Segurança em Ambiente Linux

Uma visão geral das tecnologias, ferramentas e abordagens utilizadas na área de segurança do Sistema Operacional Linux

Parte I:

Segurança: introdução, conceitos e exemplos

Ademar de Souza Reis Jr.
<ademar@conectiva.com.br>
http://www.ademar.org

XII Congresso C. Computação Bolívia
Tarija – Bolívia – Outubro 2005

última versão atualizada disponível em
http://www.ademar.org/

Conteúdo

- Definições
- Segurança, uma visão pragmática
- Requisitos para um sistema seguro
- Políticas de segurança
- Anúncios de segurança e “full-disclosure”
- E agora? O que fazer em determinadas situações
- Conclusões

Definições

O que é segurança?

- Manter algo livre de perigo (acesso indevido inclusive)
- Manter algo em um estado/situação confiável

O que é um ataque?

- Tentativa de burlar/romper a segurança
- Algo não autorizado ou prejudicial

O que é uma vulnerabilidade?

- Furo de segurança
- Defeito de software + cenário

Sobre segurança

- **Ponto mais fraco**

  "Um sistema é tão seguro quanto seu ponto mais fraco"

- **Relação complexidade <-> segurança**

  20 opções de configuração: pouco?

- **Relação comodidade <-> segurança**

  Regra geral: quanto mais seguro, mais difícil de se usar (e quanto mais inseguro, mais fácil de se usar)

- **Criatividade do atacante**

  - Liu Die Yu: Ataque IE em 6 etapas (2003-11-11)

Ainda sobre segurança...

- **O que estou defendendo?**

  Segurança nacional ou minha senha de registro do slashdot.org?

- **De quem estou me defendendo?**
  - Meu vizinho
  - FBI/NSA

- **Engenharia Social**

  Regra geral: o ponto mais fraco em um sistema é o ser humano
  - Zelador, vigias, colegas de trabalho
  - Você mesmo :-)

Ainda sobre segurança...

- **Quanto custa me defender**
  - Famosa relação “custo-benefício”
  - Um seguro pode sair mais barato
- **Falsa sensação de segurança**

  Achar que está seguro é pior do que **saber** que está inseguro

Tipos de ataques/vulnerabilidades

- **Negação de Serviço**
  - Denial of Service: DoS
  - Distributed Denial of Service: DDoS
- **Vazamento de informação**
- **Quebra de autenticação (acesso não autorizado)**
- **Manipular comportamento do sistema (controle da máquina/aplicação)**

Tipos de ataque e motivação

- **Barulhento:** é descoberto rapidamente
  - Fama
  - Vingança
  - Diversão
- **Silencioso:** pode demorar a ser detectado
  - Crimes diversos (espionagem, roubo, etc)
  - Ponte para ataques mais sofisticados
  - Curiosidade
  - Uso de recursos

Vulnerabilidades mais comuns

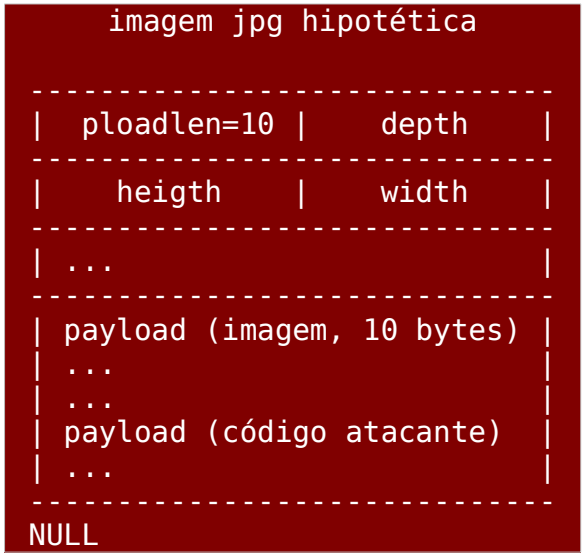
- **Buffer overflow e afins**
  - Execução de código/comandos arbitrários
  - DoS
- **Format strings**
- **Cross-site-scripting**
- **SQL Injection**

Exemplos práticos de vulnerabilidades

Buffer overflows

```
int main(int argc, char **argv)
{
     char buf[128];

[...]
     strcpy(buf, argv[1]);
[...]
}
```




```
char *jpg_get_payload(JPGImage img)
{
     char *buf;
     int len, depth;
     int i = 0;

     len = jpg_get_ploadlen(img);
     depth = jpg_get_depth(img);

     buf = malloc(len * depth);

     while(img->payload != NULL) {
          buf[i] = img->data[i];
          i++;
     }

     return buf;
}
```

Exemplos práticos de vulnerabilidades

Format strings e caracteres de escape

```
C:
 ...
 printf(variable);
 ...

bash:
 rm -rf /home/$user
 ...
 bash: rm -f $file
 ...
```

+

```
variable = “%s %p foobar”

user=“”;

file=“-r /”
```

= !!!

Cross site scripting

URL: http://www.microsoft.com/products/?&download=myserver.com/winupdate.exe

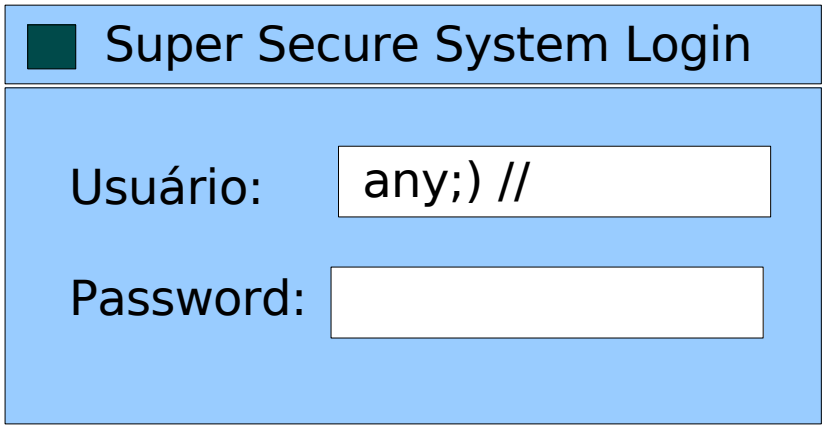
(exemplo fictício)

Exemplos práticos de vulnerabilidades

SQL Injection

```
if (SELECT user FROM auth_db WHERE user = $user AND password = $password;)
     /* user auth OK */
else
     /* error, user not found or invalid pass */
endif
```

+



=

```
if (SELECT user FROM auth_db WHERE user = any;) // AND password = “$password”)
     /* user auth OK */
else
     /* error, user not found or invalid pass */
endif
```

O que um sistema seguro precisa ter

- **Tecnologia correta**
  - Firewall
  - Criptografia
  - Autenticação
- **Software de qualidade**
  - Código maduro e estável
  - KISS (Keep it Simple and Small)
  - Atualizações
- **Boa política de segurança**

Política de Segurança

Principal tarefa do “Analista de Segurança”

- **Usuários**
  - Quem
  - Quando
  - Como
- **Software**
  - Escolha
  - Instalação
  - Atualizações
- **Concientização**

  Lembrar que:
  1. A segurança depende do ponto mais fraco
  2. O ponto mais fraco geralmente é o ser humano

Atualizações de Segurança

```
-------------------------------------------------------------------------
CONECTIVA LINUX SECURITY ANNOUNCEMENT
-------------------------------------------------------------------------
PACKAGE   : lynx
SUMMARY   : Security fix for lynx
DATE      : 2005-10-18 15:08:00
ID        : CLA-2005:1037
RELEASES  : 10
-------------------------------------------------------------------------

DESCRIPTION
 lynx[1] is a lightweight text-mode browser.

 This announcement fixes a buffer overflow vulnerability[2] found by
 Ulf Harnhammar. A remote attacker could exploit this via a specially
 crafted server to execute arbitrary code with the privileges of the
 lynx's user.

SOLUTION
 It is recommended that all lynx users upgrade their packages.

REFERENCES
 1.http://lynx.browser.org/
 2.http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-3120

UPDATED PACKAGES
...
```

- **Bugtraq:** http://www.securityfocus.com
- **Conectiva:** http://disto.conectiva.com.br/atualizacoes/
- **Mandriva:** http://www.mandriva.com/security/advisories

Fui invadido, e agora?

- Não entre em pânico!
- É fundamental descobrir como e quando a invasão ocorreu
- Identifique a razão do ataque;
- Não confie nos programas da máquina;
- Não reinstale tudo imediatamente;
- Tente capturar informações com a máquina ainda online;
- Faça um análise detalhada com um disco de boot e montando as partições como read-only;
- Registre tudo (pode servir como prova criminal);
- Cuidado com backups comprometidos;
- Identifique o que não é mais confiável na rede. Na dúvida, não arrisque, troque todas as senhas e chaves;
- Ataques podem ser reportados (http://www.nic.br/nbso.html).

Descobri uma vulnerabilidade, e agora?

- Certifique-se de que o problema realmente existe e não foi corrigido;
- Contate o(s) fabricante(s) ou um órgão responsável;
- Agende uma data para divulgação pública (geralmente 1 semana a 1 mês);
- Publique um relatório/anúncio detalhado na data prevista.
- Se o fabricante não responder ou se recusar a corrigir o problema, faça o anúncio público (cuidado!)

Quem contatar:

- **Fabricante:** security@
- **CERT:** http://www.cert.org
- **Programas OpenSource:** vendor-sec@lst.de

Conclusões

- Nada é tão simples como parece
- Um sistema é tão seguro como seu ponto mais fraco
- O ponto mais fraco de um sistema geralmente é o humano
- Segurança não é um produto de caixinha
- Achar que está seguro é pior do que saber que está inseguro
- Todo sistema requer atenção e atualizações constantes
- Cuidado com mitos:
  - “Ninguém vai achar meu servidor”
  - “Não tenho nada importante na minha rede”
  - “Linux é super-seguro, posso ficar tranquilo”

Para saber mais...

- Ross J. Anderson. Security Engineering, A Guide to Building Dependable Distributed Systems. ISBN 0-471-38922-6.
- Niels Ferguson and Bruce Schneier. Practical Cryptography. ISBN 0-471-22357-3.
- Simson Garfinkel and Gene Spafford. Practical Unix and Internet Security (Second Edition). ISBN 1-56592-148-8.
- Bruce Schneier. Secrets & Lies, Digital Security in a Networked World. ISBN 0-471-45380-3.
- Crypto-Gram newsletter: http://www.schneier.com/crypto-gram.html
- Bugtraq: http://www.securityfocus.com
- Phrack: http://www.phrack.org
- CERT: http://www.cert.org
- Anúncios Conectiva: http://distro.conectiva.com.br/atualizacoes
- Anúncios Mandriva: http://www.mandriva.com/security/advisories