

HNTOOL

HARDENING TOOL FOR *NIXES

Hugo Doria <mail@hugodoria.org>

Rafael Gomes <rafaelgomes@techfree.com.br>

AGENDA

- Quem somos
- História
- HnTool hoje
- Instalando e usando
- Criando um módulo
- Como contribuir

HUGO DÓRIA

- Administrador de sistemas
- Consultor em segurança
- Desenvolvedor do Arch Linux
- LPIC
- Pai coruja
- Viciado em sushi
- POGamador nas horas vagas

RAFAEL GOMES

- Administrador de sistemas
- Responsável pela segurança da UFBA
- Embaixador do Projeto Fedora
- MCSO e LPIC-1
- Pós-graduando em SD na UFBA
- Viciado em carne de sol
- POGamador nas horas vagas

SENTA QUE LA VEM HISTÓRIA

- Dia a dia do trabalho
- Conversa no FISL
- Conversa no IRC
- Necessidade de automação
- Ausência de ferramenta parecida



```
if vezes_mesma_tarefa > 3:  
    criar_software()
```

SISTEMAS SUPORTADOS



MÓDULOS

- Apache
- Authentication
- SSH
- PHP
- Filesystems
- Remote
- System-Wide
- PostgreSQL
- Ports

REQUISITOS

- Python 2.4 ou superior
- Isof
- Kernel unix like
- Cérebro
- Vontade

INSTALANDO

```
# python setup.py install
```

Pacotes para ArchLinux e Debian

[Starting HnTool checks...]

Checks for services with remote access allowed

By default, services are rejecting connections

[OK]

Checks security problems on system-wide configuration

Core dumps are disabled

[OK]

ExecShield is enabled

[OK]

TCP SYN Cookie Protection is enabled

[OK]

GRUB does not ask for a password

[LOW]

Permissions on /boot/grub/menu.lst are greater than 600

[LOW]

Ignore broadcast request is disabled

[LOW]

Ping reply is enabled

[LOW]

Single-User mode does not requires authentication

[MEDIUM]

Checks filesystems for security problems

mlocate.db found.

[OK]

Did not found old file(s) (+30 days) in /tmp

[OK]

Found old file(s) (+30 days) in /var/db/locate.database

[LOW]

Please run /usr/libexec/locate.updatedb

[INFO]

Checks users, groups and authentications

Permissions on shadow file are correct (600)

[OK]

Permissions on passwd file are correct (644)

[OK]

There aren't users (not root) with UID 0

[OK]

User "hugo" may have a harmful shell (/bin/bash)

[MEDIUM]

Permissions on /home/lost+found are greater than 700

[MEDIUM]

Permissions on /home/hugo are greater than 700

[MEDIUM]

By default passwords do not expires on 90 days or less

[MEDIUM]

Checks security problems on sshd config file

Root access is not allowed

[OK]

HnTool – A hardening tool for *nixes – Report

Checks for services with remote access allowed

OK By default, services are rejecting connections

Checks security problems on system-wide configuration

OK Core dumps are disabled

OK ExecShield is enabled

OK TCP SYN Cookie Protection is enabled

LOW GRUB does not ask for a password

LOW Permissions on /boot/grub/menu.lst are greater than 600

LOW Ignore broadcast request is disabled

LOW Ping reply is enabled

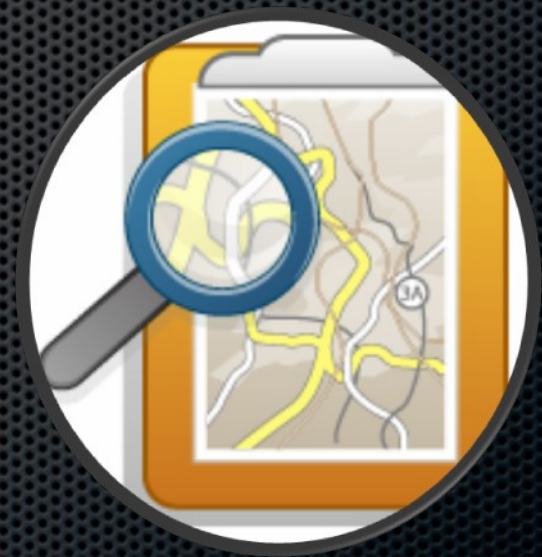
MEDIUM Single-User mode does not requires authentication

Checks filesystems for security problems

OK mlocate.db found.

ROADMAP

- Módulos para MySQL, FTP, Iptables, Samba, Squid
- Informações mais detalhadas
- Suporte a traduções
- Reformulação na estrutura interna
- Checagem WEB



COMO CONTRIBUIR



- Reportando bugs
- Enviando sugestões
- Divulgando
- Criando pacotes
- Portando para outros sistemas
- Criando módulos

CRIANDO UM MÓDULO

```
class Rule:
    def short_name(self):
        return "ssh"
    def long_name(self):
        return "Checks security problems on sshd config file"
    def __init__(self, options):
        pass
    def analyze(self, options):
        check_results = {'ok': [], 'low': [], 'medium': [], 'high': [], 'info': []}
        ssh_conf_file = ['/etc/ssh/sshd_config', '/etc/ssh/sshd_config']

        for sshd_conf in ssh_conf_file:
            if os.path.isfile(sshd_conf):
                try:
                    fp = open(sshd_conf, 'r')
                except IOError, (errno, strerror):
                    check_results[4].append('Could not open %s: %s' % (sshd_conf, strerror))
                    continue

                lines = [x.strip('\n') for x in fp.readlines()]

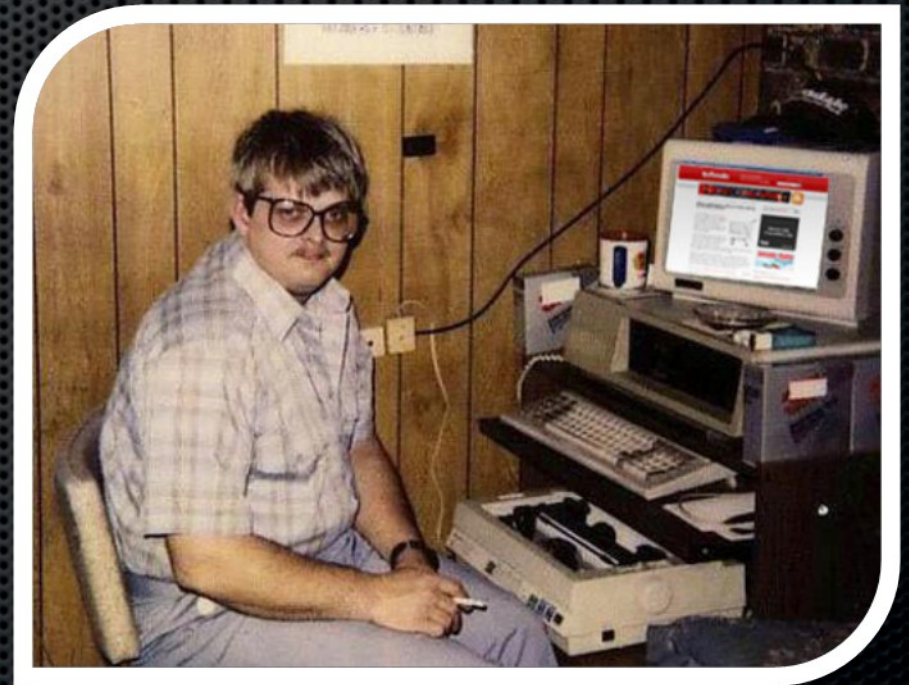
                # Checking if SSH is using the default port
                if 'Port 22' in lines or '#Port 22' in lines:
                    check_results['low'].append('SSH is using the default port')
                else:
                    check_results['ok'].append('SSH is not using the default port')
```

NOVAS FUNÇÕES

```
def requires(self):  
    return '/usr/bin/lsof'
```

CONTRIBUIDORES

- Aurélio Heckert
- Cândido Vieira
- Elton Pereira
- Filipe Rosset
- Italo Valcy
- Nycholas
- Késsia Pinheiro
- Rafael Martins
- Silas Ribas



MAIORES INFORMAÇÕES

http://hntool.net

PERGUNTAS?



OBRIGADO!!

http://hntool.net

Hugo Doria <mail@hugodoria.org>

Rafael Gomes <rafaelgomes@techfree.com.br>