**28 de Fevereiro de 2022**

1.

a)

**Aquisição** : capturar pacotes -> onde por o tap (datacenter, saída da empresa, colocar numa entrada do switch) e como?

Logs dos servidores. DNS, https… (que maquina ligou-se, utilizador autenticou-se e que troca de eventos)

Fluxos? Em que maquinas ? Firewall(report dos fluxos origem destino e timestamp), routers(inicio, fim, quem falou com quem, durante quanto tempo, upload e download) IPxx?

**Tratamento de dados**. O que fazer com dados?

Contar os pacotes(upload e download) e gerar gráficos que descrevam o trafego de rede num intervalo de tempo

Fluxos: olhar para as características de um fluxo observando ou colocar critérios (intervalos entre fluxos, quantos fluxos houve)

Logs: evento com timestamp -> contar eventos, com timestamp -> juntar pedidos do tipo x de um determinado cliente e depois conta-los …

Que dados queremos medir no caso deste alínea? Localização -> logs do servidor (servidor x tentou se ligar) recuperandos os eventos para um ponto central e analisando os resultados -> nome do utilizador + ip

Deteção: criar histórico de acesso aos servidores -> verificar mudanças “estranhas” de ip -> se houver um ip novo a aceder bloquear ou notificar gestor de rede

Comprometer maquina em vez de roubar credencias ? (ip credível com palavra passe correta) como ? Analise de comportamento -> analisar fluxo em vez de logs

Se for logs podíamos analisar as horas de acesso, e que ações estão a fazer por segundo e comparar com o histórico/passado do utilizador.

b) enquanto na alínea a) era serviço aqui é uma questão de rede interna

botnet -> processos ilícitos nas maquinas falando entre si

como detetar botnets? Que dados precisam? Fluxos ou pacotes

fluxos vs pacotes -> fluxos são bons para identificar quem fala com quem e quantidade de trafego

pacotes -> quem fala com quem, quantidade de trafego e maios resolução temporal

Aqui neste caso fluxos era mais eficiente pq so queríamos saber quem fala com quem.

No core da rede(distribuição) ativar *netflow* para saber quem fala com quem.

Como identificar as maquinas? Que dados vamos medir? (Se As maquinas não falam entre si falam entre servidores. Identificar novas comunicação)

Identificar quem fala com quem, quando e que intervalos de tempo e que quantidades (tempo absoluto ou relativo). Identificar nr de fluxos por janela temporal (5mn p.e ).

Verificar se anomalias de histórico

Para cada par de maquinas ver o nr de fluxos criados ao longo de um dia e criar gráficos

E observar **modelo de comunicação** a ver se há mais fluxos ou mais ou menos a mesma quantidade.

c) exfiltração por https -> se é ao nível da rede geralmente não são logs

ips das maquinas + servidores -> difícil de destinguir comunicações licitas vs ilícitas pois estão a usar o mesmo protocolo

Precisamos de pacotes para ver como as transferências estão a ser realizadas -> gráficos

Ver todas as maquinas da empresa e ver como os uploads foram feitos num dado intervalo (medir trafego) e ver como as transferências foram feitas acima de um treshold acima de x mb/s e comparar com histórico.

Upload de botnet é indestiguinvel com o upload normal

Ver padrão de transferências

2) (Criar um blacklist de ips a bloquear de maquinas que estão a gerar pacotes mas se for um ataque inteligente as maquinas vao mandando poucos pacotes entre elas.

Bloquear ips de geolocalizações estranhas )

Distinguir clientes bons vs maus ? identificar ips que so mandam SYN’s e não recebem ACK e bloquear ips

Atacante pode pedir a pagina ou objetos da pagina e completa a sessão tcp

Ver log do servidor e observar se o cliente que esta sempre a pedir a mesma cena durante um ataque de ddos -> bloquear ip

No entanto, o atacante pode ser inteligente e ir variando os pedidos -> podemos comparar intervalos tempo entre cliques com o histórico de clientes lícitos num intervalo (intervalo entre cliques)(modelo de dados) isto se for ao nível da rede

OU acedendo ao log do servidor e ver onde os cliques estão a acontecer e ver a posição dos links onde estão a ser clicados. Se o atacante estiver a clicar com sequencias do objeto pode se criar um modelo de acesso ao serviço.

Neste caso aqui os fluxos não da pq os fluxos juntam as mesmas ligações

**14 de Fevereiro de 2022**

1)

a) SERVIDORES -> não implica logs !

Comunicações de servidores que não sejam normais

Fluxos ou pacotes.

Fluxos -> procurar servidores que iniciam comunicações(do servidor) para fora (ou receber pedidos de fora) ou sincronização entre servidores. Se um servidor começa a contactar um ip que nunca contactou -> possível anomalia

Fluxos -> ip’s + quantidade de trafego + tempos

Tambem podemos ver como os uploads e transferências de dados estão a ser feitos. As comunicações de dados entre servidores

Identificar servidores se esta a comunicar com um padrão diferente

b) **métricas** : quantidade de pacotes upload e download e bytes upload e download) -> pacotes

**métricas**: quantos fluxos num intervalo de tempo, intervalo entre fluxos-> fluxos

**features** -> varias janelas de obs

pacotes : quantos pacotes usados na comunicao, media maxima variância das 4 metricas

pegar em vários fluxos-> dinâmicas das diferentes comunicações e ver o nr de fluxos, máximo de fluxos, media de fluxos, variância de fluxos, bytes de cada fluxo (em fluxos a janela temporal é maior se for pacotes é mais pequenos)

c) Detetar periodicidades :

colocar um limiar -> calcularam os intervalos de silencio acima desse pico e abaixo desse pico e ver intervalos de silencio para calcular periodicidade (se desvio padrao for 0 é um ataque periódico)

Contar pacotes e nr de 0 seguidos e calcular a media desse valores.

2)Ataque de disrupção (negação de serviço e fácil de detetar pq há um elevado trafego de rede. O difícil é detetar cliente licito vs ilícito)

vs exfiltração (detetar transferência de dados para acima de um limiar, e se for um ataque inteligente stealth temos de comparar os comportamentos por maquina e as comunicações por fora e se esta dentro dos padroes de comunicação)

**16 janeiro 2023**

1)a) exfiltração via DNS por nível da rede -> ou é fluxos ou é pacotes

Aquisição de dados:

Caracterizar comunicações DNS

Pacotes -> upload e downlod nr de pacotes + bytes

Features -> 2 a 5 mn janela de obs, máximo, media variância

Fluxos 🡪 cada fluxo é uma interação com o servidor DNS, e calcular intervalo entre fluxos e nr de fluxos (uma resolução é um pedido dns)

Se não fosse ao nível de rede, podíamos ir aos logs DNS

Procurar subdomínios esquisitos (com muitos caracters)

Ver os pedidos dos pacotes?

DNS hoje vai sobre https (cifrados) que fica indestinguivel

VARIANCIA DE INTERVALO DE SILENCIOS