

* ou SRV de monitorização de tráfego
 * Para ver os pacotes, esses mesmos
 nes atacam como sniffers capturando e
 analisando o tráfego em tempo real.

1

Metodologias

a) Metodologias para aquisição de dados no cenário dado

São:

ou medir

- Capturar pacotes de dados, utilizando ferramentas de Captura de pacotes, como o Wireshark, para analisar o tráfego na rede e identificar padrões suspeitos de acessos remotos. Pode ser usado Gws.
- Medir fluxos de dados, implementando sondas de monitorização de fluxos em pontos estratégicos da rede para detectar padrões anormais no tráfego de dados, indicativos de acessos externos não autorizados. Aqui,

→ Obtenção dos logs dos serviços de dados, uma alternativa pode ser medir fluxos

pode ser utilizado Router ou firewalls dedicados ou máquinas dedicadas que estão a identificar os fluxos (quando começou, Pontos, SRC, DST no FW e for Router pode-se ver inicio e fim, quem fez o fluxo com quem & quantidade de bytes Upload/Download). No Router pode se utilizar Netflow ou IPFix fazendo report no ponto central.

- Obtenção dos logs dos serviços, pode-se configurar servidores de acesso remoto para registrar logs detalhados de todas as atividades, e centralizar a recolha desses logs para análise, onde pode ser observado as ações feitas pelo utilizador (como pedidos DNS, HTTPS, etc). Em alto nível pode ser utilizar os sistemas IDS e IPS para alertar múltiplos sistemas e analisar os logs dos servidores.

Metodologias para o tratamento de dados São:

- No caso dos pacotes, ver o conteúdo desses se estão ou não cifrados, os cabeçalhos, colocar filtros para os diferentes tipos de pacotes (download, upload, sequências temporais).
- No caso dos fluxos, agrupá-los de acordo com vários critérios de filtragem, i.e., ver a quantidade total de tráfego, o intervalo entre os fluxos, quantos fluxos houve ao longo do tempo (ver as janelas de observação para extração de dados).
- No caso dos logs, também pode ser agrupados, como contar os eventos, juntar os grupos diferentes eventos, juntar todos pedidos por exemplo TCP, etc.

Fluxo: São muitos pedidos. SRC, DST, frequentados de tráfego.
 como proceder, resolução tipo matriz

Fluxo:
 Pkt:

Começar a responder

possível metodologia

- 1) a) Uma alternativa para aquisição de dados seria
buscar os logs (em servidores ou máquinas dedicadas para este fim) no serviço de acesso remoto, i.e., utilizando por exemplo RSysLog que permitirá recuperar os logs e reportá-los para um sistema central a fim de serem analisados e detectar os possíveis padrões de comportamentos anômalos. Outra solução seria a implementação dos sistemas IDS/IPS.
- Para tratar esses dados, uma alternativa seria agrupar os diferentes eventos, verificar os padrões a partir de onde que os utilizadores estão a tentar se conectar (se ligar), juntar todos os pedidos feitos (TCP/HTTPS) para esses utilizadores.
- b) Uma possível metodologia para aquisição de dados na rede infectada seria a verificação dos fluxos de dados da rede. Os fluxos para este caso podem ser medidos no core da rede (ativar o Netflow por exemplo). A análise do comportamento da rede pode ajudar a identificar padrões suspeitos nas máquinas infectadas. Isto significa que para o conjunto de máquinas internas, verificar a comunicação entre as máquinas e o volume de tráfego entre elas de modo a identificar atividades maliciosas. A análise da janela temporal (janelas) poderá auxiliar a averiguar comportamentos suspeitos ao longo tempo.
- c) Para identificar as máquinas comprometidas na fase de exfiltração de dados, uma metodologia eficaz pode envolver a verificação dos pacotes de dados, monitorando o tráfego HTTPS e das máquinas existentes. A análise de padrões de comunicação, volume de dados transferidos e detecção de picos de atividades pode ajudar a identificar o elemento suspeito. A implementação de sistemas de análise de tráfego SSL/TLS e detectar mudanças abruptas no padrão de comunicação pode indicar a máquina comprometida.

2

Durante um ataque DDOS a um servidor HTTP/HTTPS é importante identificar os clientes lícitos dos ilícitos para garantir que o serviço continue disponível para os utilizadores legítimos e para bloquear o tráfego malicioso.

uma possivel metodologia para diferenciar os clientes lícitos dos ilícitos é a análise do comportamento do cliente. Esta análise procura por padrões de comportamento que são típicos de clientes legítimos e compará-los com o comportamento dos clientes durante o ataque. Basicamente essa diferença consistirá basicamente em verificar a nível da rede os intervalos entre os cliques ~~na tela~~ no caso dos pacotes ou verificar o conteúdo existente no servidor no caso dos logs.

Exame-TPR 14-02-2022 (EP. Normal)

1

a) uma possivel metodologia para aquisição de dados a nível da rede seria a verificação da comunicação de certos servidores que não sejam normais, i.e., verificar os fluxos dados da rede de modo a analisar padrões de comportamentos considerados como suspeitos. (todas aquelas comunicações iniciadas de fora ou sincronização entre servidores, isto pode ser gty IPs e o instante em que ~~os~~ ^o começa).

b) As possíveis métricas (para os fluxos de dados) que poderão permitir distinguir a comunicação lícita da ilícita são: ~~o~~ Origem, destino, quem iniciou a comunicação e quantidade de tráfego trocada nos dois sentidos.

As possíveis features (para os fluxos de dados) que poderão distinguir essas comunicações são: quantos fluxos apareceram num determinado intervalo de tempo, O intervalo entre fluxos e as transferências de dados desses fluxos, Pode-se assumir que a métricas ~~que~~ referentes podem ser usadas como features.

* ~~casos~~ ^{individual} tiver uma janela de observação maior, os fluxos podem ter featuras com poucos parecidos com dos PKT. como: $n^{\text{º}}$ de fx, $n^{\text{º}}$ max fx, $n^{\text{º}}$ média fx na janela, o desvio padrão da variância do $n^{\text{º}}$ fx (upload, Download) e multiplicar isto tudo.

c) Uma possível metodologia de tratamento de dados que permita obter dados relevantes para este caso seria a utilização de secalograma para detectar periodicidade. (contagem de pacotes). Outra possível metodologia seria a verificação dos intervalos entre silêncios, fluxos de pacotes, fazer um gráfico com sequência temporal, contar o $n^{\text{º}}$ de zeros ^{síndicos} para ver os tempos de silêncio e calcular a média dos tempos de silêncios. Quando a variância é quase zero é periódico e quando for ~~zero~~ + período a variancia não é zero.

2] Por um lado, um ataque de desrupção é um tipo de ataque cibernético que visa a interromper o funcionamento de ~~uma~~ uma rede, serviço ou infraestrutura. Isto pode ser feito de várias maneiras incluindo ataques ~~D~~DDOS, fazendo com que o sistema fique lento ou indisponível. Possíveis soluções: implementações de LB, Firewall stateless e sistemas IDS/IPS.

Por outro lado, um ataque de exfiltração de dados envolve a transferência não autorizada de dados de uma rede ou sistema para um local externo. Isto pode ser feito incluindo phishing, malware, ou até mesmo ataques de força bruta para obter acesso a sistemas protegidos por senha. Possíveis soluções: Criptografia de dados, ~~PKI~~, MFA, sandbox e conscientização sobre segurança às pessoas.

1) a) Uma possível metodologia de agregação de dados a nível da rede e dos SRVs, seria a verificação dos fluxos de dados da rede. Neste caso, os fluxos podem ser medidos no core da rede (por exemplo ativar Netflow). A análise do comportamento da rede para o serviço de DNS pode ajudar a identificar padrões suspeitos no servidor específico. Além disso, a análise da janela temporal (janela de observação) poderá auxiliar a verificar comportamentos suspeitos ao longo do tempo.

b) As possíveis métricas (para os fluxos de dados) que poderão permitir distinguir a comunicação DNS lícita da ilícita são: origem, destino, quem iniciou a comunicação e a quantidade de tráfego tracado nos dois sentidos.

As possíveis features (para os fluxos de dados) que poderão distinguir essas comunicações, considerando que tem-se uma janela temporal maior são: nº de fluxo, nº máx de fluxo, nº médio de fluxo na janela, o desvio padrão, a variância do nº de fluxo (upload, download) e no final multiplicar tudo.

c) Uma possível metodologia de tratamento de dados que permite obter dados relevantes para este caso, seria a utilização de seatalogramas para detectar periodicidade. Outra possível metodologia seria a verificação dos intervalos entre silêncios, fluxos dos pacotes, fazer um gráfico com sequência temporal definida, contar o nº de zeros seguidos para ver os tempos de silêncio e calcular a média dos tempos de silêncio.

Quando a variação é igual a zero, notar-se-á um sinal periódico, e quando o sinal for ± periódico, a variação não é zero.

Ver resposta ~~para~~ no escane de recursos 2022.

I) a) Uma possível metodologia de aquisição de dados para este cenário seria a verificação dos logs de dados nos servidores de e-mail da organização, utilizando por exemplo RSYLOG que permitirá recuperar os logs e reportá-los para um sistema central de modo a serem analisados e detectar os possíveis padrões de comportamentos anômalos.

Para processar esses dados, uma alternativa seria a criação de sequências temporais com diferentes métricas estatísticas (por exemplo com período de amostragem de 10ms e janela de observação deslizante de 30 segundos) e fazer a extração de características dos logs de dados tais como: agrupar os diferentes eventos, contar o nº de eventos, verificar a partir de onde que os utilizadores estão a tentar se conectar e por fim todos os pedidos feitos por esses utilizadores.

Para a criação do "profiling", uma possível metodologia seria a criação de modelos de comportamentos a partir das métricas/features dos dados processados e com base nos dados históricos de múltiplas janelas de observação. Este modelo passa por envolver a utilização de PCA de modo a reduzir a complexidade dos dados (variable reduction), de seguida passa pela tomada de decisão usando padrões estatísticos ou ML (clustering, ANN, Ensemble, SVM, Decision Tree, etc) e por último, os dados do modelo passam pela classificação e deteção de anomalias de tal forma que esses dados sejam filtrados e agregados de acordo aos IPs origem/^{SRC}/dest^{DST}, portos SRC/DST e tipo de protocolo.

b) Uma possível metodologia de aquisição de dados para este cenário seria a verificação dos fluxos de dados. Neste caso, os fluxos podem ser medidos no core da rede, através por exemplo o protocolo Netflow ou IPFix. Também se pode implementar sondas de monitorização de fluxos nos pontos estratégicos da rede para detectar padrões anômalos no tráfego de dados.

Para processar esses dados, uma alternativa seria a criação de sequências temporais (por exemplo com período de amostragem de 10ms e sliding window de 30s) com diferentes métricas estatísticas tais como: IP SRC/DST, porto SRC/DST, quem iniciou a comunicação e a quantidade de tráfego trocado nos dois sentidos. Além disso, pode ser feito a

⇒

extração de características dos fluxos de dados (considerando que se tem uma janela temporal maior) tais como: o nº de fluxo, o nº max de fluxo, o nº médio de fluxo na janela, o desvio padrão, a variação do nº de fluxo (download/upload) e por último multiplicar todas estas features obtidas à partir das métricas.

Para criar o "Profiling", uma possível metodologia seria a criação de modelos de comportamentos a partir dos dados processados e com base nos dados históricos de múltiplas janelas de observação. Este modelo passa por ~~envolver~~ envolver a utilização de PCA para reduzir a complexidade dos dados (variable reduction), de seguida passa pela tomada de decisão usando padrões estatísticos ou ML (clustering, ANN, SVM, Decision Tree, Ensemble, etc) e por último os dados do modelo passam pela classificação ou deteção de anomalias *de acordo com os IPs SRC/DST, Portos SRC/DST e tipo de protocolo.

c) uma possível metodologia de aquisição de dados para este cenário seria a verificação dos pacotes de dados. Neste caso, para medir os pacotes de dados, podem ser usados Gateways ou Servidores de monitorização de tráfego de dados. Algumas das ferramentas mais utilizadas para que podem ser usadas neste cenário para a captura e monitoramento de dados tais como: Wireshark, Tshark, Pshark, ~~Snort~~ Zabbix e Suricata.

Para processar esses dados, uma alternativa seria a ~~extração~~ extração de sequências temporais (por exemplo com sampling period de 10ms e sliding window de 30s) com diferentes métricas estatísticas tais como: nº de pacotes de download/upload, nº de bytes de download/upload. Além disso, pode ser feita a extração de características de pacotes de dados, tais como: a média, a mediana, o desvio padrão, a variação e os percentis/quantis.

[2] a) Durante um ataque de DDoS é importante diferenciar os pedidos lícitos dos ilícitos para garantir que o serviço continue disponível para utilizadores legítimos (White List IP) e para bloquear o tráfego malicioso no caso dos utilizadores ilegítimos (Black List IP).

b) (i) - Uma possível metodologia para os diferenciar quando o ataque é dirigido a um servidor HTTPS seria a verificação dos intervalos entre cliques, verificação de sessões autenticadas, análise de padrões de tráfego e verificação dos cookies.

(ii) - uma possível metodologia para os diferenciar quando o ataque é dirigido ao serviço de DNS seria a verificação do nº de pedidos de DNS, o intervalo entre pedidos, o que foi pedido (o domínio), rate limiting e análise de padrões dos pedidos.

[3] a) Uma possível metodologia para melhorar o desempenho na deteção de anomalias ao fim de um período de observação. seria a utilização do ensemble, método Bagging cuja a decisão final é baseada nos resultados dados por cada metodologia (ou utilizar Bayes Optimal classifier, cuja a decisão final é baseada nas probabilidades dadas por cada metodologia).

b) num cenário onde a decisão pode ser mais lenta, seria ~~utilizar~~ também a utilização de decisões baseadas em ML (Ensemble), i.e., utilização do método Boosting cuja a decisão final é baseada em diferentes metodologias aplicadas em sequência.

