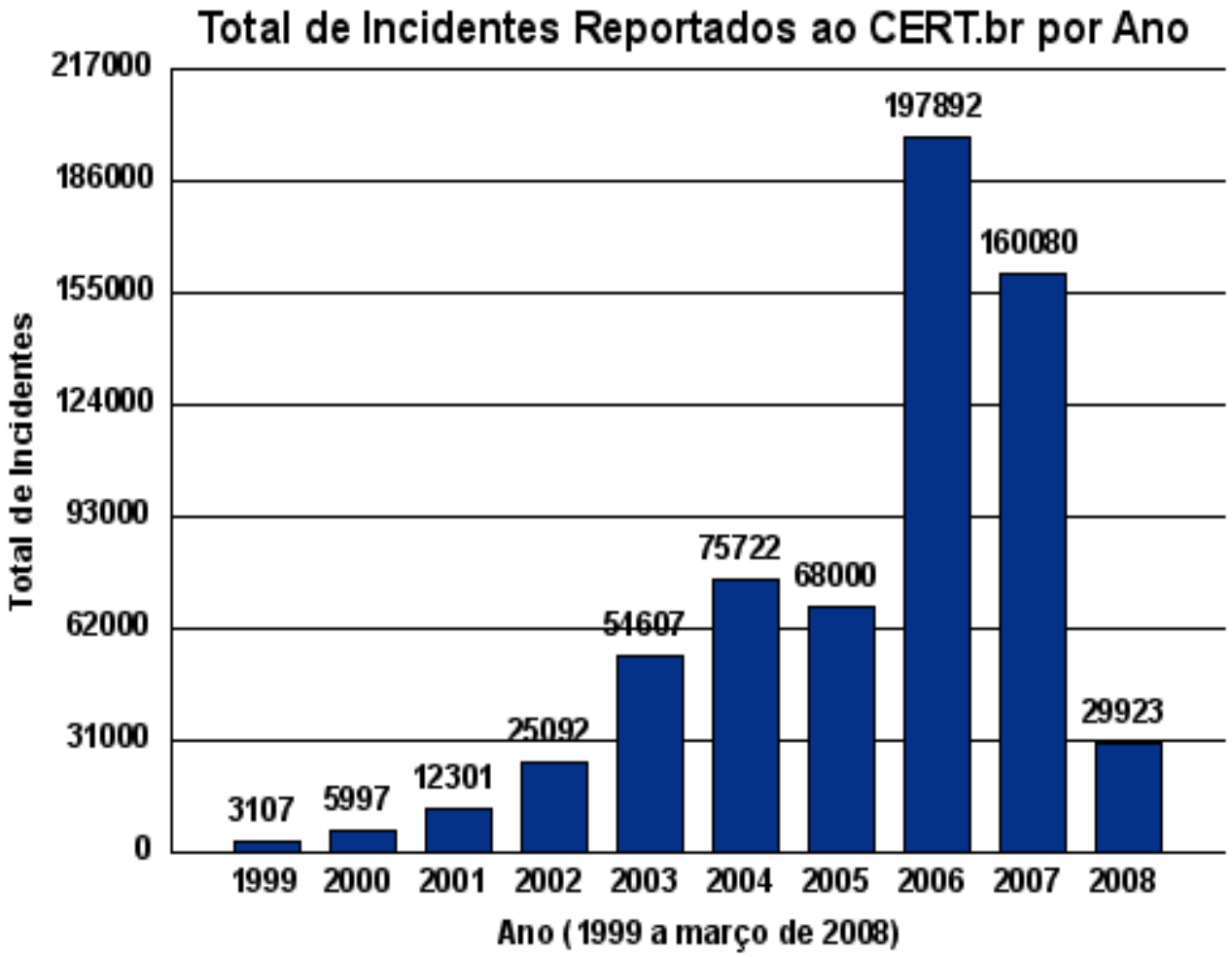

CLAVIS
segurança da informação

Hardening de Servidores Linux

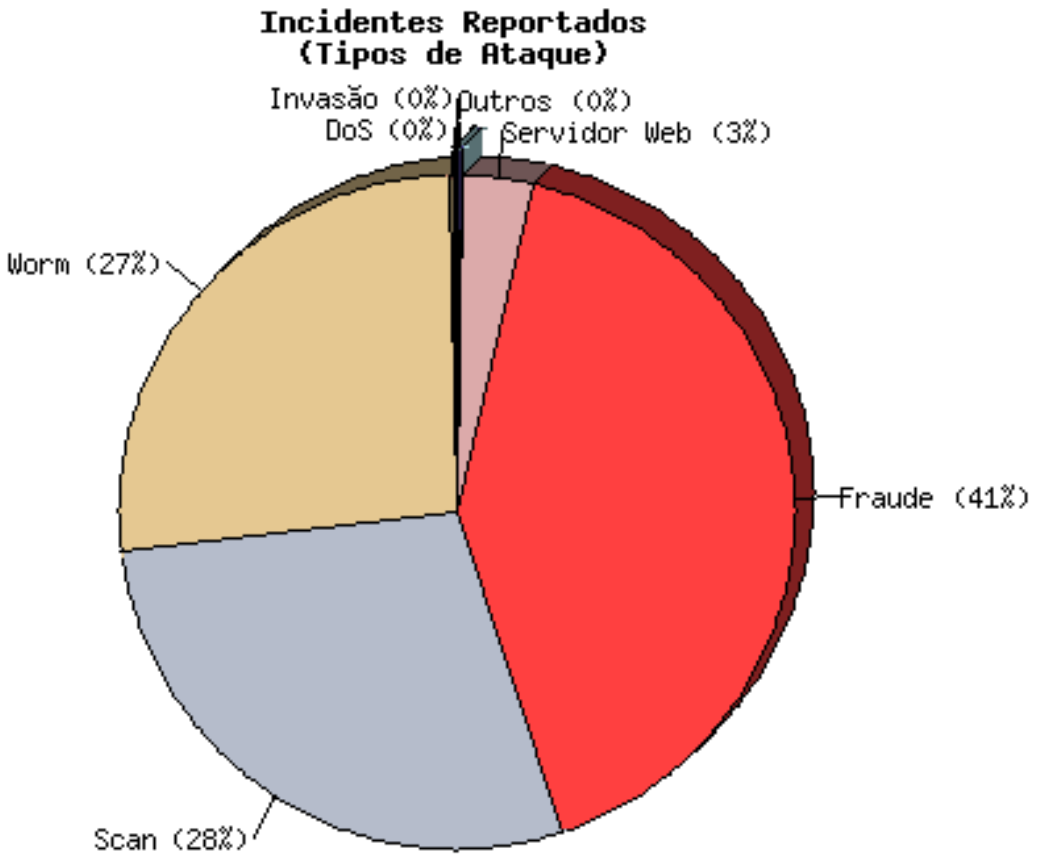
Victor Batista da Silva Santos
victor@clavis.com.br

- http://www.clavis.com.br -

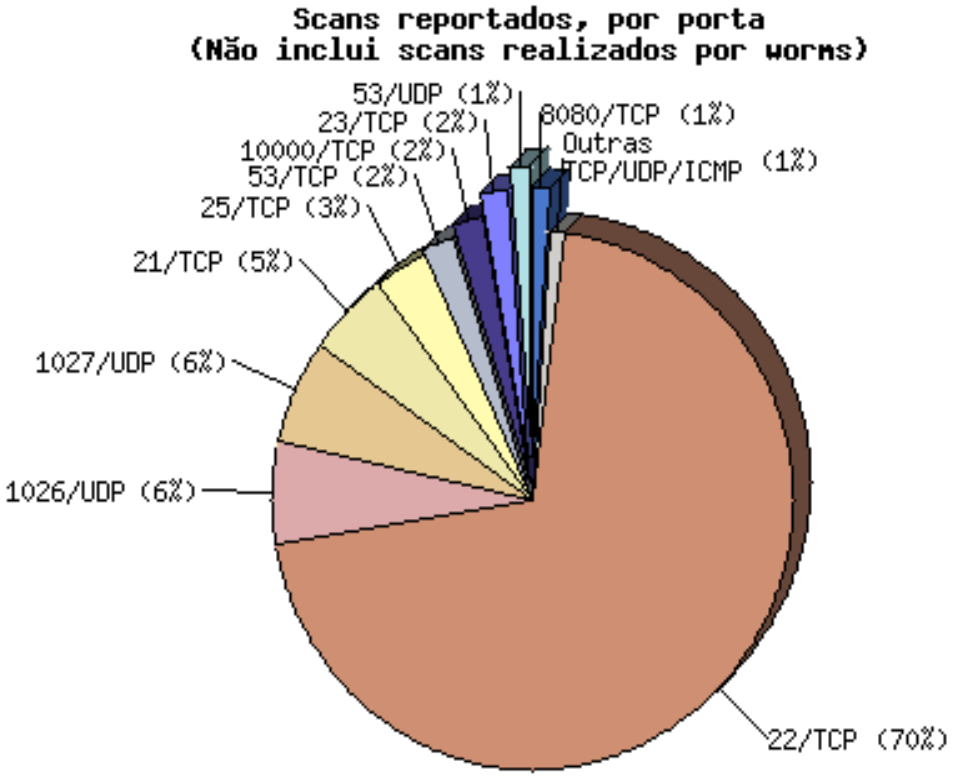
Por que se proteger?



Por que se proteger?



Por que se proteger?



O que você quer proteger?

- Seus Dados
- Seus Recursos
- Seus Sistemas
- Sua reputação

Contra o que se proteger?

- Roubo de Senhas
- Portas abertas
- Engenharia Social
- Falhas de autenticação
- Falhas de protocolo
- Negação de Serviço

Por que os ataque tem Sucesso ?

Top-10 by SANS

- Disponibildade *vs* Integridade e Confidencialidade
- Contas “default” no sistema
- Falta de atualização no sistema e nos serviços
- Utilização de serviços sem criptografia
- Envio inadequado de senhas

Por que os ataque tem Sucesso ?

Top-10 by SANS

- Falha no “rollback” dos backups
- Serviços Desnecessários
- Erros de Configuração
- Falha de implementação
- Educação dos usuários

Principais ameaças remotas

- Superexposição
- Autenticação remota
- Vulnerabilidades em aplicações web (cross site scripting, SQL Injection, Session Hijacking, etc...)

Principais ameaças locais

- Cavalo de Tróia
- Backdoors
- Rootkits
- Permissões e Privilégios (SUID/SGID)
- Arquivos e Diretórios com escrita global

Principais ameaças locais

Acesso Físico

- Acidentes
- Ataques deliberados
- Manejo de mídias
- Mesa, quadros e “*post-it*'s”

Principais ameaças locais

Confiança no usuário e no ambiente

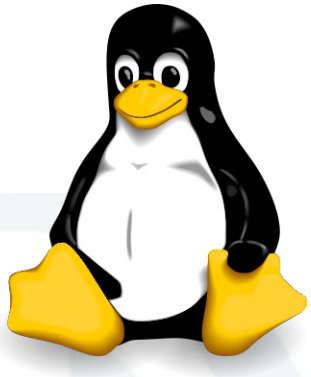
- variáveis de ambiente (especialmente “PATH”)
- Onde fica o “su”? E o “sudo”?

Onde colocar seu Servidor?

- A que ele se propõe?
- A quem ele deve atender?
- Quão sensíveis são os dados?
- Zona Desmilitarizada (DMZ)?

Sistemas UNIX-Like

- *Linux*
- *Free/Net/OpenBSD*
- *HP-UX*
- *Solaris*
- *AIX*
- *Mac OS X (Darwin)*



NetBSD®

HP-UX

solaris™

AIX

X

Mac OS X

Distribuições Linux

*UBUNTU

Red Hat/Fedora/CentOS

Debian

Slackware

Mandriva

Knoppix

SuSE

Pyramid

(entre <u>muitas</u> outras!)

Instalando o sistema

- Particione o seu disco
- LVM (Logical Volume Management)
- Swap
- Opt-in ou Opt-Out

Atendendo às suas Necessidades

- Atualizações de Software
- Atualizações de Segurança
- Suporte a dispositivos (hardware)
- Suporte técnico
- Estabilidade
- Gerenciamento de pacotes
- Tamanho

Recompilando o Kernel

- Kernel padrão vem com muito “bloatware”
- Devemos ajustá-lo às nossas reais necessidades
- E atualizar sempre que necessário

http://www.kernel.org/

Hardening de Kernel

- Pax/Grsecurity
- SELinux (Security-Enhanced Linux)
- AppArmor (Application Armor)
- Configuração de rede (Sysctl)

Registros (logs) do Sistema

- Sistema operacional e programas
- Atividades e mensagens especiais
- Acompanhamento do sistema
- Comportamento de programas e serviços
- Solução e prevenção de problemas
- Não é obrigatório – Mas é **extremamente importante**

Registros (logs) do Sistema

Renovando/Rotacionando Arquivos de Log

- Backups periódicos dos registros
- Logs menores são mais fáceis de analisar
- logrotate (*/etc/logrotate.conf*)

```
arquivo {
    create MASK USER GROUP
    rotate N
    compress
    daily|weekly|monthly|size N
    mail  ENDERECO@URL
}
```

Registros (logs) do Sistema

Protegendo seus arquivos de Log

- Mídias Confiáveis
- Atenção às permissões dos seus logs (0640 para a maioria)
- chattr -R +a /var/log/

Registros (logs) do Sistema

Gerenciando e Monitorando Arquivos de Log

- SWATCH
- Logcheck
- Entre outros

Controle de Acesso

Limpeza de Usuários do Sistema

- Bloqueie contas padrão ou inutilizadas:
  - adicione uma exclamação antes da senha no /etc/shadow
  - `passwd -l USUARIO` (-u para desbloquear)
- Removendo usuários:
  - `userdel -r USUARIO`
- Encontrando contas ociosas:
  - lastlog
- Limitando contas com permissão de login remoto
  - ssh, ftp, etc

Controle de Acesso

Gerenciamento e Política de Senhas

- login.defs
- PAM (Pluggable Authentication Modules)

Secure Shell (SSH)

- Acesso remoto ao terminal (“shell”) do servidor
- Tráfego criptografado (inclusive senhas)
- Tunelamento seguro
- Autenticação por senha ou certificado
- Suite OpenSSH:
  - ssh (rlogin/telnet)
  - scp (rcp)
  - sftp (ftp)

Secure Shell (SSH)

Configurando o Servidor :

- Desabilite login como root
- Use separação de privilégios
- Use a versão 2 do protocolo
- Libere acesso para determinados usuários
- Desabilite Forward de Portas
- Altere a porta padrão

Secure Shell (SSH)

CLAVIS segurança da informação

Defendendo-se de ataques ao SSH

- SSHTest
- Acesso somente por chaves públicas
- Limitando início de conexões (`ipt_recent`)
- Knockd
- Single Package Authorization

Sistemas de Detecção de Intrusão (IDS)

- Snort (NIDS)
- Labrador (HIDS)
- Entre Outros ...

Firewall

NetFilter/IPTables

- Monitora tráfego de rede
- Permite ou Nega passagem bidirecionalmente
- Baseado em regras em diferentes camadas
- Statefull: capaz de identificar o estado da conexão
- Suporta a NAT (Network Address Translation)

Firewall

Controle de acesso :

- Endereço de origem e destino
- Protocolo (TCP, UDP ou ICMP)
- Porta de origem e destino (TCP ou UDP)
- Tipo de Mensage ICMP
- Interface de Rede de Entrada e Saída

Firewall

- Estrutura (apenas regras pertinentes a FW Local)

```
iptables -A INPUT, OUTPUT, FORWARD
         --source IP/MASCARA  (-s, --src)
         --sport  PORTA
         --destination        (-d, --dst)
         --dport
         --protocol TCP, UDP
         -m (--state, --multiport, etc)
         -j  ACCEPT, DENY
```

- Regra “lockdown”

TCP Wrappers

- Registra o nome do host remoto antes de repassar a conexão ao *daemon* daquela porta

- Pode permitir ou negar acesso a redes

  - `/etc/hosts.allow`
  - `/etc/hosts.deny`

Sincronizando Relógios

Network Time Protocol (NTP)

- Utiliza UTC
- Tolerante a falhas
- Minimiza erros acumulados
- Essencial para correlacionamento de eventos

Sistema de Monitoramento

- Nagios
- Cacti
- MRTG (Multi Router Traffic Grapher)
- Monit

Hardening de serviços

BIND (/etc/named.conf)

- Oculte a versão

```
options {
   version “Desconhecida”;
};
```

Hardening de serviços

BIND (/etc/named.conf)

- Segregando zonas: Zona interna

```
view "internal"
{
   match-clients       { 192.168.0.1/16; };
   match-destinations  { 192.168.0.1/16; };
   recursion yes;

   zone "exemplo.local" {
       type master;
       allow-query { 192.168.0.1/16; };
       file "exemplo.local.zone";
       allow-transfer { none; };
   };
};
```

Hardening de serviços

BIND (/etc/named.conf)

- Segregando zonas: Zona externa

```
view "external"
{
   match-clients          { any; !localhost; !192.168.0.1/16;};
   match-destinations     { any; !localhost; !192.168.0.1/16;};
   recursion no;

   zone "exemplo.com.br" {
      type master;
      allow-query { any; !localhost; !192.168.0.1/16;};
      file "exemplo.com.br.zone";
      allow-transfer { none; };
   };
};
```

Hardening de serviços

Apache

- Adicionem suporte a conexões criptografadas (SSL) (se necessário)
- Atenção para módulos de segurança
- Ajustem as configurações adequadamente
- Verifiquem/Testem as configurações antes de aplicar
- Façam um reinício “gracioso”

Hardening de serviços

Apache – Opções interessantes de configuração

- *StartServers*, *MaxClients*, *MaxKeepAlive, etc.* – Limitando recursos
- *Timeout* – por quantos segundos esperar para interromper uma conexão inativa?
- *ServerTokens*, *ServerSignature* – o que o servidor deve contar sobre si?

Hardening de serviços

Apache – Módulos Interessantes

- mod_evasive
  - → *contra ataques de DoS*
- mod_security
  - → *IDS/IPS integrado*
- mod_access/mod_authz
  - → *controle de acesso*

Hardening de serviços

PHP

- Habilite o *"safe-mode"* (versões < 6.0)
  - `safe_mode = On`
  - `safe_mode_gid = Off`
  - `safe_mode_exec_dir = "CAMINHO"`
  - `safe_mode_allowed_env_vars = "PHP_"`
  - `safe_mode_protected_env_vars = "LD_LIBRARY_PATH"`

Hardening de serviços

PHP

- Desative a exibição de erros do PHP
  - `display_errors = Off`
  - `log_errors = On`
  - *`[error_log = ARQUIVO]`*
  - *`[error_reporting = E_ALL]`*
- Não exponha seu interpretador
  - `expose_php = Off`
- Evite a visualização de seus scripts (no *httpd.conf*)
  - `AddType application/x-httpd-php .inc`
  - `AddType application/x-httpd-php .class`

Hardening de serviços

PHP

- *Hardened-PHP Project*
  - ➔ Auditoria de aplicativos PHP populares
  - ➔ Patches para o código original do PHP

Hardening de serviços

MySQL

- Adicione senha para o usuário “root”
  - `mysql -u root`
  - ```
    mysql> UPDATE mysql.user
           SET password=PASSWORD('NOVA SENHA')
           WHERE user='root';
    ```
  - `mysql> FLUSH PRIVILEGES;`
- Dê acesso apenas a quem precisa (*my.cnf*)
  - `bind-address = 127.0.0.1`
    ```

Hardening de serviços

MySQL

- Remova bancos não utilizados
  - `mysql> DROP DATABASE test;`
- Altere o nome da conta administradora
  - `mysql> UPDATE user`
    `SET user="voce" WHERE user="root";`
  - `mysql> FLUSH PRIVILEGES;`
- Apague o histórico do MySQL
  - `rm ~/.mysql_history`

Hardening de serviços

Vsftp (/etc/vsftpd/vsftpd.conf)

- Proibe login anônimo
  - `anonymous_enable=NO`
- Permite conexão de usuários locais
  - `local_enable=YES`
- Permite uploads
  - `write_enable=YES`
- Troca a porta padrão
  - `listen_port=4567`

Hardening de serviços

vsftp (/etc/vsftpd/vsftpd.conf)

- Define máscara para usuários locais
  - `local_umask=022`
- Permite acesso apenas a alguns usuários
  - *`[userlist_deny=YES]`*
  - `userlist_enable=YES`
  - `userlist_file=/etc/vsftpd/ftp.users`
- chroot de usuários
  - `chroot_list_enable=YES`
  - `chroot_list_file=/etc/vsftpd/chroot.users`

Hardening de serviços

vsftp (/etc/vsftpd/vsftpd.conf)

- Ativando acesso criptografado (SSL)
  - `ssl_enable=YES`
  - `allow_anon_ssl=NO`
  - `force_local_data_ssl=YES`
  - `force_local_logins_ssl=YES`
  - `ssl_sslv2=YES`
  - `rsa_cert_file=/etc/vsftpd/certs/ftp.pem`

Hardening de serviços

sendmail (/etc/mail/sendmail.mc)

- Defina opções de privacidade
  - `define('confPRIVACY_FLAGS','goaway, authwarnings,restrictmailq,restrictqrun, nobodyreturn')dnl`
- Modifica o banner de apresentação
  - `define('confSMTP_LOGIN_MSG','meuFTP')dnl`
- Oculte o domínio
  - `MASQUERADE_AS('exemplo.com.br')dnl`
  - `FEATURE('always_add_domain')dnl`
  - `FEATURE('masquerade_entire_domain')dnl`

Hardening de serviços

sendmail (/etc/mail/sendmail.mc)

- Evite Relay Aberto
  - `/etc/mail/relay-domains`
  - `FEATURE('relay_hosts_only')dnl`
  - `FEATURE('relay_entire_domains')dnl`
- Mantenha uma Lista de Acesso
  - `/etc/mail/access`
  - `FEATURE('access_db')dnl`
  - `FEATURE('blacklist_recipients')dnl`

Hardening de serviços

sendmail (/etc/mail/sendmail.mc)

- Use Anti-Spam (procmail como MDA)
  - SpamAssassin
  - OSBF-Lua
  - *http://www.ordb.org*
  - *http://cbl.abuseat.org*
  - *http://mail-abuse.org*
  - *http://www.spamhaus.org*
- Use Antivírus
  - emails verificados x carga no servidor
  - Amavis

Auditoria de Segurança

- Nmap
- Nessus
- Bastille UNIX
- Chkrootkit / RKHunter

Faça Backup's

- Rsync
- Bacula
- A.M.A.N.D.A
  (Advanced Maryland Automatic Network Disk Archiver)
- Entre outros...

Obrigado !!!

Victor Batista da Silva Santos
victor@clavis.com.br

- http://www.clavis.com.br -