Kali Linux

نظام اختبار الاختراق الأول عالمياً

اعداد الطالب / محمد سايس

تحت إشراف الدكتورة / نوال الرجوي

ما هو Kali Linux؟

التعريف:

توزيعة لينكس مبنية على دبيان (Debian)، مصممة خصيصاً لاختبار الاختراق (Penetration Testing)والتدقيق الأمني الرقمي .تجمع بين أكثر من 600أداة أمنية في بيئة واحدة متكاملة.

الأصل:

تطور من توزيعة BackTrack Linux الشهيرة

الهدف:

توفير منصة شاملة لاختبار الأمن السيبراني

الجمهور:

متخصصو الأمن، مختبرو الاختراق، الباحثون الأمنيون

أهداف Kali Linux من الدفاع إلى الهجوم الأخلاقي

التدريب والتعليم

توفير بيئة مثالية وآمنة لتعلم مهارات الأمن السيبراني المتقدمة والممارسة العملية.

- بيئة تدريب آمنة
- تطوير المهارات العملية
- بناء الخبرة الأمنية

التحليل الجنائي الرقمي

استعادة وتحليل البيانات بعد وقوع حادث أمني لتحديد مصدر الهجوم والأضرار الناجمة.

- استعادة البيانات المحذوفة
- تتبع آثار الهجمات
- جمع الأدلة الرقمية

اختبار الاختراق

تقييم أمان الشبكات والتطبيقات عن طريق محاكاة هجمات حقيقية لاكتشاف نقاط الضعف قبل استغلالها.

- فحص الثغرات الأمنية
- اختبار المنافذ المفتوحة
- تقييم قوة كلمات المرور

الإيجابيات والسلبيات

السلبيات (التحديات)

ليس للاستخدام اليومي

يتطلب معرفة عميقة بنظام لينكس والأمن السيبراني، وليس مناسباً للمستخدمين العاديين.

خطر الاستخدام الخاطئ

أدواته قوية جداً، والاستخدام غير المسؤول قد يؤدي إلى أضرار قانونية أو تقنية خطيرة.

التحديثات المتكررة

يتطلب صيانة مستمرة وتحديثات منتظمة لمواكبة أحدث الثغرات والأدوات الأمنية.

✓ الإيجابيات (نقاط القوة)

تكامل الأدوات

تجميع مئات الأدوات المصنفة مسبقاً (Metasploit, Wireshark, Nmap) في بيئة واحدة متكاملة، مما يوفر الوقت والجهد.

مجاني ومفتوح المصدر

لا تكاليف ترخيص، مع دعم مجتمعي قوي وتحديثات مستمرة من المطورين حول العالم.

المرونة والتخصيص

يدعم مجموعة واسعة من الأجهزة (Live USB, VM, Cloud) وأنماط التثبيت المختلفة حسب الاحتياجات.

تطبيقات Kali Linux

اختبار أمان الشبكات اللاسلكية

فحص نقاط الوصول (Access Points)وبروتوكولات التشفير مثل WPA/WPA2لاكتشاف الثغرات الأمنية في الشبكات اللاسلكية.

الأدوات : Aircrack-ng, Wireshark

اختبار أمان تطبيقات الويب

البحث عن ثغرات مثل SQL Injection و Cross-Site Scripting (XSS) والثغرات الأخرى في تطبيقات الويب.

الأدوات : Burp Suite, OWASP ZAP

هندسة الشبكات والاستكشاف

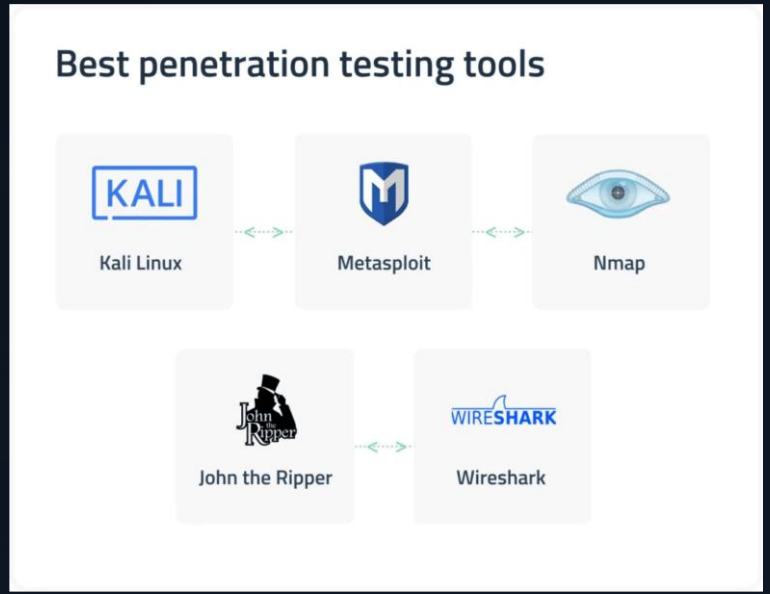
اكتشاف الأجهزة والخدمات المتاحة على الشبكة وتحديد المنافذ المفتوحة وإصدارات الخدمات.

الأدوات : Nmap, Zenmap

كسر كلمات المرور واختبار القوة

اختبار قوة كلمات المرور واستخراج البيانات المشفرة باستخدام تقنيات الهجوم المختلفة.

الأدوات : John the Ripper, Hashcat



التأثير على الأفراد والمجتمع :المسؤولية الأخلاقية

على الأفراد(المستخدم الأخلاقي)

- حماية الذات :اختبار أمان أجهزتهم وشبكاتهم المنزلية
- تطوير المهارات :بناء مسيرة مهنية قوية في مجال الأمن السيبراني
- الوعي الأمني :فهم أعمق لكيفية عمل الهجمات والدفاع عنها

على المؤسسات والشركات

- تعزيز الأمن القومي :حماية البنية التحتية الحيوية من الهجمات الإلكترونية
- الامتثال التنظيمي :تلبية معايير الأمن الدولية (ISO 27001, NIST)
- تقليل المخاطر :اكتشاف الثغرات قبل استغلالها من قبل المهاجمين

على المجتمع والدولة

- مكافحة الجريمة الإلكترونية :دعم جهود التحليل الجنائي الرقمي
- تعزيز الثقة الرقمية :بناء بيئة رقمية آمنة وموثوقة للجميع
- الاستقرار الاقتصادي :حماية الأصول الرقمية والبيانات الحساسة

التطبيق العملي - Nmap :(1/3)استكشاف الشبكة

ما هي أداة Nmap؟

Nmap (Network Mapper) : هي أداة مفتوحة المصدر قوية لاستكشاف الشبكات وتحديد المنافذ المفتوحة والخدمات المتاحة على الأجهزة المستهدفة.

الهدف من الأداة

اكتشاف الأجهزة الحية على الشبكة، تحديد المنافذ المفتوحة (Open Ports)، والخدمات التي تعمل عليها، مما يساعد في تقييم أمان البنية التحتية.

مثال عملي :الأمر

```
nmap -sV -p 1-1000 192.168.1.1
```

- **-Sv** : كشف إصدارات الخدمات (Service Version Detection)
- **-p 1-1000** : فحص المنافذ من 1 إلى 1000
- **192.168.1.1** : عنوان IP للجهاز المستهدف

```
nmap -sV -p 1:1000 192.168.1.1
Starting Nmap 7.92 ( https://nmap.org) at 2024-4-24 19:27
PORT  STATE  SERVICE    VERSTON
53 ttp open  domain     dnsmAsq 2.84
99 ttp open  hitp       lighttpd 1.4.59
443   open   https      OpenSSl 1.1.1n lighttpd 1.4.59
Service detection performed· Please report any incorrect
results at https://mmap.srg/subnlt/.
Nmap done: 1 IP address (1 host up) scanned in 7.32 seconds
```

التطبيق العملي Wireshark (2/3):

الأداة

Wireshark - محلل حركة المرور الشبكية (Network Traffic Analyzer) الأكثر استخداماً عالمياً لالتقاط وتحليل حزم البيانات.

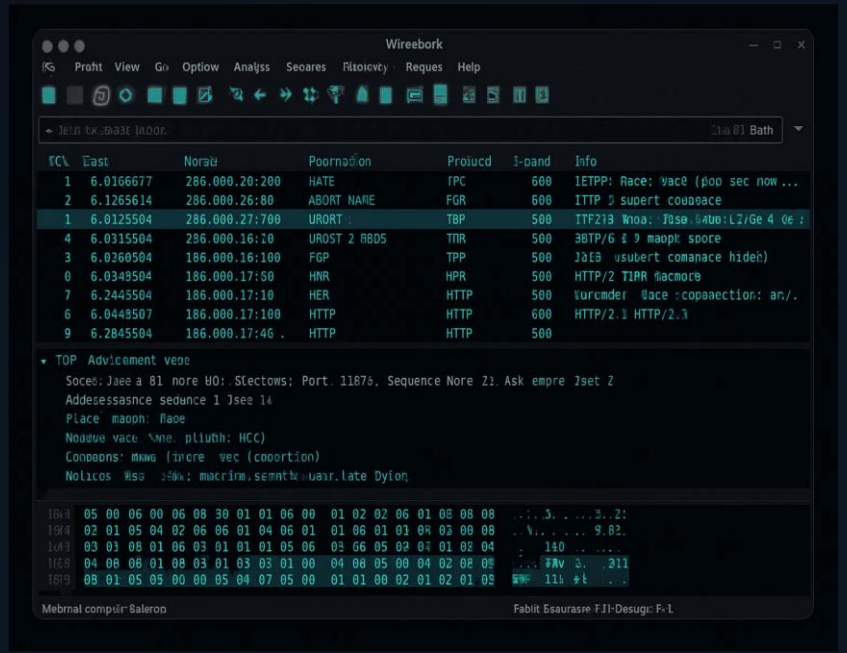
الهدف

التقاط وتحليل حركة المرور الشبكية في الوقت الفعلي لتحديد المعلومات المرسلة، كشف البيانات غير المشفرة، وفهم بروتوكولات الشبكة.

مثال عملي

```
http.request or ftp
ip.src == 192.168.1.100
tcp.port == 80 or tcp.port == 443
```

هذه المرشحات (Filters) تساعد في البحث عن حزم محددة بناءً على البروتوكول أو عنوان IP أو المنفذ.



الفوائد الأمنية

- كشف البيانات المرسلة بدون تشفير
- تحديد الاتصالات المريبة والشاذة
- تحليل أنماط حركة المرور
- اكتشاف محاولات الاختراق والهجمات

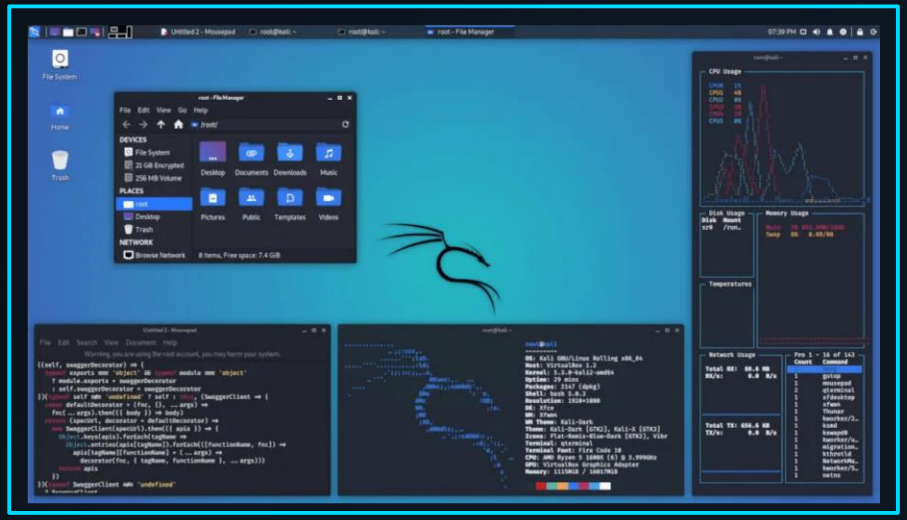
التطبيق العملي(3/3): Metasploit Framework

الأداة

- **Metasploit Framework**إطار عمل متقدم لتطوير وتنفيذ كود الاستغلال (Exploit Code)ضد الأنظمة المستهدفة بطريقة منظمة وفعالة.

الهدف

استغلال الثغرات الأمنية المعروفة في الأنظمة للحصول على وصول غير مصرح أو تنفيذ أوامر على النظام المستهدف.



خطوات الاستغلال

1. اختيار وحدة الاستغلال (Exploit Module)المناسبة للثغرة المستهدفة
2. تحديد الحمولة (Payload)المطلوبة مثل `Meterpreter` للتحكم البعيد
3. تعيين عنوان IPالهدف (RHOST)والمنفذ المستخدم (LPORT)
4. تنفيذ الأمر `exploit` لبدء الهجوم

الفوائد الأمنية

- اختبار فعال للثغرات المعروفة
- محاكاة هجمات حقيقية بطريقة آمنة
- توثيق شامل للثغرات المكتشفة
- تقييم مستوى خطورة الثغرات

نظرة بصرية :واجهة Kali Linux

بيئة سطح المكتب

Kali Linuxيوفر واجهة رسومية احترافية بناءً على XFCEأو Gnome، مصممة لسهولة الاستخدام والوصول السريع للأدوات الأمنية.

القائمة الرئيسية والتصنيفات

تنظيم منطقي للأدوات حسب الفئات :معلومات جمع، ثغرات، استغلال، أدوات ويب، وغيرها.

وصول سطر الأوامر

وصول سريع وسهل إلى محطة الأوامر (Terminal)لتنفيذ الأوامر والبرامج بكفاءة عالية.

الأدوات الرئيسية المتاحة

استغلال الثغرات - **Metasploit**	استكشاف الشبكة - **Nmap**
اختبار الويب - **Burp Suite**	تحليل المرور - **Wireshark**

ملاحظة : واجهة Kali Linux قابلة للتخصيص بالكامل، ويمكن تثبيت أدوات إضافية حسب الاحتياجات الخاصة.

المراجع والمصادر (الجزء الأول)

الموارد الرسمية

الموقع الرسمي لـ Kali Linux

الموقع الرسمي يوفر التحميل المباشر للتوزيعة، الوثائق الكاملة، والدعم الفني الشامل. https://www.kali.org/

وثائق Kali Linux الرسمية

https://docs.kali.org/

دليل شامل يغطي التثبيت والتكوين واستخدام الأدوات المختلفة في Kali Linux.

الكتب والمراجع التعليمية

Penetration Testing: A Hands-On Introduction to Hacking

كتاب شامل من تأليف Georgia Weidman يشرح مبادئ اختبار الاختراق بشكل عملي باستخدام Kali Linux.

The Web Application Hacker's Handbook

مرجع متقدم لاختبار أمان تطبيقات الويب مع أمثلة عملية وأدوات Kali Linux.

Metasploit: The Penetration Tester's Guide

دليل متخصص في استخدام Metasploit Framework لاستغلال الثغرات بشكل آمن وأخلاقي.

المراجع والمصادر (الجزء الثاني)

منصات التدريب العملية

Hack The Box
https://www.hackthebox.com/

منصة تفاعلية توفر بيئات افتراضية آمنة لممارسة اختبار الاختراق والتحديات الأمنية.

TryHackMe
https://tryhackme.com/

منصة تعليمية تقدم دورات تدريبية عملية مع غرف تدريب مباشرة لتطبيق المهارات الأمنية.

OverTheWire
https://overthewire.org/

موقع متخصص في تحديات الأمن السيبراني والبرمجة بمستويات صعوبة مختلفة.

المنتديات والمجتمع

منتدى Kali Linux الرسمي
https://forums.kali.org/

منتدى رسمي للحصول على الدعم الفني والإجابة على الأسئلة من المجتمع والمطورين.

مجتمع Reddit: r/Kalilinux

مجتمع نشط يناقش أحدث التطورات والنصائح والتحديات المتعلقة بـ Kali Linux.

المسؤولية الأخلاقية والدعوة للعمل

المسؤولية الأخلاقية

القوة تأتي مع المسؤولية .استخدام Kali Linux يجب أن يكون دائماً بموافقة صريحة من مالك النظام، ضمن إطار قانوني واضح، وبهدف تعزيز الأمن وليس انتهاكه.

الأداة ليست الشيء المهم - الأخلاق والنية هي التي تحدد الفرق بين الحماية والهجوم.

الدعوة للعمل

ندعوكم جميعاً للعمل على تعزيز الأمن الرقمي في مؤسساتكم ومجتمعاتكم .استخدموا هذه المعرفة لحماية البيانات، اكتشاف الثغرات، وبناء بيئة رقمية آمنة وموثوقة للجميع.

شكراً لحسن استماعكم .أسئلة؟