer security - for guessing user accounts, or locating modems that might provide an entry-point into computer or other electronic systems.

It can be used by security personnel to detect unauthorized devices on a company’s telephone network.

# ARP Poisoning

Address Resolution Protocol (ARP) is a stateless protocol used for resolving IP addresses to machine MAC addresses. All network devices that need to communicate on the network broadcast ARP queries in the system to find out other machines’ MAC addresses. ARP Poisoning is also known as **ARP Spoofing**.

Here is how ARP works −

* When one machine needs to communicate with another, it looks up its ARP table.
* If the MAC address is not found in the table, the **ARP\_request** is broadcasted over the network.
* All machines on the network will compare this IP address to MAC address.
* If one of the machines in the network identifies this address, then it will respond to the **ARP\_request** with its IP and MAC address.
* The requesting computer will store the address pair in its ARP table and communication will take place.

What is ARP Spoofing?

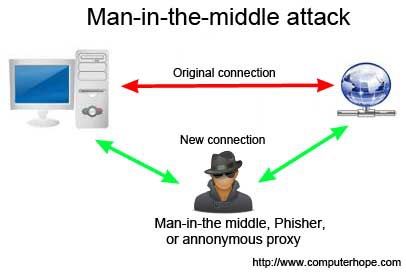
ARP packets can be forged to send data to the attacker’s machine.

* ARP spoofing constructs a large number of forged ARP request and reply packets to overload the switch.
* The switch is set in **forwarding mode** and after the **ARP table** is flooded with spoofed ARP responses, the attackers can sniff all network packets.

Attackers flood a target computer ARP cache with forged entries, which is also known as **poisoning**. ARP poisoning uses Man-in-the-Middle access to poison the network.

What is MITM?

The Man-in-the-Middle attack (abbreviated MITM, MitM, MIM, MiM, MITMA) implies an active attack where the adversary impersonates the user by creating a connection between the victims and sends messages between them. In this case, the victims think that they are communicating with each other, but in reality, the malicious actor controls the communication.



A third person exists to control and monitor the traffic of communication between two parties. Some protocols such as **SSL** serve to prevent this type of attack.

ARP Poisoning − Exercise

In this exercise, we have used **BetterCAP** to perform ARP poisoning in LAN environment using VMware workstation in which we have installed **Kali** Linux and **Ettercap** tool to sniff the local traffic in LAN.

For this exercise, you would need the following tools −

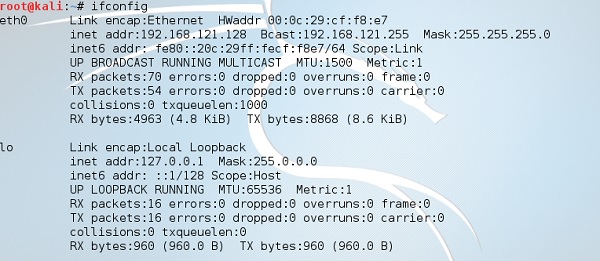
* VMware workstation
* Kali Linux or Linux Operating system
* Ettercap Tool
* LAN connection

**Note** − This attack is possible in wired and wireless networks. You can perform this attack in local LAN.

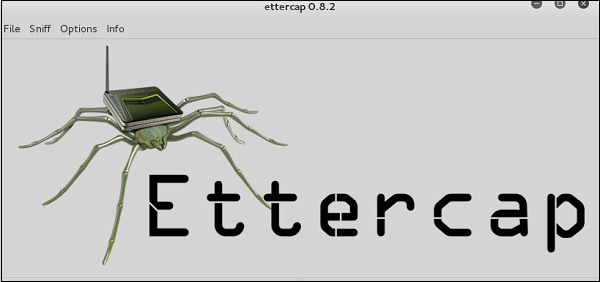
**Step 1** − Install the VMware workstation and install the Kali Linux operating system.

**Step 2** − Login into the Kali Linux using username pass “root, toor”.

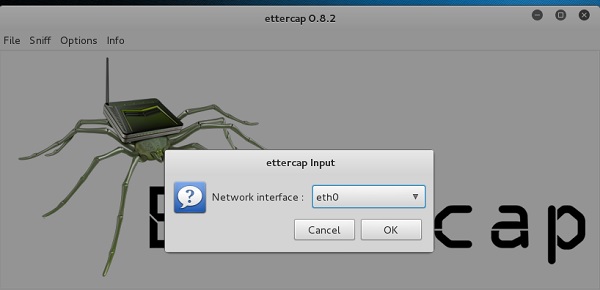
**Step 3** − Make sure you are connected to local LAN and check the IP address by typing the command **ifconfig** in the terminal.



**Step 4** − Open up the terminal and type “Ettercap –G” to start the graphical version of Ettercap.

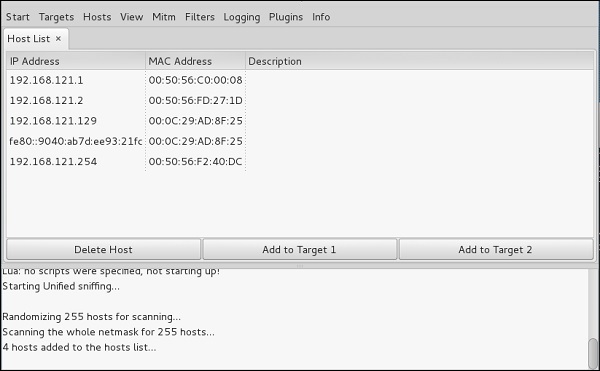


**Step 5** − Now click the tab “sniff” in the menu bar and select “unified sniffing” and click OK to select the interface. We are going to use “eth0” which means Ethernet connection.



**Step 6** − Now click the “hosts” tab in the menu bar and click “scan for hosts”. It will start scanning the whole network for the alive hosts.

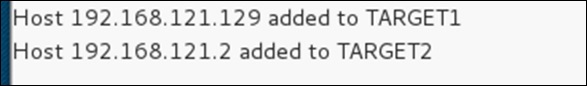
**Step 7** − Next, click the “hosts” tab and select “hosts list” to see the number of hosts available in the network. This list also includes the default gateway address. We have to be careful when we select the targets.



**Step 8** − Now we have to choose the targets. In MITM, our target is the host machine, and the route will be the router address to forward the traffic. In an MITM attack, the attacker intercepts the network and sniffs the packets. So, we will add the victim as “target 1” and the router address as “target 2.”

In VMware environment, the default gateway will always end with “2” because “1” is assigned to the physical machine.

**Step 9** − In this scenario, our target is “192.168.121.129” and the router is “192.168.121.2”. So we will add target 1 as **victim IP** and target 2 as **router IP**.



**Step 10** − Now click on “MITM” and click “ARP poisoning”. Thereafter, check the option “Sniff remote connections” and click OK.



**Step 11** − Click “start” and select “start sniffing”. This will start ARP poisoning in the network which means we have enabled our network card in “promiscuous mode” and now the local traffic can be sniffed.

**Note** − We have allowed only HTTP sniffing with Ettercap, so don’t expect HTTPS packets to be sniffed with this process.

**Step 12** − Now it’s time to see the results; if our victim logged into some websites. You can see the results in the toolbar of Ettercap.



This is how sniffing works. You must have understood how easy it is to get the HTTP credentials just by enabling ARP poisoning.

ARP Poisoning has the potential to cause huge losses in company environments. This is the place where ethical hackers are appointed to secure the networks.

Like ARP poisoning, there are other attacks such as MAC flooding, MAC spoofing, DNS poisoning, ICMP poisoning, etc. that can cause significant loss to a network.

In the next chapter, we will discuss another type of attack known as **DNS poisoning**.

# DDOS Attacks

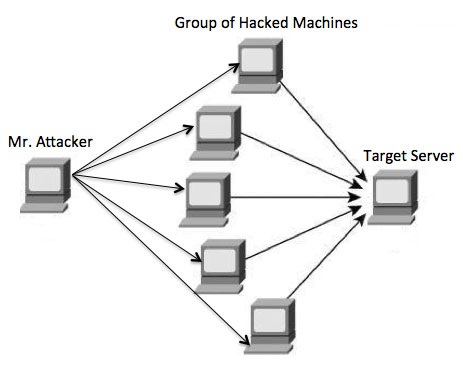
A Distributed Denial of Service (DDoS) attack is an attempt to make an online service or a website unavailable by overloading it with huge floods of traffic generated from multiple sources.

Unlike a Denial of Service (DoS) attack, in which one computer and one Internet connection is used to flood a targeted resource with packets, a DDoS attack uses many computers and many Internet connections, often distributed globally in what is referred to as a **botnet**.

A large scale volumetric DDoS attack can generate a traffic measured in tens of Gigabits (and even hundreds of Gigabits) per second. We are sure your normal network will not be able to handle such traffic.

What are Botnets?

Attackers build a network of hacked machines which are known as **botnets**, by spreading malicious piece of code through emails, websites, and social media. Once these computers are infected, they can be controlled remotely, without their owners' knowledge, and used like an army to launch an attack against any target.



A DDoS flood can be generated in multiple ways. For example −

* Botnets can be used for sending more number of connection requests than a server can handle at a time.
* Attackers can have computers send a victim resource huge amounts of random data to use up the target's bandwidth.

Due to the distributed nature of these machines, they can be used to generate distributed high traffic which may be difficult to handle. It finally results in a complete blockage of a service.

Types of DDoS Attacks

DDoS attacks can be broadly categorized into three categories −

* Volume-based Attacks
* Protocol Attacks
* Application Layer Attacks

Volume-Based Attacks

Volume-based attacks include TCP floods, UDP floods, ICMP floods, and other spoofedpacket floods. These are also called **Layer 3 & 4 Attacks**. Here, an attacker tries to saturate the bandwidth of the target site. The attack magnitude is measured in **Bits per Second** (bps).

* **UDP Flood** − A UDP flood is used to flood random ports on a remote host with numerous UDP packets, more specifically port number 53. Specialized firewalls can be used to filter out or block malicious UDP packets.
* **ICMP Flood** − This is similar to UDP flood and used to flood a remote host with numerous ICMP Echo Requests. This type of attack can consume both outgoing and incoming bandwidth and a high volume of ping requests will result in overall system slowdown.
* **HTTP Flood** − The attacker sends HTTP GET and POST requests to a targeted web server in a large volume which cannot be handled by the server and leads to denial of additional connections from legitimate clients.
* **Amplification Attack** − The attacker makes a request that generates a large response which includes DNS requests for large TXT records and HTTP GET requests for large files like images, PDFs, or any other data files.

Protocol Attacks

Protocol attacks include SYN floods, Ping of Death, fragmented packet attacks, Smurf DDoS, etc. This type of attack consumes actual server resources and other resources like firewalls and load balancers. The attack magnitude is measured in **Packets per Second**.

* **DNS Flood** − DNS floods are used for attacking both the infrastructure and a DNS application to overwhelm a target system and consume all its available network bandwidth.
* **SYN Flood** − The attacker sends TCP connection requests faster than the targeted machine can process them, causing network saturation. Administrators can tweak TCP stacks to mitigate the effect of SYN floods. To reduce the effect of SYN floods, you can reduce the timeout until a stack frees memory allocated to a connection, or selectively dropping incoming connections using a firewall or **iptables**.
* **Ping of Death** − The attacker sends malformed or oversized packets using a simple ping command. IP allows sending 65,535 bytes packets but sending a ping packet larger than 65,535 bytes violates the Internet Protocol and could cause memory overflow on the target system and finally crash the system. To avoid Ping of Death attacks and its variants, many sites block ICMP ping messages altogether at their firewalls.

Application Layer Attacks

Application Layer Attacks include Slowloris, Zero-day DDoS attacks, DDoS attacks that target Apache, Windows or OpenBSD vulnerabilities and more. Here the goal is to crash the web server. The attack magnitude is measured in **Requests per Second**.

* **Application Attack** − This is also called **Layer 7 Attack**, where the attacker makes excessive log-in, database-lookup, or search requests to overload the application. It is really difficult to detect Layer 7 attacks because they resemble legitimate website traffic.
* **Slowloris** − The attacker sends huge number of HTTP headers to a targeted web server, but never completes a request. The targeted server keeps each of these false connections open and eventually overflows the maximum concurrent connection pool, and leads to denial of additional connections from legitimate clients.
* **NTP Amplification** − The attacker exploits publically-accessible Network Time Protocol (NTP) servers to overwhelm the targeted server with User Datagram Protocol (UDP) traffic.
* **Zero-day DDoS Attacks** − A zero-day vulnerability is a system or application flaw previously unknown to the vendor, and has not been fixed or patched. These are new type of attacks coming into existence day by day, for example, exploiting vulnerabilities for which no patch has yet been released.

How to Fix a DDoS Attack

There are quite a few DDoS protection options which you can apply depending on the type of DDoS attack.

Your DDoS protection starts from identifying and closing all the possible OS and application level vulnerabilities in your system, closing all the possible ports, removing unnecessary access from the system and hiding your server behind a proxy or CDN system.

If you see a low magnitude of the DDoS, then you can find many firewall-based solutions which can help you in filtering out DDoS based traffic. But if you have high volume of DDoS attack like in gigabits or even more, then you should take the help of a DDoS protection service provider that offers a more holistic, proactive and genuine approach.

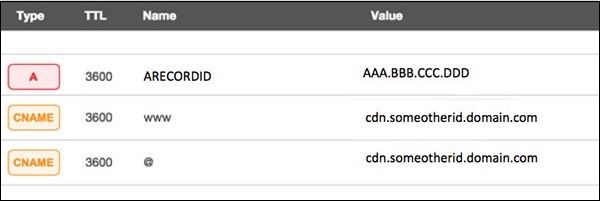
You must be careful while approaching and selecting a DDoS protection service provider. There are number of service providers who want to take advantage of your situation. If you inform them that you are under DDoS attack, then they will start offering you a variety of services at unreasonably high costs.

We can suggest you a simple and working solution which starts with a search for a good DNS solution provider who is flexible enough to configure A and CNAME records for your website. Second, you will need a good CDN provider that can handle big DDoS traffic and provide you DDoS protection service as a part of their CDN package.

Assume your server IP address is AAA.BBB.CCC.DDD. Then you should do the following DNS configuration −

* Create a **A Record** in DNS zone file as shown below with a DNS identifier, for example, **ARECORDID** and keep it secret from the outside world.
* Now ask your CDN provider to link the created DNS identifier with a URL, something like **cdn.someotherid.domain.com**.
* You will use the CDN URL cdn.someotherid.domain.com to create two CNAME records, the first one to point to **www** and the second record to point to @ as shown below.

You can take the help from your system administrator to understand these points and configure your DNS and CDN appropriately. Finally, you will have the following configuration at your DNS.



Now, let the CDN provider handle all type of DDoS attacks and your system will remain safe. But here the condition is that you should not disclose your system's IP address or A record identifier to anyone; else direct attacks will start again.

# Ethical Hacking - Social Engineering

## Example 1

You must have noticed old company documents being thrown into dustbins as garbage. These documents might contain sensitive information such as Names, Phone Numbers, Account Numbers, Social Security Numbers, Addresses, etc. Many companies still use carbon paper in their fax machines and once the roll is over, its carbon goes into dustbin which may have traces of sensitive data. Although it sounds improbable, but attackers can easily retrieve information from the company dumpsters by pilfering through the garbage.

## Example 2

An attacker may befriend a company personnel and establish good relationship with him over a period of time. This relationship can be established online through social networks, chatting rooms, or offline at a coffee table, in a playground, or through any other means. The attacker takes the office personnel in confidence and finally digs out the required sensitive information without giving a clue.

## Example 3

A social engineer may pretend to be an employee or a valid user or an VIP by faking an identification card or simply by convincing employees of his position in the company. Such an attacker can gain physical access to restricted areas, thus providing further opportunities for attacks.

## Example 4

It happens in most of the cases that an attacker might be around you and can do **shoulder surfing** while you are typing sensitive information like user ID and password, account PIN, etc.

## Phishing Attack

A phishing attack is a computer-based social engineering, where an attacker crafts an email that appears legitimate. Such emails have the same look and feel as those received from the original site, but they might contain links to fake websites. If you are not smart enough, then you will type your user ID and password and will try to login which will result in failure and by that time, the attacker will have your ID and password to attack your original account.

## Quick Fix

* You should enforce a good security policy in your organization and conduct required trainings to make all the employees aware of the possible Social Engineering attacks and their consequences.
* Document shredding should be a mandatory activity in your company.
* Make double sure that any links that you receive in your email is coming from authentic sources and that they point to correct websites. Otherwise you might end up as a victim of Phishing.
* Be professional and never share your ID and password with anybody else in any case.