Finding Low Hanging Fruit With Kali

TL;DW

Demonstrate how to find vulnerabilities on your network using Kali Linux.

Slides are available at:

https://github.com/averagesecurityguy/presentations

Commands are available at:

https://github.com/cheat-sheets

Who Am I?

Developer - github.com/averagesecurityguy

Author - wp.me/p1jUmx-fQ

Blogger - averagesecurityguy.info

Consultant - asgconsulting.co

Twit - @averagesecguy

What is Kali?

Kali is a Linux distribution purposely built for penetration testing. It includes many tools for conducting all of the typical penetration testing activities and is used by security professionals around the world.

How to Get Kali

You can download Kali Linux from *www.kali.org/downloads*

There are 32-bit and a 64-bit versions for both Intel and ARM.

They also have instructions to build a custom Kali distribution.

Kali can be installed as the primary OS on a machine or as a virtual machine.

Setup Kali

Get the latest packages using:

```
apt-get update && apt-get upgrade
```

Some packages are held back during a normal upgrade. If you need them use:

```
apt-get distupgrade or apt-get install <package_name>
```

Packages that are no longer needed can be removed using:

```
apt-get autoremove
```

Setup Metasploit

By default Kali does not run any services on boot. To use Metasploit's database functionality start the postgresql and metasploit services before starting msfconsole.

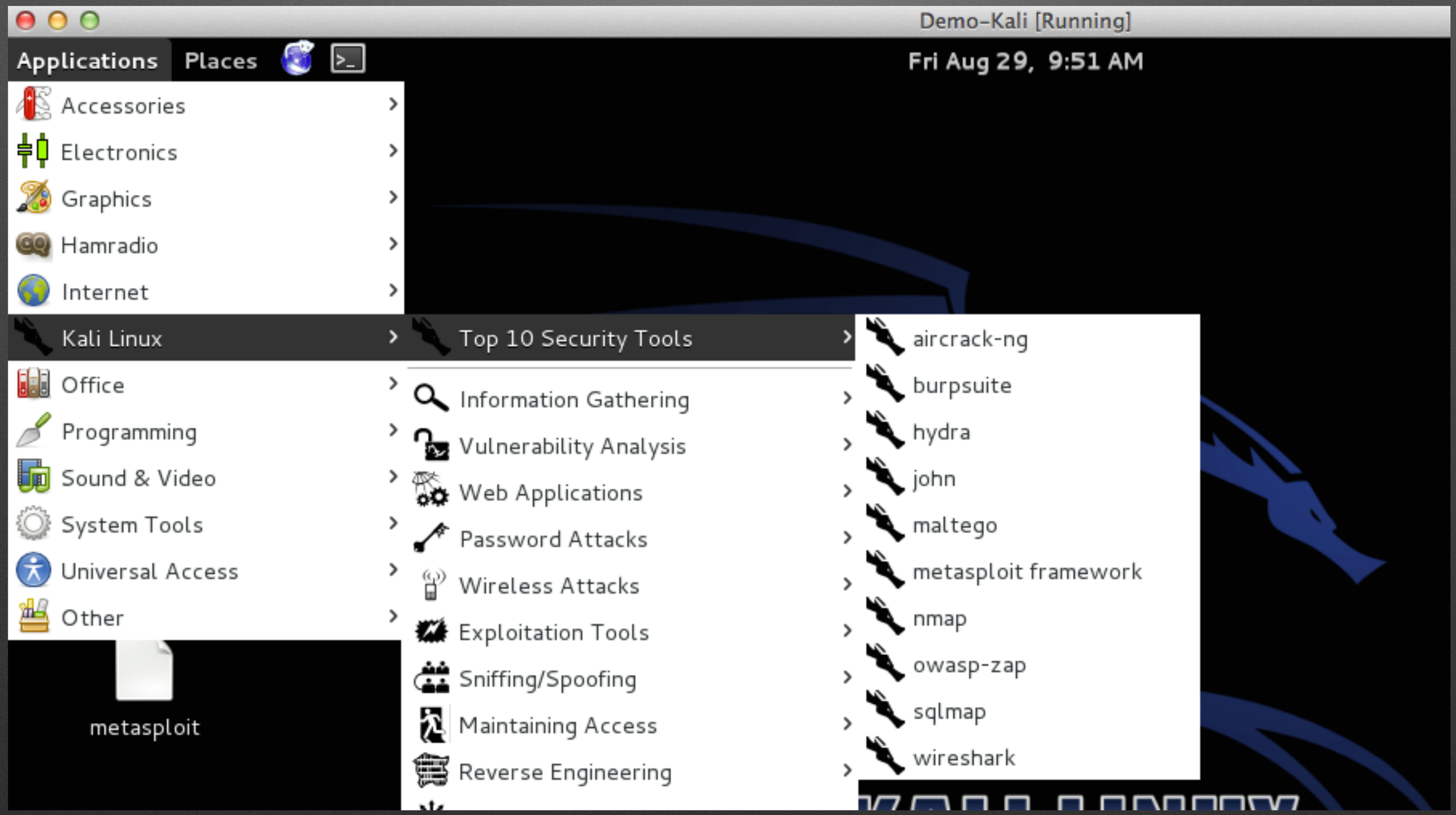
```
sudo service postgresql start
sudo service metasploit start
```

If you want to have these services start at boot, enable them.

```
sudo update-rc.d postgresql enable
sudo update-rc.d metasploit enable
```

Demo 1

A Quick Look at Kali



Low Hanging Fruit

There is a lot of low hanging fruit on most networks and many of those vulnerabilities fall into these categories.

- Unnecessary Services
- Weak Passwords
- Trivially Exploitable Vulns
- Web-Based Admin Interfaces

Unnecessary Services

Nmap (Network Mapper) is designed for network discovery and security auditing. Nmap can be used to find open ports, determine the service running on those ports, and scan for particular network vulnerabilities.

To find open TCP ports use:

```
nmap <ip_address>
```

To find open UDP ports use:

```
nmap -sU <ip_address>
```

Unnecessary Services

To identify services, run an aggressive scan.

```
nmap -A <ip_address>
```

By default Nmap scans for the top 1000 ports. Specify the ports to scan using -p or scan the top N ports using --top-ports.

```
nmap -A -p 1-1024,8080 <ip_address>
nmap -A --top-ports 100 <ip_address>
```

Save the scan results to an XML file.

```
nmap -A -oX <file_name> <ip_address>
```

Unnecessary Services

Import the Nmap XML file into Metasploit.

```
msfconsole
db_import <file_name>
```

View the hosts and services in the database.

```
services
hosts
```

View specific hosts and services

```
hosts 10.1.1.6-7
services -p 23
```

Demo 2

Weak Passwords

Services like Telnet, SSH, SMB, POP, and SMTP are excellent for finding weak passwords. Be careful of account lockout policies. Often, admin accounts such as root, admin, and administrator cannot be locked out.

Using Metasploit's auxiliary modules and the wordlists in /usr/share/wordlists, we can test for weak passwords.

Weak Passwords

There are a number of Metasploit modules designed to find weak passwords including:

auxiliary/scanner/smb/smb_login
auxiliary/scanner/ftp/ftp_login
auxiliary/scanner/ssh/ssh_login
auxiliary/scanner/ssh/ssh_login_pubkey
auxiliary/scanner/mssql/mssql_login
auxiliary/scanner/mysql/mysql_login
auxiliary/scanner/telnet/telnet_login
auxiliary/scanner/vnc/vnc_login

Demo 3

Exploitable Vulnerabilities

Nmap provides a number of NSE scripts to find particular vulnerabilities. While Nmap cannot replace a good vulnerability scanner like Nessus it can be helpful for quick checks.

Nmap organizes scripts into 14 categories. A single script can be in multiple categories. When you run Nmap with either the -A or -sC argument all of the scripts in the *default* category are run.

Exploitable Vulnerabilities

Some NSE scripts may crash services, use a lot of bandwidth, or exploit vulnerabilities. These scripts are considered unsafe and should be used with caution. Any scripts not in the *safe* category are considered unsafe.

Nmap provides an excellent overview of NSE at *nmap.org/book/nse.html*. All of the available scripts are documented at *nmap.org/nsedoc/*.

Exploitable Vulnerabilities

```
nmap --script=ssl-heartbleed <ip_address>

nmap --script=smb-check-vulns <ip_address>

nmap --script=rdp-vuln-ms12-020
<ip_address>
```

Demo 4

Web-Based Admin Interfaces

Most network devices and vendor appliances come with web-based admin interfaces. Some companies do a decent job of securing these interfaces, others do not.

Use Nmap to find these interfaces.

```
nmap -p80,443,5800,8000,8080 <ip_address>
```

The following search in Metasploit will give you some idea of how bad the problem is.

```
search /http/
```

Demo 5

Find out More

Slide deck - https://github.com/averagesecurityguy/presentations

Cheat sheet - *https://github.com/cheat-sheets*

My Book - https://averagesecurityguy.files.wordpress.com/2015/01/hack-yourself-first-final.pdf

Questions?

ASG Consulting | 423.305.3700 | asgconsulting.co