Sessão 6: Registro e correlacionamento de eventos

INTRO e, finalmente, registrar os comandos digitados pelos usuários em logs do sistema.

1) Criação da máquina

Clonar `debian-template` para `log`, IP 10.0.42.4/24. Alterar *hostname* e realizar integração LDAP/SSH-CA como usual.

Criar entrada para o novo *host* no DNS (não esqueça de aumentar o serial), assinar zona e reiniciar *daemons*. Testar.

```
# hostname ; whoami
fw
root
```

```
# grep log /etc/nsd/intnet.zone
log     IN    A                10.0.42.4
```

```
# grep log /etc/nsd/10.0.42.zone
4       IN   PTR               log.intnet.
```

```
# bash /etc/nsd/signzone-intnet.sh
reconfig start, read /etc/nsd/nsd.conf
ok
ok
ok
```

```
# systemctl reload unbound
```

```
# nslookup log
Server:         127.0.0.1
Address:        127.0.0.1#53

Non-authoritative answer:
Name:   log.intnet
Address: 10.0.42.4
```

2) Configuração do NTP

Logar como `root` na máquina `log`. Instalar o OpenNTPD.

```
# hostname ; whoami
log
root
```

```
# apt-get install openntpd
```

Fazer o backup do arquivo original e configurar o OpenNTPD.

```
# mv /etc/openntpd/ntpd.conf /etc/openntpd/ntpd.conf.orig
```

```
# cat /etc/openntpd/ntpd.conf
listen on 127.0.0.1
listen on 10.0.42.4
servers pool.ntp.br
```

Pare o OpenNTPD, sincronize o relógio imediatamente.

```
# systemctl stop openntpd.service
```

```
# mkdir /var/run/openntpd ; ntpd -s -d -f /etc/openntpd/ntpd.conf -p
/var/run/openntpd.pid
adjtimex returns frequency of 0.000000ppm
/var/lib/openntpd/db/ntpd.drift is empty
listening on 127.0.0.1
listening on 10.0.42.4
ntp engine ready
reply from 200.160.7.186: offset -0.003035 delay 0.018363, next query 8s
set local clock to Sat Nov  3 17:25:41 -03 2018 (offset -0.003035s)
reply from 200.160.7.193: offset -0.003952 delay 0.019983, next query 5s
reply from 200.160.0.8: offset -0.003851 delay 0.020152, next query 7s
reply from 200.186.125.195: offset -0.002323 delay 0.023158, next query 7s
reply from 200.20.186.76: offset -0.003652 delay 0.027538, next query 6s
```

Após a sincronização, pare o processo com `CTRL + C`, apague o diretório `/var/run/openntpd` e inicie o OpenNTPD. Cheque se está escutando como esperado.

```
^C ntp engine exiting
Terminating
dispatch_imsg in main: pipe closed
```

```
# rmdir /var/run/openntpd
```

```
# systemctl start openntpd.service
```

```
# ss -unlp | grep 123
UNCONN     0      0      10.0.42.4:123                    *:*
users:(("ntpd",pid=1643,fd=8))
UNCONN     0      0      127.0.0.1:123                    *:*
users:(("ntpd",pid=1643,fd=7))
```

Configurar todos os servidores de uma única vez: como `han@client`, crie o *script* `/home/han/scripts/install-openntpd.sh` com o seguinte conteúdo:

```
1 #!/bin/bash
2
3 # instalacao
4 DEBIAN_FRONTEND=noninteractive apt-get -yq install openntpd
5
6 # configuracao
7 mv /etc/openntpd/ntpd.conf /etc/openntpd/ntpd.conf.orig
8 echo "server 10.0.42.4" > /etc/openntpd/ntpd.conf
9
10 # reiniciar ntpd
11 systemctl restart openntpd.service
```

Executar com:

```
$ for server in fw ldap nfs; do scp ~/scripts/install-openntpd.sh ${server}:~ && ssh
han@${server} 'echo seg10han | sudo -S bash /home/han/install-openntpd.sh' && ssh
${server} rm ~/install-openntpd.sh; done
```

Verifique a correta instalação:

```
$ echo '---'; for server in fw ldap nfs; do ssh han@${server} 'hostname ; dpkg -l |
grep openntpd ; cat /etc/openntpd/ntpd.conf; ps auxwm | pgrep ntpd'; echo '---'; done
---
fw
ii  openntpd                       1:6.0p1-2                      amd64        OpenBSD
NTP daemon
server 10.0.42.4
4950
4954
4956
---
ldap
ii  openntpd                       1:6.0p1-2                      amd64        OpenBSD
NTP daemon
server 10.0.42.4
1354
1364
1366
---
nfs
ii  openntpd                       1:6.0p1-2                      amd64        OpenBSD
NTP daemon
server 10.0.42.4
5192
5193
5194
---
```

3) Registro de comandos digitados com SnoopyLog

Instalar Snoopy para gerar trilha de auditoria de comandos digitados por usuários. Como `han@client`, criar script `/home/han/scripts/install-snoopy.sh` com o seguinte conteúdo:

```
1 #!/bin/bash
2
3 # instalacao
4 DEBIAN_FRONTEND=noninteractive apt-get -yq install snoopy
5
6 # configuracao
7 echo "/lib/snoopy.so" > /etc/ld.so.preload
```

Executar com:

```
$ for server in fw ldap nfs log; do scp ~/scripts/install-snoopy.sh ${server}:~ && ssh
han@${server} 'echo seg10han | sudo -S bash /home/han/install-snoopy.sh' && ssh
${server} rm ~/install-snoopy.sh; done
```

O Snoopy será instalado em todas as VMs da DMZ. Logue em uma VM, faça `sudo` e execute alguns comandos. Verifique o arquivo `/var/log/auth.log` para verificar a funcionalidade do pacote.

4) Correlacionamento de eventos com o Graylog

Desligue a VM `log`, ajuste sua memória para 4 GB e em seguida religue-a. Acesse como `root@log` e instale as dependências do Graylog.

```
# apt-get update
# apt-get install apt-transport-https openjdk-8-jre-headless uuid-runtime pwgen
dirmngr
```

Instale o MongoDB.

```
# apt-key adv --keyserver hkp://keyserver.ubuntu.com:80 --recv
2930ADAE8CAF5059EE73BB4B58712A2291FA4AD5
# echo "deb http://repo.mongodb.org/apt/debian stretch/mongodb-org/3.6 main" >
/etc/apt/sources.list.d/mongodb-org-3.6.list
# apt-get update
# apt-get install -y mongodb-org
```

Inicie o serviço do MongoDB.

```
# systemctl daemon-reload
# systemctl enable mongod.service
# systemctl restart mongod.service
```

Instale o Elasticsearch.

```
# wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | apt-key add -
# echo "deb https://artifacts.elastic.co/packages/5.x/apt stable main" >
/etc/apt/sources.list.d/elastic-5.x.list
# apt-get update
# apt-get install elasticsearch
```

Configure o Elasticsearch, e inicie-o.

```
# sed -i 's/^#\(cluster\.name:\).*/\1 graylog/' /etc/elasticsearch/elasticsearch.yml
# systemctl daemon-reload
# systemctl enable elasticsearch.service
# systemctl restart elasticsearch.service
```

Instale o Graylog.

```
# wget https://packages.graylog2.org/repo/packages/graylog-2.4-repository_latest.deb
# dpkg -i graylog-2.4-repository_latest.deb
# apt-get update
# apt-get install graylog-server
```

Configure as senhas de acesso.

```
# SECRET=$(pwgen -s 96 1) ; sed -i -e 's/password_secret =.*/password_secret =
'$SECRET'/' /etc/graylog/server/server.conf ; unset SECRET
```

```
# PASSWORD=$(echo -n 'rnpesr' | shasum -a 256 | awk '{print $1}') ; sed -i -e
's/root_password_sha2 =.*/root_password_sha2 = '$PASSWORD'/'
/etc/graylog/server/server.conf ; unset PASSWORD
```

Inicie o Graylog.

```
# systemctl daemon-reload
# systemctl enable graylog-server.service
# systemctl start graylog-server.service
```

Instale o nginx para atuar como um proxy reverso.

```
# apt-get install nginx
# rm /etc/nginx/sites-enabled/default
```

Crie o arquivo `/etc/nginx/sites-available/graylog` com o seguinte conteúdo (edite o IP público da máquina `fw` onde apropriado).

```
server
{
  listen      80 default_server;
  listen      [::]:80 default_server ipv6only=on;
  server_name 200.130.46.146;

  location /
    {
        proxy_set_header    Host $http_host;
        proxy_set_header    X-Forwarded-Host $host;
        proxy_set_header    X-Forwarded-Server $host;
        proxy_set_header    X-Forwarded-For $proxy_add_x_forwarded_for;
        proxy_set_header    X-Graylog-Server-URL http://200.130.46.146/api/;
        proxy_pass          http://127.0.0.1:9000;
    }
}
```

```
# ln -s /etc/nginx/sites-available/graylog /etc/nginx/sites-enabled/
# systemctl restart nginx
```

Como `root@fw`:

```
# iptables -t nat -A PREROUTING -i enp0s3 -p tcp --dport 80 -j DNAT --to-destination
10.0.42.4
# iptables-save > /etc/iptables/rules.v4
```

Em sua máquina física, aponte o navegador para http://200.130.46.146 ; logue como `admin:rnpesr`. Ajuste: System > Indices > Edit > Index Shards = 1 > Save. Ajuste: System > Inputs > Syslog UDP ; Selecionar node ; Title = syslog ; Bind = 10.0.42.4 ; Port = 5140 ; Save.

Como `han@client`:

```
$ for server in fw ldap nfs log; do scp ~/scripts/configure-graylog.sh ${server}:~ &&
ssh han@${server} 'echo seg10han | sudo -S bash /home/han/configure-graylog.sh' && ssh
${server} rm ~/configure-graylog.sh; done
```

Na máquina física, visualize a aba Search.

Agora, configure a atenticação. Em System > Authentication > LDAP/Active Directory ; Enable LDAP:

Server configuration: Server Address = ldap://10.0.42.2:389 ; System Username = cn=admin,dc=intnet ; System Password = rnpesr

User mapping: Search Base DN = ou=People,dc=intnet ; User Search Pattern = (&(objectClass=posixAccount)(uid={0})) ; Display Name Attribute = cn

Group mapping: Group Search Base DN = ou=Groups,dc=intnet ; Group Search Pattern = (&(objectClass=posixGroup)(cn=sysadm)) ; Group Name Attribute = cn

Save LDAP Settings. Teste o login como usuários `luke` e `han`.

Baixe o arquivo https://raw.githubusercontent.com/graylog-labs/graylog-contentpack-nginx/master/content_pack.json . Em System > Content Packs > Import Content Pack, aponte o arquivo. Em System > Content Packs > Web Servers > nginx > Apply Content, ative o pack.

Como `root@log`, inserir ao final da seção http no arquivo `/etc/nginx/nginx.conf`:

```
log_format  graylog2_format  '$remote_addr - $remote_user [$time_local] "$request"
$status $body_bytes_sent "$http_referer" "$http_user_agent" "$http_x_forwarded_for"
<msec=$msec|connection=$connection|connection_requests=$connection_requests|cache_stat
us=$upstream_cache_status|cache_control=$upstream_http_cache_control|expires=$upstream
_http_expires|millis=$request_time>';

access_log syslog:server=10.0.42.4:12301 graylog2_format;
error_log syslog:server=10.0.42.4:12302;
```

```
# systemctl restart nginx
```

No navegador, acesse System > Inputs > nginx access_log > Show received messages.

Para mais informações, acesse https://devopsideas.com/centralized-logging-using-graylog/ .