معهد قوى الإنجاز العالي للتدريب

أختبار الاختراق

PENETRATION TESTING

م.خالد الزيداني

Date

Time

المحاور

- المقدمة أختبار الاختراق
- أنواع أختبار الأختراق
- مرحلة للاستطلاع Reconnaissance
- .....

معهد قوى الإنجاز العالي للتدريب
THE FORCES OF ACHIEVEMENT FOR HIGHER TRAINING

المقدمة اختبار الاختراق

نهدف إلى تأهيل المتدرب ليصبح لدية مهارة قوية في أختبار اختراق، قادرًا على فحص و اكتشاف الثغرات الأمنية وتقييم أمان الأنظمة باستخدام أدوات وتقنيات احترافية.

معهد قوى الإنجاز العالي للتدريب
THE FORCES OF ACHIEVEMENT FOR HIGHER TRAINING

المقدمة اختبار الاختراق

هو محاكاة هجوم حقيقي على الأنظمة بهدف **اكتشاف الثغرات** ومعالجتها قبل أن يستغلها المهاجمون.

الفرق بين اختبار الاختراق والهجوم الحقيقي

- الاختبار الأخلاقي : يتم بإذن رسمي ، يهدف للتحسين، يتم توثيقه
- الهجوم الخبيث : يتم بدون إذن ، يهدف للتدمير أو السرقة، غير موثق

هناك طريقتان رئيسيتان لاجراء اختبار الحماية:

استخدام أداة اختبار : هناك العديد من أدوات اختبار الحماية من هجمات الشبكات للشراء أو الاستخدام المجاني .يمكن لهذه الأدوات مسح شبكتك بحثا عن الثغرات الأمنية وتقييم فعالية ضمانات الأمان الخاصة بك.

توظيف خبير أمان :إذا لم تكن لديك خبرة في اختبار الحماية من هجمات الشبكات اللاسلكية، يمكنك توظيف خبير أمان لإجراء الاختبار نيابة عنك .يمكن لخبير الأمان أن يقدم لك أيضا توصيات لتحسين الأمان.

لماذا نحتاج اختبار الاختراق؟

- اكتشاف الثغرات الأمنية.
- تقييم الاستجابة للهجمات.
- تعزيز أمان الأنظمة.

أنواع اختبار الاختراق

- Black Box : بدون معرفة مسبقة عن النظام
- White Box: معرفة كاملة بالكود أو البنية. مثل ماذا ؟
- Gray Box :معرفة جزئية بالمكونات الداخلية

مراحل اختبار الاختراق

١. التخطيط والاستطلاع Reconnaissance
٢. المسح والتحليل Scanning & Enumeration
٣. الاحتفاظ بالوصول Post-Exploitation
٤. التغطية والإخفاء Covering Tracks
٥. إعداد التقرير

معهد قوى الإنجاز العالي للتدريب
THE FORCES OF ACHIEVEMENT FOR HIGHER TRAINING

التخطيط والاستطلاع Reconnaissance

جمع أكبر قدر ممكن من المعلومات عن الهدف

- دون التفاعل المباشر معه ⟸ استطلاع سلبي passive
- تفاعل بسيط ومحدود ⟸ استطلاع نشط active

معهد قوى الإنجاز العالي للتدريب
THE FORCES OF ACHIEVEMENT FOR HIGHER TRAINING

أهداف الاستطلاع:

١- تحديد أسماء النطاقات Domains

اسم النطاق الرئيسي الذي يُستخدم للدخول على موقع إلكتروني

معهد قوى الإنجاز العالي للتدريب
THE FORCES OF ACHIEVEMENT FOR HIGHER TRAINING

أهداف الاستطلاع:

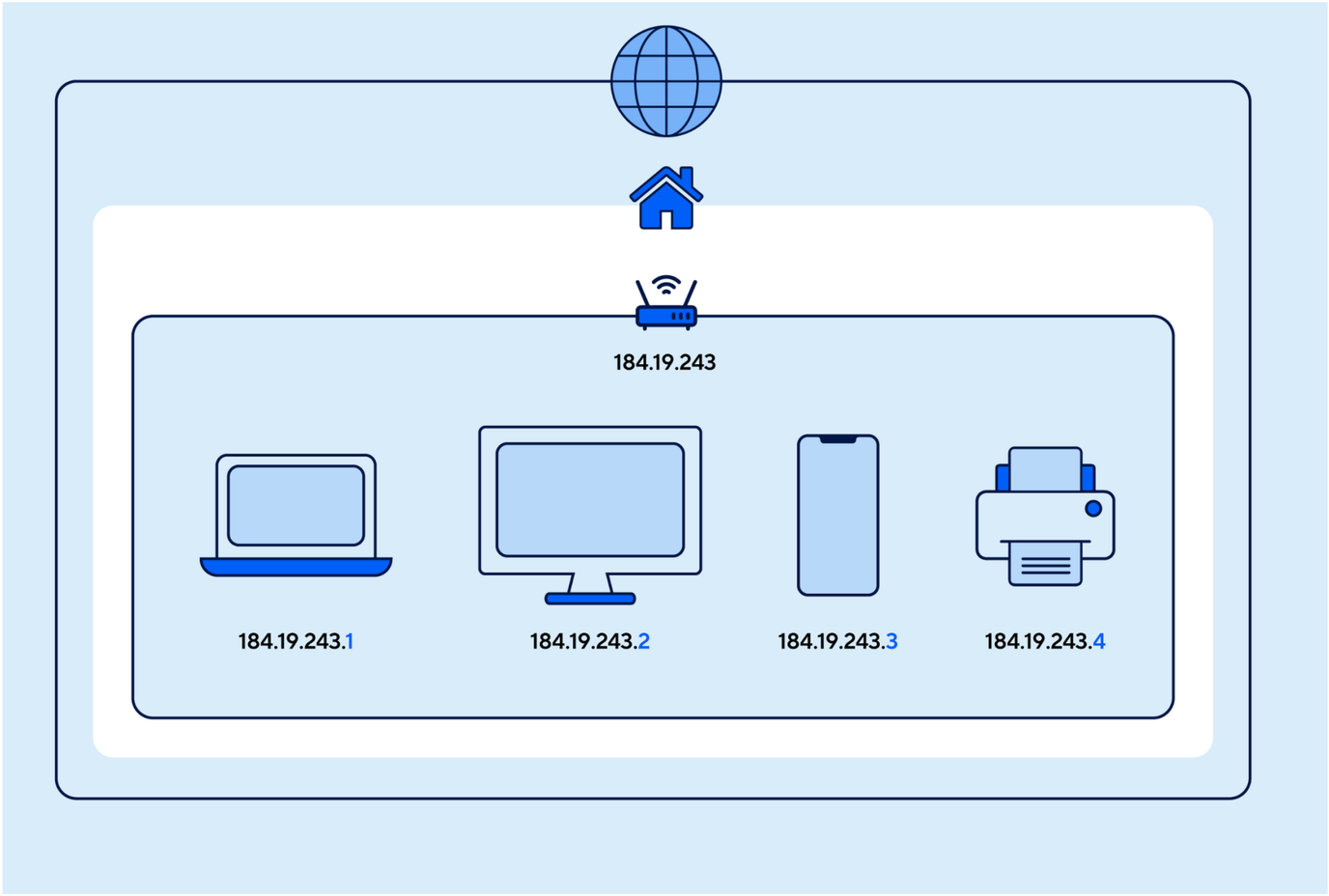
٢- اكتشاف النطاقات الفرعية Subdomains

اسم النطاق الفرعي من النطاق الرئيسي الذي يُستخدم للدخول على موقع إلكتروني

معهد قوى الإنجاز العالي للتدريب
THE FORCES OF ACHIEVEMENT FOR HIGHER TRAINING

أهداف الاستطلاع:

٣- الحصول على عناوين IP



معهد قوى الإنجاز العالي للتدريب
THE FORCES OF ACHIEVEMENT FOR HIGHER TRAINING

أهداف الاستطلاع:

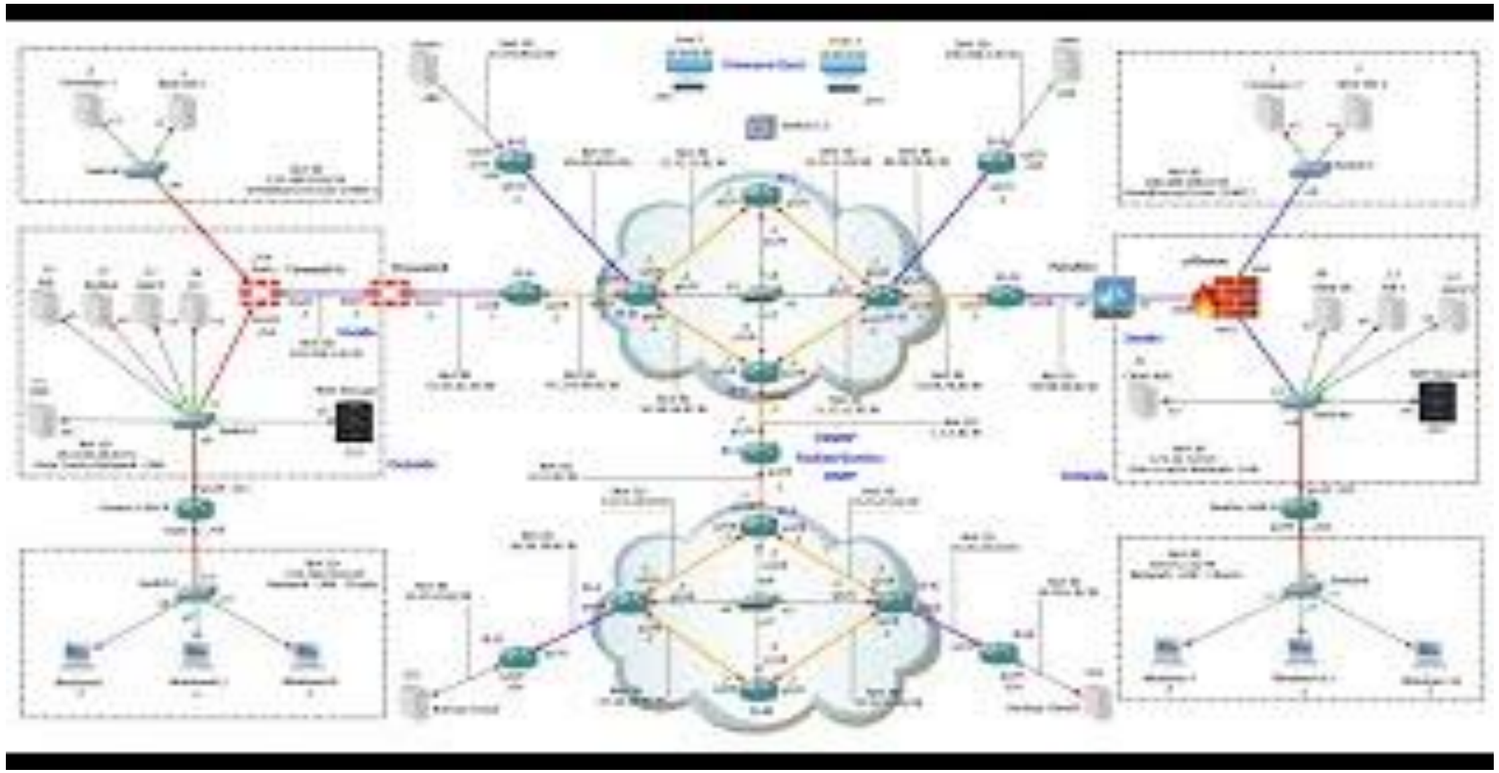
٤- جمع بيانات الموظفين Emails, LinkedIn

معهد قوى الإنجاز العالي للتدريب
THE FORCES OF ACHIEVEMENT FOR HIGHER TRAINING

أهداف الاستطلاع:

٥- اكتشاف البنية التحتية

تحديد مكونات النظام التقنية (السيرفرات، الخدمات، الأجهزة، الأنظمة، الشبكات) التي تشغل البنية التحتية للهدف، بهدف التعرف على نقاط الدخول المحتملة.



أدوات الاستطلاع السلبي Passive Recon

الأداة	الأستخدام
whois	للحصول على معلومات النطاق
theHarvester	جمع إيميلات ومعلومات عامة
Google Dorking	البحث عن معلومات حساسة في محركات البحث
nslookup / dig	للحصول على معلومات DNS يسأل السيرفر

أدوات الاستطلاع النشط Active Recon

الأداة	الأستخدام
Nmap	فحص المنافذ والبروتوكولات
WhatWeb	جمع إيميلات ومعلومات عامة
Wappalyzer	معرفة التقنيات المستخدمة في المواقع

معهد قوى الإنجاز العالي للتدريب
THE FORCES OF ACHIEVEMENT FOR HIGHER TRAINING

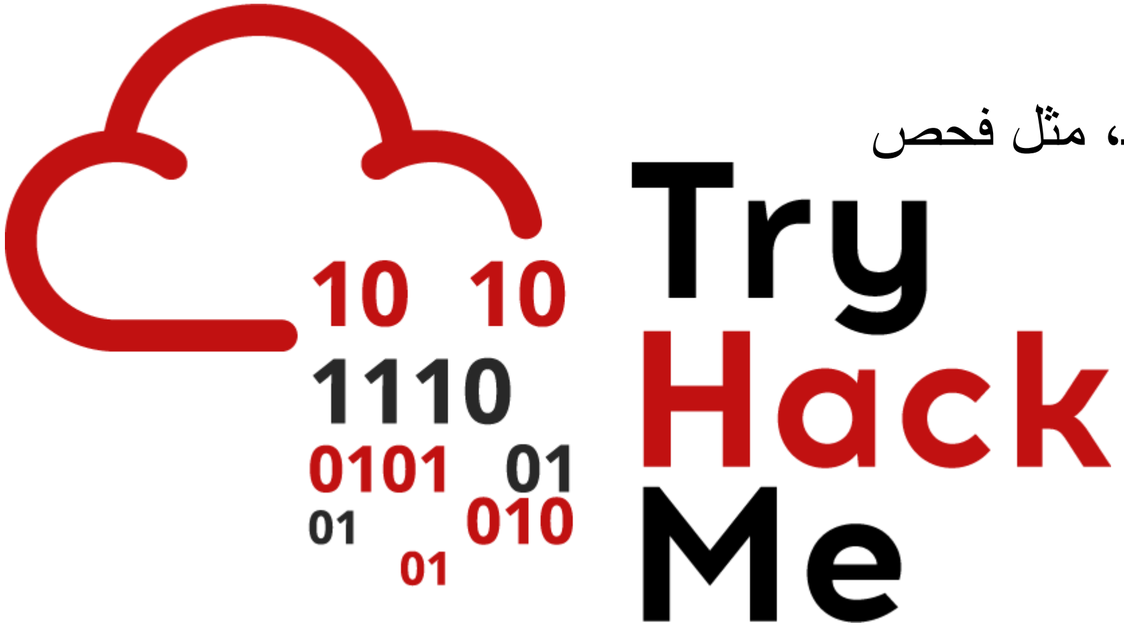
غرف للاستطلاع Reconnaissance

Passive Reconnaissance

- تُركز هذه الغرفة على تقنيات الاستطلاع السلبي

Active Reconnaissance

تُغطي هذه الغرفة تقنيات الاستطلاع النشط، مثل فحص المنافذ باستخدام Nmap



غرف للاستطلاع Reconnaissance

Terminal

```
user@TryHackMe$ whois tryhackme.com
[Querying whois.verisign-grs.com]
[Redirected to whois.namecheap.com]
[Querying whois.namecheap.com]
[whois.namecheap.com]
Domain name: tryhackme.com
Registry Domain ID: 2282723194_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.namecheap.com
Registrar URL: http://www.namecheap.com
Updated Date: 2021-05-01T19:43:23.31Z
Creation Date: 2018-07-05T19:46:15.00Z
Registrar Registration Expiration Date: 2027-07-05T19:46:15.00Z
Registrar: NAMECHEAP INC
Registrar IANA ID: 1068
Registrar Abuse Contact Email: abuse@namecheap.com
Registrar Abuse Contact Phone: +1.6613102107
Reseller: NAMECHEAP INC
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: Withheld for Privacy Purposes
Registrant Organization: Privacy service provided by Withheld for Privacy ehf
[...]
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2021-08-25T14:58:29.57Z <<<
For more information on Whois status codes, please visit https://icann.org/epp
```

غرف للاستطلاع Reconnaissance

Query type	Result
A	IPv4 Addresses
AAAA	IPv6 Addresses
CNAME	Canonical Name
MX	Mail Servers
SOA	Start of Authority
TXT	TXT Records

معهد قوى الإنجاز العالي للتدريب
THE FORCES OF ACHIEVEMENT FOR HIGHER TRAINING

غرف للاستطلاع Reconnaissance

Terminal

```
user@TryHackMe$ nslookup -type=A tryhackme.com 1.1.1.1
Server:     1.1.1.1
Address:    1.1.1.1#53

Non-authoritative answer:
Name:   tryhackme.com
Address: 172.67.69.208
Name:   tryhackme.com
Address: 104.26.11.229
Name:   tryhackme.com
Address: 104.26.10.229
```

غرف للاستطلاع Reconnaissance

Terminal

```
user@TryHackMe$ nslookup -type=MX tryhackme.com
Server:     127.0.0.53
Address:    127.0.0.53#53

Non-authoritative answer:
tryhackme.com   mail exchanger = 5 alt1.aspmx.l.google.com.
tryhackme.com   mail exchanger = 1 aspmx.l.google.com.
tryhackme.com   mail exchanger = 10 alt4.aspmx.l.google.com.
tryhackme.com   mail exchanger = 10 alt3.aspmx.l.google.com.
tryhackme.com   mail exchanger = 5 alt2.aspmx.l.google.com.
```

مراحل اختبار الاختراق

١. التخطيط والاستطلاع Reconnaissance
٢. المسح والتحليل Scanning & Enumeration
٣. الاحتفاظ بالوصول Post-Exploitation
٤. التغطية والإخفاء Covering Tracks
٥. إعداد التقرير

المسح والتحليل Scanning & Enumeration

المسح والتحليل هي المرحلة التي تسبق الاستغلال وتكشف الخدمات والمنافذ والمعلومات الحيوية عن الهدف

ما هو Scanning :

عملية إرسال طلبات إلى الأجهزة " الهدف" لفهم:

-المنافذ المفتوحة

-الخدمات المشغّلة

-أنظمة التشغيل

المسح والتحليل Scanning & Enumeration

المسح والتحليل هي المرحلة التي تسبق الاستغلال وتكشف الخدمات والمنافذ والمعلومات الحيوية عن الهدف

ما هو Enumeration :

هو **جمع المعلومات الدقيقة** بعد التأكد من وجود الخدمة :

-أسماء المستخدمين
-أسماء الأجهزة
-مشاركة الملفات
-إصدارات الأنظمة والخدمات

المسح والتحليل Scanning & Enumeration

المسح والتحليل هي المرحلة التي تسبق الاستغلال وتكشف الخدمات والمنافذ والمعلومات الحيوية عن الهدف

مسح الشبكة Network Scanning :

يحدد الأجهزة النشطة.

معهد قوى الإنجاز العالي للتدريب
THE FORCES OF ACHIEVEMENT FOR HIGHER TRAINING

المسح والتحليل Scanning & Enumeration

المسح والتحليل هي المرحلة التي تسبق الاستغلال وتكشف الخدمات والمنافذ والمعلومات الحيوية عن الهدف

مسح البورتات Port Scanning:
يكتشف المنافذ المفتوحة والخدمات المشغلة.

مسح الشبكة Network Scanning :
يحدد الأجهزة النشطة.

مسح الثغراتVulnerability Scanning
يحدد نقاط الضعف الأمنية.

ما هي المنافذ "Ports"؟

هي نقاط الدخول والخروج في الجهاز عبر الشبكة
كل خدمة أو برنامج يتواصل عبر الشبكة يستخدم رقم منفذ Port Number

ماذا يعني أن المنفذ "مفتوح"؟ :
المنفذ المفتوح يعني أن هناك **برنامج يستمع** Listeningعلى
هذا المنفذ

أشهر منافذ والخدمات؟

رقم المنفذ	الخدمة	الوصف
٢١	FTP	نقل الملفات
٢٢	SSH	دخول عن بعد مشفر
٢٣	Telnet	دخول عن بعد غير مشفر
٢٥	SMTP	إرسال بريد إلكتروني
٥٣	DNS	ترجمة أسماء المواقع
٨٠	HTTP	تصفح الويب
٤٤٣	HTTPS	تصفح آمن

كيف يستخدم المهاجمون المنافذ المفتوحة؟

المهاجم يبحث عن منافذ مفتوحة ليعرف:

-هل هي محدّثة أم لا؟
-ما نوع الخدمة؟
-هل تحتوي على ثغرات؟

أنواع المسح؟

المهاجم يبحث عن منافذ مفتوحة ليعرف:

- TCP Connect Scan
- SYN Scan
- UDP Scan

فئات أدوات الاختراق

تتنوع أدوات الاختراق إلى فئات مختلفة بناءً على وظيفتها وهدفها، وتشمل ما يلي:

- **أدوات مسح الثغرات**

تُستخدم لتحديد نقاط الضعف في:

- الأنظمة
- الشبكات
- التطبيقات

فئات أدوات الاختراق

تتنوع أدوات الاختراق إلى فئات مختلفة بناءً على وظيفتها وهدفها، وتشمل ما يلي:

- **أدوات استغلال الثغرات**

تُستخدم لاستغلال الثغرات الأمنية المكتشفة للوصول إلى النظام.

فئات أدوات الاختراق

تتنوع أدوات الاختراق إلى فئات مختلفة بناءً على وظيفتها وهدفها، وتشمل ما يلي:

- **أدوات ما بعد الاختراق**

تُستخدم لـ:

- الحفاظ على الوصول
- جمع معلومات إضافية بعد الدخول

أداة Nmap

هي واحدة من أهم أدوات المسح والتحليل في عالم الأمن السيبراني. اسمها اختصار لـ *Network Mapper*، وهي مصممة لاكتشاف الأجهزة على الشبكة، فحص المنافذ، والتعرف على الأنظمة والخدمات.

تم تطويرها من قِبل الباحث الأمني المعروف Fyodor، وتُستخدم بشكل واسع من قبل فرق الاختبار الأمني Pentesters و محللي الشبكات.

أداة Nmap

الوظيفة	الأمر	الاستخدام
يُظهر الأجهزة المتصلة بالشبكة فقط	nmap -sn 192.168.1.0/24	اكتشاف الأجهزة فقط
لتحديد المنافذ Stealthفحص المفتوحة	nmap -sS 192.168.1.1	فحص المنافذ
يحاول اكتشاف نظام التشغيل	nmap -O 192.168.1.1	تحديد نظام التشغيل
يُظهر نوع وإصدار الخدمات	nmap -sV 192.168.1.1	تحديد نوع الخدمة