C|EH™ Certified Ethical Hacker

TRAINNING EDUCATION CENTER

Curso:

(C|EH) V12

CERTIFIED ETHICAL HACKER V12 – EC-COUNCIL

Progresso do curso

Módulo 6. System Hacking

Módulo 7. Malware Threats

Módulo 8. Sniffing

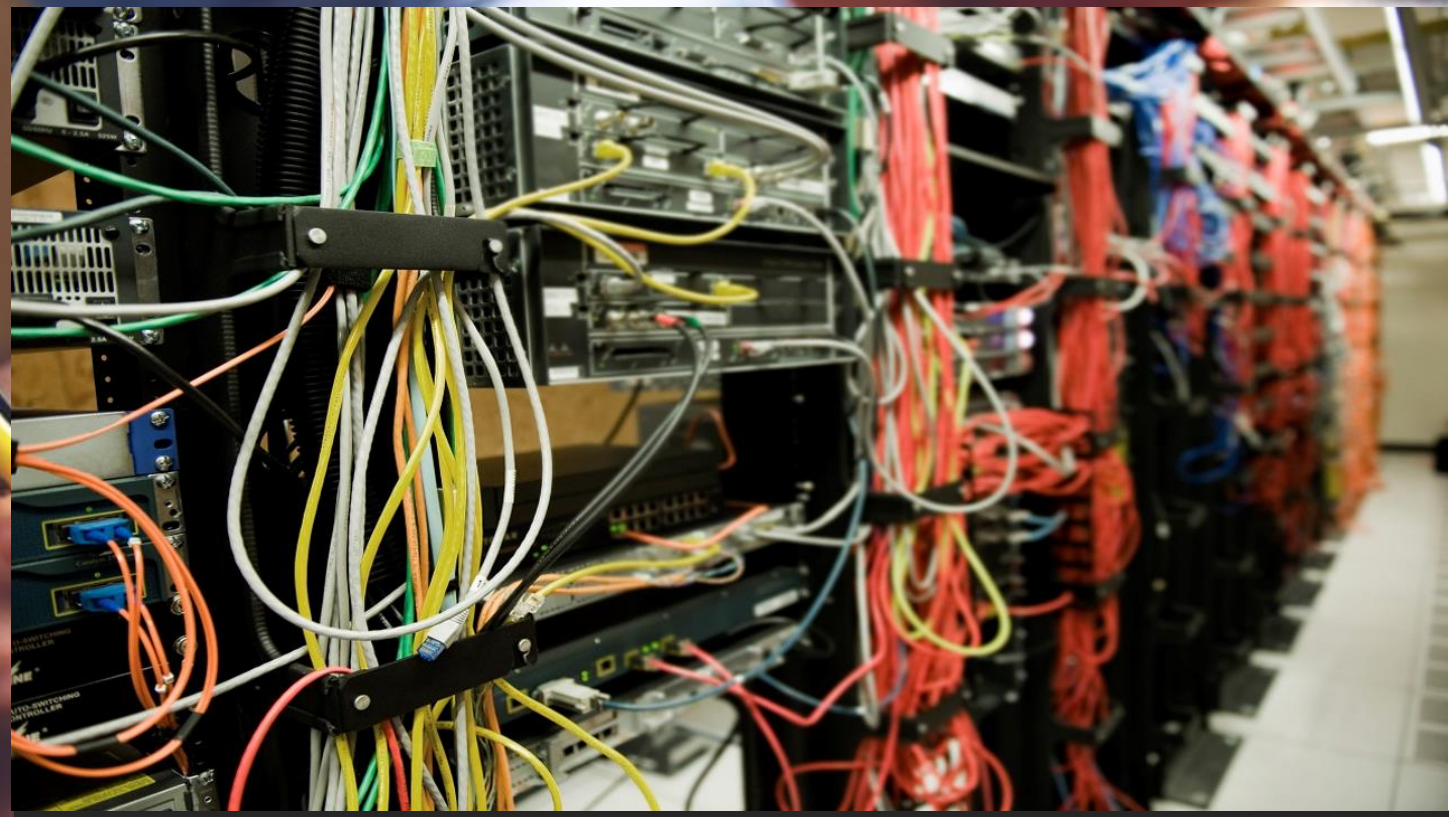
Módulo 9. Social Engineering

Módulo 10. Denial-of-Service (DoS)

Conceitos sobre Sniffing:

Packet sniffing é um processo de monitoramento e captura de todos os pacotes de dados que passam através de uma determinada rede utilizando softwares ou dispositivos de hardware. Isto é possível porque o tráfego em um segmento passa por todos os hosts associados com aquele segmento.

Programas de sniffing desligam o filtro empregado nas placas Ethernet para evitar que a máquina veja o tráfego de outras estações. Assim, os programas sniffing podem ver o tráfego de todos.



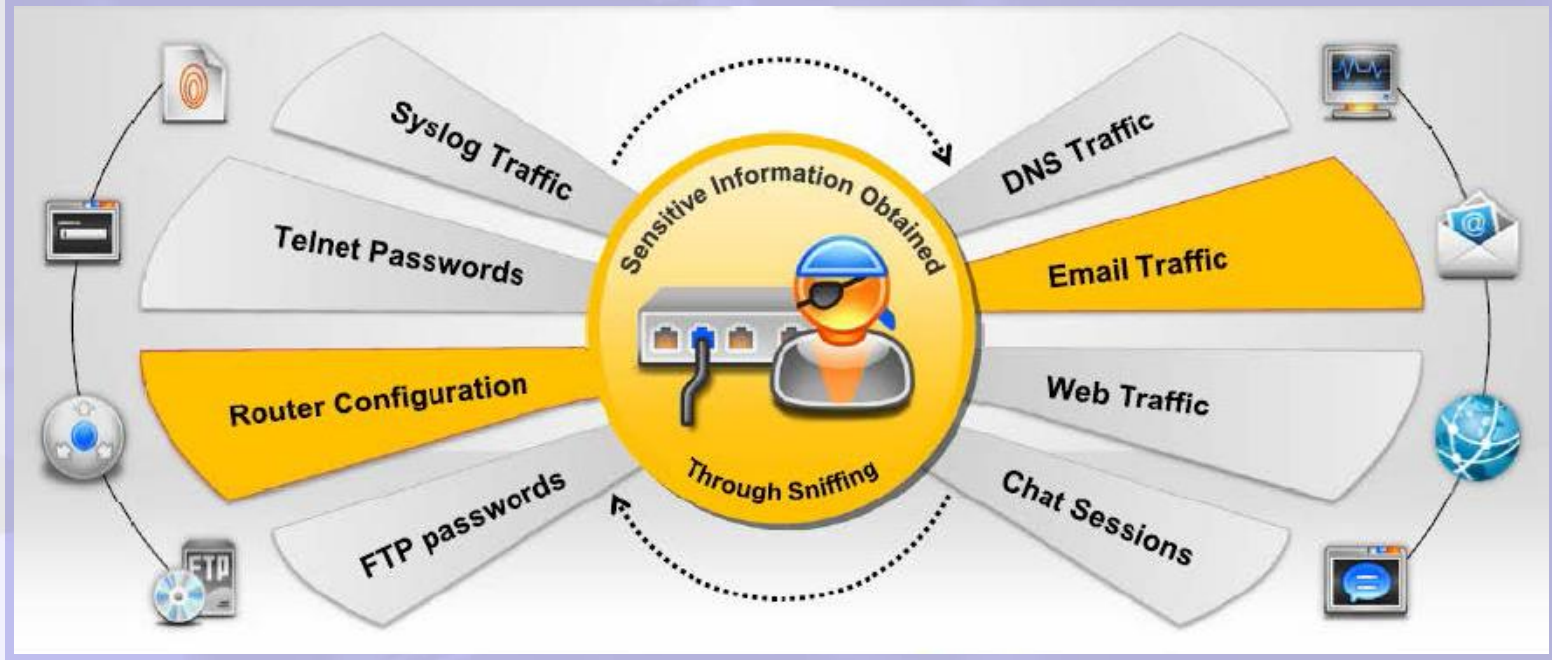
CEHv12

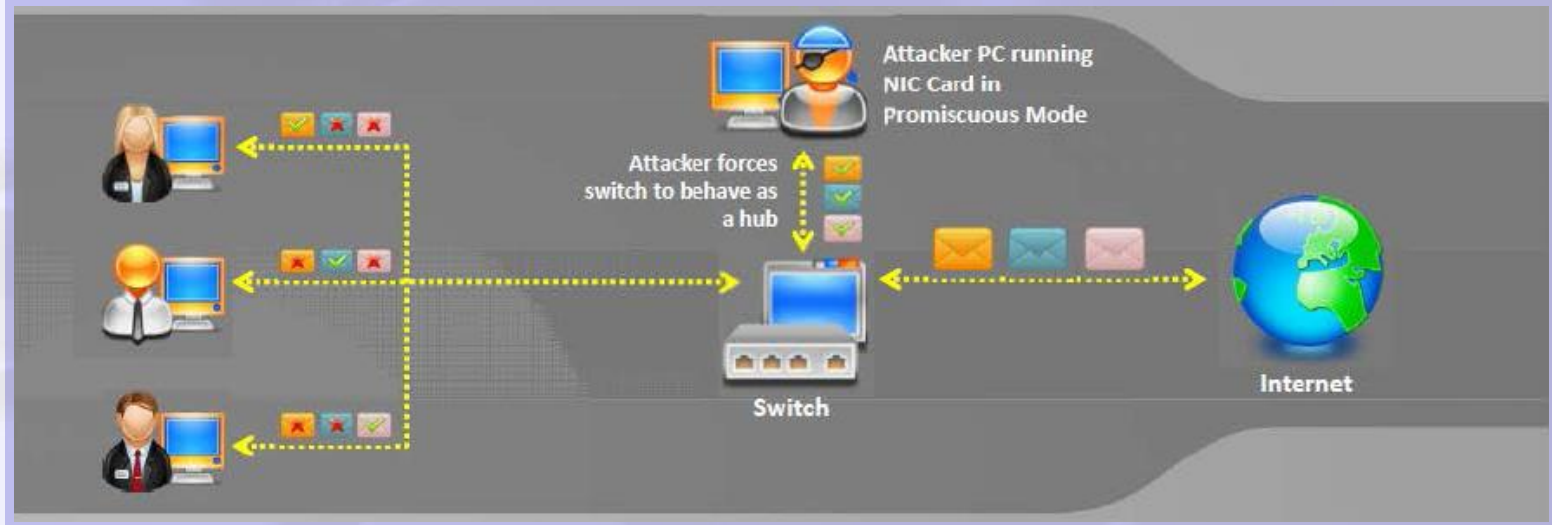
08.Sniffing

TRAINNING
EDUCATION SERVICES

Sniffing

- Embora a maioria das redes de hoje estejam utilizando a tecnologia de "switch", o packet sniffing ainda é muito útil. Ele permite que você observe e acesse todo o tráfego de rede de um ponto. Utilizando sniffers, podemos capturar pacotes de dados que contenham informações sensíveis, como senhas, informações de conta, etc.





Ameaças do Sniffing

Um sniffer é um programa ou dispositivo que monitora os dados que trafegam pela rede. Sniffers podem ser utilizados para atividades legítimas, por exemplo, gestão de rede, bem como para atividades ilegítimas, por exemplo, roubar informações encontradas em uma rede.

Alguns dos pacotes mais simples utilizam uma interface de linha de comando e despejam os dados capturados na tela, enquanto os mais sofisticados utilizam interface gráfica e gráficos de estatísticas de tráfego, eles também podem rastrear várias sessões e oferecem várias opções de configuração.

Tipos de Sniffing

Passivo

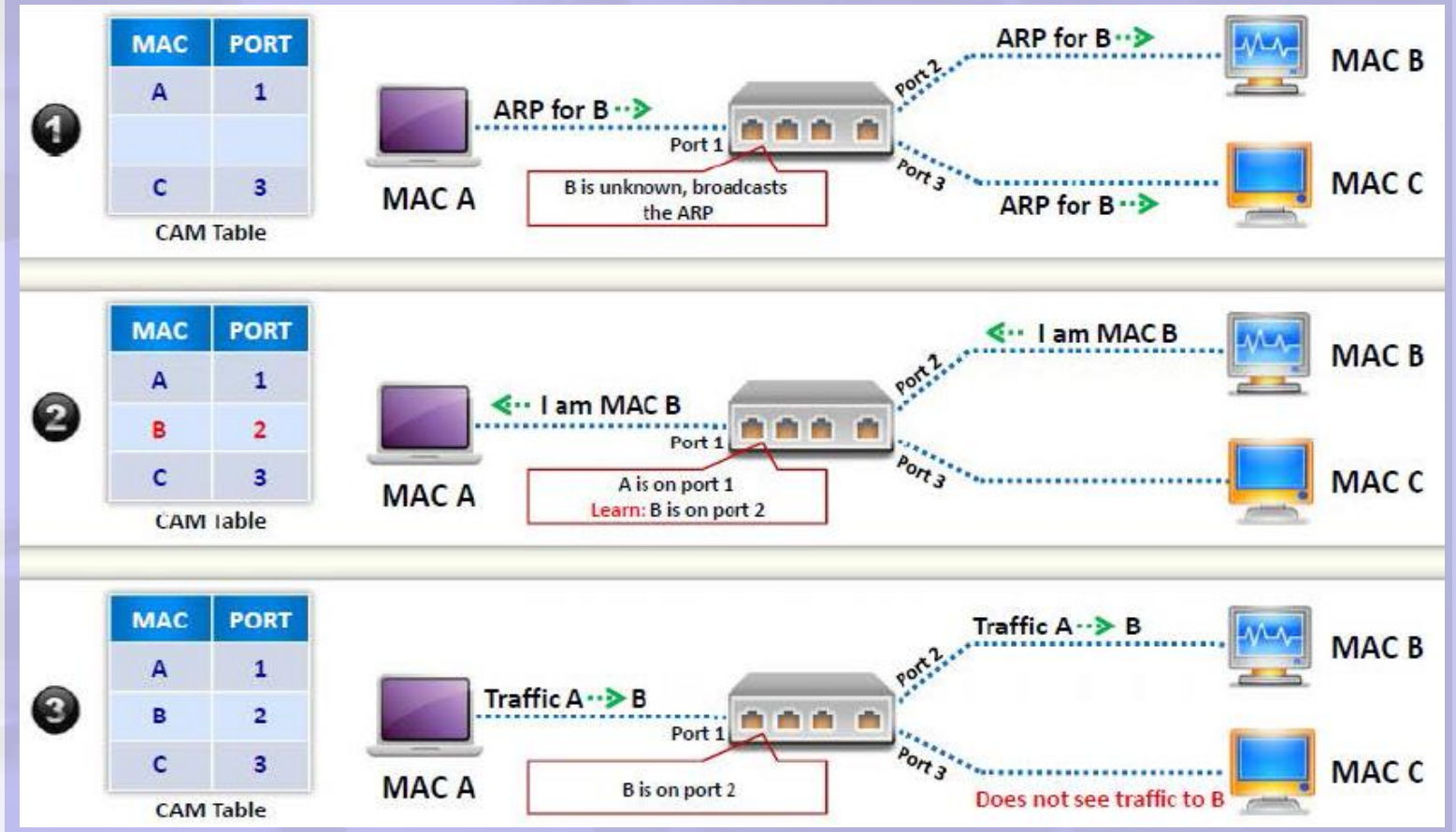
No sniffing passivo não é enviado nenhum pacote na rede, ele só captura e monitora os pacotes enviados por outros hosts. Um sniffer sozinho é raramente utilizado para um ataque, porque este ataque só funciona em um domínio de colisão comum. Domínios de colisão comuns são normalmente encontrados em ambientes com hub. O sniffing passivo é utilizado em uma rede que usa hubs para conectar sistemas. Em tais redes, todos os hosts na rede podem ver todo o tráfego dos demais hosts. Por isso, é fácil de capturar o tráfego que passa pelo centro utilizando sniffer passivo.

Ativo

0 sniffing ativo refere-se ao processo de habilitar o sniffing do tráfego em uma rede injetando ativamente pacotes na rede. No sniffing ativo, a Ethernet não transmite informações a todos os sistemas que estão conectados na LAN como faz em uma rede baseada em hub. Devido a isso, o sniffer passivo não será capaz de capturar dados sobre uma rede comutada. É fácil detectar esses programas e altamente difícil de realizar este tipo de sniffing.

Entendendo ataques MAC

- Um endereço de Media Access Control (endereço MAC) é um endereço de hardware que identifica unicamente cada nó de uma rede. Cada dispositivo na rede tem um endereço MAC associado com uma porta física, o que faz com que seja possível designar um único ponto específico da rede.
- Uma tabela de conteúdo de memória endereçável (CAM) distingue um switch de hub. Ela armazena informações como endereços MAC disponíveis nas portas físicas com os seus parâmetros de VLAN associados. Uma tabela CAM é usada por um switch para armazenar endereços MAC dos dispositivos conectados à rede. Cada MAC em uma tabela CAM é atribuído o número da porta do switch. Com esta informação, o switch sabe para onde enviar os quadros Ethernet.



MAC Spoofing

MAC flooding é uma técnica utilizada para comprometer a segurança de switches de rede que conectam segmentos de rede ou dispositivos de rede. Os switches mapeam os endereços MAC individuais da rede nas portas físicas do switch através da tabela CAM. Ao contrário de um hub, que transmite os dados através da rede, o switch envia os dados apenas para o destinatário pretendido.

Assim, uma rede de comutação é mais segura quando comparada com uma rede com hub. Mas, ele ainda pode ser comprometido pelo fato de que switches possuem memória limitada para armazenar tabelas de endereços MAC e se transformam em hubs quando são inundados com endereços MAC.

```
┌──(root㉿kali)-[~]
└─# macchanger eth0:2 -r
Current MAC:   3e:66:3a:c1:4d:76 (unknown)
Permanent MAC: 08:00:27:1f:71:5b (CADMUS COMPUTER SYSTEMS)
New MAC:       f6:4c:d2:e2:bc:c0 (unknown)

┌──(root㉿kali)-[~]
└─# macchanger eth0:2 -m 00:11:22:33:44:55
Current MAC:   f6:4c:d2:e2:bc:c0 (unknown)
Permanent MAC: 08:00:27:1f:71:5b (CADMUS COMPUTER SYSTEMS)
New MAC:       00:11:22:33:44:55 (CIMSYS Inc)
```

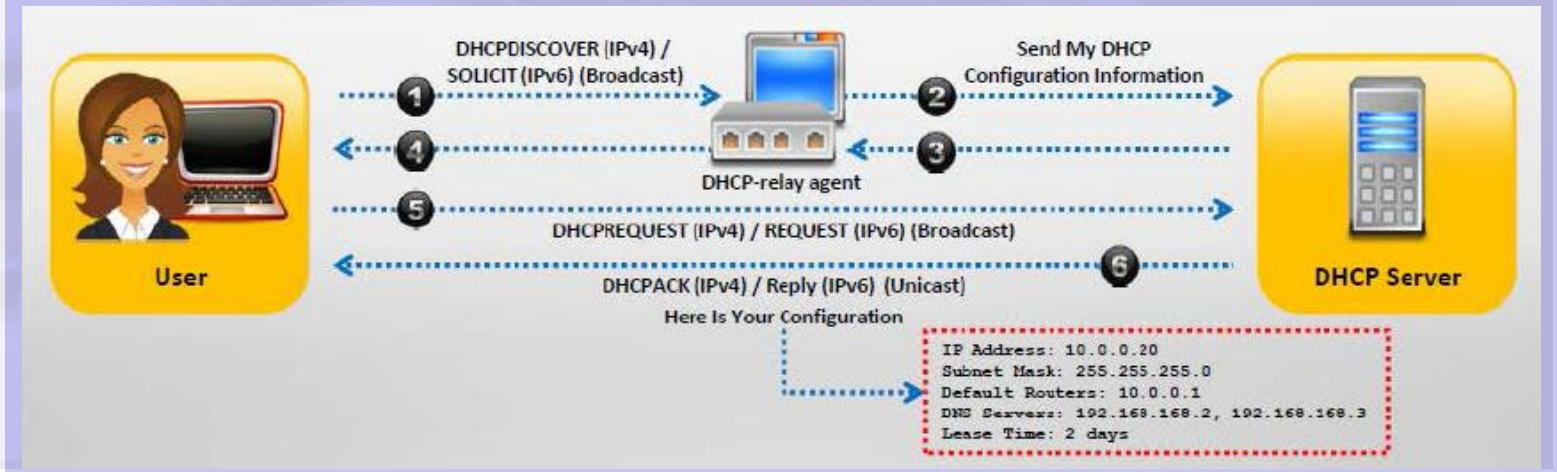
```
┌──(root㉿kali)-[~]
└─# macchanger --help
GNU MAC Changer
Usage: macchanger [options] device

  -h,  --help                  Print this help
  -V,  --version               Print version and exit
  -s,  --show                  Print the MAC address and exit
  -e,  --ending                Don't change the vendor bytes
  -a,  --another               Set random vendor MAC of the same kind
  -A                           Set random vendor MAC of any kind
  -p,  --permanent             Reset to original, permanent hardware MAC
  -r,  --random                Set fully random MAC
  -l,  --list[=keyword]        Print known vendors
  -b,  --bia                   Pretend to be a burned-in-address
  -m,  --mac=XX:XX:XX:XX:XX:XX
       --mac XX:XX:XX:XX:XX:XX Set the MAC XX:XX:XX:XX:XX:XX
```

```
┌──(root㉿kali)-[~]
└─# macchanger -p eth0
Current MAC:   00:11:22:33:44:55 (CIMSYS Inc)
Permanent MAC: 08:00:27:1f:71:5b (CADMUS COMPUTER SYSTEMS)
New MAC:       08:00:27:1f:71:5b (CADMUS COMPUTER SYSTEMS)
```

Entendendo ataques MAC

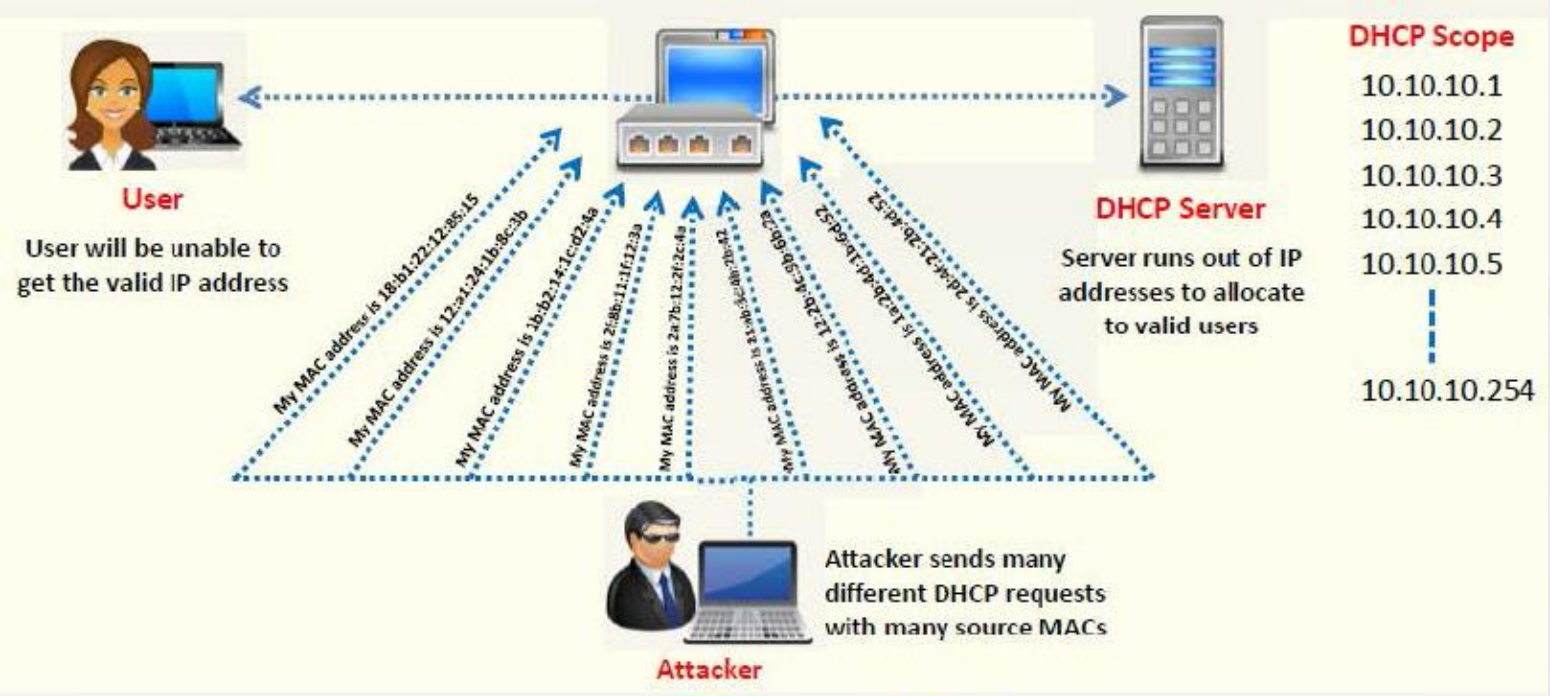
- Dynamic Host Configuration Protocol (DHCP) é um protocolo cliente/servidor que se destina a fornecer um endereço de IP a um host na rede. Além do endereço IP, o servidor DHCP também fornece informações relacionadas à configuração, como gateway padrão e uma máscara de sub-rede. Você pode usar o DHCP para atribuir a configuração de IP para hosts conectados a uma rede TCP/IP. Um cliente DHCP faz uma solicitação para o servidor na mesma sub-rede. A distribuição de configuração de IP para os hosts simplifica o trabalho do administrador para manter redes IP.

•**DHCPDISCOVER**: serve para encontrar quais servidores DHCP estão disponíveis.
•**DHCPOFFER**: uma resposta do servidor para os pacotes DHCPDISCOVER que têm os primeiros parâmetros da conexão.
•**DHCPREQUEST**: pedidos dos clientes para prolongar o tempo de aluguel do endereço IP.
•**DHCPACK**: uma resposta do servidor com os parâmetros e o IP do computador do cliente.
•**DHCPNAK**: uma resposta do servidor para informar o término do aluguel ou uma configuração inadequada da rede.
•**DHCPDECLINE**: uma mensagem do cliente para informar ao servidor que já houve uso do endereço IP.
•**DHCPRELEASE**: uma liberação do endereço IP pelo cliente.
•**DHCPINFORM**: um pedido pelo cliente com endereço IP dos parâmetros locais.
•**Relay DHCP**: Essa é uma funcionalidade que permite aos Switchs L3 e Roteadores encaminharem mensagens DHCP via broadcast para servidores fora do domínio do host. Isso viabiliza a utilização de um único DHCP em toda a rede LAN.



Ataque DHCP Starvation

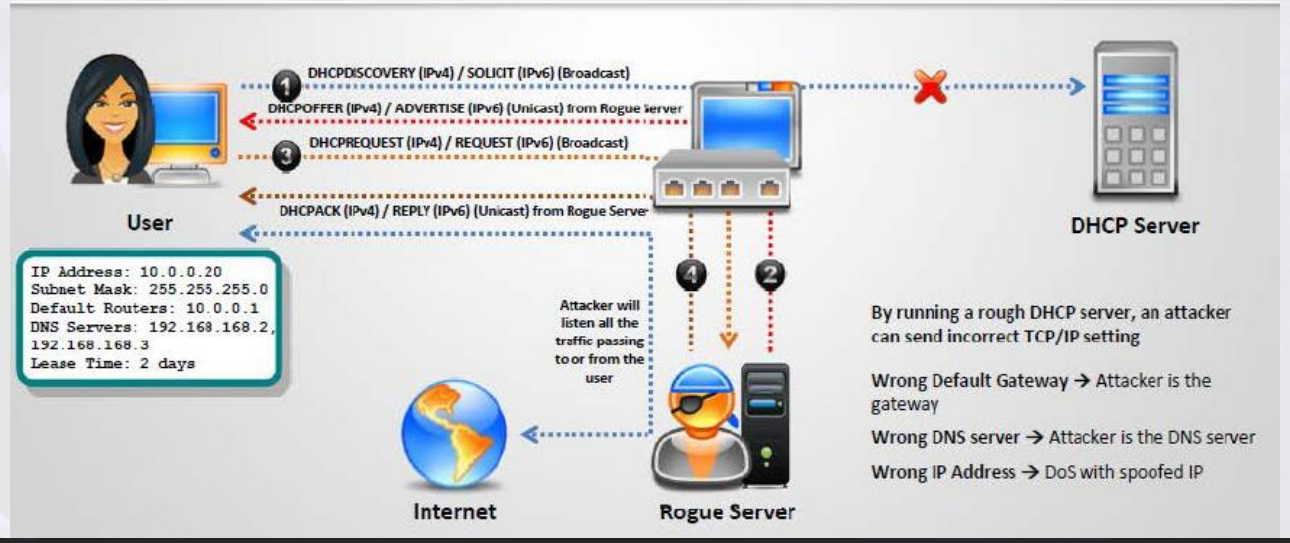
Em um ataque DHCP Starvation, o atacante inunda o servidor DHCP, enviando um grande número de solicitação de DHCP e usa todos os endereços IP disponíveis que o servidor DHCP pode emitir. Como resultado, o servidor não pode emitir mais nenhum endereço IP, levando a negação de serviço (DoS). Devido a este problema, os usuários válidos não podem obter ou renovar os respectivos endereços IP e, portanto, não conseguem acessar sua rede. Um atacante transmite pedidos DHCP com endereços MAC falsificado com a ajuda de ferramentas como o Gobbler.



Ataque Rogue DHCP Server

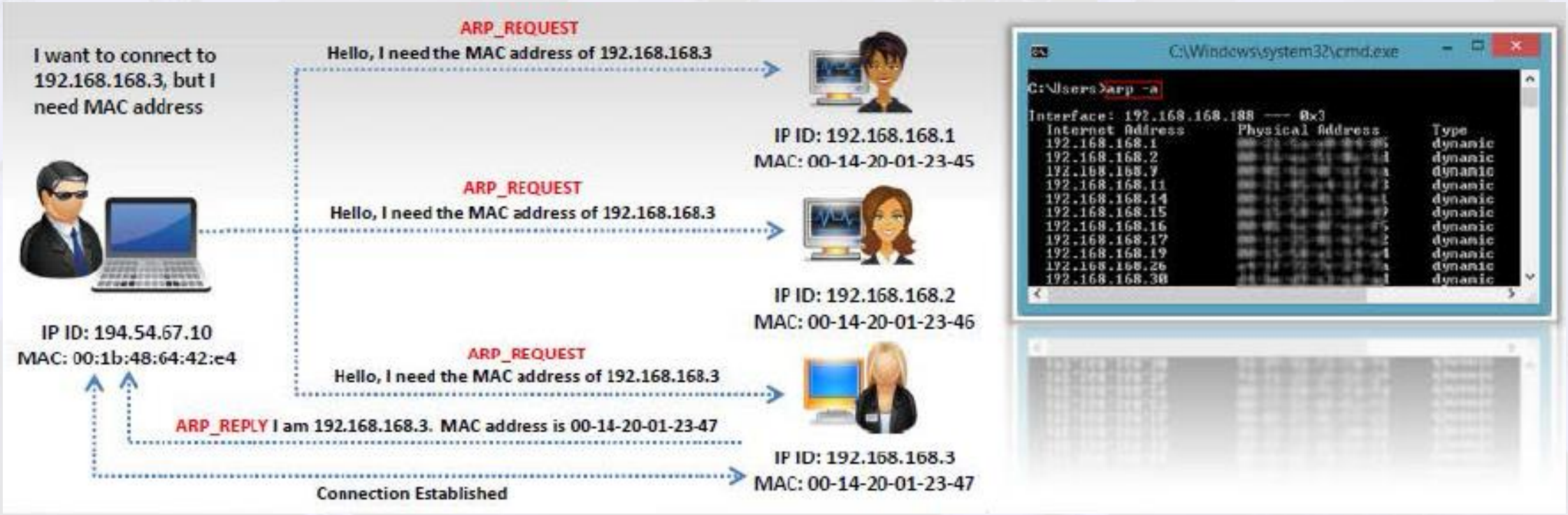
Em um ataque rogue DHCP, um atacante irá introduzir um servidor não autorizado na rede. Este servidor não autorizado tem a capacidade de responder às solicitações de descoberta DHCP dos clientes. Embora ambos os servidores respondem ao pedido, o servidor que responde primeiro será aceito pelo cliente. No caso em que o rogue DHCP dá a resposta antes do servidor DHCP real, as informações fornecidas aos clientes por este servidor impedem o seu acesso à rede, causando negação de serviço.

A resposta do rogue DHCP do atacante pode atribuir o endereço IP do atacante como gateway padrão do cliente. Como resultado, todo o tráfego do cliente será enviado para o endereço IP do atacante. O atacante, em seguida, captura todo o tráfego, do ponto de vista do cliente, ele pensa que tudo está funcionando corretamente.



Address Resolution Protocol

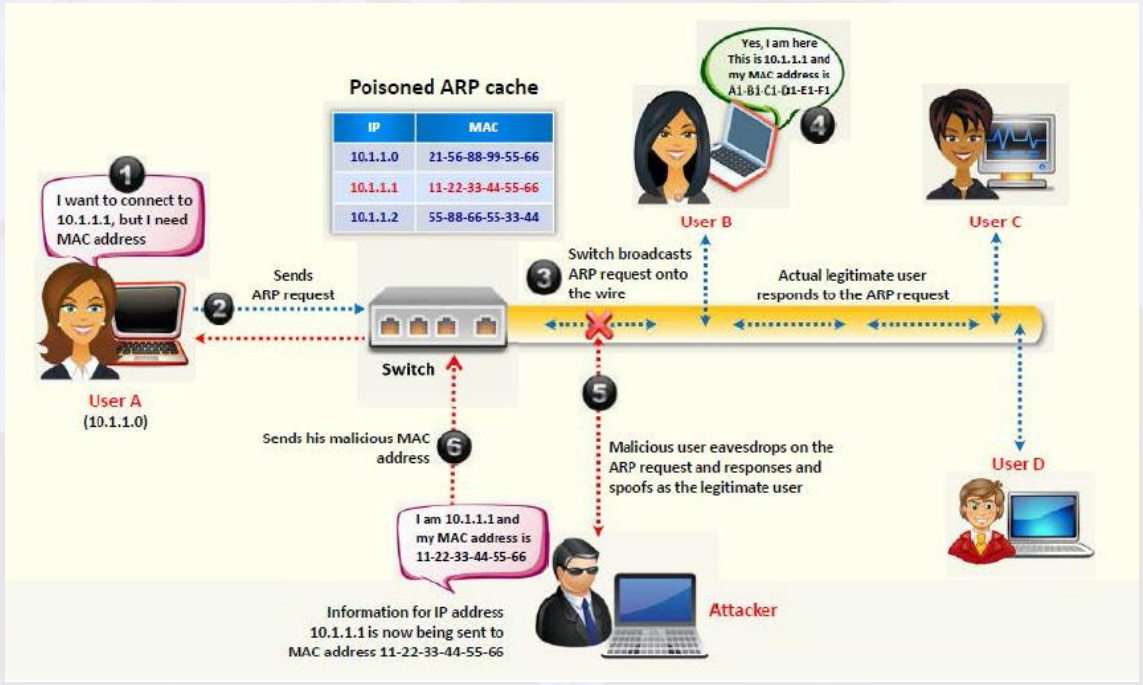
ARP (Address Resolution Protocol) é um protocolo TCP/IP que mapeia endereços IP em endereços de hardware (MAC) utilizado na camada de enlace de dados. Utilizando este protocolo, podemos facilmente obter o endereço MAC de qualquer dispositivo dentro de uma rede. Além do Switch, as máquinas também utilizam o protocolo ARP para obter endereços MAC.

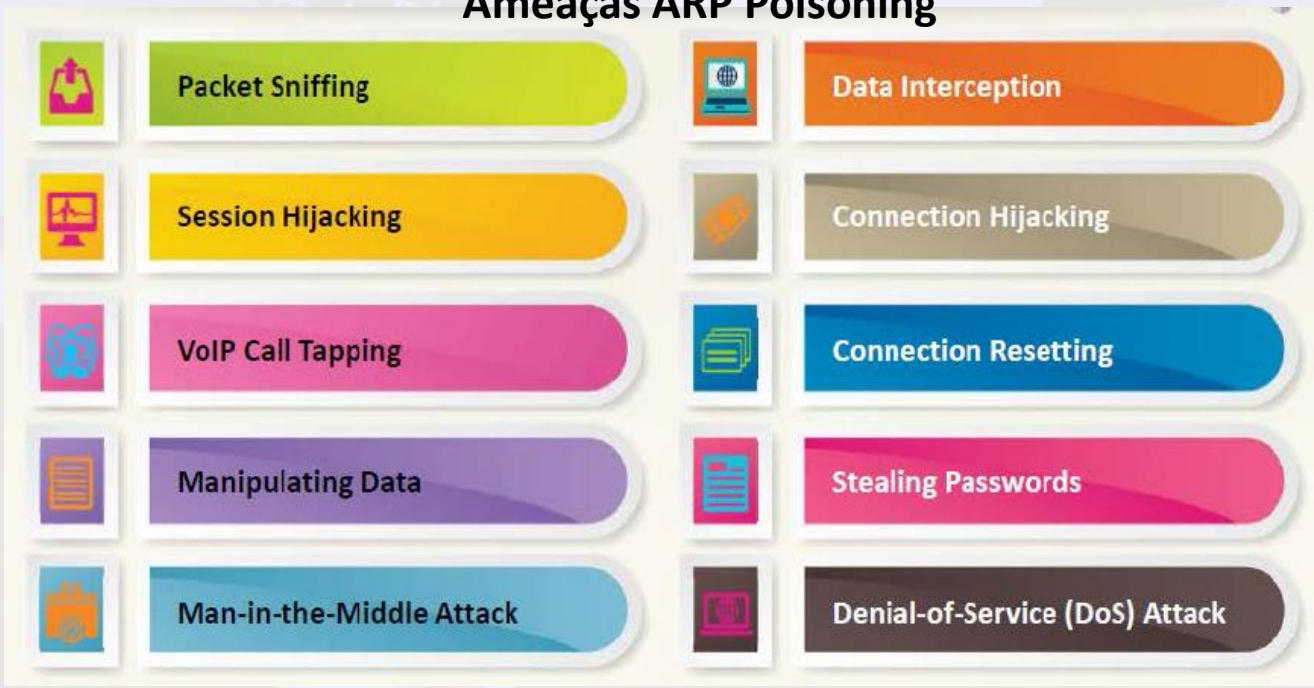


ARP Spoofing

Um computador host salva e atualiza o cache ARP local quando ele recebe um pacote "pedido de ARP" ou "ARP Reply". Qualquer host em uma LAN pode falsificar pacotes ARP livremente porque o protocolo ARP não requer autenticação. Os atacantes podem utilizar esta falha inerente como uma vantagem e pode comprometer o host ou rede.

O ARP resolve endereços IP para o endereço MAC da interface de rede para enviar os dados. Se a máquina envia um pedido ARP, ela normalmente considera que o ARP reply veio da máquina certa. Ameaças ARP Poisoning





Entendendo DNS Poisoning

DNS poising, também chamado de DNS Spoofing, é um ataque em que o atacante tenta redirecionar a vítima a um servidor malicioso em vez do servidor legítimo. O atacante pode cometer esse tipo de ataque manipulando as entradas da tabela de DNS no sistema DNS.

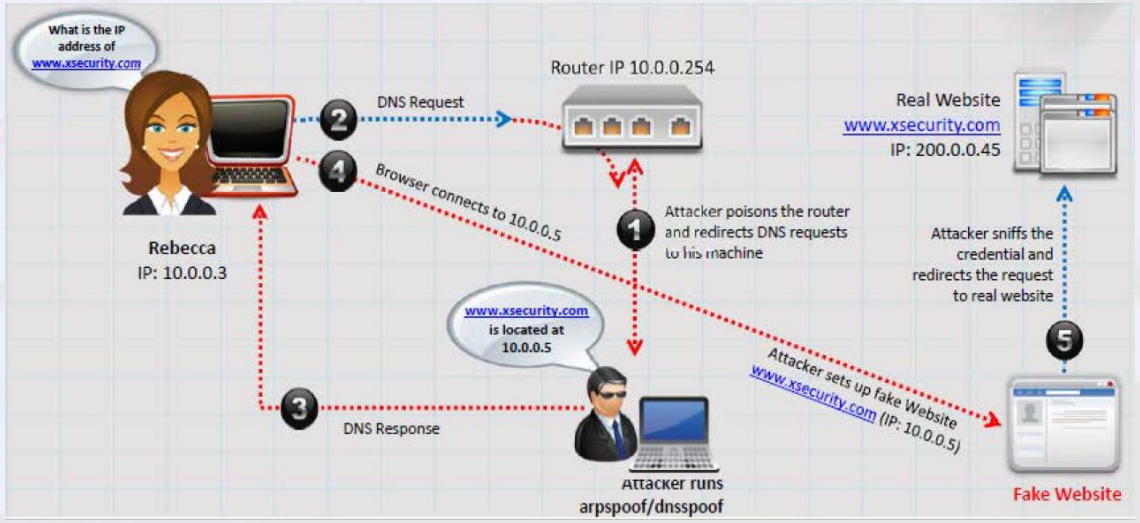
Suponha que a vítima quer acessar o site ABC.com, o atacante manipula as entradas na tabela de DNS de tal forma que a vítima está sendo redirecionada para o servidor do atacante. Isso pode ser feito alterando o endereço IP de ABC.com para o endereço IP do servidor malicioso do invasor.

Existem quatro tipos de ataques de envenenamento de DNS que você pode usar para comprometer o sistema de destino:

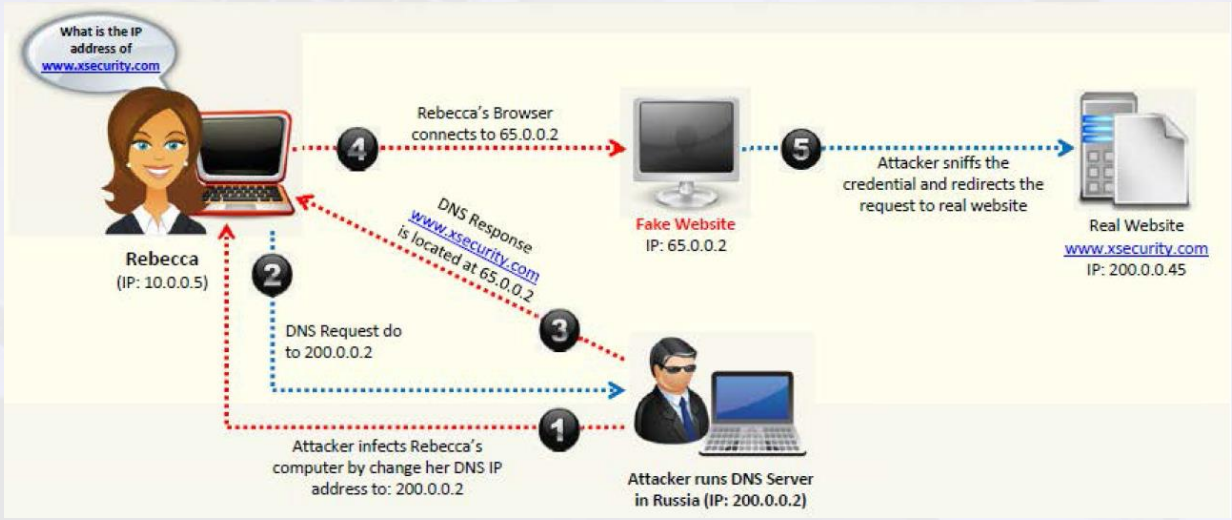
- Intranet DNS spoofing (local network)
- Internet DNS spoofing (remote network)
- Proxy server DNS poisoning
- DNS cache poisoning

Entendendo DNS Poisoning

Intranet DNS spoofing (local network)

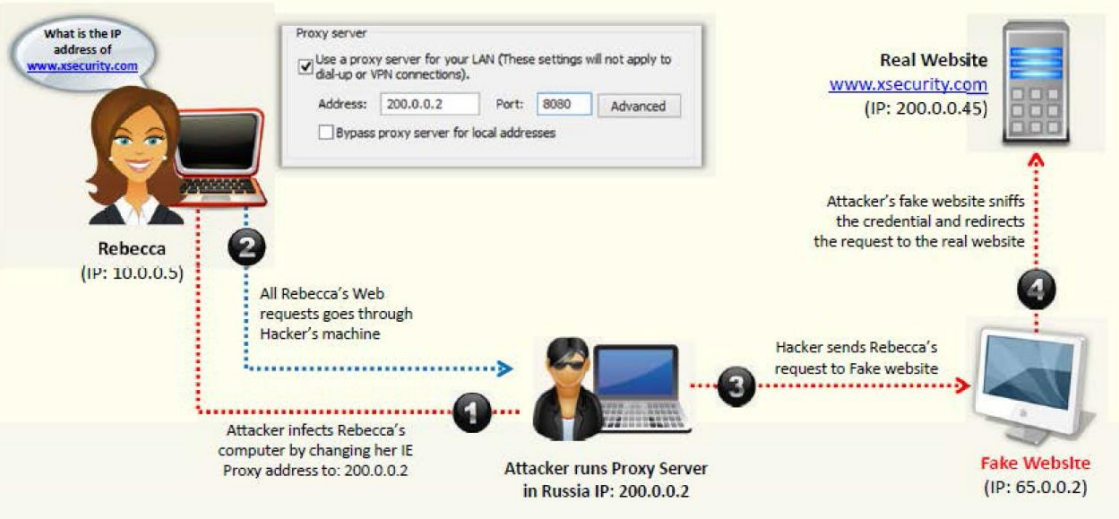


Internet DNS spoofing (remote network)

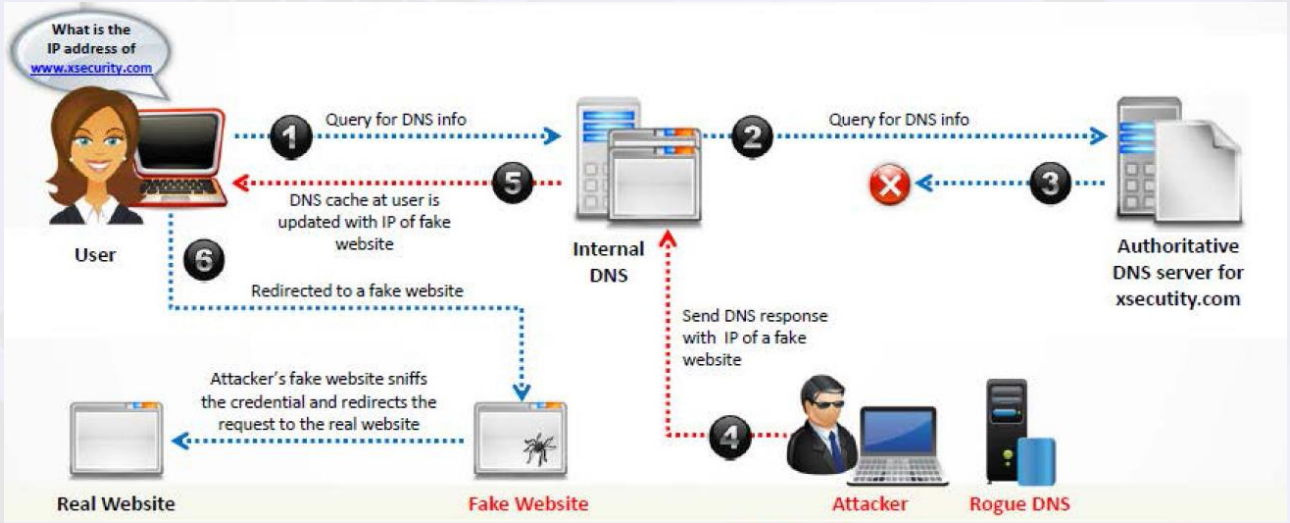


Entendendo DNS Poisoning

Proxy Server DNS poisoning



DNS Cache poisoning



Conceitos sobre Sniffing:

Packet sniffing é um processo de monitoramento e captura de todos os pacotes de dados que passam através de uma determinada rede utilizando softwares ou dispositivos de hardware. Isto é possível porque o tráfego em um segmento passa por todos os hosts associados com aquele segmento.

Programas de sniffing desligam o filtro empregado nas placas Ethernet para evitar que a máquina veja o tráfego de outras estações. Assim, os programas sniffing podem ver o tráfego de todos.

CEHv12

08.Sniffing

TRAINNING
EDUCATION SERVICES

Teoria na Prática

Wireshark

Acessar sua máquina virtual Kali

Abrir o terminal como root

Digitar o comando “wireshark &”

Filtros bônus:

ip.addr == 10.10.10.10

ip.src == 10.10.10.10

ip.dst == 10.10.10.10

tcp.port == 20

tcp.dstport == 80

tcp.srcport == 60234

udp.port == 513

icmp.type == 8

tcp.flags.syn

http.request.uri contains "login.php"

http.request.method == "POST"

Teoria na Prática

TCPDump

Acessar sua máquina virtual Kali

Abrir o terminal como root

Digitar os comandos abaixo:

tcpdump -i eth0

tcpdump -i eth0 src host ip.alvo

tcpdump -i eth0 dst host ip.alvo

tcpdump -i eth0 not host ip

tcpdump -i eth0 dst port 80

tcpdump -i eth0 src port 32881

Obrigado!

“QUEM NÃO SABE O QUE PROCURA, NÃO PERCEBE QUANDO ENCONTRA”.