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

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:

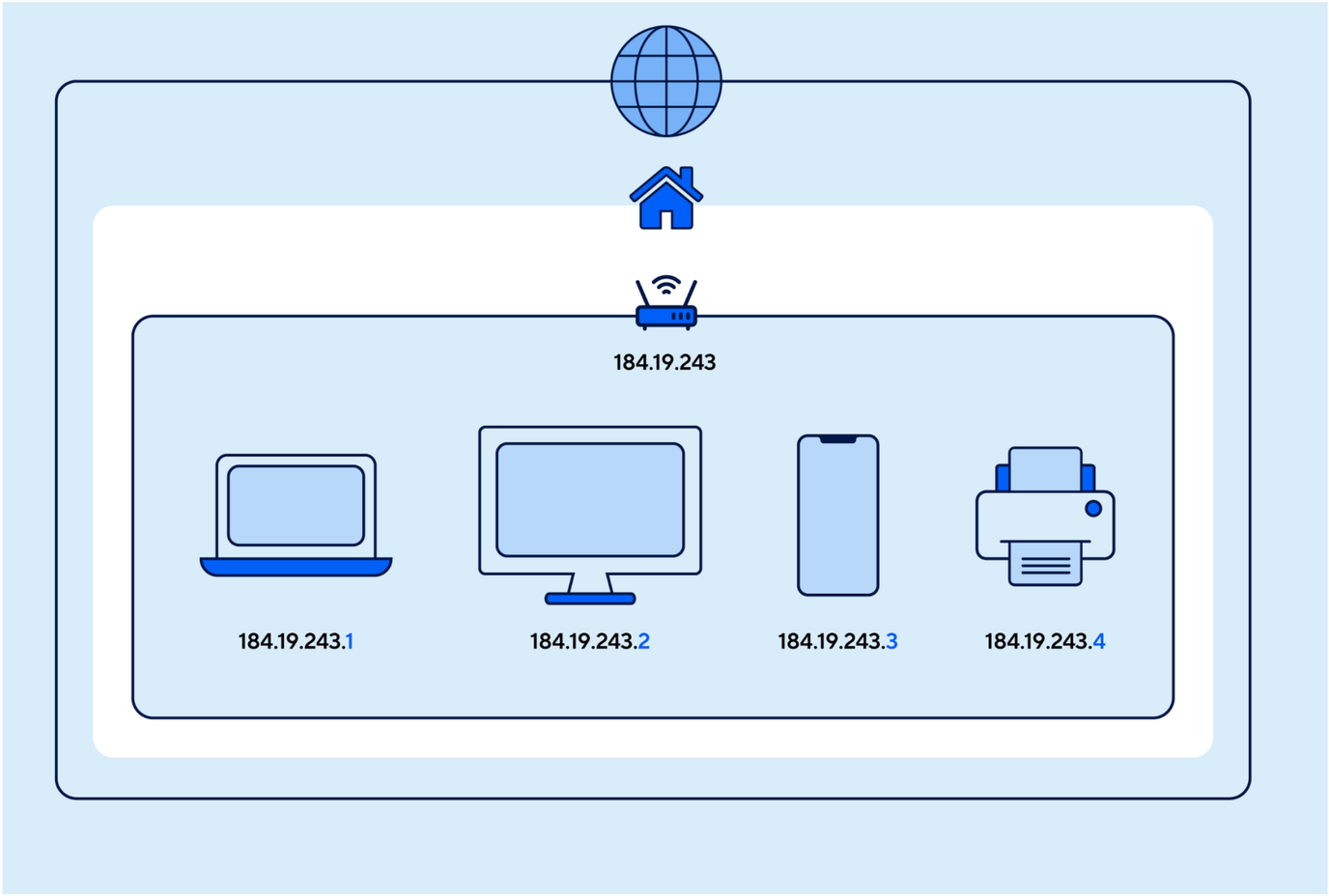
٢- اكتشاف النطاقات الفرعية Subdomains

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:

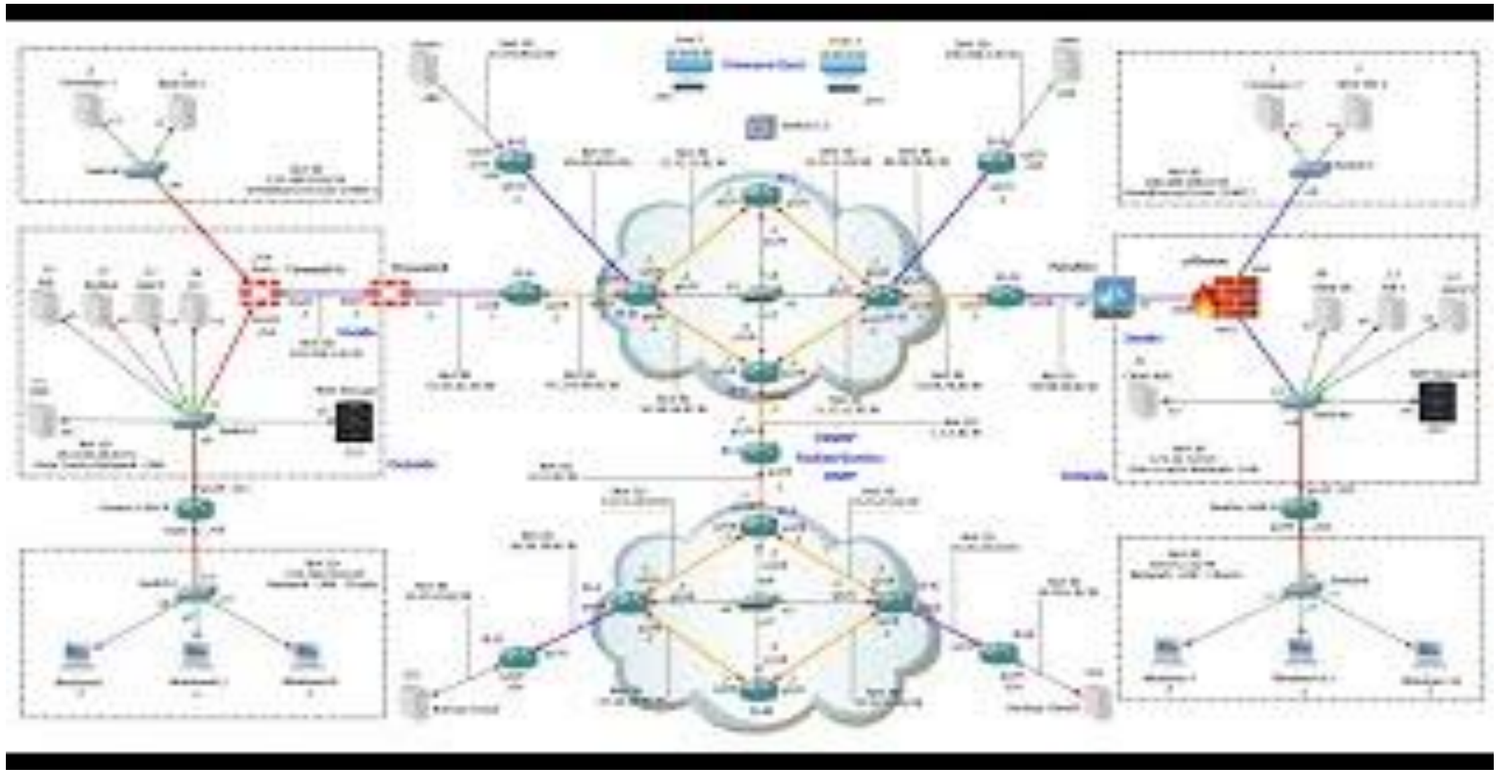
٤- جمع بيانات الموظفين Emails, LinkedIn

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