Parte III

Avaliando Ameaças
e
Anatomia de um Ataque

Objetivos

- Porque é necessário segurança.
- Desafios
- Conheça seus invasores.

Porque precisamos de segurança da rede

- Os negócios enfrentam um problema de segurança assustador: como implementar e atualizar constantemente as defesas e práticas para reduzir a vulnerabilidade dos negócios às ameaças inovadoras dos invasores?

Desafios de Segurança

- Segurança é difícil de ser implementada uniformemente em toda a empresa.

Desafios de Segurança

- Escolha de uma alternativa ou combinação adequada de diversas opções de soluções.

- Escolher entre várias opções diferentes e disponíveis e adotar aquelas que satisfaçam os requisitos exclusivos da rede e dos negócios.

Desafios de Segurança

- Os produtos diferentes devem ser integrados em toda a empresa a fim de se atingir uma única política de segurança estável.

Porque temos problemas de segurança

- Fragilidade da Tecnologia
- Fragilidade de Configuração
- Fragilidade da Política

Fragilidade da Tecnologia

- TCP/IP
- Sistema Operacional
- Equipamento de Rede

Vulnerabilidades TCP/IP

- Observação e Manipulação de Pacotes
- Limitação do NFS
- Acesso por Telnet
- Acesso Raiz através de Serviço *SendMail*

Fragilidade do Equipamento de Rede Vulnerabilidades

- Proteção de senha insegura
- Falhas de autenticação
- Protocolos de Roteamento
- Brechas no Firewall

Fragilidade de Configuração

- São problemas causados pelo fato de não se configurar equipamentos interligados para impedir problemas de segurança conhecidos ou prováveis.

Fragilidade de Configuração

- Considerações *default* inseguras nos produtos.
- Equipamento de rede configurado equivocadamente.
- Contas de usuários inseguras.
- Contas de sistemas com senhas previsíveis.

Fragilidades da Política de Segurança

- Falta de uma política escrita.
- Políticas internas
- Falta de continuidade dos negócios
- Controles de acesso para equipamentos de rede não são aplicados.
- A administração de segurança é negligente, inclusive a monitoração e a auditoria.

Fragilidades da Política de Segurança

- Falta de conhecimento sobre ataques.
- Alterações e instalação de software e hardware não seguem a política.
- Falta de Planejamento de Contingência.

Conheça seus Invasores

- **Script Kiddie**

  Não possuem muita habilidade.

  Mas teve a sorte de encontrar um sistema remoto que não aplicou o *patch* de correção a tempo.

Conheça seus Invasores

- **Script Kiddie**

- Sãos bons na razão inversamente proporcional à negligência de administradores/usuários que não acompanham listas de segurança e demais páginas de fornecedores ou CERT (Computer Emergency Response Team)

Conheça seus Invasores

- **Script Kiddie**

  Um invasor que faz intrusão vinculada a uma falha conhecida.

  Não buscam informações e/ou máquinas específicas. Ou seja, ganhar acesso de root.

  Basta ter acesso para desconfigurar home pages de forma mais fácil possível.

Conheça seus Invasores

- **Script Kiddie**

  Sua técnica consiste em ficar revirando a Internet atrás de máquinas vulneráveis e fazer explorações com *exploits*, ferramentas que permitam explorar as falhas em serviços.

Conheça seus Invasores

- **Script Kiddie**

Podem desenvolver suas próprias ferramentas.

Existem os que não conhecem nenhuma técnica, e tudo o que sabem é executar as ferramentas fornecidas por outro script kiddie.

Conheça seus Invasores

- **Cracker**

  Um invasor de bons conhecimentos técnicos e assim sendo, ele será capaz de apagar seus rastros de maneira mais sutil.

  Se caracteriza pelo alto nível técnico, na medida em que cada passo da invasão é realmente estudado e bem pensado.

Conheça seus Invasores

- **Cracker**

  Busca dados como configurações padrões ou senhas padrões que ele possa explorar.

  Tem capacidade para desenvolve seus próprios *exploits*. São geniais e criativos para a má intenção.

  Realiza ataques inteligentes para comprometer a segurança da rede.

Conheça seus Invasores

- **Cracker**

  Suas atitudes furtivas poderão enganar até aos mais experientes administradores.

  São os verdadeiros invasores (intrusos) ou até mesmo criminosos cibernéticos.

Conheça seus Invasores

- **Hacker**

  Um programador apaixonado.

  Constroem e tornam o mundo melhor.

  Exemplos: Stallman, Linus Torvalds, Ada Lovelace, Douglas Engelbart, Dennis Ritchie, Ken Thompson, Arnaldo Melo, Marcelo Tossati, Alan Cox, ...

  Não são fúteis desconfiguradores de páginas.

Conheça seus Invasores

- **Hacker** (Hacking ou Hacking Ético)

  Programador ou administrador que se reserva a questionar os problemas de segurança nas tecnologias disponíveis e as formas de provar o conceito do que é discutido.

Conheça seus Invasores

- **Hacker Ético**

  Uma pessoa que investiga a integridade e a segurança de uma rede ou sistema operacional.

  Usa o conhecimento avançado sobre SW e HW para entrar no sistema através de formas inovadoras.

Conheça seus Invasores

- **Hacker Ético**

  Compartilha seu conhecimento gratuitamente através da Internet.

  Não usa de más intenções. Tenta oferecer um serviço à comunidade interessada.

Conceito de Invasor

- Script Kiddie
- Cracker
- Hacker
- Phracker (pessoas que fazem acesso não autorizado a **recursos de telecomunicações**)

Características de um Invasor

- Sabem codificar em várias linguagens de programação.
- Conhecimentos aprofundados sobre ferramentas, serviços e protocolos.
- Grande experiência com Internet.
- Conhecem intimamente pelo menos dois Sos.

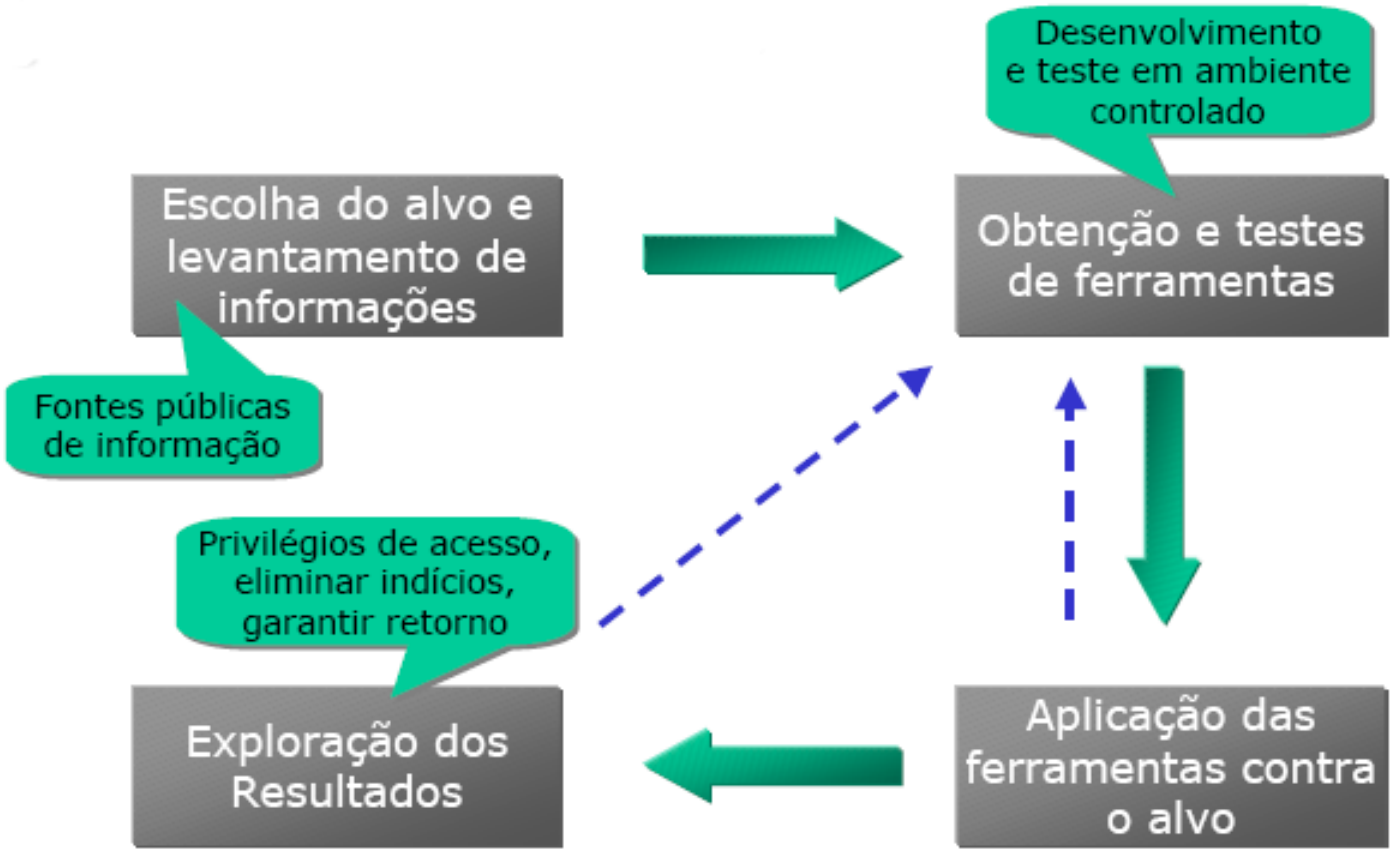
Características de um Invasor

- Tinham ou têm um tipo de trabalhos que usa redes. Usam equipamentos como se fossem modo de vida.
- Colecionam SW e HW.
- Tinham vários computadores para trabalhar.

Motivação

- Exploração de emoções (Notoriedade, Diversão).
- Concorrência de mercado
- Inimigos políticos
- Ladrões (atividades furtivas)
- Espiões (Espionagem industrial)
- Funcionários hostis (Empregados ou antigos empregados: Vingança, Ataque de Troca de Senhas ou Sessões Abertas)
- Investigação legal.

Etapas de um Ataque



Etapas Detalhadas de um Ataque

- Ver material escrito, distribuído em aula.
- **Script Kiddie**
- **Cracker**

Anatomia de Ataques

- O primeiro passo para entender um ataque é entender sua anatomia.
- Um ataque é basicamente definido (com mais detalhes) em três etapas:
  - **Footprint**
  - **Fingerprint**
  - **Enumeração**

O que é Footprint

- **Footprint** – É a organização de idéias como um todo, tentando criar o melhor e mais completo perfil do alvo a ser atacado.

- Ver detalhes no material escrito.

O que é Fingerprint

- **Fingerprint** – Parte do Footprint que tem como objetivo identificar o SO, a máquina alvo, vulnerabilidades em geral e serviços nele disponíveis.

- Ver detalhes no material escrito.

O que é Enumeração

- **Enumeração** – Extração de informações do ambiente-alvo, como recursos compartilhados, mal protegidos, contas de usuários e exploração de serviços.

- Ver detalhes no material escrito.

Ferramentas de Ataque

- Scanners de Portas.
- Scanners de Vulnerabilidades.
- RootKits (Backdoor, Trojans, Logclean e Sniffers)
- Sniffers.

Scanners de Portas

- Pesquisam faixas de endereços IP.
- Descobrem sistemas vulneráveis.
- Portas abertas.
- Informações Sobre o Sistema Operacional do alvo.

Scanners de Portas

- Nmap (http://www.nmap.org)
- Código Aberto.
- Licença GNU GPL.

Nmap

```
# /usr/local/nmap -O ganassi

Starting nmap V. 2.53 (www.insecure.org/nmap/)
Interesting ports on ganassi (10.8.10.231):
(The 1515 ports scanned but not shown below are in state: closed)
Port       State       Service
7/tcp      open        echo
9/tcp      open        discard
13/tcp     open        daytime
19/tcp     open        chargen
21/tcp     open        ftp
23/tcp     open        telnet
25/tcp     open        smtp
37/tcp     open        time
79/tcp     open        finger
111/tcp    open        sunrpc
512/tcp    open        exec
513/tcp    open        login
514/tcp    open        shell
515/tcp    open        printer
```

Scanners de Vulnerabilidades

- Nessus (http://www.nessus.org)
- Auditoria de Sistemas.
- Administração Remota.

Nessus

```
# nessus -T text localhost 1241 noorder targetfile outfile
```

Nessus

```
Nessus Scan Report
------------------

SUMMARY

  - Number of hosts which were alive during the test : 1
  - Number of security holes found : 2
  - Number of security warnings found : 15
  - Number of security notes found : 1

TESTED HOSTS

  192.168.0.90 (Security holes found)
```

Nessus

```
DETAILS

+ 192.168.0.90 :
  . List of open ports :
    o unknown (161/udp) (Security hole found)
    o unknown (32779/udp) (Security warnings found)
    o unknown (32775/tcp) (Security warnings found)
    o unknown (32776/udp) (Security warnings found)
    o unknown (32778/udp) (Security warnings found)
    o unknown (32774/udp) (Security hole found)
    o unknown (32777/udp) (Security warnings found)
    o unknown (32780/udp) (Security warnings found)
    o unknown (32775/udp) (Security warnings found)
    o lockd (4045/udp) (Security warnings found)
    o unknown (32781/udp) (Security hole found)

. Vulnerability found on port unknown (32774/udp) :

    The sadmin RPC service is running.
    There is a bug in Solaris versions of
    this service that allow an intruder to
    execute arbitrary commands on your system.

    Solution : disable this service
    Risk factor : High
```

Rookits

- Backdoor
- Trojans (Cavalos de Tróia)
- Logclean (Eliminadores de Logs)
- Sniffers

Rootkits

- Script de Instalação.
- Alteração dos Arquivos de Comando:
  - /bin/ls
  - /usr/bin/ls
  - /bin/ps
  - /bin/netstat
  - /usr/bin/netstat
  - /usr/sbin/rpcbind

Rootkits

- Após a instalação, se obtém o privilégio de administrador.
- Difícil ao administrador detectar invasões do sistema através de comandos convencionais.
- Comandos convencionais:

  ls, pf, find, netstat,...

Backdoors

- Garante acessos futuros ao sistema invadido no intuito de poupar trabalho.
- Variam daquelas que abrem uma simples porta com acesso shell até sofisticados rootkits capazes de automatizar muitos processos.
- É necessário acesso local de superusuário.

Backdoors

- Trabalha com portas ocultas associadas a serviços para facilitar acesso de forma não convencional com direito de root.

- Podem criar grandes problemas para administradores e responsáveis pela segurança.

Backdoors

- Netcat
- NSSL
- SBD
- Hping2 (montador de pacotes)

Cleanlogs

- Os logs são bem definidos em qualquer OS.
- Apagamento de logs é uma atividade vinculada à intrusão.
- Forjar rastros da invasão.
- Eliminando o rastro do invasor e dificultando a auditoria.

Sniffers

- Obtém informações sobre o tráfego na rede.
- Informações sobre protocolos.
- ID de Usuários.
- Senhas e Emails
- Exemplo: snoop

Sniffer snoop em Telnet

```
# snoop -d qfe0 port telnet ganassi
      ganassi -> nomex-lab    TELNET R port=32835
\377\373\1\377\375\1login:
    nomex-lab -> ganassi      TELNET C port=32835 r
      ganassi -> nomex-lab    TELNET R port=32835 r
    nomex-lab -> ganassi      TELNET C port=32835 o
      ganassi -> nomex-lab    TELNET R port=32835 o
    nomex-lab -> ganassi      TELNET C port=32835
    nomex-lab -> ganassi      TELNET C port=32835 o
      ganassi -> nomex-lab    TELNET R port=32835 o
    nomex-lab -> ganassi      TELNET C port=32835
    nomex-lab -> ganassi      TELNET C port=32835 t
      ganassi -> nomex-lab    TELNET R port=32835 t
    nomex-lab -> ganassi      TELNET C port=32835
      ganassi -> nomex-lab    TELNET R port=32835 Password:
    nomex-lab -> ganassi      TELNET C port=32835
    nomex-lab -> ganassi      TELNET C port=32835 t
      ganassi -> nomex-lab    TELNET R port=32835
    nomex-lab -> ganassi      TELNET C port=32835 0
      ganassi -> nomex-lab    TELNET R port=32835
```

Sniffer snoop em IMAP

```
# snoop -d qfe0 port imap2 ganassi
jordan -> ganassi IMAP C port=46600
ganassi -> jordan IMAP R port=46600
jordan -> ganassi IMAP C port=46600
ganassi -> jordan IMAP R port=46600 * OK ganassi SIMS (tm) 2.0p12
IMAP
jordan -> ganassi IMAP C port=46600
jordan -> ganassi IMAP C port=46600 1 capability\r\n
ganassi -> jordan IMAP R port=46600
ganassi -> jordan IMAP R port=46600 * CAPABILITY IMAP4 STATUS SCAN
IMAP4
jordan -> ganassi IMAP C port=46600
jordan -> ganassi IMAP C port=46600 2 login "hacked" "t00lk1t"\r\n
ganassi -> jordan IMAP R port=46600 2 OK LOGIN completed
```

Ferramentas de Ataque

- Disseminação do uso da Internet criou mais problemas de segurança.
- Existem várias ferramentas que permitem o acesso sem autorização aos sistemas.
- Melhor proteção:
  - Políticas de Segurança.
  - Informações Criptografadas (SSH, SSL, ...).

Referências para Scanners

- Noordergraaf, Alex. Enterprise Server Products. How Hackers Do It: Trick, Tools and Techniques. Sun BluePrints™ OnLine – May, 2002.
- http://www.sun.com/blueprints
- CERT: http://www.cert.org.
- Nessus: http://www.nessus.org
- NMap: http://www.nmap.org
- Serafim, Vinícius da Silveira. Atacantes: Suas principais técnicas e ferramentas. Gseg - UFRGS.

  http://www.inf.ufrgs.br/~gseg/
- CVE: http://cve.mitre.org.