**Information gathering** => هو انى بجمع معلومات عن الضحيه وهو اول خطوه ف عملية الاختراق

**two types of information gathering:**

**passive(footprinting)** =>

بجمع معلومات عن الضحيه بدون اتصال مباشر بيه من خلال المعلومات اللى متوفره بابليك عنه من خلال محركات البحث او غيرها. من اهم مراحل الاختراق. فى المرحله دى ببدأ اجمع معلومات عن الجهه اللى محتاج اعمل عليها تيستنج وابدأ اعملها تصنيف واحدد ممكن استخدم كل تصنيف ف ايه من عملية الاختراق.

**active(footprinting)** =>

بجمع معلومات عن الضحيه عن طريق اتصال مباشر بيه انى اعمله سكاننج عليه او احطله ترافك معينه على السيرفر واحدد حسب الريسبونس اللى بيرجعلى ( هتتناقش بالتفصيل بعدين).

**1.Passive footprinting:**

ايه هى المعلومات المهمه بالنسبالى اجمعها ؟

- معلومات خاصه بالنيتورك ( IP addresses – sub-domains – Services)
- معلومات عن السيستم ( نظام التشغيل – database - applications )
- بيانات الموظفين (ارقامهم – بياناتهم )

**OSINT (open source intelligence) =>**

يعنى تجميع معلومات عن طريق اى حاجه بتيح معلومات بابلك زى (social networks- forums – business websites – blogs – videos..etc)

**Search engines & Services =>**

هى المصادر المختلفه اللى اقدر اجمع منها معلومات وبتختلف ف انواع الوظايف اللى بتأديها وهى كالأتى:

- **Wikipedia**
- **Netcraft =>**

بيستخدم فى تجميع معلومات عن اى دومين وبيوفرلى معلومات زى (Sub-domains – operating system – services - last update..etc)

- **Shodan**

محرك بحث خاص بال internet of things (IOT) يعنى اى حاجه متصله بالأنتر نت زى ( راوترات – كاميرات مراقبه – سيرفرات – اى حاجه ليها IP address) بيرجعلى ايه السيرفسيس اللى شغاله عليه وممكن اعمل فلترنج للحاجات اللى عايزه يظهرهالى سواء فلترنج على حسب المكان او البروتوكول.

- **Google – Bing**
- **Geolocation: Google maps – Bing maps – wikimapia**

**People search =>**

مصادر اقدر اجمع منها معلومات عن الاشخاص من خلال المعلومات اللى متوفره عنه من خلال مواقع التوظيف او غيرها زى:

- **Pipl**

بيوفرلى معلومات عن شخص من خلال اعطائه معلومه وهو يبدأ فى اظهار باقى المعلومات المتعلقه بالشخص دا

- **Linkedin**
- **Bayt**
- **Google finance**
- **Yahoo finance**

**Advanced Google Hacking =>**

هو طريقه بعمل بيها فلترنج للسيرش بطريقه محدده وبستخدم فيها بعض ال operators اللى من خلالها اقدر احصل على المعلومه اللى محاتجها بالتحديد وال operators دى هى زى: (cache – intext – info – intitle – filetype – link – allinurl – site – related – allintitle – inurl).

**EX:- in google search input box:**

inurl: page.php?id= **=>**

ببحث عن لينكات مضمون الURL فيها موجود فيه الكلام اللى حاطه دا

intitle: hacked by **=>**

نفس موضوع ال inurl لكن ببحث فى ال title بتاع الصفحه بدل ال URL

**Google hacking database (GHDB) =>**

هى داتابيز فيها بعض الكويرز (queries) اللى اقدر استخدمها فى انى احصل على بيانات حساسه واللى بيوفرلى الكويرز دى مواقع زى:

- https://www.hackersforcharity.org
- https://www.exploit-db.com

المعلومات اللى بتوفرها زى:

- تحذيرات ونقاط ضعف السيرفرات
- رسايل الخطأ اللى فيها معلومات كتير
- الملفات اللى بتحتوى على باسوردز
- مسارات حساسه داخل الملفات... الخ.

**Bing =>**

هو محرك البحث الخاص بشركة مايكروسوفت. الميزه اللى فيه انى بقدر ادخله IP مثلا هيكون بتاع سيرفير، فهو هيرجعلى كل الدومينز والسب دومينز اللى موجوده على السيرفر دا.

**EX:- in Bing search input box:**

Ip: 172.217.171.206 **=>**

ببحث عن لينكات مضمون الURL فيها موجود فيه الكلام اللى حاطه دا

**WHOIS =>**

هو كويرى او بروتوكول بيستخدم فى جلب البيانات من الداتا بيزيز اللى بتحتوى على معلومات عن صاحب ال domain واللى بتقدر ترجعلى بيانات زى:

- اسم الدومين وتفاصيل تانيه عنه
- معلومات التواصل مع مالك الدومين
- السيرفرات اللى بتخدم اسم الدومين
- تاريخ انشاء وانتهاء اسم الدومين
- تاريخ اخر ابديت على اسم الدومين

**Tools =>**

فى عندى ادوات كتيره باستخدمها علشان اقدر اعمل footprinting زى( Maltego – Fierce – FOCA – Recon-NG – Metagoofil – Harvester – Dimtry ...etc) هنتعرف على بعض الادوات دى.

**Recon-NG =>**

هو فريم وورك مكتوب بالبايثون، فيه موديولز (code functions) اللى بتنفذلى بعض التاسكس زى انى اديله دومين يرجعلى الساب دومينز اللى موجوده فيه، اديله الساب دومينز يرجعلى الأى بى بتاعتها، اديله الأى بى يرجعلى خد الطول وخط العرض(المدينه) بتاعه، موديول اديله ايميل شخص اذا حصل تسريب للبيانات بتاع الايميل دا يرجعلى الباسوردس بتاعته.

بعمل انشلايز للتول بامر recon-ng. شوف المانيول من امر help علشان تعرف الاوامر المتاحه وازاى تقدر تتعامل مع التوول.

اكتب الامر واضغط انتر هيديك الاوبشنز بتاعته اللى ينفع تستاخدمها معاه.

بسطب موديولز من ال marketplace : -

>>**marketplace search** //show all modules.

>>**marketplace info *module*** //show info about selected modules.

>>**marketplace install *module*** //install selected module.

**Ex: - using a module to get hosts of a selected domain name**

**>>workspaces create *name*** //creating new workspace

**>>modules load *module*** //loading selected module

**>>db insert domains** //insert targeted domain

**>>run**

**TheHarvester =>**

هى tool موجوده ف ال kali بتسخدم ك command وبعمل بيها information gathering (شوف المانيوال بتاعها علشان تعرف استخدام كل option). بتقوم بدور كتير من المصادر اللى ذكرناها.

**Ex: -** theHarvester -d sisco.com -b all -l 2000 -f /root/Desktop/sisco.com

كدا انا بجمع معلومات عن دومين سيسكو عن طريق(d-) وببحث ف كل المصادر عن طريق(b-) وباخد اول 2000 نتيجه من كل مصدر عن طريق(l-) وبحفظ النتايج اللى جاتلى فى ملف HTML عندى على الديسكتوب عن طريق (f-).

**Sublist3r =>**

هى tool بحملها واسطبها على الكالى. بديها دومين بترجعلى كل السب دومينز وال IP addresses للدومين دا (بص ف المانيول ع الاوبشنز).

**Ex: -** **.** /sublist3r.py -d yahoo.com -b -v -t 100 -o /root/Desktop/yahoo.txt

**2.Active footprinting:**

**DNS footprinting =>**

الاول ال (domain name server) DNS هى سيرفرات بتخزن ال IP بتاعت الدومينز لان انا لما بتواصل مع مع موقع معين انا بتواصل من خلال ال IP بتاعه اللى هو رقمه المحدد ليه، بس انا مش هحفظ ارقام كل موقع بس بحفظ اسمه فاسمه ده اللى هو الدومين بيكون متخزن ف ال DNS ومعاه ال IP addresses اللى تخص الدومين الرئيسى والسب دومينز بتاعته، فانا لما اطلب موقع معين من خلال اسمه بيعمل اكسيس على ال DNS ويرجعلى ال Ips بتاعته اللى من خلالها اقدر اتواصل مع الموقع.

**ازاى الهاكرز ممكن يستغلوا ال DNS ؟** ممكن اذا قدر يخترق ال DNS يغير ال IP addresses اللى بتخص دومين معين ويخلي اليوزر لما يطلب دومين معين يظهرله الموقع اللى الهاكر غير ال IP ليه.

فى عندى حاجه اسمها ال DNS record type ودى بتكون زى اوبشنز بتحدد للسيرفر انا محتاج ارجع منه معلومات ايه، مثلا :

**A => points** to IP addresses

**MX => points** to domain's mail servers

**host =>**

**(See command help)**

امر بيرجعلى عدة حاجات انا بطلبها منه زى ال Ip addresses لدومين معين بالاتنين version بتوعه وبستخدم معاه اوبشنز ال DNS ريكورد علشان احددله الحاجه اللى محتاجه يرجعهالى، زى الامثله اللى جايه :

**Ex: -**

>>host -t ns google.com

دا هيرجعلى ال name servers الخاصه بالدومين اللى انا حددته. اوبشن ال t- فى الامر هنا بستخدمها علشان احدد نوع ال query اللى هو ال DNS record type اللى اتكلمت عليه فوق والعمليه هنا بيبقا اسمها DNS query ونوع الكويرى اللى استخدمته هنا هو ال ns .

>>host -t a google.com

هيرجعلى ال IP الخاص بالدومين

>>host -t mx google.com

هيرجعلى ال mail servers الخاصه بالدومين

>>for khara in $(cat domains.txt); do host $khara.google.com; done

- دى طريقه ممكن اعمل ملف تيكست مثلا(domains.txt) وجواه فكل سطر اكتب كلمه عايز اسم الدومين يبدأ بيها زى مثلا ( www – admin – login) واقدر بقا انى اخلى امر هوست يدورلى على كل الدومينز اللى بدايتهم كدا ويرجعلى ال IP بتاعتهم.
- **ازاى بقا ؟** فى الامر هنا استخدمنا for وبعدها اسم متغير اللى هو هنا اسمه khara فانا وقلتله in فى الملف اللى انا كاتب فيه الاسطر، ف for كدا بتعملى assign لكل سطر بتعرفه كمتغير اسمه khara وبقله بقا على كل khara نفذ امر host (do host) على الدومين دا وبكتب طبعا قبل الدومين المتغير بتاعى.
- ال($)dollar sign مش بستخدمها لما اكون بعرف المتغير لأول مره، انما لما اجى استخدم المتغير ف عمليه ساعتها بحطها.

**طيب نضيف شوية عمليات على الكود:**

>> for khara in $(cat domains.txt); do host $khara.google.com; done | grep -v "not found"

لما ببحث طبيعى انى اكتب كلمات ميكونش عنها نتايج فهيرجعلى not found فانا اخدت اللى خرجلى من الامر الاول وقلتله حددلى كل الاسطر اللى فيها "not found" وعن طريق اوبشن v- قلتله اعملى استثناء للسطور دى، يعنى رجع كل السطور الا السطور اللى فيها not found

لو انا حطيت لأمر host بدل الدومين حطيت ال IP هيعملى هو reverse lookup ويرجعلى ال domain name pointer .

>>for IP in $(seq 1 255); do host 172.217.18.$IP; done

فى اول جزء من الكومند بقله يعمل assign لمتغير IP بارقام من 1 ل 255 علشان بكدا هينفذهم على الجزء التانى اللى انا بستخدم فيه المتغير، يعنى كدا هيعملى هوست على 255 IP بدايتهم 1 واخرهم 255 .

**ازاى اعرف اذا كان فيه DNS server مفعل ال zone transfer ؟**

الأول ايه هو ال zone transfer ؟ لو administrator عنده اكتر من DNS وعمل تعديلات على واحد، المفروض ان نفس التعديلات بالظبط تتم على باقى ال DNS servers فعلشان يوفر الوقت ويقلل الخطأ الاعدادات دى بتتنقل عن طريق بروتوكول AXFR وبيتم تطبيقها على باقى ال DNS servers المرتبطين ببعض. اعرف تفاصيل من **هنا**

ازاى بقا اعرف لو كان ال zone transfer مفتوح على DNS معين ولا لا ؟

>> host -t ns google.com

>> host -l google.com ns1.google.com

الأول بعرف اسم ال name server بتاع الدومين عن طريق اول كومند وبعدها بستخدم امر الهوست مع اوبشن l- واحط اسم الدومين وبعده ال name server بتاعه. (طبعا جميع المواقع من المفترض انها هتكون قافله الzone transfer لان دا ممكن يسرب بيانات من خلاله)

اقدر استخدم موقع مفتوح للتدريب على ال Check دا اسمه zonetransfer.me

**dnsrecon =>**

هى tool عباره عن امر ف الكالى بيستخدم لاغراض كتير منهم انه يعمل Check على ال zone transfer (شوف الهيلب بتاعها علشان تعرف استخدامها اكتر )

Ex: - dnsrecon -d google.com -t axfr

**dnsenum =>**

برضو بتعمل اوتوميشن وبترجع حاجات كتير زى ال IPs وال mail servers وغيرها، بص بص جربها وشوف

Ex: - dnsenum google.com

**Scanning :**

عملية تجميع معلومات عن الشبكه من IPs بتاع الاجهزه اللى عليها وال operating systems بتاع الاجهزه دى ونوع الويندوس اللى شغالين بيه، اعرف لو فيه ports مفتوحه واعرف ال services اللى شغاله عليه والبورت الخاص بال service دى.

**ايه انواع الscanning ؟**

- Network scanning

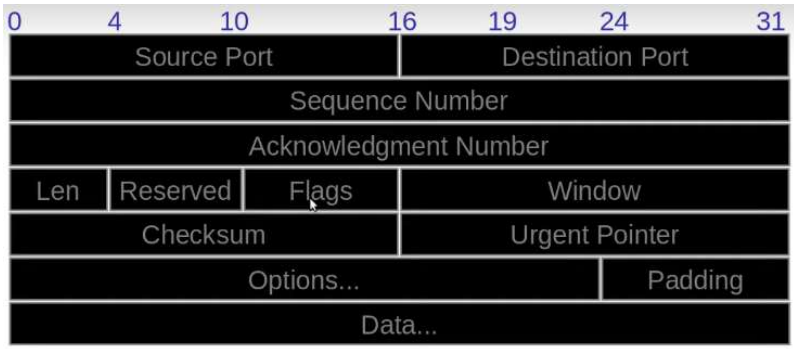
  بحدد الاجهزه اللى شغاله على الشبكه واعرف ال IPs بتاعتهم وال operating systems اللى شغالين بيها
- Port scanning

  كل service على السيستم بتستخدم بورت معين ولما يكون فى Service شغاله على بورت معين مينفعش يشتغل عليه حاجه تانيه.
  صفحات الانترنت كل صفحه بتفتح على بورت محدد . اول 1023 بروت محجوزين للسيستم
- Vulnerability scanning

  بحدد ايه نقالط الضعف بتاع ال operating system وال applications اللى شغاله عليه

**TCP segment =>**

- هو ال TCP موضوع كبير شوية (انا عندى فكره عنه) بس هناخد فيه نظرات سريعه واللى يهمنا شويه ف ال pentesting
- هو بروتوكول لنقل البيانات وبيكون reliable ( يعنى مبيبقبلش فقد ف البيانات ولو حصل فقد بيعيد ارسالها تانى)
- فى البروتوكول دا بيحصل عملية handshaking يعنى السورس بيشوف الديستنيشن جاهز للاستقبال ولا لا وبعدين يبدأ يبعت وبعد م يخلص الديستنيشن بيبعتله acknowledgement علشان يقله ان البيانات وصلت ول ال acknowledgement مرجعتش من الديستنيشن يبقا البيانات مراحتلوش فيقوم السورس يبعتها تانى
- بيهمنى ف ال pentesting موضوع ال **flags**




| Field | Purpose |
|---|---|
| Source Port | Identifies originating application |
| Destination Port | Identifies destination application |
| Sequence Number | Sequence number of first octet in the segment |
| Acknowledgment # | Sequence number of the next expected octet (if ACK flag set) |
| Len | Length of TCP header in 4 octet units |
| Flags | TCP flags: SYN, FIN, RST, PSH, ACK, URG |
| Window | Number of octets from ACK that sender will accept |
| Checksum | Checksum of IP pseudo-header + TCP header + data |
| Urgent Pointer | Pointer to end of “urgent data” |
| Options | Special TCP options such as MSS and Window Scale |

**Flags :**

- **URG (urgent)**

لو انا باعت packet وحاطط فيها URG flag = 1 يعنى فانا بقول للطرف التانى اعملى processing سريع للداتا عندك (مستعجل) يعنى اديها اولويه عن غيرها من ال packets .

- **FIN (finish)**

يعنى خلاص بقول للطرف التانى انتهت عملية نقل البيانات فاقطع الاتصال خلاص مفيش بيانات تانيه

- **RST (reset)**

بعمل restart للأتصالrestart للأتصال

- **PSH (push)**

حاجه كدا شبه ال URG

- **ACK (acknowledgement)**

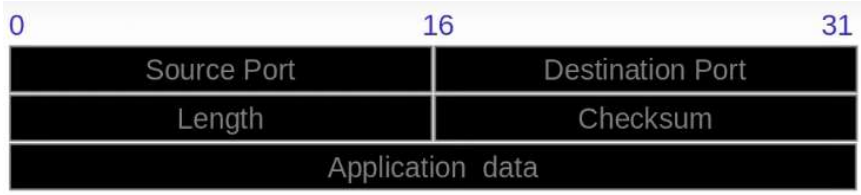
طرف بيقول للطرف التانى ان ال packet بتاعتك وصلتنى

- **SYN (synchronize)**

بتبدأ عملية الاتصال بين اتنين hosts

**UDP datagram =>**

- هو بروتوكول لنقل البيانات وبيكون unreliable ( يعنى بيقبل فقد ف البيانات عادى)
- مفيهوش عملية handshaking، هو بس بيبعت البيانات ومش بيهتم اذا تم استقبالها ولا لا
- بيستخدم ف الاغلب مع مكالمات الفديو بحيث ان مكالمات الفديو ممكن يتسمح فيه ب packet loss عادى




| Field | Purpose |
|---|---|
| Source Port | 16-bit port number identifying originating application |
| Destination Port | 16-bit port number identifying destination application |
| Length | Length of UDP datagram (UDP header + data) |
| Checksum | Checksum of IP pseudo header, UDP header, and data |

**ICMP Scanning =>**

- هو check بعرف بيه اذا كانت جهاز معين شغال ولا لا عن طريق انى ببعت ping واكتب ال IP بتاع اللى عايز اتشيك عليه ولو هو شغال هيبعتلى reply بكدا اعرف انه شغال. (e.g. ping 192.168.1.15)
- لو مبعتش reply ممكن يكون مش شغال وممكن يكون شغال بس ال firewall على الجهاز قافل برتوكول ال ICMP الخاص بعمليات ال pings .

**ازاى اقدر اعمل ICMP scanning لأكتر من جهاز ؟**

- ممكن اعمل script اخليه يكرر كومند ال ping على رنج معين من ال IPs
- او ممكن استخدم Tools زى ؟
  - **Angry IP scanner**
  - **Nmap**

**Port Scanning =>**

هو check بيتعمل علشان اقدر احدد ايه البورتات اللى مفتوحه على السيستم واعرف ال Services اللى مرتبطه بيها

**TCP Scan:**

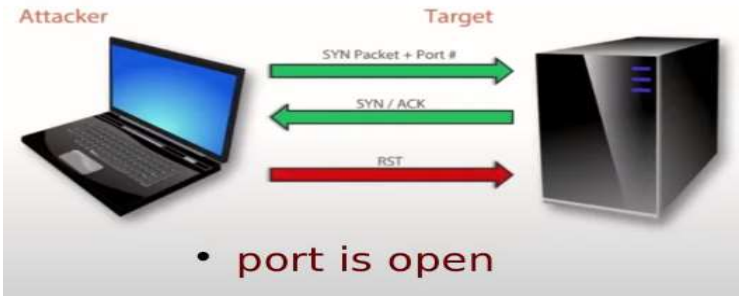
**1.TCP connect scanning**

بعمل check على ال ports الخاصه بال TCP وبيتم كالأتى:


هنا بيبعت SYN packet + رقم ال port فلو البورت مفتوح ال target بيبعت SYN + ACK وبعد كدا بيبعت ال Attacker تانى RST flag + ACK ويفصل ال connection


هنا بيبعت SYN packet + رقم ال port فلو البورت مقفول ال target بيبعت RST flag ويقفل الconnection

**2.Half open scanning**




- بعمل check(ping) على جهاز من غير م اكمل عملية ال handshaking (يعنى اول اما يجيلى reply من ال target ان البورت مفتوح بنهى الاتصال علطول) ودا هيخلى جهاز ال Attacker ميبعتش ACK انه استلم داتا وبكدا مش هيظهر لل target ان حد حاول يعمل عليه scan(logging) .
- لازم يكون عندى صلاحيات الرووت على السيستم.

**3.Xmas scanning**


- بيبعمل set(=1) لبعض ال Flags اللى هم FIN, URG, PUSH ويبعت ال TCP packet لل target لو موصلوش رد دا معناه ان ال port مفتوح ولو اتعمل RST لل connection فده معناه ان البورت مقفول.
- بتنفع على كل ال operating systems الا الويندوز لانه مش متبع ال standards بتاع TCP/IP RFC 793 .

**4.Inverse TCP scanning**

- هو زى ال Xmas بس الفرق انه فى منه 4 انواع، انه بيخلى واحد بس من ال flags قيمته set(=1) والباقى بيكون باصفار وبيتسمى نوع ال scan على اسم الflag اللى قيمته بواحد ( كدا 3 انواع ) النوع الرابع هو NULL وفيه بيكون قيمة كل ال flags ب reset(=0) .
- نفس الموضوع برضو مش بينفع على الويندوز.

**UDP Scan:**

هو نوع واحد بس اللى بيتم ف ال UDP scan لان ال UDP مفيش فيه flags .


**ازاى اقدر احمى نفسى من ال port scanning ؟**

- اعمل configuration للfirewall علشان اعرف لو فيه SYN scans
- افتح البورتات المهمه بس وافلتر ال ICMP messages واخلى ال IDS وال firewalls اخر اصدار(updated)

**Nmap =>**

هى ال Tool اللى بنستخدمها فى الاغلب لعمل Scanning وهى موجوده على ال kali، هى بحر كبير اوى واستخدامتها كتير واوبشنز كتير جدا بس هركز على شوية options مهمه منها وطبعا كل حاجه مكتوبه فى ال help بتاع ال Tool لازم تبص عليهم.

| option | Description |
|---|---|
| -iL | لو عندى text file ومسجل فيه IPs كتير وعايزه يعمل عليهم check |
| --exclude | بعمل استثناء لرينج معين من ال IPs من انه يفحصها |
| -sL | اعملى list لل IPs اللى حددتهم علشان اعرف ايه المتحدد بالظبط وايه اللى هيعمل عليه |
| -sS | دا ال SYN scan اللى اتكلمنا عنه فوق اللى هو ال half open scan |
| --scanflags | بيخلبنى اتحكم ف ال flags واعملها set و reset، برضو اللى اتكلمنا عنه فوق |
| -p | بحدد rang معين من البورتات علشان يفحصهم (Ex: nmap -p 100-200 192.168.1.15) او ممكن احدد بورت واحد بس |
| -n | بسرع من عملية ال scanning عن طريق تقليل الريزليوشن بتاع ال DNS (مش عارف يعنى ايه بس اشطا بتسرع وخلاص) |
| -sV | لو فى بورت شغال وشغال عليه service معينه بقدر احدد ال version بتاعها علشان لو ال version ده فيه ثغرات استغلها |
| -p- | بيحدد جميع البورتات ويعمل عليها فحص |
| --script | لو هستخدم script من الاسكربتات اللى موجوده ف ال nmap، فى سكريبتات كتير وكل واحد له وظيفه |
| -O | بيحددلى ال operating system اللى شغاله بيه الجهاز |
| -A | بتعمل عدة وظايف منها O- وبتنفذ بعض الاسكريبتات وغيرها علشان تطلع معلومات زياده واكتر دقه |
| -v | بيظهرلى خطوات ال scanning وهو شغال وبيعمل عليه force انه يشتغل بسرعه |
| -T<0-5> | بعد ال T بيتحط قيمه من 0 ل 5 بتحددله الوقت اللى ياخده فى عملية ال scanning (كل ما كان اكبر كل م كان اسرع بس نتايج اقل) |
| -oG | بحط بعده مسار واخليه يخزن ال output بتاعه فى تيكست فايل، وظيفة الكومند انه بيعملى filtering لل output بطريقه معينه |
| -sn | بيعمل normal ping scan (يعنى بيعمل سكان على اذا كان الجهاز شغال ولا لا) |

**About Scripts:**

ال scripts بتاع ال Nmap بتكون موجوده فى المسار ( **/usr/share/nmap/scripts** )، كل سكريبت بيعمل فحص على حاجه معينه، ممكن تدخل تقرا وتجرب وتعرف وظيفة كل ال script .

**Some examples for Nmap: -**

- **nmap <IP>**

  هيعملى scan ويعرف اذا كان الجهاز شغال ولا لا وكمان check لو فيه بورتات مفتوحه ويرجعهالى.

- **nmap -sS -p 80, 139, 445 -n -sV --script=<script> <IP> -oG /root/Desktop/IPs.txt**

  كدا بعمل TCP SYN scan وبعمل check على بورت 80 و 139 و 445، وبنفذ script معين وبخزن الناتج فى ملف تيكست على طريقة ال grepping و n- علشان اسرع العمليه بانى معملش DNS lookup و sV- علشان لو فيه service شغاله يرجعلى ال version بتاعها.

- **namp -p 139,445 --script=smb* <IP>**

  لما اكون محتاج اجرب اكتر من script على حاجه معينه زى مثلا انى انفذ سكريبت بيعل check على ال SMB protocol فمش لازم اكتب كل سكريبت لوحده وبدل دا ممكن انفذهم كلهم مع بعض عن طريق انى احط (*) بعد كلمة smb وهو كدا هينفذلى كل الاسكربتات اللى بتبدأ ب smb.

- **nbtscan -r <IP>**

كومند بيعملى check على برتوكول netbios اذا كان شغال ولا لا، هو البرتوكول دا بيشتغل على بورتس 139-136 و 445 واقدر اعمل scan عليهم بال nmap برضو.

- **enum4linux -a <IP>**

برضو بيرجعلى معلومات كتير عن بروتوكول ال netbios.

**SNMP protocol:**

- ال SNMP protocol هو اختصار ل simple network management protocol وهو برتوكول بيستخدم فانه بيعمل management للnetworks الموجوده على جهاز معين، ولو البرتوكول دا مفعل بقدر ارجع من خلاله معلومات كتير زى اسماء ال users ومعلومات شامله عن الجهاز والهارد وير الخاص بيه واصدرات قطع الهارد وير وغيرها.
- واحد من التولز اللى بتستخدم فانها ترجع معلومات عن البرتوكول دا هو موديول اسمه **snmp-enum** موجود ف ال metaspoiltable tool ودى tool شبيهه بال recon-ng وهنعرف عنها معلومات اكتر وازاى بنستخدمها بعدين.
- فى tool تانيه موجوده ف الكالى بتقوم بوظيفه مشابهه لل snmp-enum اسمها snmpwalk (اقرا ال help بتاعها و google it).

**Vulnerabilities Scanning:**

هى عملية اكتشاف الثغرات وعلشان نحققها بنستخدم تولز اللى هى :

**Nessus =>**

بعد تسطيب ال nessus بيدينى امر اشغله بيه اللى هو ( /etc/init.d/nessusd start)، وعلشان اعرف حالته هل هو شغال ولا لا بحط status بدل start وعلشان اوقفه بحط stop وبرضو فى restart .

ال nessus ليه Web UI صعب انى اوضح شرحها هنا ف الافضل ان نشوف استخدامها من جوجل او من الدرس **ده** .

**Openvas =>**

بشغل ال openvas بكومند (openvas-start) وعلشان اعرف حالتها هل هى شغاله ولا لا بشوفها فقايمة ال services بكومند (netstat -antp).

زى ال nessus برضو دى UI وصعب شرحها هنا فشوف شرحها من جوجل او من الفديو **ده** .