Relatório de Monitoramento de Conexões e Processos com sudo netstat -putan

Objetivo

O objetivo deste relatório é explorar detalhadamente o uso do comando sudo netstat -putan como uma ferramenta essencial para o monitoramento e análise de conexões de rede, processos e portas. A compreensão aprofundada dessa ferramenta permite:

- Identificar processos em execução que utilizam conexões de rede.
- Detectar comunicações suspeitas e ameaças dentro da infraestrutura de rede.
- Monitorar e diagnosticar problemas de conectividade e desempenho.
- Bloquear ou encerrar processos indesejados para garantir maior segurança.

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

Introdução

O `netstat` é um utilitário de linha de comando presente na maioria dos sistemas Unix/Linux e Windows, utilizado para exibir estatísticas detalhadas das conexões de rede, interfaces e tabelas de roteamento. No contexto de segurança da informação, seu uso é fundamental para a detecção de acessos indevidos e identificação de processos suspeitos em execução.

O comando `sudo netstat -putan` combina várias opções poderosas:

- ***p (Program**): Mostra qual processo está associado a cada conexão.*
- ***u (UDP):** Exibe conexões do protocolo UDP.*
- ***t (TCP):** Exibe conexões do protocolo TCP.*
- ***a (All):** Lista todas as conexões, incluindo as que estão ouvindo (`LISTEN`).*
- ***n (Numeric)**: Exibe endereços e portas em formato numérico, evitando resolver nomes de host.*

A análise das conexões TCP e UDP é crucial para entender como os dispositivos dentro de uma rede estão se comunicando. O TCP (Transmission Control Protocol) garante transmissão confiável de dados através de um processo de três vias (three-way handshake), enquanto o UDP (User Datagram Protocol) prioriza velocidade, sem verificação de entrega.

Ferramentas/Softwares Utilizados

VirtualBox, Terminal Linux (Comandos)

Monitoramento de Ameaças

Para encerrar um processo suspeito, podemos utilizar o kill ou killall:

- **kill -9 <PID>:** Mata um processo específico forçadamente.
- **killall <nome_do_processo>**: Finaliza todos os processos com o mesmo nome.
- **pkill -f <nome_do_processo>**: Mata processos com base em um padrão de nome.

- **fuser -k <porta>/tcp**: Mata o processo que está utilizando uma porta TCP.

Exemplo: sudo fuser -k 4444/tcp

Isso finaliza qualquer processo que esteja escutando a porta 4444/TCP.

Comandos Complementares

- ***lsof -i :<porta>****: Exibe qual processo está utilizando determinada porta.*
- ***ps aux | grep <PID>:*** *Obtém informações detalhadas sobre um processo.*
- ***iptables -A INPUT -s <IP> -j DROP:*** *Bloqueia um IP suspeito.*
- ***netstat -rn:*** *Exibe a tabela de roteamento.*
- ***ss -tulnp:*** *Alternativa moderna ao netstat, exibindo conexões ativas.*

Ataques UDP Flood e SYN Flood?

O comando sudo netstat -putan é muito útil para monitorar conexões e processos ativos na rede. Ele pode ajudar a identificar ataques de negação de serviço (DoS), como UDP Flood e SYN Flood, que sobrecarregam o sistema e podem derrubar serviços.

UDP Flood e o Netstat:

No ataque UDP Flood, o invasor envia uma grande quantidade de pacotes UDP para várias portas do alvo, consumindo recursos do sistema. O netstat pode ajudar a detectar esse ataque ao listar um número anormalmente alto de conexões UDP.

Para verificar isso, podemos rodar:

“sudo netstat -putan | grep udp”

Se um mesmo IP estiver enviando pacotes em excesso, isso pode ser um sinal de ataque.

SYN Flood e o Netstat:

O SYN Flood é um ataque que explora o processo de conexão TCP. O invasor envia várias solicitações, mas nunca completa a conexão, deixando o servidor preso esperando. Para verificar isso no netstat, podemos rodar:

“sudo netstat -putan | grep SYN_RECV”

Se houver muitas conexões no estado SYN_RECV, pode ser um ataque em andamento.

O Que Fazer?

Se identificarmos um ataque, podemos tomar medidas rápidas, como:

Bloquear o IP atacante:

“sudo iptables -A INPUT -s <IP> -j DROP”

- Usar ferramentas de proteção, como fail2ban, para bloquear automaticamente conexões suspeitas, como IPS bem elaborados.
- Configurar o firewall para limitar a taxa de conexões UDP e TCP.

Conclusão

O uso do comando sudo netstat -putan demonstrou ser uma ferramenta essencial para a análise e monitoramento da rede, permitindo uma visão aprofundada sobre os processos em execução, conexões ativas e potenciais ameaças à segurança. Através da sua aplicação, é possível identificar comunicações suspeitas, detectar anomalias e agir proativamente para mitigar riscos, como ataques de Negação de Serviço (DoS), incluindo UDP Flood e SYN Flood.

Além disso, este relatório destacou a importância da correlação entre monitoramento de rede e resposta a incidentes, evidenciando como ferramentas complementares, como lsof, iptables e fail2ban, podem ser integradas para formar uma camada robusta de defesa contra atividades maliciosas. O conhecimento e a utilização eficaz desses recursos possibilitam não apenas a detecção precoce de

ameaças, mas também a tomada de decisões estratégicas para garantir a estabilidade e segurança da infraestrutura de TI.

Diante do avanço das ameaças cibernéticas e da complexidade das redes modernas, o domínio de ferramentas como o netstat e sua aplicação em cenários reais de segurança se tornam cada vez mais indispensáveis para profissionais da área. A capacidade de interpretar os dados gerados, identificar padrões incomuns e agir rapidamente para conter incidentes é um diferencial fundamental para a proteção de sistemas e redes corporativas

Links Complementares

- ***Referência de Comandos Netstat:*** *https://example.com/netstat-guide*
- ***Guia de Monitoramento UDP:*** *https://example.com/udp-monitoring*
- ***Ferramentas de Análise de Rede:*** *https://example.com/network-tools*
- ***Práticas de Segurança em Redes:*** *https://example.com/network-security-practices*
- ***Análise de Portas e Protocolos:*** *https://example.com/port-protocol-analysis*