Segurança e visibilidade informática com Bro IDS

Thibaut Gérard Paul Pierre RA: 153014
Coordenador : Christian Esteve Rothenberg

O que acontece quando um computador entra sem proteção no o domínio público ?

O Bro IDS é um software dedicado ao monitoramento de tráfego informático. Pelo motivo de responder à pergunta precedente, deixamos um servidor, com o Bro ativo, monitorar a DMZ de um modem ADSL.

DMZ significa em inglês: « Demilitarized Zone ».
É uma área local que recebe em broadcast todas comunicações recebidas no endereço público do roteador.

Para se conectar ao servidor a distância, configuremos uma conexão SSH protegida por um casal login e senha. Por precaução, impedimos a conexão SSH com o login padrão "root" e mudemos a porta ativa padrão 22 para a porta 22222. Sem divulgar o endereço publico da DMZ, deixamos o servidor ativo, em contato com a Internet, dois dias e duas noites.

Durante esse período todo, o Bro IDS está vigiando os processos ativos na interface da máquina . Ele grava informação, na forma de arquivos log, explicativas da atividade vista.

Segue um excerto do arquivo de log a manhã o terceiro dia, entre 7h e 10h20.

```
# cat conn.07\:00\:08-10\:20\:50.log | awk '$3 !~ /192.168.17.*/ {print $3,
$6, $12}' | sort | uniq -c | sort -g
```

1	62.210.94.29	2472	REJ
1	62.210.94.29	2471	REJ
1	62.210.94.29	2472	REJ
1	62.210.94.29	2473	REJ
1	62.210.94.29	2474	REJ
1	62.210.94.29	2475	REJ
1	62.210.94.29	2476	REJ
1	62.210.94.29	2477	REJ
1	62.210.94.29	2479	REJ
1	62.210.94.29	2480	REJ
1	69.64.40.157	5060	S0
1	74.82.47.53	19	S0
1	221.229.166.28	22222	SF
1	79.114.63.55	23	REJ
1	88.250.200.59	23	REJ
1	89.248.172.154	139	RSTOS0
1	89.248.172.154	139	S0
1	89.248.172.173	22222	SH
1	90.13.157.110	0	OTH
1	90.13.157.110	22222	SH
1	91.224.132.118	8085	REJ
2	107.160.20.146	1433	REJ
2	221.229.166.30	22222	RSTOS0
2	58.218.211.166	22222	RSTOS0
2	89.91.229.157	22222	OTH
3	114.43.251.220	25	REJ
3	118.166.213.19	25	REJ
3	198.13.108.245	1433	REJ
3	218.87.111.116	22222	SH
3	58.218.205.68	22222	RSTOS0
3	58.218.205.68	22222	SH
3	58.221.236.202	3389	REJ
4	221.229.166.66	22222	RSTOS0
4	221.229.166.66	22222	SH
4	58.218.205.67	22222	SH
4	58.218.205.70	22222	RSTOS0
5	222.186.160.48	22222	RSTOS0
5	58.218.205.67	22222	RSTOS0
12	221.229.166.30	22222	SH
17	124.248.41.37	22222	SH
18	113.106.239.26	80	REJ
19	58.218.205.66	22222	SH
29	122.195.189.84	22222	SH
30	222.186.160.48	22222	SH
30	58.218.205.70	22222	SH
300	198.148.116.178	22222	SH
3588	83.174.198.14	22222	RSTOS0

Busca de portas abertas em processo.

```
$ cat conn.07:00:08-10:20:50.log | bro-cut  -nd | awk '$3 ~ /62.210.94.29/ {print $1, $3, $6, $12}' | sort
| ( head -n 1 && tail -n 1 )
    2015-05-29T07:01:45+0200    62.210.94.29    2439    REJ
    2015-05-29T10:17:39+0200    62.210.94.29    2480    REJ
```

Entre 7h 01' e 10h 17' a internauta experimentou as portas entre a 2439 e a 2480. Se ela continua manter uma velocidade constante, então ela achara a porta aberta número 22222 em 65 dias e 12 horas.

SF : Normal estabelecimento e terminação da conexão. Alguém se conectou com sucesso nossa maquina.

OTH : Nenhum indicador SYN visto, apenas dados nem identificados e nem corretamente fechados.

Os dados recebidos não obedeceram à forma prevista pelo protocolo TCP. O uso da porta 0 é também esquisito, porque não é uma porta padrão.

```
$cat conn.07:00:08-10:20:50.log | bro-cut id.orig_h id.resp_p proto conn_state | awk '$2 ~ /^0$/ {print}'
    90.13.157.110   0       icmp    OTH
```

Usou o protocolo ICMP, que serve, por exemplo, para transmitir mensagens de erro.

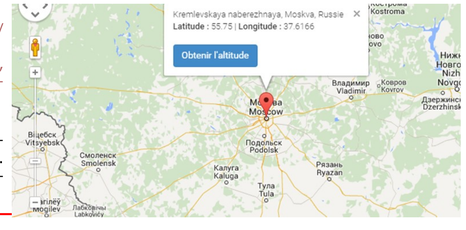
RSTOS0 : Originador emitiu o indicador SYN seguido pelo indicador RST. Nenhum indicador SYN-ACK foi visto da parte do recebedor.

As internautas emitiram um SYN, então tentaram estabelecer uma conexão TCP. Pois foram pedidos uma senha pelo protocolo SSH. Elas desistiram da tentativa de conexão com o indicador RST.

Aqui, as internautas Tentaram se conectar muitas vezes. Isso indica o uso de metodologia automatizada para conseguir a conexão. Talvez que são ataques de senha por dicionário.

```
$ bro -b /usr/local/bro-geo/scripts/geolocate.bro 83.174.198.14
   [country_code=RU, region=<uninitialized>, city=<uninitialized>, latitude=55.75, longitude=37.6166]
```

Os endereços IP do mundo inteiro estão localizados em bancos de dados por parte públicos. Quem tentou mais vezes se conectar tem hipóteses de ser Russo.



Como compensar as velocidades de comunicações sempre maiores para as ferramentas de segurança de redes?

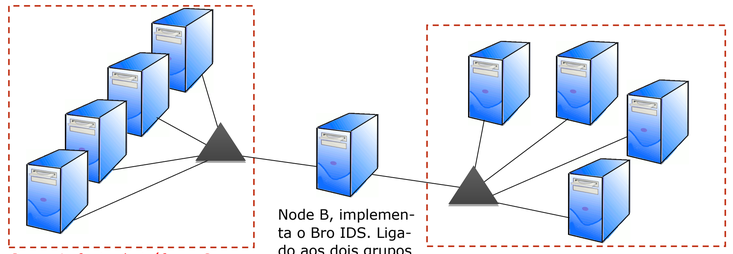
Um desafio atual da tecnologia dos IDS é manter sua pertinência para vigiar fluxos de dados com velocidade crescente. Os processadores perdem em velocidade, relativamente à aceleração dos fluxos de dados transmitidos. Por isso, estamos obrigados achar soluções para dividir a tarefa em partes independentes, que poderiam ser processadas por vá rias maquinas físicas.

Porém, essas soluções de paralelização são ainda pouco desenvolvidas. O Bro IDS possui um modo de funcionamento em cluster, que permite gerar o processamento de vária s instancias trabalhadoras desde uma má quina mestre. Experimentamos essa construção.

Usamos, para instalação da experiência, os recursos oferecidos pelo Testbed DeterLab.

Da mesma maneira que um Cloud poder fornece poder de cálculo, ou espaço de memória a distância , um Testbed oferece redes de maquinas virtuais accessíveis a distância.

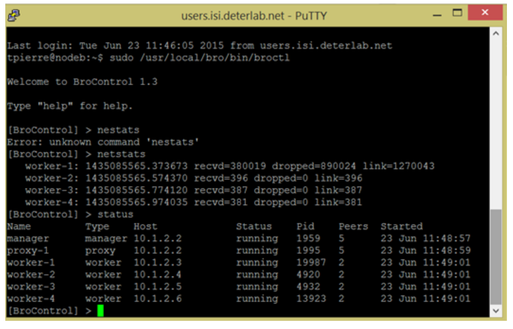
O configuramos com a topologia seguinte:



Grupo A, fonte de tráfego. Cada computador pode mandar pacotes na taxa de 280 Mbps.

Node B, implementa o Bro IDS. Ligado aos dois grupos por uma conexão de capacidade de 1Gbps.

Grupo C, trabalhadores. São relacionados com o node B, mestre do cluster.



O Bro IDS, apesar de ser um software altamente configurável, ainda não oferece soluções para dividir a carga de trabalho entre diferentes máquinas. A construção de cluster, com várias instancias trabalhadoras e uma instancia mestre, é pertinente para paralelizar a tarefa entre vários processos sobre uma máquina só, e não pode ser usado entre diferentes hardwares.

Temos, na janela à esquerda, o seguido dos dados recebidos pela instancia mestre e transmitidos pelo cluster de instancias trabalhadoras. O trabalhador worker-1 recebe o fluxo inteiro. Não tem roteamento de pacotes.

A paralelização do tratamento entre vários servidores leva a problemática de detecção de "ataques em vários passos". Os passos do mesmo ataque, tratados por servidores diferentes, perdem a significação deles.

Leva ainda problemáticas de velocidade do roteador. Ele que divide o trafego entre as instancias do IDS. A velocidade do tratamento multiplicado pelo número de instancias paralelas torna o desempenho do roteador crítico.

O compartilhamento da memória entre maquinas é também assuntos sem resposta padrão. Escolhemos implementar uma memória viva, conectada a todos processos independentes, com risco de perder desempenho quando o número de processos conectados aumenta, ou, ao contrário, devemos isolar os servidores uns dos outros, e perder a correlação entre dados analisados por diferentes servidores?

Por isso, entre outras razões, as soluções de alto desempenho envolvendo paralelização do tratamento são, até agora, soluções extraordinárias, que usam hardware específico e software de baixo nível.

CONCLUSAO

O trabalho de final de curso foi uma pesquisa experimental relacionada com os desafios atuais da segurança informática. Tratamos tanto o entendimento dos protocolos básicos, sobre quais estão baseadas as comunicações do mundo inteiro, como os problemas de alta tecnologia ainda não resolvidos e que se tornam sempre mais premente.