الجمهورية العربية السورية

جامعة تشرين

كلية الهندسة الميكانيكية والكهربائية

قسم هندسة الاتصالات

كشف هجمات ARPspoofing باستخدام أداة تحليل رزمARP

ARPspoofing detection by python

إعداد:

آصف حسين رزان الشوا

إشراف الدكتور:

مهند عيسى

٢٠٢٠-٢٠٢١

الفهرست:

الغاية من المشروع:

الهدف من هذا البحث استخدام لغة python لتشكيل أداة للحماية من هجمات arp spoofingوزياد امن الحواسيب الشخصية من الاختراق في الشبكات المحلية LAN باستخدام مكتبة scapy بالاعتماد على تفرعاتها وتحليلها الدقيق لجميع طبقات وبروتوكولات العاملة على المعيار العالمي TCP\IP

المقدمة:

يقصد بحماية الشبكات هي حماية بيانات مستخدمي الشبكة من الاختراقات أو الدخول غير المصرح به. وقد يكون من مستخدمين الشبكة أو مستخدمين خارجيين، حيث أن مستخدمين الشبكة لهم صلاحيات محدودة، وأي تعدي للمستخدم خارج نطاق صلاحياته يعتبر اختراق للشبكة، لذلك هناك مجموعة من المعايير التي تمنع أي دخول غير قانوني أو غير مصرح به إلى الشبكة.

يتضمن حماية الشبكات إذن الوصول إلى البيانات في الشبكة والتي يتحكم فيها مسؤول الشبكة، ويتم تعيين معرف أو كلمة مرور أو معلومات مصادقة أخرى تسمح لهم بالوصول إلى البرامج والمعلومات ضمن صلاحيتهم.

ولزيادة أمن المعلومات يتطلب المعرفة بالشبكات والبروتوكولات المستخدمة بها،ومعرفة البنية التحتية للشبكات

تعد لغة pythonمشهورة في مجتمع الأمن المعلوماتي هو أنها قادرة على التعامل مع حزم البياناتdata packetsمن خلال مكتباتها، واهمها مكتبةscapy.
فمن خلال اللغة يمكننا برمجة أدوات خاصة بنا لعمل امر معين او دعم أكثر من أداة في أداة واحدة.

معيار TCP\IP:

هو بروتوكول للاتصالات بين أجهزة الحاسب الآلي للاتصال بشبكة الإنترنت، وهو اختصارللمصطلحTransmission Control Protocol / Internet Protocol.وهو يعني بروتوكول التحكم في نقل البيانات.

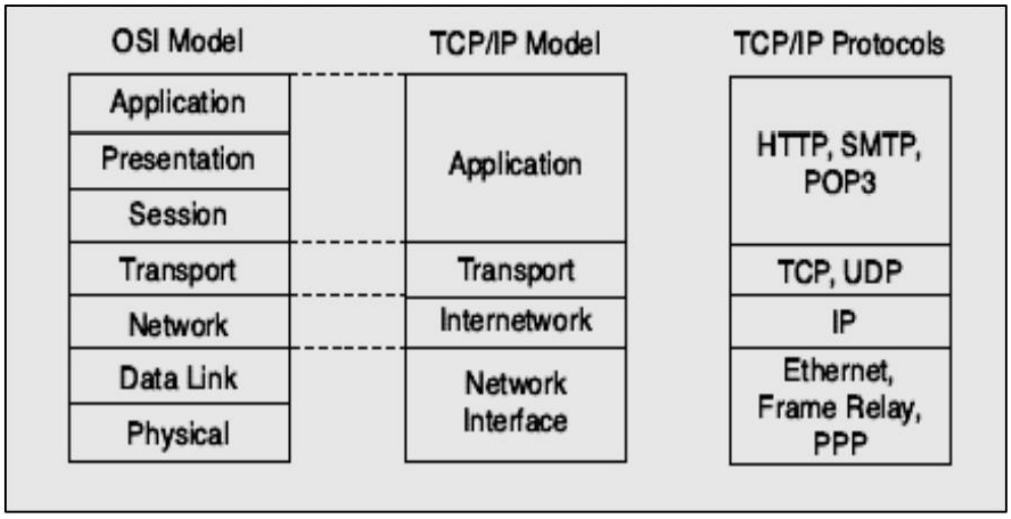
وهو يعد نظام قياسي يحدد كيف يمكن للأجهزة الإلكترونية مثل الحاسب الآلي أن تتصل بشبكة الإنترنت، وكيفية نقل البيانات والمعلومات بين تلك الأجهزة.
كما أنه يعد البروتوكول المتحكم فعلاً في إرسال واستقبال المعلومات داخل شبكة الإنترنت، بل ويضمن أن البيانات قد تم إرسالها واستقبالها بشكل صحيح.

طبقات معيار TCP\IP:

يتكون المعيار العالمي لنقل البيانات TCP\IP من أربع طبقات أساسية والتي تحوي كل طبقة على مجموعة من البروتوكولات التي تستخدم لخدمة عملية النقل بشكل امن وفعال، حيث كل طبقة تقدم خدماتها للطبقة الأعلى منها.

- وتتضمن أسباب تقسيم وظائف الشبكة التالي:
- تقسم الجزيئات المرتبطة بالعمليات المتبادلة بالشبكة إلى عناصر أقل تعقيدا.
- تحديد الواجهات القياسية الخاصة لسرعة الترابط والتوصيل والتشغيل والتكامل بين الأجهزة المختلفة.
- تمكين المهندسين من تركيز جهودهم التصميمية والتطويرية على وظائف طبقة معينة.
- ترقية التماثل بين وظائف الأقسام المختلفة المكونة للشبكات البينية بهدف قابلية التشغيل المتبادل.
- منع التغيرات في ناحية ما لتأثيرها بشكل كبير على النواحي الأخرى، حتى تتمكن كل ناحية من التطور بسرعة أكبر.
- تقسيم عمليات التشبيك البيني للشبكة إلى أقسام فرعية منفصلة حتى يمكن تعلمها بسهولة أكبر.

- طبقات معيار TCP\IP:



الشكل (١) يبين الطبقات في النموذجين ((TCP/IP), (OSI))

والطبقات هي:

١)- التطبيقات (Application):

توفر طبقة التطبيقات خدمات الشبكة لتطبيقات المستخدم. مثل: تطبيقات معالجة النصوص بواسطة إرسال الملفات الموجودة في هذه الطبقة.وتدعم طبقة التطبيقات (الطبقة٥) في سياق الطراز(TCP/IP)المرجعي،مكون الاتصال في أي تطبيق . بالرغم من أنها لا تقدم خدمات لأي طبقة (TCP/IP) أخرى لكنها تقدم خدمات لعمليات التطبيق الموجود خارج نطاق الطراز (TCP/IP) (مثلاً، برامج الصفحات الإلكترونية،www, Telnet, الخ) الذي بإمكانه أن يعمل كلياً باستعمال فقط المعلومات التي تتواجد في الحاسب . لكن قد يملك تطبيق أخر حيث يمكن لمكون الاتصال أن يتصل بواحد أو أكثر من التطبيقات الشبكية. إن مثالاً عن هكذا تطبيق قد يتضمن معالج نصوص يمكنه أن يتضمن مكون إرسال ملفات يتيح إرسال مستند إلكترونياً عبر شبكة. ومكوّن إرسال الملفات يؤهل معالج النصوص كتطبيق في السياق (TCP/IP) , وبالتالي ينتمي إلى (الطبقة ٥) للطراز (TCP/IP) المرجعي .مثال آخر عن تطبيق حاسوبي فيه مكونات إرسال بيانات هو مستعرض(Internet Explorer) . حيث ُترسل الصفحات إلى الحاسوب كلما تمت زيارة موقع (web).

٢)-النقل (Transport):

تقسم هذه الطبقة وتعيد تجميع البيانات في دفق البيانات (TCP ,data stream) هو أحد البروتوكولات في هذه الطبقة المستعمل مع (Ip) . وهي مسؤولة عن إرسال وتنظيم انسياب المعلومات من المصدر إلى الوجهة بشكل موثوق به ودقيق، وتتضمن وظائفها:

- مزامنة الاتصال.
- التحكم بالانسياب.
- الاستعادة من الخطأ.
- الموثوقية من خلال النوافذ.

تمكن طبقة النقل (الطبقة ٤) جهاز المستخدم من تجزئة عدة تطبيقات تابعة لطبقة أعلى لوضعها على نفس دفق بيانات (الطبقة ٤) , وتمكن جهاز المتلقي من إعادة تجميع أقسام تطبيق الطبقة الأعلى . دفق بيانات (الطبقة ٤) هو اتصال منطقي بين نقاط النهاية في الشبكة، ويقدم خدمات إرسال من مضيف إلى وجهة معينة تسمى هذه الخدمة أحياناً خدمة طرف لطرف.

عندما ترسل طبقة النقل أقسام بياناتها فإنها تضمن أيضاً تكاملية للبيانات. حيث أن هذا الإرسال هو علاقة ذات موثوقية عالية بين الأنظمة المتصلة. فيما يلي بعض الأسباب لإنجاز إرسال موثوق:

- إنها تضمن أن المرسلين يتلقون إشعاراً بالأقسام المسلّمة.
- إنها تهتم بإعادة إرسال كل الأقسام التي لم يتم تلقي إشعار بها.
- إنها تقدم تجنّباً للازدحام وتحكماً.

إحدى المشاكل التي يمكن أن تحدث خلال إرسال البيانات هي جعل الذاكرة المؤقتة (Buffers) تفيض في أجهزة التلقي . ويمكن أن يسبّب الفيضان حدوث مشاكل خطيرة تؤدي إلى خسارة البيانات. تستعمل طبقة الإرسال طريقة تدعى تحكماً بالانسياب لحل هذه المشكلة.

- وظائف طبقة النقل:

تنفذ كل طبقة من طبقات المستوي الأعلى وظائف خاصة بها. لكن وظائفها تعتمد على خدمات الطبقات الأدنى. كل الطبقات العليا الأربع – طبقة البرامج تعتمد على طبقة العرض وبدورها تعتمد على طبقة الجلسة وبدورها الأخيرة تعتمد على طبقة النقل.

تفترض طبقة النقل أنه يمكنها استعمال الشبكة كغيمة لإرسال رزم البيانات من المصدر إلى الوجهة. إذا فحصت العمليات التي تجري داخل الغيمة، يمكنك رؤية إحدى الوظائف تستلزم انتقاء أفضل المسارات لمسلك معين.

٣)- الشبكة (Network): تحدد هذه الطبقة أفضل طريقة لنقل البيانات من مكان إلى آخر.حيث تعمل الموجّهات في هذه الطبقة. وأيضاً نظام عنونة بروتوكول الإنترنت (Ip) في هذه الطبقة.عندما يحتاج برنامج مضيف إلى إرسال رزمة إلى وجهة في شبكة مختلفة. يعنون المضيف إطار وصلة البيانات إلى الموجّه، باستعمال عنوان إحدى واجهات الموجّه. تقوم عملية طبقة شبكة الموجّه بفحص مقدمة الرزمة الواردة لتحديد الشبكة الوجهة، ثم تستشير جدول التوجيه الذي يربط الشبكات بالواجهات الصادرة. يتم تغليف الرزمة مرة أخرى في إطار وصلة البيانات الملائم للواجهة المنتقاة، وتوضع في الطابور لتسليمها إلى الوثبة التالية في المسار.

تجري هذه العملية كلما تم تمرير رزمة من خلال موجه آخر. في الموجّه الموصول بشبكة المضيف الوجهة، يتم تغليف الرزمة في نوع إطار وصلة البيانات التابعة لشبكة المناطق المحلية الوجهة ويتم تسليمها إلى المضيف الوجهة.

٤)- وصلة البيانات (Data link): تحضر هذه الطبقة وحدة بيانات (أو رزمة)لإرسالها مادياً عبر الوسائط . كما إنها تتولى مسألة الإعلام عن الأخطاء، وطبيعة الشبكة، والتحكم بالوصول إلى الوسائط.

٥)- المادية أو الفزيائية (Physical): تقوم هذه الطبقة بالتحكم بالوسائل الكهربائية والميكانيكية والإجرائية للتنشيط والمحافظة على الوصلة المادية بين الأنظمة. وهي وسائط مادية كالأسلاك الزوجية المفتولة والمتحدة المحور والألياف الضوئية.

بروتوكول دقة العناوين Address Resolution protocol(ARP):

هو بروتوكول يعمل على طبقة NETWORK وهو واحد من أهم البروتوكولات الموجودة في عالم الشبكات لأهميته الكبيرة وهو خطر جدا في نفس الوقت وتعود أهميته للوظيفة الأساسية التي يقوم بها على الشبكة فهو يقوم بعملية تحديد العنوان الفيزيائي أو (MAC Address) الخاص بعنوان IP معلوم لدينا مسبقا وأبسط مثال على ذلك هو (GATWAY) للشبكة , فمثلا في حال أردنا الوصول إلى شبكات أخرى أو الاتصال عبر الإنترنت , يتوجب علينا تحديد IP المنفذ الذي يربطنا مع الراوتر والذي يطلق عليه (GATWAY) لذا نقوم يدويا بتحديده , أو يتم إرساله لنا أوتوماتيكيا من خلال (DHCP) ومن المؤكد أن أنك سوف تلاحظ أننا حددنا IP ولم نحدد (MAC ADDRESS)وطبعا بدونه لن تتم عملية الاتصال مع المنفذ , لذا هنا سوف يأتي دور بروتوكول ARP لكي يقوم أوتوماتيكيا بالبحث وتحديد MAC ADDRESS

من خلال طلب خاص يسأل فيه الأجهزة الموجودة على الشبكة عن عنوان (MAC ADDRESS) لهذا IP أما خطورته تكمن في حدوث عملية تزوير مثل هذه الأنواع من الرسائل.

إن بروتوكول ARP هو بروتوكول طبقة ثانية يقوم بإيجاد عنوان MAC عندما يكون عنوان IP معروفا ويحافظ أيضاً في جدول ARP على تخطيط العناوين ما بين IP-MAC ضمن الذاكرة المخبئية cache.

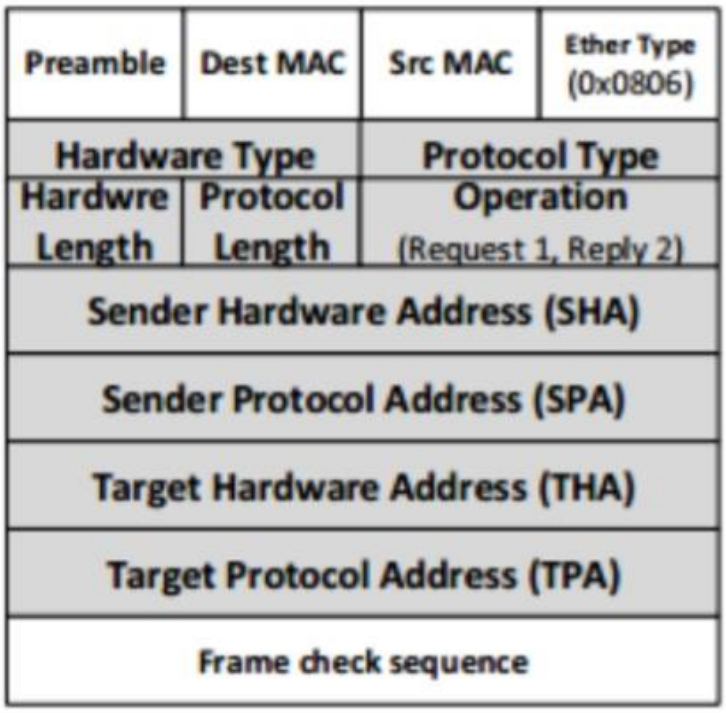
والشكل الآتي يبين مثال عن جدول ARP:

```
Router#show ip arp

Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  172.16.233.229   -          0000.0c59.f892  ARPA   Ethernet0/0
Internet  172.16.233.218   -          0000.0c07.ac00  ARPA   Ethernet0/0
Internet  172.16.168.11    -          0000.0c63.1300  ARPA   Ethernet0/0
Internet  172.16.168.254   9          0000.0c36.6965  ARPA   Ethernet0/0
```

الشكل (٢) مثال عن جدول ARP ضمن ذاكرة Cache في موجه cisco

تتكون بنية إطار ARP بشكل عام من الحقول المبينة في الشكل (٣)



الشكل (٣): بنية إطار ARP

الحقول الرئيسية لهذا البروتوكول هي:

Sender Hardware Address(SHA) : العنوان الفيزيائي للمرسل MAC.

Target Hardware Address(THA) : العنوان الفيزيائي للهدف MAC .

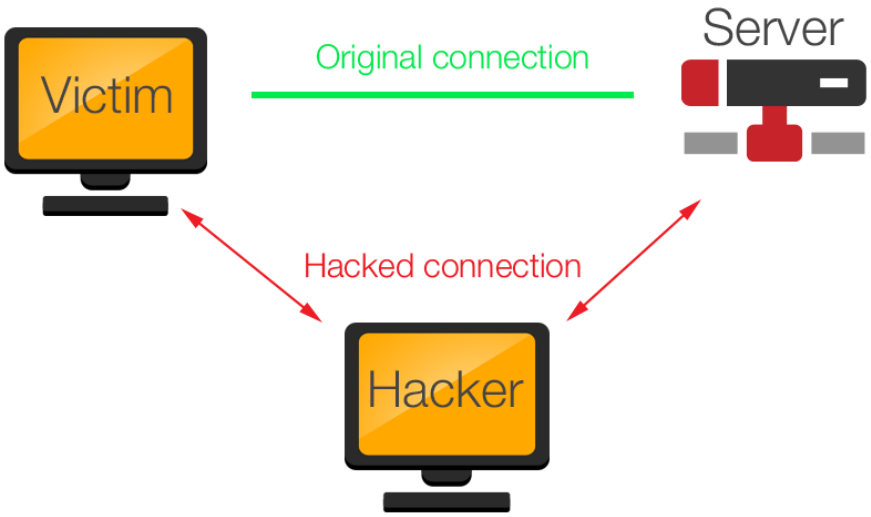
Sender Protocol Address(SPA) : العنوان المنطقي للمرسل IP .

Target Protocol Address (TPA) : العنوان المنطقي للهدف IP .

عندما تريد عقدة ما أن ترسل بياناتها إلى عقدة أخرى، فإنها تحتاج إلى إنشاء إطار والذي بدوره يجب أن يحتوي على عناوين Mac لكل من العقدتين المصدر والهدف. تقوم العقدة المرسلة بفحص جدول ARP الخاص بها لإيجاد عنوان Macللهدف. في حال لم يكن عنوان Macموجوداً تقوم هذه العقدة بإرسال طلب ARP (ARPrequest) كرسالة بث مجموعاتي إلى جميع العقد الموجودة ضمن شبكة LAN بحيث يكون حقل عنوان Mac للهدف في طلب ARP هوFF-FF-FF-FF-FF-FF تستقبل كل العقد ضمن LAN طلب ARP.

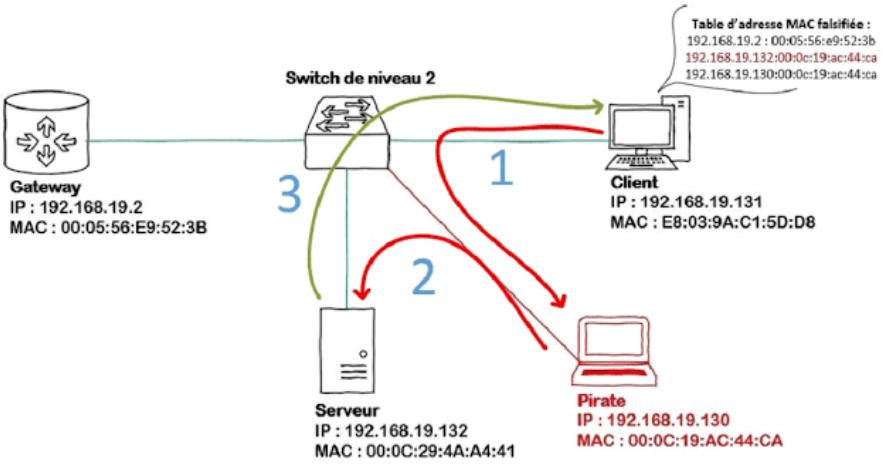
هجوم ARP Spoofing ماهو؟

هو نوع من الهجمات التي تستهدف الشبكات من المستوى الثاني، خصوصا من موديلOSI ، ويعتبر من أكثر الهجمات على الشبكة خطورة وشيوعا، وتؤدي الى ما يسمى بهجوم الـ (Man in the middle).



كيفية الهجوم؟

فكرة الهجوم غالبا ما تكون من أبسط الخطوات في عملية الاختراق، فبعد وصول الاستجابة من الجهاز، يحفظ العنوان الفيزيائي(Mac Address) و العنوان المنطقي (IP) في جدول يسمي الـ (Arp Table)، وذلك حتي يكون الوصول أسهل حالة الإتصال بالجهازين في المرة القادمة، وهذه العملية غالبا ما تكون عملية مؤقته تنتهي بمجرد إغلاق الجهاز، من هنا من هذه الخطوة يبدأ المهاجم هجومه فهو وبكل بساطة يرسل (Arp Replay) مزور لأحد الأجهزة الموجودة على الشبكة، وكأن الطلب قد صدر من الجهاز نفسه، وبناء على ذلك يتم تعديل جدول الـ (ARP) ومن هنا يبدأ الجهاز المخترق بإرسال بياناته إلى جهاز المخترق علي اعتبار أنه الراوتر، مستغلا بذلك مرور كل البيانات من خلاله.
وبالتالي فقد تمكن المخترق من تحويل جهازه الى مايعرف باسم الـ (MITM) أي (Man in the middle).
هذه الصورة للتوضيح:



إن جهازك متصل بالراوتر، الراوتر متصل بالإنترنت، جهازك يرسل طلب دخول إلى موقع معين، فيتواصل الراوتر مع الموقع، فيجيب الموقع، فتحصل بذلك على الـ (Arp-Spoof) ويعمل جهازك كأداة تجسس في المرحلة الأولى وهي لحظة تمرير طلبك إلى الراوتر، في المرحلة الأخيرة التي يرسل لك الراوتر فيها رد طلبك، يعمل هو الآن كأداة تجسس ويرى كل ما يحدث بينك وبين الراوتر بمنتهى السلاسة.

الأدوات المستخدمة في هجوم الـ (Arp-Spoofing) و(MITM)

الكثير من الأدوات التي تستخدم في هذا الهجوم ولكن أشهرها(DNS Sniff)، (Ettercap)، والبرنامج الغني عن التعريف(NetCut)، على الرغم من أن برنامج (NetCut)لا يقوم بتنفيذ هجوم الـ (MITM)إلا أن فكرة عمله واحده، وهي تغيير الـ(Getway)، يبقي لك أن تعلم أن هذه البرامج لا تحتاج إلى احترافية كبيرة.

كيف تحمي الجهاز من هذه الهجمات؟

إن أفضل طريقة لحماية جهازك من هذه الهجمات هو أن تقوم بعمل Static ARP لـ Getway الخاص بالشبكات العامة أو المفتوحة، أو أن تستخدم بعض البرامج المتخصصة لذلك والتي تقوم بتغيير الـ Mac Address الخاص بجهازك قبل اتصالك بالشبكات المشكوك فيها او العامة بشكل خاص.
أما أن كنت تحاول أن تتصل بأحد الأجهزة الموجودة على السيرفر عن بعد، فيجب عليك استخدام الـ SSH فهو يؤمن لك سرية كاملة لبياناتك، ويوجد أيضا بعض البرامج التي تمكنك من مراقبة وتتبع الترافيك الخاص بالشبكة ومنها (Snort)-(XARP ومن وظائفهما مراقبة الترافيك ومراقبة عملية الـ Mapping والتي تحدث على الـ Arp Cash.

في هذا البحث لقد قمنا باستخدام أداة تقوم بتحليل رزم arpوإعلام الضحية فور تعرضه للهجوم وذلك باستخدام لغة pythonومكتبة scapy

التطبيق العملي :

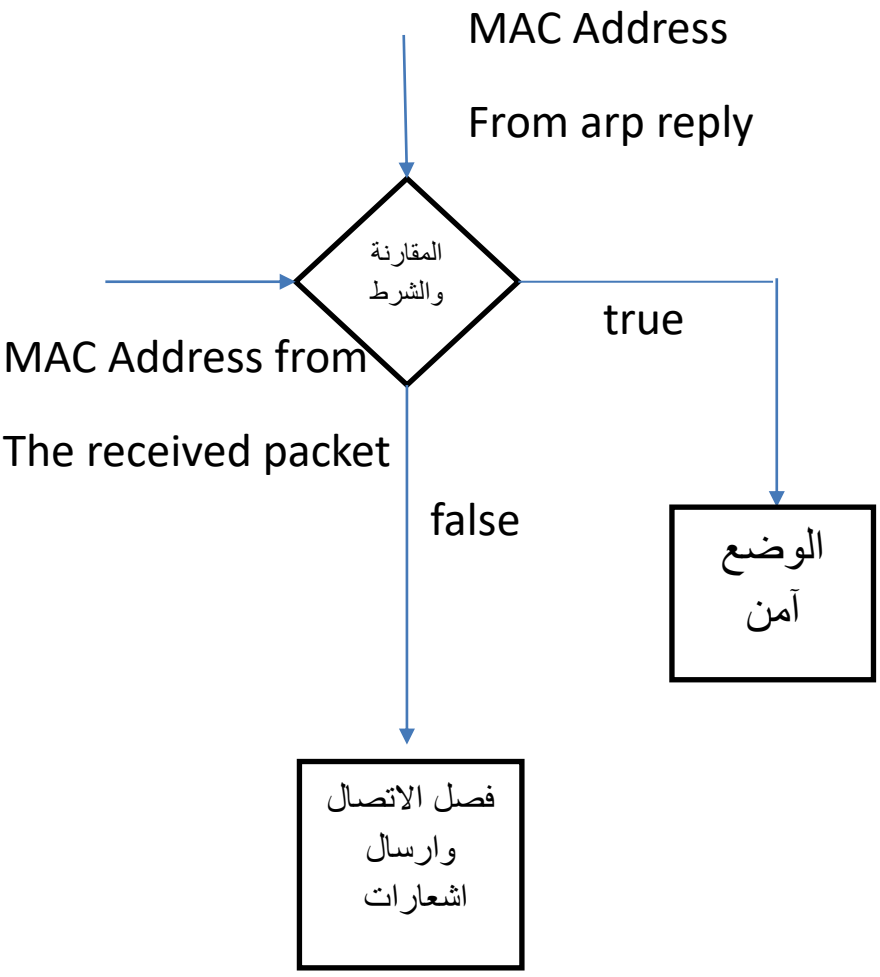
Scapy

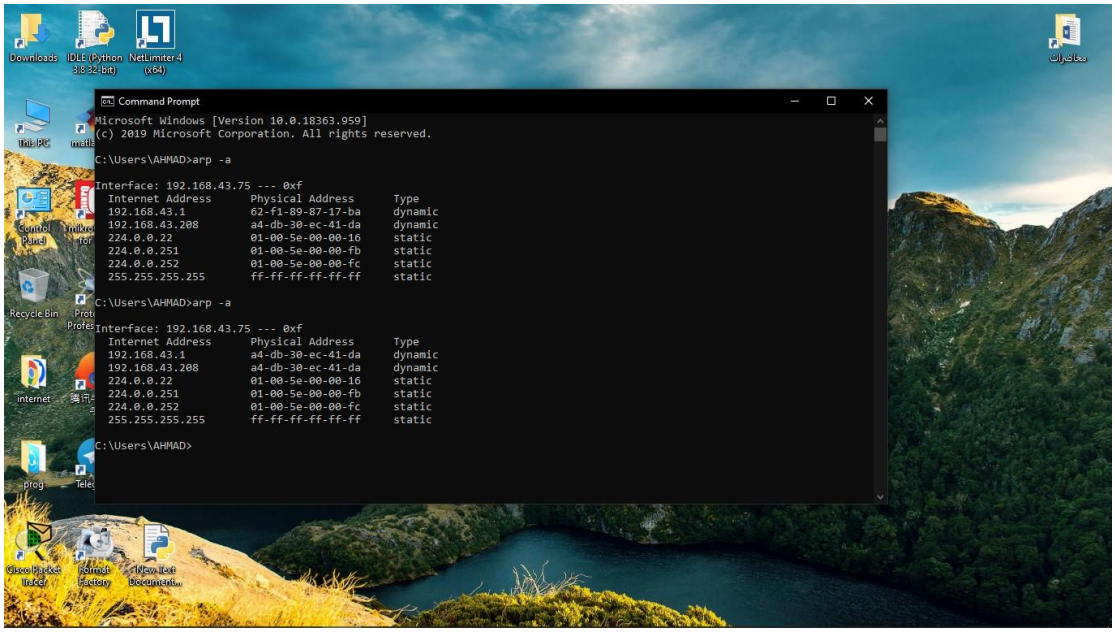
تعتبر مكتبةScapyمكتبة تفاعلية قوية في مجالها وهو التعامل مع حزم الشبكات المختلفة حيث بإمكانها إعادة صياغة و فك شفرات الحزم لمجموعة واسعة من البروتوكولات المختلفة بعد ذلك تقوم بإرسالهم إلى الشبكة أو التقاطها ، القيام بعملية تطابق بين الطلبيات والردود والكثير من الأمور ، كما يمكن لهذه المكتبة القيام بمعظم عمليات الخاصة بالشبكات المختلفة مثل : المسح ، تتبع مسار الشبكة، فحص الوحدات، الهجوم أو اكتشاف الشبكات ،كما يمكن لها أن تقوم بما يقارب ٨٥٪ من عمليات برنامجnmap،tcpdumpوالكثير من عمليات الهجوم المختلفة.
كما يمكن لهذه المكتبة القيام بعمليات محددة لا يمكن لمعظم البرامج القيام بها مثل : إرسال حزم غير صحيحة ، حقن الإطار ٨٠٢,١١، فك تشفيرvoipعلى القنوات المشفرة ب. WEP

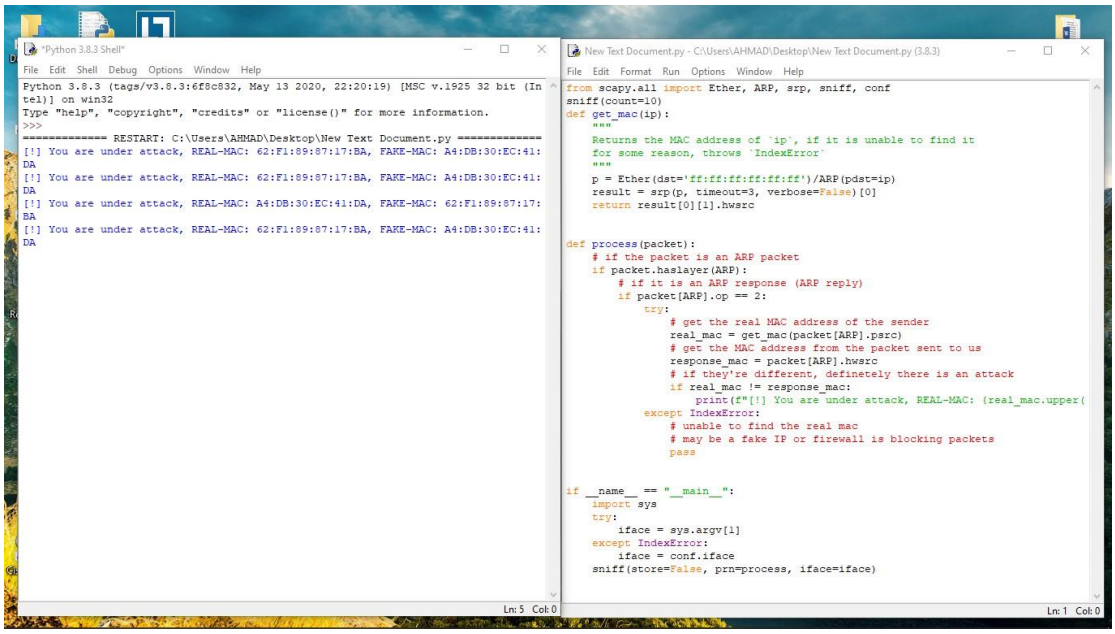
فكرة الكود البرمجي:

يعمل البرنامج على المقارنة بين عنوانين فيزيائيين لاكتشاف الهجوم وذلك من خلال إرسال رسالة للمرسل بإعطائه العنوان الفيزيائي الخاص به وثم مقارنته مع العنوان الفيزيائي الموجود في الباكيتات المستقلة فاذا كان هنالك اختلاف فان المستقبل يتعرض للهجوم وإذا كانا متماثلين فان المستقبل أمن .

مخطط صندوقي







الصورة الأولى: عملية الهجوم وتغير عنوان MAC Address

الصورة الثانية: توضح عمل الكود البرمجي في كشف الهجوم

المراجع:

-Philippe BIONDI, Corporate Research Center, Packet generation and network based attacks with Scapy

-Behrouz A. Forouzan , De Anza College, DATA COMMUNICATIONS AND NETWORKING