3
Ataques e Intrusões

Para se avaliar a eficácia e precisão de um sistema de detecção de intrusões é necessário testá-lo contra uma ampla amostra de ataques e intrusões reais. Parte integrante do projeto MIT/DARPA 1998 foi selecionar técnicas e procedimentos de intrusão e ataques contra sistemas computacionais empregados em redes reais e que consistiam uma ameaça a segurança destas redes. A base de dados gerada como resultado deste projeto inclui 38 diferentes padrões de ataques e intrusões. Todos os 38 ataques são reais e possuem código fonte ou versão binária de software que o realiza disponível publicamente em sítios Internet como [19] [20] [21].

3.1.
Taxonomia para Ataques e Intrusões

Taxonomia para ataques e intrusões em sistemas computacionais proposta originalmente em [22] foi utilizada para selecionar os ataques e padrões de intrusão inseridos nos dados utilizados para treinamento e testes do sistema proposto. Uma boa taxonomia permite agrupar ataques e intrusões em grupos que possuem características distintas. As principais características da taxonomia usada são:

- Cada ataque pode ser enquadrado em um único grupo.
- Todos os possíveis ataques e intrusões podem ser classificados pela taxonomia definida.
- A taxonomia pode ser extendida no futuro.

3.1.1.
Níveis de Privilegio

A taxonomia proposta define a seguinte classificação de privilégios que o usuário de um sistema computacional em rede pode possuir:

Identificador	Privilegio
R	Acesso **R**emoto via rede.
L	Acesso **L**ocal a rede
U	Acesso como **U**suário normal.
S	Acesso como **S**uperusuário (root ou administrador)
P	Acesso físico (**P**hysical) ao sistema.

Tabela 3-1 : Privilêgios

Possuir privilégio de acesso remoto via rede (**R**) significa obter algum tipo de acesso através de rede de sistemas interconectados ao computador alvo. Acesso local a rede (**L**) permite ao usuário ler e "escrever" no segmento de rede em que o sistema alvo esta conectado. Acesso com usuário normal (**U**) envolve a capacidade de executar comandos de usuário na máquina alvo, assim como o privilégio acesso como superusuário (**S**) significa ter a capacidade de executar comandos privilegiados (de administração) na vítima. Finalmente o privilégio acesso físico corresponde a capacidade de acessar fisicamente o hardware e componentes do computador em referencia.

3.1.2.
Métodos de Transição e Exploração

Um atacante / intruso irá invariavelmente explorar alguma falha ou brecha existente nos sistemas computacionais para conseguir acesso indevido ou comprometer aspectos da integridade, disponibilidade e confidencialidade das informações. O projeto DARPA/MIT 1998 considerou os seguintes métodos de ataque/intrusão :

Id.	Método	Descrição
M	*Masquerading*	Esconder ou utilizar identificação falsa para obter acesso não autorizado ou indevido a um sistema. Exemplo comum seria alteração do endereço IP de origem em ataques *spoofing.*
A	Abuso de funcionalidade	Ações legítimas podem, em casos extremos, comprometer a operação de sistemas. Estabelecimento de milhares de conexões Telnet com um servidor Unix pode causar situação de falha devido a uso excessivo de tabela de processos ativos.
B	*Bug* de implementação	Erros de programação e falhas sistêmicas podem ser exploradas por usuários mal intencionados. Falhas como *buffer overflow* (estouro de área de memória) que permitem acesso não autorizado são exemplos.
C	Configuração indevida de sistema	Configuração inapropriada de determinado sistema pode ser utilizada em ataques. Sistemas de gerenciamento de banco de dados costumam, ao ser instalados, manter a senha de usuário administrador em branco.
S	Engenharia social	Técnicas que envolvem enganar os usuários (reais, os seres humanos) do sistema para obter algum benefício.

Tabela 3-2 : Métodos de Transição e Ataque

É importante ressaltar que várias técnicas de intrusão e ataque podem utilizar mais de um dos métodos de transição e exploração aqui apresentados.

3.1.3. Transição entre níveis de privilégio

Com as definições dos níveis de privilégio e métodos de transição e exploração destes, é possível descrever de forma sucinta, através dos identificadores, diversas situações que ocorrem nas diversas técnicas de ataque estudadas. Por exemplo, o ataque ftp-write ocorre quando um intruso obtém, via rede, acesso como usuário local em um servidor de FTP configurado indevidamente. De acordo com as definições apresentadas podemos descrever este ataque como : **R-c-U** ou seja, usuário com privilégio **R** – acesso remoto via rede – obtem novo privilegio **U** – acesso como usuário normal – através do mecanismos de transição **c** – configuração indevida de sistema.

3.1.4. Ações

As ações que podem ocorrer um uma determinada técnica de ataque são descritas na taxonomia por palavras chaves predefinidas seguidas de variáveis que especificam com mais detalhes a ação.

Categoria	Tipo específico	Descrição
Probe (reconhecimento)	*Probe(Machines)*	Determina quantidade, tipo de máquinas ativas na rede.
	Probe(Services)	Determina serviços ativos em determinado computador/sistema.
	Probe(Users)	Determina contas de usuários existentes e outras características referentes a usuários.
Deny (Negação)	*Deny(Temporary)*	Negação de serviço temporário com recuperação automática após ataque.
	Deny(Administrative)	Negação de serviço com recuperação dependente de ação de administrador.
	Deny(Permanent)	Negação de serviço tornando o serviço/computador alvo indisponível.
Intercept (Interceptação)	*Intercept(Files)*	Intercepta arquivos.
	Intercept(Network)	Intercepta pacotes trafegando em segmento de rede.
	Intercept(Keystrokes)	Intercepta teclas digitadas por usuário.
Alter (Alteração)	*Alter(Data)*	Altera dados armazenados na vítima.
	Alter(Intrusion-Traces)	Altera evidências que intrusão ocorreu.
Use	*Use(Recreational)*	Uso do sistema comprometido para fins pessoais.
	Use(Intrusion related)	Uso do sistema comprometido para novos ataques/intrusões.

Tabela 3-3 : Ações

3.1.5.
Uso da taxonomia para descrever ataques

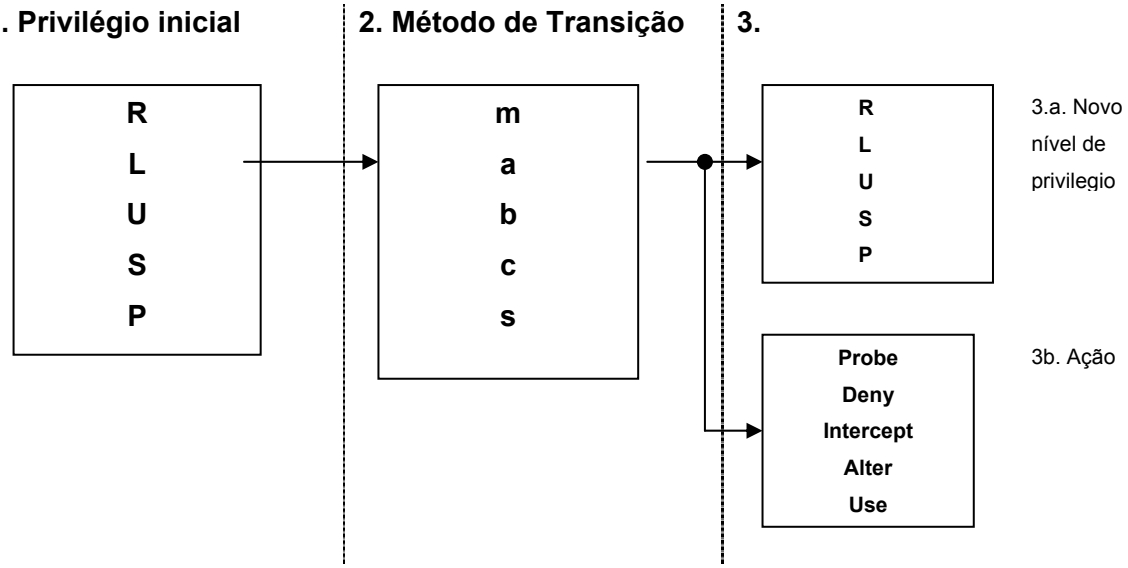

Figura 3-1 : Descrevendo ataques com a Taxonomia

3.2.
Categorias de Ataques / Intrusões

A taxonomia propõe a classificação das técnicas de ataques e intrusões em quatro categorias distintas : negação de serviço (*denial of service*), remoto para usuário, usuário para super usuário, reconhecimento (*probing*). A tabela 3.4 mostra a classificação das técnicas de ataque e intrusão selecionadas para esta avaliação nas categorias.

	Solaris	SunOS	Linux
Negação de Serviço (Denial Of Service) (R-Deny)	Apache2 Back Mailbomb Neptune Ping Of Death Process Table Smurf Syslogd UDP Storm	Apache2 Back Land Mailbomb Neptune Ping of death Process Table Smurf UDP Storm	Apache2 back Mailbomb Neptune Ping of death Process Table Smurf Teardrop UDP Storm
Remoto para Usuário (Remote to User)	dictionary ftp-write guest phf xlock xsnoop	dictionary ftp-write guest phf xlock xsnoop	dictionary ftp-write guest imap named phf sendmail xlock xsnoop
Usuário para Superusuário (User to Super-user)	eject ffbconfig fdformat ps	loadmodule ps	perl xterm
Reconhecimento (Probing / Surveillance)	ip sweep mscan nmap saint satan	ip sweep mscan nmap saint satan	ip sweep mscan nmap saint satan

Tabela 3-4 : Categorias de Padrões de Ataque

3.2.1. Negação de Serviço (DOS ou *Denial of Service*)

Negação de serviço é uma classe de ataques contra a disponibilidade de sistemas computacionais. O objetivo do atacante é causar a indisponibilidade do serviço alvo, seja através do consumo excessivo de recursos computacionais como memória, processador ou rede para atendimento a solicitações falsas ou seja através de indisponibilidade total do serviço por exploração de uma falha grave existente no mesmo. O primeiro ataque de negação de serviço em larga escala ocorrido na Internet foi causado pelo *Morris Worm* em novembro de 1989 [4] [5]. Este software malicioso que explorava vulnerabilidades em sistemas Unix atacava a disponibilidade dos sistemas computacionais de duas formas distintas:

- Máquinas infectadas pelo *Morris Worm* se tornavam inúteis pois toda sua capacidade de processamento era seqüestrada.

- Diversas organizações, universidades conectadas a Internet simplesmente eliminaram sua presença na Internet para evitar a contaminação, até que o problema fosse solucionado.

Episódios mais recentes demonstraram que a evolução de medidas de segurança da informação não conseguiu eliminar esta ameaça. Em fevereiro de 2000, uma seqüência de ataques de negação de serviço [23] causou total indisponibilidade de serviços de empresas com alta visibilidade na Internet como Yahoo, e-Bay, Amazon.com dentre outras. Este episódio marcou o surgimento, em situações práticas, dos chamados ataques de negação de serviço distribuído (*DDOS – Distributed Denial of Service*). Variação dos ataques de negação de serviço envolvendo um número enorme de computadores e sistemas controlados remotamente pelo intruso e utilizados como robôs para atacar determinado alvo. Muitas destas empresas afetadas dependem parcialmente ou exclusivamente da Internet para gerar receitas.

Os ataques de negação de serviço presentes na base de dados de referência MIT/DARPA estão apresentados na tabela 4.

Nome	Serviço	Plataforma vulnerável	Mecanismo	Efeito
Apache2	http	Apache	Abuso de funcionalidade	Interrupção do serviço http
Back	http	Apache	Abuso / Bug no sistema	Queda no tempo de resposta.
Land	N/A	SunOS	Bug no sistema	Sistema operacional indisponível
MailBomb	Smtp	Todas	Abuso de funcionalidade	Consumo de recurso.
SynFlood	TCP	Todas	Abuso de funcionalidade	Negação de serviço.
Ping of Death	Icmp	Todas	Bug no sistema	Indisponibilidade
Process Table	TCP	Todas	Abuso de funcionalidade.	Impede execução de novos processos.
Smurf	Icmp	Todas	Abuso de funcionalidade	Queda no desempenho da rede
SyslogD	Syslog	Solaris	Bug no sistema	Queda do serviço Syslog.
TearDrop	N/A	Linux	Bug no sistema.	Reinicializa computador vítima.
UDPStorm	Echo / chargen	Todas	Abuso de funcionalidade.	Queda no desempenho da rede.

Tabela 3-5 : Negação de Serviço

3.2.2. Usuário para Superusuário (*User to Root*)

Esta categoria de ataques e intrusões engloba todos os ataques em que o intruso possui acesso ao sistema como um usuário normal e consegue elevar seu nível de privilégio para o de um usuário especial (como o usuário *root* em sistemas Unix ou administrador em outras plataformas). Existem diversos tipos de ataques nesta classe sendo o mais comum os ataques que empregam técnicas de estouro de *buffer* ou *buffer overflow.*

Nome	Serviço	Plataformas vulneráveis	Mecanismo	Efeito
Eject	Qualquer sessão de usuário	Solaris	*Buffer overflow*	Shell com privilégios de administrador
Ffbconfig	Qualquer sessão de usuário	Solaris	*Buffer overflow*	Shell com privilégios de administrador
Fdfomat	Qualquer sessão de usuário	Solaris	*Buffer overflow*	Shell com privilégios de administrador
Loadmodule	Qualquer sessão de usuário	SunOS	Bug	Shell com privilégios de administrador
Perl	Qualquer sessão de usuário	Linux	Bug	Shell com privilégios de administrador
PS	Qualquer sessão de usuário	Solaris	Bug	Shell com privilégios de administrador
Xterm	Qualquer sessão de usuário	Linux	*Buffer overflow*	Shell com privilégios de administrador

Tabela 3-6 : User-to-Root

3.2.3. Remoto para usuário (*Remote to User*)

Ataques da classe “remoto para usuário” correspondem a situações em que o intruso possui conectividade com a máquina vítima – sem, entretanto, possuir uma conta de usuário – e explorando alguma vulnerabilidade existente consegue obter acesso local a máquina.

Nome	Serviço	Plataformas vulneráveis	Mecanismo	Efeito
Dictionary	Qualquer serviço que possua autenticação por nome e senha	Todas	Abuso de funcionalidade	Acesso como usuário legitimo
ftp-write	FTP	Todas	Configuração indevida	Acesso como usuário legitimo
Guest	Telnet, Rlogin	Todas	Configuração indevida	Acesso como usuário legitimo
Imap	IMAP4	Linux	Bug	Shell com privilégios de administrador
Named	DNS	Linux	Bug	Shell com privilégios de administrador
Phf	http	Todas	Bug	Execução de comandos como usuário http
Sendmail	SMTP	Linux	Bug	Execução de comandos como *root*
Xlock	X	Todas	Configuração indevida	Obtém senha através de falsificação da identidade
Xsnoop	X	Todas	Configuração indevida	Capacidade de monitorar teclas digitadas remotamente

Tabela 3-7 : Remote-to-User

3.2.4. Reconhecimento (*Probing*)

Técnicas de ataque e intrusão da categoria reconhecimento são normalmente empregadas, usualmente, em uma etapa que antecede o ataque ou intrusão. Nesta categoria estão ferramentas e mecanismos automatizados que permitem ao invasor encontrar novas vítimas e conhecer melhor sua vítima. Através das técnicas desta categoria o invasor pode descobrir, por exemplo, quais sistemas estão ativos em determinado momento, quais serviços estão ativos em determinado computador, o fabricante e versão do software que

fornece cada um destes serviços dentre outras informações. Após este levantamento, resta apenas selecionar quais técnicas de ataque e intrusão terão sucesso para aquele perfil levantado do alvo.

Do ponto de vista dos sistemas de detecção de intrusão, detectar atividade relacionada a esta categoria é importante uma vez que permite uma preparação e resposta adequada a próxima etapa que provavelmente será iniciada pelo intruso.

Nome	Serviço	Plataformas vulneráveis	Mecanismo	Efeito
Ipsweep	Icmp	Todas	Abuso de funcionalidade	Encontra computadores ativos
Mscan	Vários	Todas	Abuso de funcionalidade	Descobre vulnerabilidades conhecidas
Nmap	Vários	Todas	Abuso de funcionalidade	Encontra serviços (portas tcp e udp) ativas
Saint	Vários	Todas	Abuso de funcionalidade	Descobre vulnerabilidades conhecidas
Satan	Vários	Todas	Abuso de funcionalidade	Descobre vulnerabilidades conhecidas

Tabela 3-8 : Reconhecimento