Análise de Redes de Computadores

Palavras chaves:
PCAPs, TCPDump, tráfego de redes, redes de computadores;

Principais carreiras em Cibersegurança:

- Threat Hunter: threat hunters irão analisar pacotes de redes e e tráfego ao vivo enquanto caçam por ameaças avançadas que estão agindo secretamente dentro da rede. Isso pode incluir procurar comunicações incomuns, como não utilizar portas que não são padrões, escanear atividades, exfiltração.
- Analista de Segurança ou SOC: responsáveis por monitorar e responder a ataques contra a rede e têm que saber diferenciar atividades normais de atividades maliciosas. Eles provavelmente irão observar e responder a escaneamento de portas, vulnerabilidades, negação distribuída de ataques e casos de tráfego incomum de redes.
- Resposta de Incidentes: necessitam estar preparados para identificar, delegar e responder a um alcance infinito de incidentes de segurança, e ocasionalmente isso pode vai incluir algum tipo de de análise de rede para entender conexões entre sistemas comprometidos internos ou externos, ou um malware direcionado para um servidor comando e controle.

Redes

Palavras-chave: switch, router, hub, bridge, firewall.

- Roteadores: são dispositivos de rede que encaminham dados baseado em endereços lógicos. No caso da rede TCP/IP, o roteador pode encaminhar dados baseados nos endereços IPs dos sistemas. Uma pessoa que estiver em sua rede privada e deseja acessar o google, por exemplo, a requisição irá para o roteador, enquanto isso, o protocolo DNS irá converter o domínio do nome google.com para o endereço ip, e a requisição será enviada através da internet para o servidor web do google.

- Hub: São equipamentos que conectam os dispositivos em redes locais. Quando um sistema envia dados por meio do hub através de um hub, o hub enviará por meio de uma mensagem de broadcast para todos os outros dispositivos conectados nas outras portas. Por esse motivo, o hub é sempre referido como um dispositivo burro, por não saber identificar para quem os dados devem ser enviados. Embora os dados eventualmente cheguem ao sistema desejado. Esse tipo de transmissão gera tráfego desnecessário e pode possibilitar o roubo de dados.

- Switch: Este dispositivo desempenha a função do hub com mais inteligência, pois ele entende para onde deve enviar os dados ao invés de enviá-los para todos os

dispositivos. Isso é alcançado porque o switch usa o endereço mac como um identificador único para quem for receber os dados.

- Bridge: Conecta redes separadas para fazer com que elas se tornem uma rede maior. É diferente do que um roteador, que possibilita a rede se conectar mas trabalhar independentemente. No modelo OSI, a bridging trabalha na camada 2, na camada de enlace.

- Firewall: dispositivo de rede que provê segurança de rede, monitorando o tráfego que entra e sai, determinando o que deve ser bloqueado ou liberado, baseado em regras. O Firewall pode ser implementado como software ou hardware conectado à infraestrutura de rede. Isso possibilita criar redes privadas.

Portas e Serviços

- 20 (FTP) - esse protocolo é usado para transferir arquivos entre sistemas, onde usuários podem conectar a um produto FTP e podem visualizar, fazer upload ou fazer download.

- 22 (SSH) - SSH permite usuários se conectarem a dispositivos remotos, como servidores que possuem o serviço de SSH aberto. Esse canal é encriptado, portando, qualquer dado movimentado entre dois dispositivos conectados não são claramente visualizados.
- 23 (Telnet) - este serviço era utilizado antes do SSH, pois possui a mesma funcionalidade, porém Telnet não utilizava encriptação e o tráfego podia ser interceptado e visualizado por um atacante.
- 25 (SMTP) - Este protocolo é utilizado para enviar emails entre servidores através da rede, ou através de redes externas. É um método de transporte para realmente fazer o download e visualizar emails você necessita usar um cliente de e-mail e o protocolo POP ou IMAP.
- 53 (DNS) - DNS opera nas portas TCP e UDP 53 e usa banco de dados relacionais para converter nomes de domínios legíveis por humanos para seus respectivos endereços de IPs, então, essas comunicações podem ser enviadas para estes dispositivos.
- 67, 68 (DHCP) - foi desenhado para assinar informações de endereços ips relacionados para qualquer dispositivo na rede automaticamente, como máscara de subnet e endereço IP.
- 80 (HTTP) - permite que clientes se conectem em servidores webs e façam requisição de conteúdos,que aparecem em formas de downloads, páginas webs e serviços de streaming. Como o HTTP não é encriptado, é possível conduzir ataques de sniffing e visualizar texto claro como é transmitido entre cliente e servidor, como senhas.
- 443 (HTTPS) - HTTPS é uma versão segura do HTTP, e possui a mesma funcionalidade de recuperar conteúdos de servidores web. HTTPS usa encriptação para proteger os dados transferidos entre servidores web e clientes. Como virar o HTTP para HTTPS? Tem que utilizar TLS(transport layer security), anteriormente, conhecido como (SSL) Secure Socket Layer.