

107 ساير

# اختبار الاختراق

م. سمر سعيد الهواري



# نبذة عن المقرر

التعرف على اختبار الاختراقات للشبكات والأنظمة  
والأدوات والأساليب المستخدمة



# الأهداف العامة والتفصيلية من المقرر

- تحديد مراحل الهجوم
- عمليتي الاستطلاع والتتبع
- حماية الأجهزة من البرمجيات الخبيثة
- الهندسة الاجتماعية

## مقدمة في القرصنة الاخلاقية

القرصنة الأخلاقية تسمى باللغة الإنجليزية Ethical Hacking والاسم الشائع لها باللغة العربية هو "الهاكينج الأخلاقي".  
تعبر القرصنة الأخلاقية عن عملية اختراق للأنظمة والبرامج والبيانات بهدف اختبار نظام الحماية بها واكتشاف الثغرات بنظام الأمان.

## من هم White Hats

يعبر هذا المصطلح عن خبراء القرصنة الأخلاقية، وهم من يختبرون نظام الحماية في المؤسسة من خلال تطبيق التطبيقات الأمنية بهدف تطوير نظام الحماية في المؤسسة، ويتم ذلك بموافقة مالك المؤسسة وفريق عمل تكنولوجيا المعلومات.

## من هم Black hat

هم من يخترقون الأنظمة بهدف السرقة او الاحتيال

## Ethical Hacking: المبادئ الأساسية للقرصنة الأخلاقية

### لبقاء قانونيًا

لابد من موافقة المؤسسة قبل اتخاذ الإجراءات حتى تتم العملية بشكل قانوني.

### تحديد نطاق معين للعمل

تحديد نطاق الاختبار بشكل واضح حتى يظل العمل ضمن حدود المؤسسة.

### الإبلاغ عن الثغرات الأمنية

إخطار المؤسسة بالثغرات الأمنية ونقط الضعف وتقديم حلول لتقويتها أو حل المشكلات.

### احترام حساسية البيانات

يجب الموافقة على عدم كشف البيانات أو المعلومات بالإضافة للشروط والأحكام التي تفرضها المؤسسة لضمان الحماية.

## أوجه الاختلاف بين الهاكر الأخلاقي والهاكر الخبيث

### الهاكر الأخلاقي Ethical Hacker

يستخدم معرفته وخبرته في حماية وتطوير نظام الأمان الشركة أو المؤسسة.  
يقدم خدمة اختبار وفحص الثغرات الأمنية.  
يبلغ عن الثغرات الأمنية ونقاط الضعف في نظام الحماية مع تقديم حلول للقضاء على هذه الثغرات.  
يقوم بالاختبار أكثر من مرة ليتم التأكد من قوة نظام الحماية.

### الهاكر الخبيث Malicious Hacker

هدفه هو ايجاد طريقة غير مصرح بها لاختراق الأنظمة والشبكات والوصول إلى البيانات والمعلومات.  
يستخدم البيانات والمعلومات لكسب المال، أو للتسبب في الخسارة المادية، أو تدمير السمعة، ومنهم من يفعل ذلك بهدف التسلية فقط!  
لا يقدموا النصيحة للقضاء على الثغرات الأمنية ولكن على العكس يقوموا باستغلالها لتدمير الموقف الأمني للمنظمة أو المؤسسة.

## الهكر الأخلاقي والأمن السيبراني

الأمن السيبراني: يضع استراتيجيات الحماية والدفاع ضد الهجوم.

الهكر الأخلاقي: يستخدم طرق لاختراق هذا النظام واختباره واكتشاف الثغرات الأمنية به.

### مثال:

إذا قامت شركة بإنشاء تطبيق لها يحتوي على بيانات ومعلومات العملاء، فبالطبع يمكن للقرصنة الخبيثة اختراقه والحصول على هذه البيانات.

لذلك يعمل الأمن السيبراني على وضع نظام حماية لهذه البيانات بالطرق المناسبة.

بينما الهكر الأخلاقي يحاول اختراق نظام الحماية بوجود موافقة مسبقة من مالك الشركة المنتجة تطبيق لكي يحدد الثغرات الأمنية ويضع حلول لها.

# تحميل برنامج Kali Linux

- **What is Kali Linux?** <https://www.kali.org/docs/introduction/what-is-kali-linux/>
- **Installing Kali Linux (Hard Disk Install)**  
<https://www.kali.org/docs/installation/kali-linux-hard-disk-install/>
- **Installing Kali inside VMware (Guest VM)**  
<https://www.kali.org/docs/virtualization/install-vmware-workstation-player-kali-guest-vm/>

# مراجعته اهم أوامر Linux على موقع try hack me

Try Hack Me

Learn Compete For Education For Business Pricing

Join For FREE

## Anyone can learn cyber security with TryHackMe

Hands-on cyber security training through real-world scenarios

The screenshot shows the TryHackMe website interface. At the top left is the TryHackMe logo with the text '10 10 1110 0101 01 01 010'. The navigation menu includes 'Dashboard', 'Learn', 'Compete', and 'Other'. On the right, there are search, notification, and 'Go Premium' buttons, along with a user profile icon. The main banner features the Linux penguin mascot and the title 'Linux Fundamentals Part 1'. Below the title, it says 'Embark on the journey of learning the fundamentals of Linux. Learn to run some of the first essential commands on an interactive terminal.' There are also buttons for 'Awards', 'Help', settings, and a bookmark icon. A thumbs up icon and the number '8824' are visible on the left side of the banner.

2023

النهاية

مراجعة سريعة  
القرصنة الاخلاقية



# سؤال و إجابة

عملية اختراق للأنظمة والبرامج والبيانات بهدف اختبار نظام الحماية بها واكتشاف الثغرات بنظام الأمان.

A. الهاكر الخبيث

B. الهاكر الأخلاقي

C. الهاكر الحكومي

يضع استراتيجيات الحماية والدفاع ضد الهجوم.

A. الهاكر الأخلاقي

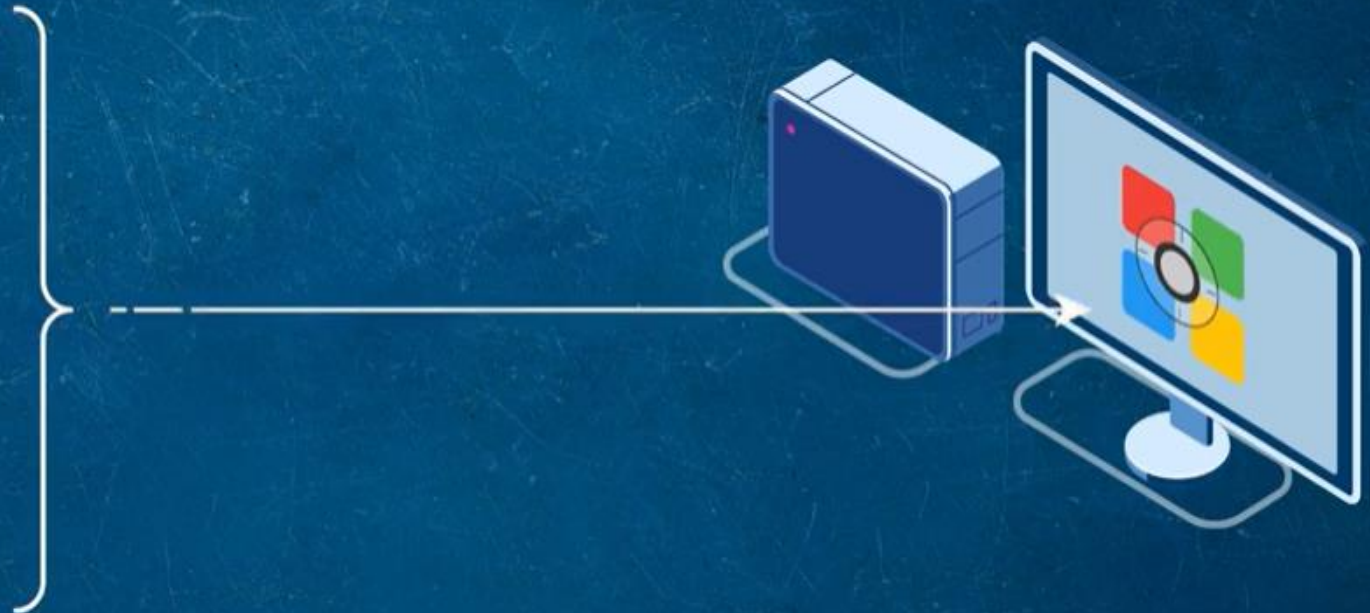
B. الامن السيبراني

C. التشفير

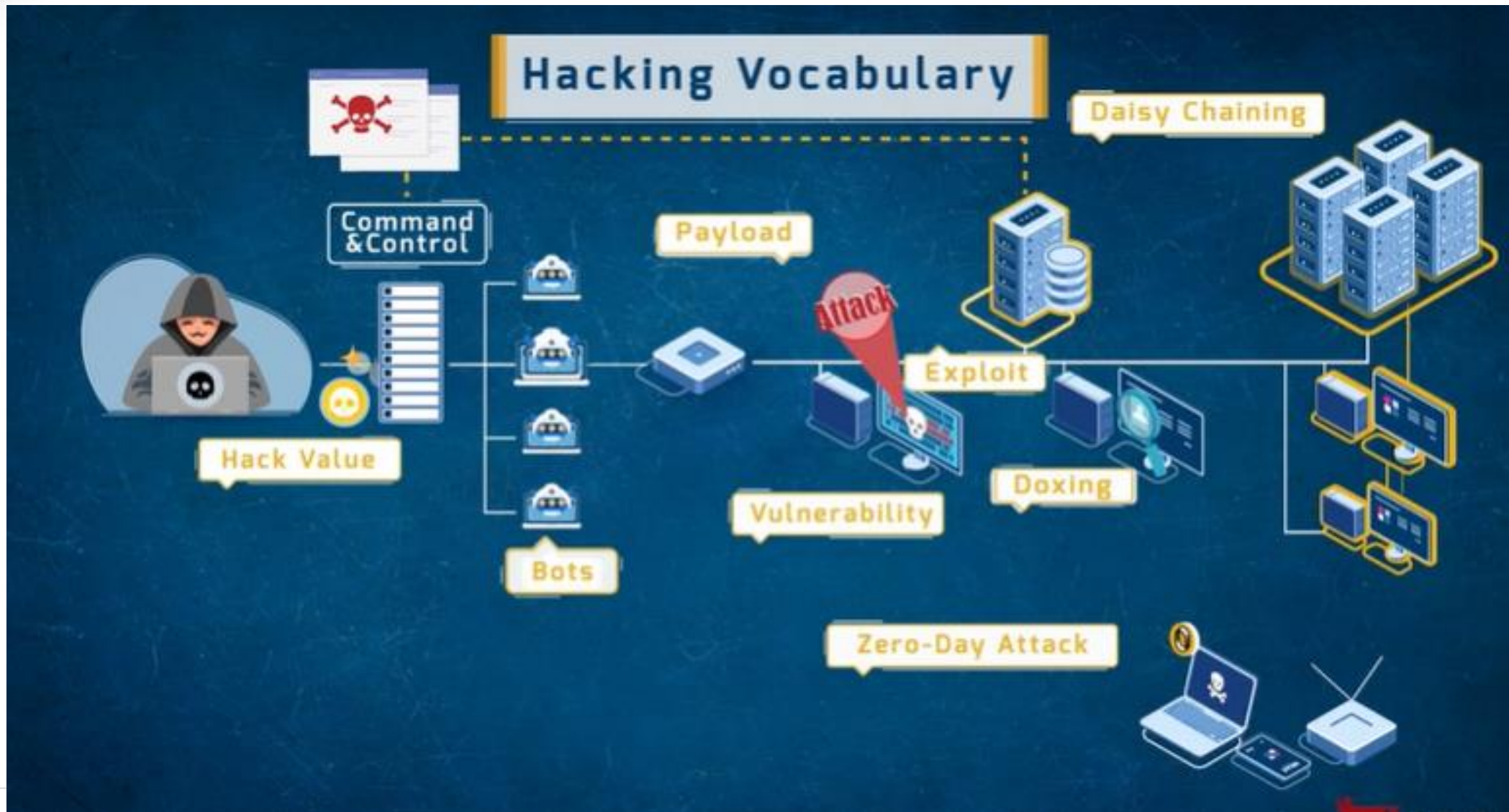


شكرا

## Hacking VS. Ethical Hacking



# مصطلحات في الاختراق



# عناصر امن المعلومات

## Elements of Information Security

السرية

النزاهة

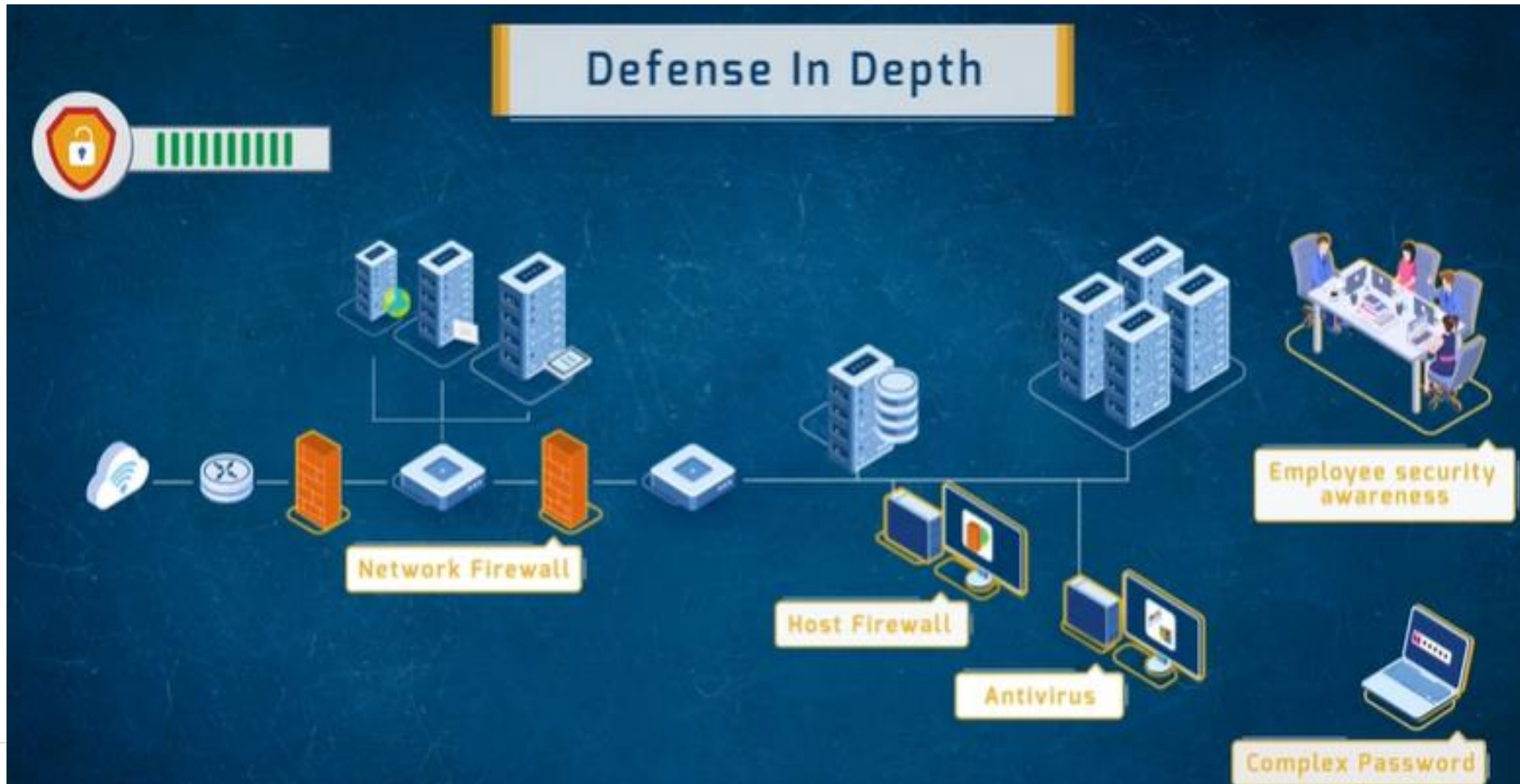
Confidentiality

Integrity

الآتاحة

Availability

# الدفاع في العمق





## Hacking phases مراحل الاختراق



1

Reconnaissance

الاستطلاع

تجميع معلومات

Gather information about a target

Passive Reconnaissance

Active Reconnaissance

## 2

## Scanning

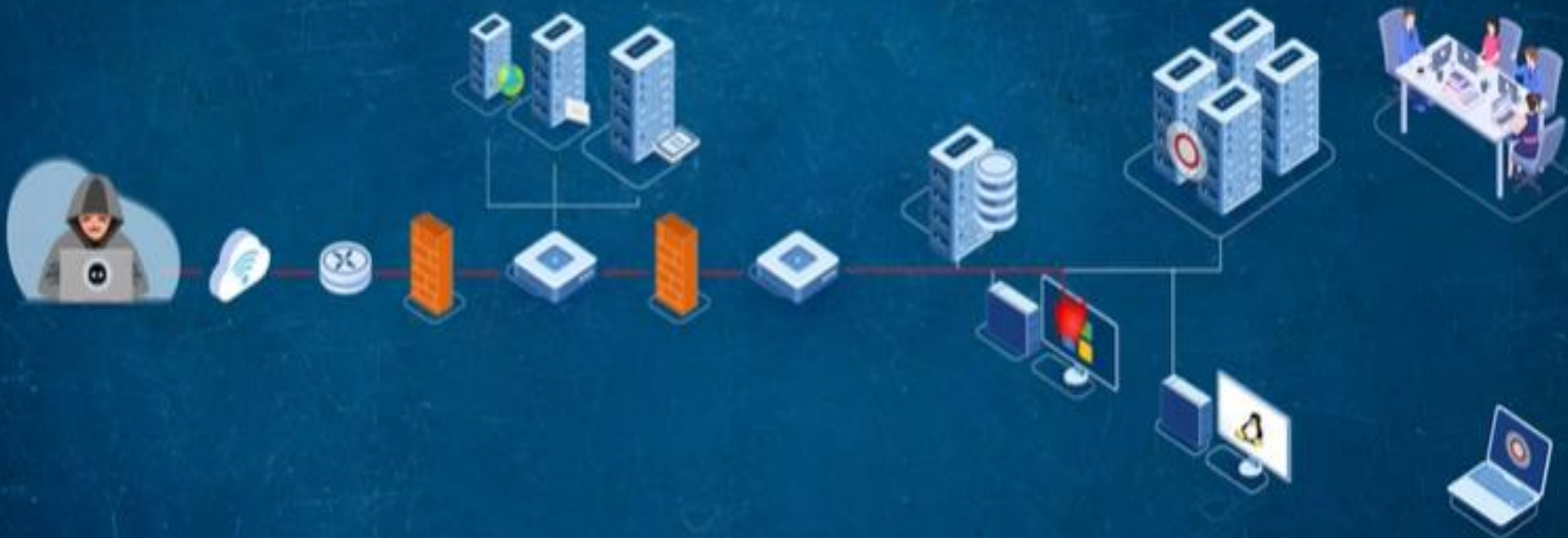
مسح

- 1- الأجهزة
  - 2- ports
  - 3- vuln.
- الثغرات



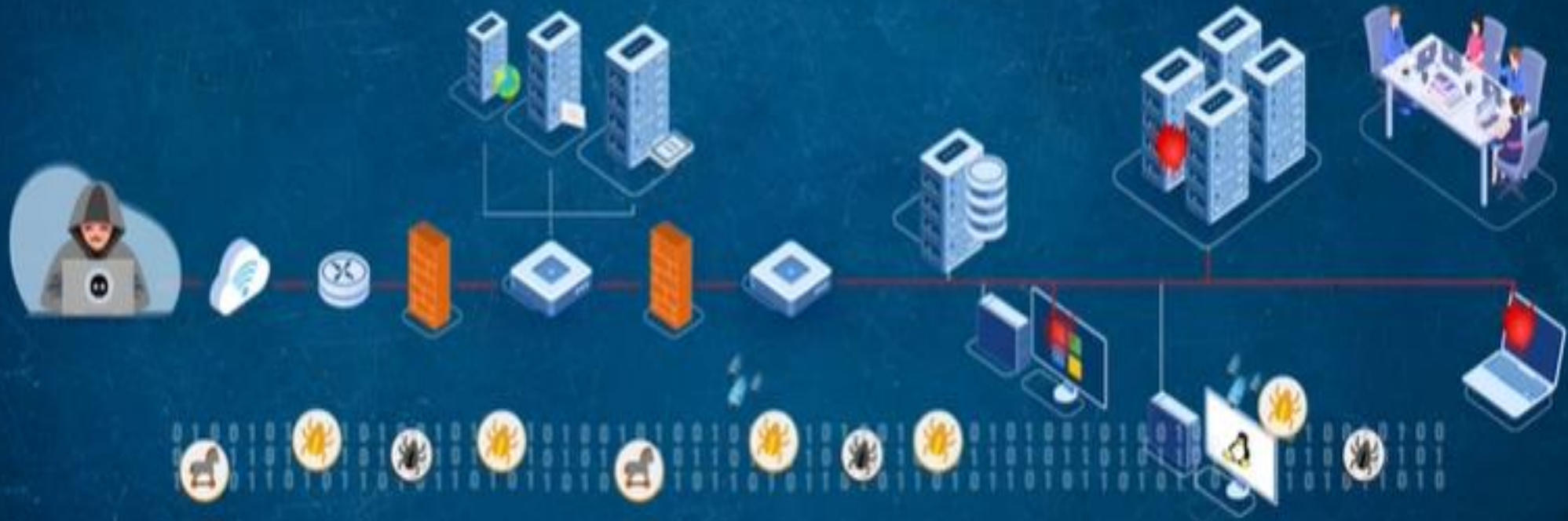
### 3 Gaining Access

التنفيذ



## 4 Maintaining Access

Retain ownership of the system



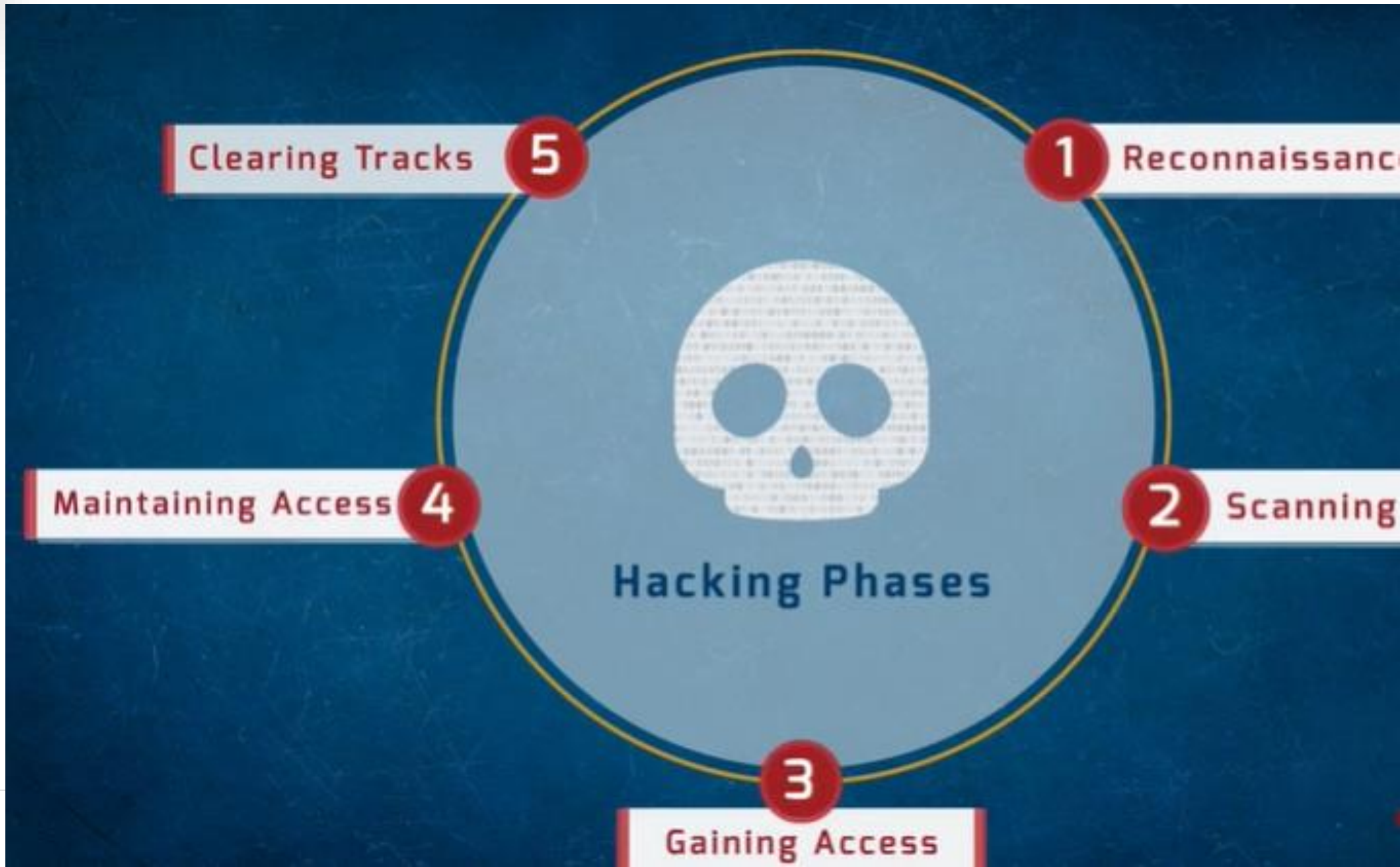
# 5

## Clearing Tracks

## تنظيف الاثار

- Hide malicious acts
- Avoid suspicion
- Unnoticed continuing access







## الاستطلاع Recon

- فائدة الاستطلاع
- اهداف الاستطلاع
- طرق الاستطلاع



## 1 Reconnaissance

- Know security Posture

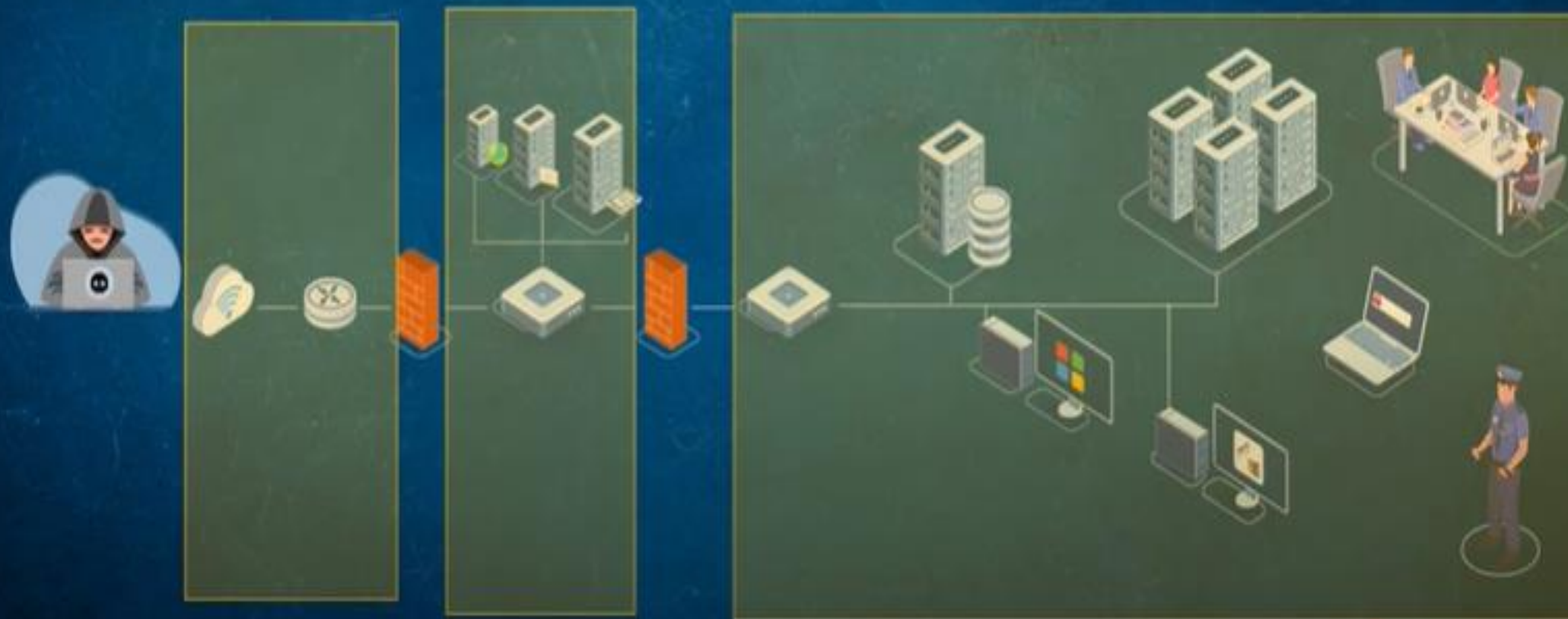
تقدير الوضع الأمني



# 1 Reconnaissance

- Know security Posture
- Reduce focus Area

تقليل مساحة التركيز



# 1 Reconnaissance

- Know security Posture
- Reduce focus Area
- **Identify vulnerabilities**

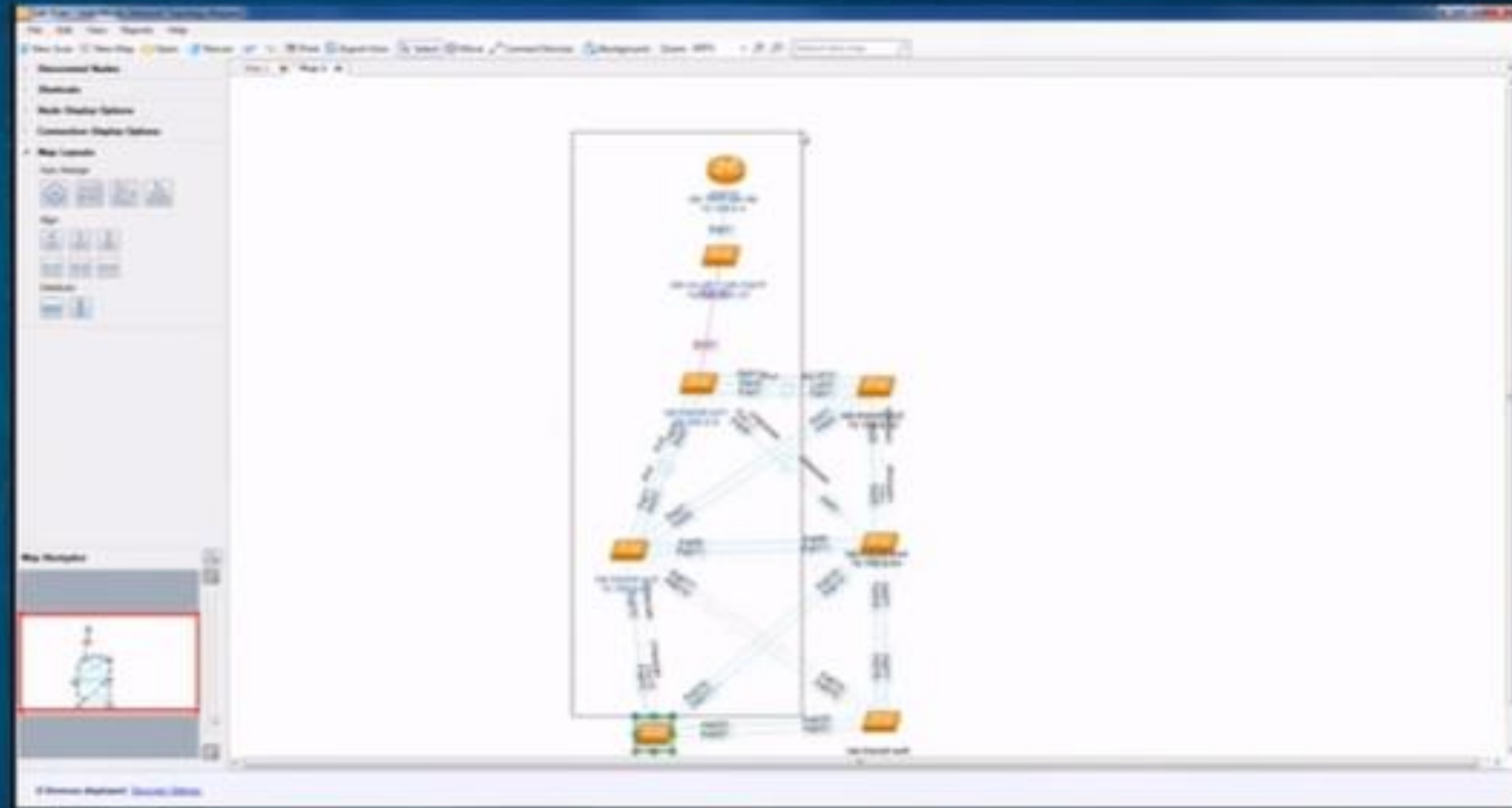
تعريف الثغرات



# 1 Reconnaissance

- Know security Posture
- Reduce focus Area
- Identify vulnerabilities
- Draw network Map

رسم الشبكة





# أدوات محرك البحث



# 1- HackThisSite

The image shows a Google search for 'hackthissite'. The search bar at the top contains the text 'hackthissite'. Below the search bar, there are tabs for 'All', 'Videos', 'Images', 'Books', 'News', 'Maps', 'Settings', and 'Tools'. The search results show 'About 289,000 results (0.32 seconds)'. The first result is 'Hack This Site!' with the URL 'https://www.hackthissite.org/'. Below this, there are several sections: 'User/login', 'HTS', 'Register', 'Lectures', 'About the Project', and 'Hall of Fame'. To the right of these sections is a featured snippet for 'HackThisSite' with a red circle around the title. The snippet includes a description of the site, its founders, origin, and location. Below the featured snippet are three video thumbnails, each with a play button and a duration. The first video is 'Hack This Site, Basic 1, Tutorial', the second is 'Hack This Site, Basic 5, Tutorial', and the third is 'Hack This Site, Basic 3, Tutorial'. All videos are by 'TRUE MILLER' and were uploaded on 'Sep 20, 2017'.



<https://livethreatmap.radware.com/>

hackthissite

All Images Videos News My saves

72,800 Results Date Language Region

### Hack This Site!

<https://www.hackthissite.org>  
HackThisSite! is a legal and safe network security resource where users test their hacking skills on various challenges and learn about hacking and network security.

### HackThisSite - Wikipedia

<https://en.wikipedia.org/wiki/HackThisSite>  
Location: United States, International - Origin: Chicago, Illinois  
Purpose: Hacking/media Formation: 2003

Overview IRC and forums Mission challenges Root This Site Controversy

HackThisSite.org, commonly referred to as HTS!, is an online hacking and security website founded by Jeremy Hammond, with the site being maintained by members of the community after his departure. It aims to provide users with a way to learn and practice basic and advanced "hacking" skills through a series of challenges in a safe and legal environment. The organization has a user base of over 1,500,000, though the actual number of active members is believed to be much lower. The most users online

See more on en.wikipedia.org - Text under CC-BY-SA license

### Hack This Site (@hackthissite) | Twitter

<https://twitter.com/hackthissite>  
The latest Tweets from Hack This Site (@hackthissite): HackThisSite is a free, safe, legal training ground for new and experienced hackers alike!

### Videos of hackthissite

bing.com/videos



Hack This Site - Basic 1 Tutorial "SPOILER"  
YouTube 21040000 152K



Hack This Site Basic Missions 1-5  
YouTube 08000012 85K



Hack This Site, Basic 1 Tutorial @HackThisSite.org  
YouTube 20080017 41K

See more videos of hackthissite

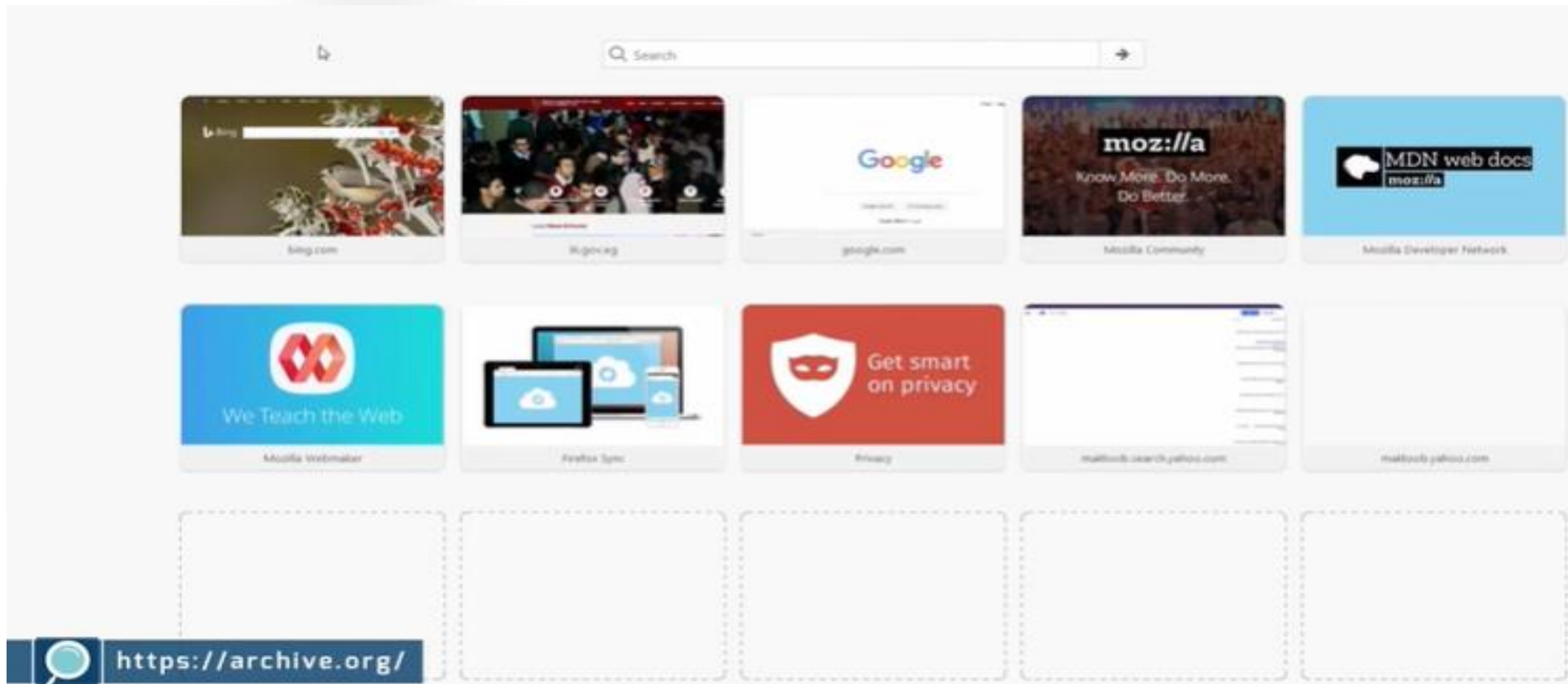
### HackThisSite Mirror | HackThisZine

### Related searches

- Learn to hack for beginners
- hackthissite basic 7
- hackthissite basic mission 8
- hackthissite realistic 3
- hack this site solutions
- hackthissite discord
- sites like hackthissite
- hackthissite basic 3



## 2- Archive.org



# 3- netcraft site report

The image shows a Google search interface. The search bar contains the text "netcraft site report". Below the search bar, there are tabs for "All", "Images", "Videos", "News", "Maps", "More", "Settings", and "Tools". The search results are displayed below, starting with "About 150,000 results (0.37 seconds)". The first result is "Netcraft Site Report - Netcraft Toolbar" with the URL "https://toolbar.netcraft.com/site\_report". The second result is "Netcraft | Internet Research, Anti-Phishing and PCI Security Services" with the URL "https://www.netcraft.com". The third result is "Netcraft | Monitoring Services" with the URL "https://www.netcraft.com/monitoring-services/". The fourth result is "Netcraft - Search Web by Domain" with the URL "https://searchdms.netcraft.com/". The fifth result is "Netcraft Extension - Phishing Protection and Site Reports" with the URL "https://toolbar.netcraft.com/". The sixth result is "Netcraft | Hosting Provider Index" with the URL "https://www.netcraft.com/hosting-provider-index/". At the bottom of the page, there is a dark blue bar with a magnifying glass icon and the URL "https://toolbar.netcraft.com/site\_report".

Google

netcraft site report

All Images Videos News Maps More Settings Tools

About 150,000 results (0.37 seconds)

**Netcraft Site Report - Netcraft Toolbar**  
[https://toolbar.netcraft.com/site\\_report](https://toolbar.netcraft.com/site_report)  
Site title: Netcraft | Internet Research, Anti-Phishing and PCI Security ... Reporting and Conformance) is a mechanism for domain owners to indicate how their ...


**Netcraft | Internet Research, Anti-Phishing and PCI Security Services**  
<https://www.netcraft.com/>  
Netcraft provide internet security services including anti-fraud and ... Proactively defend your brand against phishing sites attempting to steal your users' details. ... If you receive a phishing mail, please report the URL of the attacker's site.  
Netcraft Toolbar - Monitoring Services - Hosting Provider Analysis - About Netcraft

**Netcraft | Monitoring Services**  
<https://www.netcraft.com/monitoring-services/>  
Netcraft has developed several services whereby companies can have access to detailed information on the performance of their prospects' sites or their own ...

**Netcraft - Search Web by Domain**  
<https://searchdms.netcraft.com/>  
Anti-Phishing Toolbar - Phishing Site Feed - Hosting Phishing Alerts - Fraud Detection - Phishing Site Countermeasures - Audited by Netcraft - Open Redirect ...

**Netcraft Extension - Phishing Protection and Site Reports**  
<https://toolbar.netcraft.com/>  
The Netcraft Extension in Google Chrome™ (Firefox version similar) ... Site Reports: Link to a detailed report about the site, helping you to make informed ...

**Netcraft | Hosting Provider Index**  
<https://www.netcraft.com/hosting-provider-index/>

 [https://toolbar.netcraft.com/site\\_report](https://toolbar.netcraft.com/site_report)



## 4- البحث عن اشخاص

pipl

Name, Email, Username or Phone

Location (optional)



# Search Over 3,249,152,266 People

With the world's largest people search engine, Pipl is the place to find the person behind the email address, social username or phone number.



<https://pipl.com/>

Business Solutions



## مصادر أخرى

- Anywho
- whitepages



2023

النهاية

مراجعة سريعة



# سؤال و إجابة

ثاني مرحله من مراحل عملية الاختراق.

A. الاستطلاع

B. التنفيذ

C. المسح

مميزات الاختراق الأخلاقي.

A. سرقة المعلومات

B. انتحال الشخصيات

C. حماية المؤسسات



شكرا

## Google operators

The screenshot shows a Google search interface. The search bar contains the query: `"physical security" site:sans.org filetype:pdf`. Below the search bar, a list of suggested search terms is displayed:

- physical security pdf
- levels of physical security
- physical security standards
- physical security manual pdf
- corporate physical security strategy
- physical security handbook pdf
- physical security threats and vulnerabilities
- advantages of physical security

At the bottom of the suggestions, there is a link that says "Report inappropriate predictions". Below the suggestions, there is a section titled "People also ask" with three questions:

- What does physical security mean?
- What are the levels of physical security?
- What are the primary threats to physical security?

Google Operators: **intitle:**

Google

intitle:"physical security"

All Images News Videos Books More Settings Tools

About 111,000 results (0.33 seconds)

**Physical security** is the protection of personnel, hardware, software, networks and data from physical actions and events that could cause serious loss or damage to an enterprise, agency or institution. This includes protection from fire, flood, natural disasters, burglary, theft, vandalism and terrorism. Sep 21, 2016



www.getkisi.com

What is physical security? - Definition from WhatIs.com - SearchSecurity  
<https://searchsecurity.techtarget.com/definition/physical-security>

About this result Feedback

Google

inurl:login site:www.microsoft.com



All

Images

Videos

Maps

News

More

Settings

Tools

About 201,000,000 results (0.29 seconds)

## Login

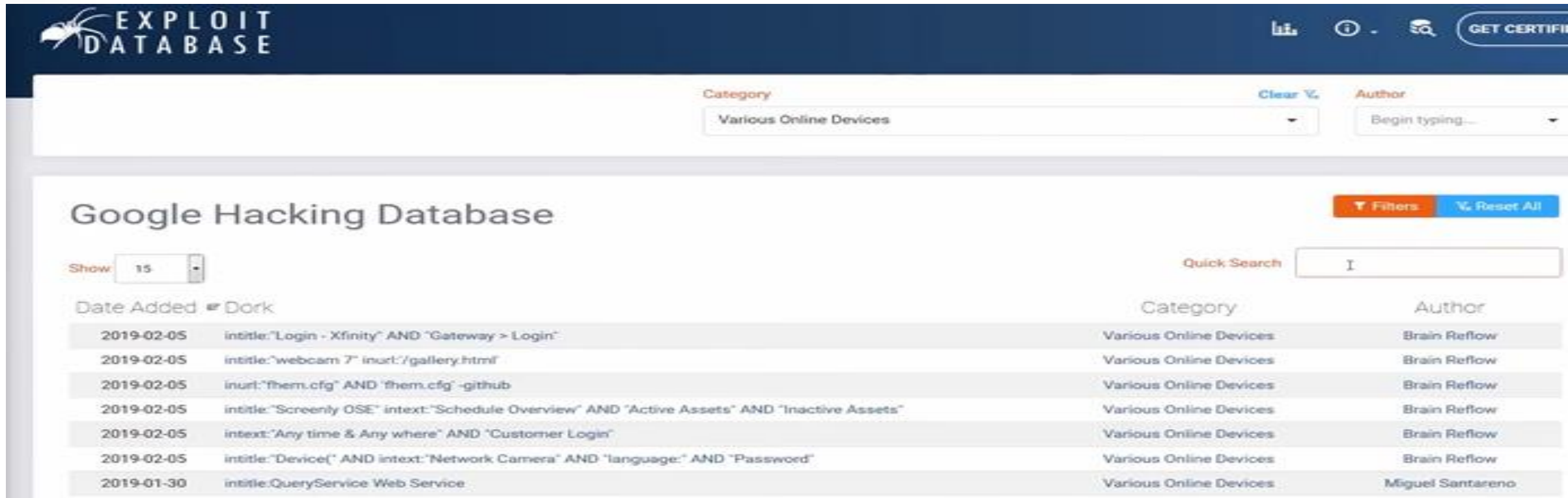
<https://account.genndi.com/login> ▼

Don't worry, we can send it again! An email with a password reset link has just been sent to you! Email address. Send my password 3. Copyright © Genndi 2019.

## Portal Login - PerfectMind

<https://login.perfectmind.com/socialsite/memberregistration/membersignin> ▼

CRM Perfectmind is a suite of on-demand CRM and highly cost effective small Business Software applications packaged with a comprehensive platform that ...



**EXPLOIT DATABASE**

Category: Various Online Devices Clear Author: Begin typing...

## Google Hacking Database

Show: 15 Quick Search: I Filters Reset All

Date Added	Dork	Category	Author
2019-02-05	intitle:"Login - Xfinity" AND "Gateway > Login"	Various Online Devices	Brain Reflow
2019-02-05	intitle:"webcam 7" inurl:./gallery.html	Various Online Devices	Brain Reflow
2019-02-05	inurl:"them.cfg" AND "them.cfg" -github	Various Online Devices	Brain Reflow
2019-02-05	intitle:"Screenly OSE" intext:"Schedule Overview" AND "Active Assets" AND "Inactive Assets"	Various Online Devices	Brain Reflow
2019-02-05	intext:"Any time & Any where" AND "Customer Login"	Various Online Devices	Brain Reflow
2019-02-05	intitle:"Device(" AND intext:"Network Camera" AND "language:" AND "Password"	Various Online Devices	Brain Reflow
2019-01-30	intitle:QueryService Web Service	Various Online Devices	Miguel Santareno

intitle: webcam 7 inurl:8080 -intext:8080

الأدوات

المزيد : صور الكتب التسوق فيديو الكل

حوالي ١٠٦ نتيجة (٠,٢١ ثانية)

webcam 7

ترجم هذه الصفحة · http://109.206.96.249

webcam 7

Source 6. JavaScript, Motion JPEG [Firefox], Flash JPEG Stream, Flash FLV Stream. Live View. Live Stream. Pan, Tilt & Zoom. powered by webcam 7 v1.5.3.0. xhtml ...

77.173.146

ترجم هذه الصفحة · http://77.173.146.165

webcam 7

webcam 7. webcams and ip cameras server for windows. HomeMulti ...iewSmartphoneGalleryAdministration. Not logged in. Source 1, Source 2, Source 3,

95.255.183

ترجم هذه الصفحة · http://95.255.183.164

webcam 7

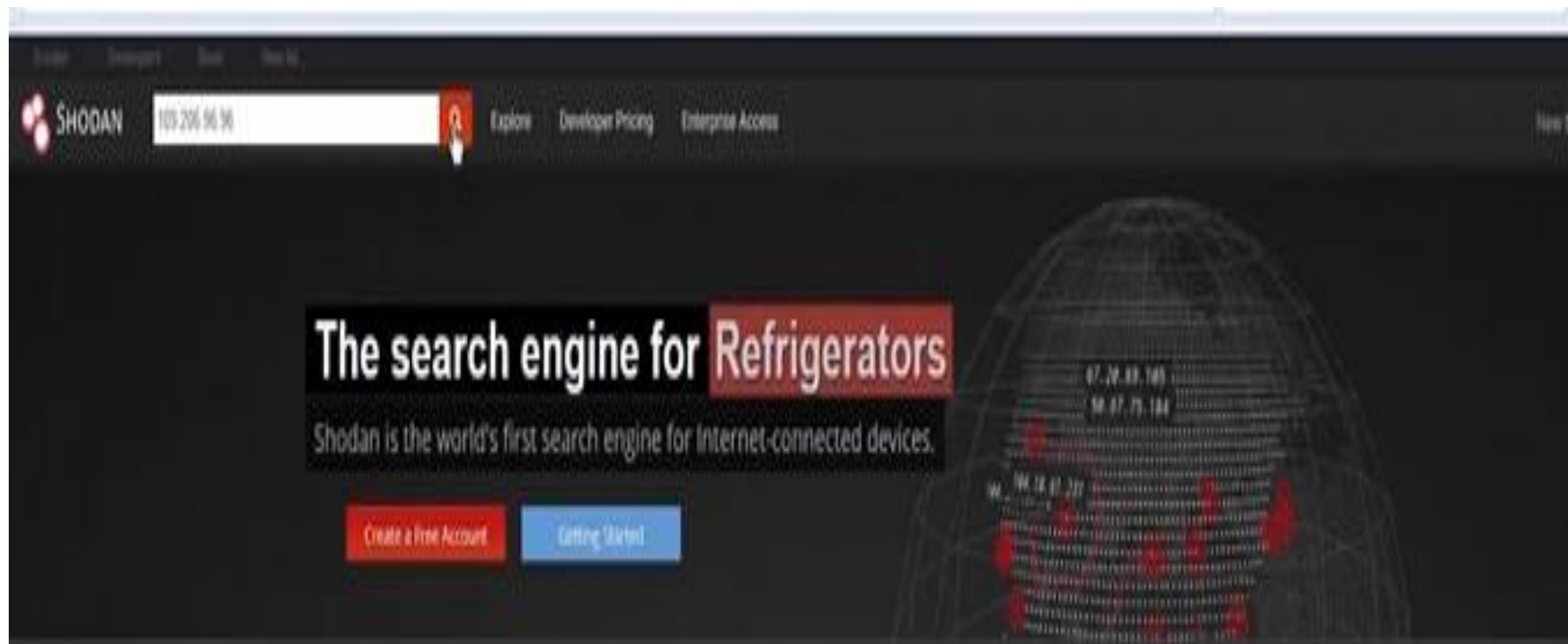
webcam 7. webcams and ip cameras server for windows. HomeMulti viewSmartphoneGalleryAdministration. Not logged in. Source 1, Source 2.

99.114.240

ترجم هذه الصفحة · http://99.114.240.169



Online  
devices  
الأجهزة المتصلة  
بالنت



### Explore the Internet of Things

Use Shodan to discover which of your devices are connected to the internet, where they are located and who is using them.



### See the Big Picture

Websites are just one part of the internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!



<https://www.shodan.io/>





## Website Reconnaissance Tools أدوات استطلاع مواقع الويب



## تحميل اداة



<http://www.webextractor.com/>



## تحميل اداة



WinHTTrack Website Copier - [sm.whtt]

e Preferences Mirror Log Window Help

- (C:) Local Disk<C:>
  - hadoop-3.2.4
  - Intel
  - Java
  - msys64
  - PerfLogs
  - Program Files
  - Program Files (x86)
  - tmp
  - Users
  - Windows
  - xampp
  - Project.log
- (D:) Local Disk<D:>
- (F:) DVD RW Drive<F:>

- Mirroring Mode -

Enter address(es) in URL box

Action:

Download web site(s)

Web Addresses: (URL)

Add URL...

www.certfiedhacker.com

URL list (.txt):

Preferences and mirror options:

Set options...

< Back

Next >

Cancel

Help



## Email Tracking Tools أدوات تتبع البريد الإلكتروني



1- فتح موقع

2- تسجيل حساب جديد

3- تطبيق عمليه التتبع

Re@dNotify

track your email

Welcome to ReadNotify.com !

ReadNotify lets you know when email you've sent gets read

Was your email forwarded?  
Find out if your reader sent your email to someone else

Start here! Optional Plugin PDF Tracking

Member Sign-in

email:

password:

Sign-in

Sign up now - Free!

Your existing email address:

GO!

home  
https://www.readnotify.com/readnotify/

about Re@dNotify business solutions member utilities

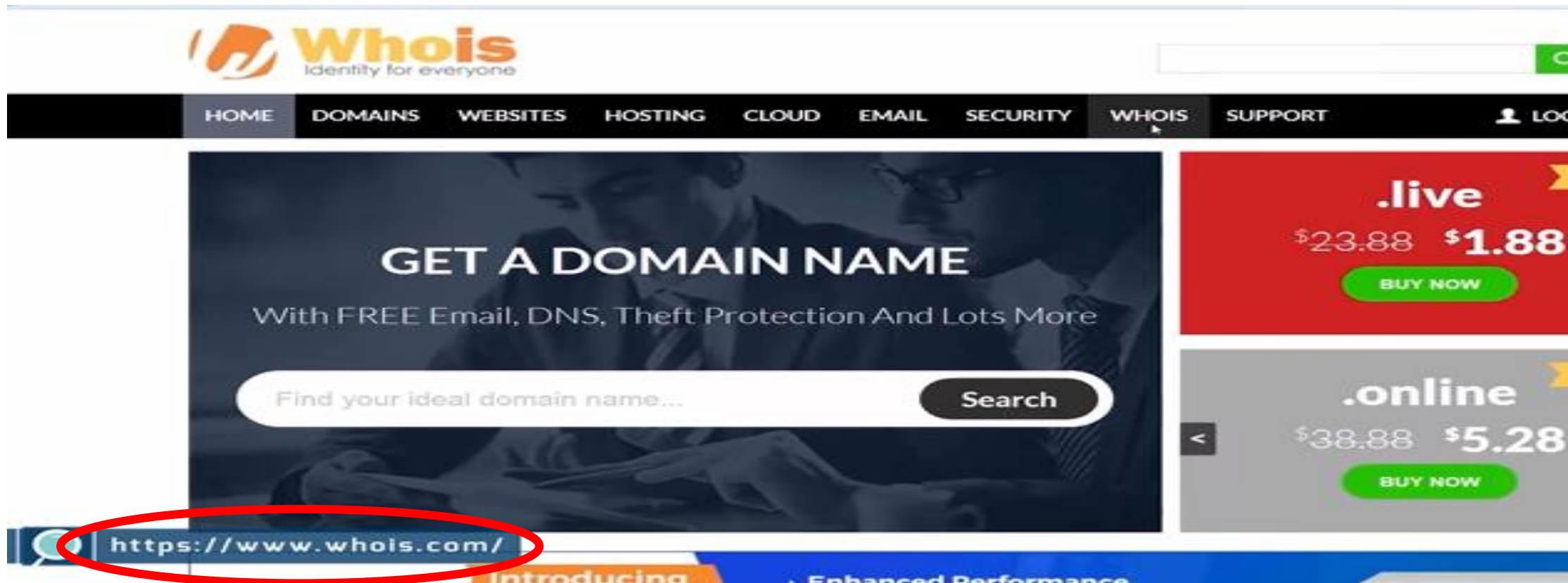




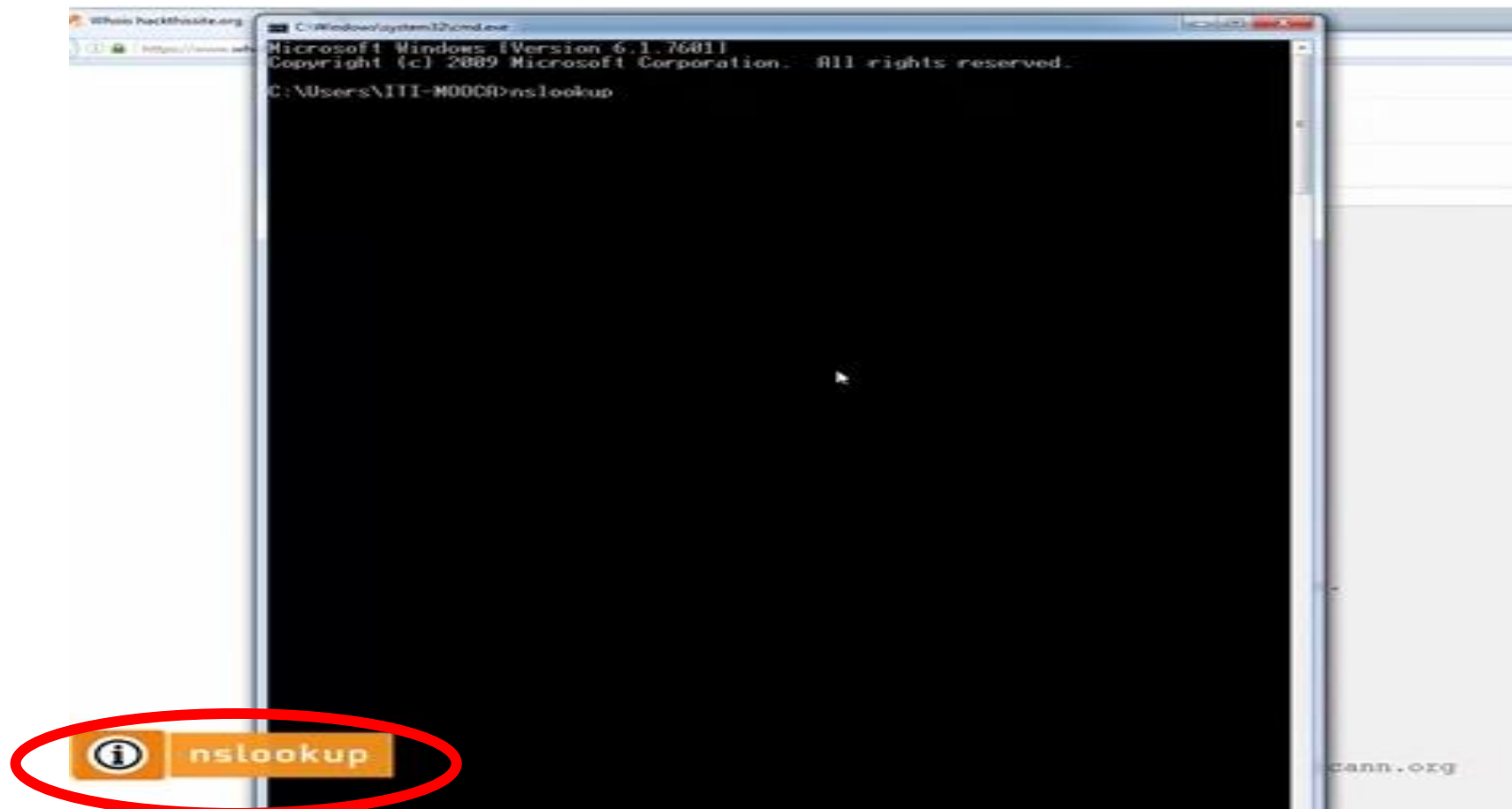
**Domain reconnaissance tools**  
أدوات استطلاع المدى



## دخول موقع



## استخدام اداة



```

C:\Windows\system32\cmd.exe - nslookup
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\ITI-MOCCA>nslookup hackthissite.org
Server: google-public-dns-a.google.com
Address: 8.8.8.8

Non-authoritative answer:
Name: hackthissite.org
Addresses: 2001:41d0:8:ccd8:137:74:187:102
           2001:41d0:8:ccd8:137:74:187:103
           2001:41d0:8:ccd8:137:74:187:104
           2001:41d0:8:ccd8:137:74:187:100
           2001:41d0:8:ccd8:137:74:187:101
           137.74.187.103
           137.74.187.104
           137.74.187.101
           137.74.187.102
           137.74.187.100

C:\Users\ITI-MOCCA>nslookup
Default Server: google-public-dns-a.google.com
Address: 8.8.8.8

> set type=NS
> hackthissite.org
Server: google-public-dns-a.google.com
Address: 8.8.8.8

Non-authoritative answer:
hackthissite.org nameserver = c.ns.buddyns.com
hackthissite.org nameserver = f.ns.buddyns.com
hackthissite.org nameserver = g.ns.buddyns.com
hackthissite.org nameserver = h.ns.buddyns.com
hackthissite.org nameserver = j.ns.buddyns.com
> set type=MX
> hackthissite.org
Server: google-public-dns-a.google.com
Address: 8.8.8.8

Non-authoritative answer:
hackthissite.org MX preference = 10, mail exchanger = aspmx1.google.com
hackthissite.org MX preference = 20, mail exchanger = alt1.aspmx1.google
.com
hackthissite.org MX preference = 20, mail exchanger = alt2.aspmx1.google
.com
hackthissite.org MX preference = 30, mail exchanger = aspmx2.googlemail.c
om
hackthissite.org MX preference = 30, mail exchanger = aspmx3.googlemail.c
om
hackthissite.org MX preference = 30, mail exchanger = aspmx4.googlemail.c
om
hackthissite.org MX preference = 30, mail exchanger = aspmx5.googlemail.c
om
>

```

2023

النهاية

مراجعة سريعة



# سؤال و إجابة

اول مرحله من مراحل عملية الاختراق.

.A الاستطلاع

.B التنفيذ

.C المسح

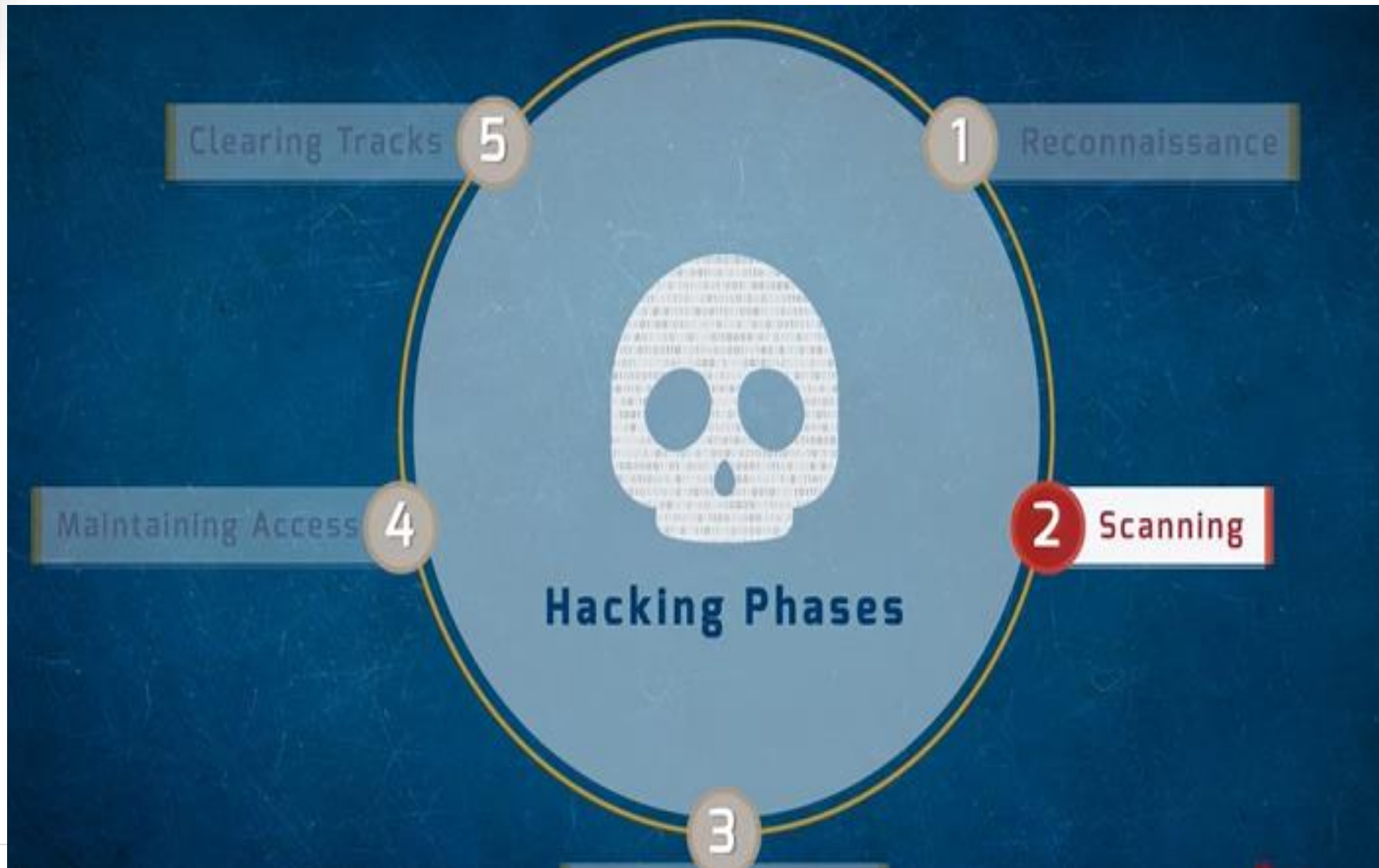
موقع لمعرفة معلومات عن ال domains.

.A whois

.B httrack

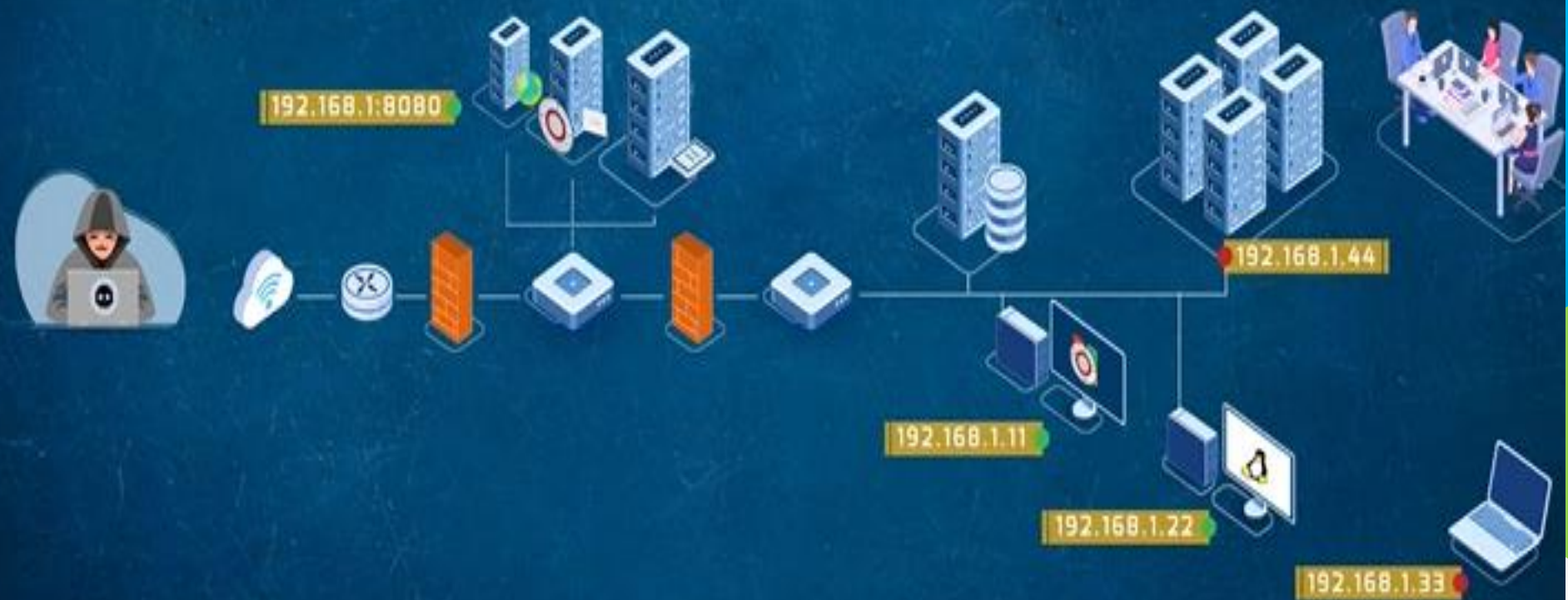


شكرا



## 2 Scanning

- discover live hosts, IP address, open ports
- Operating System
- Discover Vulnerabilities

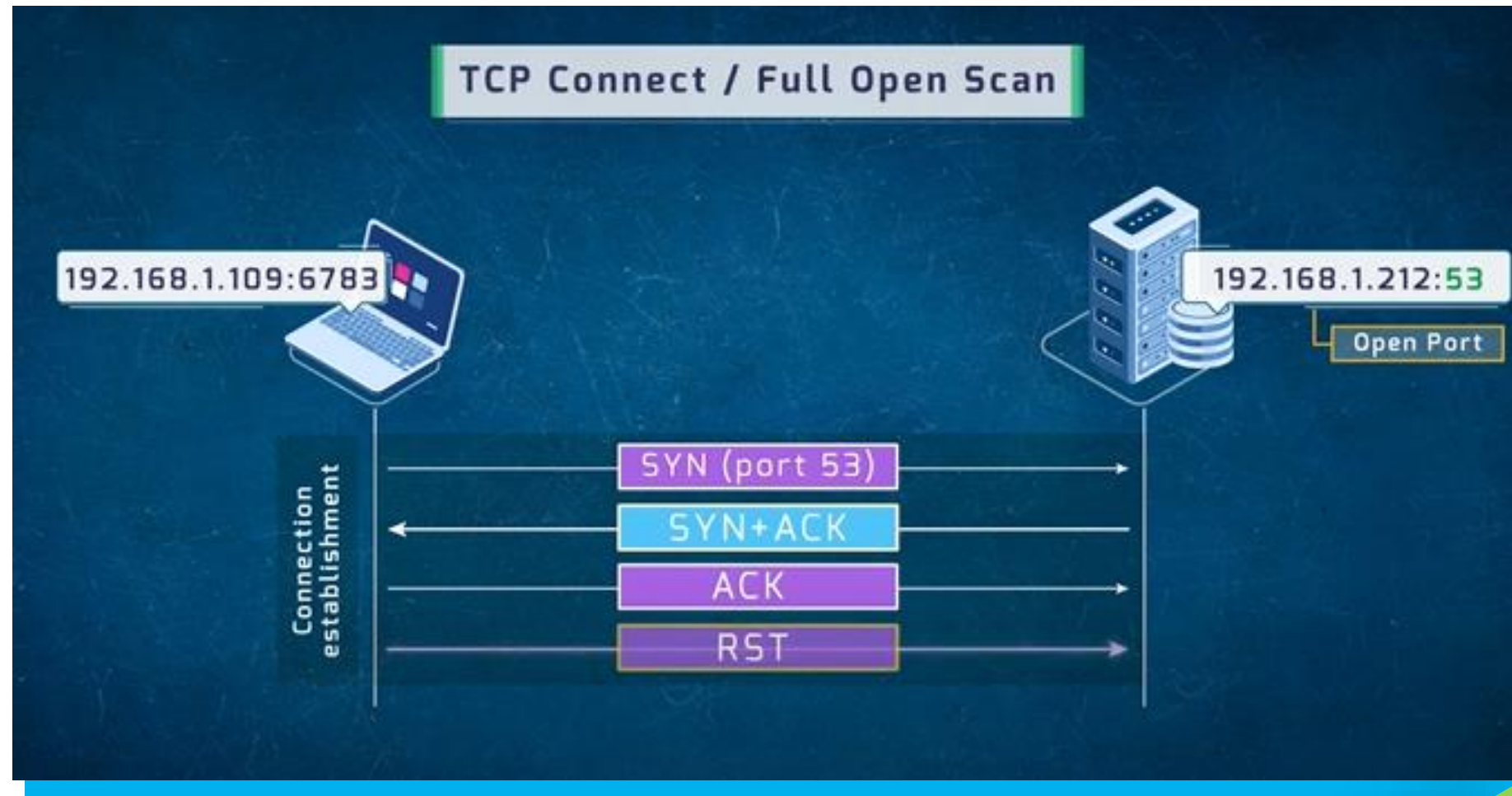


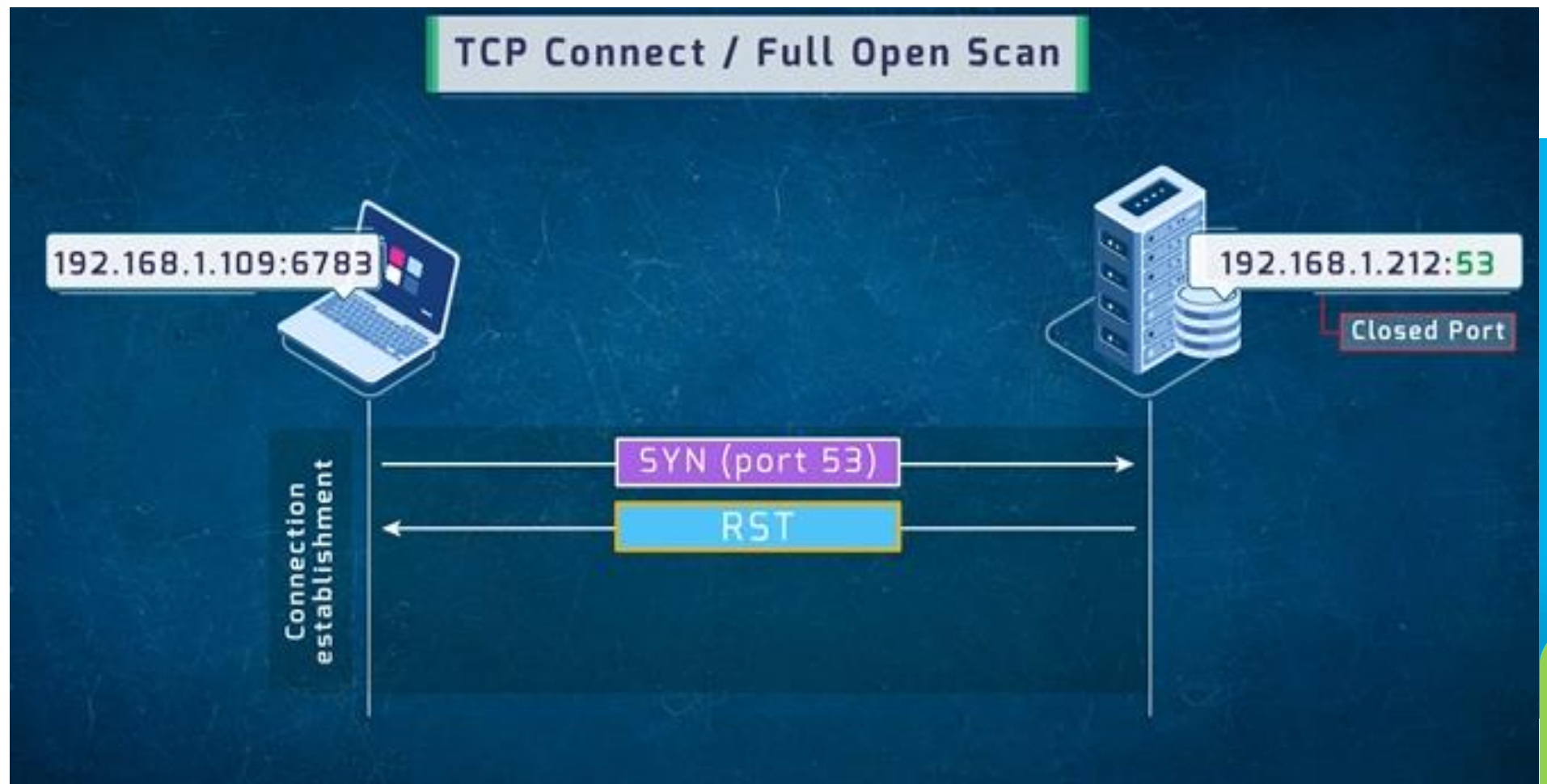
# Port scanning

## ■ Scanning **TCP** Network Services:

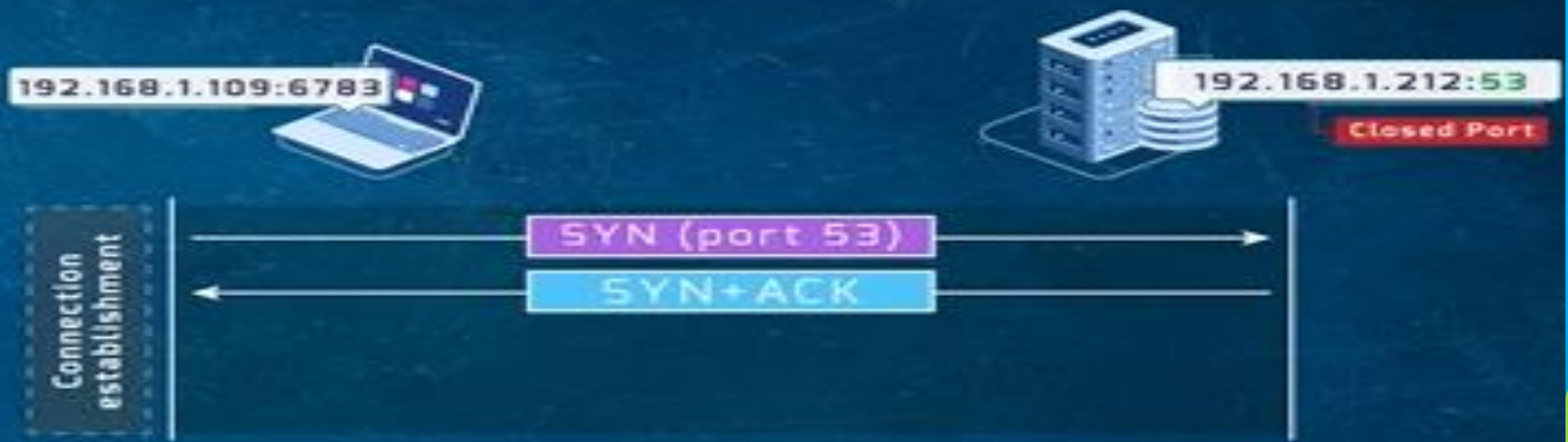
- 1 TCP Connect / Full Open Scan
- 2 Stealth Scan / Half -Open Scan
- 3 Xmas Scan

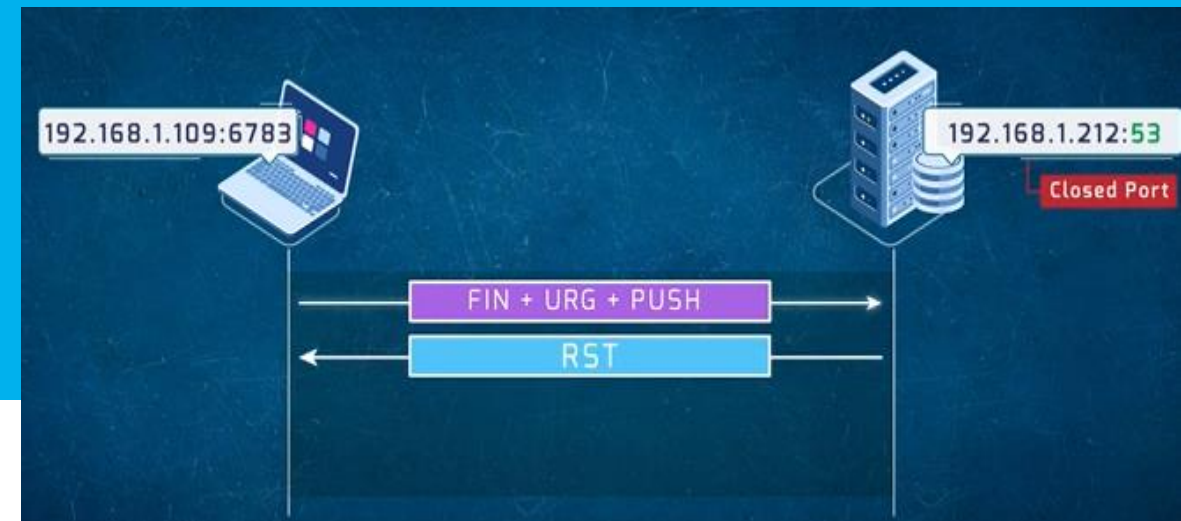
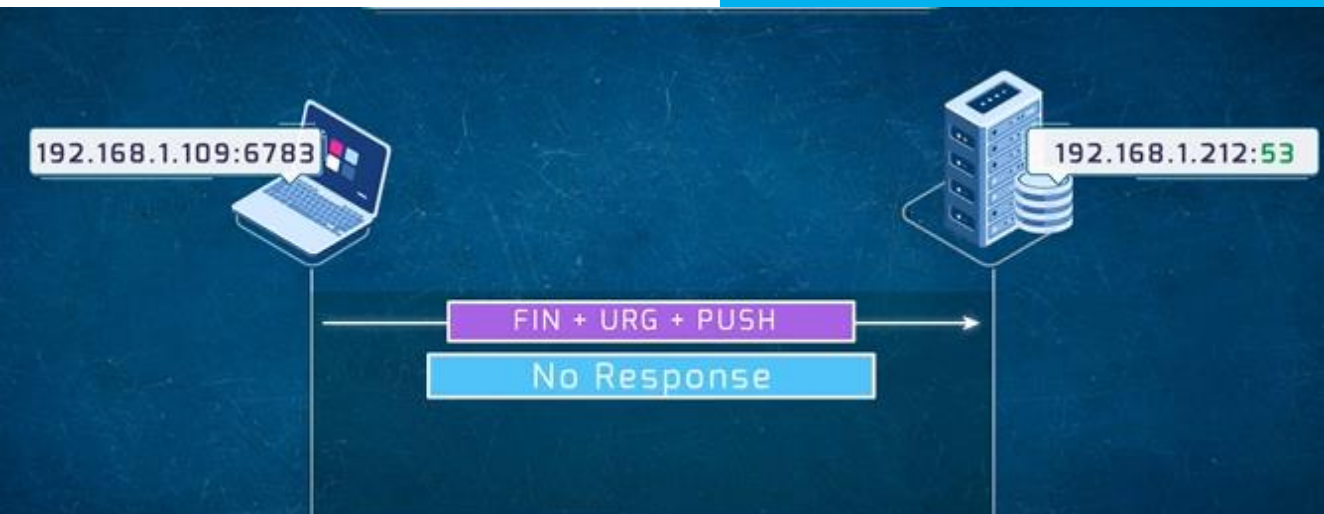
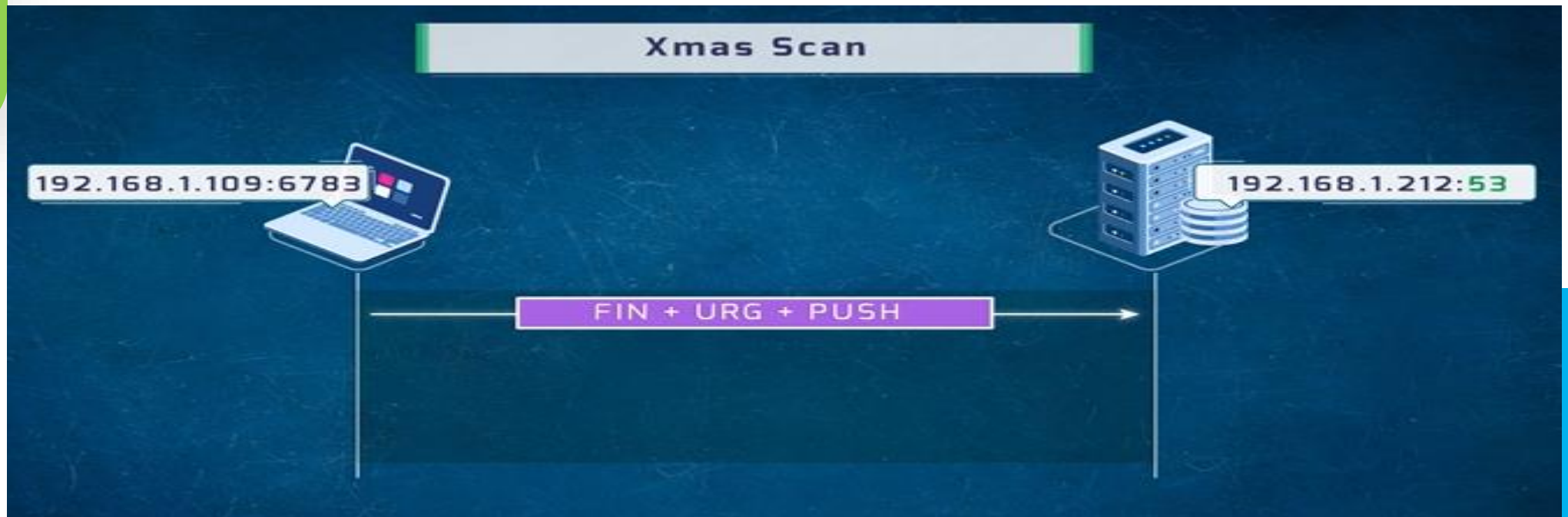
Flag	الشرح
SYN	بداية الاتصال
ACK	انتهاء الاتصال
PSH	ارسال البيانات
URG	طارئ
FIN	انهاء
RST	





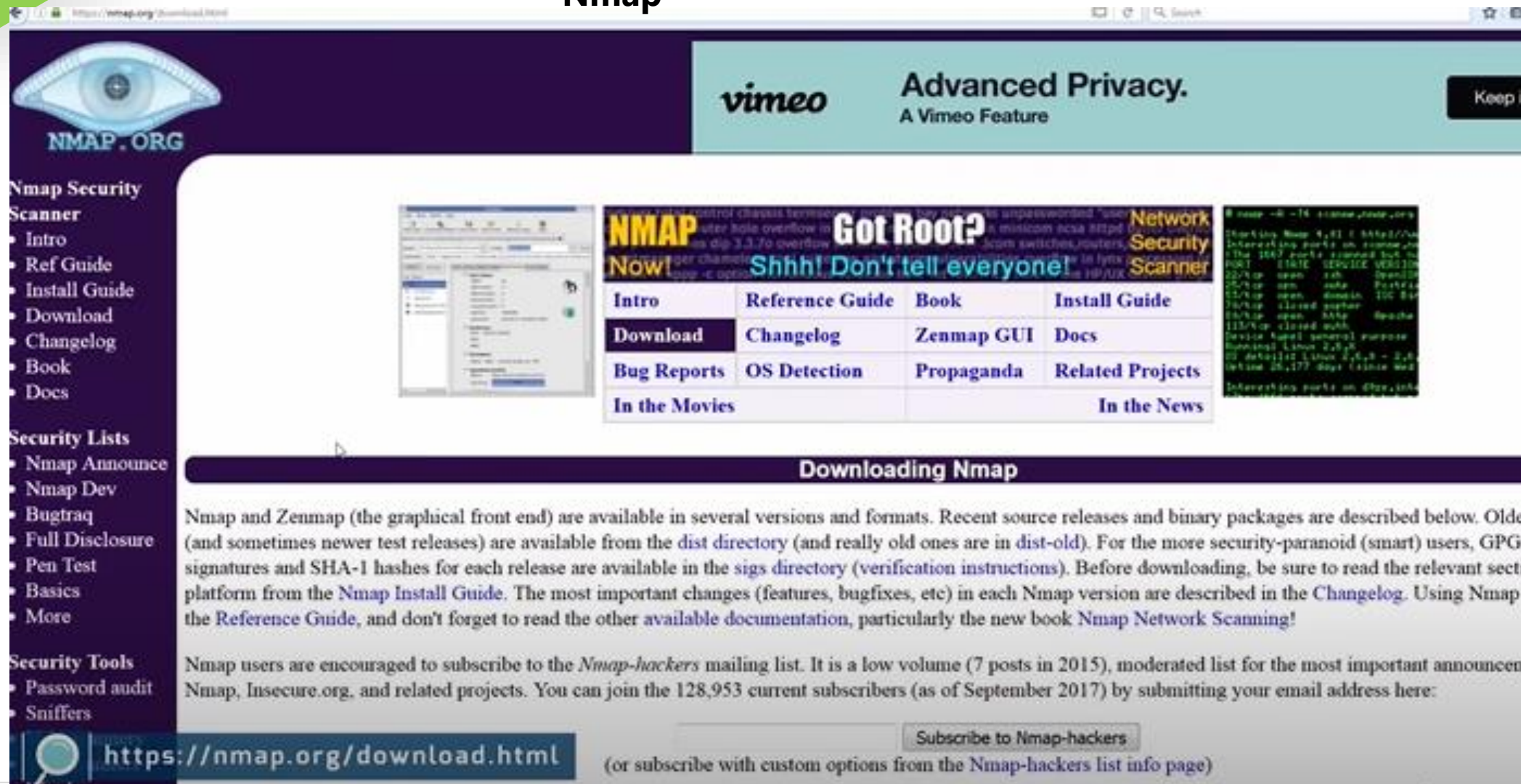
## Stealth Scan / Half -Open Scan





# Port scanning

## Nmap



**NMAP.ORG**

**Nmap Security Scanner**

- Intro
- Ref Guide
- Install Guide
- Download
- Changelog
- Book
- Docs

**Security Lists**

- Nmap Announce
- Nmap Dev
- Bugtraq
- Full Disclosure
- Pen Test
- Basics
- More

**Security Tools**

- Password audit
- Sniffers

**Advanced Privacy.**  
A Vimeo Feature

**Got Root?**  
Shhh! Don't tell everyone!

Intro	Reference Guide	Book	Install Guide
<b>Download</b>	Changelog	Zenmap GUI	Docs
Bug Reports	OS Detection	Propaganda	Related Projects
In the Movies			In the News

**Downloading Nmap**

Nmap and Zenmap (the graphical front end) are available in several versions and formats. Recent source releases and binary packages are described below. Older (and sometimes newer test releases) are available from the `dist` directory (and really old ones are in `dist-old`). For the more security-paranoid (smart) users, GPG signatures and SHA-1 hashes for each release are available in the `sigs` directory (verification instructions). Before downloading, be sure to read the relevant section of the `INSTALL` file on your platform from the [Nmap Install Guide](#). The most important changes (features, bugfixes, etc) in each Nmap version are described in the [Changelog](#). Using Nmap is described in the [Reference Guide](#), and don't forget to read the other available documentation, particularly the new book [Nmap Network Scanning!](#)

Nmap users are encouraged to subscribe to the *Nmap-hackers* mailing list. It is a low volume (7 posts in 2015), moderated list for the most important announcements for Nmap, Insecure.org, and related projects. You can join the 128,953 current subscribers (as of September 2017) by submitting your email address here:

<https://nmap.org/download.html>

(or subscribe with custom options from the [Nmap-hackers list info page](#))

# الهندسة الاجتماعية



## انتحال الشخصية

 Human-based

**IDENTIFICATION CARD**

	Name: <b>Geoff Sample</b>
	D.O.B: <b>Area manager</b>
	ID No: <b>1238626AB4</b>
	Issued: <b>January 2011</b>
	Expires: <b>December 2013</b>



# التجسس



Human- based



Eavesdropping





Human- based



Shoulder Surfing





Human- based



Dumpster Diving





Computer-based



Phishing





## Mobile-based



# الحلول



تحديد الصلاحيات



التدريب





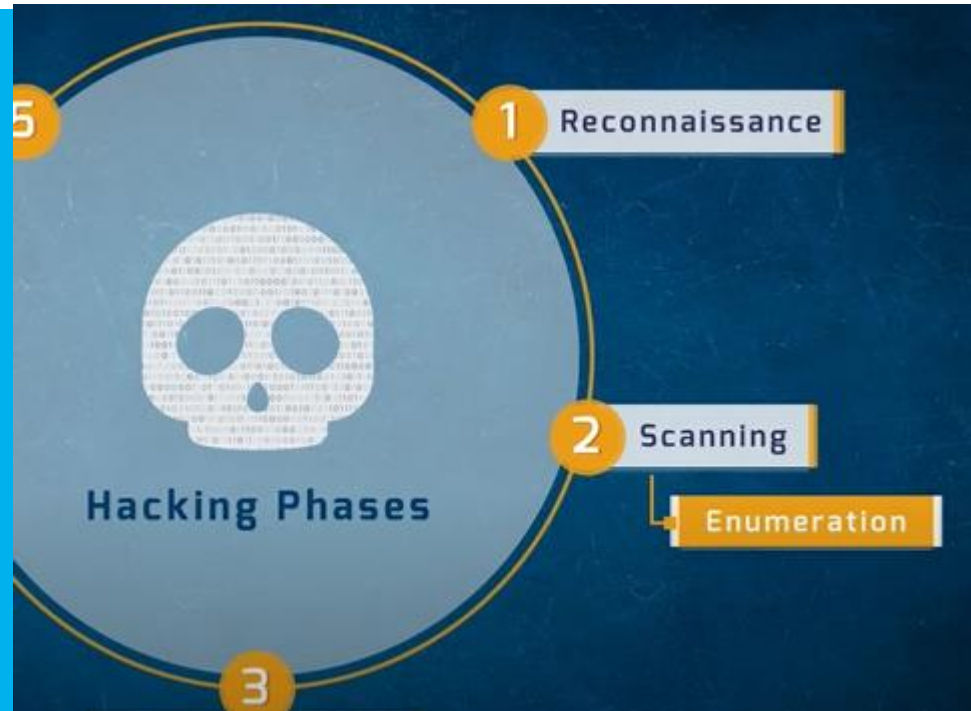
## Enumeration

هي جزء من مرحلة المسح



يتم الوصول الى:

User name  
User groups  
passwords





من خلال:  
System hacking  
Password cracking



# تقنيات الاذونات والصلاحيات

## Identification and Authentication Techniques



**Passwords**

Something you  
**KNOW**

AND  
OR



**Biometric**

Something you  
**ARE**

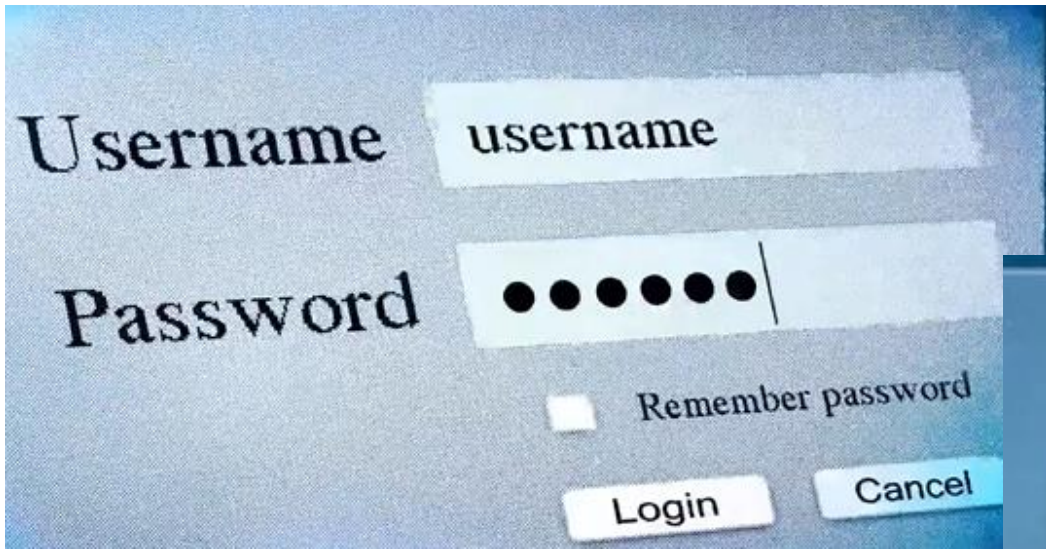
AND  
OR



**Tokens**

Something you  
**HAVE**





# أنواع كلمات المرور

## Static passwords

- Always remain the same



## Dynamic passwords

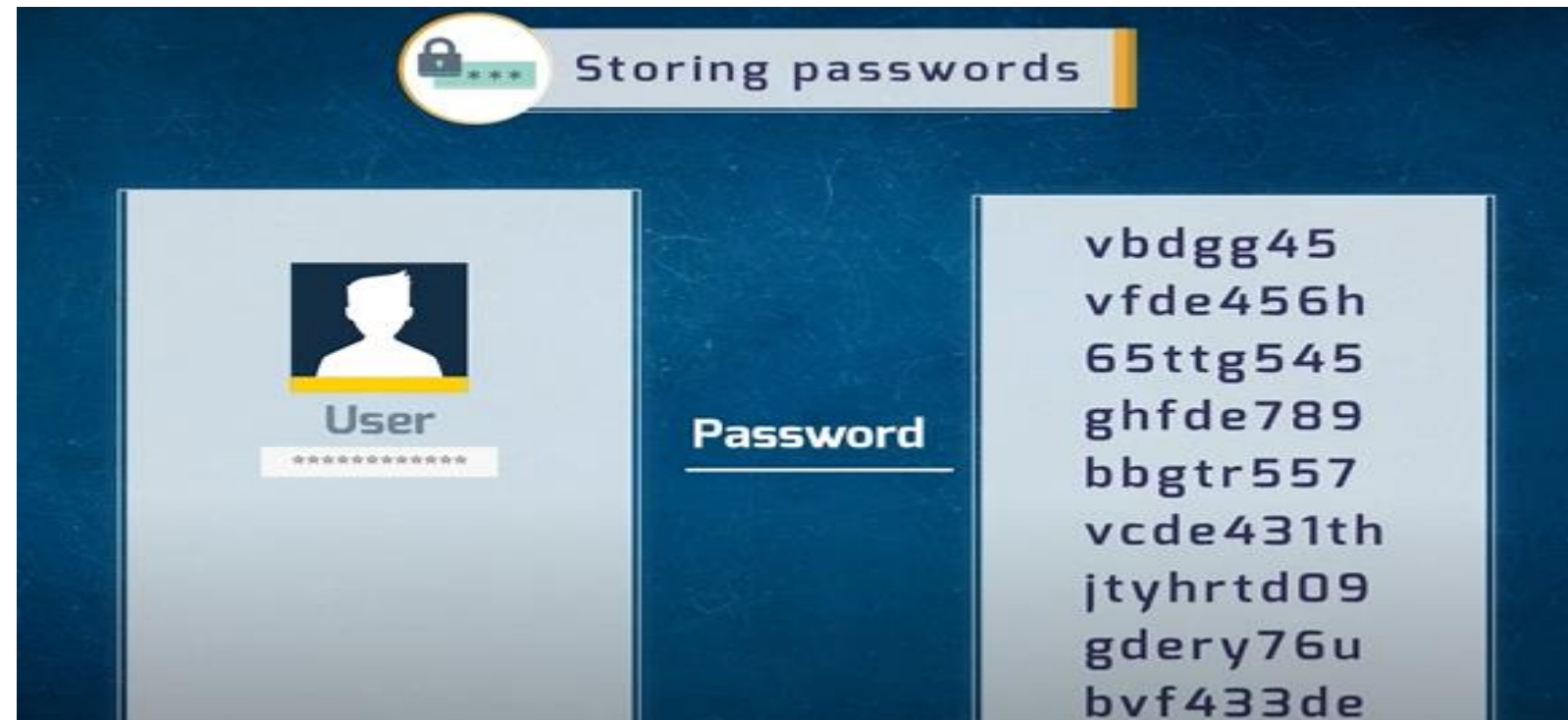
- change after a specified interval of time or use

Please enter the OTP(One Time Password)  
sent to your registered mobile #:974xxxx5968  
This OTP will expire in 5 minutes.

Validate OTP If you have not receive your OTP then click here



# دالة الهاش Hash



هجمات كلمات المرور



## Passwords Attacks

Network traffic analysis

تحليل حركة الشبكة

Brute-force attack

هجم القوة الغاشمة

Dictionary attack

هجمة القاموس

Rainbow tables /  
Pre-computation Brute force

هجمة الرينبو

Hybrid attack

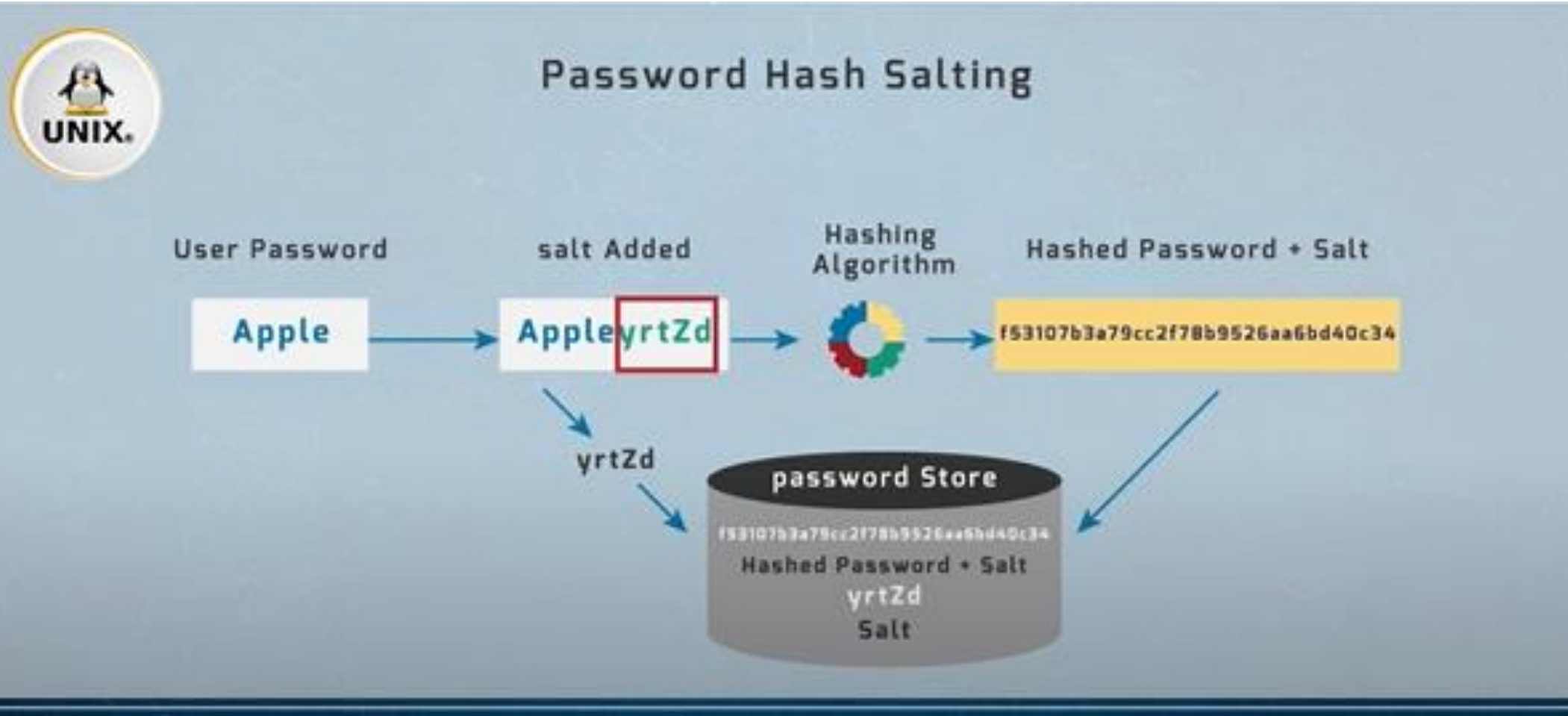
هجمة المختلطة

Social Engineering

الهندسة الاجتماعية



# الحماية



إضافة على كلمه  
المرور قبل  
دخولها دالة  
الهاش



## زيادة امان كلمة المرور



### Increasing password security



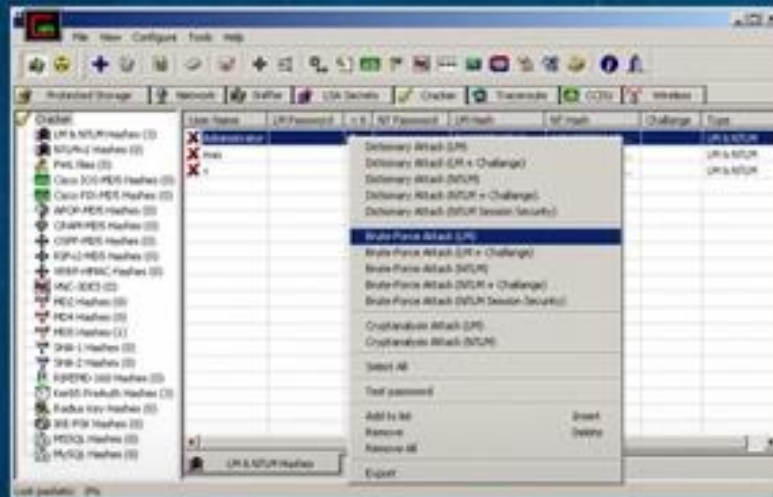
- Use complex, strong form (Longer passwords)
- Use password verification tools against your password database file.
- Disable inactive user accounts
- Users training about using of strong passwords.
- **Root or administrator should be changed regularly**



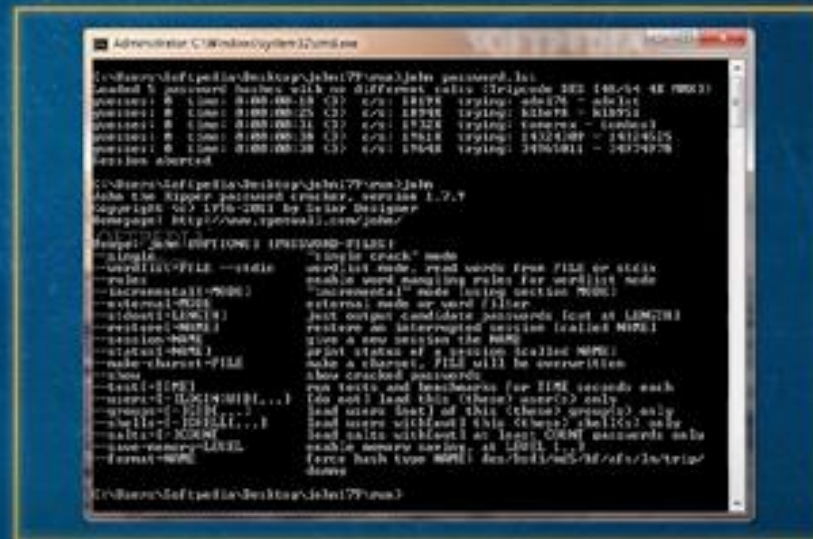
# أدوات كسر كلمة المرور



## Passwords Cracking Tools



Cain and Abel



John the Ripper



2023

النهاية

مراجعة سريعة  
القرصنة الاخلاقية



# سؤال و إجابة

الهندسة الاجتماعية من وسائلها:

1. التصيد
2. التجسس
3. جميع ما سبق

رساله ACK تكون ل :

1. بدء الاتصال
2. انشاء الاتصال
3. ارسال البيانات



شكرا

# مسح الشبكات

Web server ??

Command Prompt

```
Microsoft Windows [Version 10.0.18363.657]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\Qebaa>telnet certifiedhacker.com 80
```

<https://www.grc.com/id/idserve.htm>

The screenshot shows the ID Serve web application interface. The title bar reads "ID Serve" and the subtitle is "Internet Server Identification Utility, v1.02 Personal Security Firewall by Steve Gibson Copyright (c) 2003 by Gibson Research Corp". The interface has three tabs: "Background", "Server Query", and "GSA/Help". The "Server Query" tab is active. It contains a text input field with the URL "certifiedhacker.com" and a "Query The Server" button. Below the input field, there is a section for "Server query processing" with the following details: "Content-Length: 3660", "Connection: close", "Last-Modified: Thu, 10 Feb 2011 11:01:38 GMT", "Accept-Ranges: bytes", and "Query complete". At the bottom, it states "The server identified itself as: nginx/1.14.1". There are "Copy", "Go to ID Serve web page", and "Exit" buttons at the bottom of the interface.

# إخفاء الاثر

PROXYSWITCHER.COM

MAIN

PLUGINS

DOWNLOAD

KNOWLEDGE BASE

ORDER

SUPPORT

## Proxy Switcher - surf anonymously change proxy settings on the fly

There are times when you have to cloak your true IP address. It might be that you want to remain anonymous when you visit a particular website. Or your access to various social networking and entertainment sites has been blocked.

The solution is to use Proxy Switcher for all the anonymous browsing needs. It can be used to avoid all sorts of limitations imposed by various sites. Be that a download site that limits amount of downloads. Or video site works only in a particular country - more often than not it gets defeated by the anonymous browsing features Proxy Switcher provides.

On top of that, if you used to manually change proxy settings Proxy Switcher provides a way to change them much faster and easier.

DOWNLOAD

PURCHASE

https://www.proxyswitcher.com/

# Text file in text file

```
Administrator: Command Prompt
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd C:/Test

C:\Test>echo "Clear Content" > 1st.txt

C:\Test>echo "hiddent content" > 1st.txt:hidden.txt

C:\Test>dir
Volume in drive C has no label.
Volume Serial Number is 20D7-A27F

Directory of C:\Test

10/27/2019  12:49 PM    <DIR>          .
10/27/2019  12:49 PM    <DIR>          ..
10/27/2019  12:50 PM                18 1st.txt
                1 File(s)                18 bytes
                2 Dir(s)  10,772,221,952 bytes free

C:\Test>_
```

2023

النهاية

مراجعة سريعة  
القرصنة الاخلاقية



شكرا