

Módulo 17:Atacando o que Fazemos



CyberOps Associate v1.0

Prof. Clemilson Oliveira

clemilson.oliveira@edu.sc.senai.br



Objetivos do módulo

Título do módulo: Atacando o que Fazemos

Objetivo do módulo: explicar como aplicativos e serviços de rede comuns são vulneráveis a ataques.

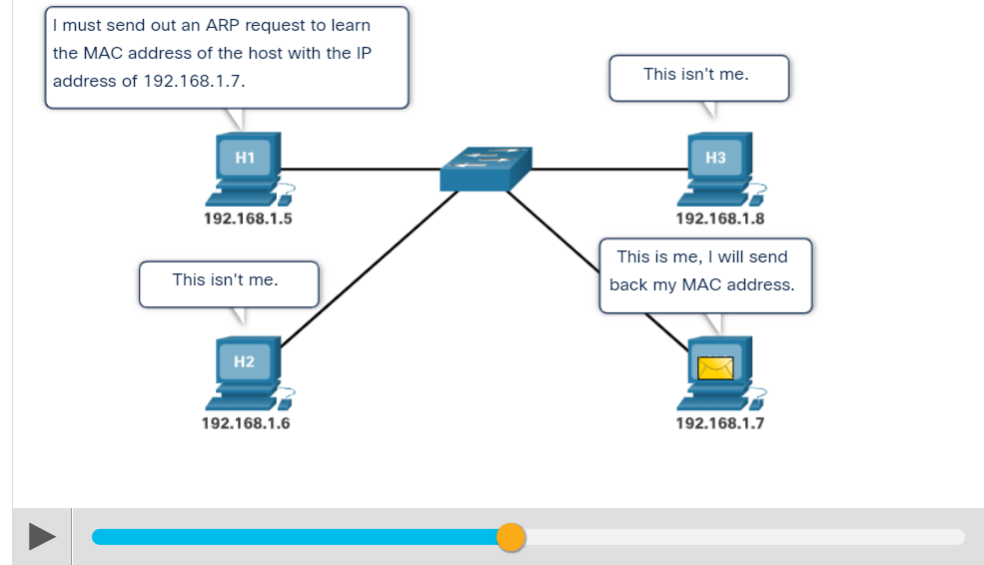
Título do Tópico	Objetivo do Tópico
Serviços IP	Explicar vulnerabilidades de serviço IP
Serviços Corporativos	Explique como as vulnerabilidades de aplicativos de rede permitem ataques de rede

17.1 Serviços IP

Vulnerabilidades ARP

- Os hosts transmitem uma solicitação ARP para outros hosts no segmento de rede para determinar o endereço MAC de um host com um endereço IP específico.
- O host com o endereço IP correspondente na solicitação ARP envia uma resposta ARP chamada “ARP gratuito”.
- Um ator de ameaça pode envenenar o cache ARP de dispositivos na rede local
- O objetivo é associar o endereço MAC do ator de ameaça ao endereço IP do gateway padrão nos caches ARP dos hosts no segmento LAN.

Reproduza a animação para ver o processo ARP funcionando.

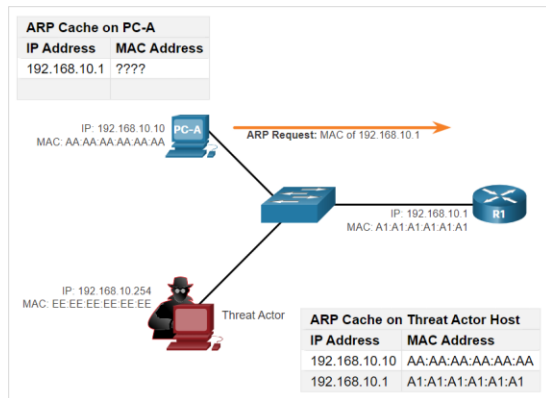


Envenenamento de cache ARP

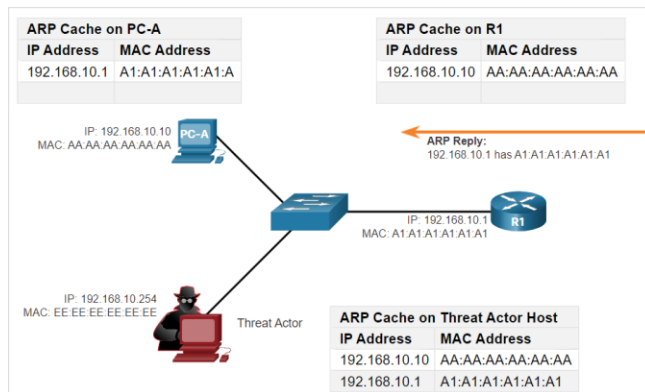
- O envenenamento do cache ARP pode ser usado para iniciar vários ataques do tipo man-in-the-middle.

Processo de envenenamento de cache ARP

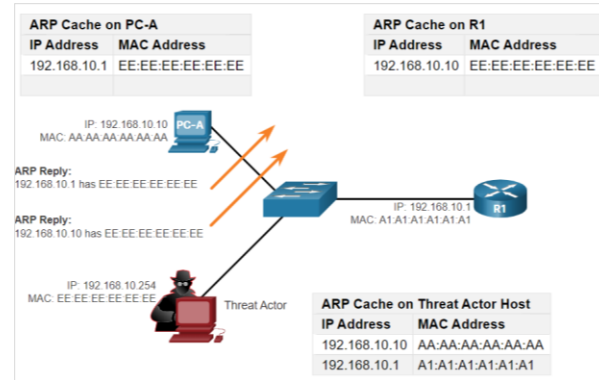
Requisição ARP



Resposta ARP



Respostas falsas gratuitas de ARP



Nota: Existem muitas ferramentas disponíveis na Internet para criar ataques ARP MITM, incluindo dsniff, Cain & Abel, ettercap, Yersinia e outros.

Ataques de DNS

Os ataques de DNS incluem os seguintes:

Ataques de resolução aberta de DNS:

- Um resolvidor de DNS aberto é um servidor DNS aberto publicamente, como o DNS do Google (8.8.8.8) que responde às consultas do cliente fora do seu domínio administrativo. Os resolvers abertos de DNS são vulneráveis a várias atividades maliciosas descritas na tabela.

Vulnerabilidades de resolvidor de DNS	Descrição
Ataques de envenenamento de cache DNS	Os agentes da ameaça enviam informações falsificadas de Recurso de Registro (RR) para um resolvidor de DNS para redirecionar os usuários de sites legítimos para sites maliciosos.
Ataques de amplificação e reflexão de DNS	Os agentes de ameaças enviam mensagens DNS para os resolvers abertos usando o endereço IP de um host de destino.
Ataques de utilização de recursos DNS	Esse ataque do DoS consome todos os recursos disponíveis para afetar negativamente as operações do resolvidor aberto do DNS.

Ataques DNS (Cont.)

Ataques furtivos de DNS

- Para ocultar sua identidade, os agentes de ameaças também usam as técnicas furtivas de DNS descritas na tabela para realizar seus ataques.

técnicas furtivas de DNS	Descrição
Fluxo Rápido	Os agentes de ameaças usam essa técnica para ocultar seus sites de entrega de phishing e malware. Os endereços IP do DNS são alterados continuamente em minutos.
Fluxo de IP duplo	Os atores de ameaças usam essa técnica para alterar rapidamente o nome do host para os mapeamentos de endereço IP e também para alterar o servidor de nomes autoritativo. Isso aumenta a dificuldade de identificar a fonte do ataque.
Algoritmos de geração de domínio	Os atores de ameaças usam essa técnica em malware para gerar aleatoriamente nomes de domínio que podem ser usados como pontos de encontro para seus servidores de comando e controle (C&C).

Ataques DNS (Cont.)

Ataques de sombreamento de domínio DNS

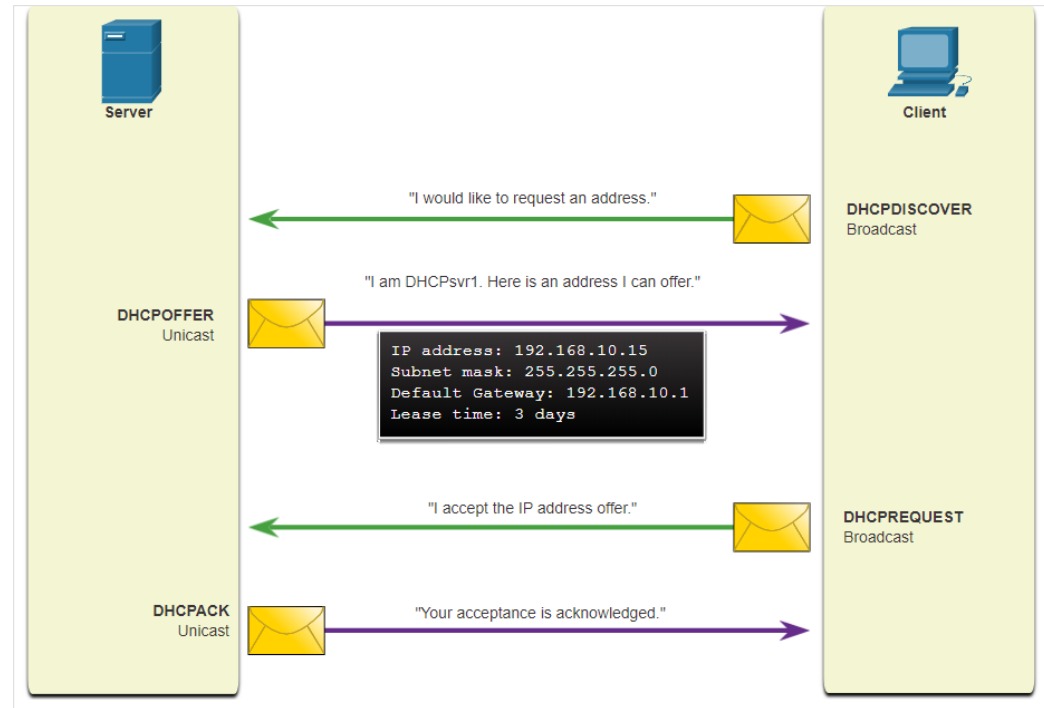
- No Domain Shadowing, o ator da ameaça reúne as credenciais da conta do domínio para criar vários subdomínios que serão usados durante os ataques.
- Esses subdomínios normalmente apontam para servidores mal-intencionados sem alertar o proprietário real do domínio pai.

Tunelamento DNS

- É necessário que o analista de segurança cibernética seja capaz de detectar quando um invasor está usando tunelamento DNS para roubar dados e prevenir e conter o ataque.
- Para isso, o analista de segurança deve implementar uma solução que possa bloquear as comunicações de saída dos hosts infectados.
- Os agentes de ameaças que usam o tunelamento DNS colocam tráfego que não é de DNS, dentro do tráfego DNS. Esse método geralmente contorna soluções de segurança.
- Para que o agente da ameaça use o túnel DNS, os diferentes tipos de registros DNS, como TXT, MX, SRV, NULL, A ou CNAME, são alterados. Por exemplo, um registro TXT pode armazenar os comandos enviados para os bots de host infectados como respostas DNS.
- Para interromper o túnel DNS, um filtro que inspecione o tráfego DNS deve ser usado.

DHCP

- Os servidores DHCP fornecem dinamicamente informações de configuração de IP aos clientes.
- Na figura, um cliente transmite uma mensagem de descoberta DHCP.
- O servidor DHCP responde com uma oferta direta (unicast) que inclui informações de endereçamento que o cliente pode usar.
- O cliente transmite em difusão (broadcast) uma solicitação DHCP para informar ao servidor que aceita a oferta.
- O servidor responde com uma confirmação de direta (unicast) aceitando a solicitação.



Operação normal do DHCP

Ataques à DHCP

Ataque de falsificação de DHCP

- Um ataque de spoofing de DHCP ocorre quando um servidor DHCP invasor está conectado à rede e fornece falsos parâmetros de configuração IP aos clientes legítimos.

Um servidor não autorizado pode fornecer uma variedade de informações enganosas, como:

- **Gateway padrão errado** - o ator da ameaça fornece um gateway inválido ou o endereço IP de seu host para criar um ataque MiTM.
- **Servidor DNS errado** - O agente de ameaças fornece um endereço de servidor DNS incorreto, apontando o usuário para um site malicioso.
- **Endereço IP errado** - O agente de ameaças fornece um endereço IP inválido, um endereço IP de gateway padrão inválido ou ambos. O agente de ameaça cria um ataque de negação de serviço no cliente DHCP.

Explorando o tráfego DNS

Neste laboratório, você completará os seguintes objetivos:

- Capture o tráfego DNS
- Explore o tráfego de consulta DNS
- Explore o tráfego de resposta do DNS

17.2 Serviços corporativos

Serviços Corporativos

HTTP e HTTPS

- Para investigar ataques baseados na Web, os analistas de segurança devem ter uma boa compreensão de como funciona um ataque padrão baseado na Web.

Estágios comuns de um ataque típico da Web:

- A vítima visita inconscientemente uma página web que foi comprometida por malware.
- A página Web comprometida redireciona o usuário para um site contendo código mal-intencionado.
- O usuário visita este site com código malicioso e seu computador fica infectado.
- Depois de identificar um pacote de software vulnerável em execução no computador da vítima, o kit de exploração entra em contato com o servidor do kit de exploração para baixar o código malicioso.
- Depois que o computador da vítima foi comprometido, ele se conecta ao servidor de malware e baixa uma carga útil.
- O último pacote de malware é executado no computador da vítima.

HTTP e HTTPS (continuação)

- Os logs de conexão do servidor geralmente podem revelar informações sobre o tipo de varredura ou ataque.
- Os diferentes tipos de códigos de status de conexão são:
 - **Informativo 1xx**
 - **Bem sucedido 2xx**
 - **Redirecionamento 3xx**
 - **Erro do cliente 4xx**
- Para se defender contra ataques baseados na Web:
 - Sempre atualize o sistema operacional e os navegadores com patches e atualizações atuais.
 - Use um proxy da Web para bloquear sites mal-intencionados.
 - Use as melhores práticas de segurança do Open Web Application Security Project (OWASP) ao desenvolver aplicativos Web.
 - Educar os usuários finais mostrando-lhes como evitar ataques baseados na Web.

Explorações HTTP comuns

IFrames maliciosos

- Um iFrame é um elemento HTML que permite que o navegador carregue outra página da Web de outra fonte.
- Em ataques iFrame, os atores da ameaça inserem anúncios de outras fontes na página.
- Os atores de ameaças comprometem um servidor da Web e modificam páginas da Web adicionando HTML para o iFrame malicioso.
- Como o iFrame está sendo executado na página, ele pode ser usado para fornecer uma exploração maliciosa, como publicidade de spam, kits de exploração e outros malwares.

Etapas para impedir ou reduzir iFrames maliciosos:

- Use um proxy da Web para bloquear sites mal-intencionados.
- Certifique-se de que os desenvolvedores da Web não usem iFrames.
- Use um serviço como o Cisco Umbrella para impedir que os usuários naveguem para sites mal-intencionados.
- Certifique-se de que o usuário final entenda o que é um Iframe.

Explorações HTTP comuns (Cont.)

Amortecimento HTTP 302

- Os atores de ameaças usam o código de status de resposta 302 Found HTTP para direcionar o navegador da Web do usuário para um novo local.
- O navegador acredita que o novo local é o URL fornecido no cabeçalho. O navegador é convidado a solicitar este novo URL. Esta função de redirecionamento pode ser usada várias vezes até que o navegador finalmente chegue na página que contém o exploit.

Etapas para evitar ou reduzir ataques de amortecimento HTTP 302:

- Use um proxy da Web para bloquear sites mal-intencionados.
- Use um serviço como o Cisco Umbrella para impedir que os usuários naveguem para sites mal-intencionados.
- Certifique-se de que o usuário final entenda como o navegador é redirecionado por meio de uma série de redirecionamentos HTTP 302.

Explorações HTTP comuns (Cont.)

Sombreamento de domínio

- Quando um ator de ameaça cria um ataque de sombreamento de domínio, primeiro compromete um domínio. Em seguida, eles devem criar vários subdomínios desse domínio para serem usados para os ataques usando logins de registro de domínio seqüestrado.
- Depois que esses subdomínios tiverem sido criados, os invasores podem usá-los mesmo se descobrirem que eles são domínios mal-intencionados. Eles podem simplesmente fazer mais do domínio pai.

Etapas para evitar ou reduzir ataques de sombreamento de domínio:

- Proteja todas as contas de proprietário do domínio.
- Use um proxy da Web para bloquear sites mal-intencionados.
- Use um serviço como o Cisco Umbrella para impedir que os usuários naveguem para sites conhecidos por serem mal-intencionados.
- Certifique-se de que os proprietários de domínio validem as suas contas de registro e procure quaisquer subdomínios que não tenham autorizado.

E-mail

- À medida que o nível de uso do e-mail aumenta, a segurança se torna uma prioridade maior.
- A forma como os usuários acessam o email hoje também aumenta a oportunidade de a ameaça de malware ser introduzida.

Exemplos de ameaças de e-mail:

- **Ataques baseados em anexos** - atores de ameaças incorporam conteúdo malicioso em arquivos de negócios, como um e-mail do departamento de TI.
- **Falsificação de e-mails** - Os atores de ameaças criam mensagens de e-mail com um endereço de remetente falsificado que visa enganar o destinatário a fornecer dinheiro ou informações confidenciais.
- **E-mail spam** - Os agentes de ameaças enviam e-mails não solicitados contendo anúncios ou ficheiros maliciosos.
- **Servidor de retransmissão de correio aberto** - Este é um servidor SMTP que permite que qualquer pessoa na internet envie e-mails.

Bancos de dados expostos pela Web

- Aplicativos Web geralmente se conectam a um banco de dados relacional para acessar dados.
- Como os bancos de dados relacionais geralmente contêm dados confidenciais, os bancos de dados são um alvo freqüente para ataques.

Injeção de código

- Os comandos do intruso são executados através da aplicação Web e tem as mesmas permissões que a aplicação Web.
- Este tipo de ataque é usado porque muitas vezes há validação insuficiente de entrada.

Injeção de SQL

- Os agentes de ameaças usam injeções SQL para violar o banco de dados relacional, criar consultas SQL mal-intencionadas e obter dados confidenciais do banco de dados relacional.
- Uma exploração de injeção SQL bem-sucedida pode ler dados confidenciais do banco de dados, modificar dados do banco de dados, executar operações de administração no banco de dados e, às vezes, emitir comandos para o sistema operacional.

Scripts do lado do cliente

Scripting através de sites

- Cross-Site Scripting (XSS) é onde as páginas da Web executadas no lado do cliente, dentro de seu próprio navegador da Web, são injetadas com scripts mal-intencionados.
- Esses scripts podem ser usados pelo Visual Basic, JavaScript e outros para acessar um computador, coletar informações confidenciais ou implantar mais ataques e espalhar malware.
- Os dois tipos principais de XSS são **armazenados (persistentes)** e **refletidos (não persistentes)**.
- **Formas de prevenir ou reduzir ataques XSS:**
 - Certifique-se de que os desenvolvedores de aplicativos da Web estejam cientes das vulnerabilidades XSS e de como evitá-las.
 - Use uma implementação IPS para detectar e evitar scripts mal-intencionados.
 - Use um proxy da Web para bloquear sites mal-intencionados.
 - Use um serviço como o Cisco Umbrella para impedir que os usuários naveguem para sites mal-intencionados.

Atacando um banco de dados MySQL

Neste laboratório, você concluirá o seguinte objetivo:

- Exibir um arquivo PCAP de um ataque anterior contra um banco de dados SQL.

Leitura de logs do servidor

Neste laboratório, você completará os seguintes objetivos:

- Lendo Arquivos de Log com **cat**, **more** e **less**
- Arquivos de log e Syslog
- Arquivos de log e **journalctl**

17.3 Resumo do ataque ao nosso trabalho

O Que Aprendi neste Módulo?

- Qualquer cliente pode enviar uma resposta ARP não solicitada denominada "ARP gratuito".
- Um ator de ameaça pode envenenar o cache ARP de dispositivos na rede local, criando um ataque MiTM para redirecionar o tráfego.
- O protocolo DNS (Domain Name Service) utiliza registros de recursos (RR) para identificar o tipo de resposta DNS.
- Os resolvedores abertos DNS são vulneráveis a várias atividades mal-intencionadas, incluindo envenenamento de cache DNS, em que registros falsificados são fornecidos ao resolvedor aberto.
- Em ataques de amplificação e reflexão DNS, a natureza benigna do protocolo DNS é explorada para causar ataques DOS/DDoS.
- Em ataques de utilização de recursos DNS, um ataque DoS é iniciado contra o próprio servidor DNS.
- Os atores de ameaças usam o Fast Flux, no qual servidores mal-intencionados mudarão rapidamente seu endereço IP.
- Para interromper o túnel DNS, um filtro que inspecione o tráfego DNS deve ser usado.

O que aprendi neste módulo?

- Um ataque de spoofing de DHCP ocorre quando um servidor DHCP invasor está conectado à rede e fornece falsos parâmetros de configuração IP aos clientes legítimos.
- A página Web comprometida redireciona o usuário para um site que hospeda código mal-intencionado, conhecido como download de drive-by.
- Os ataques XSS (Cross-Site Scripting) ocorrem quando os navegadores executam scripts mal-intencionados no cliente e fornecem aos agentes da ameaça acesso a informações confidenciais no host local.
- O OWASP Top 10 Riscos de Segurança de Aplicativos Web foi projetado para ajudar as organizações a criar aplicativos Web seguros.

