Tratamento de Incidentes de Segurança

Módulo 2: Análise de Logs

Italo Valcy
Gildásio Júnior

Supported by

Tópicos

- O que é log
- Motivação
- Protocolos
- Formatos
- Boas práticas
- Ferramentas para análise de logs

O que é

- Um log é um registro dos eventos que ocorrem nos sistemas ou na rede de uma organização (SOUPPAYA; KENT, 2006)
  - Sistemas operacionais, aplicações web, tráfego de rede…

Motivação

- *Logs* são importantes quando um incidente de segurança ocorre
- Marcos legais e regulatórios
  - Marco Civil da Internet
  - Normas complementares

Marco Civil da Internet

- Provedores de acesso devem guardar logs por 1 ano
  - Não é permitido terceirização na guarda de logs
  - Não é permitido guardar logs de acesso a aplicações
- Provedores de aplicação devem guardar logs por 6 meses
- Disponibilização de logs deve ser precedida de autorização judicial
- Data, hora, duração, IP de origem, identificação do host

NC 21 / IN 01 / DSIC

- Aplicável para entidades da APF
- Campos: IP, porta, identificação inequívoca do usuário, data/hora e duração, função requisitada
- Dados devem ser armazenados por 01 ano

Registro de Eventos do Sistema

- Logs armazenam uma série de eventos dos sistemas
  - Ex: erros, alertas, violações etc
- Logs são importantes para procedimentos de manutenção preventiva, corretiva e **investigação de incidentes**
- Segurança de redes
  - Alertar atividades suspeitas
  - **Determinar a extensão das atividades de um intruso**
  - **Investigar *modus operandi* de uma invasão**

Registro de Eventos do Sistema

- Configuração padrão: armazenamento em arquivos texto no próprio sistema operacional
  - Problema: Vulnerável à alterações ou remoção em caso de o sistema estar comprometido
  - Solução: **servidor de logs remoto centralizado** armazenando de forma segura os registros de logs

Servidor de Logs Centralizado

- Facilita gerenciamento e monitoramento dos logs
  - Ex: Instalação de ferramentas para análise e geração de relatórios
- Centraliza a demanda de recursos computacionais

Servidor de Logs Centralizado

BELLA
Building the Europe Link to Latin America

- Funcionamento
  - Protocolo Syslog (RFC 5424)
  - TCP ou UDP (porta padrão 514)
    - Mensagens trafegam em texto claro, sem criptografia
- Ferramentas utilizadas
  - Servidor de logs: **syslog-ng**
  - Rotacionamento dos logs: **logrotate**
  - Análise dos logs: **swatch, logcheck, lowatch, OSSEC etc.**

Syslog-ng: Syslog New Generation

BELLA
Building the Europe Link to Latin America

- Atuação como cliente ou servidor
- Disponível para diversos sistemas: Linux, BSD …
- Permite filtragem por *facility*, *level*, *data*, *origem*, *regex* etc.

Syslog-ng: Syslog New Generation

- ***Facility***: tag existente em cada mensagem do syslog para identificar qual parte do sistema gerou o evento
  - Ex: auth, cron, daemon, ftp, kern, mail, syslog, user, local0..local7 etc.

Facility	Descrição
auth e authpriv	Mensagens de segurança / autenticação
cron	Mensagens do agendador de tarefas
daemon	Mensagens de daemons do sistema
kern	Mensagens do kernel
mail	Mensagens do sistema de e-mails
syslog	Mensagens do processo syslog em geral
local0 .. local7	Mensagens de aplicações de usuário

Syslog-ng: Syslog New Generation

- ***Level*** (ou **Priority**): indica quão crítica é a mensagem de log enviada ao sistema
  - Severidades: emerg, alert, crit, err, warning, notice, info, debug, none

Level / Priority	Descrição
emergency	Mensagem de emergência por erro no sistema
alert	Ação imediata é necessária
critical	Funcionalidade do sistema está afetada
error	Uma condição de erro existe, podendo afetar o sistema
warning	Funcionalidade pode ser afetada
notice	Informação sobre eventos normais
info	Informações gerais sobre o sistema
debug	Utilizado para resolução de problemas apenas

Syslog-ng: Instalação e Configuração

- Instalação em sistemas Debian:

```
$ sudo apt install  -y syslog-ng
```

- Configuração
  - /etc/syslog-ng/syslog-ng.conf
- Reiniciar o daemon

```
$ sudo systemctl restart syslog-ng
```

Syslog-ng: Opções Gerais

- Options {}
  - **time_reopen(60)**: tempo para reconectar com o cliente em caso de erro
  - **use_fqdn(no)**
  - **keep_hostname(yes)**
  - **sync(0)**: quantidade de mensagens na memória antes de salvar no disco
  - **create_dirs(yes)**
  - **owner(root), group(wheel), perm(0600)**
  - **dir_owner(root), dir_group(wheel), dir_perm(0700)**
  - **...**

Syslog-ng: Fontes de Origem

- **source {}** - onde receber as mensagens

```
source s_udp { udp(port(514)); };

source s_tcp { tcp(port(514)); };

source s_servidores { udp(ip(192.168.0.1); port(10514)); };

source s_local {
   internal();
   unix-stream("/dev/log");
   file("/proc/kmsg" log_prefix("kernel: "));
};
```

Syslog-ng: Destino de Logs

- **destination {}** - onde enviar/salvar os logs

```
# Salva em arquivo
destination d_servidores_syslog {
   File(
      "/var/syslog-ng/servidores/${HOST}/${FACILITY}.log"
      perm(0640)
      create_dirs(yes)
   );
};

# Envia para outro servidor
destination d_server {
   tcp("192.168.0.1" port(10514));
};
```

Syslog-ng: Filtros

- **filter {}** - permite a criação de filtros para organizar os logs

```
filter f_cron { facility(cron); };
filter f_auth { facility(auth, authpriv); };
filter f_kernel { facility(kern); };
filter f_mail {
   facility(mail) and level(info..warn);
};
filter f_mail_err {
   facility(mail) and level(err..emerg);
};
filter f_others {
   not facility(mail, auth, authpriv, cron, kern);
};
```

Syslog-ng: Configuração

- **log {}** - responsável por armazenar os logs, ligando origem-destino-filtro

```
log {
   source(s_servidores);
   filter(f_auth);
   destination(d_servidores_auth);
};
```

Syslog-ng: Cliente Linux

- Editar arquivo */etc/syslog-ng/syslog-ng.conf*

```
destination d_net { udp("192.168.0.1" port(10514)); };

log { source(s_src); destination(d_net); };
```

- Reiniciar o serviço:

```
$ sudo systemctl restart syslog-ng
```

Rsyslog: Cliente Linux

- Editar arquivo */etc/rsyslog.conf*

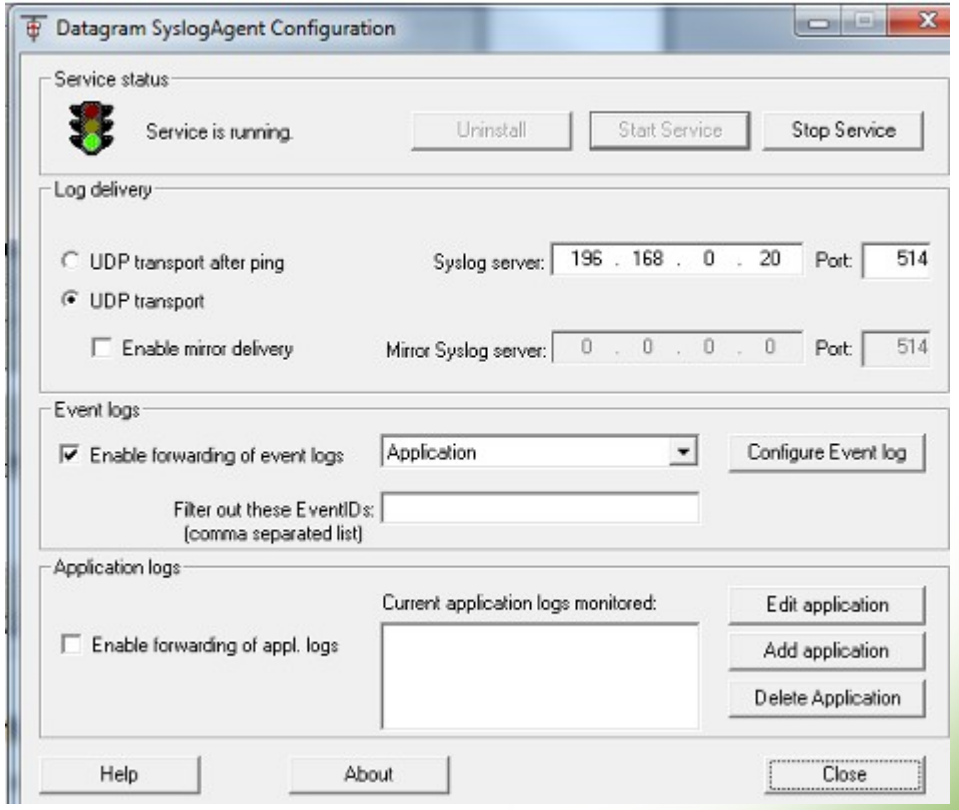
```
*.*                 @192.168.0.2:10514
```

- Reiniciar o serviço:

```
$ sudo systemctl restart rsyslog
```

Cliente Windows

- Windows não suporta syslog nativamente
  - Logs são gerenciados com Windows Event Log
  - Aplicações podem gerar logs em arquivos
- Alternativas
  - Cygwin + Syslog-NG (opensource)
  - Datagram SyslogAgent (freeware)
  - NXLogs Community Edition (opensource)
  - *WinLogD*



Syslog-ng: Cliente Cisco

- Configuração em roteadores Cisco (IOS):

```
config term
logging facility syslog
logging source-interface FastEthernet0/1
logging 192.168.0.2
ip ssh logging events
logging userinfo
```

Syslog-ng: Cliente Juniper

- Configuração em roteadores Juniper:

```
system {
   syslog {
      host 192.168.0.2 {
         any notice;
         authorization info;
         daemon info;
         kernel info;
         interactive-commands info;
      }
   }
}
```

Syslog-ng: Cliente Extreme

- Configuração em roteadores Extreme:

```
enable cli-config-logging
configure syslog add 192.168.0.2:514 vr VR-Default local0
```

Rotacionamento de Logs

- Rotacionamento de logs => compactar arquivos
- Ferramenta mais utilizada: **logrotate**
- Exemplo

```
/var/log/srv01/*.log {
    rotate 156
    weekly
    compress
    olddir /var/log/srv01/old
}
/var/log/dbserver/*.log {
    rotate 156
    weekly
    compress
    olddir /var/log/dbserver/old
}
```

Alertas / Relatórios

- Após configurar o serviço de logging centralizado é necessário estabelecer rotinas de análise dos logs
  - Busca de padrões específicos
  - Busca de padrões não previamente conhecidos
  - Relatórios/estatísticas de uso e comportamento
- Ferramental
  - Exemplos: logwatch, logcheck, OSSEC etc
  - Desenvolvimento de scripts especializados

Logwatch

- Analisador de logs escrito em perl que envia relatórios diários com estatísticas do sistema:
  - Serviço de e-mail
  - Serviço de autenticação
  - Antivírus
  - Serviço LDAP
  - Sistema operacional (disco, login, processos)

Logwatch

```
-------------------- pam_unix Begin -----------------------
cron:
    Sessions Opened:
        root: 2240 Time(s)
sshd:
    Sessions Opened:
        payal: 545 Time(s)
        payal by payal: 8 Time(s)
su:
    Sessions Opened:
        root → nobody: 3 Time(s)
--------------------- pam_unix End ------------------------
...
--------------------- SSHD Begin --------------------------
Users logging in through sshd:
    payal:
        192.168.0.5 (laptop.nizcraft.in): 460 times
        192.168.0.7 (desktop.nixcraft.in): 93 times
---------------------- SSHD End ---------------------------
```

Snoopy

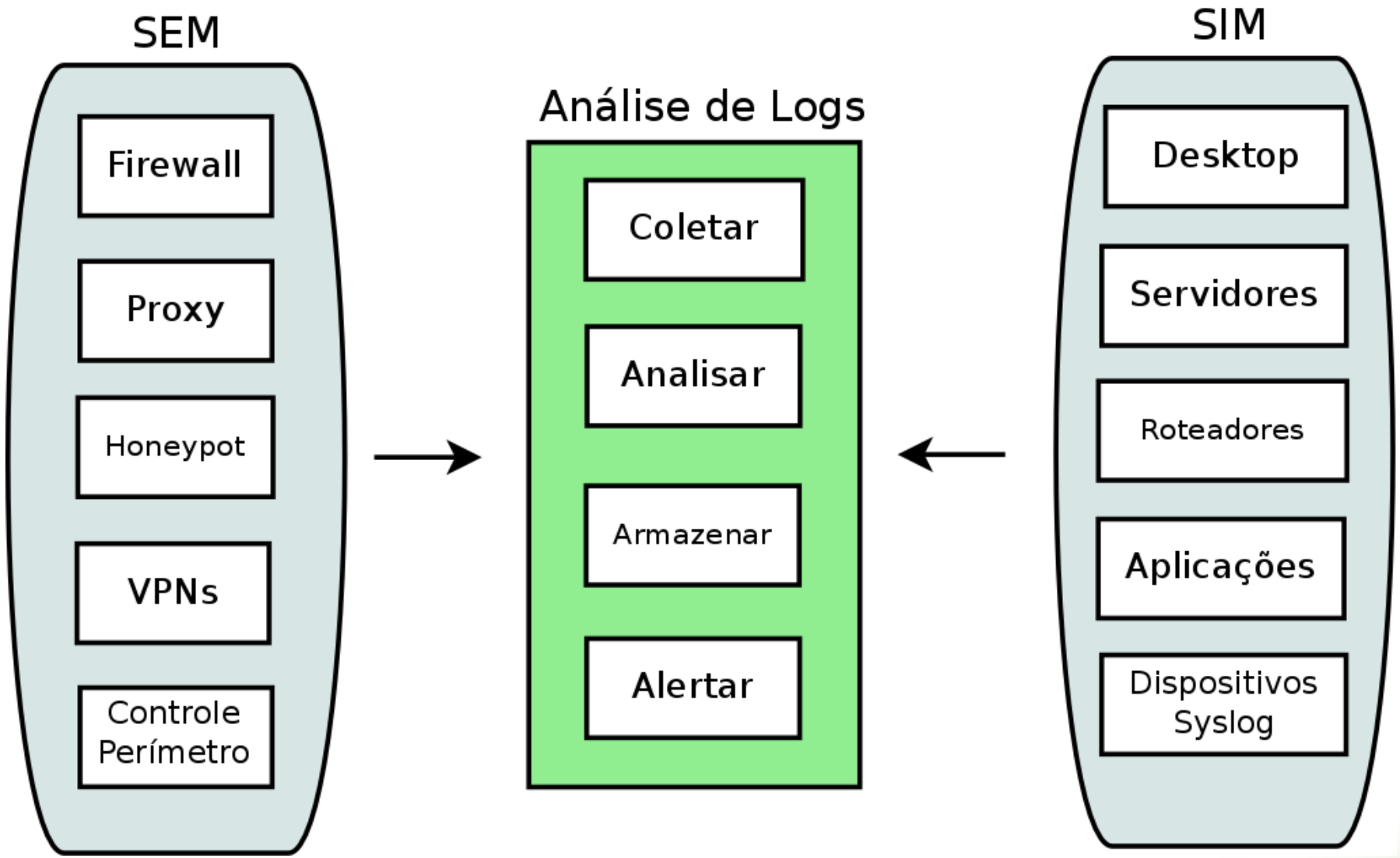
- Logging dos comandos executados no sistema
  - Incluindo argumentos
- Log em */var/log/auth.log*

```
$ sudo apt install -y snoopy
```

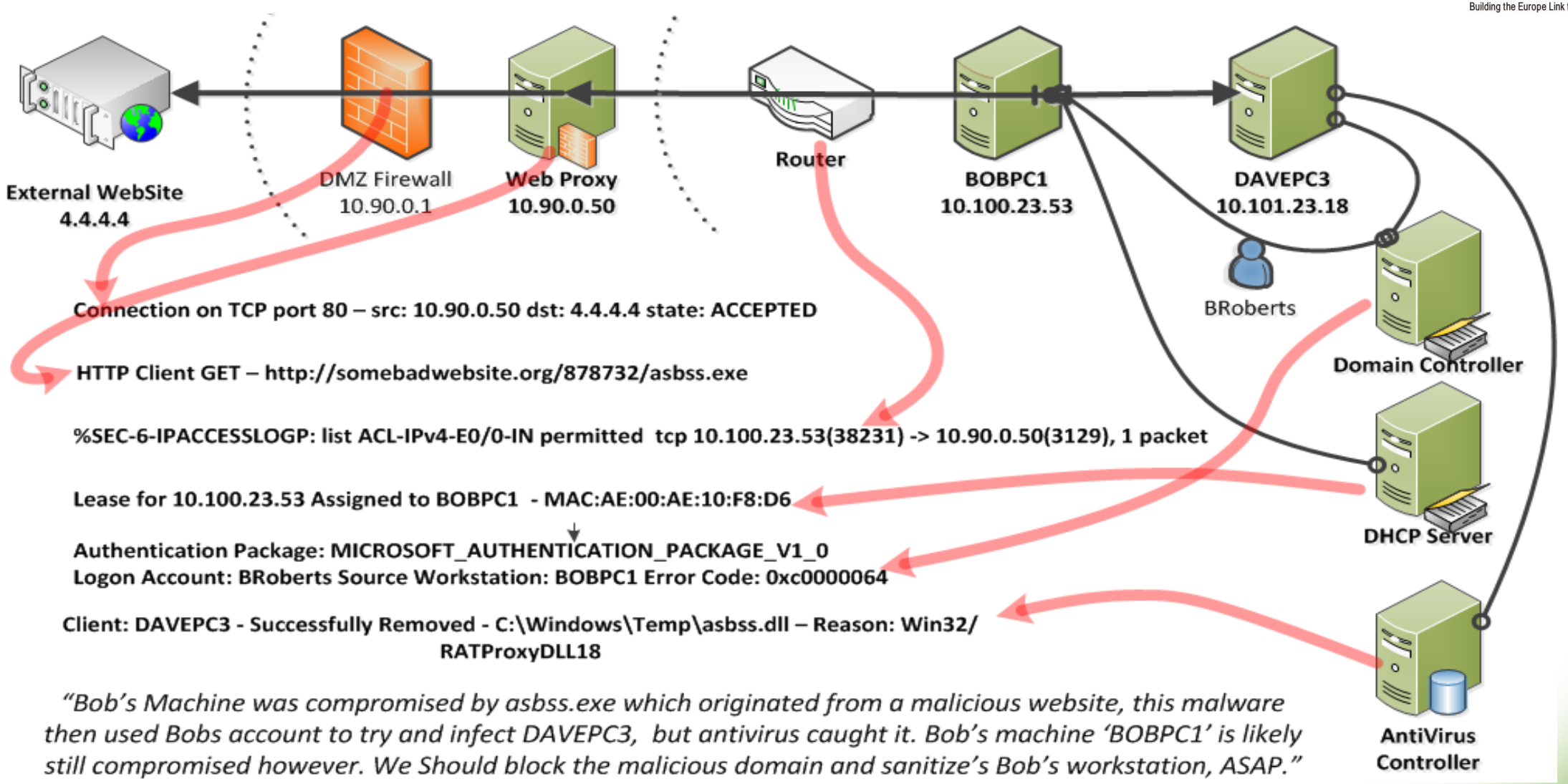
SIEM

- SIM – Security Information Management
  - Análise histórica e geração de relatórios
  - Indexação de dados e busca flexível
  - Armazenamento, análise e correlação de eventos
- SEM – Security Event Management
  - Monitoramento e correlação de eventos em tempo real
  - Coletar, analisar, visualizar eventos de segurança
  - Monitoramento dinâmico, adaptativo, automatizado

SIEM


SEM
Firewall
Proxy
Honeypot
VPNs
Controle Perímetro
Análise de Logs
Coletar
Analisar
Armazenar
Alertar
SIM
Desktop
Servidores
Roteadores
Aplicações
Dispositivos Syslog

SIEM



"Bob's Machine was compromised by asbss.exe which originated from a malicious website, this malware then used Bobs account to try and infect DAVEPC3, but antivirus caught it. Bob's machine 'BOBPC1' is likely still compromised however. We Should block the malicious domain and sanitize's Bob's workstation, ASAP."

SIEM: Benefícios

- Grande volume de logs para analisar
- Soluções heterogêneas
- Ameaças avançadas
- Falsos positivos
- Retenção de informações a longo prazo

OSSIM – Open Source SIEM

- SIEM open source – GPLv3
- Monitoramento de ativos de rede
- Centralização de informações e gerenciamento
- Levantamento de vulnerabilidades e riscos
- Provê capacidade de detecção de ameaças
- Aprendizado colaborativo de APT
- OTX (Open Threat Exchange)

http://communities.alienvault.com

Ferramentas Integradas ao OSSIM

BELLA
Building the Europe Link to Latin America

Mapeamento
- nmap
- prads

Detecção de Ameaças
- ossec
- snort
- suricata

Monitoramento
- fprobe
- nfdump
- ntop
- tcpdump
- nagios

Levantamento de Vulnerabilidades
- osvdb
- openvas

Erros Comuns

BELLA
Building the Europe Link to Latin America

- Ausência de logs
- Não analisar logs
- Não coletar todas as informações (ex: porta de origem, URL, etc)
- Armazenar informações por curto período
- Ignorar logs de aplicações
- Buscar apenas por padrões maliciosos conhecidos

Boas Práticas

- Faça log de todos recursos da instituição (ex: servidor web, banco de dados, roteadores...)
- Faça log remotamente enviando para um servidor cetralizador **imediatamente**
- Rotacione e faça backup dos logs
- Utilize poucos arquivos de logs
- Evite complexidade
- Configure corretamente o horário das máquinas

BELLA
Building the Europe Link to Latin America

Prática

Configuração do Syslog-NG

- Configurar o servidor de logs
  - Instalar servidor de logs
  - Configurar para receber logs na porta 10514/tcp
  - Separar mensagens de autenticação das demais
  - Salvar arquivos em /*var/syslog-ng/servidores/nome-do-servidor/{auth.log,syslog}*
  - Configurar rotacionamento dos arquivos de log conforme Marco Civil
  - Configurar host para enviar logs ao servidor
    - Usar envio criptografado? Com stunnel?

Análise de Logs

- Analisar o log de NAT e criar scripts/comandos para fazer a análise mais performática das entradas de log,p bem como responder a questões como: recomendações para ações de erradicação, conteção e recuperação do incidente

Referências

- Guide to Computer Security Log Management – NIST
- Implementando uma Infraestrutura de Rede Segura – 20º SCI
- SIEM For Beginners
- OSSEC & OSSIM Unified Open Source Security
- Scarfone and Souppaya, 2006. Guide to Computer Security Log Management. NIST