معهد العراب العالي للتدريب

107 سايبر

اختبار الاختراق

م. سمر سعيد الهوارى

نبذة عن المقرر

التعرف على اختبار الاختراقات للشبكات والأنظمة
والأدوات والأساليب المستخدمة

معهد العراب العالي للتدريب

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 Hackingوالاسم 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

المبادئ الأساسية للقرصنة الأخلاقية: Ethical Hacking

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
اخطار 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.

الهاكر الأخلاقي والأمن السيبراني

الامن السيبراني: يضع استراتيجية الحماية والدفاع ضد الهجوم.

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

مثال:

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

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

بينما الهاكر 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/

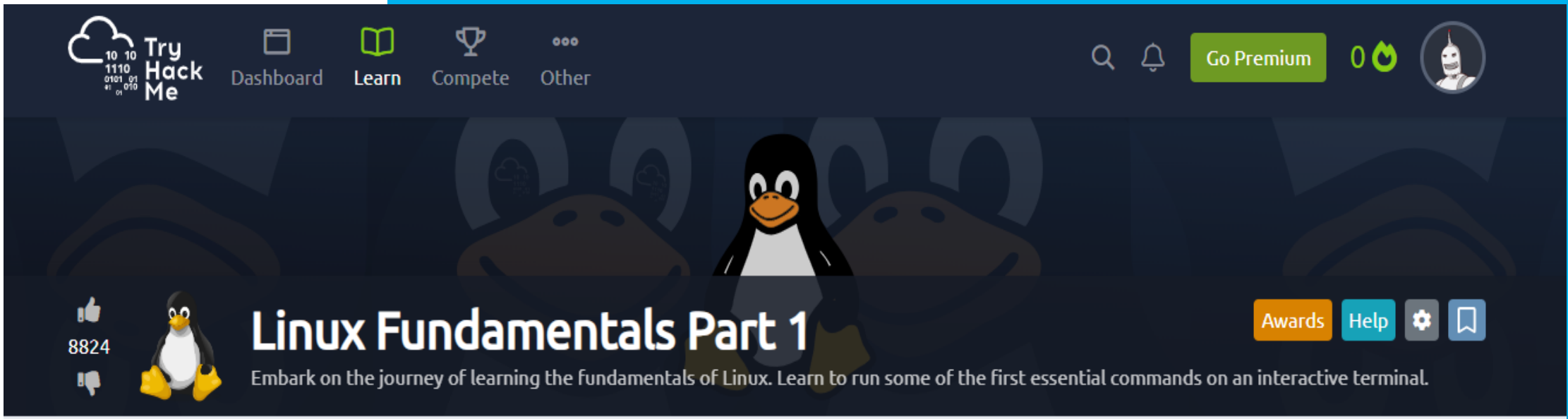
- **Installing Kali Linux (Hard Disk Install)**

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/

مراجعه اهم أوامر Linuxعلى موقع try hack me


Try Hack Me
Dashboard
Learn
Compete
Other
Go Premium
0
8824
Linux Fundamentals Part 1
Embark on the journey of learning the fundamentals of Linux. Learn to run some of the first essential commands on an interactive terminal.
Awards
Help

معهد العراب العالي للتدريب

مراجعة سريعة

القرصنة الاخلاقية

2023

النهاية

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 استراتيجية الحماية والدفاع ضد الهجوم.

A. الهاكر الأخلاقي

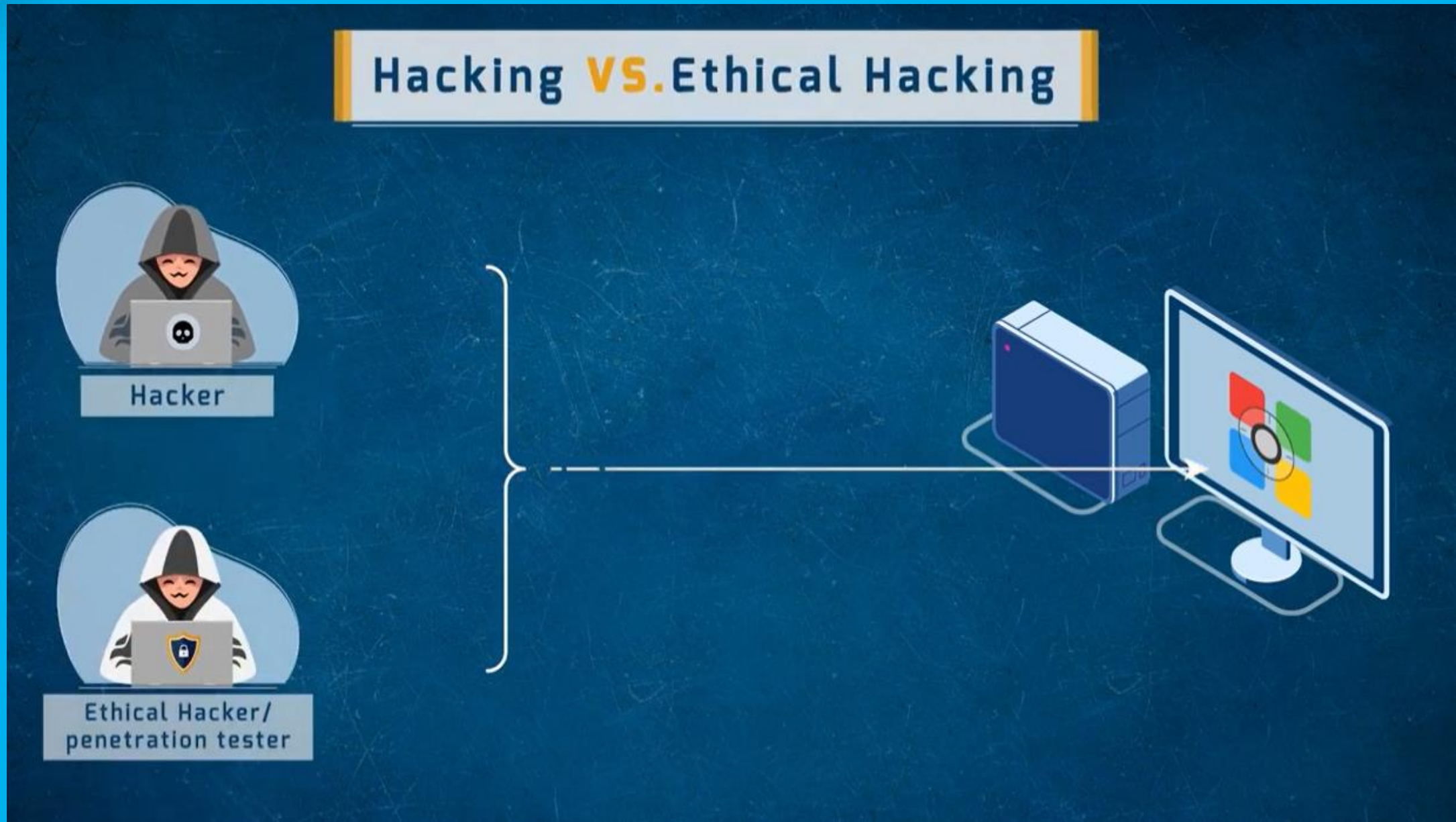
B. الامن السيبراني

C. التشفير

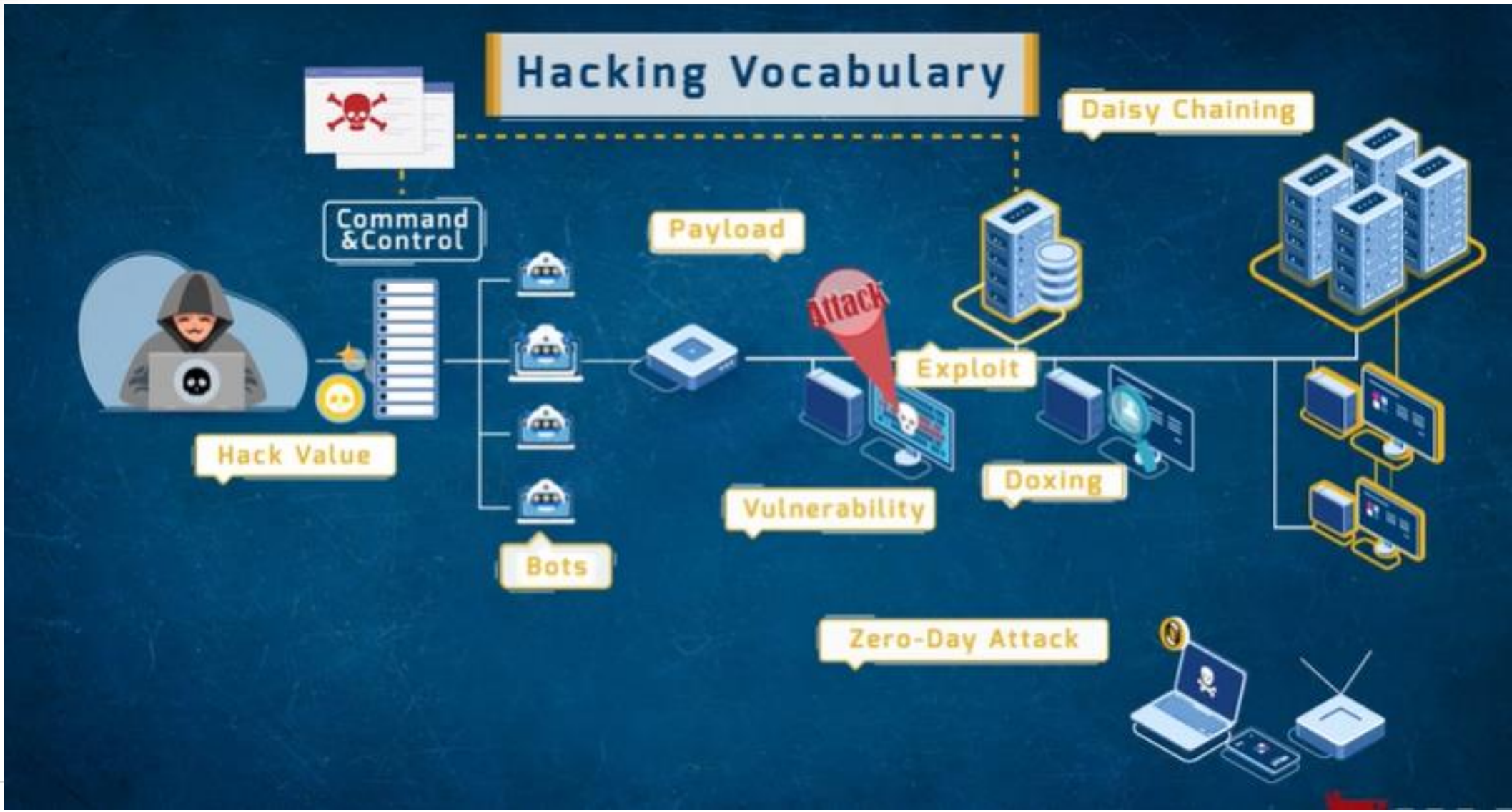
معهد العراب العالي للتدريب

شكرا

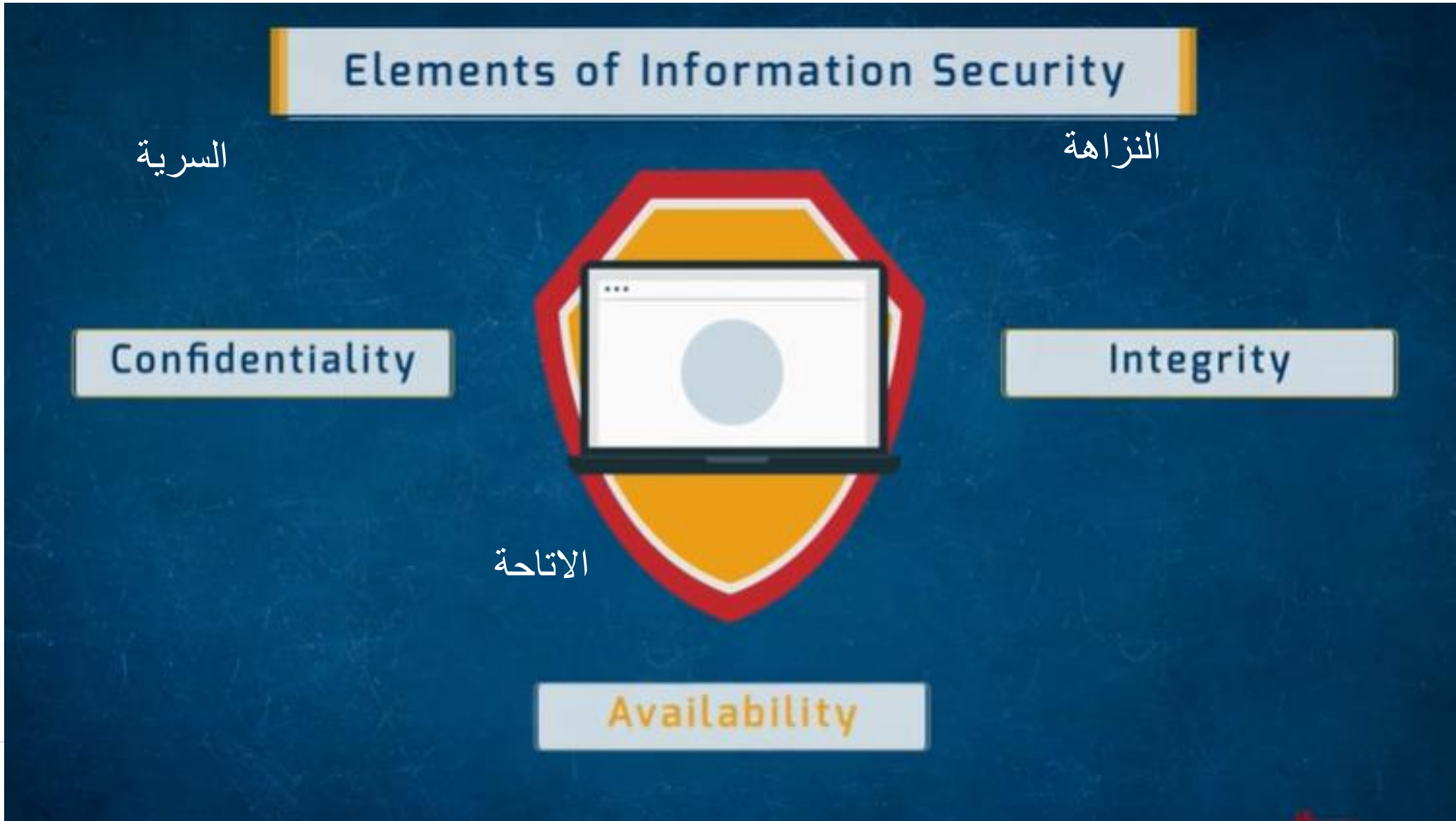
الاختراق والاختراق الأخلاقي



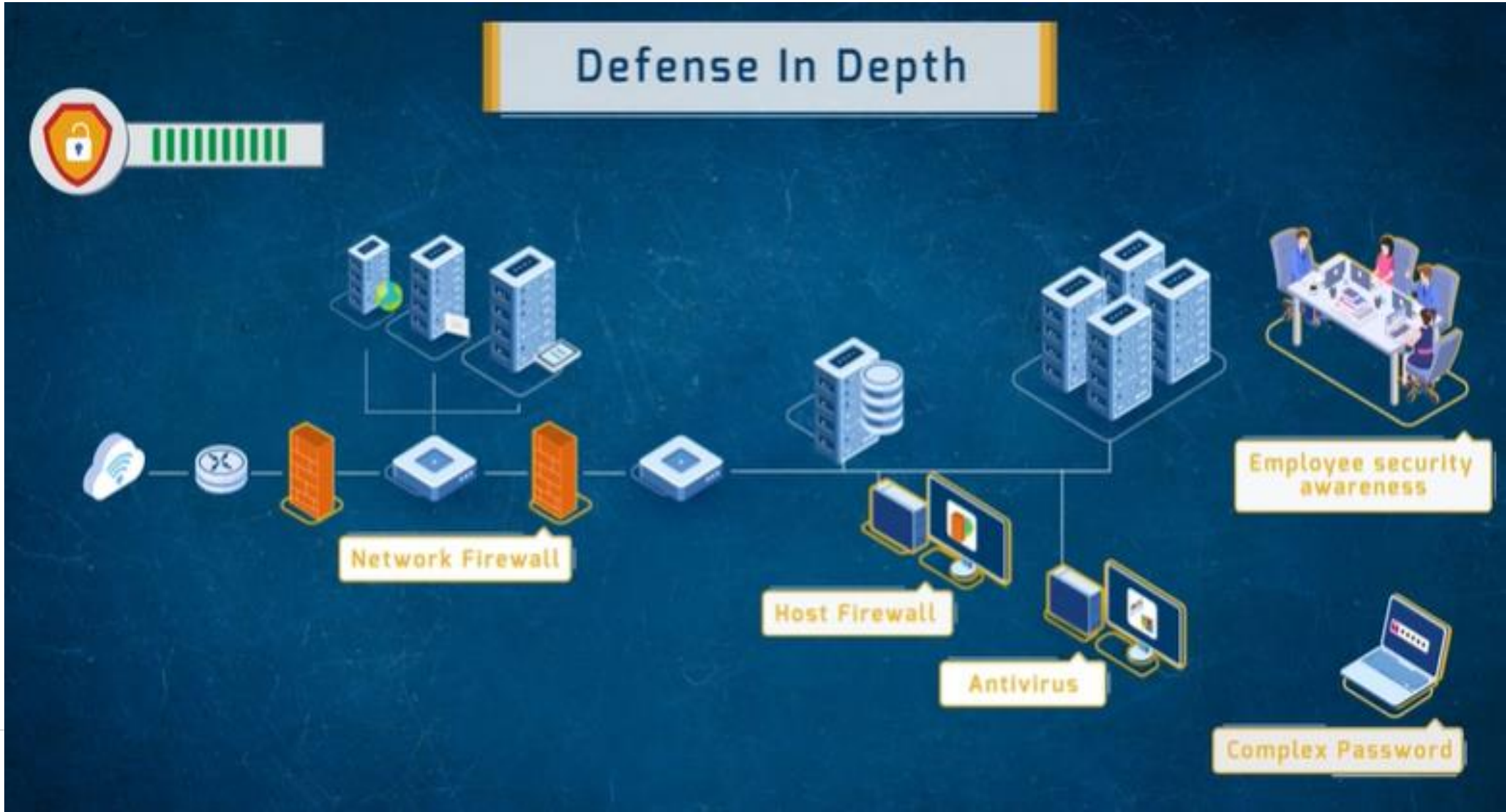
مصطلحات في الاختراق



عناصر امن المعلومات

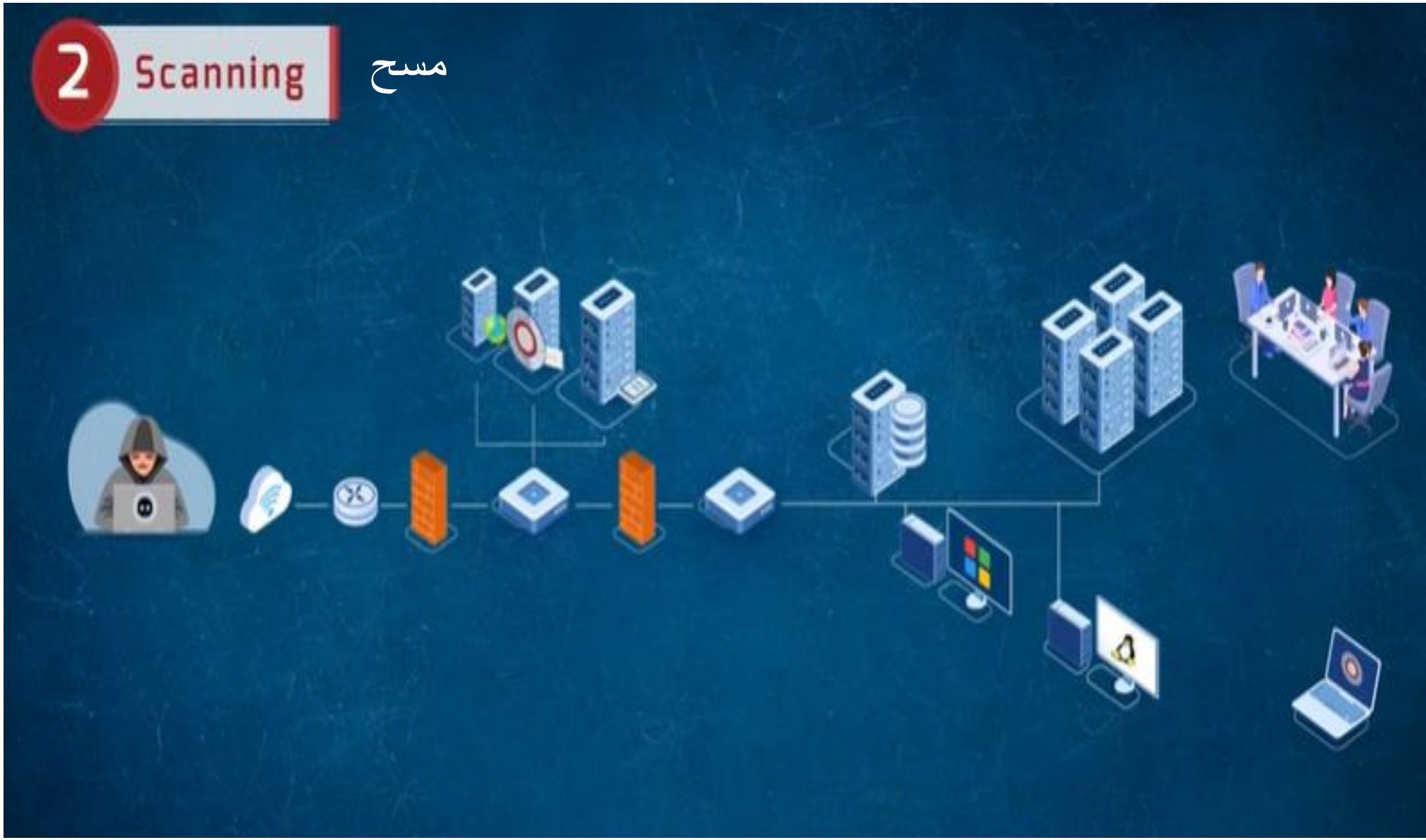


الدفاع في العمق



مراحل الاختراق Hacking phases


1 Reconnaissance
الاستطلاع
تجميع معلومات
Gather information about a target
Passive Reconnaissance
Active Reconnaissance



1- الأجهزة
2- ports
3- vuln. الثغرات

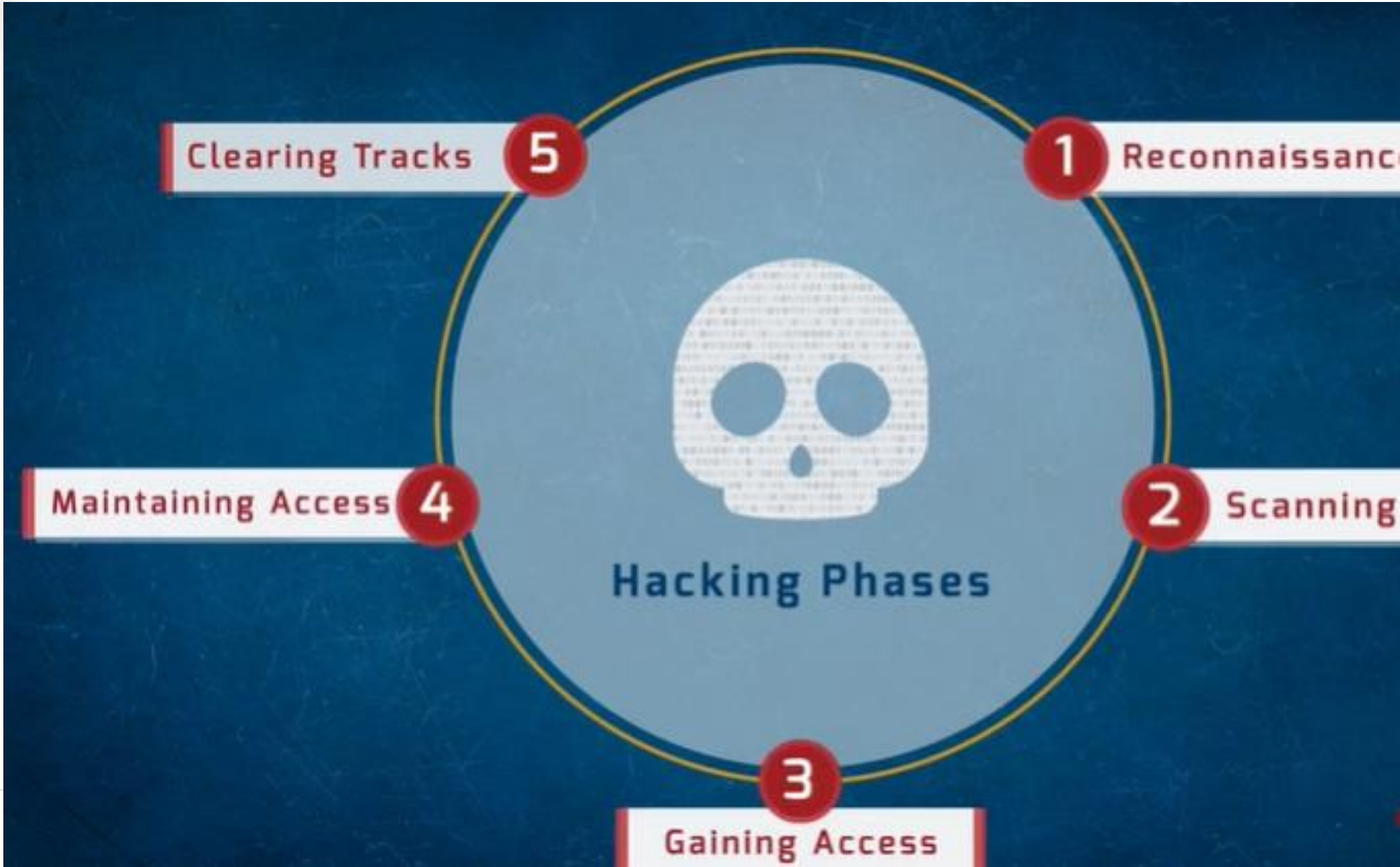
التنفيذ


4 Maintaining Access
Retain ownership of the system

5 Clearing Tracks

تنظيف الاثار

- Hide malicious acts
- Avoid suspicion
- Unnoticed continuing access


Clearing Tracks
5
1
Reconnaissanc
Maintaining Access
4
2
Scanning
Hacking Phases
3
Gaining Access

الاستطلاع Recon

- فائدة الاستطلاع
- اهداف الاستطلاع
- طرق الاستطلاع

فائدة الاستطلاع

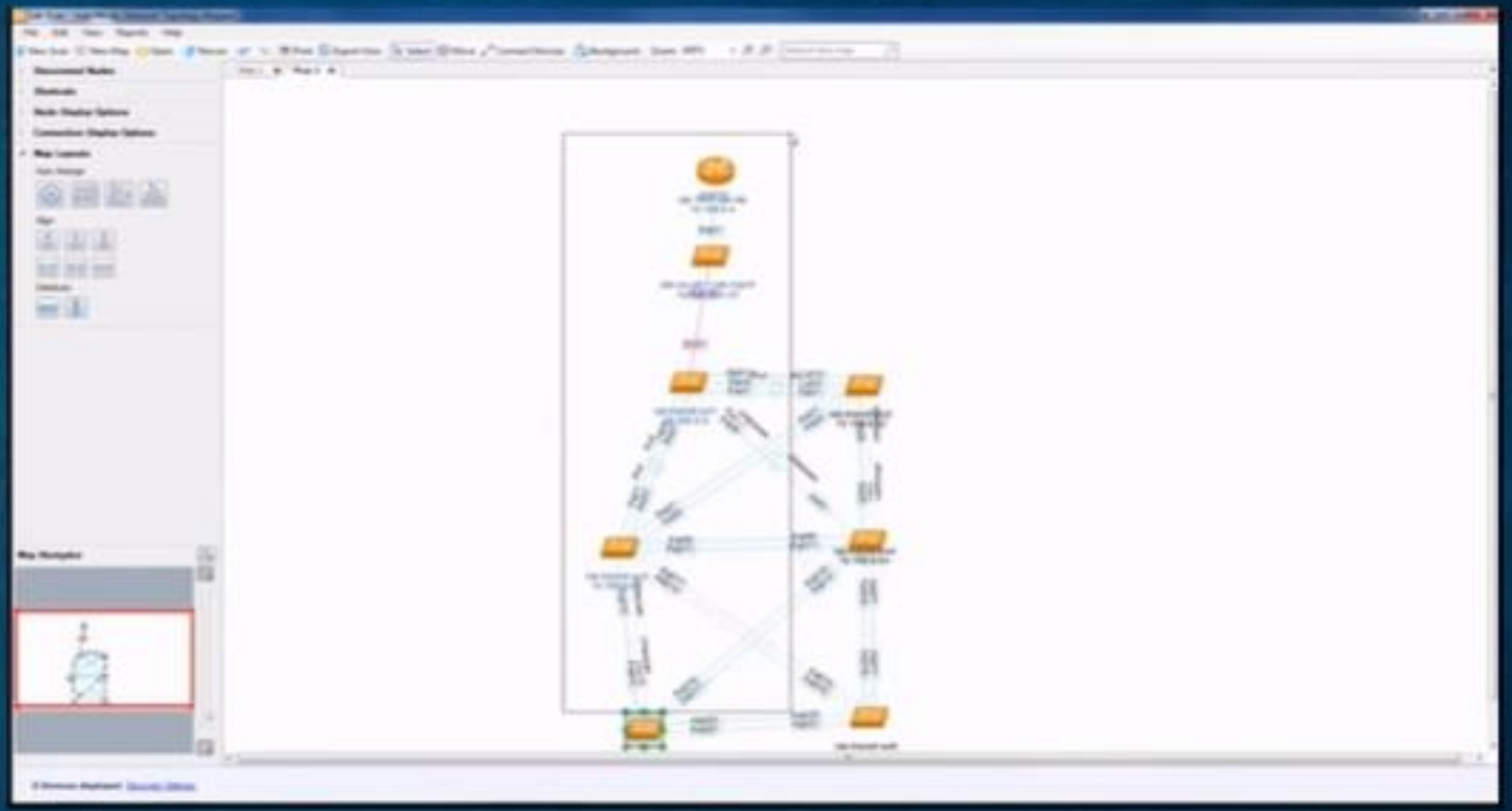
تقليل مساحه التركيز


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

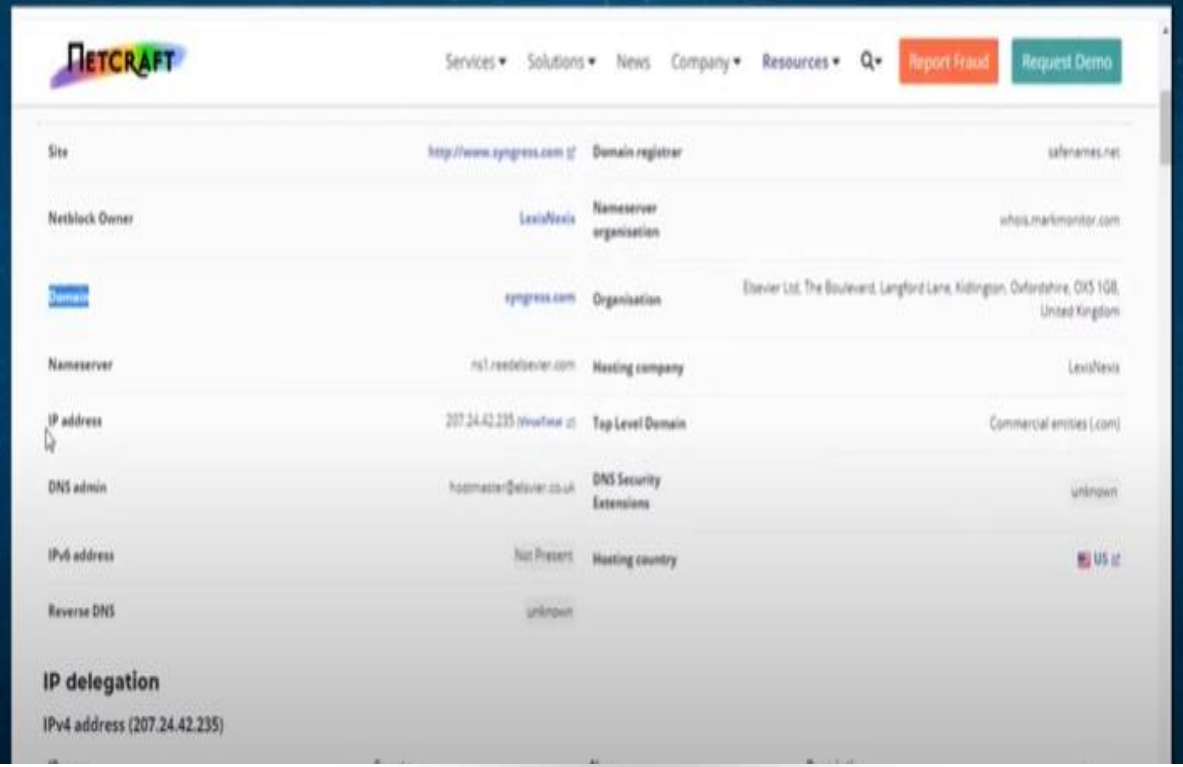


اهداف الاستطلاع

Objectives of Reconnaissance

- Collect Network Information

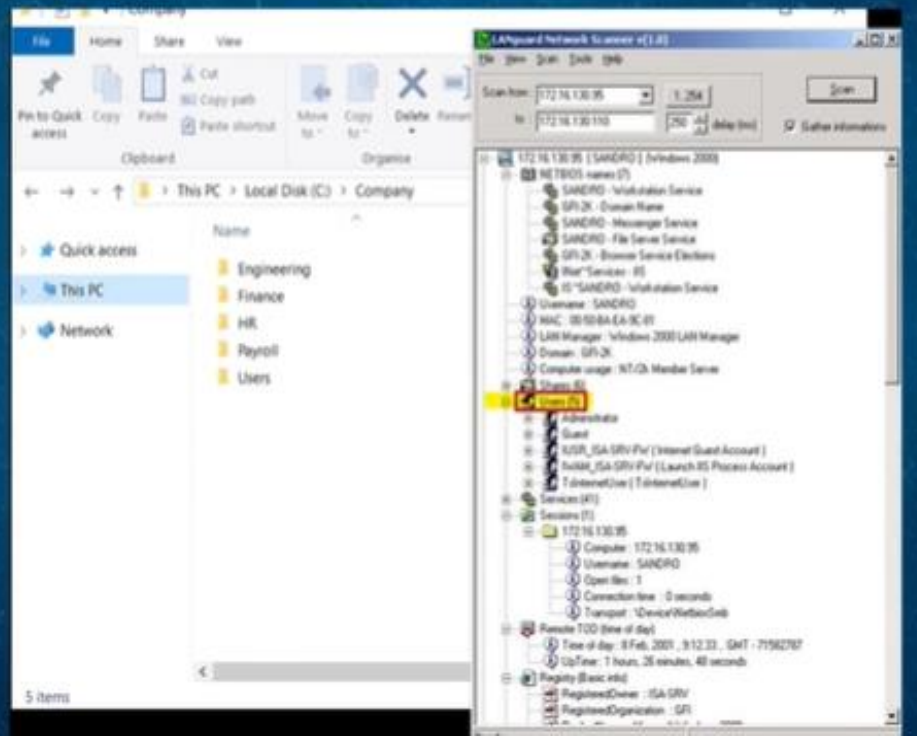
تجميع معلومات الشبكة



Objectives of Reconnaissance

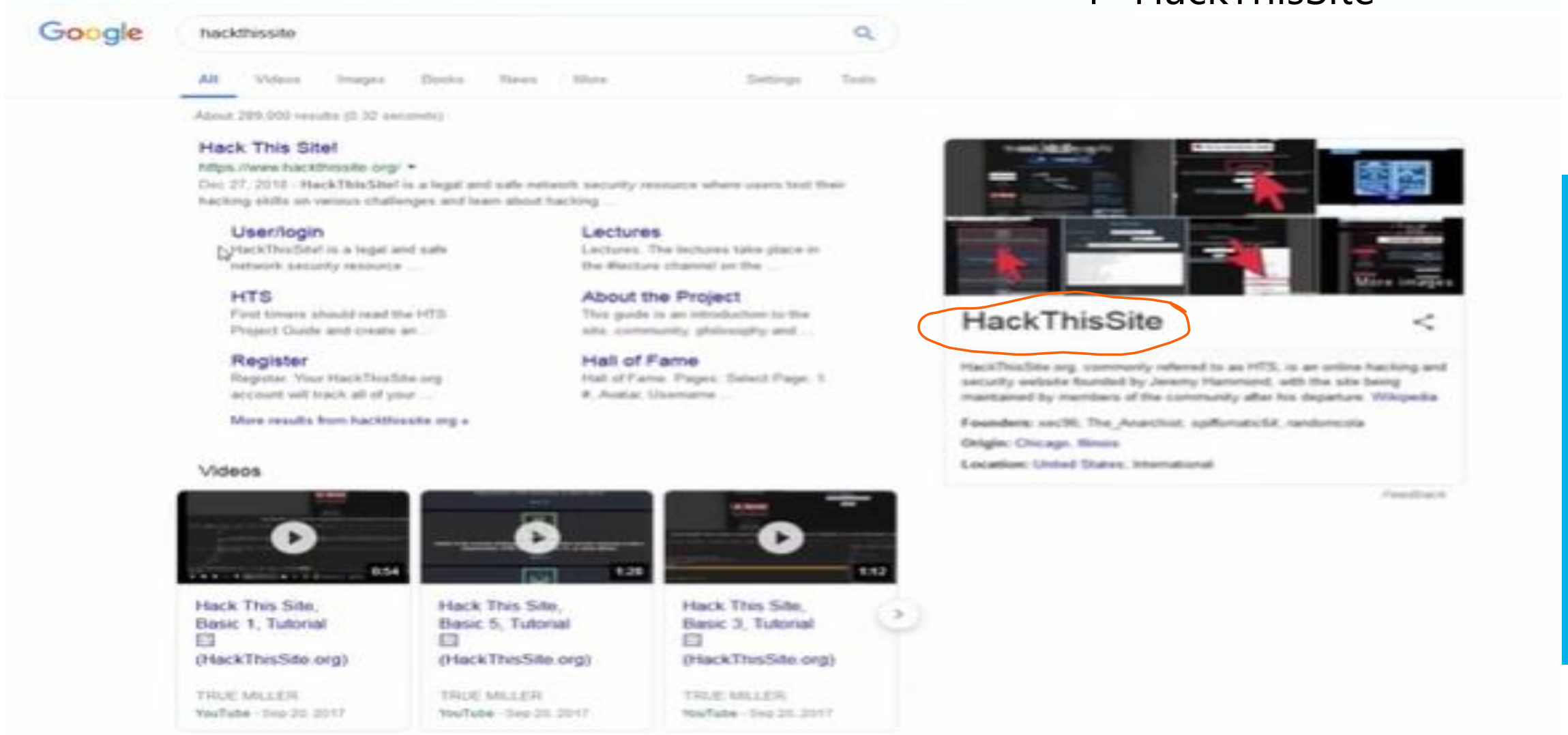
- Collect system Information

تجميع معلومات النظام والافراد

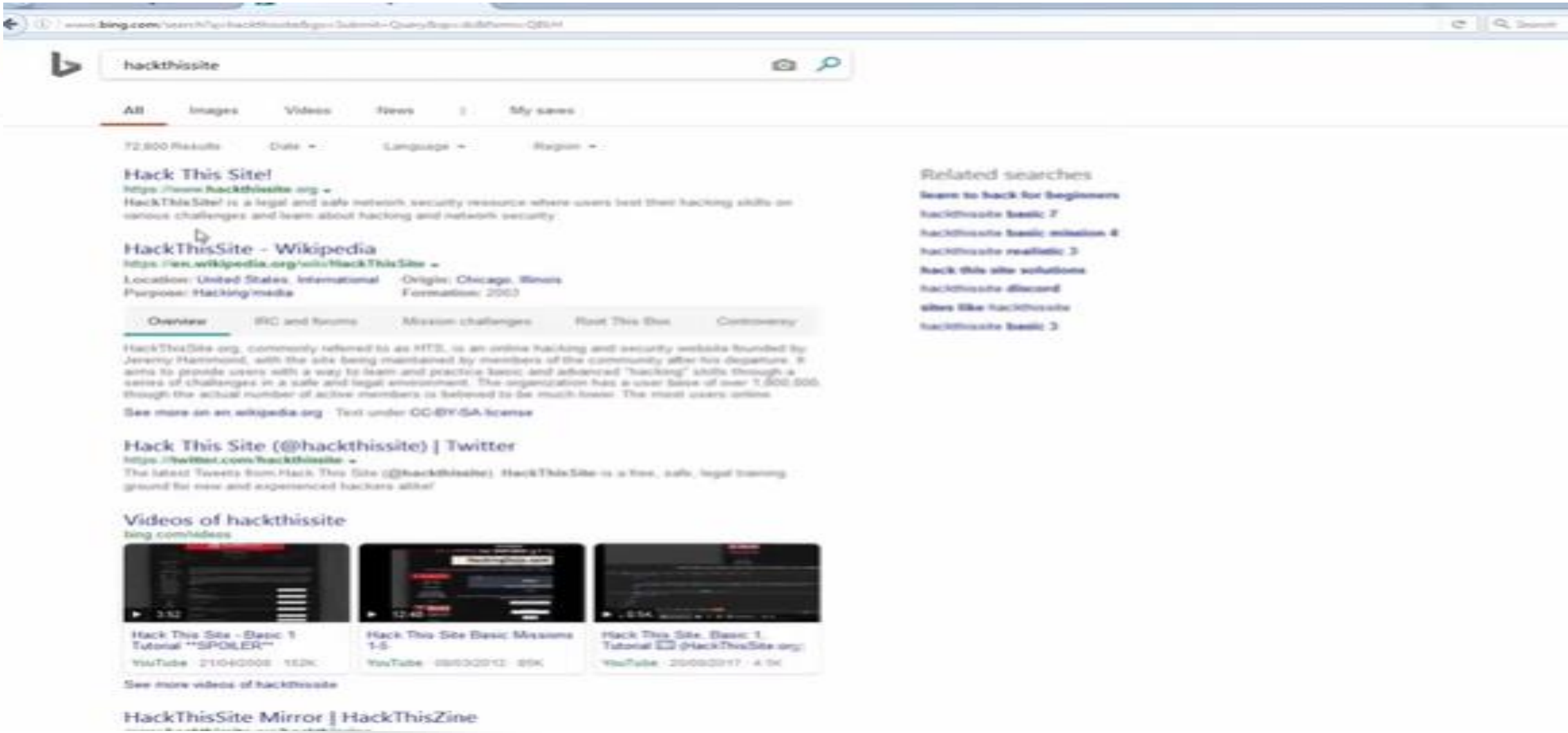


أدوات محرك البحث

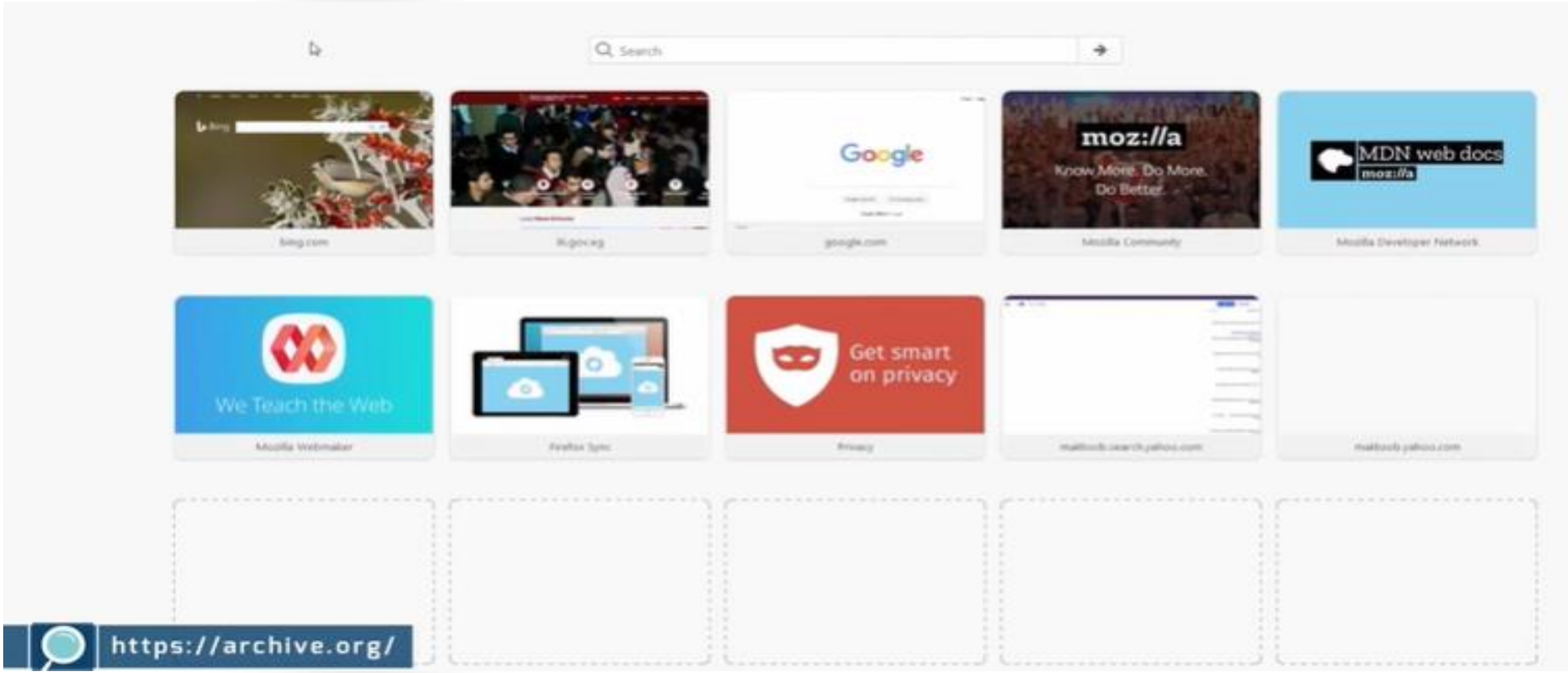
1- HackThisSite



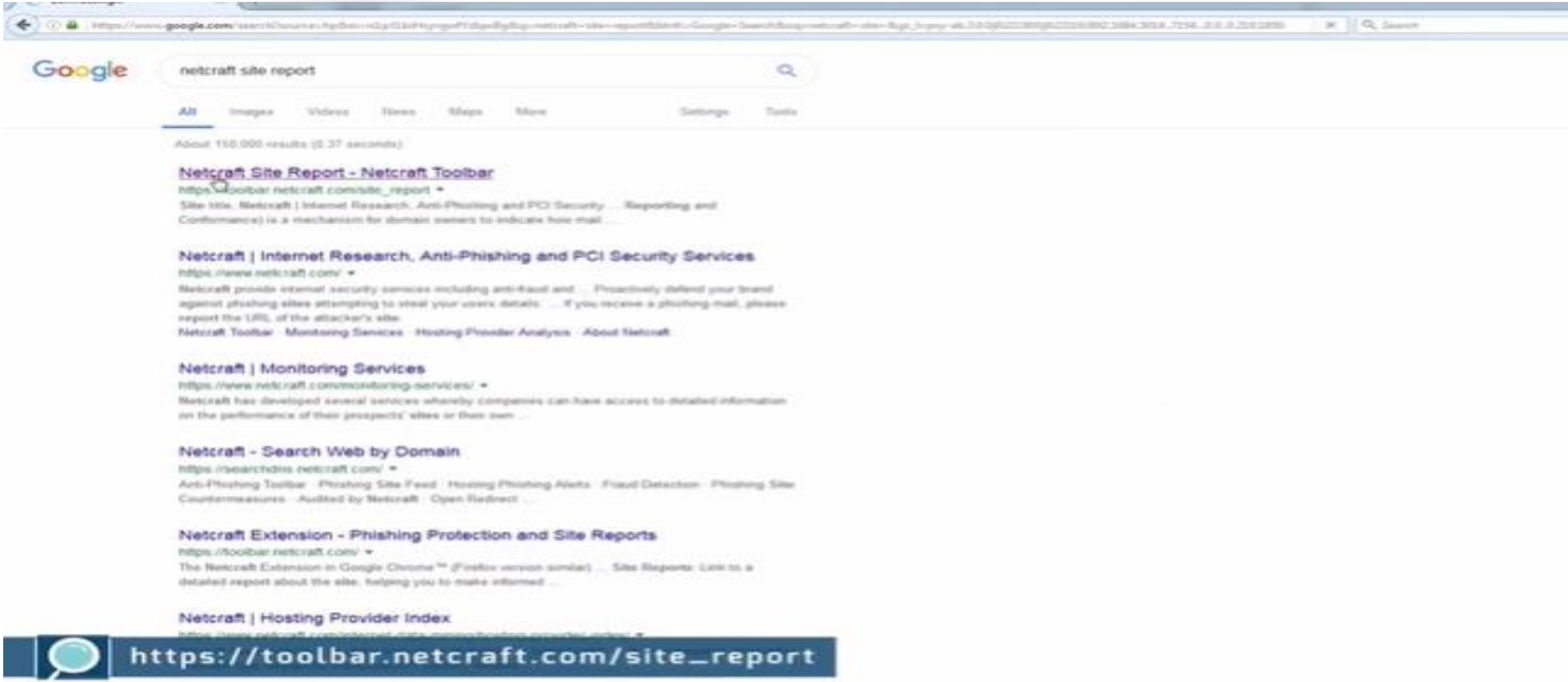
https://livethreatmap.radware.com/


hackthissite
All
Images
Videos
News
My saves
Hack This Site!
HackThisSite - Wikipedia
Hack This Site (@hackthissite) | Twitter
Videos of hackthissite
HackThisSite Mirror | HackThisZine
Related searches

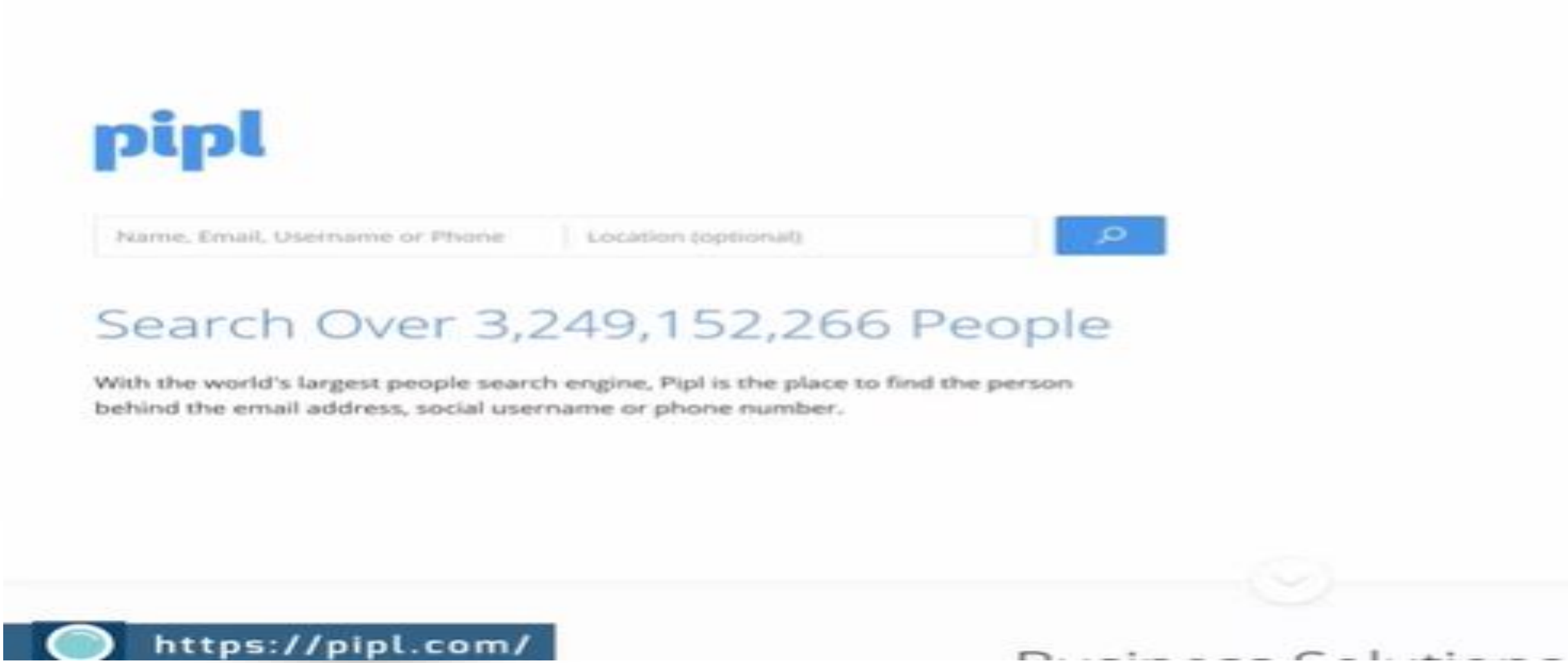
2- Archive.org



3- netcraft site report



4- البحث عن اشخاص



مصادر أخرى

- Anywho
- whitepages

معهد العراب العالي للتدريب

2023

النهاية

مراجعة سريعة

سؤال و إجابة

ثانى مرحله من مراحل عملية الاختراق.

A. الاستطلاع

B. التنفيذ

C. المسح

مميزات الاختراق الأخلاقي.

A. سرقة المعلومات

B. انتحال الشخصيات

C. حماية المؤسسات

معهد العراب العالي للتدريب

شكرا

Google operators

معهد العراب العالي للتدريب

Google Operators: intitle:

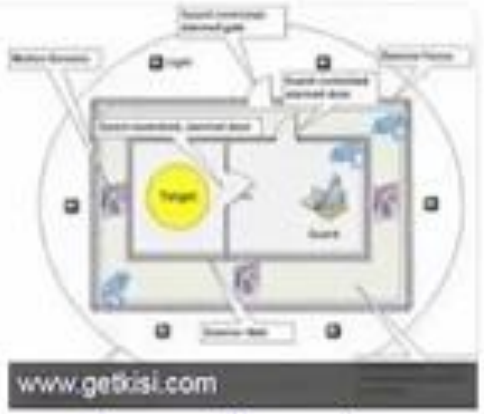
Google

intitle:"physical security"

All Images News Videos Books More Settings Tools

About 111,000 results (0.33 seconds)

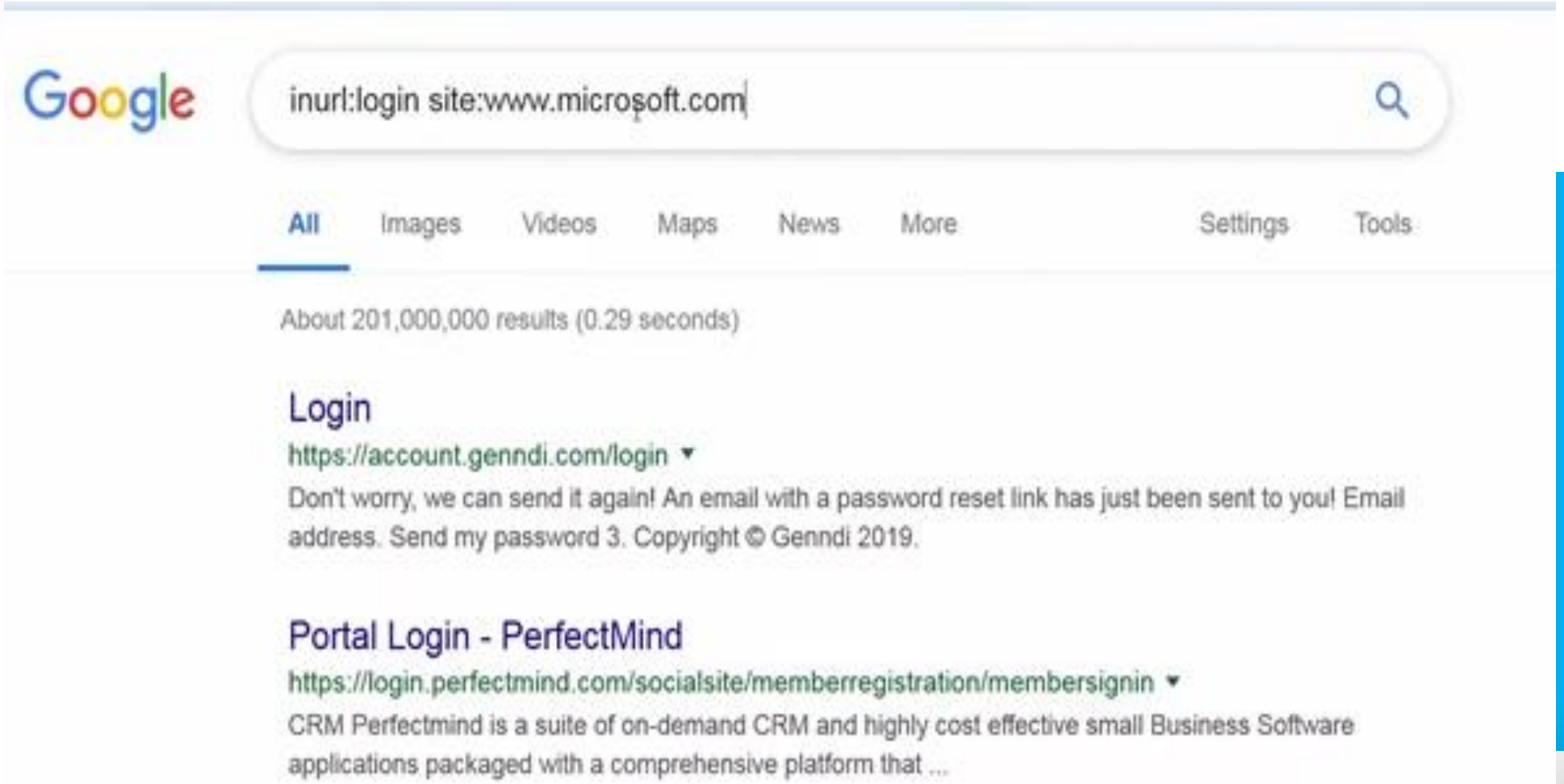
Physical security is the protection of personnel, hardware, software, networks and data from physical actions and events that could cause serious loss or damage to an enterprise, agency or institution. This includes protection from fire, flood, natural disasters, burglary, theft, vandalism and terrorism.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

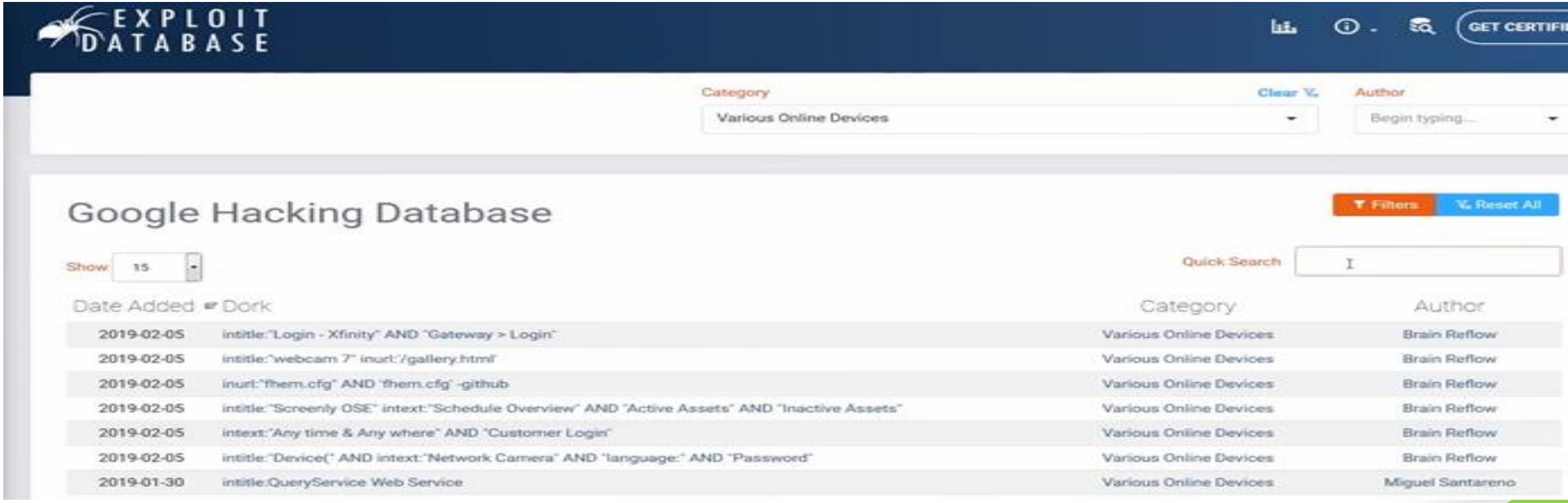


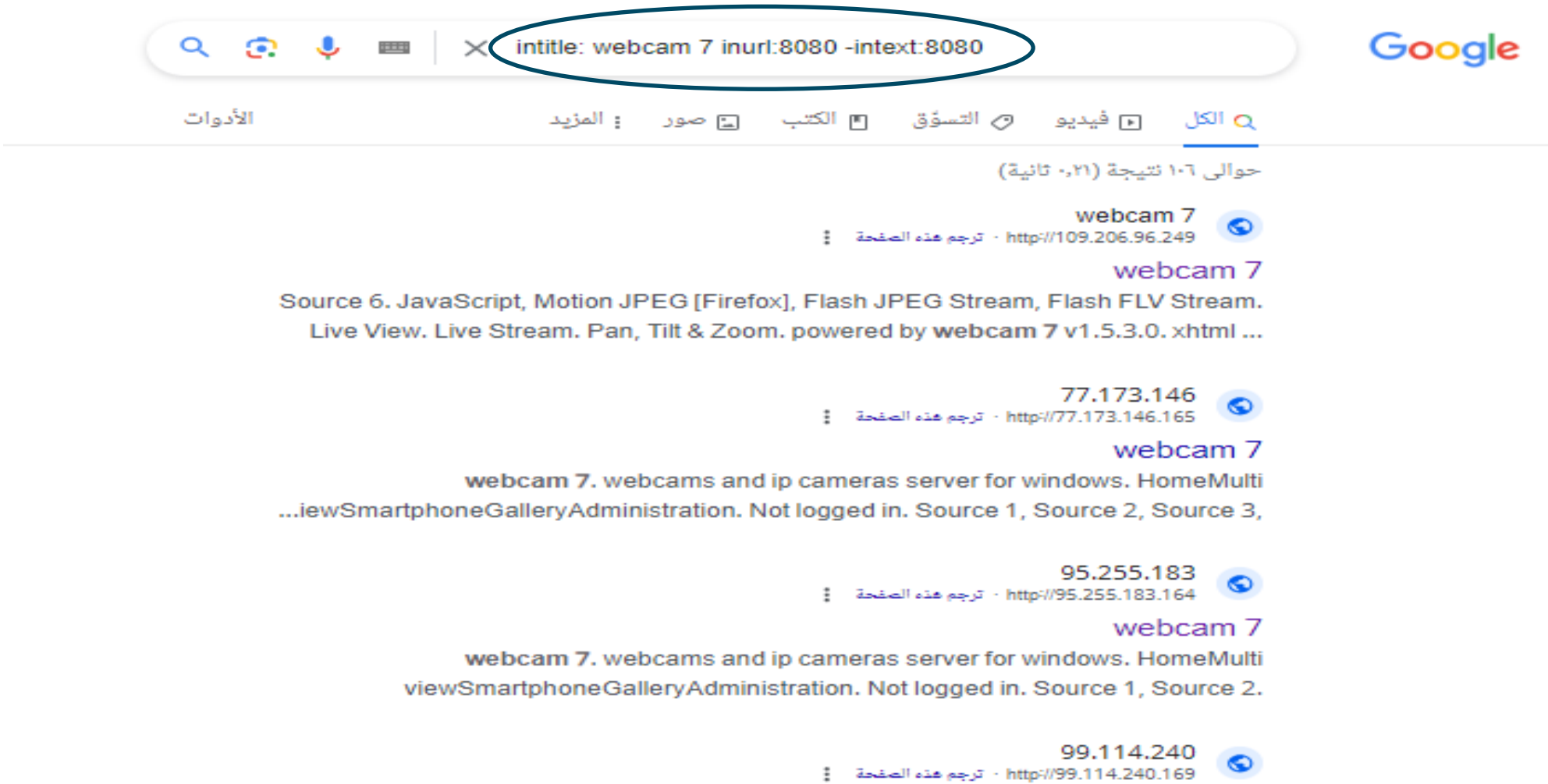
What is physical security? - Definition from WhatIs.com - SearchSecurity

https://searchsecurity.techtarget.com/definition/physical-security

About this result Feedback

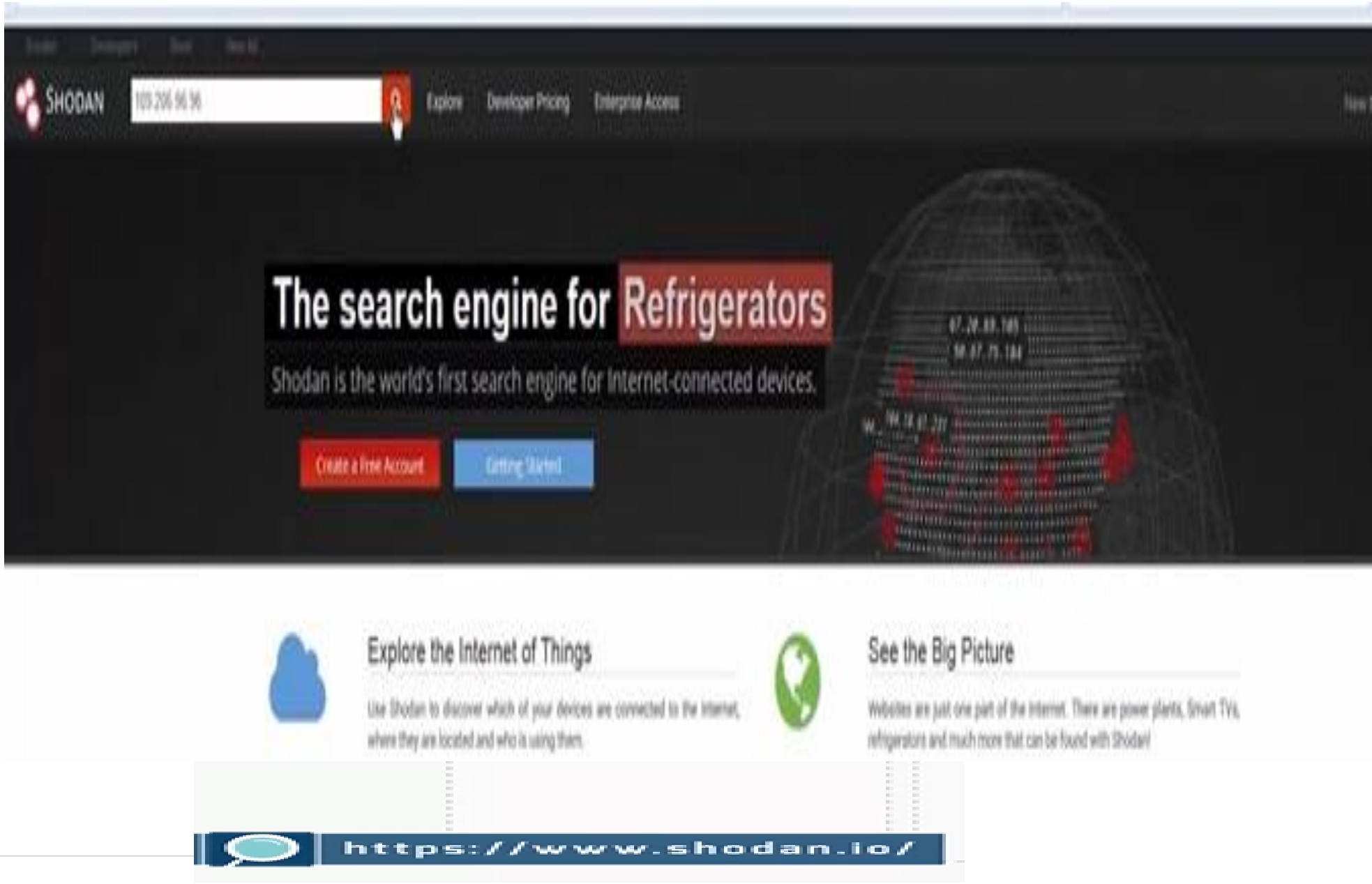

Google
inurl:login site:www.microsoft.com
All
Images
Videos
Maps
News
More
Settings
Tools
About 201,000,000 results (0.29 seconds)
Login
https://account.genndi.com/login
Don't worry, we can send it again! An email with a password reset link has just been sent to you! Email address. Send my password 3. 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
GET CERTIFI
Category
Various Online Devices
Clear
Author
Begin typing...
Google Hacking Database
Filters
Reset All
Show 15
Quick Search
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:"fhem.cfg" AND "fhem.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
Google
الكل
فيديو
التسوّق
الكتب
صور
المزيد
الأدوات
حوالى ١٠٦ نتيجة (٠٫٢١ ثانية)
webcam 7
http://109.206.96.249 · ترجم هذه الصفحة
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
http://77.173.146.165 · ترجم هذه الصفحة
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
http://95.255.183.164 · ترجم هذه الصفحة
webcam 7
webcam 7. webcams and ip cameras server for windows. HomeMulti viewSmartphoneGalleryAdministration. Not logged in. Source 1, Source 2.
99.114.240
http://99.114.240.169 · ترجم هذه الصفحة

Online devices

الأجهزة المتصلة بالنت

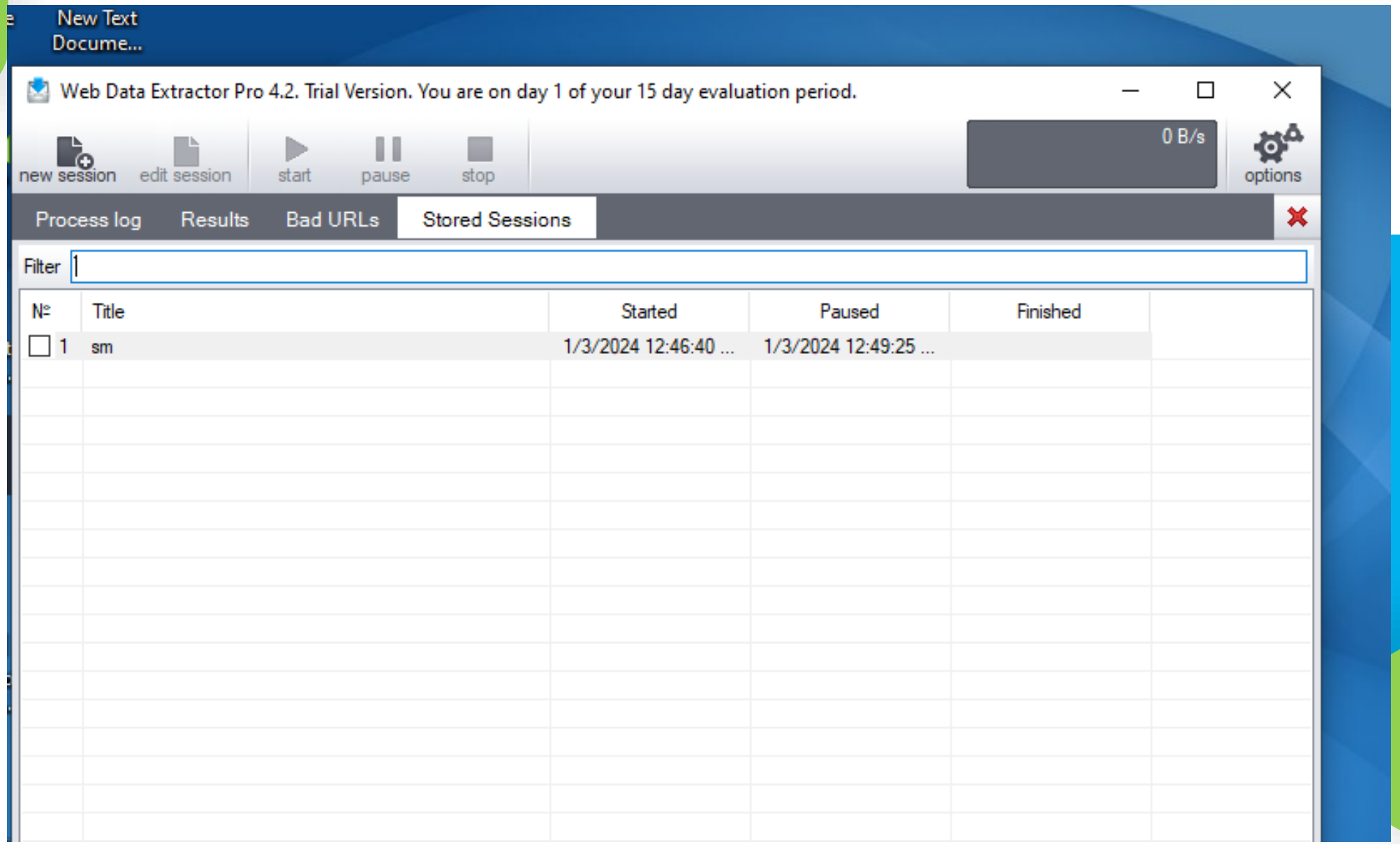


Website Reconnaissance Tools

أدوات استطلاع مواقع الويب

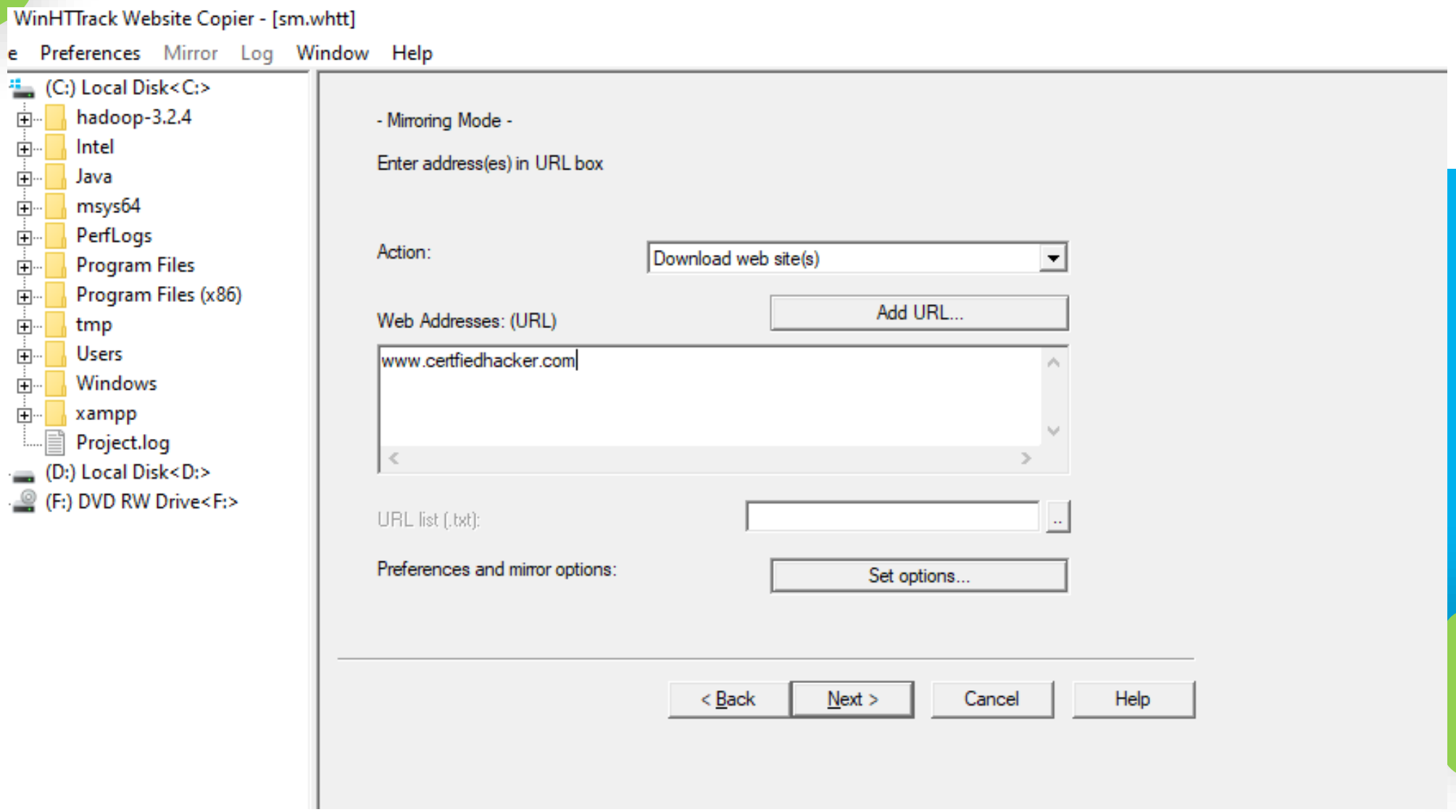
معهد العراب العالي للتدريب

تحميل اداة


New Text
Docume...
Web Data Extractor Pro 4.2. Trial Version. You are on day 1 of your 15 day evaluation period.
new session
edit session
start
pause
stop
0 B/s
options
Process log
Results
Bad URLs
Stored Sessions
Filter
№
Title
Started
Paused
Finished
1
sm
1/3/2024 12:46:40 ...
1/3/2024 12:49:25 ...

معهد العراب العالي للتدريب

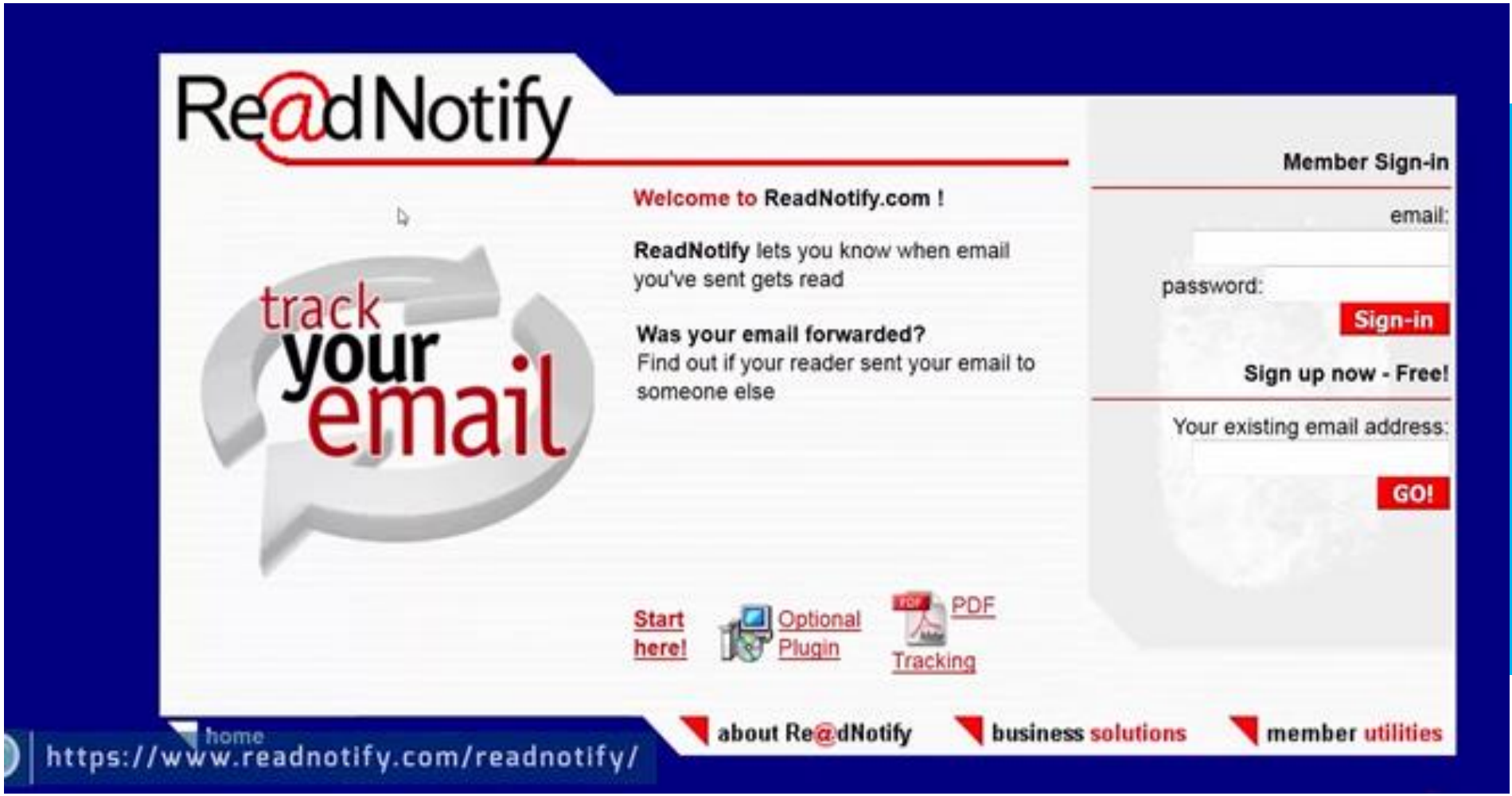
تحميل اداة


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

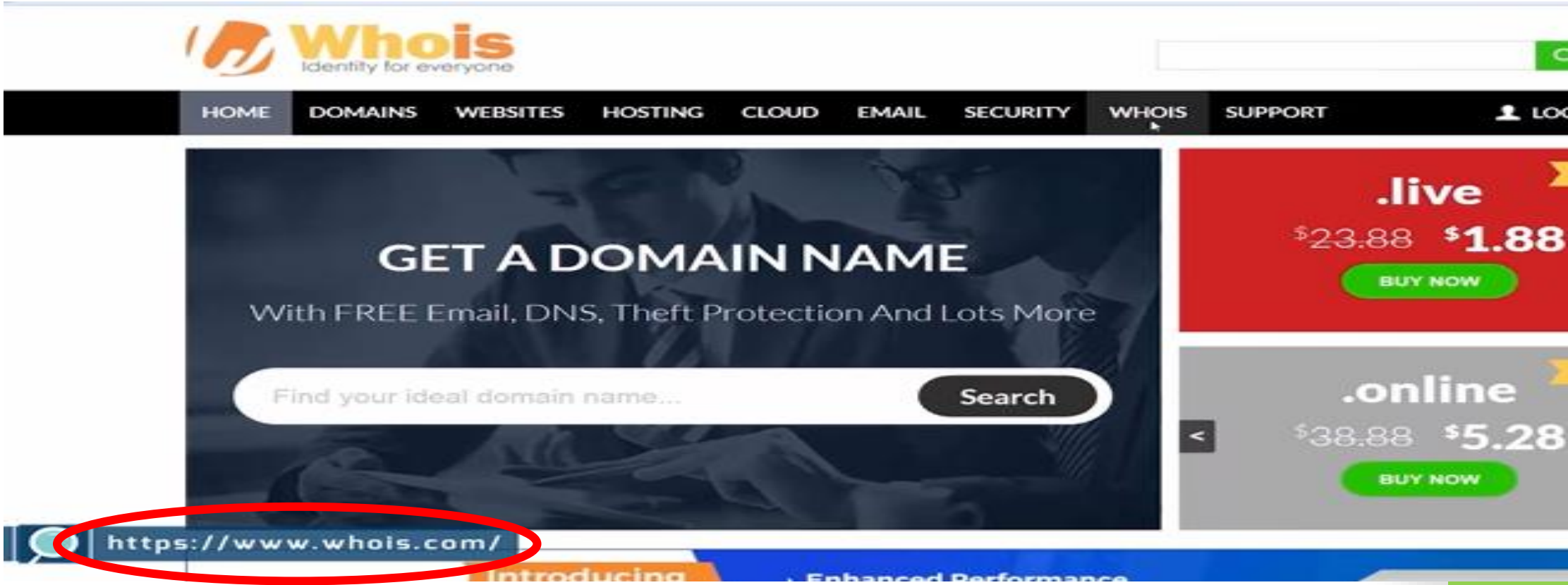


Domain reconnaissance tools

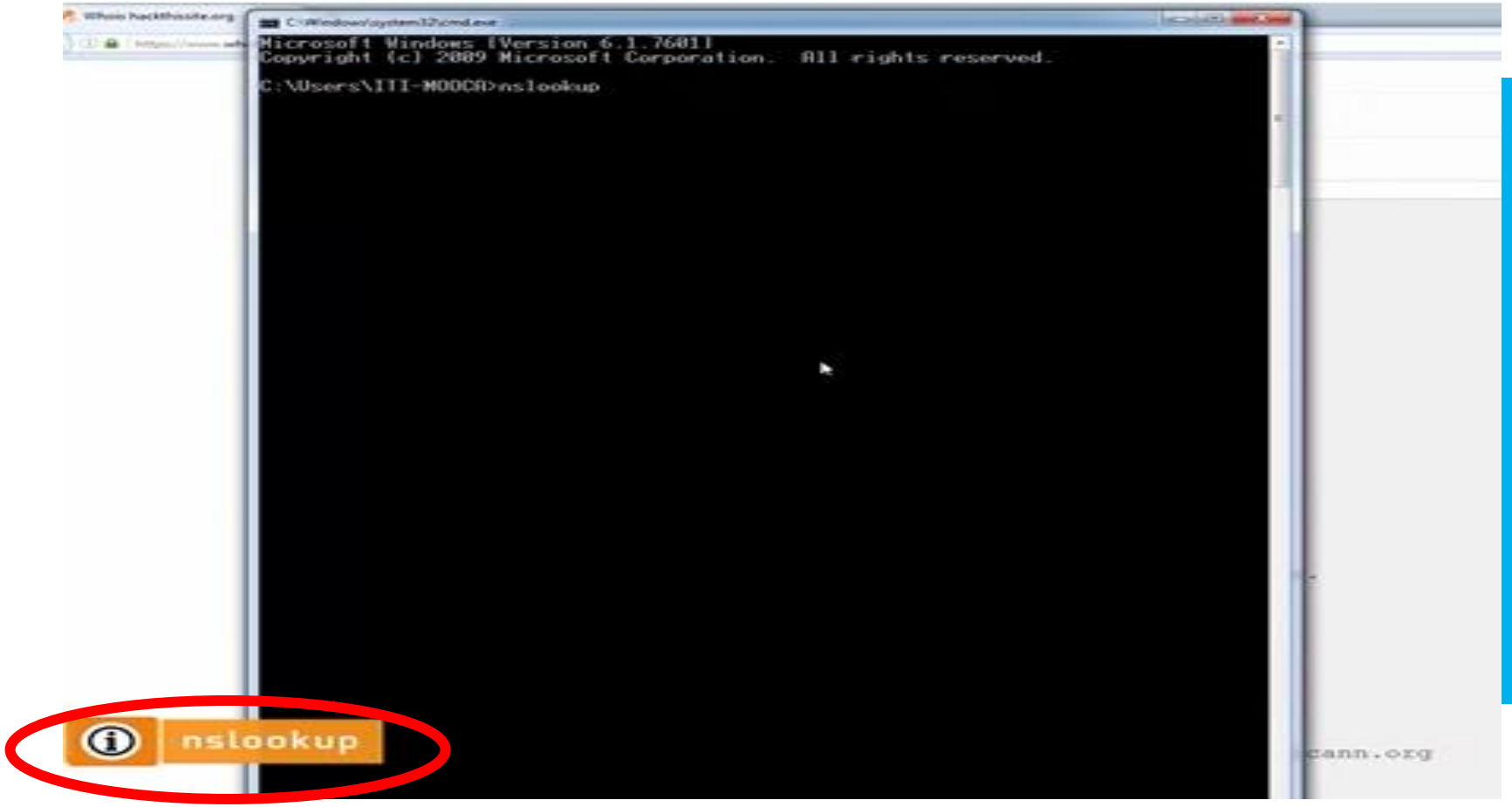
أدوات استطلاع المدى

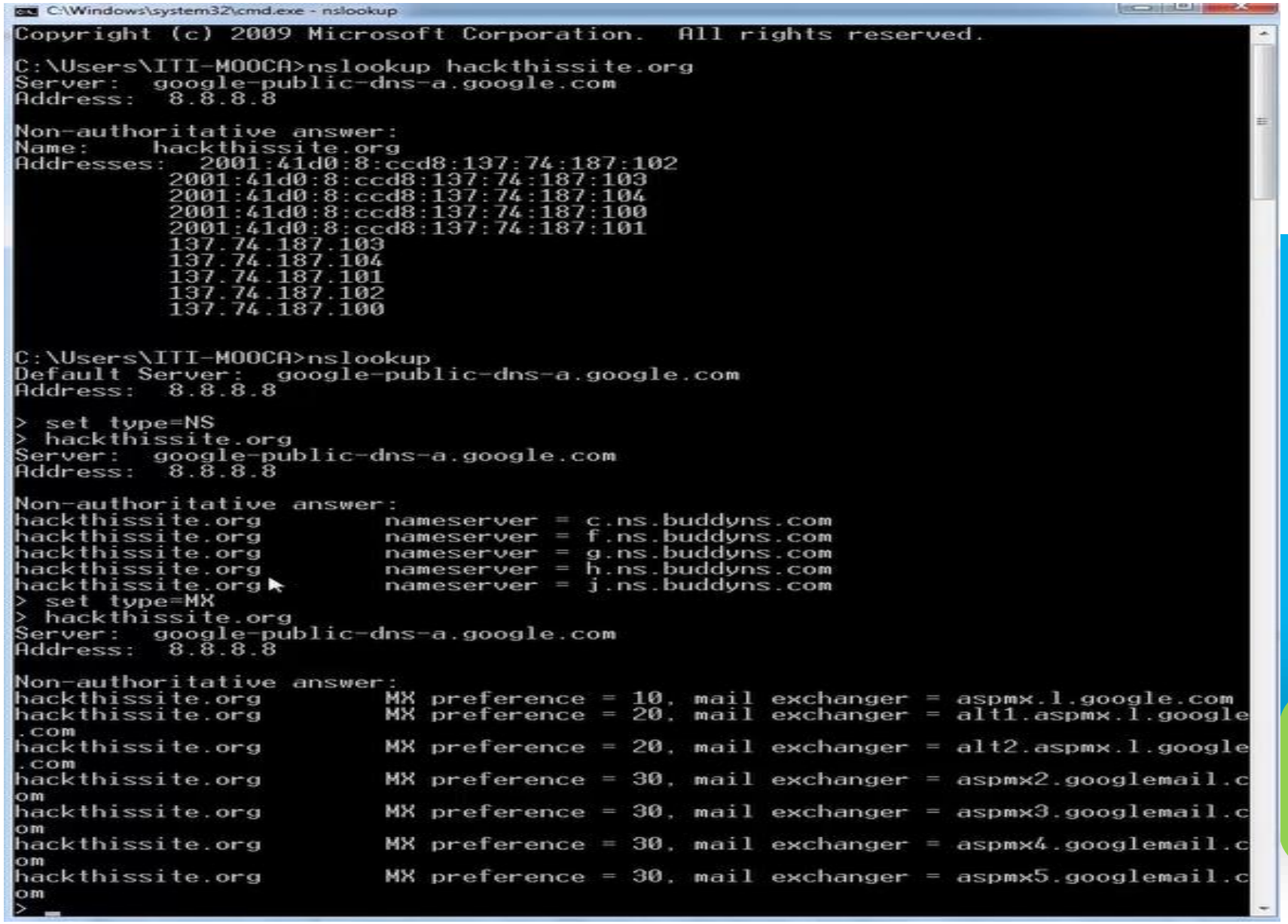
معهد العراب العالي للتدريب

دخول موقع



استخدام اداة




C:\Windows\system32\cmd.exe - nslookup
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Users\ITI-MOOCA>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-MOOCA>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 = aspmx.l.google.com
hackthissite.org MX preference = 20, mail exchanger = alt1.aspmx.l.google
.com
hackthissite.org MX preference = 20, mail exchanger = alt2.aspmx.l.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
>

معهد العراب العالي للتدريب

مراجعة سريعة

2023

النـهايـة

سؤال و إجابة

اول مرحله من مراحل عملية الاختراق.

A. الاستطلاع

B. التنفيذ

C. المسح

موقع لمعرفة معلومات عن ال domains.

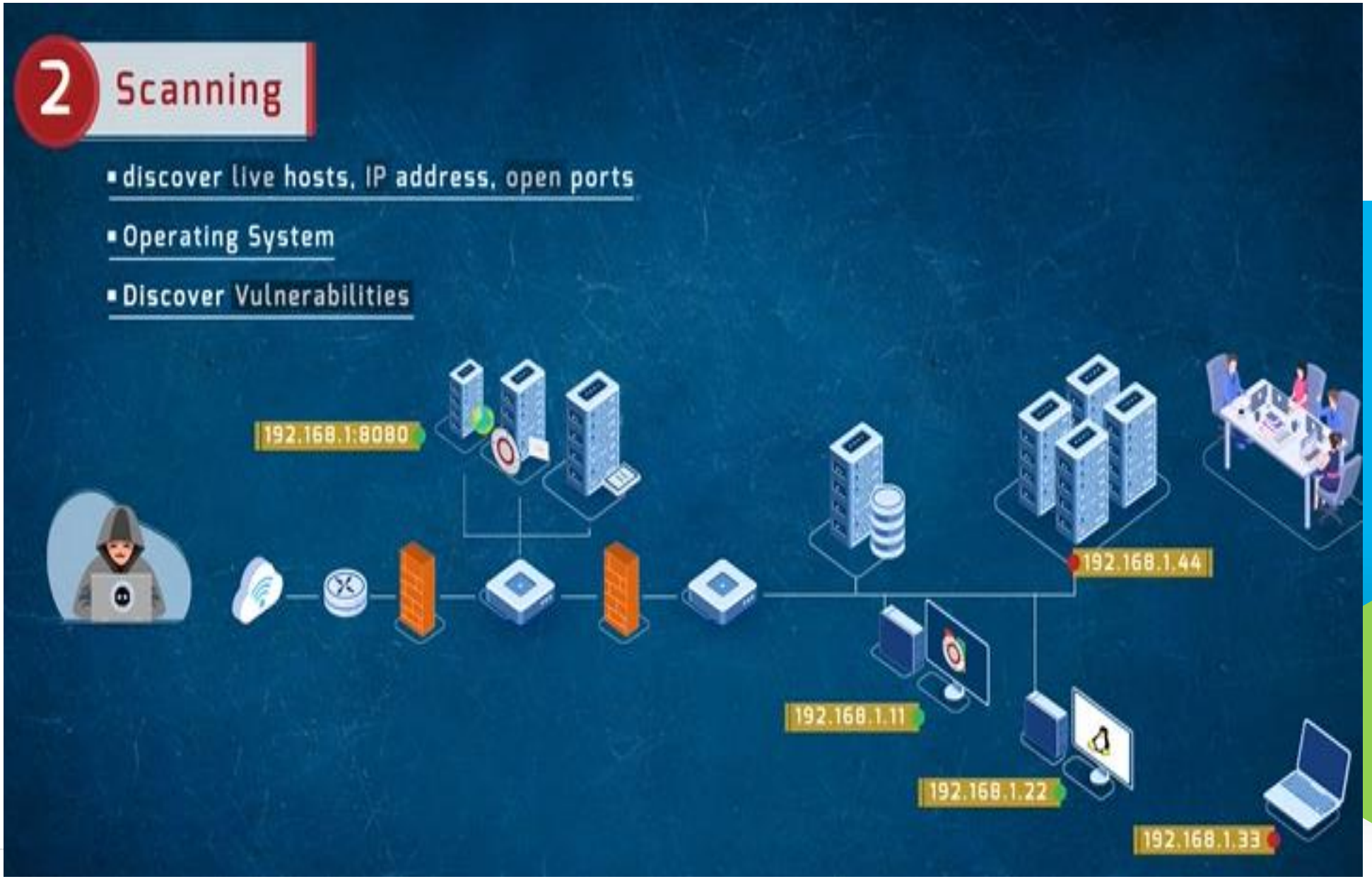
A. whois

B. httrack

معهد العراب العالي للتدريب

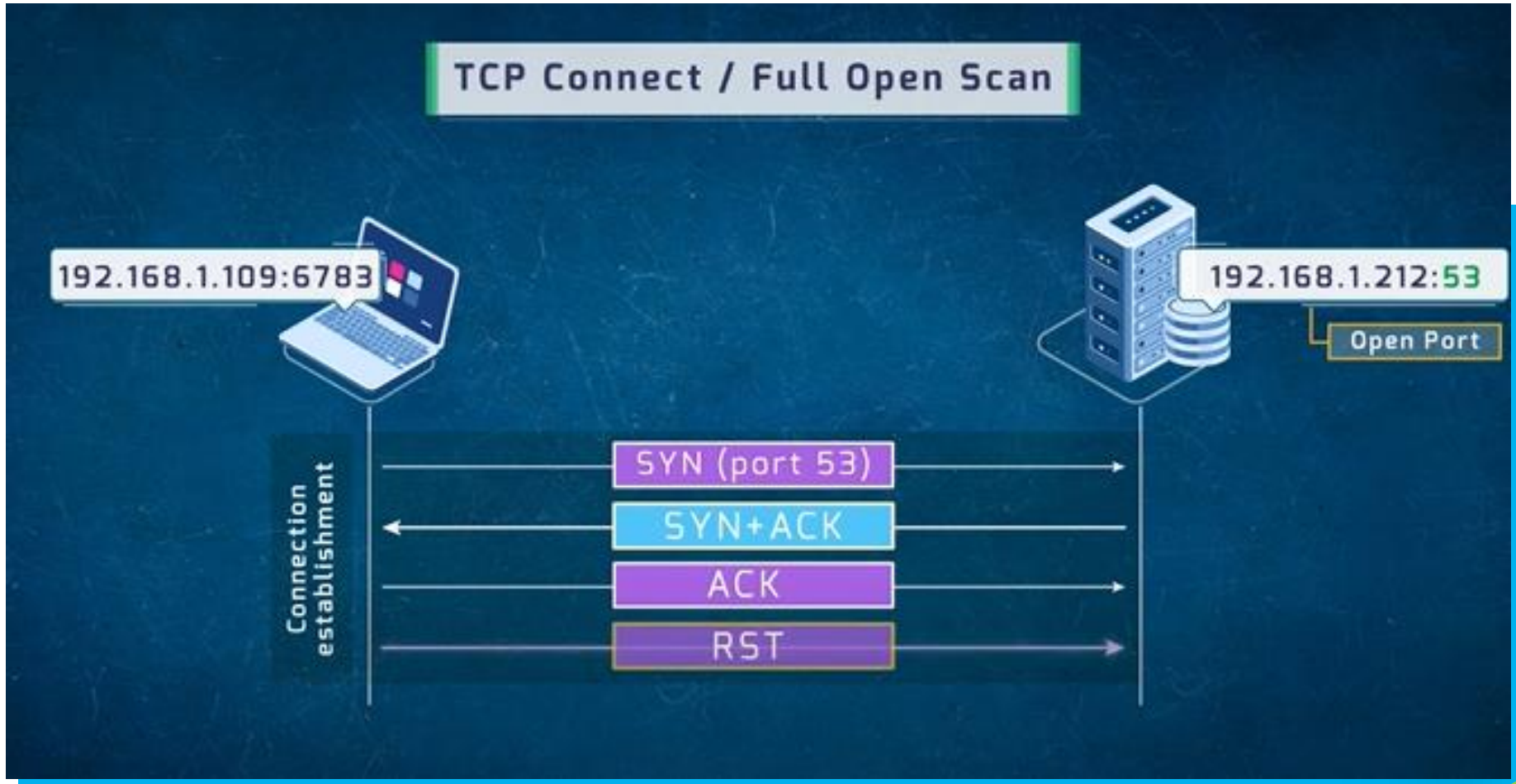
شكرا

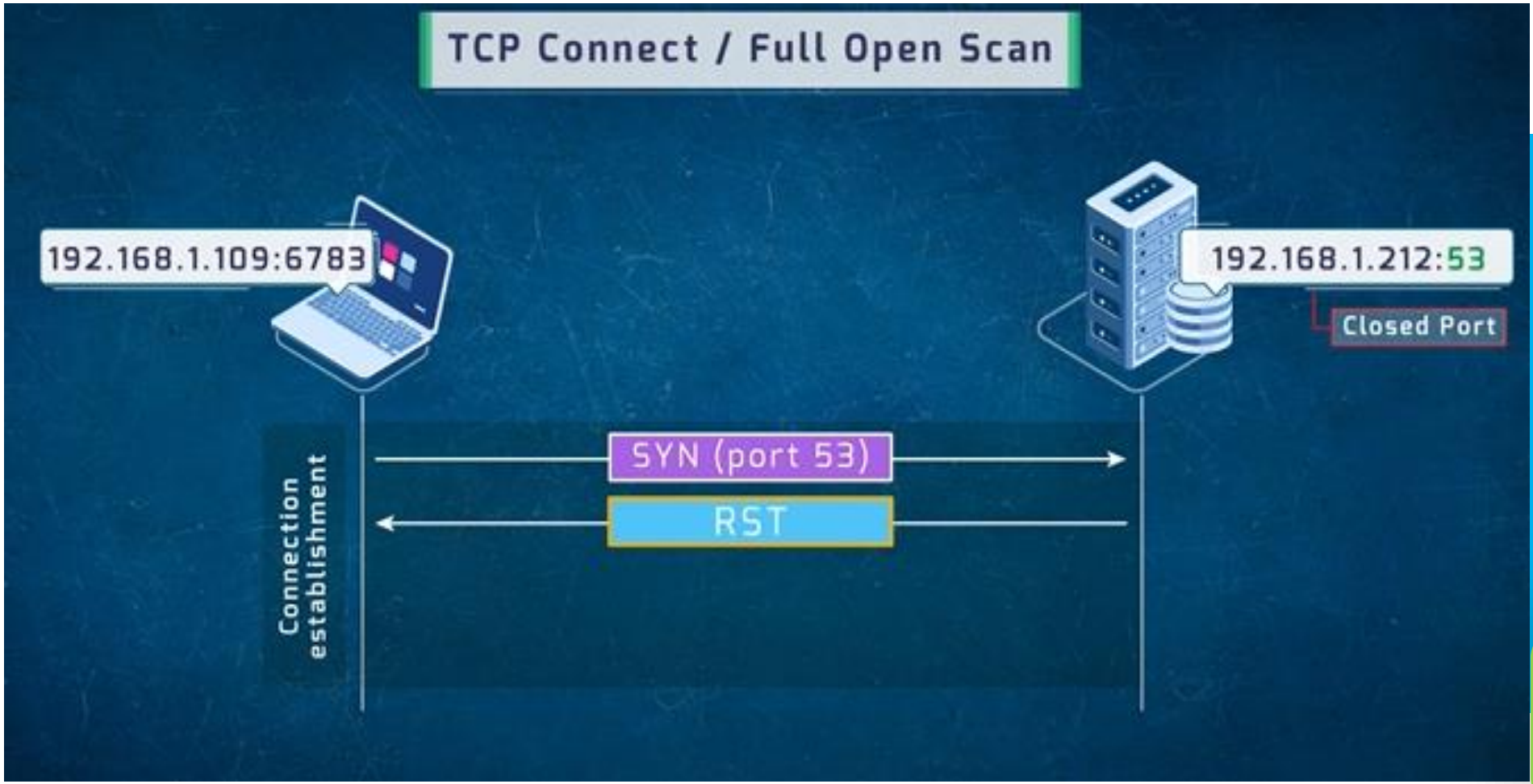

Clearing Tracks
5
1
Reconnaissance
Maintaining Access
4
2
Scanning
Hacking Phases
3


2 Scanning
discover live hosts, IP address, open ports
Operating System
Discover Vulnerabilities
192.168.1:8080
192.168.1.44
192.168.1.11
192.168.1.22
192.168.1.33

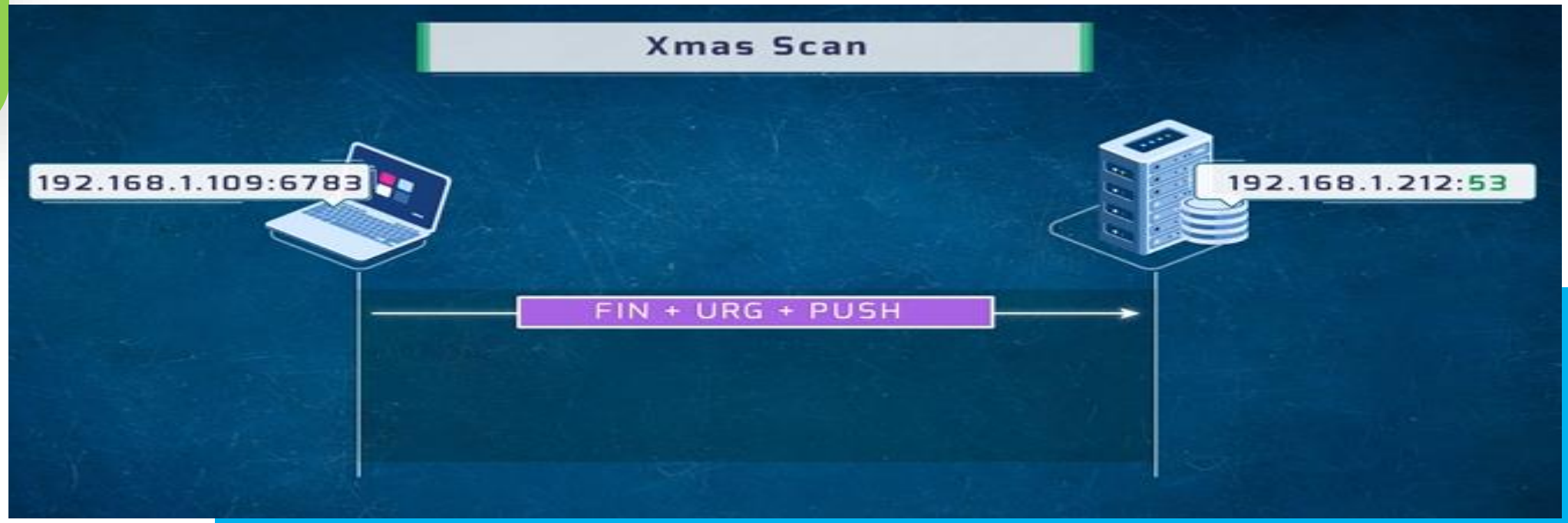
Port scanning

Flag	
SYN	بدايه الاتصال
ACK	انشاء الاتصال
PSH	ارسال البيانات
URG	طارئ
FIN	انهاء
RST	




TCP Connect / Full Open Scan
192.168.1.109:6783
192.168.1.212:53
Closed Port
SYN (port 53)
RST
Connection establishment


Stealth Scan / Half -Open Scan
192.168.1.109:6783
192.168.1.212:53
Closed Port
Connection establishment
SYN (port 53)
SYN+ACK

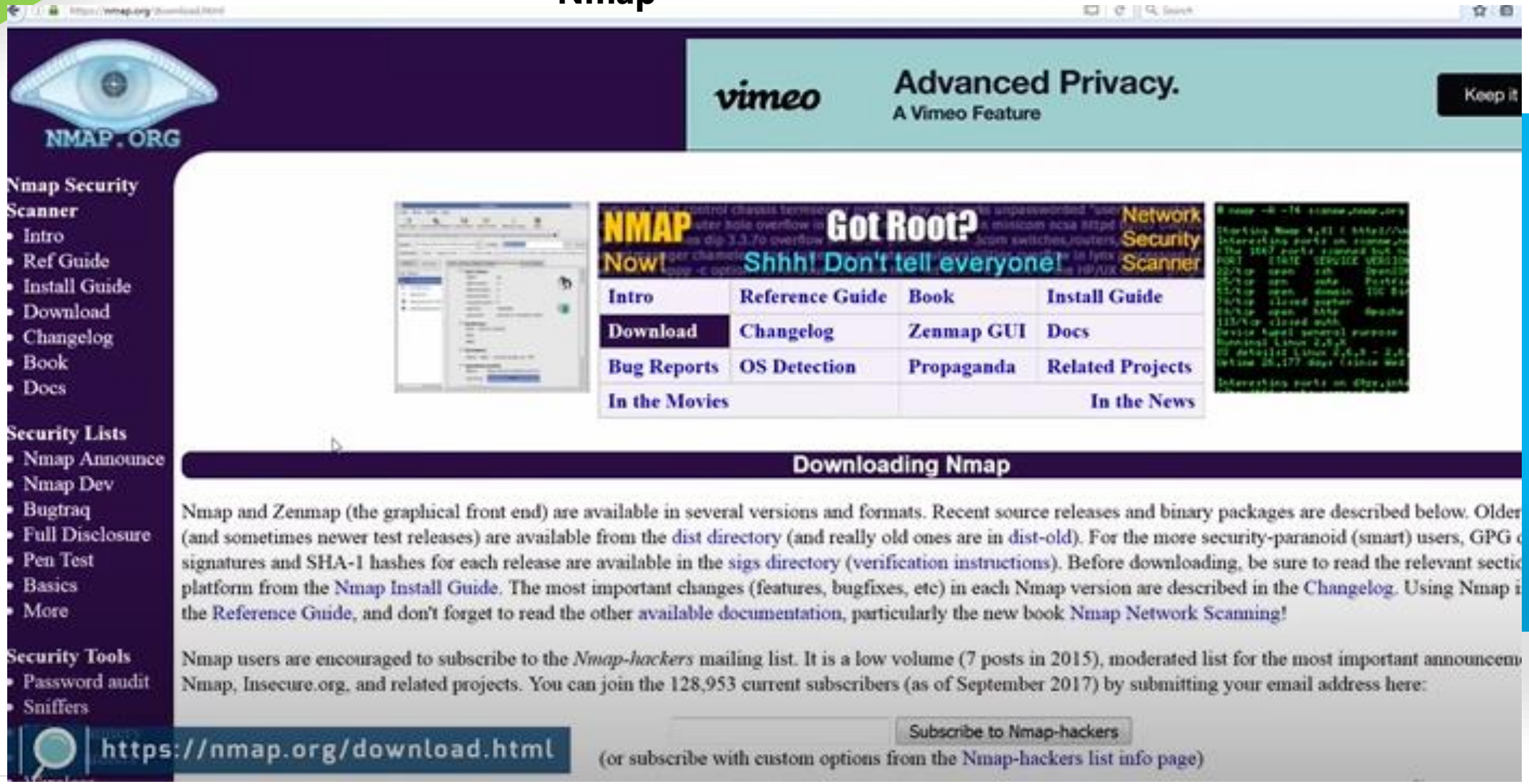

Xmas Scan
192.168.1.109:6783
192.168.1.212:53
FIN + URG + PUSH


192.168.1.109:6783
192.168.1.212:53
FIN + URG + PUSH
No Response


192.168.1.109:6783
192.168.1.212:53
Closed Port
FIN + URG + PUSH
RST

Port scanning

Nmap



الهندسة الاجتماعية

انتحال الشخصية

التجسس

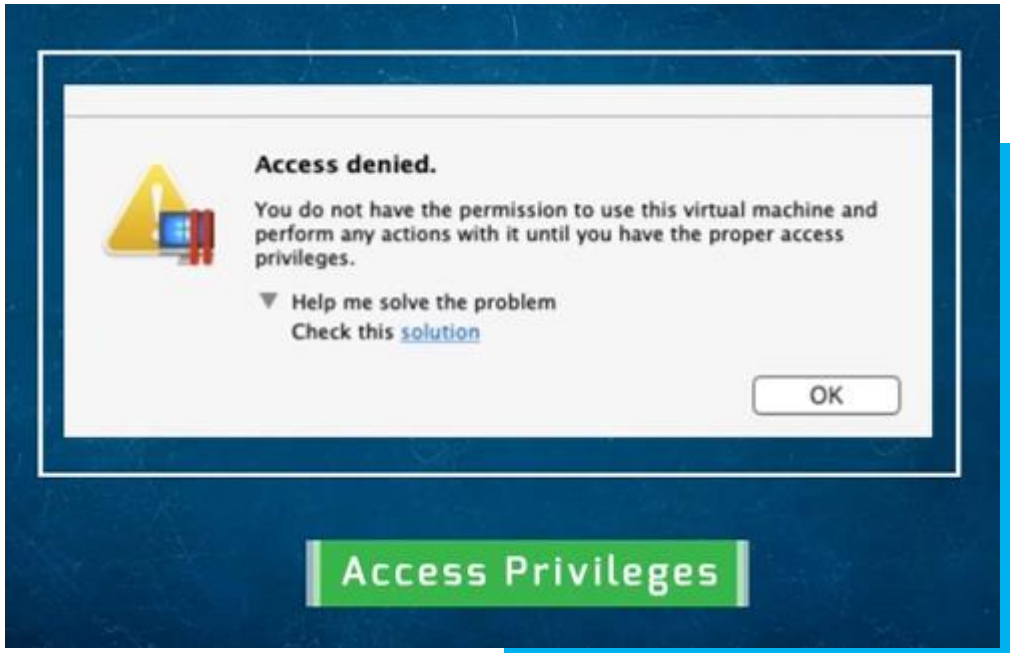

Human- based
Shoulder Surfing


Human- based
Dumpster Diving


Computer-based
PayPal
Buy
Sell
Send
Business
Join more than 6 million Australians shopping with PayPal.
How PayPal Works
Why PayPal?
Shop
Phishing


Mobile-based
For you
Top charts
Premium
SCRABBLE GO
Install
Explore recommended games
PUBG MOBILE - Mad Miramar
Games
Apps
Movies
Books

الحلول



تحديد الصلاحيات

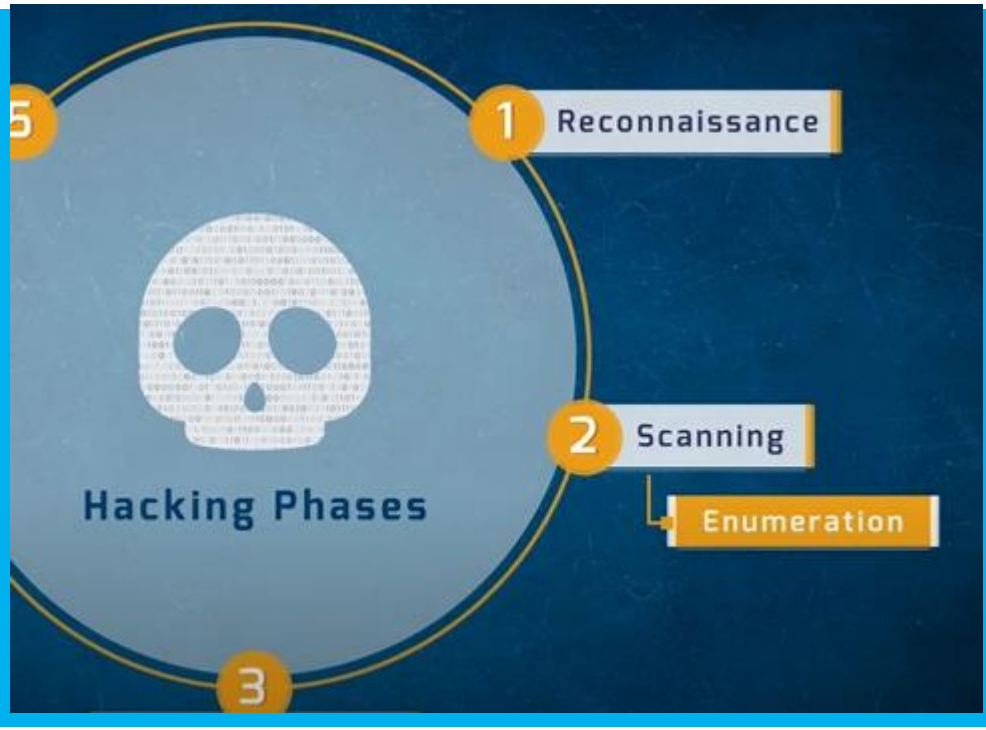
التدريب

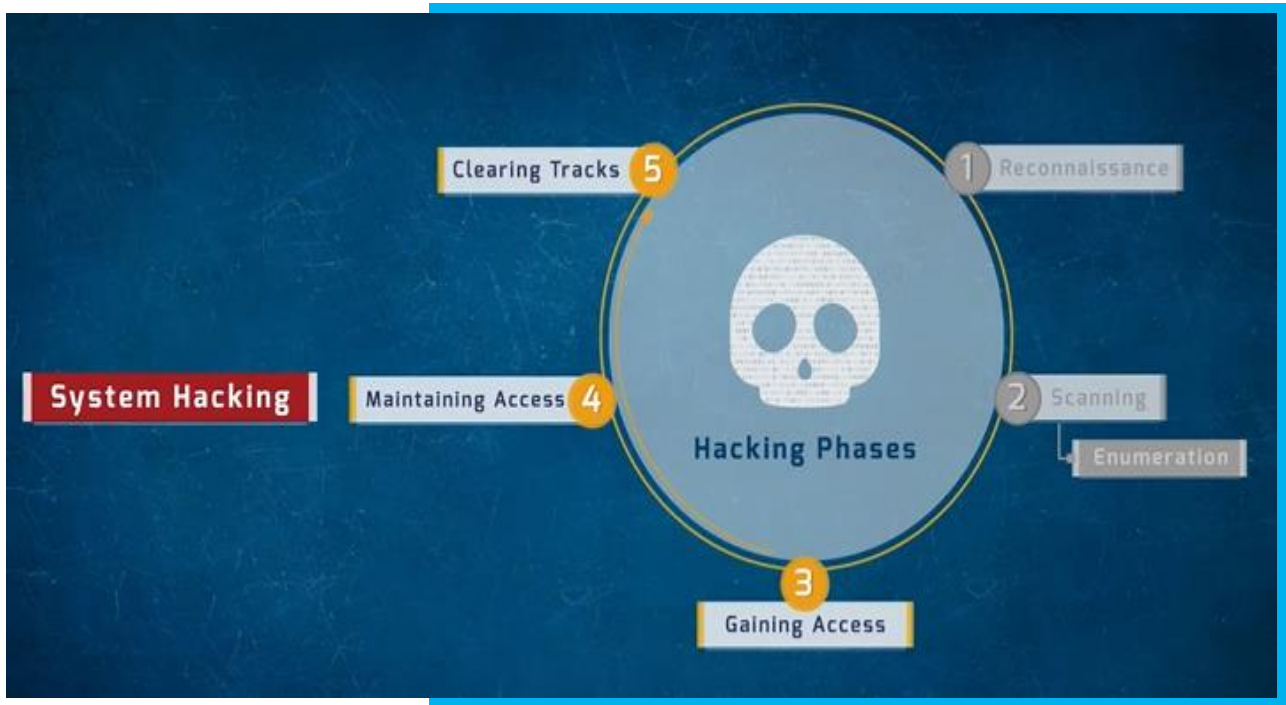
Enumeration

هي جزء من مرحلة المسح

يتم الوصول الى:

User name
User groups
passwords



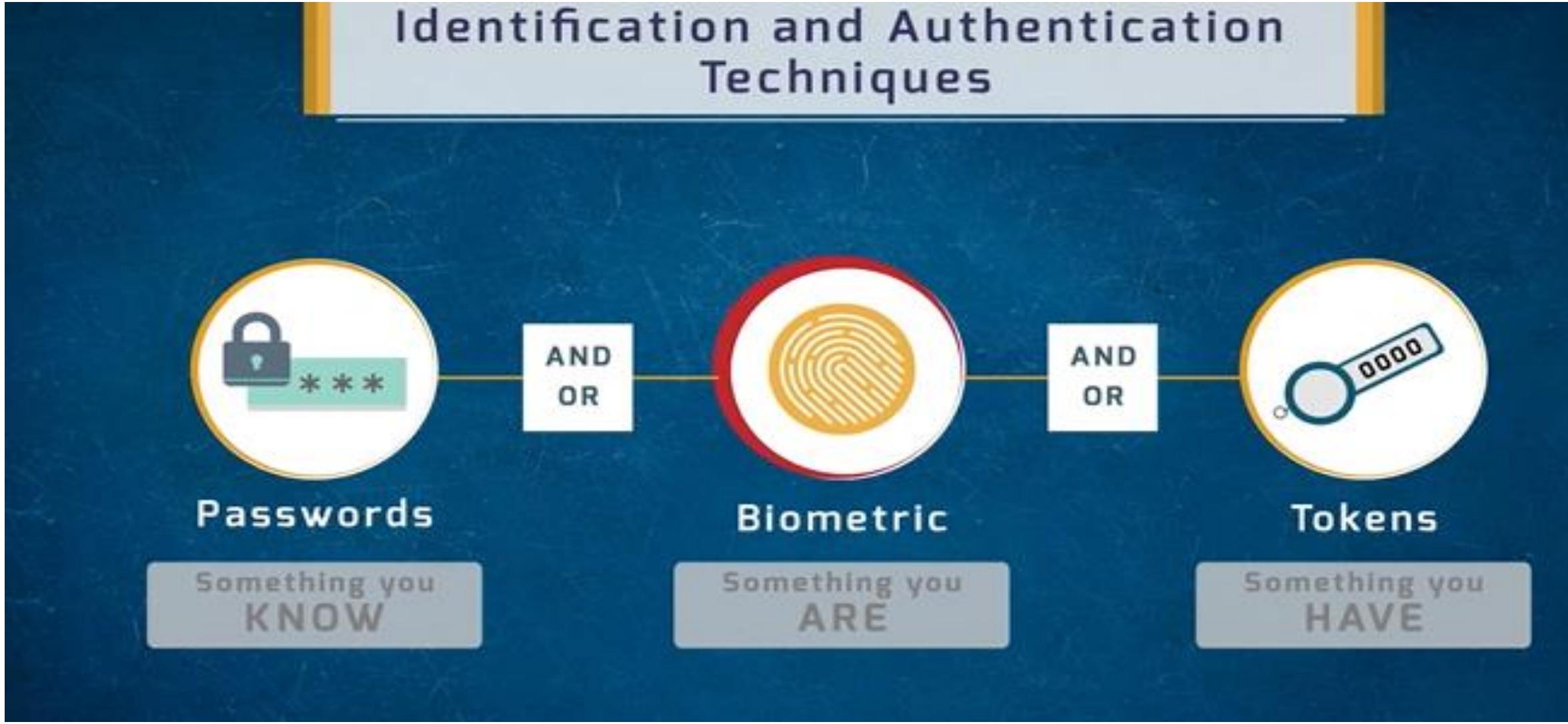


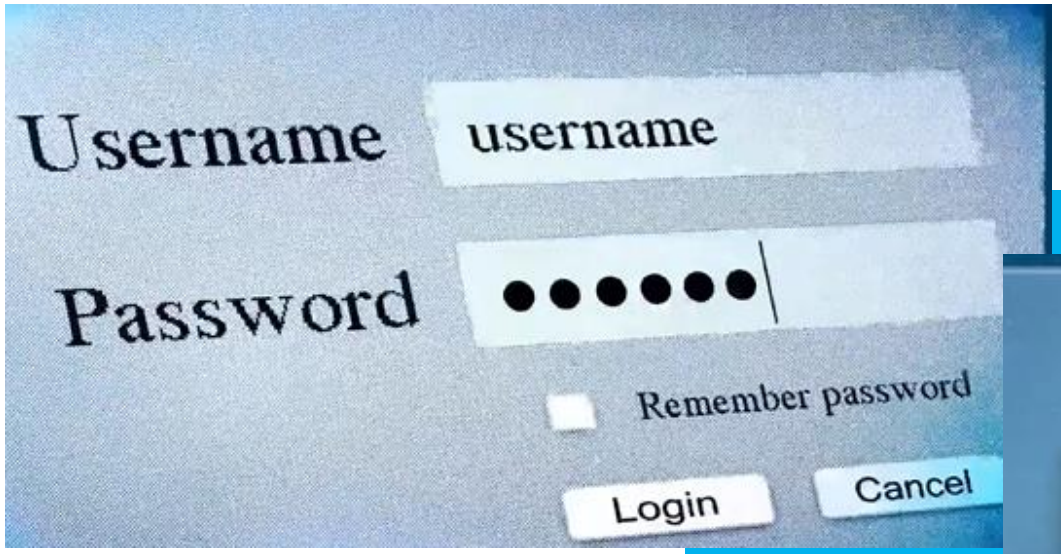
من خلال:

System hacking

Password cracking

تقنيات الاذونات والصلاحيات

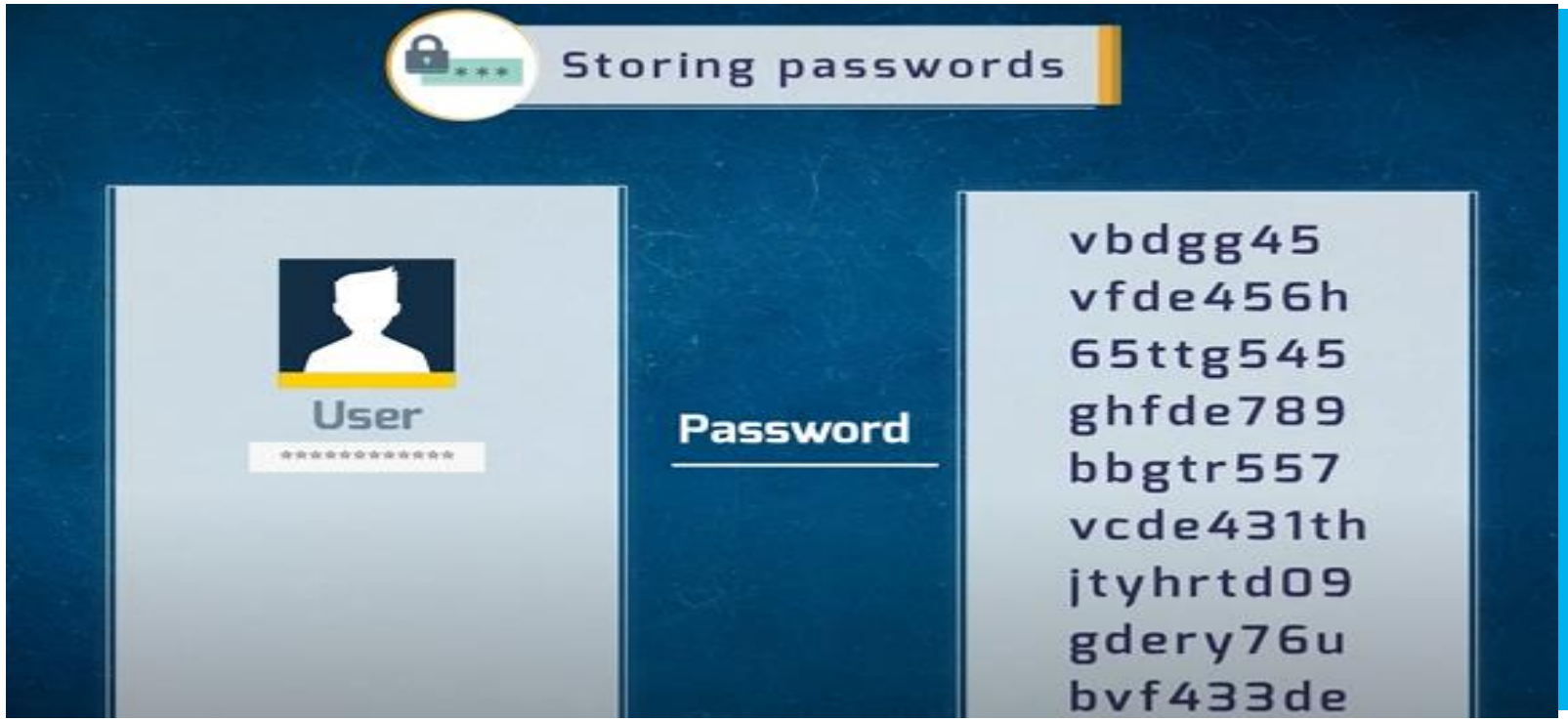



Username
username
Password
Remember password
Login
Cancel

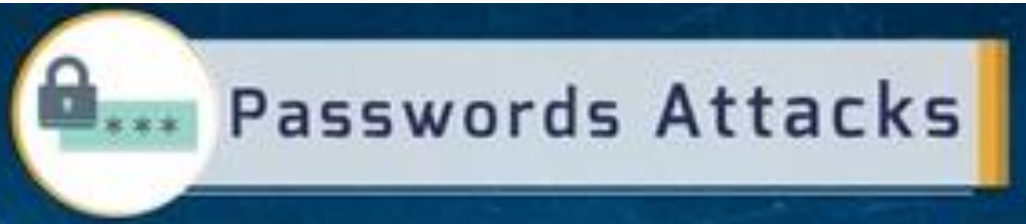

User name:
john_smith
Password:
PASSCODE:
Log On
54392971
CRYPTOCard

أنواع كلمات المرور

دالة الهاش Hash



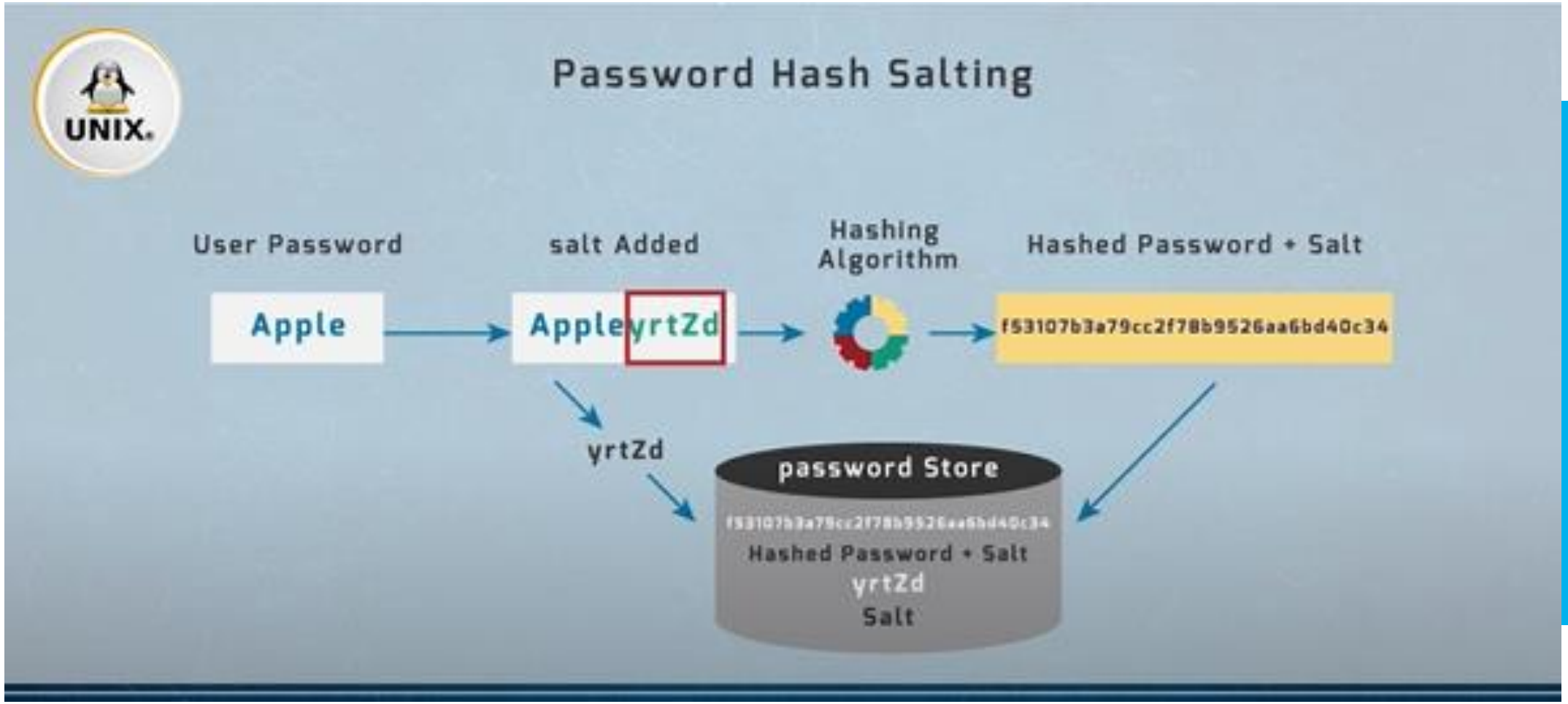
هجمات كلمات المرور



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

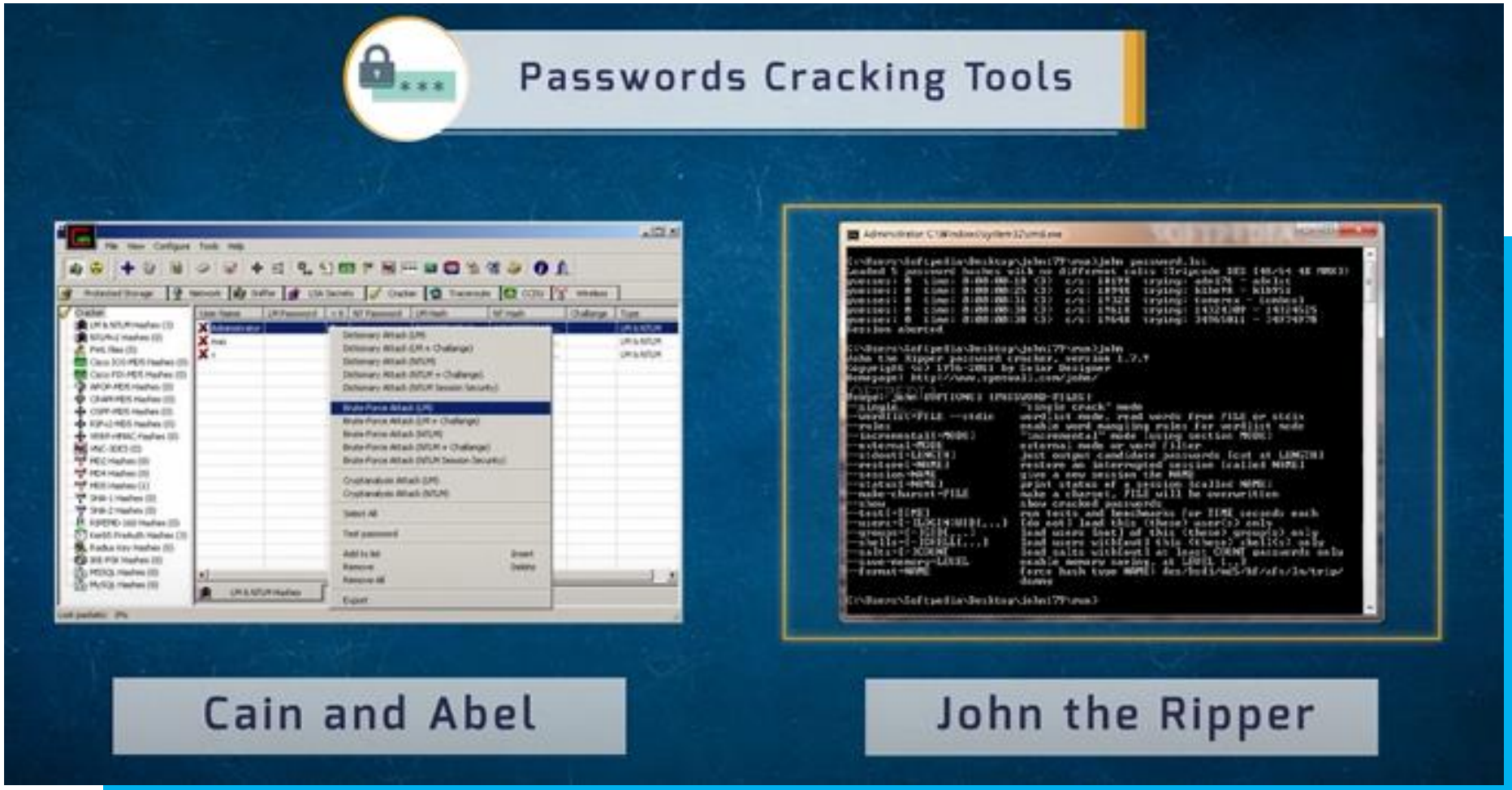
الحماية

إضافة على كلمه المرور قبل دخولها دالة الهاش



زيادة امان كلمة المرور

أدوات كسر كلمة المرور



معهد العراب العالي للتدريب

مراجعة سريعة

القرصنة الاخلاقية

2023

النهاية

سؤال و إجابة

الهندسة الاجتماعية من وسائلها:

1. التصيد
2. التجسس
3. جميع ما سبق

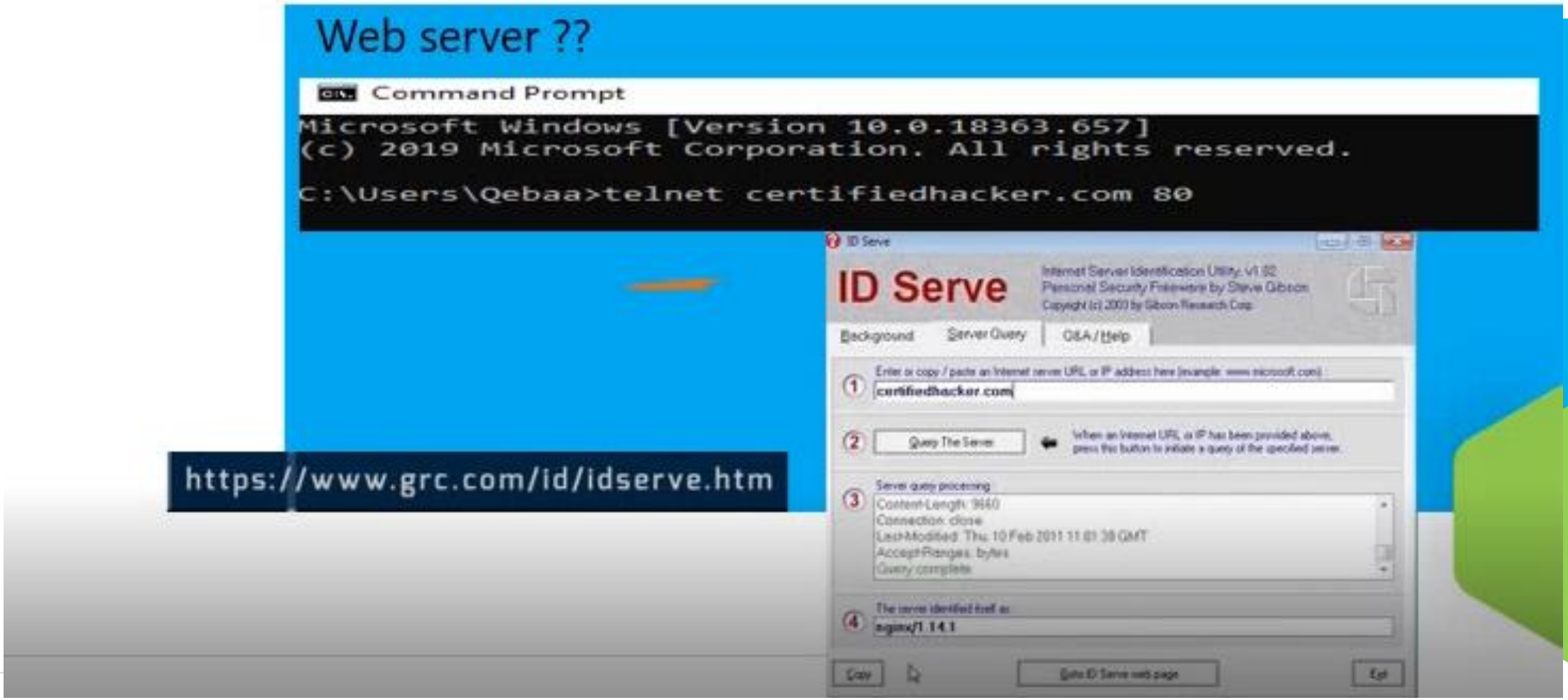
رساله ACK تكون ل :

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

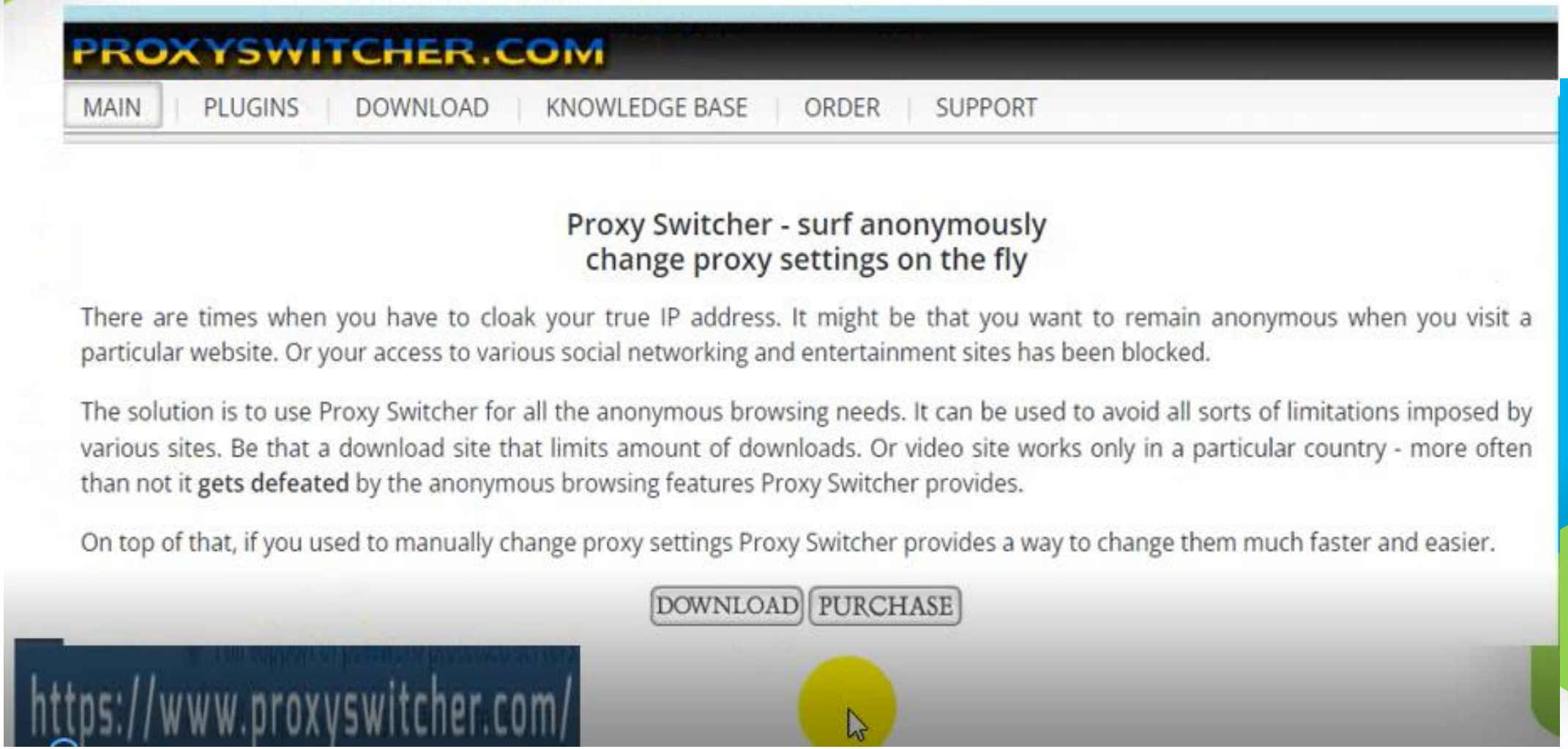
معهد العراب العالي للتدريب

شكرا

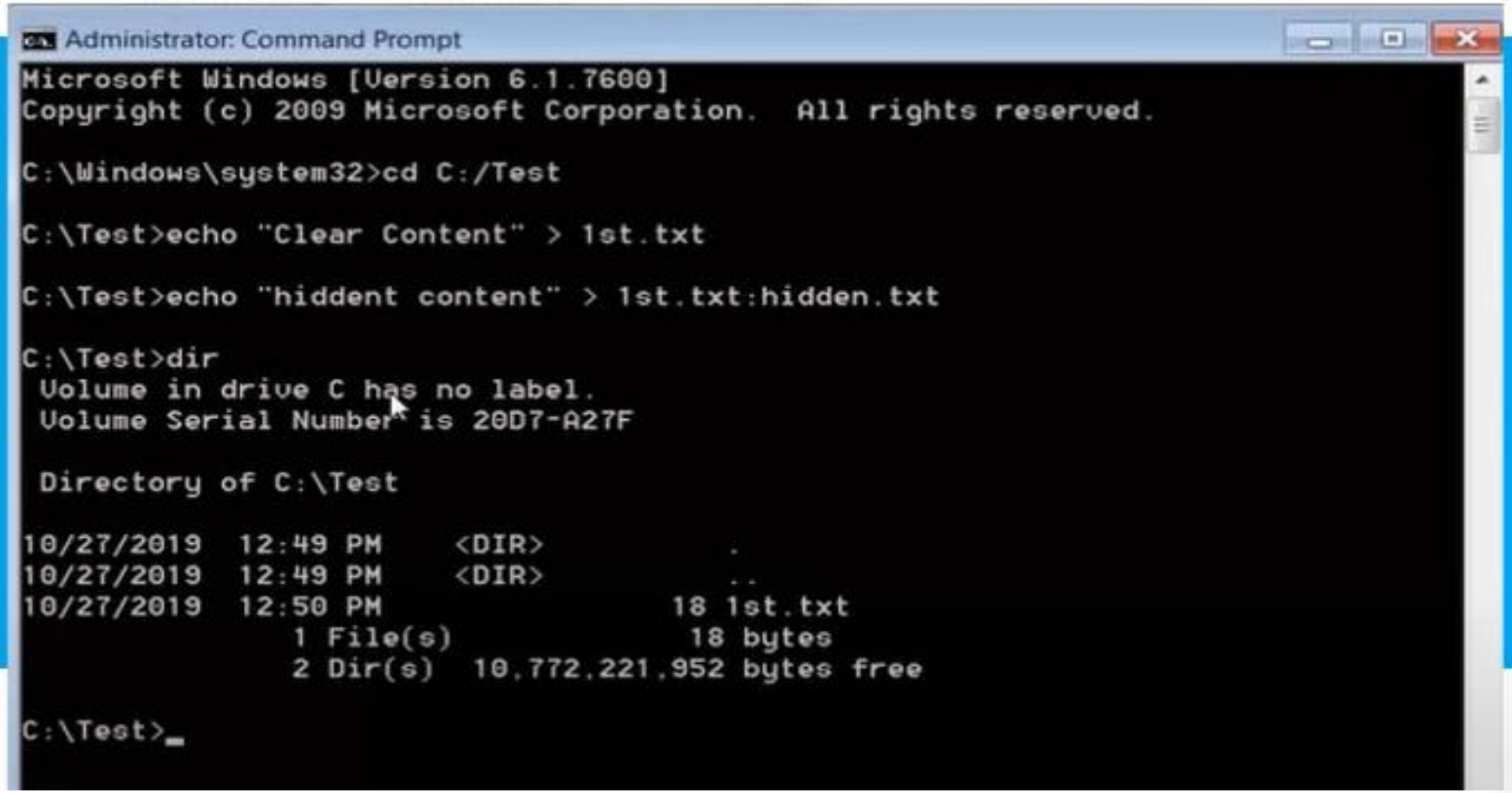
مسح الشبكات


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
ID Serve
Internet Server Identification Utility, v1.02
Personal Security Freeware by Steve Gibson
Copyright (c) 2000 by Gibson Research Corp.
Background
Server Query
Q&A / Help
Enter or copy / paste an Internet server URL or IP address here (example: www.microsoft.com)
certifiedhacker.com
Query The Server
When an Internet URL or IP has been provided above, press this button to initiate a query of the specified server.
Server query processing
Content-Length: 9660
Connection: close
Last-Modified: Thu, 10 Feb 2011 11:01:38 GMT
Accept-Ranges: bytes
Query complete
The server identified itself as:
nginx/1.14.1
Copy
Goto ID Serve web page
Exit

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



معهد العراب العالي للتدريب

مراجعة سريعة

القرصنة الاخلاقية

2023

النهاية

معهد العراب العالي للتدريب

شكرا