

## 目录

<b>1 Tools for Hackers</b>	<b>1</b>
1.1 网络工具 (Networking Tools)	1
1.2 攻击工具 (Offensive Tools)	1
1.3 防御工具 (Defensive Tools)	2
1.4 取证/逆向工程工具 (Forensics/Reverse Engineering Tools)	2
1.5 加密工具 (Encryption Tools)	3

## 1 Tools for Hackers

### 1.1 网络工具 (Networking Tools)

1. Nmap: 一个用于网络发现和安全审计的开源工具。 \ <https://nmap.org>]
2. Wireshark: 一个流行的网络协议分析器，用于捕获和交互式浏览网络流量。 \ <https://wireshark.org>]
3. Maltego: 一种开源情报 (OSINT) 和取证应用程序，用于连接数据点并分析网络中的关系。 \ <https://maltego.com>]

### 1.2 攻击工具 (Offensive Tools)

1. Aircrack-ng: 一组用于Wi-Fi网络安全评估的工具，主要用于破解WEP和WPA-PSK密钥。  
<https://aircrack-ng.org>]
2. Metasploit: 一个渗透测试框架，用于开发和执行安全漏洞利用。  
<https://metasploit.com>]
3. Burp Suite: 一个集成的平台，用于Web应用安全测试。  
<https://portswigger.net/burp>]

4. OWASP ZAP (Zed Attack Proxy): 一个开源的Web应用程序安全扫描工具, 主要用于发现Web应用中的安全漏洞。  
<https://zapproxy.org>

### 1.3 防御工具 (Defensive Tools)

1. Snort: 一个开源的网络入侵检测系统 (IDS), 可以实时流量分析和数据包记录。  
<https://snort.org>
2. pfSense: 一个开源防火墙和路由平台, 基于FreeBSD。  
<https://pfsense.org>
3. ClamAV: 一个开源的反病毒引擎, 用于检测各种恶意软件。

### 1.4 取证/逆向工程工具 (Forensics/Reverse Engineering Tools)

1. Radare2: 一个开源的逆向工程框架和工具集, 用于分析二进制文件。  
<https://rada.re/n/>
2. OllyDbg: 一个32位的汇编级调试器, 用于Windows操作系统。  
<http://ollydbg.de>
3. Ghidra: 一个由NSA开发的开源逆向工程工具套件。  
<https://ghidra-sre.org>
4. x64dbg: 一个开源的Windows调试器, 适用于x64和x32位的程序。  
<https://x64dbg.com>
5. dnSpy: 一个.NET调试器和程序集编辑器。  
<https://github.com/dnSpy/dnSpy>

## 1.5 加密工具 (Encryption Tools)

1. VeraCrypt: 一个免费的开源磁盘加密软件, 基于TrueCrypt。 <https://veracrypt.fr/en/Downloads.html>
2. OpenSSL: 一个强大的开源工具库, 用于实现SSL和TLS协议的加密通信。