Testes de Invasão: Metodologia, Técnicas e Ferramentas

Prof. Felipe S. Barbosa

Sobre mim...

Trabalho:

Analista de Redes - Núcleo de Informática do DNIT/PI

Formação:

Graduado em Tecnologia de Redes

Esp. em Segurança com Ênfase em Perícia Forense

Certificações:

ISO 27002 – Information Security System – ISFS

ITIL®V3 – Information Technology Infrastructure Library

Lead/Auditor ISO/IEC 27001 – ISMS

Consultor / Sebrae/PI:

Segurança da Informação, Análise de Riscos e CN

Professor: Faculdade Maurício de Nassau Parnaiba/PI

Pós em Gestão de Projetos de TI

- **Segurança da Informação**
- **Teste de Invasão e aspectos legais**
- **Levantamento de Informações**
- **Google Hacking**
- **Engenharia Social**
- **Varreduras Ativas, Passivas e Furtivas de Rede**
- **Enumerações de informações e serviços**
- **Testando o Sistema**

Laboratório:

Disponível:

- 3 máquinas virtuais preparadas para execução dos ataques (.virtualbox)
- Backtrack 5 R3
- Kali Linux
- Debian (metasploitable)

Objetivos

- É simular de forma controlada um ataque real que normalmente é executado por criminosos.
- Entender a importância da segurança da informação no mundo de hoje.
- Visão geral sobre Testes de Invasão.

Justificativa / Motivação

- Entender reais **riscos** que vulnerabilidades específicas apresentam ao negócio.
- Testar **de fato** a segurança da rede ou sistema de informação.
- Determinar se **investimentos** atuais estão realmente detectando e prevenindo ataques.
- É **mais barato** ser Proativo

Segurança da Informação

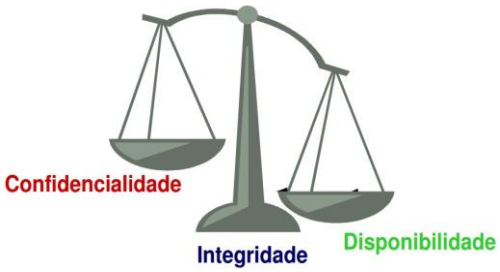
"Segurança da Informação está relacionada com proteção de um conjunto de dados, no sentido de preservar o valor que possuem para um indivíduo ou uma organização."

Nossa Realidade

As empresas estão usando cada vez mais a Internet para a realização de seus negócios.

O valor da informação é o cerne do negócio.

Princípios básicos da Segurança da Informação



Integridade: Garantir que a informação estará Íntegra, livre de alterações e completa.

Confidencialidade: Garantir que a informação será acessada somente por quem de direito.

Disponibilidade: Garantir que a informação estará disponível para quem tem o direito de acessar.

Autenticidade: Garantia da origem da informação

Princípios básicos da Segurança da Informação

Vulnerabilidades
AMEAÇAS
Riscos
ATAQUES

Vulnerabilidades

Fragilidade que pode fornecer uma porta de entrada para um atacante.

Vulnerabilidades = ponto fraco

Exemplo de vulnerabilidade:

Instalação:
- Falta de mecanismo de monitoramento
- Proteção física inadequada
- Energia elétrica instável

Banco de dados:
- Falta de backup
- Armazenamento inadequado

Ameaças

Agente ou ação que se aproveita de uma vulnerabilidade.

Ameaça = uma ocorrência, um fato

- Funcionário descontentes ou desmotivados.
- Baixa conscientização no assunto de Segurança.
- Desastres (naturais ou não, como incêndio, inundação, terremoto, terrorismo).
- Falta de políticas e procedimentos implementados.

Riscos

É a relação entre a probabilidade e o impacto da ameaça ocorrer.

Exemplos de Impacto

- Perda de clientes e contratos.
- Danos a imagem.
- Perda de produtividade.

Ataques

Incidência da ameaça sobre a vulnerabilidade.

Ataques

- **Interno** (***70% do ataques***)
  - ✓ Funcionários insatisfeitos
  - ✓ Funcionários despreparados

- **Externo**
  - ✓ Crackers
  - ✓ Concorrentes
  - ✓ Espionagem Industrial
  - ✓ Terroristas

Áreas de atuação e Serviços de Segurança

- Criação de Políticas de Segurança
- Hardening de Servidores
- Análise de Vulnerabilidade
- Teste de Invasão
- Análise de Aplicação
- Perícia Computacional
- Treinamento de Colaboradores
- Auditória

Testes de Invasão

Objetivos:

- Fornecer uma visão geral sobre testes de invasão
- Entender a anatomia e os tipos diferentes de ataques
- Conhecer as fases de um teste de invasão
- Conhecer as metodologias e os aspectos legais.

Visão geral sobre Teste de Invasão

- **Teste de Invasão** é um processo de análise detalhada do nível de segurança de um sistema ou rede usando a perspectiva de um infrator.

Tipos de abordagens de Teste de Segurança

O que você sabe sobre o ambiente?

- Blind
- Double blind
- Gray Box
- Double Gray Box
- Tandem
- Reversal

Tipos de Pentest

- **Blind:**

  Auditor não conhece nada sobre o alvo que irá atacar, porém o alvo sabe que será atacado e o que será feito durante o teste.

- **Double Blind:**

  Auditor não conhece nada sobre o alvo, e o alvo não sabe que será atacado e tão pouco sabe quais testes o auditor irá realizar.

Tipos de Pentest

- **Gray Box:**

  Auditor tem conhecimento parcial do alvo, e o alvo sabe que será atacado e também sabe quais testes serão realizados..

- **Double Gray Box :**

  Auditor tem conhecimento parcial do alvo, e o alvo sabe que será atacado, porém, não sabe quais testes serão executados.

Tipos de Pentest

- **Tandem: (caixa de cristal)**

  Auditor tem total conhecimento sobre o alvo, o alvo sabe que será atacado e o que será feito durante o ataque.

- **Reversal: (equipe de respostas a incidente)**

  Auditor tem conhecimento total do alvo, porém o alvo não sabe que será atacado, e tão pouco sabe quais testes serão executados.

White Hat ≠ Black Hat

Há um mundo de diferença entre os dois lados, essas diferenças podem ser reduzidas a três pontos principais:

- Autorização
- Motivação
- Intenção

Kali e o Backtrack Linux: ferramentas, muitas ferramentas

Fases de um Teste de Invasão

- Levantamento de Informações
- Varredura
- Ganhar acesso
- Manter acesso
- Apagar rastros

Levantamento de Informações

É fase mais importante de um ataque e de um teste de invasão. Baseado no que é descoberto nessa fase, todo o planejamento é realizado e os vetores de ataque definidos.

- Concorrentes
- Nome de Funcionários
- Endereços
- Telefones
- Sites
- Empresas
- Comunidades Sociais

Varredura

O atacante busca informações mais detalhadas do alvo, que permitir enxergar as possibilidades em ganhar acesso ao sistema, através da exploração de alguma falha encontrada.

- Qual sistema operacional o alvo utiliza?
- Quais os serviços estão sendo executados no alvo?
- Quais serviços estão disponíveis para acesso?
- Qual a versão de cada serviço sendo executado?
- Há IDS/IPS na rede?
- Há firewalls na rede?
- Existe uma rede interna e outra externa, como uma DMZ?

Ganhando acesso

O atacante coloca em prática tudo aquilo que planejou a partir das informações obtidas previamente.

- Captura de tráfego de rede
- Ataque de engenharia social
- Ataques às aplicações WEB
- Exploração de sistema operacional

Mantendo acesso

O atacante busca, de alguma forma, manter o acesso conseguido através de seus ataques.

O risco de configurar o sistema, implantando uma backdoors é que outras pessoas podem descobri-las, explorá-las e ganhar acesso facilmente ao sistema comprometido.

Apagar rastros

O atacante apaga todos os seus rastros, todos os registros de operações realizadas dentro do sistema comprometido.

Como o pentester tem AUTORIZAÇÃO para realizar os testes, não é necessário apagar os rastros.

Metodologias existente

- **OSSTMM:** voltada mais para testes em sistemas e infraestrutura.
- **OWASP Testing Guide:** já é específica para testes de invasão em aplicações Web.
- **ISSAF:** foca na análise e Testes de segurança, nas áreas técnicas e gerencial.

Como conduzir um Teste de Invasão

Case Penetration testing

Suponha que você seja um pentester ético trabalhando para uma empresa de segurança. Seu chefe entra em seu escritório e entrega um pedaço de papel a você. “Acabei de conversar com a Gerente daquela empresa por telefone. Ela quer que meu melhor funcionário – ou seja VOCÊ – realize um pentest em sua empresa. Você acena com a cabeça, aceitando a tarefa. Ele sai... Você revira o papel – há apenas uma única palavra escrita:

É uma empresa da qual você nunca tinha ouvido falar antes e não há nenhuma outra informação no papel. E agora?????

Abraham Lincoln, que dizia: *"Se eu tivesse seis horas para derrubar uma árvore, eu gastaria as primeiras quatro horas afiando o meu machado."*

Aspectos legais de um Teste de Invasão

- **Limites do teste:** até onde pode ir;
- **Horários:** períodos de menor utilização ou menos críticos;
- **Equipe de suporte:** caso haja alguém para tomar providências caso alguém ataque tenha efeitos colaterais;
- **Contatos:** ao menos três contatos, com e-mail, endereço e telefone;
- **Permissão assinada:** um documento assinado pelo responsável pela empresa, com os nomes das pessoas da equipe autorizadas a realizar os testes.

Estratégia no Levantamento de Informações

Um levantamento de ativo inclui a interação com o alvo:

O alvo pode gravar nosso endereço IP e registrar nossas atividades em um log. Isso tem uma chance bem alta de ser detectado se estivermos tentando realizar um teste de invasão de maneira discreta.

Estratégia no Levantamento de Informações

O levantamento passivo faz uso da vasta quantidade de informações disponíveis na web.

Quando conduzimos um levantamento passivo, não interagirmos diretamente com o alvo e, desse modo, ele não terá nenhuma maneira de saber, gravar ou registrar nossas atividades em um log.

HTTrack: clonador de sites

O HTTrack é um utilitário gratuito que cria uma cópia **off-line** idêntica do site alvo.

O site copiado inclui todas as páginas, links figuras e o código do site original, porém permanecerá em seu computador local.

HTTrack: clonador de sites

httrack

- Usando o Kali, o site clonado ficará no diretório **/root/websites/<nomedoprojeto>**

- Ao abrir o Firefox inserir na URL **/root/websites/<nomedoprojeto>**

Obs: <nomedoprojeto> deve ser substituído pelo nome que foi usado ao criar a cópia.

Google Hacking

Google Hacking

Google Hacking é a atividade de usar recursos de busca do site, visando atacar ou proteger melhor as informações de uma empresa.

Livros: "Google Hacking for Penetration Testers" e "Google Hacking Database".

Apresentação de **Johnny long** na Defcon 13.

http://www.defcon.org/html/links/dc-archives.html

Comandos Avançados do Google

Para usar adequadamente uma diretiva do Google, três dados são necessários:

1. O nome da diretiva que você quer usar;
2. Dois pontos;
3. O termo que você quer usar com a diretiva.

Hands-on

Localizar páginas potencialmente interessantes:

- intitle:index.of
- inurl:admin
- inurl:login

Busca por conexão VNC:

- intitle:VNC inurl:5800/5900

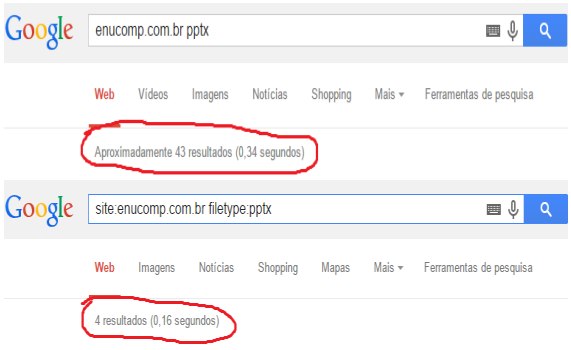
Pesquisar por versão de cache da homepage:

- cache:enucomp.com.br

Buscar por arquivos de base de dados em sites do governo:

- site:gov.br filetype:pptx
- site: gov.br ext: SQL

A eficiência das diretivas no Google



Consultando websites antigos

- www.archive.org

❑ Possibilita que acessemos versões mais antigas de qualquer site que já tenha sido publicado na web.

- **Vamos consultar algum site!**

Webspiders

- http://www.dominio.com.br**/robots.txt**

❑ São programas que navegam automaticamente por websites para coletar informações.

❑ Portanto, os arquivos robots.txt podem revelar informações sobre arquivos e diretórios que poderíamos não conhecer e até mesmo não estando linkado no site.

- **Vamos consultar algum site!**

FootPrint

É a etapa a ser realizada em um teste de intrusão. Durante essa etapa, o Pentester coleta o máximo de informações para alimentar a anatomia de ataque.

Ex: topologia da rede, sistemas operacionais, quantidade de máquinas e localização física.

Podemos dizer que é a fase em que o Pentester se prepara para realizar o ataque.

Footprint:

Em média, um pentester gasta 70% do tempo analizando um alvo levantando informações sobre o mesmo.

Apenas 30% do tempo e usado para realizar o ataque e avaliar a possibilidade de um atacante realizar procedimentos pós-invasão na máquina alvo.

Consulta a informações de domínio

Whois: Conhecer detalhes referentes ao domínio do cliente.

whois <domínio.com.br>

Consulta através da web:

http://registro.br/cgi-bin/whois/

Consultando servidores DNS

Servidores DNS são um alvo excelente para os hackers e os pentesters. Normalmente, esses servidores contêm informações consideradas altamente valiosas pelos invasores.

Consultando servidores DNS

Ferramentas pra extrair informações do DNS.

- host –v –t NS <dominio>
- host –v –t MX <dominio>

- dig NS <dominio>
- dig MX <dominio>

- Dnsenum <dominio> dns.txt **(Transferência de Zona)**
  # cd/pentest/enumeration/dns/dnsenum/
  # ./dnsenum.pl <dominio.com.br> dns.txt

Netcraft

- http://www.netcraft.com

Dentro de alguns serviços que ela fornece está a análise de mercado para empresas de web hosting e servidores web, incluindo detecção do sistema operacional e versão do servidor web,

The Harvester: descobrindo e tirando proveito de end. de e-mail

Essa ferramenta nos permite catalogar de forma rápida e precisa tanto os endereços de e-mail quanto os subdomínios diretamente relacionados ao nosso alvo.

The Harvester: descobrindo e tirando proveito de end. de e-mail

O The Harvester pode ser usado para pesquisas de e-mails, hosts e subdomínios em servidores Google, Bing e PGP, bem como por usuários no LinkedIn.

theharvester **(Kali)**
pentest/enumeration/theharvester **(BackTrack)**

./theharvester.py –d <domínio> -l 10 –b <google, bing, Linkedin> all

Extraindo informações do cabeçalho do e-mail

- Análise de e-mails é normalmente feita pela área de Forense Computacional. Porém, podemos obter informações sobre o host da pessoa,

Extraindo informações do cabeçalho do e-mail

- No cabeçalho é onde encontramos diversos campos com informações de controle, destinatário, remetente, data de envio, dentre outras informações.

- O campo que interessa nós é o campo “Received” onde contem o endereço IP de onde a mensagem de correio eletrônico partiu.

Teste de cabeçalho de e-mail
Sexta-feira, 7 de Maio de 2010 11:56
From Felipe Santos Fri May 7 14:56:10 2010
X-Apparently-To: baphometloki@yahoo.com.br via 67.195.8.190; Fri, 07 May 2010 07:56:36 -0700
Return-Path: <neetfel@gmail.com>
X-YMailISG:
D22GNBEWLDv3S52h.i1n2Q_RMHotyj8fEgkpy6vkLjqgVXe0ou9d8z3JRi_HzPp9ulv8sGxKEFuZJoSGKEjcmpQKNgO2IEl06uKtpgmsDoJngYof4
JakGFNaN1rFAYx38yNwtkzVfpF2P.auE.DUqm
qhkbpAdApCKdbIMNDQFEwnwGoVq1JMtx5jQ0ANyS4z3P1M.0_4_0u2Ne7sbg13Oq9yPuH6b5f4GC6A2ljj0QPOF2Vg.u9Cl5IGztq4IchdE.wFC
ewHWVdxY_vnYzZXxc.Br1ycrag1E08id1tMTdaF2f7kU1OR
u0KAdvm1y72YWXPtLB4c2uX0AKYWgZPoA6O37IvV6lwkLQXT8fQ7AezVgr7DHPblQe1finVguXwmCDFsmCicAx5ph2060NUgA4qah19chxR
RGbT12Q9pkkYaO3lVvZfZQuG8lXedP7dzXJMOwX2GTDm 1wNAUfAp.z0SA--
X-Originating-IP: [209.85.217.219]
Authentication-Results: mta1079.mail.sk1.yahoo.com from=gmail.com; domainkeys=pass (ok); from=gmail.com; dkim=pass (ok)
Received: from 127.0.0.1 (EHLO mail-gx0-f219.google.com) (209.85.217.219) by mta1079.mail.sk1.yahoo.com with SMTP; Fri, 07 May 2010 07:56:36 -0700
Received: by mail-gx0-f219.google.com with SMTP id 19so660108gyk.0 for <baphometloki@yahoo.com.br>; Fri, 07 May 2010 07:56:35 -0700 (PDT)
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=gmail.com; s=gamma; h=domainkey-signature:received:mime-version:received:from:date :message- id:subject:to:content-type; bh=zsRzXjYMy4NDiWycSOHoC4K65BBPQ2mLafsg2/koiuw=;
b=CYkBO1Xf3yKkxCEx7UvNmaW/cWNEMA/r36T4PB1JSK5eVKUJo9C9hR4swWXwiR7viL
TVSM2su9lxQEDeze7exMMS3AMlyhRxzp7QQ68bZ4xoBVuR0RYVlkWUTszHt4dykALpDjJW9xejN3sknjCsTFUp2ObbUqiA6gpELFcIW2I=
DomainKey-Signature: a=rsa-sha1; c=nofws; d=gmail.com; s=gamma; h=mime-version:from:date:message-id:subject:to:content-type;
b=Med0d9Uy5GBRwXazfwundBvqX1ZJNUH8VoLIZhudCurMouAQscyQz5mxE/ig1cyH0L
qe9J5pqC2y27SNjwoqR0eaPVGwRfdg/PCN6DN9IsKvYhVZqKdv9JUVKSAFRZSZ60RswaSHUIJcbqyPXhPXYk6GKNDBAKTC3Ty/4ZnKEXE=
Received: by **10.150.243.17** with SMTP id q17mr4368907ybh.103.1273244190925; Fri, 07 May 2010 07:56:30 -0700 (PDT)
MIME-Version: 1.0
Received: by 10.151.8.14 with HTTP; Fri, 7 May 2010 07:56:10 -0700 (PDT)
From: Este remetente é verificado pelo DomainKeys
Felipe Santos <neetfel@gmail.com>
Adicionar remetente à lista de contatos
Date: Fri, 7 May 2010 11:56:10 -0300
Message-ID: <r2v4da5820810050707 56pc0de571fu78a59b6aa99d4bb2@mail.gmail.com>
Subject: =?ISO-8859-1?Q?Teste_de_cabe=E7alho_de_e=2Dmail?=
To: baphometloki@yahoo.com.br
Content-Type: multipart/alternative; boundary=000e0cd29860b6e12e04860243f6
Content-Length: 482

Varreduras ativas, passivas e furtivas de rede

Objetivos

- Mapear hosts ativos na rede
- Obter versões dos sistemas operacionais
- Identificar os serviços em execução

Motivação

"Cada porta aberta é um **ponto de ataque** em potencial..."

Fingerprint Passivo

❑ Fica "ouvindo" a rede para coletar informações(S.O) sobre os dispositivos.

- Vamos executar o p0f

obs: colocar interface em modo promíscuo

```
# p0f –i eth0 –o log
```

Descobrindo o S.O usando icmp

Um simples **ping** é capaz de revelar o sistema operacional de uma máquina. A informação importante está no campo TTL (**Time To Live**). A maioria dos sistemas operacionais se diferencia pelo valor retornado de TTL

Ping <host> -> Ver TTL

- Linux - Normalmente 64
- Windows - Normalmente 128
- Cisco - Normalmente 255
- Linux + iptables - Normalmente 255

Calculando o HOP

Usando os comandos traceroute e ping conjugados para obter informações, podemos calcular o ttl e descobrir o S.O

traceroute <domínio>

mtr <dominio:>

nmap –v –O <dominio.com.br>

Realiza varredura, buscando ativos, portas abertas e serviços sendo executados.

xprobe2 <dominio.com.br>

Analisa banners de sistemas operacionais, comparando com um banco de dados interno, onde compara-os e informa o S.O. utilizado e a versão do mesmo.

xprobe2 –p TCP:80:open <dominio>

Engenharia Social

Objetivos

- Entender o que é Engenharia Social
- Entender Dumpster Diving
- Entender os riscos associados à Engenharia Social

Engenharia Social

- Arte de enganar pessoas para conseguir informações, as quais não deviam ter acesso.

Tipos de Engenharia Social

❑ **Baseadas em Pessoas**

- Disfarces
- Representações
- Uso de HelpDesk

❑ **Baseadas em Computadores**

- E-mails falsos
- Cavalos de troias anexados a e-mails
- Web site falso

Tipos de ataques

- Insider Attacks
- Roubo de identidade
- Phishing Scam
- Dumpster Diving

Tipos de ataques

- **Insider Attacks:**
  Insiders são pessoas de dentro da própria organização.

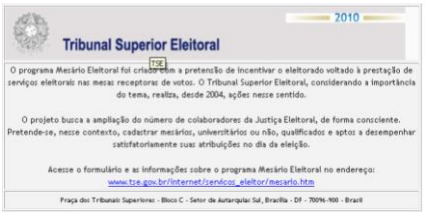
- **Roubo de identidade:**
  Quando alguém cria uma nova identidade baseando-se em informações de outra pessoa, essa identidade é chamada de "laranja".

Tipos de ataques

- **Phishing Scam:**
  É uma forma de fraude eletrônica, caracterizada por tentativas de adquirir informações sigilosas, ou instalar programas maliciosos na máquina alvo.

- **Dumpster Diving:**
  É o ato de vasculhar lixeiras em busca de informações.

Phishing Scam



http://ad.vu/zcfh?www.tse.gov.br/internet/servicos_eleitor/mesario.htm

Engenheiros Sociais

Características humanas exploradas para aplicação da engenharia social:

- ✓ Formação profissional;
- ✓ Vontade de ser útil;
- ✓ Busca por novas amizades;
- ✓ Vaidade pessoal e/ou profissional;

O Básico sobre o SET

Social Engineer Toolkit

O SET é uma framework de exploração de falhas totalmente dedicado a engenharia social, permitindo criar vários vetores sofisticados de ataque.

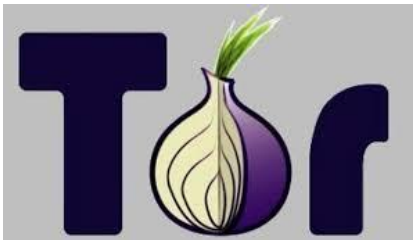
No Kali Linux

se-toolkit

BackTrack

/pentest/exploits/set/

Navegação Anônima



Anonymizer

- Os programas de anonymizer funcionam basicamente mascarando o IP fazendo com que se navegue utilizando um proxy externo, fornecendo o dele como IP real.

- Versões pra Linux e Windows
  TOR – The Onion Router
  - http://www.torproject.org/

- Acesse o site **http://www.geoiptool.com** e veja se o IP está diferente, assim como o local de onde está acessando.

Enumeração de Informações e Serviços

Objetivos

- Mapear a rede
- Descobrir serviços e versões sendo executadas no sistema alvo.
- Facilitando a posterior pesquisa de vulnerabilidades e exploits específicos.

Enumeração

- As técnicas de enumeração são utilizadas como um complemento às fases de **fingerprint** e **varredura.**
- Além disso, na fase de enumeração, mapeamos toda a rede do alvo, descobrindo os pontos falhos e onde podemos explorar para conseguir acesso a informações estratégicas.

Técnicas Clássicas

Sem utilizar ferramentas específicas, é possível conseguir informações dos serviços que estão sendo executados em determinada porta.

Obtendo banner de um servidor ftp:

#ftp <IP MT>

Obtendo banner de um servidor de e-mail:

#telnet <IP MT> 25

Capturando banner de aplicações (de forma ativa)

nmap –sV –O <IPMT> -p 25

xprobe2 –p TCP:80:open <IPMT>

amap <IP MT> <porta>

Mapeando graficamente a rede

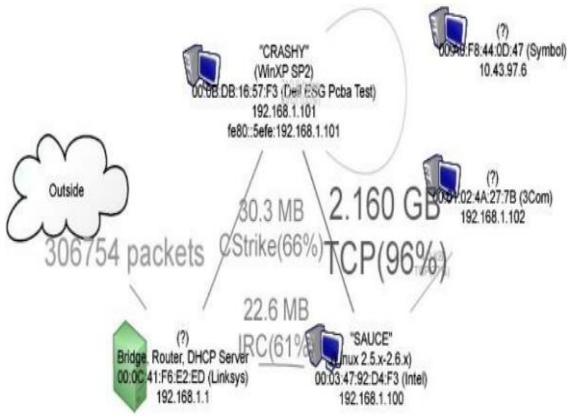
Abordaremos nos tópicos seguinte exemplos de ferramentas existentes no Backtrack 5 R3 que permitem mapear a rede graficamente.

Ferramentas

- Lanmap2
- AutoScan

Ferramentas

- **Lanmap2:**
  Varre toda a rede e captura pacotes, criando ao longo de sua execução um arquivo .PNG com o mapa da rede, informando graficamente a relação das máquinas encontradas.



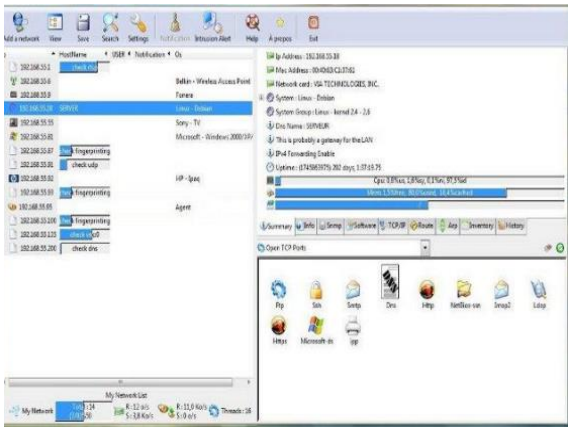
Mapeando graficamente a rede

- **Lanmap2**

pentest/enumeration/lanmap2/src
./cap (capturar informações da rede alvo)

pentest/enumeration/lanmap2/graph
./graph.sh (permite gerar o gráfico da captura)

pentest/enumeration/lanmap2/graph
net.png → Arquivo gerado



Ferramentas

- **AutoScan:**
  Faz varredura na rede e informa hosts ativos, portas abertas e serviços sendo executados. Funciona através de uma interface gráfica.

Vulnerabilidades em Aplicações Web

OWASP
The Open Web Application Security Project

Objetivos

- Entender o funcionamento das aplicações web.
- Aprender a explorar as principais classes de vulnerabilidades em aplicações web.

Conceito

- Aplicações web são programas que ficam em um servidor web e executam tarefas para dar uma resposta ao usuário.
- Webmails, web fóruns, blogs, Lojas virtuais etc... são exemplos de aplicações web.

Por que é tão perigoso?

- Aplicações web são críticas para a segurança de um sistema porque usualmente elas estão conectadas com uma base de dados que contém informações tais como cartões de crédito e senhas.

Principais Classes de Vulnerabilidades

- Baseado no **TOP 10 OWASP**, que é um ranking das 10 maiores vulnerabilidades WEB atualizado anualmente, seguem abaixo as vulnerabilidades mais exploradas em aplicações WEB:

Top 10 OWASP

- **SQL Injection**
- Command Injection
- Cross Site Scripting (XSS)
- Insecure Direct Object Reference
- Falha de Autenticação e gerenciamento de sessão
- Falhas em configuração de segurança
- Insecure Cryptographic Storage
- Failure to Restrict URL Access
- Insufficient Transport Layer Protection
- Unvalidated Redirects and Forwards

SQL Injection

- **SQL Injection** é um problema que ocorre quando o programa não filtra caracteres especiais enviados pelo usuário antes de fazer a requisição para o banco de dados, enviando caracteres que serão interpretados pelo banco de dados.

Vamos analisar o trecho do código abaixo:

```
Select * from usuarios where username = '" + username + "' and password
= '" + password "';
```

Como ficaria a chamada no banco de dados se enviássemos no username e password o conteúdo: ‘ or ‘1’=‘1

Resposta:

```
Select * from usuarios where username = '' or '1'='1' and password = '' or
'1'='1';
```

Como **1** é sempre igual a **1**, teremos uma “verdade” e passaremos pela checagem.

Exemplos de SQL Injection

- 'or '1
- 'or '1'='1
- 'or 1=1-'or''='
- 'or 'a'='a
- ') or ('a'='a
- 'or '=1

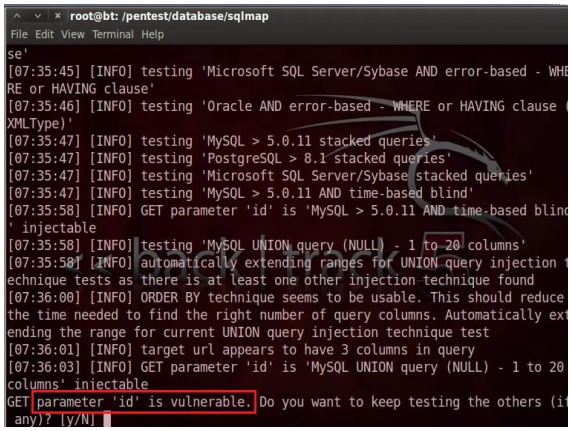
Sqlmap

Exemplo:
http://dominio.com.br/?paginas=conteudo&id=**10**

cd /pentest/database/sqlmap

Executar: (tentar extrair o nome da base de dados)

./sqlmap.py --url http://dominio.com.br/?paginas=conteudo&id=**10** **--current-db**



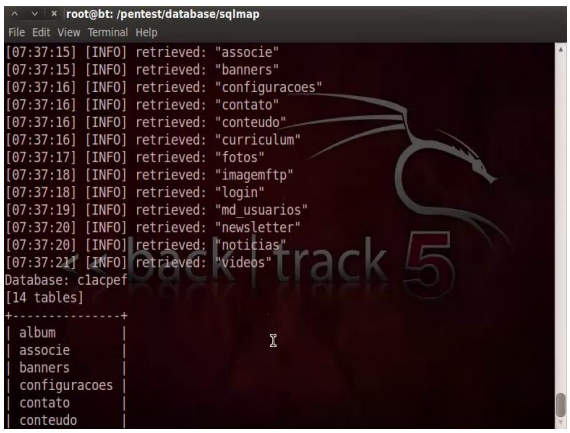
Sqlmap

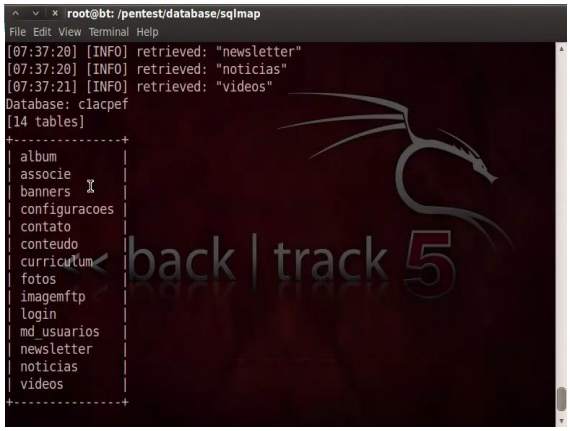
Exemplo:
http://dominio.com.br/?paginas=conteudo&id=**10**

cd /pentest/database/sqlmap

Executar: (tentar extrair tabelas)

./sqlmap.py --url http://dominio.com.br/?paginas=conteudo&id=10 **–D ‘c1acpef’ -- tables**





Sqlmap

Exemplo:
http://dominio.com.br/?paginas=conteudo&id=**10**

cd /pentest/database/sqlmap

Executar: (tentar extrair colunas da tabela "login")

./sqlmap.py --url http://dominio.com.br/?paginas=conteudo&id=10 **–D 'c1acpef' –T 'login' -- columns**

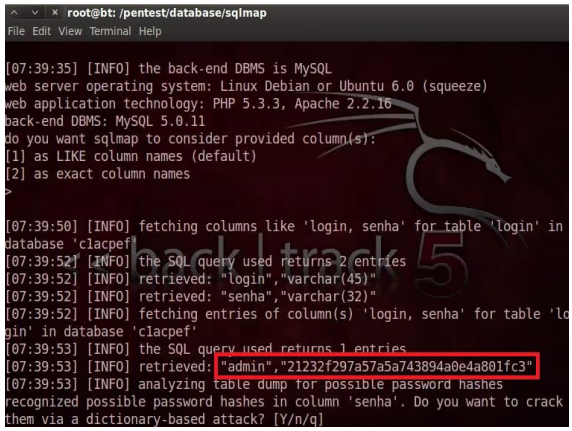
Sqlmap

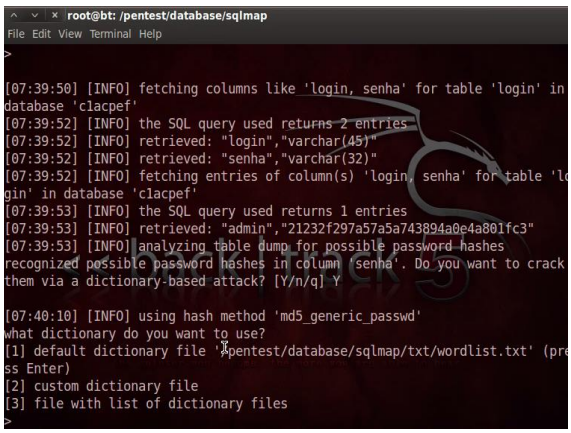
Exemplo:
http://dominio.com.br/?paginas=conteudo&id=**10**

cd /pentest/database/sqlmap

Executar: (extrair os dados de "login,senha")

./sqlmap.py --url http://dominio.com.br/?paginas=conteudo&id=10 **–D 'c1acpef' –T 'login' –C 'login,senha' --dump**





Testando o Sistema

Objetivos

- Entender o que é DoS, DDoS.
- Entender como ocorrem ataques de negação de serviço.

Denial of Service Attack

- Qualquer tipo de ataque que afete o pilar "**Disponibilidade**" da tríade Confidencialidade-Integridade-Disponibilidade, pode ser considerado um ataque de negação de serviço.
- **Exemplos:**

*****puxar a tomada de alimentação de energia de um servidor.

*****até utilizar uma rede zumbi para ataque em massa.

- Na maior parte das vezes, o objetivo do atacante não é conseguir acesso à informações, roubo de dados, ou tomar o controle da máquina.
- O **objetivo** é realmente causar a indisponibilidade de serviços nos sistemas do alvo, e isso pode levar a potenciais prejuízos financeiros, do ponto de vista comercial, por exemplo.

DoS

- Tentativas de impedir usuários legítimos de utilizarem um determinado serviço de um computador.
- Quando um computador/site sofre ataque DoS, ele não é invadido, mas sim sobrecarregado.

DoS

- Realizado através de um único computador.
- **Ping da Morte:** envia pacotes de tamanho elevado e numa frequência também alta (milhares de vezes por segundo).

- **Ping da Morte**

ping -i 1 -l 65500 (ip de destino ou nome host) -t

-i 1 - o intervalo entre cada ping. No caso, 1 ms.

-l 65500 - o tamanho do pacote, em bytes **(este é o maior tamanho possível)**.

alvo - o IP ou o nome (se houver uma tabela de hosts ou um servidor DNS disponível) do destino.

-t enviar a requisição por tempo indeterminado ou até usuario cancelar (CONTROL + C)

Exemplos de DoS

- $ **:(){ :|:& };:**
- $ dd if=/dev/zero of=/var/spool/mail/meu_usuario
- $ perl – e 'while (1) { fork();
  - open $fh, "</proc/meminfo";
  - open $hf, ">/tmp/bla"; }'
- $ dd if=/dev/urandom of=/dev/mem
- $ perl -e 'fork while fork'

Em Windows:
- Em um .bat: %0|%0

Ou:
- :s
- start %0
- goto :s

Fork_Bomb

:(){ :|:& };:

Fork_Bomb :(){ :|:& };:

Cria uma função
função **:(){**

Dentro dela chama ela mesma e direciona a saida pra ela mesma "Looping"
função **:|:** função **&**

E depois chama a função
};: função

Ferramenta DoS

C4

- Ferramenta que gera ataques de DoS em redes locais com SYN Flood.

 # ./c4 -h [ip_alvo]

Parâmetros:

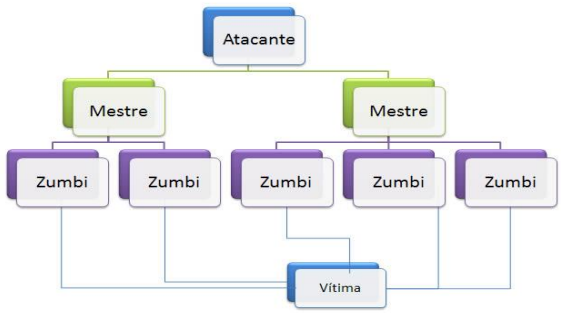
-h destination ip/host
-p destination port range [start,end]
-t attack timeout
-l % of box link to use

DDoS

- É um ataque DoS ampliado, ou seja, que utiliza até milhares de computadores para atacar um determinado alvo.

- Esse é um dos tipos mais eficazes de ataques e já prejudicou sites conhecidos, tais como os da **CNN**, **Amazon**, **Yahoo**, **Microsoft, Sony, eBay...**

Modelo de ataque - DDoS



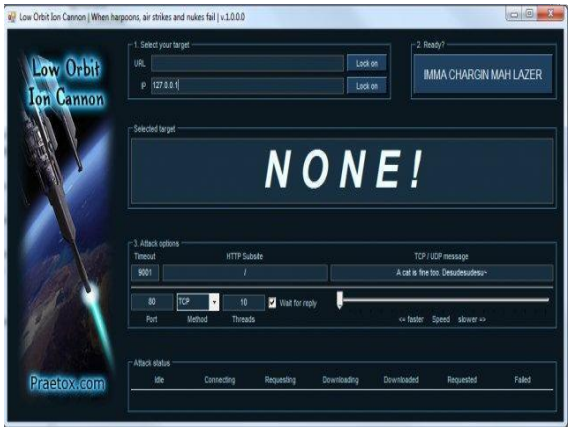
Ferramenta DDoS

- **Loic**
- **SlowLoris**
- **t50**

Ferramentas DDoS

- **Loic** (**Windows**, Mac e Linux)
- **Funcionamento:**
  O site alvo é inundado com pacotes de requisição TCP ou UDP com a intenção de sobrecarregar o servidor, fazendo com que ele deixe de responder às requisições legítimas.

É frequente o uso de **botnets** para efetuar ataques através do LOIC.



Ferramentas DDoS

- **SlowLoris**

Funcionamento:
Tentar manter muitas conexões aberta com servidor web destino e mantê-los abertos o maior tempo possível até encher o máximo de conexões simultânea.

 # perl slowloris.pl –dns <domínio>

Ferramentas DDoS

Ferramentas DDoS

- **t50** criada pelo brasileiro **Nelson Brito** no intuito de fazer testes de invasão e estabilidade de uma rede ou sistema.

Funcionamento:
Envia um numero altíssimo de requisições de pacotes, de tal forma que o alvo não consiga atender a todas requisições ou as atenda de forma lenta, dessa forma o alvo pode cair ou ficar lento..

 # ./t50 <dominio> --turbo --syn --flood

Ferramentas DDoS

Atualmente o t50 é capaz de emitir as seguintes requisições:

- Mais de 1.000.000 (1 milhão) de pacotes por segundo de SYN Flood (+50% do uplink da rede) em uma rede 1000BASE-T (Gigabit Ethernet).
- Mais de 120.000 pacotes por segundo de SYN Flood (+60% do uplink da rede) em uma rede 100BASE-TX (Fast Ethernet).

Recomendações

Exceto em casos que o cliente solicite tal tipo de ataque, não devemos realizar esse ataque, pois pode prejudicar os negócios da empresa.

OBRIGADO!!!!!

http://www.facebook.com/nettfel

neetfel@gmail.com

http://www.linkedin.com/in/fesantos

@nettfel