Post Connection Attacks

Ataques pós-conexão

All the attacks we carried out in the previous sections can be done without knowing the key to the AP[1], i.e.[2]: without connecting to the target network.

Todos os ataques que realizamos na seção anterior podem ser feitos sem o conhecimento da chave do **Access Point,** isto é, sem se conectar com o alvo.

We saw how we can control all the connections around us, gather some information, sniff[3] packets and crack WEP/WPA/WPA2 keys.

Nós vimos como nós podemos controlar todas as conexões ao nosso redor, obtendo informações, sniff pacotes e crackeando chaves WEP/WPA/WPA2.

In this section, we shall have a look on more sophisticated attacks that can only be used after connecting to the target AP.

Nesta seção nós devemos mostrar ataques mais sofisticados que podem somente ser usados depois da conexão com o algo no AP.

Gathering Information

Obtendo informações

In section 1 we saw how we can user airodump-ng to discover all the AP's around us and the clients associated with them.

Nesta primeira seção, nós vimos como nós podemos usar **airodump-ng** para descobrir todos os AP's ao nosso redor e os clientes associados com eles.

Now that we are connected to a specific AP, we can gather more detailed info about the clients connected to this AP.

Agora que nós estamos conectados com um específico AP, nós podemos obter mais detalhes sobre os clientes conectados no AP.

---

[1] Assess Point – Ponto de acesso – modem – roteador – switch ou outro equipamento que conecta ou redireciona a internet.
[2] ABBREVIATION -- that is to say (used to add explanatory information or to state something in different words): "a walking boot that is synthetic, i.e., not leather or suede"
[3] Um programa ou equipamento que monitora dados pela internet. Sniffers podem ser usados legitimamente para o gerenciamento da internet ou para ações mais obscuras como roubo de informações.

There is a number of programs that can be used to do this, we shall talk about 3 programs starting with the simplest and quickest one.

Há um número de programas que podem ser usados para isto, nós devemos falar sobre 3 programas começando com o mais simples e rápido dentre eles.

--

Netdiscover

Netdiscover is a program that can be used to discover the connected clients to our current network, its very quick but it does not show detailed information about the clients: IP , MAC address and some times the hardware manufacturer for the client's wireless card.

Netdiscover é um programa que pode ser usado para descobrir os clientes conectados com a nossa corrente network, é muito rápido mas não mostra muitos detalhes sobre os clientes: IP, endereço MAC e algumas vezes o hardware (fabricante) para o cartão da rede sem fio.

Usage:

Comando:

netdiscover -i [INTERFACE] -r [RANGE]

ex: netdiscover -i wlan0 -r 192.168.1.1/24

Você pode usar wlan de maneiras diferente, pensar que o curso Ethical Hacker não evidencia um rastreamento de todas as funções que a placa wireless capta.

Autoscan

Autoscan is another program that can be used to discover the connected clients to our current network, its not as quick as net discover, but it shows more detailed information about the connected devices and it has a graphical user interface.

Autoscan é outro programa que pode ser usado para descobrir os clientes conectados com a nossa corrente network, não é tão rápido quanto o net discover, mas mostra mais detalhes sobre os equipamentos conectados e tem uma aparência gráfica mais acessível.

You can download Autoscan from:

Você pode baixar Autoscan de:

Then open the directory where you extracted it and run

Então abra a pasta onde você extraiu e execute

http://autoscan-network.com/download/

./AutoScan*.sh

--

Nmap

Nmap is a network discovery tool that can be used to gather detailed information about any client or network. We shall have a look on some of its uses to discover connected clients and gather information about them.

Nmap é uma ferramenta de descobrimento que pode ser usada para obter detalhes sobre qualquer cliente ou network. Nós devemos olhar em alguns usos para descobrir clientes conectados e obter informações sobre eles.

Nmap

We are going to use Zenmap – the GUI for Nmap.

Nós usaremos Zenmap – o GUI para Nmap.

1. Ping[4] scan: Very quick – only shows connected clients.

1. Ping scan: muito rápido – somente mostra clientes conectados.

2. Quick scan plus: Quick – shows MAC and open ports.

2. Quick scan plus: rápido – mostra Mac e portas abertas.

3. Quick scan plus: Slower then the 2 above, more detailed info.

3. Quick scan plus: devagar em relação aos acima, mais informações detalhadas.

These are just sample scans, you can experiment with the scan options and see the difference between them.

Há justamente sample scans, você pode experimentar com o scan opções e ver a diferença entre eles.

https://nmap.org/zenmap/man.html **Zenmap – the GUI for Nmap**

https://sourceforge.net/projects/nmapfe-win/ **Nmap GUI for Windows**

---

[4] Computing: query (another computer on a network) to determine whether there is a connection to it.

Man In The Middle Attacks[5]

Ataque homem no meio (tradução sugerida por um site português-Portugal, mas sei que não há consenso entre as traduções).

ARP Poisoning

This is one of the most dangerous and effective attacks that can be used, it is used to redirect packets to and from any client to our device, and since we have the network key, we can read/modify/drop these packets. This allows us to launch very powerful attacks.

Isto é um dos mais perigosos e efetivos ataques que podemos utilizer, é usado para redirecionar pacotes para e de qualquer cliente para nosso equipamento, e desde que nós já temos a chave da network, nós podemos ler, modificar, baixar estes dados/pacotes. Isto permite-nos lançar ataques poderosos.

It is very effective and dangerous because it's very hard to protect against it as it exploits the insecure way that ARP works.

É muito efetivo e perigoso por que é muito difícil de se proteger contra, assim como há maneiras de explorar e trabalhar com ARP.

Man In The Middle Attacks

ARP Poisoning

ARP main security issues:

ARP principais questões sobre segurança:

1. Each ARP request/response is trusted.

1. Cada ARP requisição/resposta é confiável.

2. Clients can accept responses even if they did not send a request.

2. Clientes podem aceitar respostas mesmo que eles não enviassem uma requisição.

We can exploit theses two issues to redirect the flow of packets in the network.

Nós podemos explorer estas duas questões redirecionando o pacote de fluxo na internet.

We will first send an ARP response to the client telling it that “I am the Router”, this done by telling the client that the device with the router IP address has MY MAC address.

Nós primeiramente enviaremos um ARP response para o cliente dizendo que “Eu sou o Router”, isto feito dizendo para o cliente que o aparelho com o roteador IP address tem Meu MAC address (endereço).

---

[5] https://blog.kaspersky.com.br/what-is-a-man-in-the-middle-attack/462/ **O que é um Ataque Man-in-the-Middle?**

Then we will send an ARP response to the router this time telling it that “I am the client”, this done by telling the router that the device with the client ip address has MY MAC address.

Depois nós iremos enviar um ARP response para o router, desta vez dizendo que (Eu sou o cliente), isto feito dizendo para o router que o device com o cliente IP address tem MEU MAC address.

This means that the router thinks that I am the client, and the client thinks that I am the router. So my device is in the middle of the connection between the client and the router, ie:every packet that is going to/from the client will have to go through my device first.

Isto significa que o router pensa que eu sou o cliente, e que o cliente pensa que eu sou o router. Então meu aparelho é um intermediário (ponto central) da conexão entre o cliente e o Router, isto é, todo pacote que está sendo enviado para/do cliente terá que passar pelo meu device.

ARP Poisoning

arpspoof

Arpspoof is a tool part of a suit called dsniff, which contains a number of network penetration tools. Arpspoof can be used to launch a MITM attack and redirect traffic to flow through our device.

Arpspoof é uma ferramenta parte da suíte chamada dsniff, no qual contem um numero de ferramenta para testes de penetração. Arpspoof pode ser usado para lançar um MITM ataque e redirecionar o tráfico fluindo para nosso aparelho ou captador.

1. Tell the target client that I am the router. Diz ao algo que eu sou o router.

arpspoof -i [interface] -t [Target IP] [AP IP]

Ex: arpspoof -i wlan0 -t 192.168.1.5 192.168.1.1

2. Tell the AP that I am the target client. Diz ao AP que eu sou o alvo cliente.

arpspoof -i [interface] -t [AP IP] [Target IP]

Ex: arpspoof -i wlan0 -t 192.168.1.1 192.168.1.5

3. Enable IP forward to allow packets to flow through our device without being dropped. Habilita a emissão de IP para fluir para nosso aparelho sem ser desconectado.

Echo 1 > /proc/sys/net/ipv4/ip_forward

ARP Poisoning

ettercap

Ettercap is a program that allows us to launch a number of MITM attack, in all of the next tutorials we shall use ettercap to launch MITM attacks.

Ettercap é um programa que permite-nos o lançamento de um numero de MITM ataque, nos próximos tutoriais nós devemos usar ettercap para lançar MITM ataques.

Basic ARP poisoning attack and display logins:

ARP poisoning attack básico e logins apresentados:

Ettercap -Tq -M arp:remote -i [interface] [AP MAC]/[AP IP]/[PORT] [TARGET MAC]/[TARGET IP]/[TARGET PORT]

Ex: ettercap -Tq -M arp:remote -i wlan0 /192.168.1.1/ /192.168.1.5/

Ex2: ettercap -Tq -M arp:remote -i wlan0 // #target all networks

Echo 1 > /proc/sys/net/ipv4/ip_forward

MITM – bypassing HTTPS

Websites like facebook, yahoo .... use https in their login pages, this means that these pages are validated using an SSL certificate and there for will show a warning to the user that the certificate is invalid. To bypass this we are going to use a tool called sslstrip which will downgrade https connections to http.

Sites como facebook, yahoo... usam https nas páginas de login, isto significa que essas páginas são validadas usando um SSL certificado e que irão mostrar um aviso dizendo que o certificado está inválido. Para passar isto nós vamos usar uma ferramenta chamada sslstrip no qual irá regredir conexões https para http.

1. Redirect packets to sslstrip so that it downgrades HTTPS connections to HTTP.

> iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 10000

2. Run sslstrip.

> sslstrip -p

3. ARP poison client and AP.

Ettercap -Tq -M arp:remote -i [interface] [AP MAC]/[AP IP]/[PORT] [TARGET MAC]/[TARGET IP]/[TARGET PORT]

Ex: ettercap -Tq -M arp:remote -i wlan0 /192.168.1.1/ /192.168.1.5/

Sniffing Cookies

Session Hijacking

What if the user uses the “remember me” feature ?? If the user uses this feature the authentication happens using the cookies and not the user and password. So instead of sniffing the password we can sniff the cookies and inject them into our browser, this will allow us to login to the user's account without using the password. You can download it from: Then arp spoof you target and run it using :

E se o usuário usar o “Lembre-me”? Quando o usuário usar a opção de autenticação preferindo escolher por logar pelos cookies e não pelo usuário – senha. Então, ao invés de sniffing a senha, nós podemos sniff o cookies e injetar neles no nosso navegador, isto permite-nos logar sem usar senha. Voce pode baixar – https://www.cookiecadger.com/?page_id=19

depois arp spoof seu alvo e rodar usando:

java -jar cookiecadger.jar

MITM – DNS Spoofing

DNS Spoofing allows us to redirect any request to a certain domain to another domain, for example we can redirect any request to facebook.com to a fake facebook page !!

DNS spoofing permite-nos redirecionar qualquer request/requerimento para um certo domínio para outro domínio, exemplo nós redirecionamos qualquer requerimento para facebook.com para um falso facebook.

1. Edit etter.dns to add the dns spoof rules.

> gvim /etc/ettercap/etter.dns

2. Run ettercap to arp poison the target(s) and enable the dns_spoof plugin.

Ettercap -Tq -M arp:remote -P dns_spoof -i [interface] [AP MAC]/[AP IP]/[PORT] [TARGET MAC]/[TARGET IP]/[TARGET PORT]

Ex: ettercap -Tq -M arp:remote -P dns_spoof -i wlan0 /192.168.1.1/ /192.168.1.5

MITM

Ettercap Plugins

● Ettercap plugins allow us to carry out a number of different MITM attacks or help filter the sniffed packets in a certain way.

Ettercap plug-ins permite-nos utilizar um diferente número de MITM ataques ou ajudar filtrar o pacote sniffed numa certa maneira.

● We have already used an ettercap plugin in the dns spoofing video.

Nós já temos usado um ettercap plugin em dns spoofing video.

● There is a number of ettercap plugins , all of which can be used in the same way, therefore we shall only have a look on another example of using a plugin.

Há um numero de ettercap plugins, todos no qual podem ser usados do mesmo jeito, no entanto nós teremos que olhar outro exemplo da utilização do plugin.

Usage:

Ettercap [options] -P [Plugin name] //

Ex: ettercap -Tq -M arp:remote -P dns_spoof -i wlan0 /192.168.1.1/ /192.168.1.5/

MITM – Ettercap Filters

Controlling internet connection – Controlando a conexao na internet

Ettercap filters can be used to carry out extra tasks with ettercap.

Ettercap filtros podem ser usados para carregar tarefas extras com ettercap.

We are going to use a simple filter to disable internet connection to any client in our network without disconnecting it from the network.

Nós vamos usar um simples filtro para desabilitar a conexão da internet para qualquer cliente na nossa network sem desconectar da internet.

Usage:

1. Create an ettercap filter.

> echo “kill();drop(); > drop-packets.filter

2. Compile the filter.

> etterfilter drop-packets.filter -o drop-packets.ef

3. ARP poison client and AP and activate the filter.

Ettercap -Tq -M arp:remote -F [Filter] -i [interface] [AP MAC]/[AP IP]/[PORT] [TARGET MAC]/[TARGET IP]/[TARGET PORT]

Ex: ettercap -Tq -M arp:remote -F drop-packets.ef -i wlan0 /192.168.1.1/ /192.168.1.5/

MITM

Wireshark

Wireshark is a network protocol analyser that is designed to help network administrators to keep track of what is happening in their network and analyse all the packets. Wireshark works by logging each packet that flows through the device.

Wireshark é um protocolo de análise da internet que é designado para ajudar administradores a manter os rastros de tudo que acontece e analisar todos os pacotes. Wireshark funciona logando cada pacote que flui pelo aparelho.

Usage:

> Wireshark

Protecting against MITM attacks

● It is very difficult to protect against MITM attacks, this is due to the fact that they exploit the insecure way that ARP works.

É muito difícil proteger contra MITM ataques, isto é devido ao fato que eles exploram o modo inseguro como ARP funciona.

● Using static ARP tables can protect against MITM attacks but its not practical in large networks. Even in small networks you have to configure ARP tables every time a new device connects to your network.

Usando estatístico ARP tables, podemos proteger contra MITM ataques, mas isto não é praticado em largas networks. Mesmo em pequenas voce terá que configurar ARP tables toda vez que um novo device conectar na sua network.

● We can discover ARP poisoning easily by only looking at our ARP tables.

Nós podemos descobrir ARP poisoning facilmente somente olhando nossos ARP tables.

● If the MAC address of the router changes then we have been poisoned.

Se o MAC address do router mudar então nós estamos sendo envenenados.

There is also tools that would monitor our ARP table automatically and would notify us if anything suspicious happens.

Há ferramentas que monitorariam nosso ARP table automaticamente e faria a ação de nos notificar se qualquer coisa suspeita acontecesse.

● And we can use Wireshark to detect ARP poisoning and other suspicious activities in the network.

E nós podemos usar Wireshark para detector ARP poisoning e outros perigosas atividades na internet.