
# Teste de invasão

*Relatório de atividades, resultados e recomendações*

# Sumário

Capítulo 1

# Introdução

Este documento inicia-se pela descrição das atividades realizadas e escopo do teste de invasão realizado. Posteriormente será apresentado a descrição das vulnerabilidades encontradas, bem como suas recomendações e níveis de criticidade e o impacto que pode ser causado.

Capítulo 2

# Atividades Realizadas

A consultoria de segurança proposta para o teste de invasão, aplicou testes de segurança no seguinte escopo definido:

IPs:

```
123.456.789.1
123.456.789.2
```

URL: http://app.example.org

O trabalho foi iniciado pela identificação de portas, serviços e versões dos serviços, para isso foi utilizado a ferramenta `nmap`:

```
$ nmap -sS -sV -A -Pn app.example.org

Starting Nmap 6.40 ( http://nmap.org ) at 2014-03-07 20:54 BRT
Nmap scan report for app.example.org (123.456.789.1)
Host is up (0.13s latency).
Not shown: 995 closed ports
PORT     STATE    SERVICE    VERSION
22/tcp   open     ssh        OpenSSH 5.9p1 Debian 5ubuntu1.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey: 1024 1b:9e:64:7c:7c:e0:39:48:87:dc:65:32:00:5e:14:33 (DSA)
| 2048 74:e3:34:80:5c:d2:87:04:30:7e:f7:c6:97:a3:d6:3e (RSA)
|_256 9c:8e:9e:f8:7a:61:c4:63:ca:c4:02:3c:8b:a1:49:7d (ECDSA)
25/tcp   filtered smtp
80/tcp   open     http       nginx 1.4.1
|_http-methods: No Allow or Public header in OPTIONS response (status code 404)
| http-robots.txt: 1 disallowed entry
|_/
|_http-title: The page you were looking for doesnt exist (404)
```

```
OS fingerprint not ideal because: Didnt receive UDP response. Please try again with -sSU
No OS matches for host
Network Distance: 12 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

$ namp -sS -sV -A -Pn 123.456.789.2

Starting Nmap 6.40 ( http://nmap.org ) at 2014-03-08 15:04 BRT
Nmap scan report for 123.456.789.2
Host is up (0.13s latency).
Not shown: 995 closed ports
PORT     STATE    SERVICE    VERSION
22/tcp   open     ssh        OpenSSH 5.9p1 Debian 5ubuntu1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey: 1024 f9:78:bd:aa:d6:4d:84:24:18:4f:b5:d2:b7:f7:da:5f (DSA)
| 2048 02:04:f0:d6:6a:c5:c1:60:e9:73:62:c9:01:b2:04:e6 (RSA)
|_256 16:9e:e4:0c:7e:c1:73:6e:eb:f6:56:15:54:30:69:63 (ECDSA)
5432/tcp open     postgresql PostgreSQL DB 9.2.0 - 9.2.2
OS fingerprint not ideal because: Didn't receive UDP response. Please try again with -sSU
No OS matches for host
Network Distance: 11 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Foram realizados diversos tipos de ataques com base nos serviços que foram listados em cada endereço IP e principalmente na aplicação web. Durante os testes todas as classes de vulnerabilidades listadas na OWASP Top 10 foram exploradas.

Com base nas informações passadas na primeira reunião via hangout, testes foram realizados na aplicação web e algumas vulnerabilidades foram encontradas.

As ferramentas utilizadas para automatizar uma parte no processo de pentest foram:

- Arachni
- Xenotix
- w3af

- OpenVas
- Metasploit Pro
- Nexpose Pro

O próximo capítulo detalhará sobre os resultados.

Capítulo 3

# Resultados Obtidos

Vulnerabilidades encontradas na camada de aplicação:

## Transmissão de Informações Sensíveis

Um atacante pode monitorar o tráfego de rede dos usuários da aplicação de forma a conseguir facilmente ler os dados que passam, isso inclui conseguir ler os dados preenchidos e enviados via formulários. Esta falha pode expor dados de usuários individuais, se a conta de administrador for comprometida todo o sistema poderia ser exposto.

- Exploração: `difícil`
- Risco: `médio`
- Referências: CWE-319, CWE-200

```
Na verificação do Gemfile.lock em busca de dependências vulneráveis, nada foi
encontrado, todas as Gems estão devidamente atualizadas.
```

## Brute-force Login Form

Um atacante pode fazer uso de ferramentas de brute force como o Hydra e assim conseguir descobrir algum usuário e senha para login na aplicação.

- Exploração: `média`

- Risco: `alto`

---

Vulnerabilidades encontradas na camada de infraestrutura:

# Dos Attack

Tanto o servidor de aplicação como o de banco de dados estão vulneráveis a ataques de negação de serviços do tipo mais simples. Um ataque deste tipo pode deixar os servidores e consequentemente a aplicação indisponível por um longo tempo.

- Exploração: `fácil`
- Risco: `médio`
- Referência: CVE-2004-0230

# Brute-force SSH

Nos 2 servidores, o OpenSSH está configurado de forma a aceitar senha para efetivar a autenticação no processo de login, por não ter nenhum impeditivo é possível realizar um ataque de força bruta e descobrir a senha de root para acesso total ao servidor.

- Exploração: `média`
- Risco: `alto`

# Brute-force Postgres

O Postgres por está visível e habilitado para operar em network, na configuração atual é vulnerável a ataques de força bruta e interceptação de dados por meio de sniffer. É possível descobrir o login e senha de acesso ao banco ou ainda interceptar os dados que são trafegados para o servidor de aplicação.

- Exploração: `média`
- Risco: `alto`

Capítulo 4

# Recomendações

Abaixo segue as recomendações de segurança para correção das falhas listadas:

## Uso de SSL

Fazer uso de SSL e ativar o módulo SPDY no Nginx, isso irá barrar a captura de dados por análise de tráfego de rede. Outro benefício é o de dificultar as tentativas de brute-force nos formulários da aplicação.

Complemento: SPDY, HTTP2 e por que você deveria conhecê-los Configurando o Nginx com SPDY

## Estratégia de Login

Implementar o bloqueio de ip por tentativas de login excessivas, se por exemplo um determinado ip realizar 5 tentativas de login e errar, ele seria bloqueado, desta forma barraria qualquer tentativa de brute-force. Uma outra maneira seria fazer uso de um captcha bem simples, no estilo (Quanto é 1 + 1 ?).

Complemento: TextCaptha

## Implementar Firewall

Ativar firewall nos 2 servidores no formato de whitelist onde por default tudo é bloqueado e apenas alguns serviços são liberados, isso evita ataques Dos simples e a captura de informações por meio de scans.

Recomendo o uso do UFW, que é uma interface facilitadora para o iptables.

Complemento: UFW - Uncomplicated Firewall

## Configurar OpenSSH

Desativar a opção `PasswordAuthentication` no arquivo /etc/ssh/sshd_config desta forma o SSH será forçado a trabalhar somente com autenticação por meio de chave pública e com isso atques de brute-force serão evitados. Isto deve ser feito nos 2 servidores.

Complemento: Aumentando a segurança das chaves ssh

## Habilitar Private Networking

A opção de private networking deve ser ativada e seu uso implementado na comunicação entre os 2 servidores, isso evita a interceptação dos dados entre os servers e escapa de ataques de brute-force no Postgres. Outro ponto importânte é a ocultação do serviço no servidor de banco de dados.

Complemento: How To Set Up And Use DigitalOcean Private Networking

Capítulo 5

# Conclusão

O teste de invasão realizado apresentou o nível de exposição a ataques que a infraestrutura e aplicação estão sujeitas a qualquer momento.

É importante lembrar que não houve qualquer bloqueio nas tentativas de exploração por meio de algum Firewall e que outros testes de maior densidade foram evitados para não causar qualquer interrupção da aplicação em produção.

A Initsec encontra-se à disposição para detalhar os tipos de ataques efetuados e prestar auxílio nas definições decorrentes das recomendações que foram descritas neste relatório.


Teste de invasão

Daniel Romero