

Top 10 tools for Ethical Hacking - Meghraj Patil

Nmap

[Nmap](#) is a [command-line](#) network scanning utility for discovering and mapping networks, [hosts](#), and services. It helps users perform network [vulnerability assessments](#) and improve [network security](#).

Nmap works by sending data packets to a specified [port](#) and [IP address](#). It waits for a response, analyses it, and provides a report.

```
(kali㉿kali)-[~]
└─$ nmap -p 80 10.0.2.15
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-29 10:03 EDT
Nmap scan report for 10.0.2.15
Host is up (0.00011s latency).

PORT      STATE SERVICE
80/tcp    closed http

Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds
```

Features

- Network hosts identification by protocol or port.
- [Ping](#) scan for host testing.
- Fast scan for quick [port scanning](#).
- TCP/IP stack fingerprinting determines a network device's [OS](#) and [hardware](#) elements.

Netcat

[Netcat](#) is a command-line utility that allows users to read and write data across network connections. It scans and listens to ports and transfers files using [TCP](#) and [UDP](#) protocols.

The tool facilitates debugging and investigation, but developers can include it as a [backend](#) for their programs and scripts. Netcat syntax includes various options for communicating and analyzing external websites and their ports.

```
(kali㉿kali)-[~]
└─$ nc -zv google.com 443
DNS fwd/rev mismatch: google.com ≠ bud02s33-in-f14.1e100.net
google.com [142.250.180.206] 443 (https) open

(kali㉿kali)-[~]
└─$
```

Features

- TCP/UDP connections using any port.
- Port scanning with randomization.
- Full [DNS](#) forward and reverse checking.
- Usage of locally configured source port or network source address.
- Loose source-routing.

- TCP/UDP [tunneling](#) mode.

Fluxion

Fluxion is a tool for [security auditing](#) and researching user responses to [social engineering](#) attacks. It can conduct Wi-Fi [access point](#) attacks by providing a simple interface for setting up fake wireless networks.

Aside from the social engineering aspect, security professionals also use Fluxion to test the access point security of wireless networks by simulating [Man in the Middle \(MITM\) attacks](#).



Features

- Handshake Snopper and Captive Portal for simulating an MITM attack.
- Evil Twin attacks.
- Credential harvesting.
- De-authentication attacks.

Lynis

Lynis is a system hardening and compliance testing tool that performs comprehensive system health scans. Aside from IT security professionals, developers use Lynis to improve [web application](#) security, while sysadmins utilize it to discover new weaknesses.

Lynis uses an opportunistic and modular approach to scanning, meaning it can scan for available system tools and then perform a tailor-made system test. This approach allows Lynis to require no dependencies to run.

```
[+] File systems UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link 00:00:00:00:00:00
- Checking mount points host:lo
- Checking /home mount point d_lft forever [ SUGGESTION ]
- Checking /tmp mount point [ SUGGESTION ]
- Checking /var mount point ed_lft forever [ SUGGESTION ]
- Query swap partitions (fstab) LOWER_UP> mtu 1500 qdisc fq_codel [ OK ] late UP group default qlen 10
- Testing swap partitions [ OK ]
- Checking for old files in /tmp d_lft 100000000 [ OK ]
- Checking /tmp sticky bit [ OK ] scope global dynamic noprefixroute [ OK ] late eth0
- Checking /var/tmp sticky bit ed_lft 85953sec [ OK ]
- Mount options of / [ NON DEFAULT ]
- Mount options of /dev preferred_lft forever [ PARTIALLY HARDENED ]
- Mount options of /dev/shm [ PARTIALLY HARDENED ]
- Mount options of /run [ HARDENED ]
- Total without noexec:6 noexec:8 nosuid:4 ro or noexec (W^X): 8 of total 27
- Checking Locate database failed: Unknown host [ NOT FOUND ]
- Disable kernel support of some filesystems used
```

Features

- Over 300 built-in tests.
- Plugin and custom test support.
- Dynamic operating system detection.
- Detailed logging.
- Hardening index.

Nessus

Nessus is a comprehensive vulnerability assessment tool for identifying vulnerabilities, misconfigurations, and potential threats in systems and applications. It offers an extensive database of regularly updated vulnerability checks for up-to-date security assessment.



Features

- Fast asset discovery.
- Configuration auditing.
- Discovery of sensitive data.
- Malware detection.

Tiger

Tiger is a command-line tool written in [shell](#) language that performs security auditing and host-side intrusion detection. It can also provide a framework for combining other tools, like [intrusion detection systems](#), integrity checkers, and logcheckers.

The modular nature of the tool allows users to decide which aspect of a [UNIX](#) system they want to check. For example, Tiger can check [filesystem permissions](#), dormant users, and system file configuration. It can also scan for available patches not installed on the system.

```

(kali@kali)-[~]: ssh (http) - Connection refused
$ sudo tiger
Tiger UN*X security checking system
  Developed by Texas A&M University, 1994
  Updated by the Advanced Research Corporation, 1999-2002
  Further updated by Javier Fernandez-Sanguino, 2001-2018
  Contributions by Francisco Manuel Garcia Claramonte, 2009-2010
  Covered by the GNU General Public License (GPL)

Configuring ...
Will try to check using config for 'x86_64' running Linux 6.1.0-kali9-amd64 ...
--CONFIG-- [con005c] Using configuration files for Linux 6.1.0-kali9-amd64. Using
Tiger security scripts *** 3.2.4rc1, 2018.02.10.20.30 ***
10:19> Beginning security report for kali.
10:19> Starting file systems scans in background...
10:19> Checking password files...
10:19> Checking group files...
10:19> Checking user accounts...

```

Features

- Easily expandable modular design.
- Wide range of available checks.
- Highlights vulnerabilities in password policies, system logs, and network settings.

John the Ripper

John the Ripper (also known as John) is a password-hacking tool with a simple command-line interface. Cyber-security professionals use it for password security auditing and password recovery.

```

(kali@kali)-[~]
$ john
John the Ripper 1.9.0-jumbo-1+bleeding-aec1328d6c 2021-11-02 10:45:52 +0100 OMP [linux-gnu 64-bit
x86_64 AVX2 AC]
Copyright (c) 1996-2021 by Solar Designer and others
Homepage: https://www.openwall.com/john/

Usage: john [OPTIONS] [PASSWORD-FILES]

Use --help to list all available options.

(kali@kali)-[~]
$

```

Features

John the Ripper supports many different [hash](#) and [cipher](#) types, such as:

- User passwords for Linux, BSD, macOS, and Windows users.
- User passwords for web apps and [database servers](#).
- Network traffic captures.
- Encrypted [private keys](#).
- Filesystems, documents, and archives.

Hydra

Hydra is a password-cracking tool that supports parallelized connects and attacks on multiple protocols. It combines various types of [brute-force attacks](#) for guessing the username/password pair.

Penetration testing experts often use Hydra with wordlist generators such as **cupp** and **crunch**.

Hydra is a tool to guess/crack valid login/password pairs.
Licensed under AGPL v3.0. The newest version is always available at;
<https://github.com/vanhauser-thc/thc-hydra>
Please don't use in military or secret service organizations, or for illegal
purposes. (This is a wish and non-binding - most such people do not care about
laws and ethics anyway - and tell themselves they are one of the good ones.)

Example: `hydra -l user -P passlist.txt ftp://192.168.0.1`

Welcome to the Hydra Wizard

```
Enter the service to attack (eg: ftp, ssh, http-post-form):
```

Features

- Support for multiple protocols such as FTP, SSH, POP3, and IMAP.
- Support for website forms.
- Modular architecture.
- Dictionary-based and brute-force attacks.
- Parallel attacks.
- Support for custom scripts.

Social-Engineer Toolkit (SET)

Social-Engineer Toolkit (SET) is a [penetration testing kit](#) for social engineering research written in [Python](#). It allows security professionals to create a believable social engineering attack using custom attack vectors.

SET helps security professionals evaluate how susceptible organizations and individuals are to **phishing**, credential harvesting, and manipulation.

```

--kali@kali:~$ python3 set.py
:::=====
:::=====
:::=====
=====
:::=====
:::=====
:::=====
=====

[—] The Social-Engineer Toolkit (SET) [—]
[—] Created by: David Kennedy (ReL1K) [—]
      Version: 8.0.3
      Codename: 'Maverick'
[—] Follow us on Twitter: @TrustedSec [—]
[—] Follow me on Twitter: @HackingDave [—]
[—] Homepage: https://www.trustedsec.com [—]
Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: https://www.trustedsec.com

It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!

Select from the menu:

1) Social-Engineering Attacks
2) Penetration Testing (Fast-Track)
3) Third Party Modules

```

Features

- Support for various attack vectors (e.g., **spear phishing**, credential harvesting, etc.).
- Infectious media generation.
- Phishing website creation.
- Email-based attacks.
- Malicious USB device creation.

WPScan

WPScan is a tool for detecting vulnerabilities, misconfigurations, and security issues in WordPress websites. It checks a manually updated database of WordPress vulnerabilities and reports on the state of a website.

WPScan can be integrated into a WordPress installation or used as a CLI tool. The CLI tool has a simple interface featuring the **wpscan** command:

```

    _____
   /         \
  /           \
 /             \
/               \
\               /
 \             /
  \           /
   \         /
    \       /
     \     /
      \   /
       \ /
        V

WordPress Security Scanner by the WPScan Team
Version 3.8.22

@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart

_____

Usage: wpscan [options]
--url URL

The URL of the blog to scan
Allowed Protocols: http, https
Default Protocol if none provided: http
This option is mandatory unless update or help

```

Features

- Scanning outdated plugins, themes, and core files.
- Security checks for weak passwords, exposed sensitive information, and potential entry points.
- Version checks for the WordPress installation and plugins.
- Brute-force attacks for login credentials testing.