



Módulo 24: Tecnologias e protocolos



CyberOps Associate v1.0

Prof. Clemilson Oliveira

clemilson.oliveira@edu.sc.senai.br

Objetivos do módulo

Título do Módulo: Tecnologias e protocolos

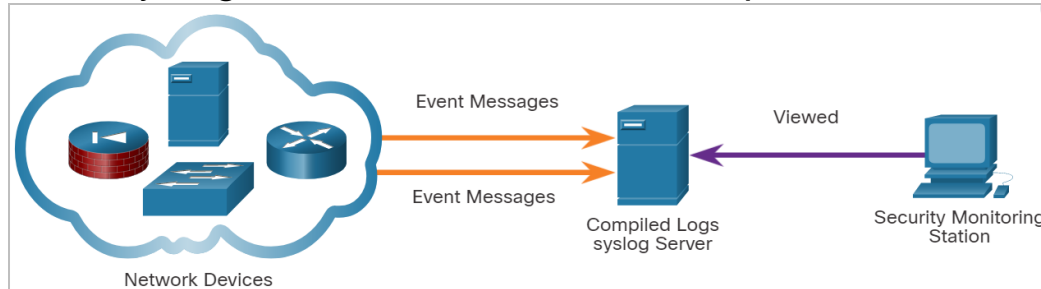
Objetivo do Módulo: Explique como as tecnologias de segurança afetam o monitoramento de segurança.

Tópico	Objetivo do Tópico
Monitorando protocolos comuns	Explicar o comportamento dos protocolos de rede comuns no contexto do monitoramento de segurança.
Tecnologias de segurança	Explicar como as tecnologias de segurança afetam a capacidade de monitorar protocolos de rede comuns.

24.1 Protocolos comuns de monitoramento

Syslog e NTP

- Syslog e Network Time Protocol (NTP) são essenciais para o trabalho do analista de segurança cibernética.
- O padrão syslog é usado para registrar mensagens de eventos de dispositivos de rede e endpoints.
- O padrão permite um meio neutro de sistema de transmissão, armazenamento e análise de mensagens.
- Muitos tipos de dispositivos de vários fornecedores diferentes podem usar syslog para enviar entradas de log para servidores centrais que executam um daemon syslog. Esta centralização da coleta de logs ajuda a tornar o monitoramento de segurança prático. Os servidores que executam syslog normalmente escutam na porta UDP 514.



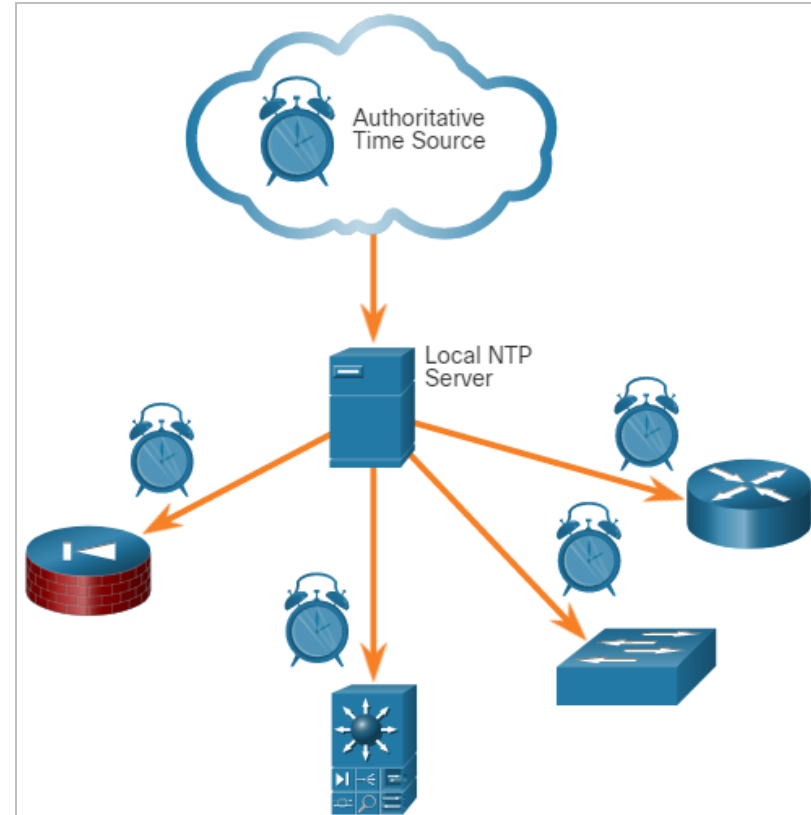
Syslog e NTP (Cont.)

- Como o syslog é tão importante para o monitoramento de segurança, os servidores syslog podem ser um alvo para atores de ameaças.
- Algumas explorações, como as que envolvem exfiltração de dados, podem levar muito tempo para serem concluídas devido às formas muito lentas em que os dados são secretamente roubados da rede.
- Alguns atacantes podem tentar ocultar o fato de que a exfiltração está ocorrendo. Eles atacam os servidores syslog que contêm as informações que podem levar à detecção da exploração.
- Os hackers podem tentar bloquear a transferência de dados de clientes syslog para servidores, adulterar ou destruir dados de log ou adulterar o software que cria e transmite mensagens de log.
- A implementação do syslog de próxima geração (ng), conhecida como syslog-ng, oferece aprimoramentos que podem ajudar a evitar algumas das explorações que visam o syslog.

Tecnologias e Protocolos

NTP

- As mensagens do Syslog geralmente são carimbadas de data e hora. Como as mensagens vêm de muitos dispositivos, é importante que os dispositivos compartilhem um timeclock consistente. Isso pode ser alcançado usando o Network Time Protocol (NTP).
- O NTP usa uma hierarquia de fontes de tempo autoritativas para compartilhar informações de tempo entre dispositivos na rede. O NTP opera na porta UDP 123.
- Os atores de ameaças podem tentar atacar a infraestrutura NTP para corromper as informações de tempo usadas para correlacionar eventos de rede registrados.
- Os atores de ameaças são conhecidos por usar sistemas NTP para direcionar ataques DDoS por meio de vulnerabilidades no software cliente ou servidor. Esses ataques podem interromper a disponibilidade da rede.



DNS

- O DNS agora é usado por muitos tipos de malware. Algumas variedades de malware usam DNS para se comunicar com servidores de comando e controle (CNC) e para exfiltrar dados no tráfego disfarçados como consultas DNS normais.
- O malware pode codificar dados roubados como a parte de subdomínio de uma pesquisa DNS para um domínio onde o servidor de nomes está sob controle de um invasor.
- Uma pesquisa de DNS para 'long string-of-exfiltrated-data.example.com' seria encaminhada para o servidor de nomes de example.com, que gravaria 'long string-of-exfiltrated-data' e responderia de volta ao malware com uma resposta codificada. Este uso do subdomínio DNS é mostrado na figura. Os dados exfiltrados são o texto codificado mostrado na caixa. O ator de ameaça coleta os dados codificados, decodifica e combina, e agora tem acesso a um arquivo de dados inteiro.



DNS (Cont.)

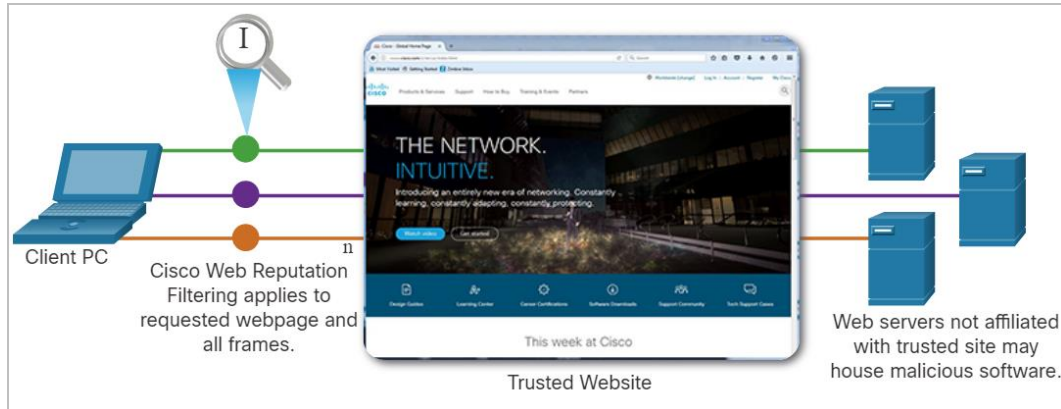
- É provável que a parte do subdomínio de tais solicitações seria muito mais longa do que as solicitações usuais. Analistas cibernéticos podem usar a distribuição dos comprimentos de subdomínios dentro de solicitações DNS para construir um modelo matemático que descreva a normalidade.
- Eles podem então usar isso para comparar suas observações e identificar um abuso do processo de consulta DNS. Por exemplo, não seria normal ver um host na rede enviando uma consulta para AW4GCGXHy2UGDG8GCHJVDGVJDC.Example.com.
- Consultas DNS para nomes de domínio gerados aleatoriamente, ou subdomínios com aparência aleatória extremamente longos, devem ser consideradas suspeitas, especialmente se a ocorrência deles aumentar drasticamente na rede.
- Os logs de proxy DNS podem ser analisados para detectar essas condições.
- Como alternativa, serviços como o serviço DNS passivo do Cisco Umbrella podem ser usados para bloquear solicitações para CNC suspeitos e domínios de exploração.

HTTP e HTTPS

- O Hypertext Transfer Protocol (HTTP) é o protocolo de backbone da World Wide Web.
- Todas as informações transportadas em HTTP são transmitidas em texto simples do computador de origem para o destino na internet.
- O HTTP não protege os dados contra alteração ou interceptação por partes mal-intencionadas, o que é uma séria ameaça à privacidade, identidade e segurança das informações.
- Todas as atividades de navegação devem ser consideradas em risco.

HTTP e HTTPS (Cond.)

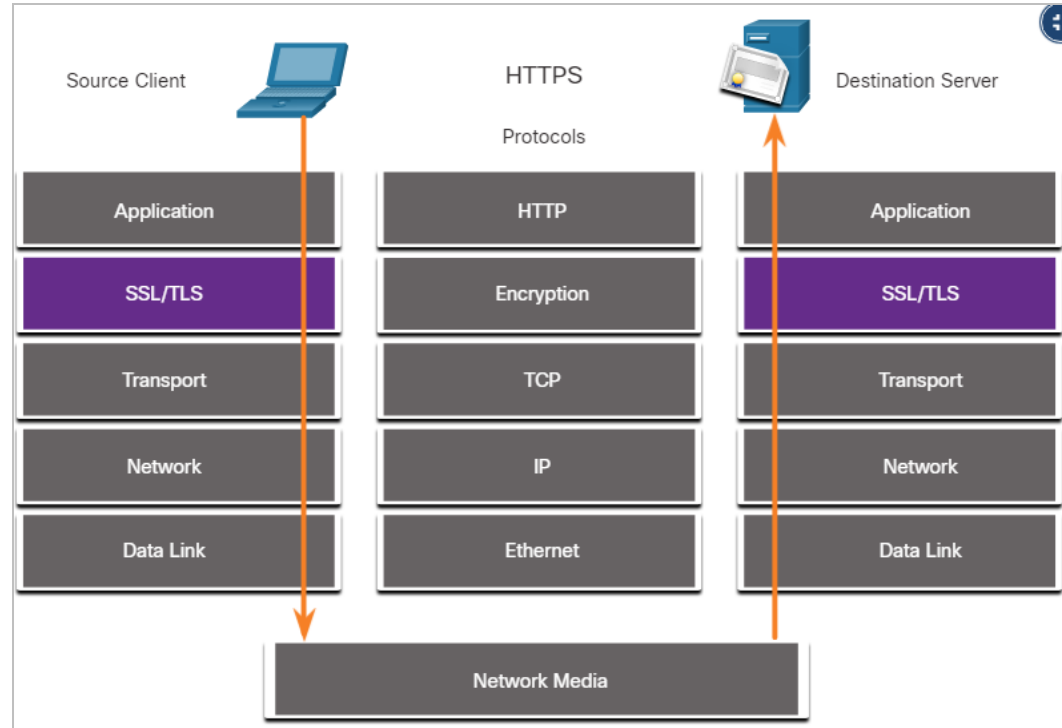
- Uma exploração comum de HTTP é chamada de injeção iFrame (quadro inline). Na injeção iFrame, um ator de ameaça compromete um servidor da Web e planta código malicioso que cria um iFrame invisível em uma página da Web comumente visitada.
- Quando o iFrame é carregado, o malware é baixado, freqüentemente de um URL diferente da página da Web que contém o código iFrame.
- Os serviços de segurança de rede, como a filtragem Cisco Web Reputation, podem detectar quando um site tenta enviar conteúdo de um site não confiável para o host, mesmo quando enviado de um iFrame.



HTTP e HTTPS (Cont.)

- Para resolver a alteração de dados confidenciais, muitas organizações adotaram HTTPS ou implementaram políticas somente HTTPS para proteger os visitantes de seus sites e serviços.
- HTTPS adiciona uma camada de criptografia ao protocolo HTTP usando Secure Socket Layer (SSL), como mostrado na figura.
- Isso torna os dados HTTP ilegíveis, pois deixam o computador de origem até chegar ao servidor.
- HTTPS não é um mecanismo para a segurança do servidor web. Ele só protege o tráfego de protocolo HTTP enquanto está em trânsito.

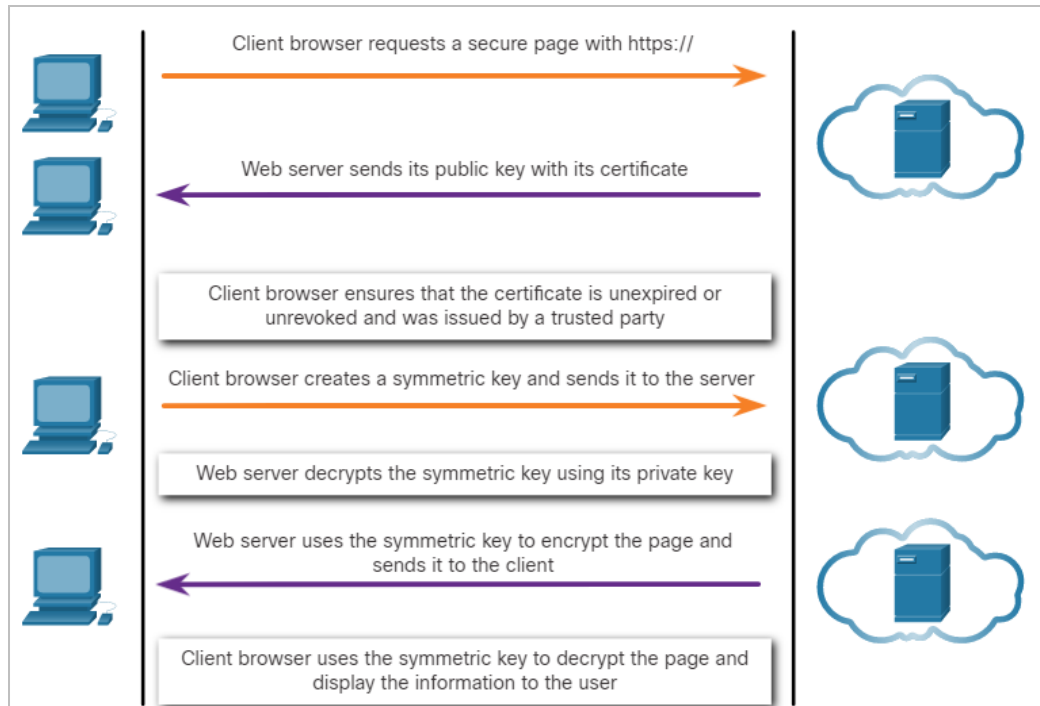
Diagrama de protocolo HTTPS



HTTP e HTTPS (Cont.)

- Infelizmente, o tráfego HTTPS criptografado complica o monitoramento de segurança de rede.
- Alguns dispositivos de segurança incluem descryptografia e inspeção SSL; no entanto, isso pode apresentar problemas de processamento e privacidade.
- HTTPS adiciona complexidade às capturas de pacotes devido às mensagens adicionais envolvidas no estabelecimento da conexão criptografada.
- Esse processo é resumido na figura e representa sobrecarga adicional sobre HTTP.

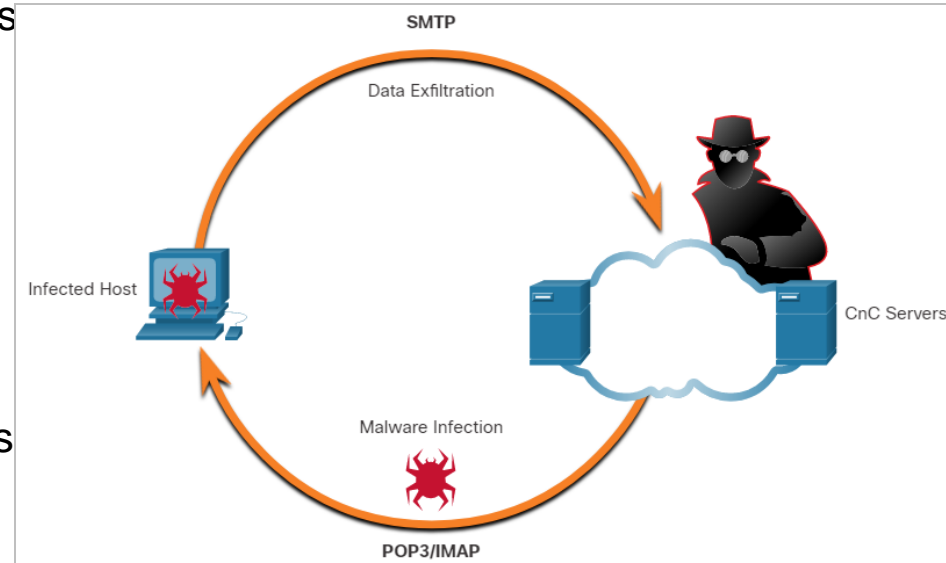
Transações HTTPS



Protocolos de Email

- Protocolos de e-mail como SMTP, POP3 e IMAP podem ser usados por atores de ameaças para espalhar malware, exfiltrar dados ou fornecer canais para servidores CNC de malware, como mostrado na figura.
- SMTP envia dados de um host para um servidor de email e entre servidores de email.
- IMAP e POP3 são usados para baixar mensagens de email de um servidor de email para o computador host. Eles são os protocolos de aplicativos que são responsáveis por trazer malware para o host.
- O monitoramento de segurança pode identificar quando um anexo de malware entrou na rede e qual host ele infectou pela primeira vez.

Ameaças de protocolo de email



ICMP

- O ICMP pode ser usado para identificar hosts em uma rede, a estrutura de uma rede e determinar os sistemas operacionais em uso na rede. Ele também pode ser usado como um veículo para vários tipos de ataques DoS.
- ICMP também pode ser usado para exfiltração de dados.
- Devido à preocupação de que o ICMP possa ser usado para vigiar ou negar o serviço de fora da rede, o tráfego ICMP de dentro da rede às vezes é ignorado.
- Algumas variedades de malware usam pacotes ICMP criados para transferir arquivos de hosts infectados para agentes ameaçadores usando esse método, conhecido como túnel ICMP.

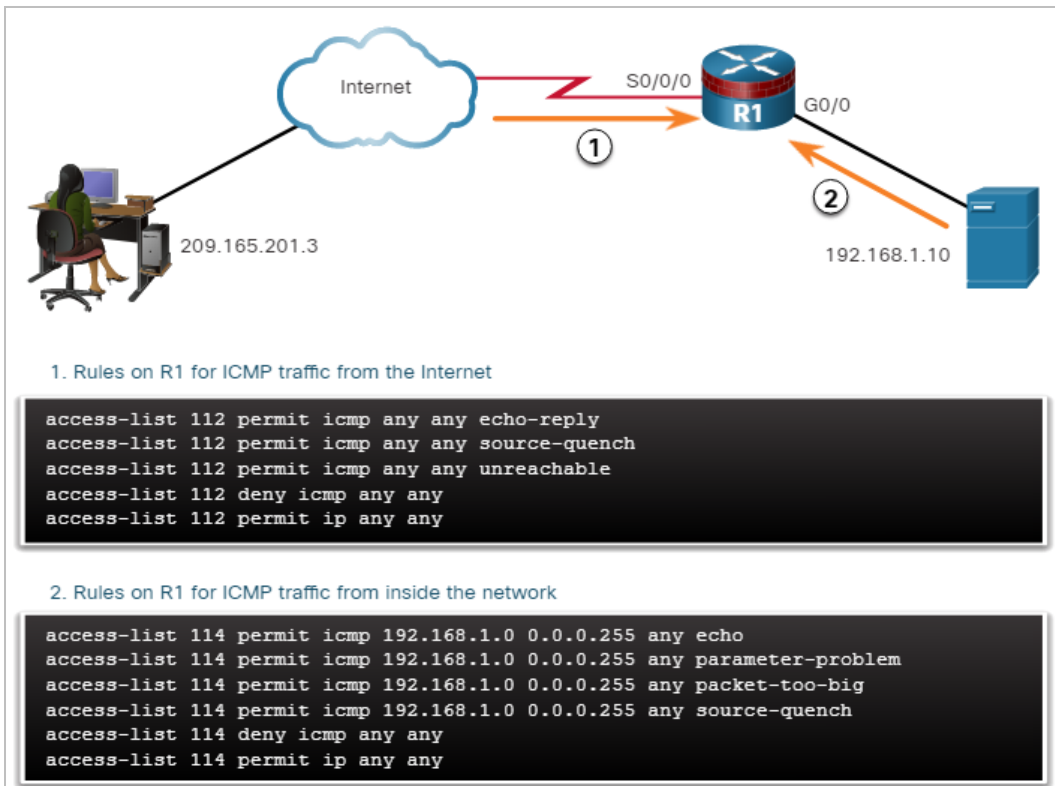
24.2 Tecnologias de segurança

Tecnologias de segurança

ACLs

- As Listas de Controle de Acesso (ACLs) e a filtragem de pacotes são tecnologias que contribuem para um conjunto em evolução de proteções de segurança de rede.
- A figura mostra o uso de ACLs para permitir apenas tipos específicos de tráfego ICMP (Internet Control Message Protocol). O servidor em 192.168.1.10 faz parte da rede interna e tem permissão para enviar solicitações de ping para o host externo em 209.165.201.3.
- O tráfego ICMP de retorno do host externo é permitido se for uma resposta ICMP ou qualquer mensagem ICMP inacessível. Todos os outros tipos de tráfego ICMP são negados.

Atenuante o abuso de ICMP



ACLs de tecnologias de segurança (Cont.)

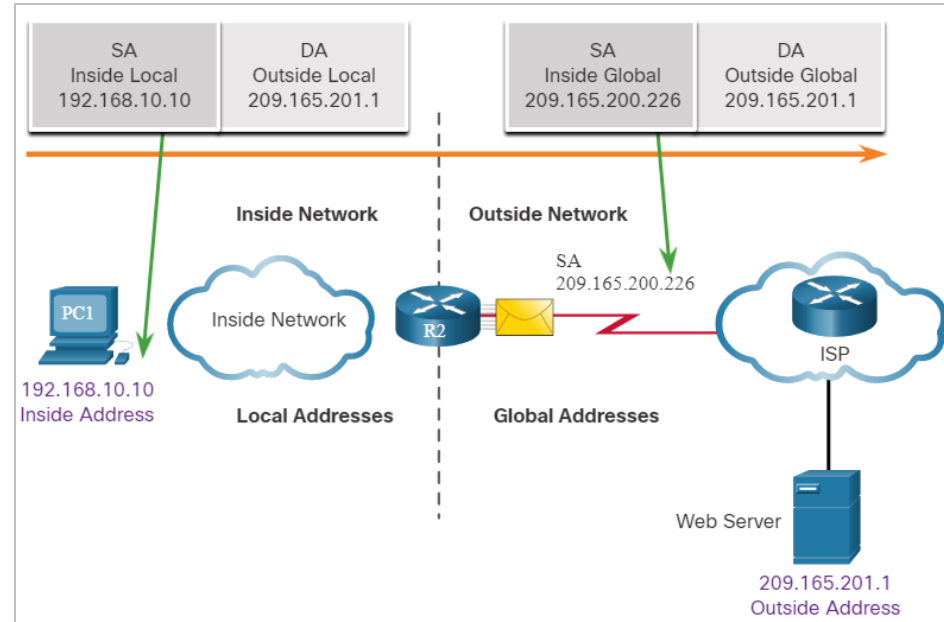
- Os invasores podem determinar quais endereços IP, protocolos e portas são permitidos pelas ACLs. Isso pode ser feito por varredura de portas ou testes de penetração, ou através de outras formas de reconhecimento.
- Os atacantes podem criar pacotes que usam endereços IP de origem falsificados.
- Os aplicativos podem estabelecer conexões em portas arbitrárias. Outros recursos do tráfego de protocolo também podem ser manipulados, como o sinalizador estabelecido em segmentos TCP. As regras não podem ser antecipadas e configuradas para todas as técnicas de manipulação de pacotes emergentes.
- Para detectar e reagir à manipulação de pacotes, comportamentos mais sofisticados e medidas baseadas em contexto precisam ser tomadas.
- Os firewalls de próxima geração da Cisco, o AMP (Advanced Malware Protection) e os appliances de conteúdo de e-mail e Web são capazes de resolver as deficiências das medidas de segurança baseadas em regras.

Tecnologias de Segurança

NAT e PAT

- Conversão de Endereços de Rede (NAT) e Tradução de Endereço de Porta (PAT) podem complicar o monitoramento de segurança.
- A figura mostra a relação entre endereços internos e externos que são usados como endereços de origem (SA) e endereços de destino (DA).
- Se o PAT estiver em vigor, pode ser difícil registrar o dispositivo interno específico que está solicitando e recebendo o tráfego quando ele entra na rede.
- Esse problema pode ser relevante com dados NetFlow. Os fluxos de NetFlow são unidirecionais e são definidos pelos endereços e portas que eles compartilham.

Network Address Translation



Criptografia, encapsulamento e encapsulamento de tecnologias de segurança

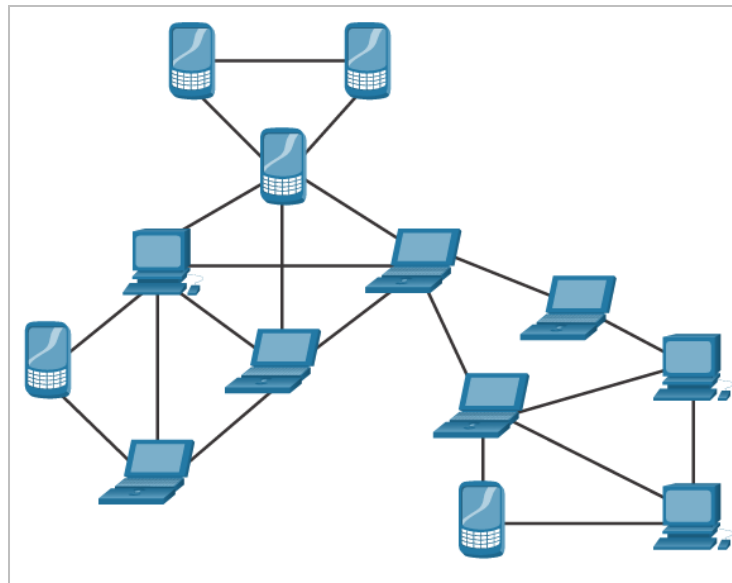
- A criptografia pode apresentar desafios para o monitoramento de segurança tornando os detalhes do pacote ilegíveis.
- A criptografia faz parte das tecnologias VPN. Nas VPNs, o IP é usado para transportar tráfego criptografado.
- O tráfego criptografado essencialmente estabelece uma conexão virtual ponto a ponto entre redes através de instalações públicas.
- A criptografia torna o tráfego ilegível para outros dispositivos, exceto os endpoints VPN.
- Uma tecnologia semelhante pode ser usada para criar uma conexão virtual ponto a ponto entre um host interno e dispositivos de atores de ameaças.
- O malware pode estabelecer um túnel criptografado que usa um protocolo comum e confiável e usá-lo para extrair dados da rede.

Tecnologias de Segurança

Rede Peer-to-Peer e Tor

- Na rede ponto a ponto (P2P), mostrada na figura, os hosts podem operar em funções de cliente e servidor.
- Os três tipos de aplicativos P2P são compartilhamento de arquivos, compartilhamento de processadores e mensagens instantâneas.
- No compartilhamento de arquivos P2P, os arquivos em uma máquina participante são compartilhados com membros da rede P2P.
- Bitcoin é uma operação P2P e BitTorrent é uma rede de compartilhamento de arquivos P2P.
- Aplicativos P2P de compartilhamento de arquivos não devem ser permitidos em redes corporativas. A atividade de rede P2P pode evitar proteções de firewall e é um vetor comum para a propagação de malware.

P2P

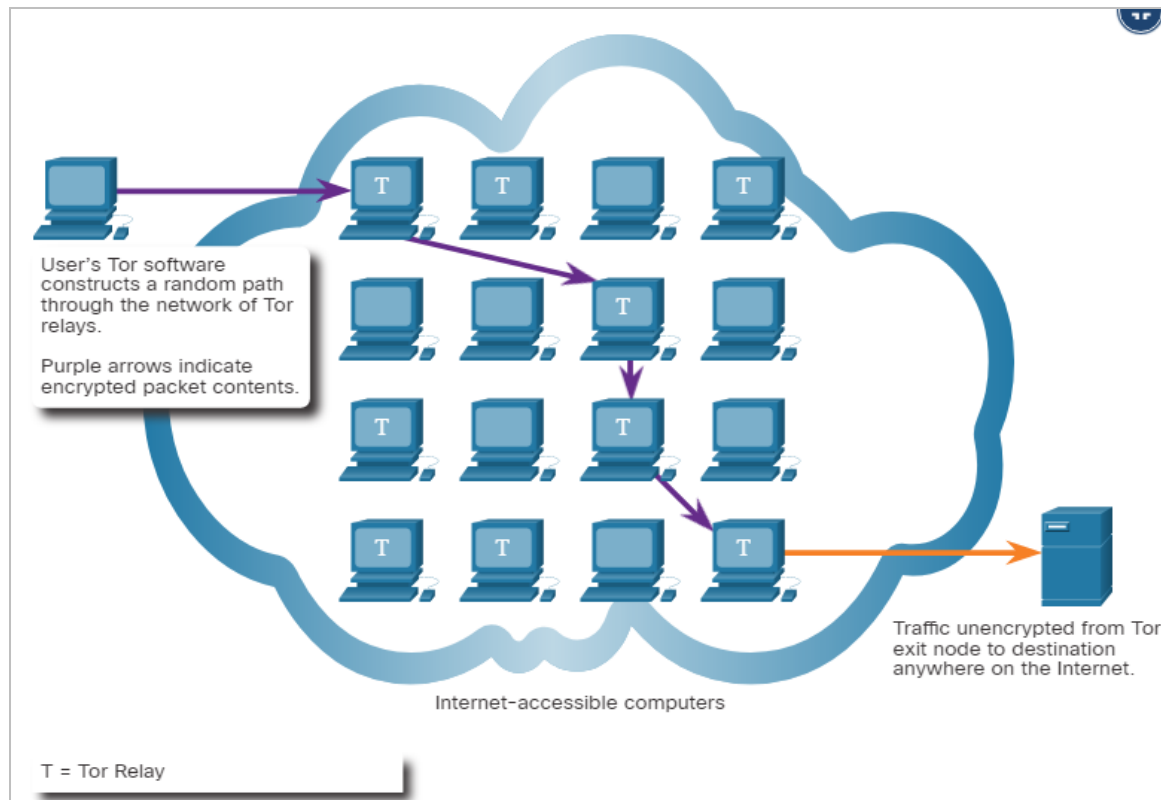


Tecnologias de Segurança Rede Peer-to-Peer e Tor (Condd.)

- P2P é inerentemente dinâmico. Ele pode operar conectando-se a vários endereços IP de destino e também pode usar numeração dinâmica de portas.
- As redes P2P de compartilhamento de processadores doam ciclos de processador para tarefas computacionais distribuídas.
- Pesquisa de câncer, pesquisa de extraterrestres, e pesquisa científica usam ciclos de processador doados para distribuir tarefas computacionais.
- Mensagens instantâneas (IM) também é considerado um aplicativo P2P.
- IM tem valor legítimo dentro de organizações que têm equipes de projeto distribuídas geograficamente.
- Nesse caso, aplicativos de IM especializados estão disponíveis, como a plataforma Webex Teams, que são mais seguras do que as mensagens instantâneas que usam servidores públicos.

Tecnologias de Segurança Rede Peer-to-Peer e Tor (Cont.)

- Tor é uma plataforma de software e rede de hosts P2P que funcionam como roteadores de internet na rede Tor.
- A rede Tor permite que os usuários naveguem na internet anonimamente. Os usuários acessam a rede Tor usando um navegador especial.
- Quando a navegação começa, o navegador constrói um caminho de ponta a ponta em camadas na rede do servidor Tor que é criptografado, como mostrado na figura.



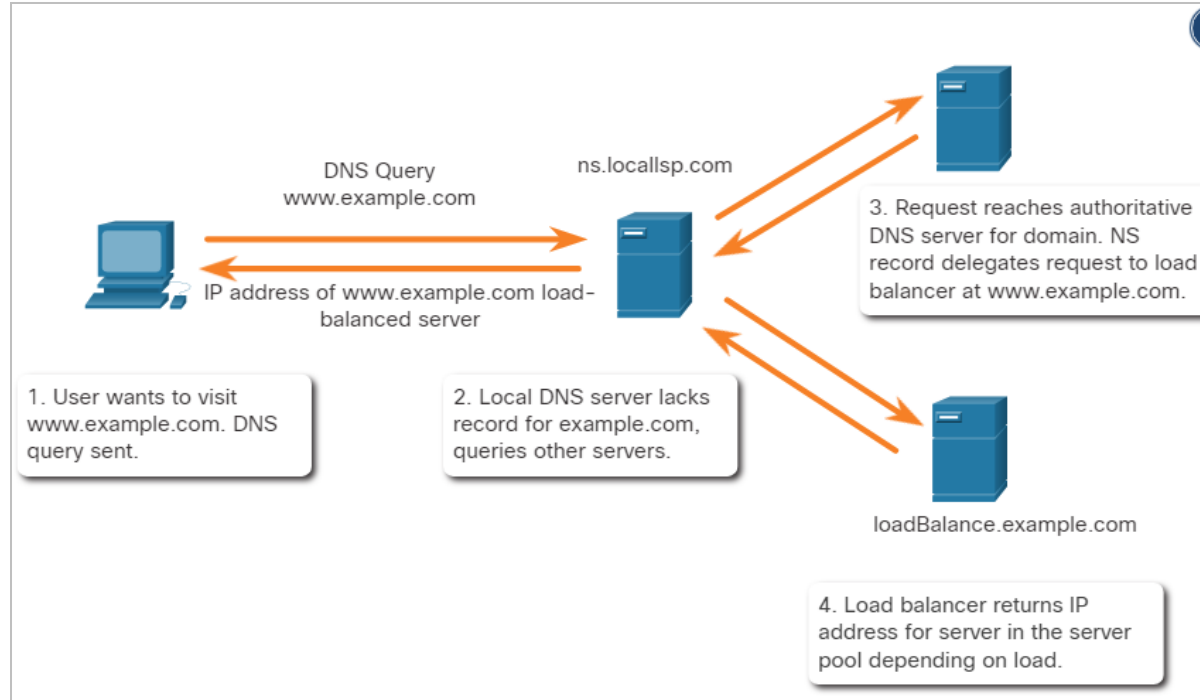
Tecnologias de Segurança Rede Peer-to-Peer e Tor (Cont.)

- Cada camada criptografada é “removida” como as camadas de uma cebola à medida que o tráfego atravessa um retransmissor do Tor. As camadas contêm informações criptografadas do próximo salto que só podem ser lidas pelo roteador que precisa ler as informações.
- Dessa forma, nenhum dispositivo único conhece todo o caminho para o destino e as informações de roteamento só podem ser lidas pelo dispositivo que as requer.
- Finalmente, no final do caminho do Tor, o tráfego atinge seu destino na internet.
- Quando o tráfego é retornado à origem, um caminho criptografado em camadas é construído novamente.
- Tor apresenta uma série de desafios aos analistas de segurança cibernética.
- Primeiro, Tor é amplamente utilizado por organizações criminosas na “Dark Net”.
- Além disso, Tor tem sido usado como um canal de comunicação para malware CNC.
- Como o endereço IP de destino do tráfego Tor é confundido pela criptografia, com apenas o nó Tor próximo salto conhecido, o tráfego Tor evita listas negras que foram configuradas em dispositivos de segurança.

Balanceamento de carga das tecnologias de

- O balanceamento de carga envolve a distribuição do tráfego entre dispositivos ou caminhos de rede para evitar recursos de rede sobrecarregados com muito tráfego.
- Se existirem recursos redundantes, um algoritmo ou dispositivo de balanceamento de carga funcionará para distribuir o tráfego entre esses recursos, conforme mostrado na figura.
- Uma maneira de fazer isso é através de técnicas que usam DNS para enviar tráfego para recursos que têm o mesmo nome de domínio, mas vários endereços IP.

Balanceamento de carga com delegação DNS



Balanceamento de carga de tecnologias de segurança (Cont.)

- Em alguns casos, a distribuição pode ser para servidores que são distribuídos geograficamente. Isso resulta em uma única transação de internet que é representada por vários endereços IP nos pacotes de entrada. Isso pode fazer com que recursos suspeitos apareçam em capturas de pacotes.
- Além disso, alguns dispositivos do gerenciador de balanceamento de carga (LBM) usam testes para testar o desempenho de diferentes caminhos e a integridade de diferentes dispositivos.
- Um LBM pode enviar testes para os diferentes servidores para os quais ele está balanceando o tráfego de carga, a fim de detectar que os servidores estão operando.
- Isso é feito para evitar o envio de tráfego para um recurso que não está disponível.
- Esses testes podem parecer tráfego suspeito se o analista de segurança cibernética não estiver ciente de que esse tráfego faz parte da operação do LBM.

24.3 Resumo de tecnologias e protocolos

O que aprendi neste módulo?

- Syslog é usado para enviar entradas de log para servidores centrais que executam um daemon syslog. Esta centralização da coleta de logs ajuda a tornar o monitoramento de segurança prático. Como o syslog é tão importante para o monitoramento de segurança, os servidores syslog podem ser um alvo para atores de ameaças.
- As mensagens do Syslog geralmente são carimbadas de data e hora. Como as mensagens vêm de muitos dispositivos, é importante que os dispositivos compartilhem um timeclock consistente usando o Network Time Protocol (NTP).
- Os atacantes encapsulam protocolos de rede diferentes dentro do DNS para evitar dispositivos de segurança.
- O DNS agora é usado por muitos tipos de malware. Algumas variedades de malware usam DNS para se comunicar com servidores de comando e controle (CnC) e para vaziar dados no tráfego disfarçado de consultas DNS normais.
- Uma exploração de HTTP é chamada de injeção iFrame (quadro inline). Para resolver a alteração ou interceptação de dados confidenciais, HTTPS deve ser adotado.
- HTTPS adiciona uma camada de criptografia ao protocolo HTTP usando SSL (Secure Socket Layer), tornando os dados HTTP ilegíveis.

O que aprendi neste módulo? (Continuação)

- Protocolos de e-mail como SMTP, POP3 e IMAP podem ser usados por atores de ameaças para espalhar malware, exfiltrar dados ou fornecer canais para servidores CNC de malware.
- O ICMP pode ser usado para identificar hosts em uma rede, a estrutura de uma rede e determinar os sistemas operacionais em uso na rede.
- Ele também pode ser usado como um veículo para vários tipos de ataque DoS e também pode ser usado para exfiltração de dados.
- Os invasores podem determinar quais endereços IP, protocolos e portas são permitidos pelas ACLs. Isso pode ser feito por varredura de portas ou testes de penetração, ou através de outras formas de reconhecimento.
- Conversão de Endereços de Rede (NAT) e Tradução de Endereço de Porta (PAT) podem complicar o monitoramento de segurança.
- Esse problema pode ser especialmente relevante com dados NetFlow que são unidirecionais e são definidos pelos endereços e portas que eles compartilham.

O que aprendi neste módulo? (Continuação)

- A criptografia pode apresentar desafios para o monitoramento de segurança tornando os detalhes do pacote ilegíveis. A criptografia faz parte das tecnologias VPN.
- Na rede ponto a ponto (P2P), os hosts podem operar em funções de cliente e servidor.
- Existem três tipos de aplicativos P2P: compartilhamento de arquivos, compartilhamento de processadores e mensagens instantâneas.
- Tor é uma plataforma de software e rede de hosts P2P que funcionam como roteadores de internet na rede Tor. Isso permite que os usuários naveguem na internet anonimamente.
- O balanceamento de carga envolve a distribuição do tráfego entre dispositivos ou caminhos de rede para evitar recursos de rede sobrecarregados com muito tráfego.
- Isso pode ser alcançado através de várias técnicas que usam DNS para enviar tráfego para recursos que têm o mesmo nome de domínio, mas vários endereços IP.
- Alguns dispositivos do gerenciador de balanceamento de carga (LBM) usam testes para testar o desempenho de diferentes caminhos e a integridade de diferentes dispositivos.

