

Luiz Vieira – luizwt@gmail.com

Ferramentas Livres para Teste de Invasão

Apresentação de ferramentas livres para as
diversas fases de um teste de invasão.

Quem sou eu?

- Nome
- Formações
- Experiências



Definições

Indo além da análise de vulnerabilidades...



Categorias de Avaliações

- Toda organização utiliza diferentes tipos de avaliações de segurança para avaliar o nível de segurança de seus sistemas.
- As categorias de avaliações são: auditoria de segurança, análise de vulnerabilidades, e teste de invasão.
- Cada tipo de avaliação requer que as pessoas que conduzem-na, tenham diferentes habilidades.

Teste de Invasão

- Um teste de invasão avalia o modelo de segurança da organização como um todo.
- Revela potenciais consequências de um ataque real que obtêm sucesso ao “quebrar” a segurança da rede.
- Um profissional que realiza testes de invasão se diferencia de um atacante apenas por seu intento e ausência de atitudes maliciosas.



Tipos de Teste de Invasão

- **Teste Externo**

- Avalia a disponibilidade de informações públicas, enumera os serviços da rede, e o comportamento dos dispositivos de segurança analisados.

- **Teste Interno**

- Realizado a partir de pontos de acesso na rede, representando cada segmento físico e lógico.
 - Black box = zero conhecimento
 - Grey box = conhecimento parcial
 - White box = conhecimento total

Metodologias



OSSTMM - Open Source Security Testing Methodology Manual



OWASP - Open Web Application Security Project



NIST 800.42 - Guideline on Network Security Testing



ISSAF - Information Systems Security Assessment Framework

Escopo do Teste



Definição do escopo

- Determinar o escopo do teste de invasão é essencial para decidir se o teste será um teste direcionado ou um teste global.
- Avaliações globais, são esforços coordenados pelo profissional para descobrir tantas vulnerabilidades quanto possível no sistema/organização avaliado.
- O teste direcionado, buscará identificar vulnerabilidades em um sistema específico.
- A definição de escopo determinará também:
 - A extensão do teste;
 - O quê será avaliado;
 - A partir de onde será testado;
 - Por quem será avaliado.

Tiger Team



Blue Team

- Realiza o teste de invasão com o conhecimento e consentimento do setor de TI da organização.
- Tem menor custo e é o mais frequentemente utilizado.
- O papel primário é pensar sobre como ataques surpresa podem ocorrer.



Red Team

- Realiza o teste de invasão sem o conhecimento do setor de TI da empresa, e com o consentimento da alta gerência.
- Pode ser conduzido com ou sem o aviso (teste anunciado ou não).
- Propõe-se a detectar vulnerabilidades da rede e do sistema, e avaliar a segurança pelo ponto de vista do atacante no que diz respeito à rede, ao sistema ou o acesso a informação.



Fases do Teste de Invasão



Fases

- I. Aquisição de informação
- II. Varredura
- III. Ganhar acesso
- IV. Manter acesso
- V. Apagar rastros

Técnicas comuns para Testes de Invasão

- Pesquisa passiva
- Monitoramento de atividades públicas
- Mapeamento de rede e SO's
- Spoofing
- Sniffing de rede
- Ataques com trojan
- Ataques de força bruta
- Análise de vulnerabilidades
- Análise de cenário

Ferramentas

Teste de Invasão e Hacking Ético



Aquisição de Informações

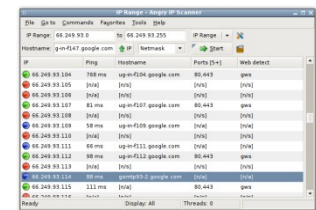
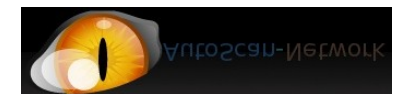
- **Maltego** - O Maltego é simplesmente uma das melhores ferramentas open source de network discovery e relational networks que permite reunir vários tipos de informações.
 - <http://www.paterva.com/web4/index.php/maltego>



- **Binging** – Binging é uma ferramentas simples de busca no sistema Bing.
 - <http://www.blueinfy.com/tools.html>

Scanner de rede e enumeração

- **Nmap** - Network Mapper é uma ferramenta livre e de código aberto para exploração de rede e auditoria de segurança.
 - <http://www.nmap.org>
- **Netifera** - Netifera é uma plataforma modular de código aberto para a criação de ferramentas de segurança de rede.
 - <http://netifera.com>
- **AutoScan** - AutoScan-Network é um scanner de rede. Seu principal objetivo é gerar uma lista de equipamentos conectados na rede.
 - <http://autoscan-network.com>
- **Angry IP Scanner** - Angry IP Scanner é um scanner de rede multiplataforma desenvolvido para ser simples e rápido. Varre Ip's e portas dentre outras características.
 - <http://www.angryip.org>



Scanner de vulnerabilidades

- **Nessus** - É um scanner de vulnerabilidades que possui, inclusive, uma linguagem própria para o desenvolvimento de plugins próprios, a NAS
 - <http://www.nessus.org>
- **NeXpose** - NeXpose é uma solução unificada que escanea a rede para identificar os dispositivos executados para testá-los em busca de vulnerabilidades.
 - <http://community.rapid7.com>
- **OpenVAS** - Open Vulnerability Assessment System é um scanner de segurança de rede com ferramentas associadas como uma GUI, por exemplo.
 - <http://www.openvas.org>
- **SARA** - O Security Auditor's Research Assistant (SARA) é uma ferramentas de rede para análise de segurança.
 - <http://www-arc.com/sara/>



Análise de Tráfego

- **Wireshark** - Ferramenta para análise de protocolo de rede.
 - <http://www.wireshark.org/>
- **Tcpdump** - Captura tráfego de rede.
 - <http://www.tcpdump.org/>
- **Ettercap** - Ettercap é uma suite para ataques man in the middle em LAN's. Fareja conexões ativas, filtra conteúdos "on the fly" e muitas outras coisas interessantes.
 - <http://ettercap.sourceforge.net/>
- **Dsniff** - dsniff é uma coleção de ferramentas de rede para auditoria e teste de invasão.
 - <http://monkey.org/~dugsong/dsniff/>



Scanner de aplicação

- **W3AF** - w3af é o Web Application Attack and Audit Framework. O objetivo do projeto é criar um framework para buscar e explorar vulnerabilidades de aplicações web.

- <http://w3af.sourceforge.net>

- **Samurai WTF** - O Samurai Web Testing Framework é um ambiente live Linux previamente configurado para funcionar como um ambiente de web pen-testing..

- <http://samurai.inguardians.com>

- **Nikto** - web server scanner que realiza testes contra múltiplos ítems em servidores web.

- <http://cirt.net/nikto2>

- **Paros** - Através do Paros proxy, todos os dados HTTP e HTTPS entre o cliente e o servidor, incluindo cookies e campos de formulários, podem ser interceptados e alterados.

- <http://www.parosproxy.org/>



Frameworks para exploração (exploiting)

- **Metasploit** – Este projeto foi criado para fornecer informações sobre técnicas de exploração e criar uma reconhecida base funcional para desenvolvedores de exploits e profissionais de segurança.
 - <http://www.metasploit.org>
- **Exploit DB** – Arquivo de exploits e software vulneráveis. Uma imensa fonte para pesquisadores de vulnerabilidades e interessados por segurança.
 - <http://www.exploit-db.com>



Wireless Hacking

- **OSWA** - Organizational Systems Wireless Auditor
 - <http://securitystartshere.org/page-training-oswa.htm>
- **AirCrack-NG Suite** - Aircrack-ng é um programa para quebra de chaves 802.11 WEP e WPA-PSK que pode capturá-las uma vez que um número suficiente de pacotes de dados tenha sido capturado.
 - <http://www.aircrack-ng.org>
- **AiroScript-NG** - Airoscript é “text-user-interface” para aircrack-ng. Uma ótima ferramenta para tornar sua vida mais fácil durante um pentest em redes wireless.
 - <http://airoscript.aircrack-ng.org>



Live CDs

- **BackTrack 4** - BackTrack é uma distribuição Linux que possui um arsenal de ferramentas para testes de invasão.
 - <http://www.backtrack-linux.org/>
- **Katana** - Katana é uma suíte portátil multiboot de segurança. Inclui distribuições com foco em Teste de Invasão, Auditoria, Forense, Recuperação de Sistema, Análise de Rede, Remoção de Malware e outras coisas mais.
 - <http://www.hackfromacave.com/katana.html>
- **Matriux** - É uma distribuição de segurança, caracterizando-se inteiramente em ferramentas gratuitas, poderas e open-source, que podem ser usadas para os mais diversos fins, como por exemplo, testes de invasão, para hackers éticos, para administração de sistemas e rede, para investigações forenses de crimes cibernéticos, análise de vulnerabilidades e muito mais.
 - <http://www.matriux.com>



Auditoria de sistemas Windows

- **Oval Interpreter** - O Open Vulnerability and Assessment Language Interpreter é uma implementação livre de referência que demonstra a avaliação das OVAL Definitions. Baseado no conjunto de definições o interpretador coleta informações do sistema, avalia-as e gera um arquivo detalhado de resultado.
 - <http://oval.mitre.org>
- **Nessus Local Plug-ins** - <http://www.nessus.org>



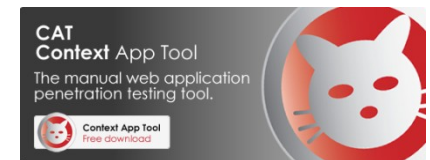
Auditoria de sistemas Unix

- **Lynis** - Lynis é uma ferramenta para auditoria Unix. Vasculha o sistema e software disponíveis para detectar problemas de segurança. Além de informações sobre segurança, também varre em busca de informações gerais do sistema, pacotes instalados e erros de configuração.
 - <http://www.rootkit.nl>
- **CIS Scoring tools** - CIS-CAT é uma ferramenta de auditoria e análise de configuração de hosts. Inclui tanto uma interface de comando, quanto interface gráfica.
 - <http://www.cisecurity.org>
- **OpenSCAP** - SCAP é um conjunto de padrões gerenciados pelo NIST com o objetivo de prover uma linguagem padronizada relacionada à Defesa de Redes de Computadores. OpenSCAP é um conjunto de bibliotecas de código aberto que permite uma fácil integração do padrão SCAP.
 - <http://www.open-scap.org>



Avaliação de aplicações

- **BurpSuite** – é uma plataforma integrada para ataque e teste de aplicações web.
 - <http://portswigger.net>
- **Websecurify** – automaticamente identifica aplicações web vulneráveis através da utilização de tecnologia fuzzing e advanced discovery.
 - <http://www.websecurify.com>
- **CAT The Manual Web Application Audit**
 - é uma aplicação para facilitar testes de invasão manuais em aplicações web.
 - <http://cat.contextis.co.uk>



Análise de senhas

- **OphCrack** - programa livre para quebra de senhas Windows baseado em rainbow tables.
 - <http://ophcrack.sourceforge.net>
- **John the Ripper** - programa rápido para quebra de senhas.
 - <http://www.openwall.com/john>
- **THC-Hydra** - *network logon cracker* multiplataforma que faz ataques de força bruta contra uma gama considerável de serviços.
 - <http://www.thc.org/thc-hydra/>



Auditoria de Banco de Dados

- **DB Audit Free Edition** - ferramenta de auditoria e análise de segurança para bancos de dados Oracle, Sybase, DB2, MySQL e Microsoft SQL Server.
 - <http://www.softtreetech.com>
- **SQL Map** - ferramenta automática em linha de comando para testes de sql-injection.
 - <http://sqlmap.sourceforge.net>
- **Wapiti** - Wapiti permite realizar auditoria de segurança de aplicações web.
 - <http://wapiti.sourceforge.net>



Auditoria de telefonia VOIP

- **VAST Viper** - VAST é uma distribuição que contém ferramentas desenvolvidas pela VIPER tais como UCsniff, videojak, videosnarf e outras mais. Juntamente com as ferramentas VIPER e outras ferramentas essenciais de segurança VOIP, também há ferramentas de testes de invasão tais como Metasploit, Nmap e Hydra.
 - <http://vipervast.sourceforge.net>
- **WarVox** – é uma suíte de ferramentas para explorar classificar e auditor sistemas de telefonia.
 - <http://warvox.org>



**Esperamos que tenham
gostado!**



Obrigado!
luizwt@gmail.com