**TAREFA PRÁTICA DE AVALIAÇÃO DE FERRAMENTAS**

**Scanner de Vulnerabilidades de Redes**

|  |
| --- |
|  |
|  |  |

**SARA** - O Security Auditor's Research Assistant (SARA) é uma ferramentas de rede para análise de segurança: <http://www-arc.com/sara/>

OpenVAS –

Nessus -

 **Scanner de Aplicação Web**

**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](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](http://samurai.inguardians.com/)

**Paros** – Através do proxy Paros, 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/>

**Websecurify**  - is a powerful web application security testing environment designed from the ground up to provide the best combination of automatic and manual vulnerability testing technologies.

**Avaliação da Segurança em Aplicações Web**

**Burp Suite** - Burp Suite is an integrated platform for performing security testing of web applications. Download: <http://portswigger.net/burp/download.html>

1. [**Web Application Firewall (WAF) Testing Framework**](http://www.imperva.com/products/wsc_web-application-firewall-testing-framework.html)
Do you know if your applications are safe? The Web Application Firewall (WAF) Testing Framework is a free software tool that enables you to evaluate the security efficacy of your Web application security solution. Unlike application scanners, which only check for vulnerabilities, the WAF Testing Framework generates both legitimate traffic and attack traffic to determine if your security solution stops attacks without blocking valid requests.
2. [**Imperva Incapsula Trial**](http://www.imperva.com/products/wsc_incapsula.html)
Worried about Web application attacks like SQL injection or Cross Site Scripting (XSS)? Trying to become PCI 6.6 compliant? Request a trial of Imperva Incapsula, an easy and affordable service designed to provide midsized businesses with best of breed protection for their critical web assets. Imperva Incapsula integrates three effective web solutions – a Web Application Firewall (WAF), a DDoS mitigation service, and a content delivery network (CDN) — into a single cloud-based service that ensures malicious traffic is blocked before reaching Websites, and legitimate traffic is accelerated – creating a more secure, more enjoyable experience for Website visitors.

**Websecurify** – automaticamente identifica aplicações web vulneráveis através da utilização de tecnologia *fuzzing* e *advanced discovery*. [http://www.websecurify.com](http://www.websecurify.com/)

**Wapiti** - *Wapiti* permite realizar auditoria de segurança de aplicações web. [http://wapiti.sourceforge.net](http://wapiti.sourceforge.net/)

**Netsparker** - is a web application security scanner, with support for both detection and exploitation of vulnerabilities. It aims to be false positive–free by only reporting confirmed vulnerabilities after successfully exploiting or otherwise testing them.

 **Multillidae -

Maltego -**

 **Auditoria de Bancos 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](http://www.softtreetech.com/)

**SQL Map** – ferramenta automática em linha de comando para testes de *sql-injection*. sqlmap is an open source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of back-end database servers. It comes with a broad range of features, from database fingerprinting to fetching data from the DB and even accessing the underlying file system and executing OS commands via out-of-band connections. [http://sqlmap.sourceforge.net](http://sqlmap.sourceforge.net/)

[**Scuba: A Free Database Vulnerability Scanner**](http://www.imperva.com/products/dsc_scuba-database-vulnerability-scanner.html)
Download Scuba by Imperva, a free tool that scans leading enterprise databases for security vulnerabilities and configuration flaws, including patch levels. Reports deliver actionable information to reduce risk, and regular software updates ensure that Scuba keeps pace with new threats. Scuba offers nearly 1,200 assessment tests for Oracle Database, Microsoft SQL Server, SAP Sybase, IBM DB2, Informix and MySQL.
<http://www.imperva.com/products/dle_downloads-and-evaluations-overview.html>

HAVIJ *- Havij is an automated SQL Injection tool that helps penetration testers to find and exploit SQL Injection vulnerabilities on a web page.

It can take advantage of a vulnerable web application. By using this software user can perform back-end database fingerprint, retrieve DBMS users and password hashes, dump tables and columns, fetching data from the database, running SQL statements and even accessing the underlying file system and executing commands on the operating system.

The power of Havij that makes it different from similar tools is its injection methods. The success rate is more than 95% at injectiong vulnerable targets using Havij.

The user friendly GUI (Graphical User Interface) of Havij and automated settings and detections makes it easy to use for everyone even amateur users.*

 [Havij v1.15 Free](http://www.itsecteam.com/files/havij/Havij1.15Free.rar)

 [Downlaod Help (pdf format)](http://www.itsecteam.com/files/havij/havij_help-english.pdf)

**Honeypots**

**Honeyd -** Honeyd is a small daemon that creates virtual hosts on a network. The hosts can be configured to run arbitrary services, and their personality can be adapted so that they appear to be running certain operating systems. Honeyd enables a single host to claim multiple addresses - I have tested up to 65536 - on a LAN for network simulation. Honeyd improves [cyber security](http://www.citi.umich.edu/u/provos/cybersecurity/)by providing mechanisms for threat detection and assessment. It also deters adversaries by hiding real systems in the middle of virtual systems. Honeyd is open source software released under GNU General Public License. <http://www.honeyd.org/>

**IDS Intrusion Detection System / IPS (Intrusion Prevent System)**

OSSEC HIDS - performs log analysis, integrity checking, rootkit detection, time-based alerting and active response. In addition to its IDS functionality, it is commonly used as a SEM/SIM solution. Because of its powerful log analysis engine, ISPs, universities and data centers are running OSSEC HIDS to monitor and analyze their firewalls, IDSs, web servers and authentication logs.

SNORT -

**Testes de Invasão (Explotation)**Metasploit Framework **Metasploit** took the security world by storm when it was released in 2004. It is an advanced open-source platform for developing, testing, and using exploit code. The extensible model through which payloads, encoders, no-op generators, and exploits can be integrated has made it possible to use the Metasploit Framework as an outlet for cutting-edge exploitation research. It ships with hundreds of exploits, as you can see in their [list of modules](http://www.metasploit.com/modules/). This makes writing your own exploits easier, and it certainly beats scouring the darkest corners of the Internet for illicit shellcode of dubious quality. One free extra is [Metasploitable](https://community.rapid7.com/docs/DOC-1875), an intentionally insecure Linux virtual machine you can use for testing Metasploit and other exploitation tools without hitting live servers. <http://www.metasploit.com/>

**SET** - The Social-Engineer Toolkit (SET) was created and written by the founder of TrustedSec. It is an open-source Python-driven tool aimed at penetration testing around Social-Engineering. SET has been presented at large-scale conferences including Blackhat, DerbyCon, Defcon, and ShmooCon. With over two million downloads, SET is the standard for social-engineering penetration tests and supported heavily within the security community.
<https://github.com/trustedsec/social-engineer-toolkit/set/>
<https://www.trustedsec.com/downloads/social-engineer-toolkit/>

 **Ferramentas de Análise de Tráfego**

**Dsniff** - dsniff é uma coleção de ferramentas de rede para auditoria e teste de invasão: <http://monkey.org/~dugsong/dsniff/>

Ettercap - is a suite for man in the middle attacks on LAN. It features sniffing of live connections, content filtering on the fly and many other interesting tricks. It supports active and passive dissection of many protocols (even ciphered ones) and includes many feature for network and host analysis. <http://ettercap.sourceforge.net/>

**Wireshark -**

**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](http://oval.mitre.org/)

 **Microsoft Security Compliance Manager**

<http://technet.microsoft.com/en-us/library/jj898542.aspx>

Launch the download of [Security Compliance Manager 3.0](http://go.microsoft.com/fwlink/?LinkId=182512).

Learn more about the [Security Compliance Manager 3.0](http://go.microsoft.com/fwlink/?LinkId=113940).

The **Microsoft Security Compliance Manager 3.0** download includes the following components:

* **Security\_Compliance\_Manager\_Setup.exe –**The Microsoft Security Compliance Manager allows you to view, update, and export security baselines.
* **LocalGPO.msi –**This tool is designed to manage local Group Policy on a computer by applying a security baseline and exporting the local Group Policy.
* After you download and install the SCM 3.0 tool, you can view all available Microsoft product security baselines. For more information, refer to the getting started guidance in the [SCM TechNet Wiki](http://go.microsoft.com/fwlink/?LinkId=201324).

The .cab file for the Windows Server 2012 Security Compliance Baseline includes the following components:

* WS2012 AD Certificate Services Server Security 1.0
* WS2012 DHCP Server Security 1.0
* WS2012 DNS Server Security 1.0
* WS2012 Domain Controller Security Compliance 1.0
* WS2012 Domain Security Compliance 1.0
* WS2012 File Server Security 1.0
* WS2012 Hyper-V Security 1.0
* WS2012 Member Server Security Compliance 1.0
* WS2012 Network Policy and Access Services Security 1.0
* WS2012 Print Server Security 1.0
* WS2012 Remote Access Services Security 1.0
* WS2012 Remote Desktop Services Security 1.0
* WS2012 Web Server Security 1.0
* Windows Server 2012 Security Guide.docx
* Windows Server 2012 CCE Reference.xlsm

Attack Surface Analyzer (Analise de Vulnerabilidades no Windows) <http://www.octaviocampanol.com/2012/08/analise-de-vulnerabilidades-no-windows.html>

O Microsoft  **Attack Surface Analyzer** foi desenvolvido pelo grupo Trustworthy Computing Security e é a mesma ferramenta usada por diferentes equipes da empresa para catalogar as mudanças feitas na superfície de ataque do sistema operacional por softwares instalados pelos usuários.
O aplicativo registra o estado do Sistema operacional antes e depois da instalação de softwares e exibe as mudanças feitas em alguns elementos chave do Windows.
Assim os profissionais de TI podem analisar os resultados para saber quais mudanças podem deixar o Windows vulnerável.
Sistemas operacionais suportados: Windows 7, Windows 8, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Vista.

|  |  |
| --- | --- |
| http://1.bp.blogspot.com/-itu-3a_K0J8/UCQwzhG2HaI/AAAAAAAAAZI/QLaIVXHHb7A/s1600/Button-Download-icon.png     | **Download:** Microsoft Attack Surface Analyzer v1.0 -[**x86**](http://download.microsoft.com/download/1/4/F/14FE12D0-7D89-45DE-BD98-EF497D66BE5D/Attack_Surface_Analyzer_x86.msi) |
| http://1.bp.blogspot.com/-itu-3a_K0J8/UCQwzhG2HaI/AAAAAAAAAZI/QLaIVXHHb7A/s1600/Button-Download-icon.png     | **Download:** Microsoft Attack Surface Analyzer v1.0 - [**x64**](http://download.microsoft.com/download/1/4/F/14FE12D0-7D89-45DE-BD98-EF497D66BE5D/Attack_Surface_Analyzer_x64.msi) |
|  |  |