الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

المخيم الشبابي للأمن السيبراني 2026
CYBER SECURITY YOUTH CAMP 2026

academy.ncsa.gov.qa


welcome
to a safer
cyber world...

How to use this handbook

This handbook has been designed for the National Cyber Security Agency of Qatar for inspiring children to pursue a career in the field of cyber security.

The content of this handbook is based on educational material from **TryHackMe.com** and in cludes interactive activities designed to help students understand cybersecurity concepts in an engaging and accessible way.

It is also a complimentary guidebook to the physical camps that are held in Doha, Qatar, and not designed to be consumed for self-study.

Unlock
The journey

Introduction to Cyber Security

Imagine a world where you are the guardian of secret treasure, defending it from sneaky thieves. That's what cyber security is all about! It's the exciting practice of protecting computers, networks, and data from hackers and digital villains.
You'll learn cool techniques to spot threats, how to keep your information safe, and even how to outsmart cyber criminals.

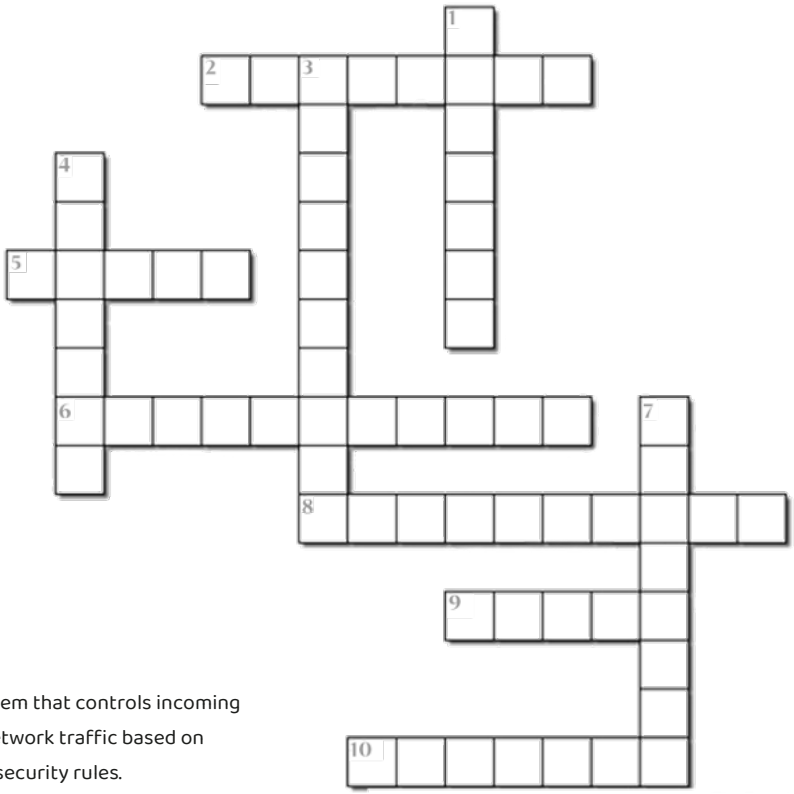
Get ready to dive into a thrilling world
where you'll become the hero of the internet.

Fact alert!

October is National Cybersecurity Awareness Month, dedicated to raising awareness about the importance of cybersecurity.

Take
the cyber quest

Complete the crossword puzzle below



Across

2. Security system that controls incoming and outgoing network traffic based on predetermined security rules.

5. Malicious software that replicates itself and spreads to damage or disrupt systems and data.

6. Deliberate exploitation of computer systems, networks, or devices.

8. Process of encoding data to prevent unauthorized access, ensuring privacy and security.

9. Update to fix vulnerabilities or improve functionality in software or systems.

10. Unauthorized access or manipulation of computer systems or networks.

Down

1. Malicious software designed to disrupt, damage, or gain unauthorized access to systems or data.

3. Malware that encrypts files, demanding payment for decryption.

4. Protection of personal data from unauthorized access or disclosure.

7. Deceptive attempts to acquire sensitive information, often through disguised communication.

Protecting
Our Digital Castle

We need your support to protect our castle!

Write a list of everything you can see in this picture

Now let's imagine this picture as the cyber world you live in...

Our digital world with the devices and storages

The medieval castle with towers and walls is the fortress for our digital world

The Red Team knights are the "Friendly Foes" who are the ethical hackers launching simulated attacks.

The shadowy figures lurking outside the castle walls are "Cyber Criminals"

The Blue Team knights are the "Guardians of the Wall" who are cybersecurity professionals defending the castle

Fact alert!

Did you know that not all hackers are bad? There are ethical hackers, also known as "white hat" hackers, who help organizations find and fix security vulnerabilities.

Navigating
cyber security careers

Cyber Career Fit

Which of the following jobs would you like to do someday?

Shade the stars on the jobs, if it interests you.

Security Analyst

A Security Analyst monitors networks and systems for security breaches, analyzes incidents, investigates alerts, and implements measures to protect the organization's data and infrastructure.

Security Engineer

They design and build strong walls and gates for our digital world, keeping out bad guys who try to sneak in. They use special tools and smart plans to keep everything secure.

Incident Responder

When a cyberattack strikes, these digital firefighters jump into action! They quickly figure out what happened, stop the bad stuff from spreading, and help fix everything fast. It's like playing a fast-paced game where they need to move quickly to keep things safe.

Digital Forensics Investigator

Love solving puzzles and uncovering secrets? Digital forensics is all about using cool gadgets to hunt down clues and catch cyber bad guys. It's like being a digital detective on a mission to keep the online world safe!

Penetration Tester (Ethical Hacker)

A computer expert who uses their hacking skills for good. They're like digital detectives, uncovering weaknesses in systems to keep everyone's information safe from bad guys.

Chief Information Security Officer (CISO)

They plan how to protect an organization's computers, networks, and data, and lead the team that keeps everything secure. It's like being the coach of a sports team, planning the winning strategy and leading the team to success.

Malware Analyst

Meet the code detectives of cybersecurity: malware analysts! They study sneaky computer programs, figuring out how they work and what they're up to. It's like unraveling a mystery puzzle to catch digital troublemakers and keep our computers safe.

Linux Fundamentals

- Hey there! Linux is like a super cool playground for computers. It's a special operating system that gives your computer the power to run all sorts of amazing programs and games. Just like a magical toolbox, Linux lets you customize and tweak your computer in awesome ways.

  It's like having a secret code to unlock endless possibilities for your computer.

  So, if you love exploring and discovering new things, Linux is your very own digital adventure land!

Linux is a super cool operating system, just like Windows or macOS, but it's free and open-source! This means you can download it, use it, and even change it if you know how. Many servers, supercomputers, and even your Android phone run on Linux.

It's popular because it's super secure and customizable. If you love tinkering with technology and want to learn how computers really work, Linux is like a playground where you can explore and create!

Fun task

Pick two cool words about Linux that really grabbed your attention and write them down!

Meet the
Linux Heroes

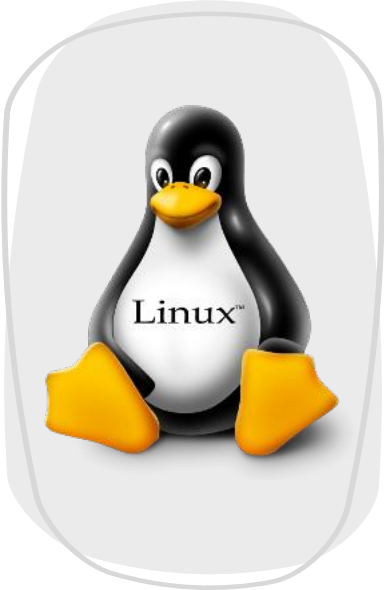
Ubuntu is a user-friendly Linux operating system that's great for beginners. It's known for its easy installation process and large community support. You can use it for everything from browsing the web to programming and running servers.

Fedora is a cutting-edge Linux operating system that offers the latest features and technologies. It's great for developers and tech enthusiasts who want to try out the newest software. Fedora is also known for its strong security features.

Debian is a stable and reliable Linux operating system that's the base for many other distributions, including Ubuntu. It's known for its robustness and is often used for servers. It's a bit more technical but highly customizable.

CentOS is a free, enterprise-class Linux operating system that's often used for servers. It's known for its stability and long-term support, making it a popular choice for businesses and web hosting. It's based on Red Hat Enterprise Linux.

Linux commands



Linux commands are simple instructions you give to your computer to make it do things. Just like using shortcuts on a keyboard, these commands let you find files, move around in folders, and run programs.

It's a bit like speaking a secret code that makes your computer listen and respond. Learning these commands will help you become a pro at navigating and using Linux.

Let's start and see how powerful these little words can be!

Fact alert!

Many Linux commands have origins dating back to the Unix operating system, which was developed in the 1970s. They have evolved over time but still retain their core functionalities.

Echoes & Identities

Discover the basics of Linux commands with echo for sending messages and whoami to find your computer identity. These are your first steps into the world of essential commands!

Echo

This command simply repeats whatever you type after it. It's like shouting into a canyon and hearing your echo come back!

whoami

This command helps you find out who you are in the system, like looking in a mirror.

```
tryhackme@linux1:~$ echo "Hello World!"
"Hello World!"
```

```
tryhackme@linux1:~$ whoami
tryhackme
```

Fun task

If we wanted to output the text "LinuxIsFun" what would our command be?

What's in a filesystem?

Now, let's dive into how you can explore and manage your computer's folders and files using simple commands. Get ready to manage your digital space like a pro!

ls (listing)

This command lists all the files and folders in your current directory. It's like opening a treasure chest and seeing what's inside!

```
tryhackme@linux1:~$ ls
access.log  folder1  folder2  folder3  folder4
```

cd (change directory)

This command lets you move between different folders. It's like teleporting to different locations in a video game!

```
tryhackme@linux1:~$ cd folder4
tryhackme@linux1:~/folder4$ ls
note.txt
```

What's in a filesystem?

cat (concatenate, outputting the contents of a file)

This command displays the contents of a file.
It's like opening a book and reading what's written inside.

```
tryhackme@linux1:~/folder4$ ls
note.txt
tryhackme@linux1:~/folder4$ cat note.txt
Hello World!
```

pwd (print working directory)

This command tells you the full path of your current location in the file system. It's like using a GPS to find your way around!

```
tryhackme@linux1:~/folder4$ pwd
/home/tryhackme/folder4
tryhackme@linux1:~/folder4$
```

Hidden Easter Eggs

Some Linux commands have hidden Easter eggs or quirky responses when you enter certain inputs. Try the command "apt-get moo" and you'll be surprised!

Searching for files

Explore how to hunt down and discover specific items in your computer's digital treasure trove.

Find

This command lets you search for files by name, type, or other criteria. It's like having a search dog sniff out the exact file you need!

```
tryhackme@linux1:~$ find -name note.txt
./folder4/note.txt
tryhackme@linux1:~$
```

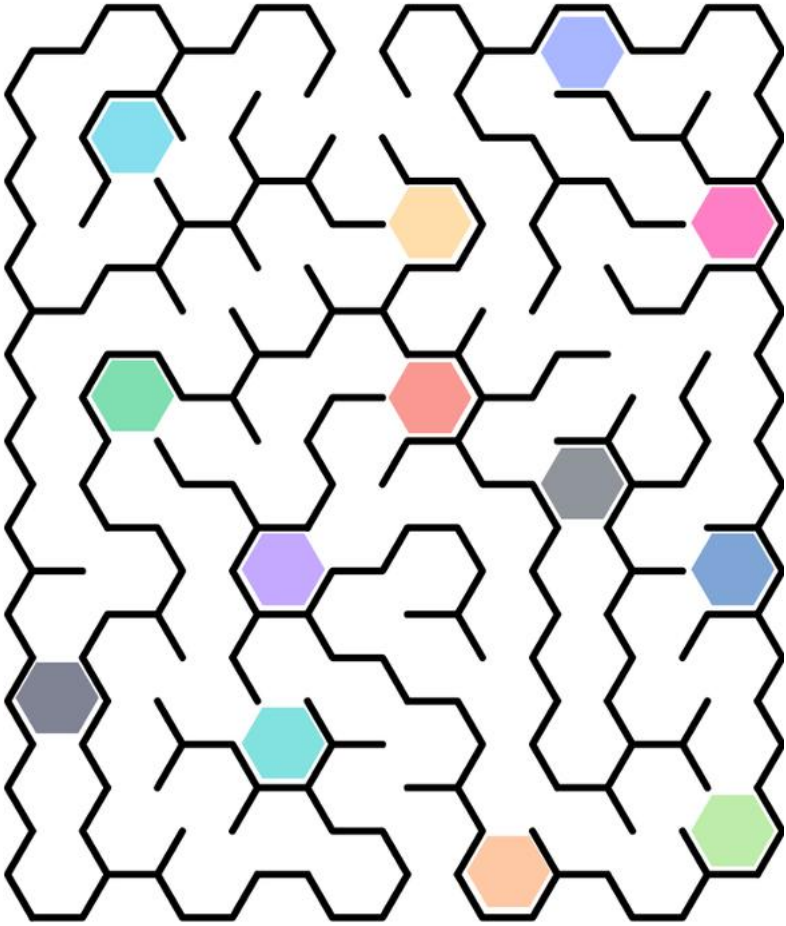
Grep

This command lets you search for specific text patterns within files. It's like using a metal detector to find hidden treasures in the sand!

```
tryhackme@linux1:~$ grep "81.143.211.90" access.log
81.143.211.90 - - [25/Mar/2021:11:17 + 0000] "GET / HTTP/1.1" 200 417
"-" "Mozilla/5.0 (Linux; Android 7.0; Moto G(4))"
tryhackme@linux1:~$
```

Discovery Maze

You are in a mysterious digital world where files and folders are hidden! Navigate through the maze to find all the hidden files and folders in your path.



Fun task

Hint

Colored Hexagons along the correct path are only the hidden files and folders. Well , others are just hexagons!

How many did you find?

Secret
Agent Commands

Learn to deploy specialized tools for executing commands discreetly and managing data effectively in your digital operations! Dive into the world of shell operators where each symbol serves a unique purpose, enhancing your control over computer tasks.

& (background)

This operator lets you run commands in the background, so you can continue using the terminal for other tasks. It's like having a multitasking superpower!

```
tryhackme@linux1:~$ sleep 20 &
[1] 3124
tryhackme@linux1:~$
[1]+ Done sleep 20
```

Operator "&&" (and)

This operator lets you chain multiple commands together, but only if the first command succeeds. It's like setting up a domino effect – one command triggers the next!

```
tryhackme@linux1:~$ echo "Peter" && "James"
"Peter"
"James"
```

Secret
Agent Commands

Operator “>” (output redirection)

This operator lets you redirect the output of a command to a file. It's like channelling a river into a new stream!

```
tryhackme@linux1:~$ echo hey > welcome
tryhackme@linux1:~$ cat welcome
hey
```

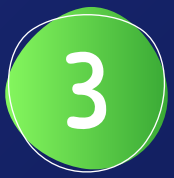
Operator “>>” (append)

This operator is similar to >, but it appends the output to the end of a file instead of overwriting it. It's like adding a new chapter to a book!

```
tryhackme@linux1:~$ echo hello >> welcome
tryhackme@linux1:~$ cat welcome
hey
hello
```

Hidden Easter Eggs

You can use the ‘history’ command to view a list of previously executed commands, making it easy to repeat or recall actions.



Web Security

Welcome to the exciting world of the web! The internet is like a massive library where you can find almost anything, from games and videos to information about your favorite topics. Websites are like the books in this library, and web browsers like Chrome or Firefox are the tools you use to read them. Understanding how these work helps you navigate the digital world more safely and efficiently!

While the web is full of fun and useful things, there are also dangers lurking around. Just like in a video game, there are "bad guys" trying to trick you, steal your information, or mess with your devices. These threats can come in the form of viruses, phishing scams, or hackers. Knowing about these threats is the first step in staying safe online!

To protect yourself online, you need some cool defensive moves! Think of it like having a shield and armor in a game. Using strong passwords, updating your software, and being careful about the links you click are just a few ways to keep your digital world secure. Learning these skills will make you a cybersecurity hero!

Surfing safely like a cyber security hero

The Web
Building Blocks

Let us brush up on
the fundamentals of the web...

The Internet

A treasure map filled with all kinds of amazing places to explore. It's where you can find colorful websites, fun games, and fascinating videos all ready to be discovered. You can find information about animals, outer space, and even your favorite superheroes.

World Wide Web

A magical network, connecting people worldwide like a spider web weaving through computers and gadgets. Messages and videos zip across the globe, offering endless entertainment. Discover a universe of knowledge in this vast network of exciting possibilities!

How Websites
Appear on screens?

Ever wondered how your favorite games and videos pop up so quickly? It's all thanks to the client-server model, where your web browser talks to powerful computers around the world (servers) to fetch and display web pages.

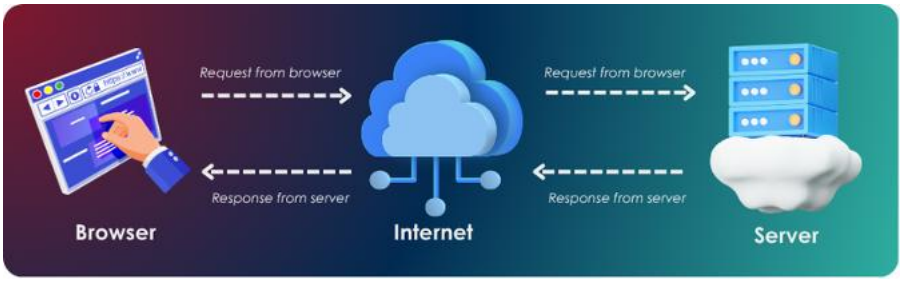
Imagine your browser as a superhero, zooming across the internet to bring you awesome stuff with just a click! And those web addresses (URLs)? They're like magic keys that guide your browser to find exactly what you're looking for in this amazing digital universe. Ready to explore how the internet makes all this happen right on your screen?

URL

A URL (Uniform Resource Locator) is like an address for websites. It tells your web browser where to find a specific page or file on the internet. **For example**, "www.example.com" is a URL that directs you to a website named "example".

Fact alert!

The first website, created by Tim Berners-Lee in 1991, is still online! It's a basic page explaining the World Wide Web project.



Front-End vs. Back-End

Aspect	Front-end (Client side)	Back-end (Server side)
Purpose	Deals with what users see and interact	Manages server-side operations and database tasks
Languages	HTML (Hyper Text Markup Language), CSS (Cascading Style Sheets), JavaScript	Python, PHP, Ruby, Java
Responsibilities	Designing user interfaces, layouts, and navigation	Handling server requests, data storage, and retrieval
Execution	Executes on the user's browser	Executes on the server
Focus	User experience (UX)	Server performance and data management
Tools	Web browsers, text editors, design tools	Servers, databases, integrated development environments (IDEs)
Skills	Design, UI/UX principles	Programming, database management, security
Examples	Buttons, menus, forms, animations	Server scripts, database queries, APIs

Your Website's
Secret Decoder Ring

Domain Name

A domain name, like "google.com" or "amazon.com", is an easy-to-remember name that uniquely identifies a website on the internet. It's similar to using a friend's address to find their house instead of remembering numbers. Each domain name is registered through special organizations to ensure it's unique. This way, you can easily visit your favorite sites without needing to remember complicated numbers.

IP Address

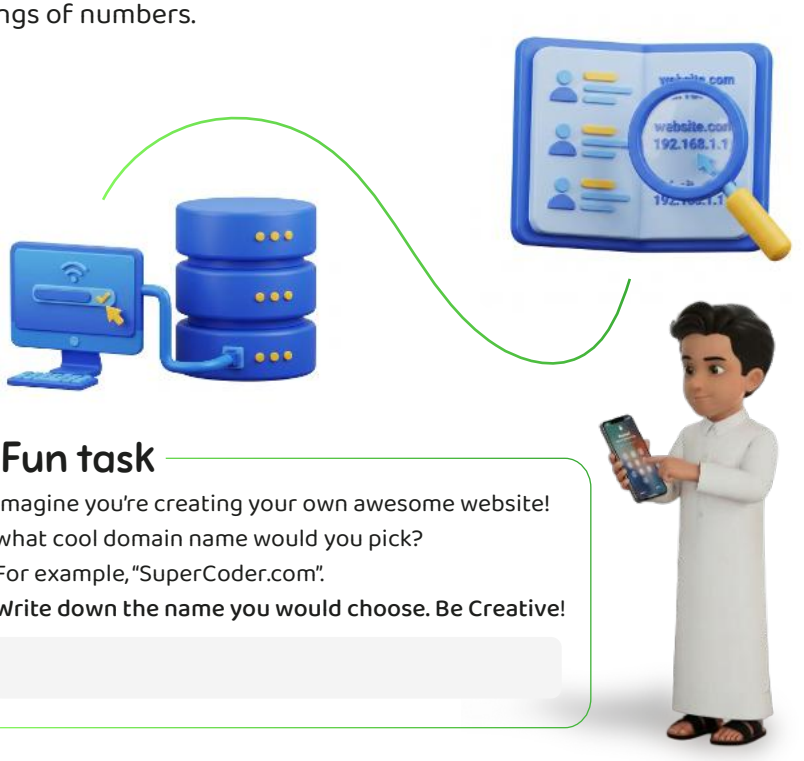
An IP address (Internet Protocol address) is a unique set of numbers assigned to every device connected to the internet. It's like a phone number for your computer, tablet, or smartphone, helping it communicate with other devices. When you visit a website, your device uses its IP address to find and connect to the website's server, which also has its own IP address. These addresses ensure that data reaches the correct destination, just like mailing a letter to a specific address.

Your Website's
Secret Decoder Ring

DNS

The Domain Name System (DNS) is like the internet's phone book. It translates human-friendly domain names, like www.example.com, into computer-friendly IP addresses, **like 192.0.2.1**, so your device can find and connect to the right server.

When you type a website address into your browser, DNS servers quickly look up the IP address associated with that domain name and direct your browser to it. **This process happens behind the scenes** in milliseconds, making it easy for us to browse the web without remembering complex strings of numbers.



Fun task

Imagine you're creating your own awesome website!
what cool domain name would you pick?
For example, "SuperCoder.com".
Write down the name you would choose. Be Creative!

Domain Hierarchy

TLD (Top-Level Domain)

A TLD is the last part of a domain name, like .com in tryhackme.com. There are two types of TLDs:

1) gTLDs (Generic Top-Level Domain) tell you the purpose of the website. For example,

- .com for commercial sites
- .org for organizations
- .edu for education
- .gov for government

2) ccTLDs indicate the country of the site. For example,

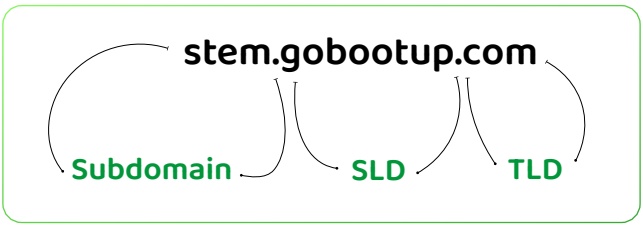
- .qa for Qatar
- .ae for United Arab Emirates

Nowadays, many new gTLDs exist, like .online, .club, .website, and .biz.

SLD (Sub-Level Domain)

In tryhackme.com, "tryhackme" is the Second-Level Domain (SLD) and ".com" is the TLD. The SLD is what you choose to name your website, and it can have up to 63 characters.

It can include letters (a-z), numbers (09-), and hyphens, but it can't start or end with hyphens, nor have consecutive hyphens. This unique name, combined with the TLD, helps identify your website on the internet.



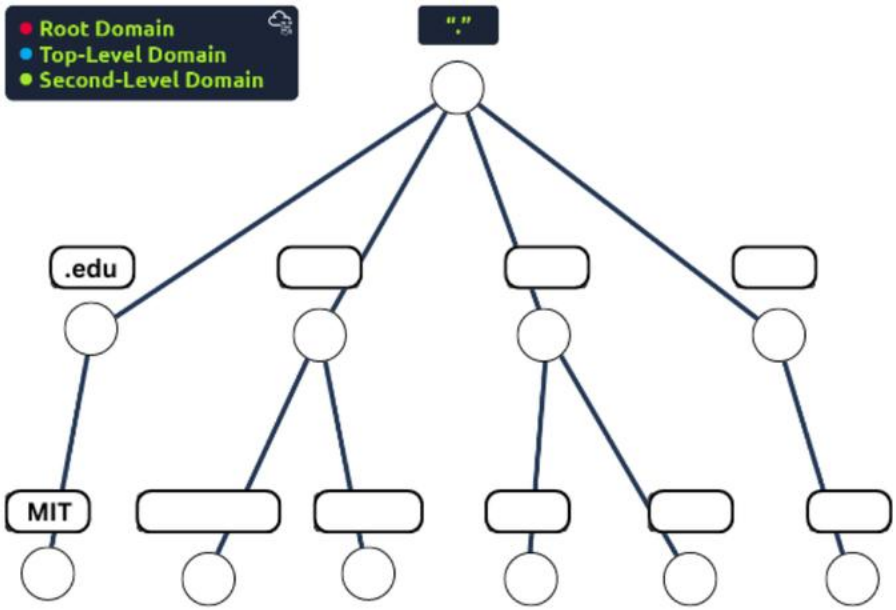
Subdomains

A subdomain appears before the Second-Level Domain (SLD) and is separated by a period. For example, in admin.tryhackme.com, "admin" is the subdomain. Subdomains have the same rules as SLDs: they can be up to 63 characters long and can include letters (a-z), numbers (09-), and hyphens (but not start or end with hyphens or have consecutive hyphens).

You can have multiple subdomains, like jupiter.servers.tryhackme.com, as long as the total length is 253 characters or less. There's no limit to the number of subdomains you can create.

Can you work it out?

Using the domain hierarchy diagram and the legend provided below, search for examples and write down TLDs (Top-Level Domains) and the relevant SLDs (Second-Level Domains) for each one. One example has been done for you. Color each domain level according to the legend.



What happens when you make a DNS request?

1. Local Cache Check

When you type a website address (like www.example.com) into your browser, your computer first checks its local memory (cache) to see if it already knows the corresponding IP address.

2. Recursive DNS Server Request

If the address isn't found locally, your computer sends a request to a Recursive DNS Server. This server is usually provided by your internet service provider (ISP) or can be one you choose.

3. Server Lookup

The Recursive DNS Server also has its own cache. If it finds the address there, it sends it back to your computer.

4. Root DNS Servers

If the address isn't in the local cache or the Recursive DNS Server's cache, the Recursive DNS Server starts a journey. It begins by asking the Root DNS Servers, which are like the backbone of the internet.

5. Top-Level Domain (TLD) Servers

The Root DNS Servers direct the request to the appropriate Top-Level Domain (TLD) server. For example, if you're looking for a .com domain, it sends you to the .com TLD server.

What happens when you make a DNS request?

6. Authoritative DNS Server

The TLD server knows which Authoritative DNS Server (also called nameservers) is responsible for the specific domain (like example.com). The authoritative server holds the most current DNS records for that domain.

7. DNS Record Retrieval

The Recursive DNS Server queries the authoritative server for the DNS records related to the domain you requested.

8. Response Back to Client

The authoritative server sends back the DNS records (like IP addresses) to the Recursive DNS Server.

9. Local Cache Update

The Recursive DNS Server saves these records in its local cache for future use, according to their Time To Live (TTL) value. TTL is how long the record should be stored before checking again.

10. Final Response to Client

Finally, the Recursive DNS Server sends the DNS records back to your computer. Your browser can now use these records to connect to the website's server and load the webpage.

HTTP Vs. HTTPS

What is HTTP?

HTTP (Hyper Text Transfer Protocol) is like a set of rules that helps your computer talk to websites. It was created by Tim Berners-Lee and his team in the late 1980s and early 1990s. It's how your computer asks for and gets all the stuff on webpages, like pictures, videos, and words.

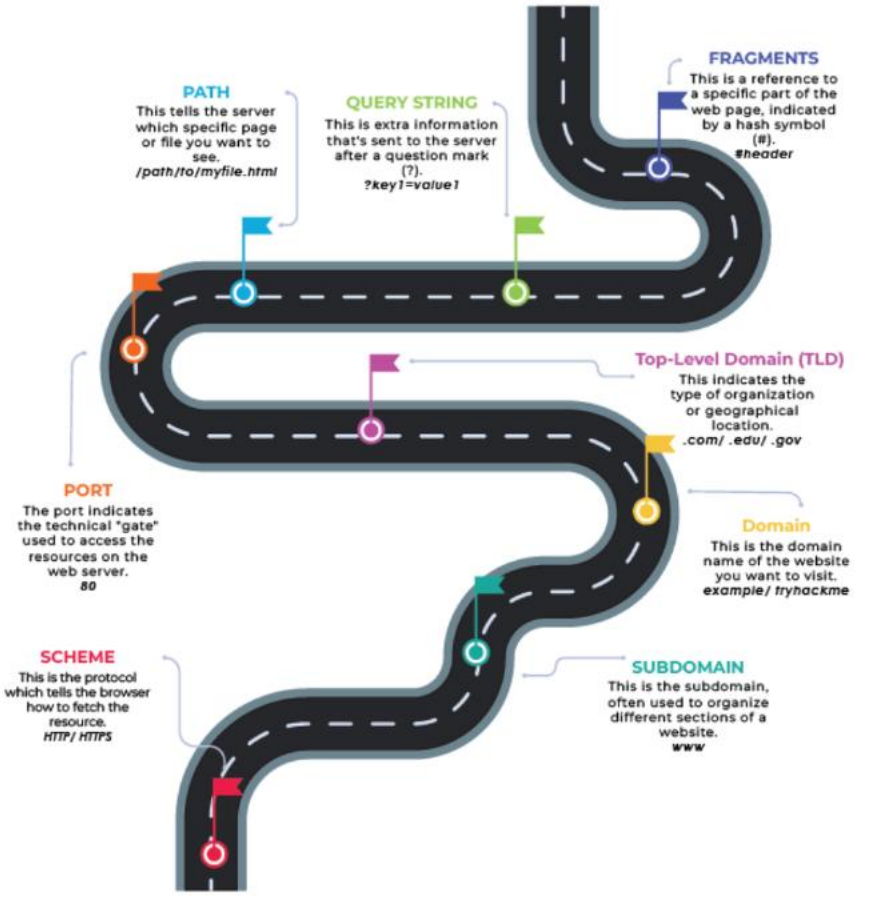
What is HTTPS?

HTTPS (Hyper Text Transfer Protocol Secure) is a safer version of HTTP. It keeps your data private by encrypting it, which means it's like putting your information into a secret code that only the right website can unlock. This helps make sure you're talking to the real website and not someone pretending to be it.

Navigating through a URL

Think of a URL like a magical address for the internet! Just like your home address tells the mailman where to deliver letters, a URL tells your web browser where to find websites. It's a special code made of words and symbols that guides your browser through the vast internet maze.

https://www.example.com:80/path/to/myfile.html?key1=value1#header



HTTP Methods

HTTP methods tell the web server what action you want to take when you make a request.

GET

This is used for getting information from a web server.

POST

This is used for submitting data to the web server and potentially creating new records

PUT

This is used for submitting data to a web server to update information

Delete

This is used for deleting information/records from a web server.

Fact alert!

HTTPS helps prevent man-in-the-middle attacks by encrypting data between the client (your browser) and the server, ensuring secure communication.

HTTP Status Codes

HTTP status codes are messages from the server that tell you how your request was handled. They can indicate success (like "200 OK"), errors (like "404 Not Found"), or other important information about what happened when you tried to access a web page.

100–199 **Information Response**	These are sent to tell the client the first part of their request has been accepted and they should continue sending the rest of their request. These codes are no longer very common.
200–299 **Success**	This range of status codes is used to tell the client their request was successful.
300–399 **Redirection**	These are used to redirect the client's request to another resource. This can be either to a different webpage or a different website altogether.
400–499 **Client Errors**	These are client-side error status codes. They indicate that there was a problem with the request sent by the client, such as invalid syntax, missing authentication, or requesting a resource that does not exist.
500–599 **Server Errors**	This is reserved for errors happening on the server-side and usually indicate quite a major problem with the server handling the request.

Common HTTP Status Codes

200 OK	The request was completed successfully.
201 Created	A resource has been created (for example a new user or new blog post).
301 Moved Permanently	This redirects the client's browser to a new webpage or tells search engines that the page has moved somewhere else and to look there instead.
302 Found	Similar to the above permanent redirect, but as the name suggests, this is only a temporary change and it may change again in the near future.
400 Bad Request	This tells the browser that something was either wrong or missing in their request. This could sometimes be used if the web server resource that is being requested expected a certain parameter that the client didn't send.
401 Not Authorised	Authentication is required to access this resource. You must log in or provide valid credentials, such as a username and password, before the server will allow access.

Common HTTP Status Codes

There are many different HTTP status codes, and even applications can define their own.
Let's look at the most common ones you're likely to encounter:

403 **Forbidden**	You do not have permission to view this resource whether you are logged in or not.
404 **Page Not Found**	The page/resource you requested does not exist.
405 **Method Not Allowed**	The resource does not allow this method request, for example, you send a GET request to the resource /create-account when it was expecting a POST request instead.
500 **Internal server Error**	The server has encountered some kind of error with your request that it doesn't know how to handle properly.
503 **Service Unavailable**	This server cannot handle your request as it's either overloaded or down for maintenance.

Unscramble the letters to find meaningful terms below

NPGI 

ATCH 

GERAN 

TENLIC 

DAIMON 

ORPT 

NIRGTS 

DOFERA 

TODHEM 

ERQYU 

RMNIFOU 

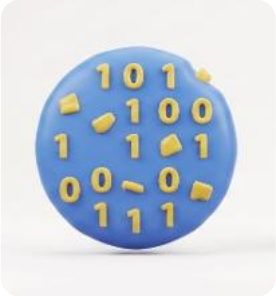
IKSD 

What HTTP Status Code did you find?

Behind the Scenes of Your Web Adventures

Headers

Headers are additional bits of data you can send to the web server when making requests. Although no headers are strictly required when making a HTTP request, you will find it difficult to view a website properly.



Cookies

Cookies are small files stored on your computer by websites. They remember your preferences and login information, making your web experience smoother and more personalized.

Cookies

Fact alert!

First Cookies: The first web cookies were used by Netscape in 1994 to store user information on e-commerce sites, allowing for the creation of virtual shopping carts.

Web Technologies & Frameworks

When you visit a website, your browser (like Safari or Google Chrome) makes a request to a web server asking for information about the page you're visiting.

It will respond with data that your browser uses to show you the page; a web server is just a dedicated computer somewhere else in the world that handles your requests.

Websites are primarily created using

HTML

to build websites and define their structure (images, texts, links)

CSS

to make websites look pretty by adding styling options

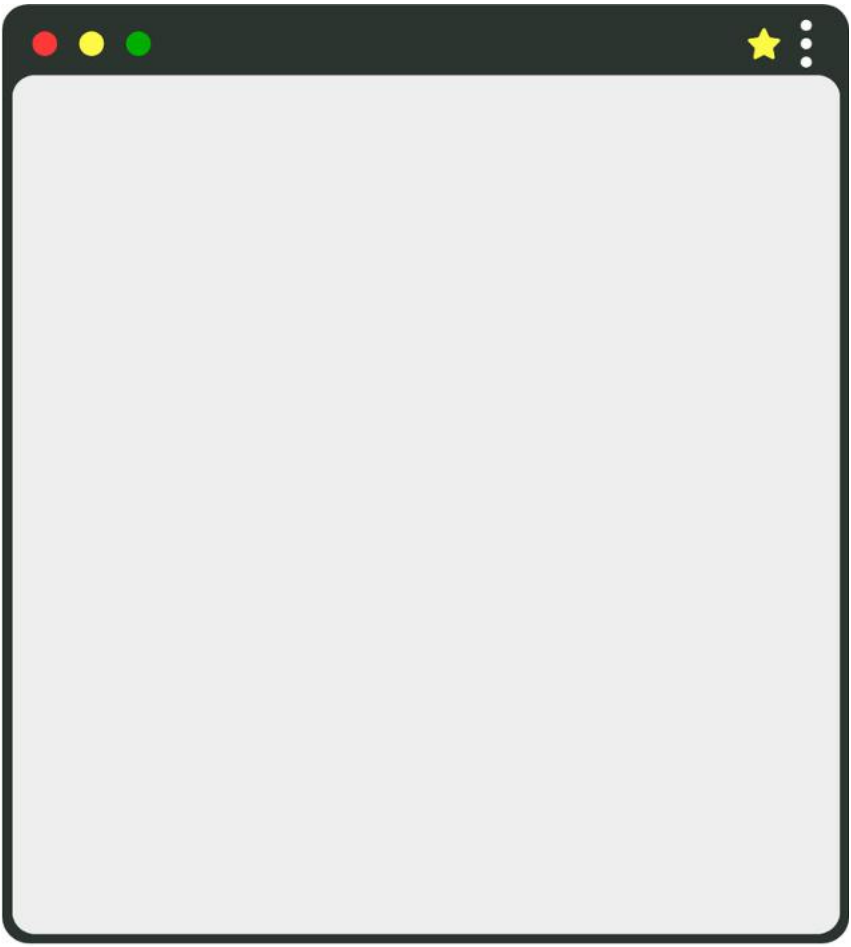
JS

implement complex features on pages using interactivity

Design
Your Dream Website!

Draw a sketch of your dream website

Be creative with the layout, colors, and content. Include elements like navigation bars, images, text, and any interactive features you imagine. Think about what would make your website unique and enjoyable to use. Have fun and let your creativity flow!



HTML
(HyperText Markup Language)

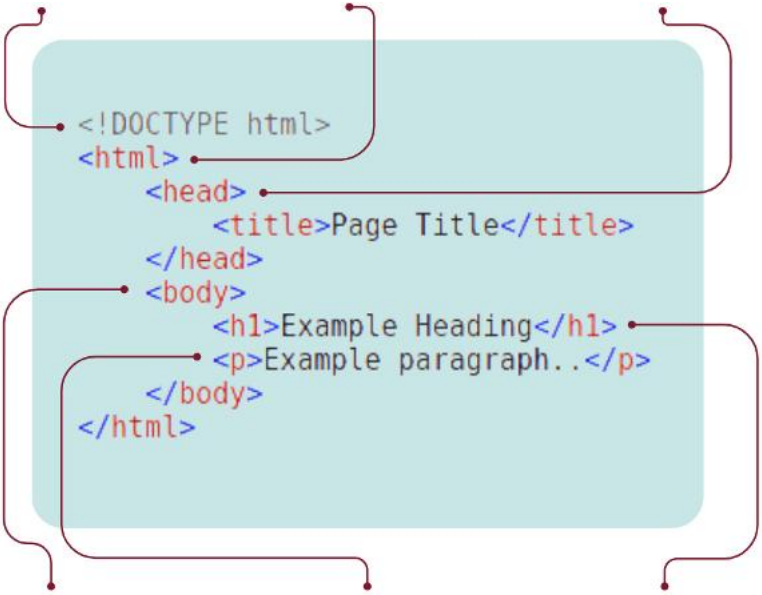
HyperText Markup Language (HTML) is the language websites are written in. Elements (also known as tags) are the building blocks of HTML pages and tells the browser how to display content.

The code snippet below shows a simple HTML document, the structure of which is the same for every website:

Defines that the page is a HTML5 document

It is the root element of the HTML page

Contains information about the page



Defines the HTML document's body

Defines a paragraph

Defines a large heading

HTML Tags

HTML tags are the building blocks of a web page.
They tell the browser how to display content.

For example:

<h1> This tag creates a main heading (the biggest heading on the page).

<p> This tag creates a paragraph of text.

<img> This tag inserts an image.

<a> This tag creates a link to another webpage.

HTML Attributes

Tags can have attributes, which are like extra information that provides more context about the element.

class

```
<div class="container">Content</div>
```

This attribute is used to group multiple elements together and apply the same styles to them. class' specifies a class name for CSS styling.

src & alt

```
<img src="image.jpg" alt="A description">
```

src - This attribute is used for images to specify the source file.
alt - This attribute provides alternative text for images in case they don't load or for screen readers used by visually impaired people.
'src' specifies the image source, 'alt' provides alternative text.

id

```
<p id="intro">Hello, welcome to my website!</p>
```

id - This attribute is used to identify a specific element uniquely.
'id' attribute assigns a unique identifier "intro" to the <p> element, which can be used to style or manipulate this specific paragraph using CSS or JavaScript.

CSS Cascading Style Sheets

Inline CSS

```
<p style="color: blue;">This text is blue.</p>
```

Styles are applied directly within the HTML tag using the style attribute.

Internal CSS

Styles are written inside the <style> tag within the HTML document's <head> section.

```
<head>
  <style>
    p { color: blue; }
  </style>
</head>
```

External CSS

Styles are written in a separate CSS file, which is linked to the HTML document using the <link> tag.

```
<head>
  <link rel="stylesheet" href="styles.css">
</head>
```

JavaScript

A programming language to make websites interactive, by creating dynamic content like animations, form validations, and interactive maps.

Key JavaScript Concepts

Variables

These are containers for storing data, like numbers, text, or even entire objects.

Functions

These are reusable blocks of code that perform specific tasks, like calculating a discount or animating a button.

Events

These are actions that happen on the webpage, like a button click or a mouse hover. JavaScript can listen for these events and react accordingly.

3 ways
to add JavaScript

Inline JavaScript

is written directly within the HTML element using the onclick, onload, or other event attributes. Although suitable for simple examples, it is generally discouraged because it makes code harder to maintain and can increase security risks, such as Cross-Site Scripting (XSS).

```
<button onclick="alert('Hello!')">Click Me</button>
```

Internal JavaScript

is placed within a '<script>' tag inside the HTML document's '<head>' or '<body>' section. It's useful for scripts specific to that single HTML page.

```
<!DOCTYPE html>
<html>
<head>
  <script>
    function sayHello() {
      alert('Hello from Internal JavaScript!');
    }
  </script>
</head>
<body>
  <button onclick="sayHello()">Click Me</button>
</body>
</html>
```

```
<!DOCTYPE html>
<html>
<head>
  <script src="script.js"></script>
</head>
<body>
  <button onclick="sayHello()">Click Me</button>
</body>
</html>
```

External JavaScript

is stored in separate '.js' files and linked to the HTML document using a '<script>' tag with the 'src' attribute. It's best for larger scripts and code reuse across multiple pages.

Javascript

```
function sayHello() {
  alert('Hello from External JavaScript!');
}
```

Web Browsers

A web browser is a software application used to access and view websites on the internet. It retrieves information from the web and displays it on your device. Common web browsers include Google Chrome, Mozilla Firefox, Microsoft Edge, and Safari. Browsers allow you to navigate between web pages, bookmark your favorite sites, and use various web applications.

They are essential tools for browsing the internet, ensuring you can find and enjoy content online easily.

Security Features of Your Browser

(Sandboxing)

Each website has its own "sandbox," stopping harmful code from affecting your computer or stealing your information.

(Pop-up Blockers)

These stop annoying and potentially harmful pop-up windows from appearing, like a security guard keeping out unwanted guests.

Warning Messages

Your browser warns you if a website is dangerous or trying to install suspicious software. A friendly neighbourhood watch keeping you safe.

Fun task

Which of these cool browser logos do you recognize?
Circle the ones you've seen or used before!

Servers

Client-Server

The client-server model is like a conversation between two friends. The client, like you using a web browser, asks for something (like a webpage) from the server, which is like a helpful friend that provides what you asked for. It's a way computers communicate over a network, where clients make requests and servers respond by .sending data back

What does a Client Server do?

Browser Requests

When you type a website address into your browser, it sends a request to the server asking for the webpage's files.

Server Responds

The server receives the request, finds the requested files (like HTML, images), and sends them back to your browser.

Browser Renders

Once your browser gets the files, it puts everything together and displays the webpage on your screen, including text, images, and buttons you can interact with.

Web Servers

A web server is a powerful computer that stores and delivers website content to your browser. When you type a website address into your browser, the web server sends the site's pages, images, and other files to your device, allowing you to see and interact with the website. Think of it as a library that gives you the book you want !to read

What does a Web Server do?

Stores Website Files

store all
the parts of a website in a safe place.

Handles Requests

When someone wants to view a website, they request the web server for the website's files.

Delivers Content

responds by sending back the requested files to the user's browser, which then displays the website.

Manages Data

For websites that change or have dynamic content (like news updates or shopping items), web servers interact with databases to store, retrieve, and update information as needed.

Databases

Databases are like organized digital filing cabinets where computers store and manage information.

They're designed to store large amounts of data in a structured way, making it easy to find, update, and retrieve information when needed. Databases are used by websites, apps, and many other computer systems to store everything from user accounts and product inventories to scientific data and financial records.

Relational Databases

Relational databases store data in tables with rows and columns, using SQL (Structured Query Language) to manage it.
They're good for structured data like financial records and business applications.

NoSQL Databases

NoSQL databases store data in flexible formats like documents or key-value pairs. They're great for handling large amounts of unstructured data, like in web apps and big data analytics.

Databases are the secret ingredient that makes websites dynamic.

They allow websites to,

Personalize content - Show you recommendations based on your past purchases or browsing history.

Handle user interactions - Store your comments, likes, shares, and other interactions with the website. It's like having a conversation with the website.

Manage transactions - Process your orders, payments securely and other sensitive information securely. It's like having a trusted bank vault that keeps your money safe.

The Web Development Toolbox

Web frameworks

Tools that provide developers with pre-written code and libraries to streamline the process of building web applications. They offer a structured way to create and organize web pages, manage databases, handle user interactions, and more.

Some popular web development frameworks:

Bootstrap

A front-end framework that makes it easier to design responsive and mobile-first websites using HTML, CSS, and JavaScript.

React

A JavaScript library for building user interfaces,and created as single-page applications where content updates without refreshing the page.

Angular

A TypeScript-based front-end framework developed by Google. It's used for building dynamic web applications with two-way data binding and dependency injection.

Vue.js

A progressive JavaScript framework used for building interactive web interfaces. It's known for its simplicity and flexibility, making it easy to integrate into other projects.

Django

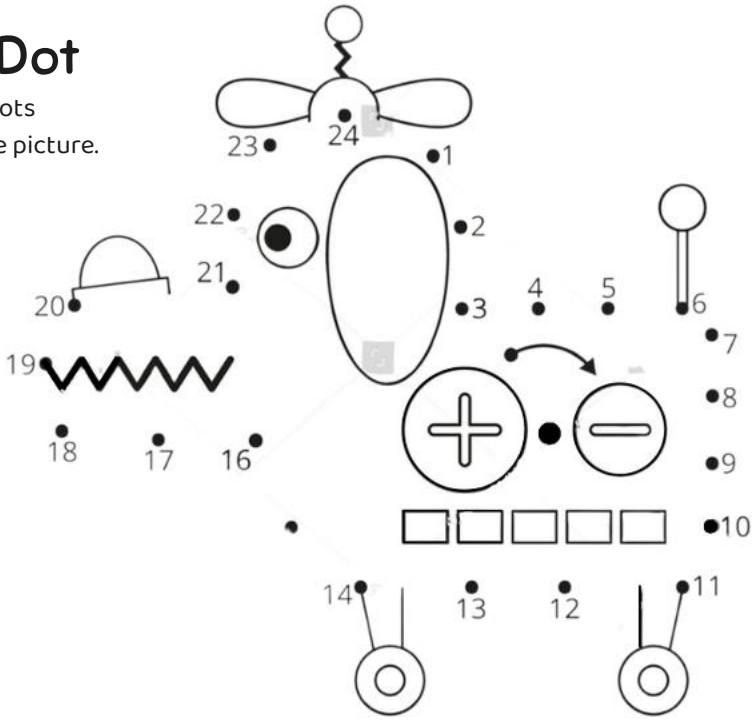
Django is a high-level Python web framework that encourages rapid development and clean, pragmatic design. It follows the MVC (Model-View-Controller) architectural pattern.

Ruby on Rails

Often referred to as Rails and is a web application framework written in Ruby. It emphasizes convention over configuration and aims to simplify the development of web applications.

Dot to Dot

Connect the dots
and Colour the picture.



WAF (Web Application Firewall)

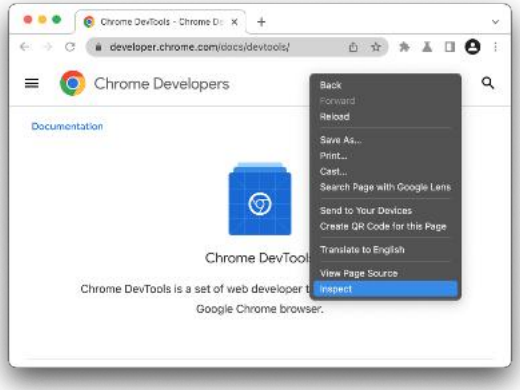
A WAF sits between your web request and the server to protect against hacking and denial of service attacks. It checks web requests for common attack methods, verifies if the request is from a real browser, and limits the number of requests per second from an IP address. If it detects a potential attack, it blocks the request before it reaches the server.

Web Inspection

Developer Tools

Inspector

The "Browser Inspector" is a tool built into web browsers that allows developers and users to view and interact with the underlying code and structure of a web page. It is also known as the "Developer Tools" or "DevTools" in many browsers like Google Chrome, Mozilla Firefox, Microsoft Edge, and Safari.



Here's what it allows you to do:

1. Inspect Elements
2. Make live edits to the HTML and CSS code
3. Debug JavaScript code
4. Monitor network activity
5. Measure page load times and analyze performance
6. Console to execute JavaScript commands interactively

Fun Fact!

The Browser Inspector optimizes websites, ensuring they function correctly and provide a smooth user experience.

Uncovering Hidden Comments and Elements

Web developers sometimes leave hidden comments or elements in the code. These can be notes to themselves, reminders for other developers, or even secret messages! The Browser Inspector can uncover these hidden gems and learn more about the website's security or functionality.

Developer Tools

Debugger

This panel in the developer tools is intended for debugging JavaScript, and again is an excellent feature for web developers wanting to work out why something might not be working. But as penetration testers, it gives us the option of digging deep into the JavaScript code. In Firefox and Safari, this feature is called Debugger, but in Google Chrome, it's called Sources.

Here's what it allows you to do:

1. **Pause code execution** by setting breakpoints in the code allowing you to examine the code.
2. **Inspect variables** to identify errors or understand the code at any point in the code's execution.
3. **Modify JavaScript code** in real-time to see how it affects the website's behaviour.

Network

The network tab on the developer tools can be used to keep track of every external request a webpage makes.

Analysing Network Traffic

Each entry in the Network tab represents a single request or response. You can click on an entry to see more details.

URL: The address of the requested resource.

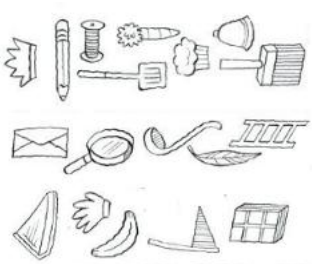
Method: The HTTP method used for the request (e.g., GET, POST).

Status: The HTTP status code of the response (e.g., 200 OK, 404 Not Found).

Type: The type of resource that was requested (e.g., document, script, image).

Size: The size of the requested resource.

Time: The time it took for the request to be completed.



Find the hidden objects

This family is spending time together by camping on their own backyard. Can you find these hidden objects?

Phishing

A phishing attack is a type of cyber attack where malicious actors attempt to trick individuals into revealing sensitive information such as usernames, passwords, credit card numbers, or other personal data.

Phishing attacks often rely on social engineering tactics to exploit human trust and curiosity, making it important for users to be cautious and verify the authenticity of any requests for personal information they receive online

Common Phishing Tactics

How to identify phishing attacks

Check the sender's email address - Phishing emails often use addresses that mimic legitimate ones but may have slight variations or misspellings.
Look for generic greetings - like "Dear User" instead of addressing you by your name.
Beware of urgency or threats - such as claiming your account will be closed if you don't respond quickly.
Verify links before clicking - Hover your mouse over links in emails (without clicking) to see the actual URL which maybe fake websites designed to steal your information.
Check for spelling and grammar errors
Avoid providing personal information - like passwords, Social Security numbers, or account details.
Verify requests for payment or account changes - before taking action.

Common Web Vulnerabilities (OWASP Top 10)

Injection Attacks

An injection attack is a type of cyber attack where malicious code or commands are injected into a vulnerable system or application. These attacks exploit vulnerabilities that allow an attacker to insert unauthorized commands or data into a system, which can then be executed by the system.

Types of Injection Attacks

Command Injection

Attack targets websites that allow users to execute commands on the server. By injecting malicious commands into a website's input fields, attackers can trick the server into executing their commands, potentially giving them control over the server or access to sensitive files.

SQL Injection (SQLi)

Attack targets websites that use SQL databases. By injecting malicious SQL code into a website's input fields, attackers can trick the database into revealing sensitive information or even modifying or deleting data.

Cross-Site Scripting (XSS)

Attack targets websites that allow users to input data that is then displayed to other users. By injecting malicious scripts into a website's input fields, attackers can trick the website into executing their scripts in the browsers of other users, potentially stealing their cookies, session tokens, or other sensitive information.

1 SQL Injection

A SQL injection (SQLi) attack is a type of cyber attack that exploits vulnerabilities in web applications that interact with databases.

Here's how it works:

Vulnerability Identification - Construct SQL queries based on these inputs without proper validation or sanitization.

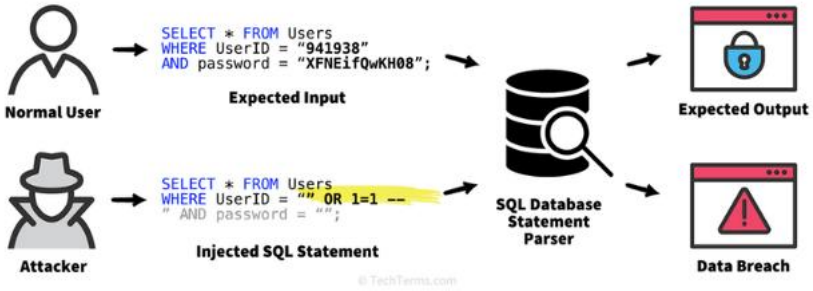
Malicious Input - Insert malicious SQL code and send it to the backend database server for execution.

Execution of Malicious SQL Code - Executed by the database server as part of a legitimate SQL query.

Unauthorized Actions - Depending on the nature of the injected SQL code, attackers can:

- **Retrieve** sensitive data from the database
- **Modify or delete** data stored in the database
- **Execute** administrative commands and gain control over the entire database system.

Example: Suppose a web application uses user input to construct a SQL query to authenticate users during login:



In this case: 'OR 1=1' is always true, bypassing the password check. '--' comments out the rest of the query, ignoring the password condition.

As a result, the attacker can log in as the administrator without knowing the password, exploiting the SQL injection vulnerability in the application.

2 Command Injection

A command injection attack is a type of security vulnerability where an attacker can execute arbitrary commands on the host operating system via a vulnerable application. This typically occurs when the application passes unsafe user inputs to a system shell or command line interpreter.

Here's how it works:

User Input - The application accepts input from a user.

Command Execution - The application includes this input in a system command without proper validation or sanitization.

Arbitrary Commands - The attacker crafts the input to include malicious commands, which the application executes with its own privileges.

How Websites Work:

The Command Center

A web server is like the command centre of a website. It receives requests from your browser (like when you click a link) and responds by sending back the requested information (like a webpage).

Programming Languages

Web servers use special languages (like PHP, Python, or NodeJS) to understand and process these requests.

System Calls

Sometimes, these languages need to talk to the server's operating system to do things like read files or execute commands.

The Hacker's Trick: Injecting Commands

Hackers can exploit this communication by injecting their own commands into the website's input fields.

For example, a search bar might expect you to type in a keyword, but a hacker could type:

Bash

whoami;

This command tells the server to reveal the username it's running under, giving the hacker valuable information.

Spotting the Signs: Blind vs. Verbose Blind:

1. Blind Command Injection - The website doesn't show any output from the injected command. Hackers need to use tricks like time delays or file manipulation to confirm if their attack worked.

2. Verbose Command Injection - The website displays the output of the injected command directly on the page. This is easier to spot but also easier for website owners to fix.

Hacker's Toolkit: Useful Payloads

Linux

whoami - Reveals the server's username.
ls - Lists files and directories.
ping - Creates a time delay (useful for blind injection).
sleep - Another way to create a time delay.
nc - Can be used to create a backdoor into the server.

Windows

whoami - Reveals the server's username.
dir - Lists files and directories.
ping - Creates a time delay (useful for blind injection).
timeout - Another way to create a time delay.

Broken Authentication

Broken Authentication refers to weaknesses in the authentication process that allow attackers to gain unauthorized access to user accounts. This can happen because of weak passwords, poor session management, or flaws in how a website verifies a user's identity.

Common broken authentication attacks include :

Credential stuffing - using stolen usernames and passwords to gain access to other accounts.

Brute force attacks - guessing a user's password by trying many different combinations.

Session hijacking - Stealing a user's session cookie, which allows them to impersonate the user and access their account.

What can it lead to?

Identity theft - Steal your personal information and impersonate you.

Financial fraud - Use credit card information to make unauthorized purchases.

Blackmail - Threaten to expose sensitive information unless you pay them ransom.

Broken Authentication can occur when a website:

- Allows weak or easy-to-guess passwords.
- Does not limit repeated login attempts.
- Uses insecure session management.
- Fails to require strong authentication, such as multi-factor authentication (MFA).
- Has insecure password reset or account recovery processes.

How to spot it?

- Test whether weak passwords are accepted.

Check if the website limits repeated failed login attempts.

- Verify that session IDs change after logging in.
- Look for secure login features, such as HTTPS and multi-factor authentication (MFA).

Word Search

Circle the words related to 'Web Attacks' below

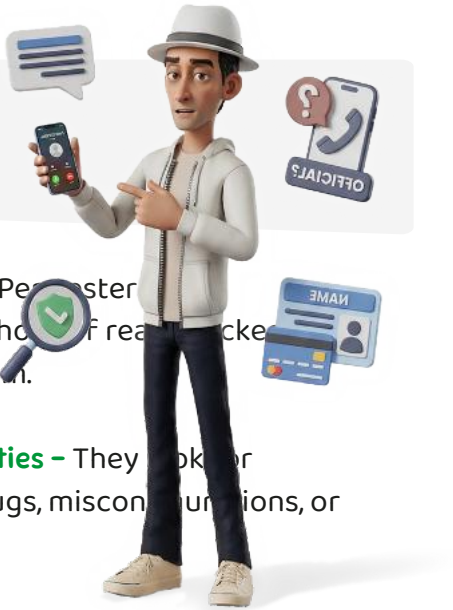
SOCIAL	SCRIPTING	MALICIOUS
URGENCY	REQUESTS	ENGINEERING
SPOOFING	GENERIC	AUTHORIZATION
WEBSITES	INJECTION	AUTHENTICATION
PAYMENT	PHISHING	VULNERABILITIES

T	R	A	U	T	H	E	N	T	I	C	A	T	I	O	N	R	P	E	C
O	G	M	U	N	I	C	A	T	I	O	N	O	X	Y	H	A	E	O	R
Y	E	I	P	I	B	W	T	A	P	M	O	C	R	E	Y	T	I	N	E
A	N	E	T	H	A	E	I	H	S	D	N	E	I	M	F	U	O	V	Q
V	E	R	P	M	I	B	I	O	A	T	N	I	E	A	T	R	E	S	U
U	R	Y	T	S	E	S	C	H	R	D	L	N	E	L	N	G	M	M	E
L	I	E	S	C	S	I	H	P	P	O	T	T	E	I	E	E	R	F	S
N	C	P	I	Y	A	T	M	I	R	E	V	O	L	C	A	N	T	P	T
E	L	R	F	L	S	E	F	S	N	F	E	F	F	I	N	C	O	C	S
R	P	A	R	T	N	S	R	R	E	G	O	T	P	O	T	Y	M	P	S
A	U	T	H	O	R	I	Z	A	T	I	O	N	I	U	R	A	O	I	M
B	E	C	R	E	P	S	E	R	D	N	E	I	R	S	S	O	O	R	P
I	T	E	N	G	I	N	E	E	R	I	N	G	C	N	F	T	A	M	U
T	E	I	T	N	E	M	M	I	T	M	O	C	I	I	M	A	T	N	I
I	E	R	T	I	I	N	J	E	C	T	I	O	N	O	C	M	M	U	N
E	M	S	C	S	S	E	N	O	H	Y	T	G	L	A	P	O	R	T	P
S	S	S	C	A	R	T	S	C	R	I	P	T	I	N	G	I	L	I	A

Penertation Testers

Penetration testers, often called "pen testers" or "ethical hackers," are cybersecurity professionals who simulate cyberattacks on a system, network, or application to identify security vulnerabilities. Their goal is to find and fix weaknesses before malicious hackers can exploit them

What do they do?



1. Simulated Attacks – Pe ester techniques similar to tho f rea cke test security of a syste .

2. Identify Vulnerabilities – They ok r weaknesses such as bugs, miscon ur ions, or outdated software.

3. Report Findings – After testing, they provide a detailed report of findings and recommendations to fix issues.

4. Enhance Security – By identifying and fixing vulnerabilities to strengthen organization's security.

Web Application Best Practices

Securing Web Applications

Secure coding practices:

1. Input Validation – (The bouncer at the door) never trust what users type into your website! Always check their input to make sure it's the right kind of data (like a name or email address) and doesn't contain any sneaky code.

2. Output Encoding – (The secret decoder ring) Output encoding converts special characters into a safe format before displaying them in a web page. This helps prevent attackers from injecting malicious code, such as Cross-Site Scripting (XSS).

3. Parameterized Queries (for SQLi) – (The database shield) for websites that use databases, parameterized queries are like a special shield that protects against SQL injection attacks. They separate the data the user provides from the actual commands that talk to the database.

4. Escaping (for Command Injection) – (The command deflector) escaping is like adding armor to your commands. It makes sure that any special characters in user input are treated as plain text, not as secret commands for the server.

5. Error Handling – (The poker face) don't give hackers any clues! If there's an error, display a generic message instead of revealing sensitive details about your system.

6. Least Privilege – (The need-to-know basis) imagine each part of your web application as a different guard. Each guard should only have the keys they need to do their specific job, not access to the entire fortress.

Regular Updates and Patch Management

Critical practices in web security that involve consistently updating software and systems to protect against vulnerabilities and threats.

Why They Matter:

1. Fixing Vulnerabilities

2. Software Vulnerabilities: regular updates fix security flaws.

3. Security Patches: applying patches closes security gaps.

Improving Features and Performance

4. New Features: making systems more efficient and secure.

5. Bug Fixes: updates resolve bugs potentially exploited

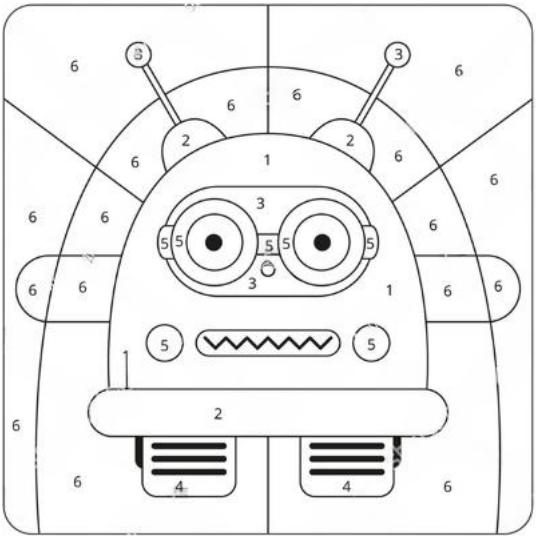
Staying Ahead of Threats

6. Evolving Threats: cyber threats constantly evolve.

Compliance: many regulations require up-to-date systems

Colour by number

Use the colour code to complete the picture



Authentication and Authorization

Protecting Against Broken Authentication

Use Strong Password Policies:

Complexity: Require passwords to be a mix of letters (both upper and lower case), numbers, and special characters.

Length: Enforce a minimum length (e.g., at least 12 characters).

Expiration: Implement periodic password changes.

Prohibition of Reuse: Prevent users from reusing old passwords.

Store Passwords Securely:

Hashing: Use strong, salted hashing algorithms (e.g., bcrypt, Argon2) to store passwords.

Avoid Plaintext: Never store passwords in plaintext or in a reversible encryption format.

Limit Login Attempts:

Rate Limiting: Implement rate limiting to restrict the number of login attempts from a single IP address.

Account Lockout: Temporarily lock accounts after a certain number of failed login attempts.

Advanced Authentication

Implement Multi-Factor Authentication (MFA):
MFA requires users to provide two or more verification factors to gain access. Adds an extra layer of security beyond just a password, making it harder for attackers to gain access.

Use Secure Session Management:

Session IDs: Generate unique session IDs for each login.

Timeouts: Automatically log out after a period of inactivity.

Secure Cookies: Use secure (HTTPS) and HttpOnly cookies to store session information

---

Data Protection

Encryption

Encryption is a method of converting readable data (plaintext) into an unreadable format (ciphertext) to protect it from unauthorized access. This process ensures that only authorized parties can read the original information using a special key.

Here's a simple breakdown of how encryption works:

1. Plaintext: The original readable data or message that needs to be protected.

2. Encryption Algorithm: A set of mathematical rules used to transform the plaintext into ciphertext.

3. Key: A secret value used by the encryption algorithm to perform the transformation. Only those with the correct key can decrypt the ciphertext back into plaintext.

4. Ciphertext: The resulting scrambled and unreadable data after encryption.

Benefits of Encryption:

1. Confidentiality: Ensures that sensitive information remains private and accessible only to authorized individuals.

2. Integrity: Helps verify that the data has not been altered during transmission.

3. Authentication: Confirms the identity of the parties involved in communication.

4. Non-repudiation: Prevents the sender from denying that they sent the information.

Fun task

Check the strong password.

Remember, a strong password keeps your accounts secure!

- [ ] sunshine123
- [ ] P@ssw0rd!2024
- [ ] aB1!z9X2?mY7!L3

Encrypting and Decrypting

Use a +2 shift key to encrypt the following sentence

SECURITY FIRST

Decrypt the following sentence using a shift key of -2

JGNNQ YQTNF

Secure Storage

Secure Storage refers to the methods and practices used to protect sensitive data from unauthorized access, tampering, and loss. This involves using various technologies and protocols to ensure that data remains confidential and intact whether it is stored on physical devices or in digital formats.

Key Components of Secure Storage:

1. Encryption: Data is encrypted before storage using strong encryption algorithms. Encryption can be applied to both data at rest (stored data) and data in transit (data being transferred).

2. Access Controls: Implementing strict access controls ensures that only authorized users and systems can access the stored data. Access can be controlled through user authentication, permissions, and roles.

3. Backups: Regular backups of data are made to prevent data loss in case of hardware failure, accidental deletion, or other disasters. Backups should also be stored securely, often in a different location than the original data.

Data Integrity

Data Integrity refers to the accuracy, consistency, and reliability of data throughout its lifecycle. Ensuring data integrity means that the data is accurate and remains unchanged unless altered through authorized processes. It is a critical aspect of data management, cybersecurity, and database design.

Hashing is a cryptographic technique used to ensure data integrity by generating a fixed-size string of characters (called a hash value or hash code) from input data of any size. This hash value represents a unique fingerprint of the original data.

Regular Security Audits and Penetration Testing

Security Audits

It is a systematic evaluation of a website or web application's security measures and practices. Its primary goal is to identify vulnerabilities, weaknesses, and potential threats that could compromise the confidentiality, integrity, or availability of the web system.

Key Aspects of Security Audits

Evaluation of Security Controls

This includes examining firewalls, intrusion detection systems, access controls, encryption mechanisms, and more.

Identification of Vulnerabilities

Vulnerability scanning, penetration testing, and code review, to uncover weaknesses in the web application or website.

Compliance Verification

Audits adheres to relevant security standards, regulations, and best practices

Risk Assessment

Prioritizing risks based on their potential impact and likelihood of exploitation.

Penetration Testing

Penetration testing, often abbreviated as "pen testing," is a proactive and authorized simulated cyberattack on a computer system, network, or web application to evaluate its security. The objective of penetration testing is to identify vulnerabilities that could be exploited by malicious attackers.

Types of Penetration Testing

Black Box Testing

The ethical hackers have no knowledge of your web application's inner workings. It's like a detective trying to solve a case with limited information.

White Box Testing

The ethical hackers have full knowledge of your web application's code and architecture. It's like a detective who has access to all the evidence and can examine it closely.

Network Fundamentals

- Networks are simply things connected. A network is a interconnection two or more devices which can transfer and receive data and information.
  The connection can be wired (such as cables or telephone wires) or wireless (such as radio waves or micro waves).
  A network enables us to share resources, exchange files

Networks are integrated into our everyday life. Be it gathering data for the weather, delivering electricity to homes or even determining who has the right of way at a road.

Because networks are so embedded in the modern-day, networking is an essential concept to grasp in cybersecurity.

Networks can be found in all walks of life:

-A city's public transportation system
-Infrastructure such as the national power grid for electricity
-Meeting and greeting your neighbours

What is
the Internet?

The Internet is one giant network that consists of many, many small networks within itself.

History of Internet

The first iteration of the Internet was within the ARPANET project in the late 1960s. This project was funded by the United States Defence Department and was the first documented network in action.
However, it wasn't until 1989 when the Internet as we know it was invented by Tim Berners-Lee by the creation of the World Wide Web (WWW).

Public Network

A public network is a type of network wherein anyone, namely the general public, has access and through it can connect to other networks or the Internet. This is in contrast to a private network, where restrictions and access rules are established in order to relegate access to a select few.

Private Network

Private Networks are smaller networks that are commonly used in homes, businesses, and organizations to provide secure communication and data exchange. It is restricted to a specific group of users or devices.

Network Protocol

It is a set of rules that determines how data is transmitted between different devices in a network regardless of any differences in their internal processes, structure or design.

In order to communicate together, two devices must support the same protocol or a gateway will need to be used to translate the communication.

Types of network protocols

Network management protocols

These protocols set out policies designed to monitor, manage and maintain a network. Examples include
Syslog
NETCONF
ICMP

Network communication protocols

A group of protocols used to establish rules and formatting (such as syntax, synchronization and semantics) for exchanging data across a network. Types of network communication protocols include TCP, UDP, IP, HTTP, IRC, BGP and ARP.

Network security protocols

Security protocols are protocols that use security measures such as cryptography and encryption to protect data. Examples include SFTP, SSL and HTTPS.

IP Address

IP address (or Internet Protocol) is an unique address used to identify a computer when connecting to internet. IP address can be used as a way of identifying a host on a network for a period of time, where that IP address can then be associated with another device without the IP address changing.

IP addresses can change from device to device but cannot be active simultaneously more than once within the same network.

Types of IP Address:

1. Private IP address - given to the devices connected to a private network such as at home or business network. This IP address cannot be accessed from outside this private network.

2. Public IP address - given to a private network when connecting to internet and it is globally unique. Public IP addresses are given by your Internet Service Provider (or ISP) at a monthly fee.

3. Static and Dynamic IP addresses - IP addresses that are configured manually to a devices on a network is called Static IP address. This static IP address cannot be changed automatically. Dynamic IP addresses are automatically configured and assigned when a router is set up with internet. These dynamic IP addresses are managed by the Dynamic Host Control Protocol (DHCP) which can be the Internet router.

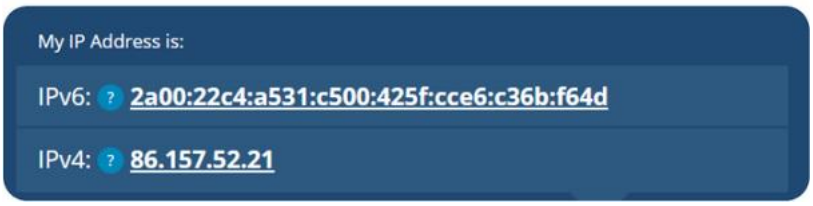
IPv4

IPv4 is unique address on the network made up of 32 binary bits. IPv4 is an older version which consumes only up to 4 billion IP addresses, but it is still in use. IPv4 is expressed in four sets of numbers, each set separated by a dot. Each set is the decimal representation of an eight-digit binary number, also called as an Octet. This number is calculated through a technique known as IP addressing & subnetting.

Each octet can range between 00000000 - 11111111 in binary and 0 - 255 in decimal. Some numbers in the above ranges are reserved for some specific purposes on TCP/IP networks.

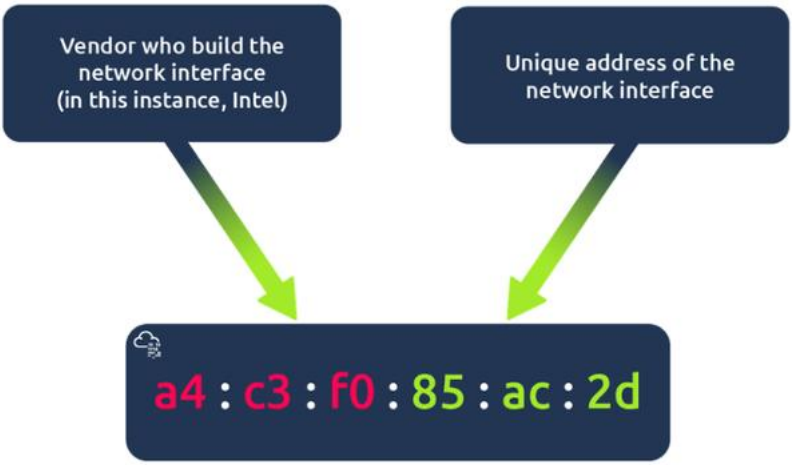
IPv6

IPv6 is the successor to a previous addressing infrastructure, IPv4, which had limitations IPv6 was designed to overcome. It is an unique address made up of 128 binary bits. It is expressed in eight groups of hexadecimal numbers, each group is separated by a colon.



MAC Addresses

Devices on a network will all have a physical network interface, which is a microchip board found on the device's motherboard. This network interface is assigned a unique address at the factory it was built at, called a MAC (Media Access Control) address.



The MAC address is a twelve-character hexadecimal number (a base sixteen numbering system used in computing to represent numbers) split into two's and separated by a colon. In this example, the first six characters represent the company that made the network interface, and the last six is a unique number.

MAC addresses can be faked or "spoofed" in a process known as spoofing. This spoofing occurs when a networked device pretends to identify as another using its MAC address. When this occurs, it can often break poorly implemented security designs that assume that devices talking on a network are trustworthy.

Ping (ICMP)

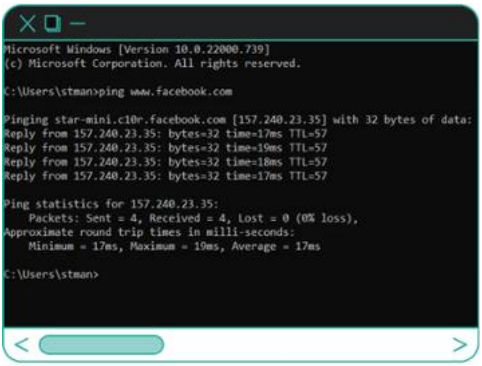
Ping is one of the most fundamental network tools available to us. Ping uses ICMP (Internet Control Message Protocol) packets to determine the performance of a connection between devices.

When a ping command is issued, an echo request packet is sent to the address specified. When the remote host receives the echo request, it responds with an echo reply packet. By default, the ping command sends several echo requests, typically four or five.

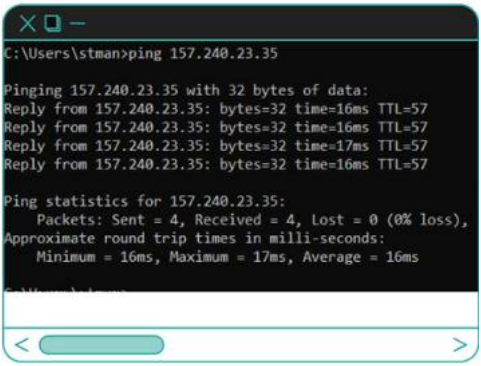
The result of each echo request is displayed, showing whether the request received a successful response, how many bytes were received in response, the Time to Live (TTL), and how long the response took to receive, along with statistics about packet loss and round trip times.

The syntax for a basic ping command is similar for both Windows and Linux systems. It's just "ping" followed by the destination URL or IP address.

1. Ping www.facebook.com



2. Ping 157.240.23.35



Types
of network

There are different types of network based on its size as well its purpose. The size of the network is based on the geographical area and number of computers. It can be devices interconnected within a single room or across the world.

Main types

WAN
(Wide Area Network)

This is larger network which is spread in a larger geographical area such as a country, region or continent. This network can be considered as a connection of a few LANs through wired or wireless medium. It is limited to an organization.

PAN
(Personal Area Network)

It is the smallest network type which is used to connect personal devices such as Smart phones, tablets computer and personal computers for establishing digital communication and to connect to internet.

LAN
(Local Area Network)

It is a connection of a group of computers and peripheral devices within a single site. LANs can be setup as wired (WLAN) or wireless (Cabled LAN). It is a simple and widely used network for sharing resources like printer, games and other applications. Generally LAN is a private network which is owned or controlled by single organization.

Local Area Network
LAN Topologies

Network topology is a schematic description of how network is arranged, including the physical and logical description of how the links, devices and nodes are set up to relate to each other.
Physical connections refer to how the nodes and the network are interconnected. Logical connections refer to the conceptual understanding of how the network is set up and the movement of data.

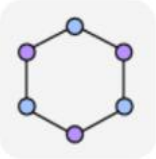
Star Topology

The main premise of a star topology is that devices are individually connected via a central networking device such as a switch or hub. This topology is the most commonly found today because of its reliability and scalability - despite the cost.
Any information sent to a device in this topology is sent via the central device to which it connects.

Bus Topology

This type of connection relies upon a single connection which is known as a backbone cable. Because everything is connected in a straight line off one central cable, it's a cost-effective topology, and simple to set up and add new nodes.

Ring Topology



In a ring network, the nodes and links are arranged in a ring. Each node has exactly two neighbors. In such a network, repeaters are used to ensure that data can reach the nodes that are farthest away from each other in the ring. Data usually flows unidirectionally in a ring network.

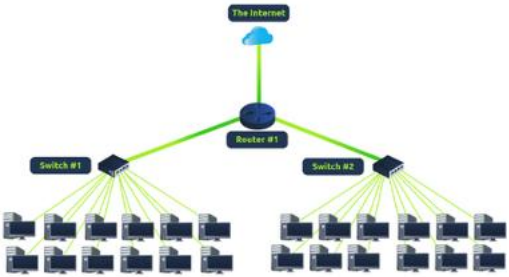
Network Devices

Network devices are hardware devices that help other devices like computers, printers, fax machines and other electronic devices to connect to a network. Network devices help to transfer data faster, securely and efficiently throughout the network.

What is a Switch?

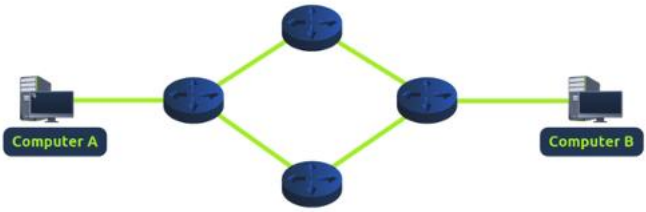
Switches are dedicated devices within a network that are designed to aggregate multiple other devices such as computers, printers, or others. These various devices plug into a switch's port.

Switches are usually found in larger networks such as businesses / schools, where there are many devices to connect to the network. Switches can connect a large number of devices by having ports of 4, 8, 16, 24, 32, and 64 for devices to plug into.



What is a Router?

It's a router's job to connect networks and pass data between them. It does this by using routing (hence the name router!). Routing is the label given to the process of data travelling across networks. Routing involves creating a path between networks so that this data can be successfully delivered.



Subnetting

When a bigger network is divided into smaller networks, to maintain security, then that is known as Subnetting. So, maintenance is easier for smaller networks.
Subnetting provides a range of benefits, including Efficiency, Security and Full control

How Does Subnetting Work?

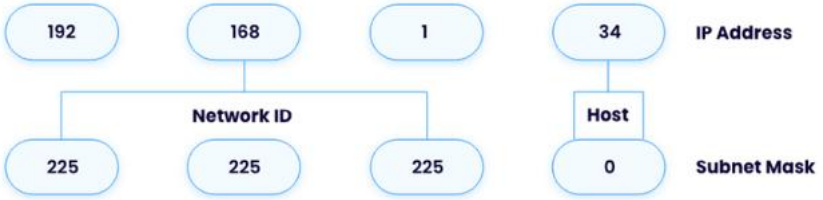
The working of subnets starts in such a way that firstly it divides the large networks into smaller subnets.
For communicating between large networks, routers are used. Each subnet allows its linked devices to communicate with each other.

What is Subnet Mask?

A subnet mask is a number that distinguishes the network address and the host address within an IP address. A subnet is a smaller network within a network that requires a subnet mask.

When you connect a device to a network, the network assigns an IP address to the device. That IP address consists of two parts: the network portion and the host portion.

The network portion of the IP address identifies the overall network while the host portion identifies the device.
The network address and host address contained in an IP address are indistinguishable from each other without a subnet mask. The subnet mask allows network traffic to understand IP addresses by splitting them into the network and host addresses.



The ARP Protocol

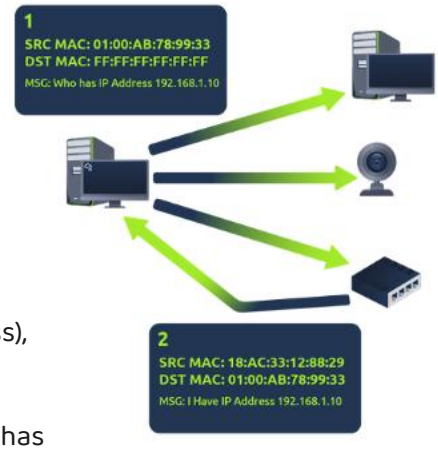
Devices on a network use two main identifiers: a MAC address and an IP address. The Address Resolution Protocol (ARP) is a protocol used to find the MAC address associated with a device's IP address on a local network. This allows devices to communicate with each other using the correct hardware address.

The Address Resolution Protocol (ARP) allows devices to discover the MAC address associated with a known IP address on a local network. Each device maintains an ARP cache, which stores recently learned IP-to-MAC address mappings.

When a device wants to communicate with another device but does not know its MAC address, it sends an ARP Request broadcast to the local network. The device with the matching IP address responds with an ARP Reply containing its MAC address, allowing communication to take place.

How does ARP Work?

Each device within a network has a ledger to store information on, which is called a cache. In the context of the ARP protocol, this cache stores the identifiers of other devices on the network.



In order to map these two identifiers together (IP address and MAC address), the ARP protocol sends two types of messages:
1- ARP Request – A device asks, "Who has this IP address?"
2- ARP Reply – The device with that IP address responds with its MAC address.

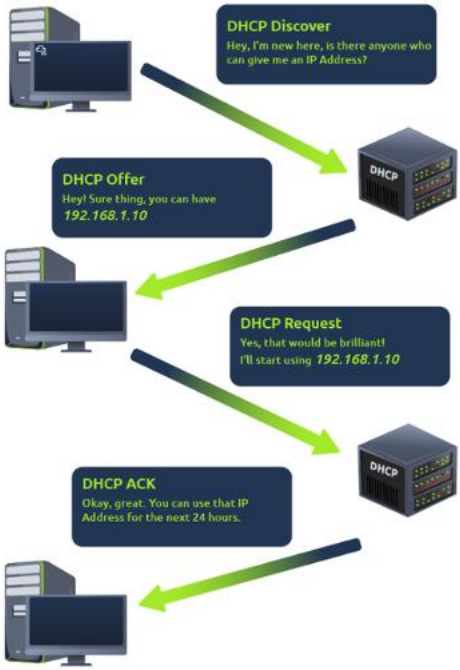
DHCP
Protocol

IP addresses can be assigned either manually, by entering them physically into a device, or automatically and most commonly by using a DHCP (Dynamic Host Configuration Protocol) server

How DHCP Protocol works?

1. DHCP Discover

When a device connects to a network and is configured to obtain an IP address automatically, it sends a DHCP Discover message to find available DHCP servers on the network.



2. DHCP Offer

A DHCP server responds with a DHCP Offer message containing an available IP address and other network configuration settings that the device can use.

3. DHCP Request

The device sends a DHCP Request message to indicate that it accepts the offered IP address and requests that the DHCP server assign it.

4. DHCP ACK (Acknowledgement)

The DHCP server sends a DHCP ACK message to confirm the IP address assignment. The device can then use the assigned IP address to communicate on the network.

Firewalls

A *firewall* is a security device or software that monitors and controls incoming and outgoing network traffic. It allows or blocks traffic based on predefined security rules configured by an administrator.

These rules can consider factors such as IP addresses, ports, protocols, and the type of traffic being transmitted.

VPN

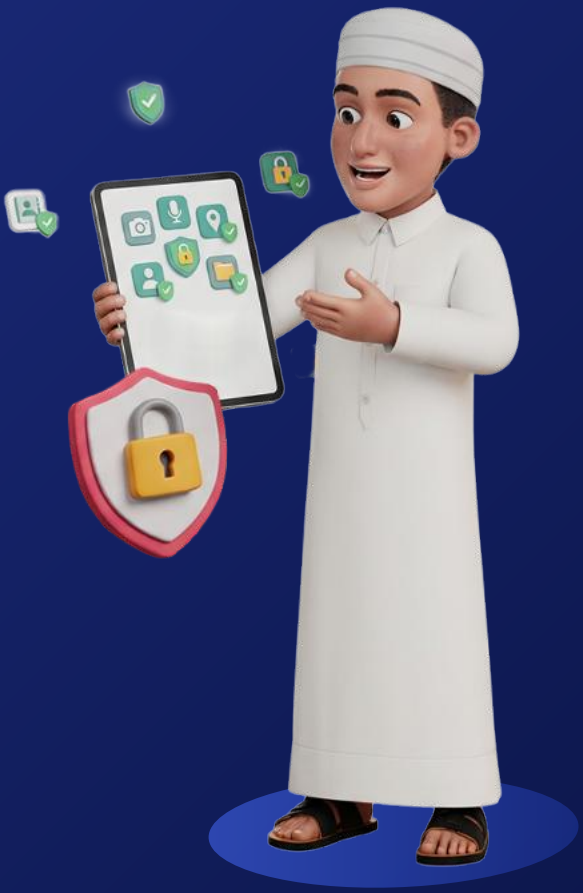
A Virtual Private Network (or VPN for short) is a technology that allows devices on separate networks to communicate securely by creating a dedicated path between each other over the Internet (known as a tunnel). Devices connected within this tunnel form their own private network.

Fact alert!

The earliest known cyberattack was in 1834 which involved Frenchmen tampering with the telegraph system to steal financial information

Building Blocks of Your Digital World

An operating system (OS) is software that manages a computer's hardware and software resources and provides common services for computer programs. It acts as an intermediary between the user and the computer hardware.



Types of Operating Systems

Linux MacOS Windows

Basic Functions of an OS

Managing Hardware Controls all the hardware devices in your computer, like your keyboard, mouse, monitor, and storage drives. It's like the mayor managing all the city's infrastructure.

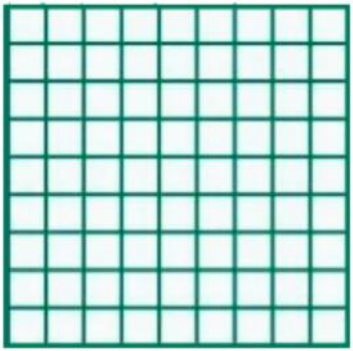
Running Applications Runs your programs and apps, making sure they have the resources they need to function properly. It's like the mayor ensuring that businesses have the permits and resources they need to operate.

File Management Organizes your files and folders, making it easy to find and access what you need. It's like the mayor maintaining a well-organized city map.

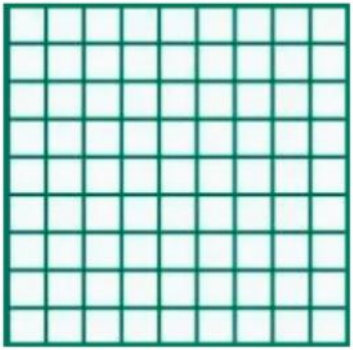
User Interface Provides a visual way for you to interact with your computer, like the windows, icons, and menus you see on your screen. It's like the mayor creating a user-friendly city guide for tourists.

Computer Talk

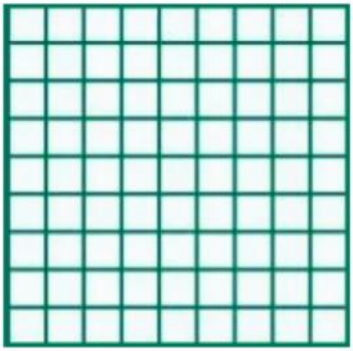
Binary only uses numbers 1 and 0, which represents two possible states of the electric signals inside computers - on (1) and off (0). Reveal the pictures below. Use white to represent 0 and green to represent 1.



1. 000000000
2. 000101000
3. 000101000
4. 000000000
5. 011000110
6. 001000100
7. 000111000
8. 000000000
9. 000000000



1. 000010000
2. 000111000
3. 001111100
4. 011111110
5. 001111100
6. 001101100
7. 001101100
8. 001101100
9. 000000000



1. 000000000
2. 001101100
3. 011111110
4. 011111110
5. 011111110
6. 001111100
7. 000111000
8. 000010000
9. 000000000

Password Cracking

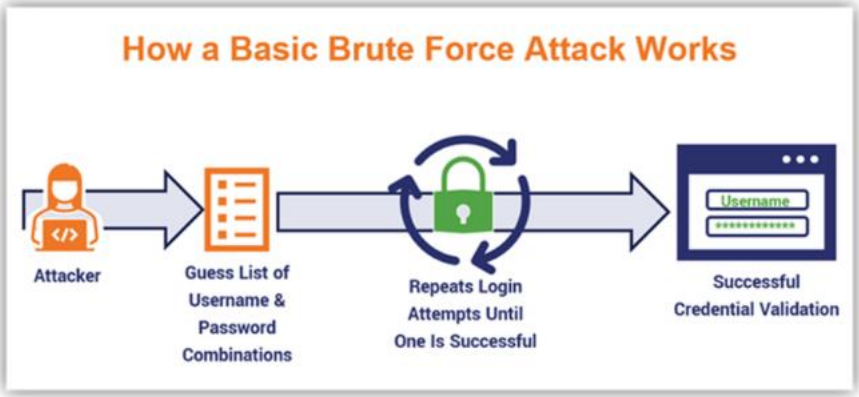
Introduction to Password Cracking

Password cracking is the art of guessing or uncovering someone's password. Hackers use various methods to try and break into your accounts, and it's essential to understand their tricks so you can protect yourself.

Common Password Cracking Techniques

1. brute-force attacks

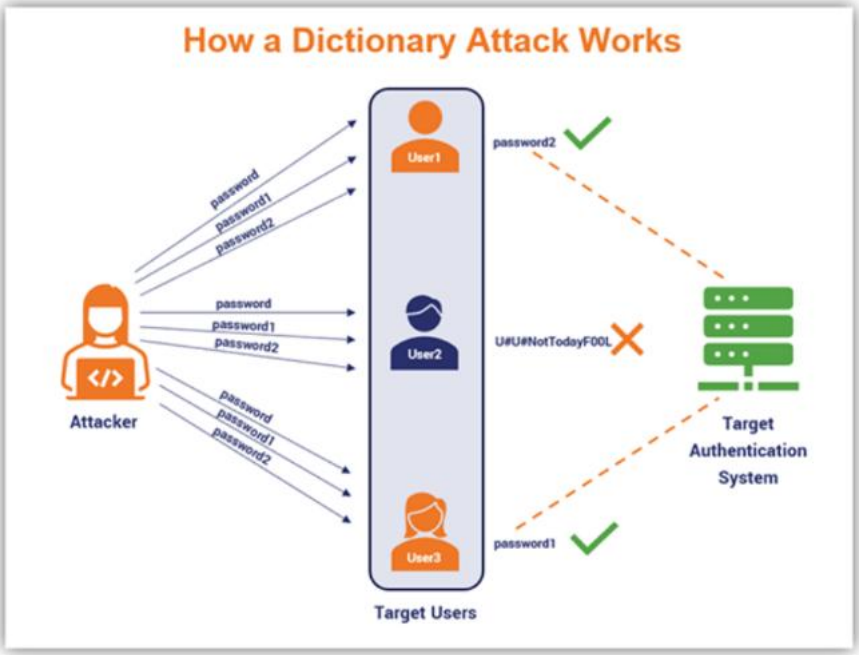
Hackers use powerful computers to try every possible combination of characters until they find the right password.



Common Password Cracking Techniques

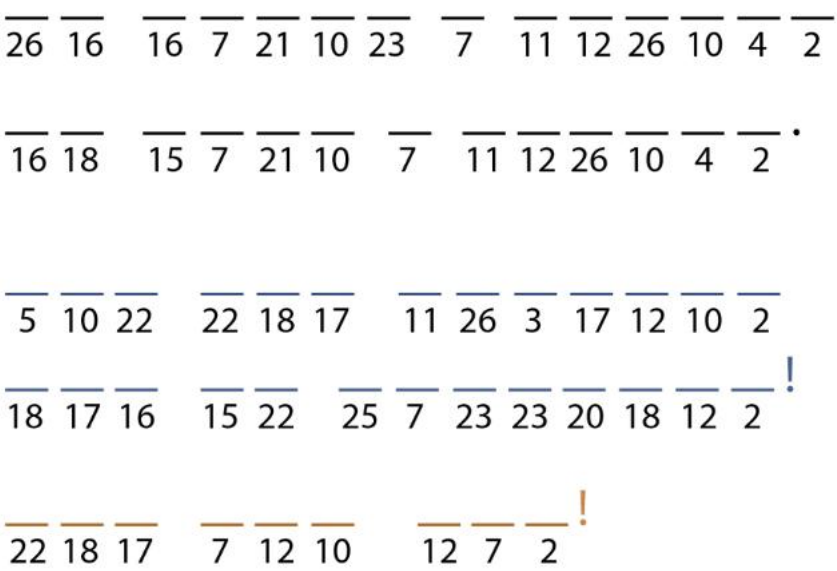
2. Dictionary Attacks

Dictionary Attacks - Hackers use lists of common words, phrases, and patterns to guess passwords.



ف

Use the code below to hack the 3 passwords!



A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
7	1	8	2	10	11	3	5	26	9	21	19	15	4	18	25

Q	R	S	T	U	V	W	X	Y	Z
6	12	23	16	17	13	20	14	22	24

Privilege Escalation

Privilege escalation is when an attacker gains higher-level permissions on a system, giving them more access and control.

There are two main types:

Vertical Privilege Escalation: Moving from a lower-level user to a higher-level user (like from a guest to an admin).

Horizontal Privilege Escalation: Gaining access to resources within the same privilege level but belonging to another user (like accessing another user's files).

Windows Privilege Escalation

Windows systems mainly have two kinds of users:

Administrators: These users have the most privileges. They can change any system configuration parameter and access any file in the system.

Standard Users: These users can access the computer but only perform limited tasks. Typically, these users cannot make permanent or essential changes to the system and are limited to their files.

Common Techniques for Windows Privilege Escalation

1

Exploiting Vulnerable Services
Windows services often run with elevated privileges (like SYSTEM). If a service has a vulnerability, hackers can exploit it to gain those privileges.

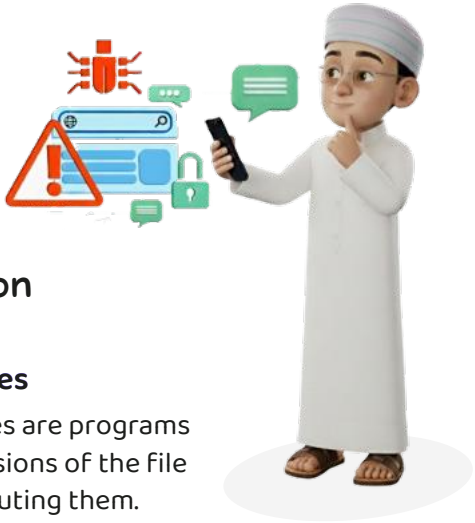
2

Misconfigurations
Sometimes, system administrators make mistakes when configuring Windows settings or permissions. Hackers can exploit these misconfigurations to gain elevated privileges.

3

Zero-Day Exploits
These are vulnerabilities that are unknown to the software vendor or the public. Hackers who discover these vulnerabilities can exploit them before a patch is available.

Linux Privilege Escalation



Common Techniques for Linux Privilege Escalation

1

Exploiting SUID Binaries
SUID (Set User ID) binaries are programs that run with the permissions of the file owner, not the user executing them.
If a SUID binary has a vulnerability, hackers can exploit it to gain the file owner's privileges.

2

Misconfigurations

Misconfigurations in Linux systems can be exploited to gain elevated privileges. This could involve incorrect file permissions, weak passwords, or insecure configurations.

3

Exploiting Services

Services running with elevated privileges can be exploited if not properly secured. This can happen if the service is misconfigured, outdated, or has a vulnerability.

Service Exploits

Services are programs that run in the background of your computer

How it works,

- **Identify a Vulnerable Service:** Hackers look for services that are running with elevated privileges (like root) and have known vulnerabilities.

- **Exploit the Vulnerability:** They use a specially crafted exploit to take advantage of the vulnerability, often gaining the privileges of the service.

- **Gain Access:** With elevated privileges, the hacker can now do things they couldn't do before, like installing malware, stealing data, or taking control of the system.

Ransomware

Ransomware works by encrypting your files, scrambling them into unreadable gibberish. The only way to unscramble them is with a special key, which the hackers hold for ransom.

How Ransomware can occur?

- **Phishing Emails:** These deceptive emails often look like they're from a trusted source, like your bank or a friend. They might contain a malicious attachment or a link that, when clicked, downloads the ransomware onto your computer.
- **Malicious File Types:** Attackers may send files that appear safe in order to trick users, such as PDF files, Word and Excel documents, and ZIP files. These files may contain links or instructions that lead to the download or execution of malware, such as ransomware. The malware itself may also be disguised as executable files (.exe) or scripts such as PowerShell (.ps1), Batch (.bat), and JavaScript (.js) files.
- **Drive-by Downloads:** Simply visiting a compromised website can trigger a drive-by download, where ransomware is silently installed without your knowledge.

Security measures against ransomware

- **Keep Your Software Updated**
- **Be Cautious of Emails and Links**
- **Use a good Antivirus Software**
- **Back Up Your Data Regularly**

Strong Authentication and Password Managers

Strong Passwords

- **Use atleast 12 characters**
- **Mix it up with uppercase and lowercase letters, numbers, and symbols (like @, #, $, %).**
- **Don't reuse the same password for different accounts.**

Multi-Factor Authentication (MFA)

Common types of MFA include:

One-Time Codes (OTPs): Sent to your phone via SMS or an authenticator app.
Push Notifications: Approve login attempts on your phone.
Biometrics: Fingerprint or facial recognition.

Password Managers

Password managers are tools that store and organize your passwords securely. They help you create strong, unique passwords for each of your accounts and automatically fill them in when you need to log in. This way, you don't have to remember multiple passwords, and your accounts are safer.

Popular password managers include:

1Password

KeePass

Bitwarden

LastPass

T

Decode the hidden words

Letter 1 - • ↓ ↓ →

Letter 2 - • ← ↑ ↑ → →

Letter 3 - • ↑ ← ←

Letter 4 - • ← ← ↓ ↓ →

Letter 5 - • → → ↑ ↑ ← ←

Letter 6 - • ↑ → →

Letter 7 - • ↑ ↑ ← ← ↓

Letter 8- • ← ↑ ↑ ←

Letter 9 - • ↓ ← ↑ ←

Letter 10 - • ↓ → ↓

Letter 11 - • ↓ ← ← ↑ ↑

Letter 12 - • → ↑ ↑ ← ← ←

Letter 13 - • ↑ → ↓ →

Letter 14 - • ↑ → ↑ → ↓

I	Y	E	U	L
T	Z	D	C	N
C	J	●	R	O
K	S	P	B	F
G	H	R	A	M

Public Network Safety

The Dangers of Public Wi-Fi

- Man-in-the-Middle Attacks: Hackers can intercept your traffic and steal your login credentials, credit card numbers, and other sensitive data.

- Eavesdropping: Hackers can listen in on your conversations and see what websites you're visiting.

- Malware Distribution: Hackers can spread malware through public Wi-Fi networks, infecting your device without your knowledge.

Staying Safe on Public Wi-Fi

- You can use a Virtual Private Network (VPN) that encrypts your traffic, making it unreadable to hackers.
- Avoid doing online banking, shopping, or accessing other sensitive accounts on public Wi-Fi.
- Surf secure websites only, look for HTTPS
- Keep your software updated

Backups

A backup is a copy of your important data, like files, photos, and documents, stored separately to keep it safe. If your original data is lost or damaged, you can use the backup to restore it

Types of Backups

Full Backup

This creates a complete copy of all your files and data. It takes longer to create but is the most comprehensive backup option.

Incremental Backup

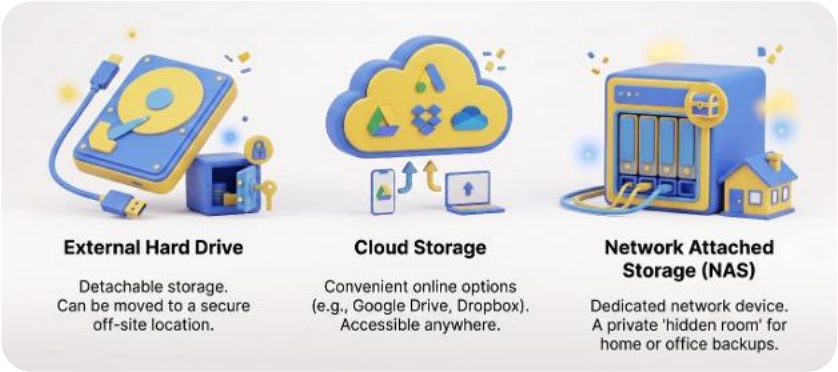
This copies only the files that have changed since the last backup. It's faster than a full backup but requires multiple backups to restore all your data.

Differential Backup

This copies all the files that have changed since the last full backup. It's faster to restore than an incremental backup but slower to create.

Backups

How to store the Backups?



1

External Hard Drive

which can be disconnected and stored in a secure location.

2

Cloud Storage

Google Drive, Dropbox, or OneDrive all offer convenient and accessible online backup options.

3

Network Attached Storage (NAS)

A dedicated device for storing backups on your home or office network. It's like having a hidden room in your house where you keep your most prized possessions.

Antivirus

Antivirus software is a program designed to detect, prevent, and remove viruses and other malicious software from your computer, keeping it safe and secure.

Functions of an Antivirus Software

It regularly checks your computer's files and programs for any signs of malware.

If it detects anything unusual, it compares it to a database of known bad guys (malware signatures).

If it confirms that something is indeed malware, it quarantines or deletes it, preventing it from causing any harm.

Some antivirus programs try to prevent malware from getting into your system in the first place. They might block malicious websites or scan files before you download them.

Types of
Antivirus Software

Signature-Based Antivirus

This type relies on a database of known malware signatures

Examples:
Norton
McAfee
Avast
AVG
Kaspersky

Heuristic-Based Detection

This analyses the behaviour of files and programs to detect suspicious activity, even if it's not a known malware signature.

Cloud-Based Protection

This leverages the power of the cloud to scan files and detect threats in real-time.

How to choose the right Antivirus software?

- Choose a well-known and trusted brand.
- Look for features like real-time protection, web filtering, email scanning, and ransomware protection.
- Make sure the antivirus doesn't slow down your computer too much.
- Choose a program that's easy to install and use.

Regular Updates and Patch Management

You should also keep your operating system and applications updated. Software updates often include patches that fix security .vulnerabilities that hackers could exploit

Additional Defensive Measures

Firewalls

Firewalls act as a barrier between your computer and the internet, controlling incoming and outgoing network traffic. They can help block unauthorized access attempts and prevent malware from spreading.

Intrusion Detection Systems (IDS)

IDS monitors network traffic for suspicious activity and alerts you to potential threats.

Security Awareness Training

Educating yourself and others about cybersecurity best practices is crucial for defence. This includes learning how to spot phishing emails, create strong passwords, and avoid risky online behaviour.

The Ethical Hacker's Playbook

Penetration testing, or "pen-testing," is an authorized simulated cyberattack on a computer system, performed to evaluate the system's security. In essence, it's a way to find out how strong your defences are before the bad guys do.

Fact alert!

Penetration testing is gaining so much traction that it is estimated that by 2026, it will be a $4.5 billion industry -(Gartner)

The Ethics of Hacking

Legality vs. Ethics

Ethical hacking, also known as penetration testing, is completely legal. But being legal doesn't mean it's a free-for-all. Before any ethical hacking takes place, there's a crucial agreement called the Rules of Engagement (ROE).
This document outlines:
Permission: Clearly states who is allowed to conduct the pentest and who's giving the green light.
Test Scope: Specifies exactly which systems, networks, or applications are fair game for testing.
Rules: Lays down the law on what tools and techniques are allowed and any off-limits areas.

The Rules of Engagement (ROE)

The ROE acts as a moral compass for ethical hackers.
It ensures they stay within the legal and ethical boundaries of their work.
It's like a set of rules for a game – everyone knows what's allowed and what's not, so there are no surprises.

The Hacker Spectrum

There are three main categories of hackers, each with their own motivations and ethical boundaries:

Gray Hats
The Wild Cards

These hackers fall in the murky middle ground. They might uncover vulnerabilities without permission, but they often report them to the organization, hoping they'll be fixed. Their actions can be both helpful and ethically questionable.

Black Hats
The Villains

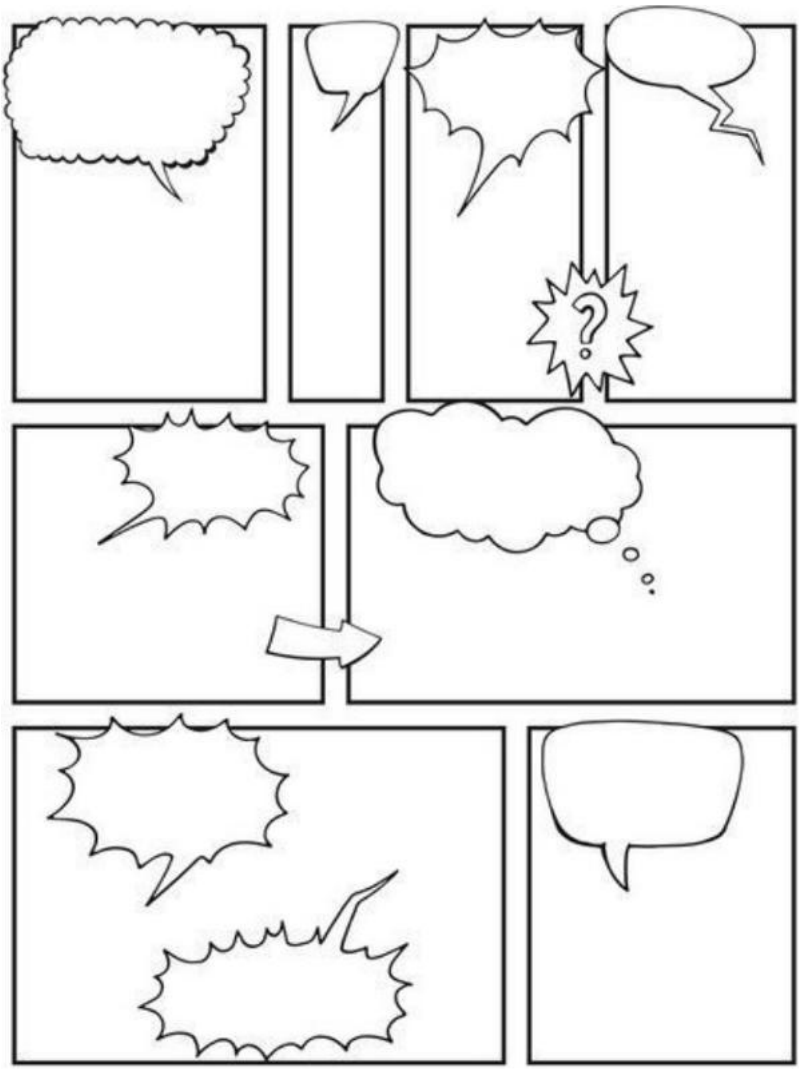
These are the bad guys – malicious hackers who exploit vulnerabilities for personal gain, financial profit, or to cause harm. Their actions are illegal and often involve cybercrime.

White Hats
The Heroes

These are the good guys – ethical hackers who use their skills to help organizations improve their security. They operate within the law and follow a strict code of ethics.

Comic time!

Use types of Hackers as your characters (white, black & gray) to illustrate a story about hacking...



Penetration Testing
Phases

The Five Phases of Penetration Testing

Phase 1 | **Reconnaissance (Recon)**
The Hacker's Intel Gathering Mission

Phase 2 | **Scanning**
Probing for Weaknesses

Phase 3 | **Gaining Access** (Exploitation)
Breaching the Defences

Phase 4 | **Maintaining Access**
(Post-Exploitation) Establishing a Foothold

Phase 5 | **Reporting**
The Detective's Report

Fact Alert!

Bug Bounties: Companies like Google, Facebook, and Microsoft run bug bounty programs, where they pay hackers to find and report security vulnerabilities. Some hackers have earned over a million dollars just by finding bugs! **Do you want to know more? More details coming up.**

Penetration Testing
Phases

Reconnaissance (Recon)

This is the information-gathering phase. Ethical hackers gather as much information as possible about the target system, like a detective gathering clues. They might use open-source intelligence (OSINT), social engineering, and other authorized methods to identify potential attack surfaces.

Scanning

This is where the pentesters start probing the target system for weaknesses. They might use automated tools to scan for open ports, vulnerabilities in software, or misconfigurations. It's like a doctor running tests to diagnose a patient.

Gaining Access (Exploitation)

Breaching the Defenses - If the hackers find a vulnerability, they'll try to exploit it to gain access to the system. This could involve using a known exploit, crafting a custom attack, or even tricking a user into clicking a malicious link. It's like a thief finding a way to pick a lock.

Maintaining Access (Post-Exploitation)

After gaining access, ethical hackers assess the potential impact of the compromise. They determine what resources could be accessed, whether privileges can be escalated, and how far an attacker could move within the environment, without causing unnecessary disruption.

Covering Tracks (Reporting)

The Detective's Report - Finally, the ethical hackers will document their findings and report them to the system owner. This report will include details about the vulnerabilities they found, how they exploited them, and recommendations for fixing them. It's like a detective writing up their case report.

Legal Frameworks and Industry Accreditation

Just like any profession, ethical hacking operates within a framework of rules and regulations. These frameworks ensure that penetration testing is conducted legally, ethically, and with a high degree of professionalism.

Industry Standards and Certifications:

1. OSSTMM (Open Source Security Testing Methodology Manual)

A comprehensive manual covering various aspects of security testing, including information gathering, vulnerability scanning, and reporting. It's known for its in-depth coverage and flexibility, but it can be complex and uses unique terminology.

2. OWASP (Open Web Application Security Project)

A community-driven project focused on web application security. OWASP provides a widely used framework for testing web applications, along with a list of the top 10 most critical web application security risks. It's easy to understand and actively maintained, but it may not always be clear how to categorize overlapping vulnerabilities.

3. NIST Cybersecurity Framework

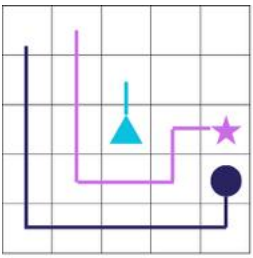
Developed by the National Institute of Standards and Technology (NIST), this framework provides guidelines for managing and reducing cybersecurity risk. It's widely adopted by organizations in the United States and offers a structured approach to cybersecurity. However, it can be complex and may not fully address the unique needs of every organization.

4. NCSC CAF (Cyber Assessment Framework)

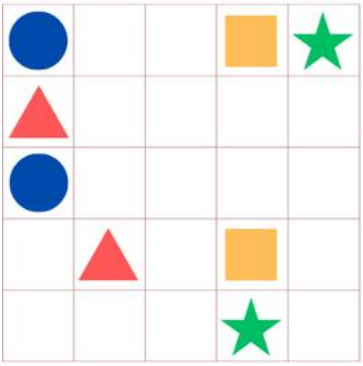
This UK government-backed framework helps organizations assess and manage their cyber risks. It covers a wide range of topics, including data security, system security, and incident response. While it's backed by a reputable authority, it's relatively new and may not be as widely adopted as other frameworks.

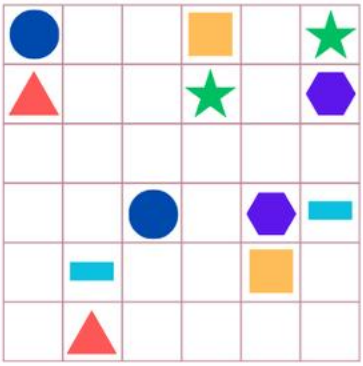
Free Flow

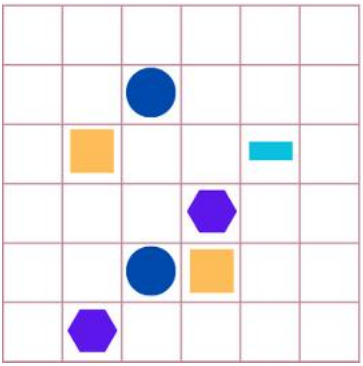
Can you draw lines to connect each pair of identical shapes together? The lines must not cross or touch each other, and only one line is allowed on each grip square.
You can't use diagonal lines.

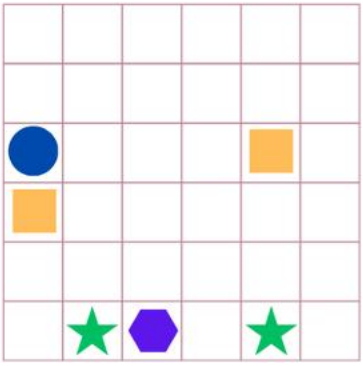


The example solution shows how it works.









Black Box, White Box, and Gray Box Penetration Testing

Fact Alert!

The first ethical hacking group was the "Tiger Teams," formed in the 1970s to test the security of computer systems by attempting to break into them

You know nothing about the organization's inner workings. You'll have to rely on your observation skills and social engineering to blend in and gather information.

You have some limited information about the organization, maybe a floor plan or a list of employees. You'll need to combine your knowledge with observation and social engineering to succeed.

You have complete access to the organization's blueprints, security protocols, and personnel records. You can use this knowledge to plan your infiltration meticulously.

Bug Bounty Programs

Understanding Bug Bounty Programs

Bug bounty programs are like a treasure map for ethical hackers. Companies create these programs and invite hackers to find "bugs" (security vulnerabilities) in their websites, apps, or networks. If you find a valid bug, you report it to the company, and they reward you with cash or other prizes.

How Bug Bounty Programs Benefit Everyone?

Companies: They get help finding and fixing vulnerabilities before the bad guys exploit them.
Hackers: They get to use their skills for good, gain recognition, and earn money.
The Internet: It becomes a safer place for everyone as more bugs are discovered and fixed.

How to Participate in Bug Bounty Programs?

1. Choose a Platform

Many platforms host bug bounty programs, like HackerOne and Bugcrowd.

2. Pick Your Target

Choose a program that interests you.

3. Read the Rules

4. Hunt for Bugs

5. Report Your Findings

6. Get Rewarded!

If your report is valid, you'll receive a bounty (usually cash) and recognition for your worki

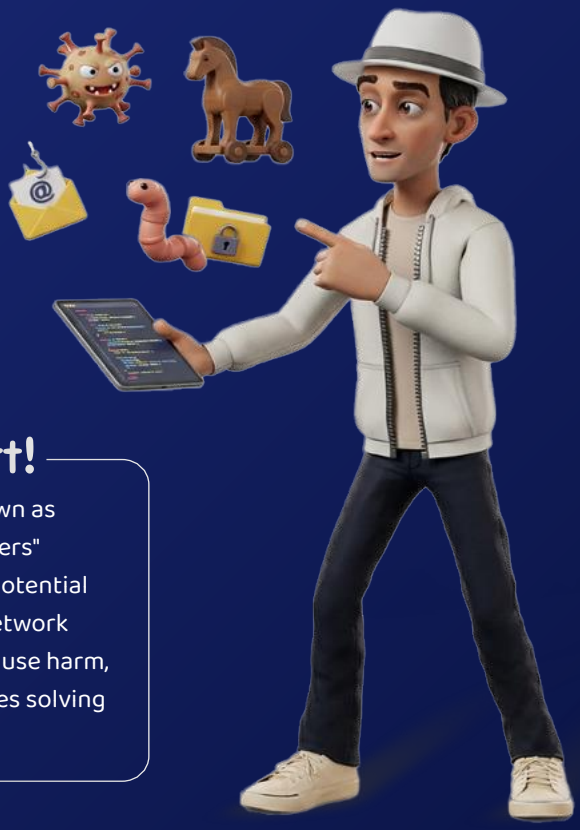
Best Practices for Bug Bounty Hunting

- Stay Within Scope
- Be Thorough
- Be Respectful
- Never Exploit Vulnerabilities
- Keep Learning

7

Cyber Threat Intelligence

Cyber Threat Intelligence (CTI) can be defined as evidence-based knowledge about adversaries, including their indicators, tactics, motivations, and actionable advice against them. These can be utilised to protect critical assets and inform cyber security teams and management business decisions.



Fact Alert!

Professionals known as "cyber threat hunters" actively seek out potential threats within a network before they can cause harm, similar to detectives solving a crime.

Data

Discrete indicators associated with an adversary, such as IP addresses, URLs or hashes.

Information

A combination of multiple data points that answer questions such as "How many times have employees accessed tryhackme.com within the month?"

Intelligence

The correlation of data and information to extract patterns of actions based on contextual analysis.

Types of Cyber Threat Intelligence

Strategic Intel

High-level intel that looks into the organization's threat landscape and maps out the risk areas based on trends, patterns and emerging threats that may impact business decisions.

Tactical Intel

Assesses adversaries' tactics, techniques, and procedures (TTPs). This intel can strengthen security controls and address vulnerabilities through real-time investigations.

Technical Intel

Looks into evidence and artefacts of attack used by an adversary. Incident Response teams can use this intel to create a baseline attack surface to analyze and develop defense mechanisms.

Operational Intel

Looks into an adversary's specific motives and intent to perform an attack. Security teams may use this intel to understand the critical assets available in the organisation (people, processes and technologies) that may be targeted.

CTI
Lifecycle

CTI Standards & Frameworks

Standards and frameworks provide structures to standardize the distribution and use of threat intel across industries. They also allow for common terminology, which helps in collaboration and communication.

MITRE ATT&CK

The ATT&CK framework is a knowledge base of adversary behavior, focusing on the indicators and tactics. Security analysts can use the information to be thorough while investigating and tracking adversarial behavior.

CTI Standards & Frameworks

TAXII

The Trusted Automated exchange of Indicator Information (TAXII) defines protocols for securely exchanging threat intel to have near real-time detection, prevention and mitigation of threats.

STIX

Structured Threat Information Expression (STIX) is a language developed for the "specification, capture, characterization and communication of standardized cyber threat information". It provides defined relationships between sets of threat info such as observables, indicators, adversary TTPs, attack campaigns, and more.

Cyber Kill Chain

Developed by Lockheed Martin, the Cyber Kill Chain breaks down adversary actions into steps. This breakdown helps analysts and defenders identify which stage-specific activities occurred when investigating an attack.

The Diamond Model

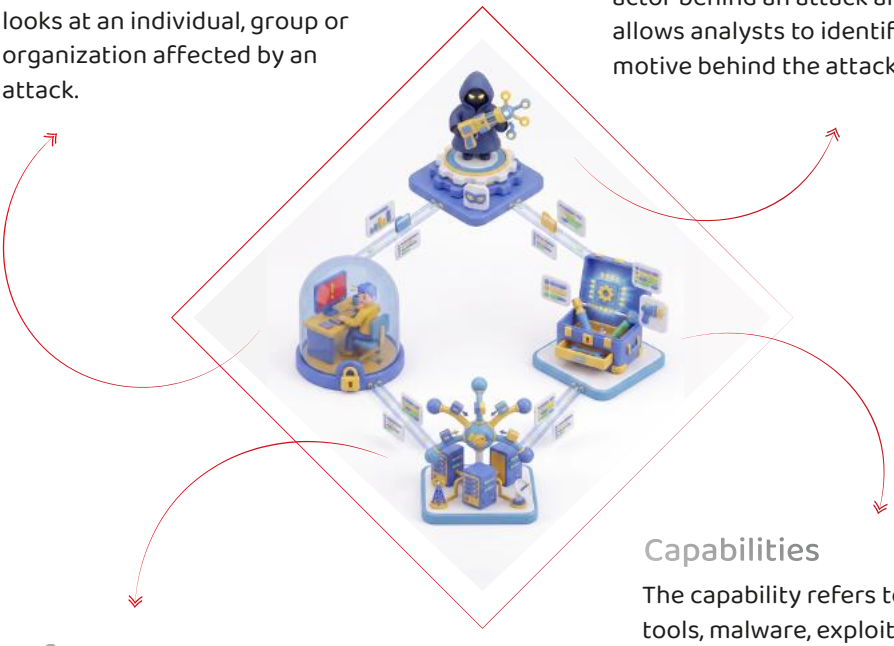
The diamond model looks at intrusion analysis and tracking attack groups over time. It focuses on four key areas, each representing a different point on the diamond.

Victim

The opposite end of adversary looks at an individual, group or organization affected by an attack.

Adversary

The focus here is on the threat actor behind an attack and allows analysts to identify the motive behind the attack.



Infrastructure

The infrastructure consists of the resources the adversary uses to conduct the attack, such as domains, IP addresses, servers, websites, and command-and-control (C2) systems. Analyzing this infrastructure helps security teams detect, track, and disrupt malicious activity

Capabilities

The capability refers to the tools, malware, exploits, and tactics, techniques, and procedures (TTPs) used by the adversary to carry out the attack.

Threat Intelligence
Tools

Threat Intelligence is the analysis of data and information using tools and techniques to generate meaningful patterns on how to mitigate against potential risks associated with existing or emerging threats targeting organizations, industries, sectors or governments.

Open-Source Intelligence (OSINT)

1. UrlScan.io - Urlscan.io is a free service developed to assist in scanning and analyzing websites. It is used to automate the process of browsing and crawling through websites to record activities and interactions.
When a URL is submitted, the information recorded includes the domains and IP addresses contacted, resources requested from the domains, a snapshot of the web page, technologies utilized and other metadata about the website.

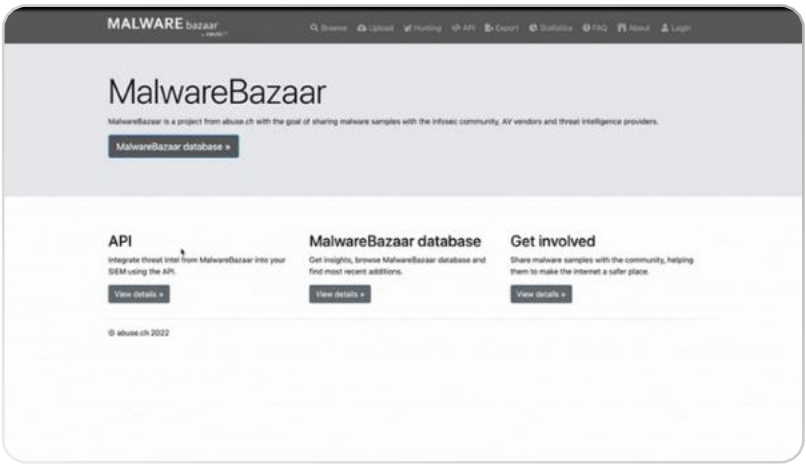
The site provides two views, the first one showing the most recent scans performed and the second one showing current live scans.

2. Abuse.ch - Abuse.ch is a research project hosted by the Institute for Cybersecurity and Engineering at the Bern University of Applied Sciences in Switzerland. It was developed to identify and track malware and botnets through several operational platforms developed under the project.

These platforms are:

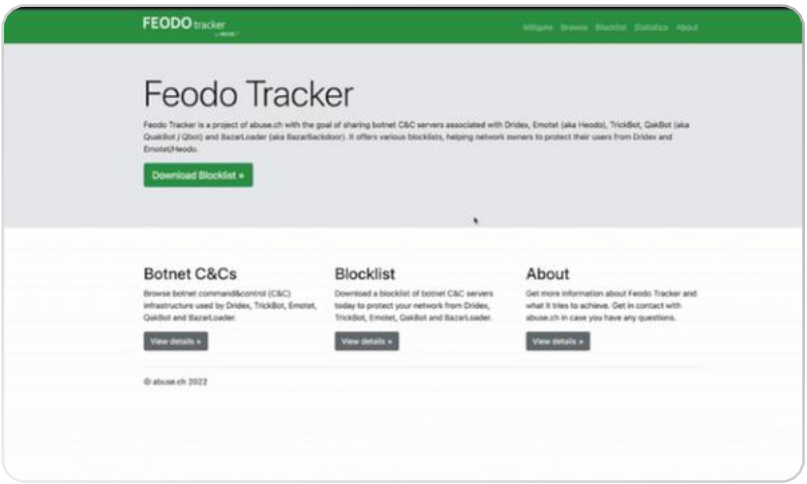
Malware Bazaar

A resource for sharing malware samples.



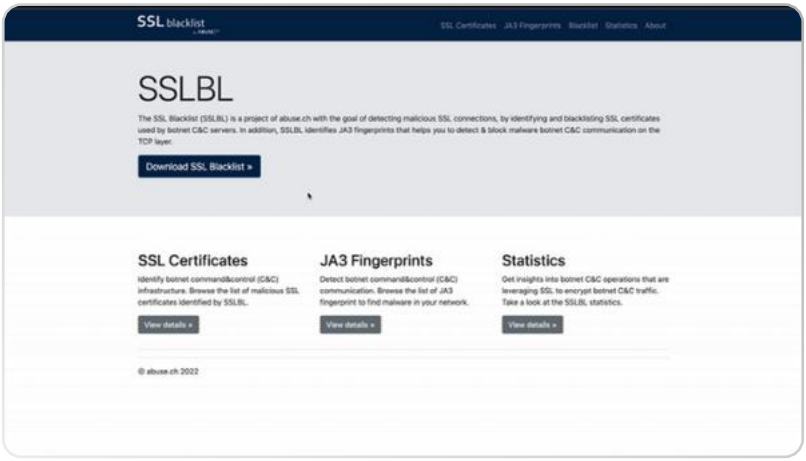
Feodo Tracker

A resource used to track botnet command and control (C2) infrastructure linked with Emotet, Dridex and TrickBot.



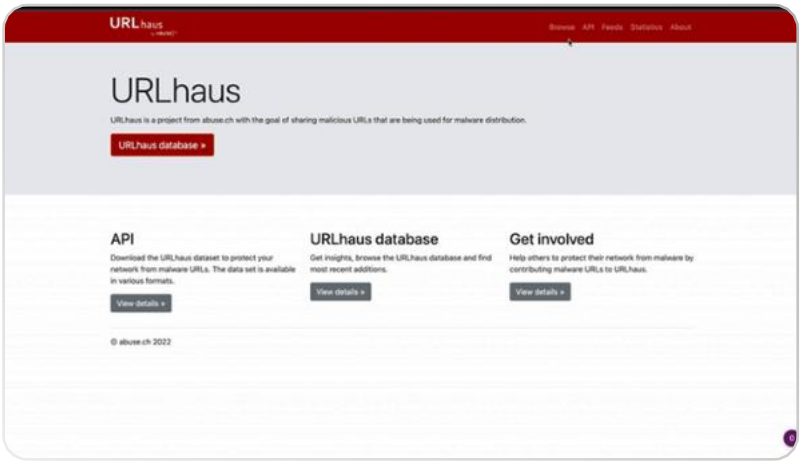
SSL Blacklist

A resource for collecting and providing a blocklist for malicious SSL certificates and JA3/JA3s fingerprints.



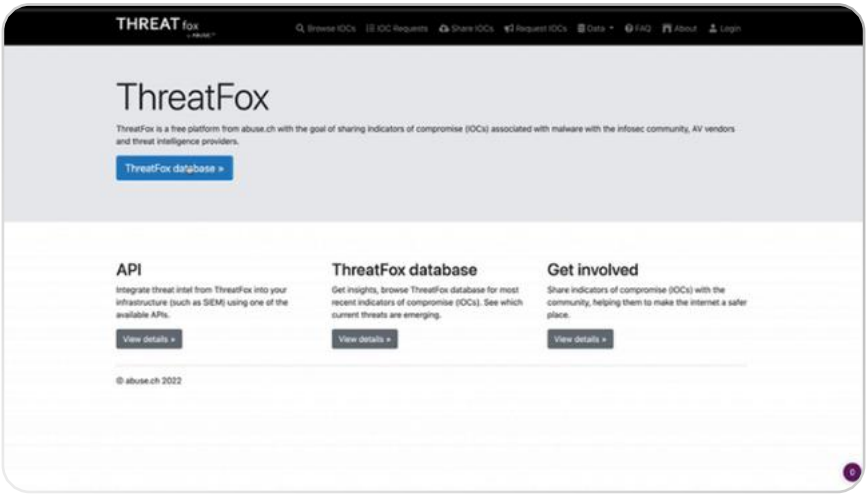
URL Haus

A resource for sharing malware distribution sites.



Threat Fox

A resource for sharing indicators of compromise (IOCs).



PhishTool

It's a tool designed to help you analyze suspicious emails and uncover the tricks that cybercriminals use to try and steal your information. Email phishing is one of the most common ways that cybercriminals try to trick you. They send emails that look like they're from a trusted source, like your bank or a social media platform, but they're actually fake.

Core features

Perform email analysis

PhishTool retrieves metadata from phishing emails and provides analysts with the relevant explanations and capabilities to follow the email's actions, attachments, and URLs to triage the situation.

Heuristic intelligence

OSINT is baked into the tool to provide analysts with the intelligence needed to stay ahead of persistent attacks and understand what TTPs were used to evade security controls and allow the adversary to social engineer a target.

Classification and reporting

Phishing email classifications are conducted to allow analysts to take action quickly. Additionally, reports can be generated to provide a forensic record that can be shared.

Threat Intelligence Platforms

Threat intelligence platforms (TIPs) are like having a whole team of cybersecurity experts working for you. They collect, analyze, and share threat intelligence data from a variety of sources, giving you a comprehensive view of the threat landscape.

ThreatConnect

This platform is like a command center for your threat intelligence operations. It helps you gather data from different sources, analyze it, and then share your findings with others.

Anomali

This platform is like a super-smart assistant that helps you automate threat intelligence analysis. It can sift through mountains of data and find the most important clues, so you can focus on taking action.

Integration of Threat Intelligence

Integrating threat intelligence into your security operations is like having a team of experts constantly monitoring the threat landscape, analysing data, and providing you with actionable insights. This allows you to detect and respond to threats faster, strengthen your defences, and ultimately, protect your organization from harm.

MISP (Malware Information Sharing Platform)

MISP (Malware Information Sharing Platform) is an open-source threat information platform that facilitates the collection, storage and distribution of threat intelligence and Indicators of Compromise (IOCs) related to malware, cyber attacks, financial fraud or any intelligence within a community of trusted members.

SIEM (Security Information and Event Management) Systems

A Security Information and Event Management (SIEM) system is like a central nervous system for your network. It collects and analyses security logs from all your devices, looking for signs of suspicious activity.

By integrating threat intelligence with your SIEM system, you can supercharge its detection capabilities. For example, your SIEM could automatically block traffic from an IP address that's been identified as malicious by a threat intelligence feed.

Spot the mistakes

From: support@rnicrosoft.co.uk
Sent: 16/05/2023 12:30
To: John Smith <John.Smith@company.com>
Subject: Urgent Action Needed!

Microsoft Account

Verify your account

We detected some unusual activity about a recent sign in for your Microsoft account. you might be signing in from a new location app or device.

please verify your account within 24 hours to avoid any disrupton in your service.

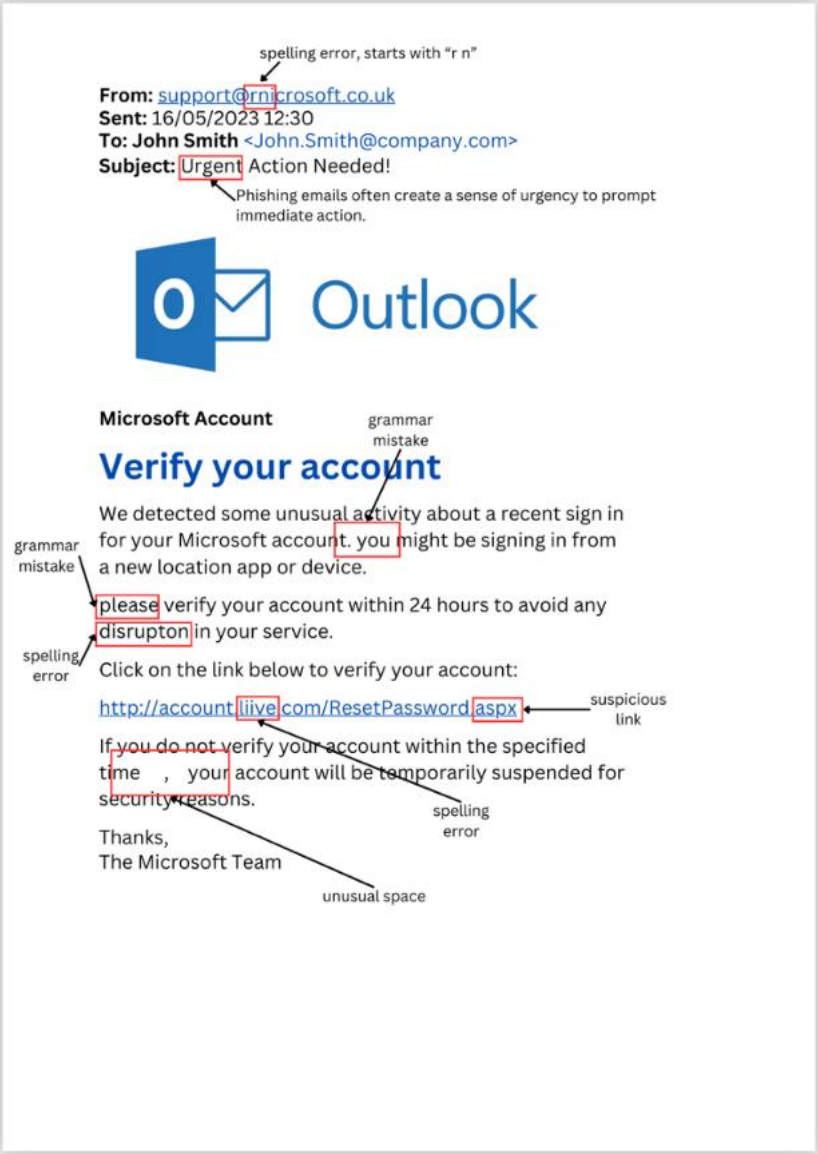
Click on the link below to verify your account:

http://account.liive.com/ResetPassword.aspx

If you do not verify your account within the specified time , your account will be temporarily suspended for security reasons.

Thanks,
The Microsoft Team

Answer


spelling error, starts with "r n"
From: support@rnicrosoft.co.uk
Sent: 16/05/2023 12:30
To: John Smith <John.Smith@company.com>
Subject: Urgent Action Needed!
Phishing emails often create a sense of urgency to prompt immediate action.
Outlook
Microsoft Account
grammar mistake
Verify your account
We detected some unusual activity about a recent sign in for your Microsoft account. you might be signing in from a new location app or device.
grammar mistake
please verify your account within 24 hours to avoid any disrupton in your service.
spelling error
Click on the link below to verify your account:
http://account.liive.com/ResetPassword.aspx
suspicious link
If you do not verify your account within the specified time , your account will be temporarily suspended for security reasons.
spelling error
Thanks,
The Microsoft Team
unusual space

Digital Forensics and Incident Response (DFIR)

This field covers the collection of forensic artifacts from digital devices such as computers, media devices, and smartphones to investigate an incident.
This field helps Security Professionals identify footprints left by an attacker when a security incident occurs, use them to determine the extent of compromise in an environment, and restore the environment to the state it was before the incident occurred.

Who performs DFIR?

Digital Forensics:

These professionals are experts in identifying forensic artifacts or evidence of human activity in digital devices.

Incident Response:

Incident responders are experts in cybersecurity and leverage forensic information to identify the activity of interest from a security perspective.

Digital Forensics
Methodologies

Artifacts

Artifacts are pieces of evidence that point to an activity performed on a system. When performing DFIR, artifacts are collected to support a hypothesis or claim about attacker activity

Evidence Preservation

When performing DFIR, we must maintain the integrity of the evidence we are collecting. For this reason, certain best practices are established in the industry.
We must note that any forensic analysis contaminates the evidence. Therefore, the evidence is first collected and write-protected. Then, a copy of the write-protected evidence is used for analysis.

Chain of custody

Another critical aspect of maintaining the integrity of evidence is the chain of custody. When the evidence is collected, it must be made sure that it is kept in secure custody. Any person not related to the investigation must not possess the evidence, or it will contaminate the chain of custody of the evidence.

Order of volatility

Digital evidence can disappear quickly! Some types of evidence, like data stored in a computer's memory (RAM), are volatile and can be lost if the device is turned off.

Other types, like data stored on a hard drive, are more persistent. Understanding the order of volatility is crucial for collecting evidence in the right order. We prioritize the most volatile data first, to ensure we don't miss any crucial clues.

Timeline creation

Once we have collected the artifacts and maintained their integrity, we need to present them understandably to fully use the information contained in them. A timeline of events needs to be created for efficient and accurate analysis. This timeline of events puts all the activities in chronological order. This activity is called timeline creation.

Activity - Evidence

Scenario

On the morning of July 10, 2024, TechSecure Inc.'s IT department discovered unusual activity in their main database server logs. Upon closer inspection, they found multiple failed login attempts followed by a successful login at 2:30 AM. Realizing the gravity of the situation, they immediately alerted the company's cybersecurity team.

The cybersecurity team, led by analyst Jane Smith, began their investigation. They isolated the compromised server to prevent further unauthorized access and created a forensic image of the hard drive for detailed analysis. Concurrently, IT Specialist Michael Johnson examined network traffic logs, which revealed a suspicious IP address making connections during the time of the breach.

On July 11, 2024, further investigation into employee records revealed that the IP address was linked to John Doe, an employee currently on vacation. Jane and Michael decided to examine John Doe's email inbox and discovered a phishing email sent to him on July 9, 2024, with a malicious link designed to steal his login credentials.

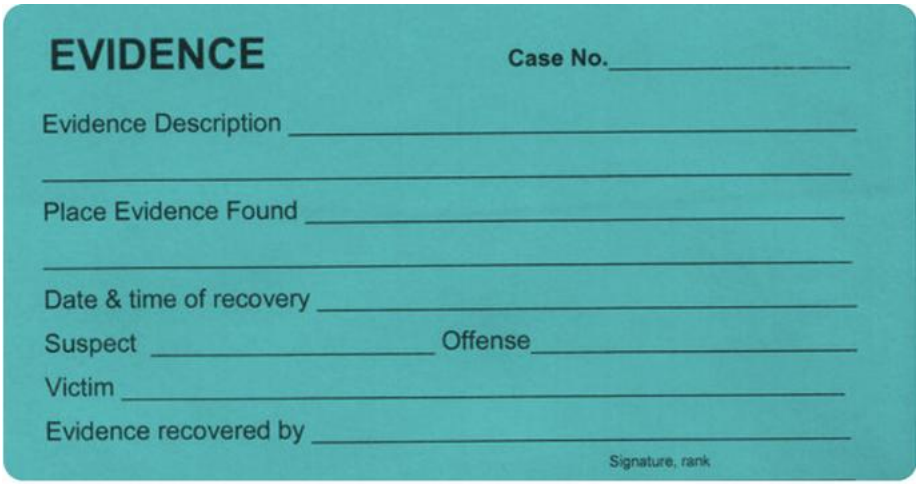
Using the forensic tools, Jane found traces of the phishing email leading to the successful login at 2:30 AM on July 10. The phishing email had tricked John into revealing his credentials, which were then used by the attacker to access the database.

By July 12, 2024, the cybersecurity team had gathered all evidence, including the phishing email, network logs, and forensic image, which were crucial in understanding the breach. They documented their findings in a report, identifying the use of stolen credentials due to a phishing attack as the cause.

TechSecure Inc. immediately took action to secure their systems, implemented multi-factor authentication, and began a company-wide training on phishing awareness. They also contacted law enforcement with the evidence to trace the attacker and prevent future incidents.

This detailed investigation not only helped identify the cause of the breach but also ensured that TechSecure Inc. could improve their security measures to protect against similar attacks in the future.

Evidence report


EVIDENCE

Case No._____

Evidence Description _____

_____

Place Evidence Found _____

_____

Date & time of recovery _____

Suspect _____ Offense_____

Victim _____

Evidence recovered by _____

Signature, rank

Incident Response Methodologies

Incident response (IR) is a structured approach to handling and managing the aftermath of a security breach or cyberattack. The goal is to handle the situation in a way that limits damage and reduces recovery time and costs.

Standardized Incident Response

Two well-known frameworks are:

• NIST SP 80061

This guide from the National Institute of Standards and Technology (NIST) outlines a four-step process for incident handling:

- **Preparation**
- **Detection and Analysis,**
- **Containment, Eradication, and Recovery**
- **Post-Incident Activity.**

• SANS PICERL

This acronym stands for

- **Preparation**
- **Identification**
- **Containment**
- **Eradication**
- **Recovery**
- **Lessons Learned**

It's a handy way to remember the key steps in incident response.

Best Practices in DFIR

DFIR professionals have a responsibility to conduct their investigations in a legal and ethical manner. This means:

• **Respecting privacy:** We need to be careful not to access or share personal information unnecessarily.

• **Maintaining confidentiality:** We need to keep sensitive information confidential, even after an investigation is complete.

• **Following the law:** We need to comply with all applicable laws and regulations, such as the Electronic Communications Privacy Act (ECPA).

Documentation and Reporting

Documentation is essential in DFIR. We need to keep detailed records of everything we do, from the initial detection of an incident to the final resolution. This documentation can be used to improve incident response processes, train new staff, and even serve as evidence in court.

Reports are also an important part of DFIR. We need to communicate our findings to stakeholders in a clear and concise way.

This could involve writing a technical report for IT staff, a summary report for executives, or even a press release for the public.

Introduction to

DFIR Tools

The security industry has built various exciting tools to help with the DFIR process. These tools help save valuable time and enhance the capabilities of security professionals.

Forensic Imaging Tools

Forensic imaging tools are the first responders of the DFIR world. They create bit-by-bit copies (forensic images) of digital media, preserving every single detail of the original evidence.

Windows Forensic Imaging Tools

FTK Imager

This popular tool from AccessData is a staple in many digital forensic labs. It's known for its user-friendly interface and ability to create forensic images of a variety of storage devices, including hard drives, USB drives, and memory cards.

KAPE

(Kroll Artifact Parser and Extractor)

Developed by the renowned Eric Zimmerman, KAPE automates the collection and parsing of forensic artifacts, saving you precious time and effort.

Forensic Analysis Tools

Forensic analysis tools are like our magnifying glass and fingerprint kit, helping us dig into the data and uncover hidden clues.

Windows Forensic Analysis Tools

Eric Zimmerman's Tools

Eric Zimmerman is a renowned cybersecurity expert who has developed a suite of powerful tools specifically for analyzing Windows systems. These tools help us dive deep into the Windows Registry, file systems, and other artifacts to uncover evidence of malicious activity.

Autopsy

This open-source platform is a one-stop shop for forensic analysis. It has a user-friendly interface and a wide range of features, making it a popular choice for both beginners and experienced investigators.

Incident Response Tools

Incident response tools are our weapons in the fight against cyber threats. They help us quickly detect, contain, and eradicate attacks, minimizing the damage and restoring normal operations.

- **Wireshark**

This network protocol analyzer is like a wiretap for your network. It captures and analyzes network traffic, allowing you to see what data is being sent and received.

- **Sysinternals Suite**

This collection of tools from Microsoft is like a toolbox full of specialized instruments for Windows systems. It includes tools like Process Explorer (for monitoring running processes), Process Monitor (for tracking file system and registry activity), and Autoruns (for identifying programs that start automatically). These tools can help you identify and investigate suspicious activity on a compromised system.

- **Redline (FireEye)**

This tool is like a first responder kit for your computer. It quickly gathers forensic data from a system, giving you a snapshot of what's happening and helping you identify potential threats.

Integration of DFIR Tools

The real power of DFIR comes from combining different tools and techniques. By integrating your DFIR tools with other security tools, like SIEMs (Security Information and Event Management) and SOAR (Security Orchestration, Automation, and Response) platforms, you can create a powerful defense system that is always on the lookout for threats.

Answers

Take the cyber quest p.07

1- Malware
2- firewall
3- ransomware
4- privacy
5- worms
6- cyberattack
7- phishing
8- encryption
9- patch
10- hacking

Domain Hierarchy Diagram p.31

Hack the Passwords p.93

IT TAKES A FRIEND
TO MAKE A FRIEND.
HEY YOU FIGURED
OUT MY PASSWORD!
YOU ARE RAD!

Decode p.100

authentication

Word Scramble p.40

PING
CHAT
RANGE
CLIENT
DOMAIN
PORT
STRING
FOLDER
METHOD
QUERY
UNIFORM
DISK

HTTP Status Code : page not found

Evidence Report p.138

Case No.:
0710-TSI-2024
Evidence Description:
Forensic image of compromised database server, phishing email, network traffic logs, authentication logs, and employee records.
Place Evidence Found: TechSecure Inc. – Database Server, Network Logs, and John Doe's Corporate Email Account.
Date & Time of Recovery: July 12, 2024
Suspect: Unknown Attacker
Offense: Unauthorized Access / Phishing / Credential Theft
Victim: TechSecure Inc. (John Doe's credentials compromised)
Evidence Recovered By:
Jane Smith (Lead Cybersecurity Analyst)
& Michael Johnson (IT Specialist)

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

For inquiries and communication
with the National Cybersecurity Academy regarding the camp, please contact us through the following channels:

Call Center
16555

Phone Numbers
00974 4046 6379
00974 4046 6623
00974 5104 5944

Email
academy@ncsa.gov.qa

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

المخيم الشبابي للأمن السيبراني 2026
CYBER SECURITY YOUTH CAMP 2026

academy.ncsa.gov.qa