

7

Working with Vulnerability Scanners

The discovery and analysis of security vulnerabilities play important roles during a penetration test. Before a penetration tester or an ethical hacker can successfully launch an exploit, they must be able to identify the security weaknesses on the attack surface. The attack surface is the area where an attacker can attempt to gain entry to or exfiltrate data from a system. A strategic approach to quickly identifying vulnerabilities and obtaining a severity rating is to use a known and reputable vulnerability scanner.

There are many popular and reputable vulnerability scanners, such as Acunetix, OpenVAS, Qualys, Nexpose, Nikto, Retina Network Security Scanner, and Nessus, to name a few in the industry. Having knowledge about all these tools is a good idea, but you won't want to run every tool as some of these are commercial and subscription-based services.

Choosing a vulnerability scanner as your preferred choice is quite important because there are many times a vendor of a product may not provide updates quickly enough to detect threats and weaknesses within a system, and this may be crucial to you as a penetration tester. Imagine running a scan to identify whether a system is susceptible to a particular exploit and the tool you're using doesn't contain the signature update to detect such a vulnerability; the results may not be fruitful.

During the course of this chapter, we will explore using Nessus as our preferred vulnerability scanner.

In this chapter, we will be exploring the following vulnerability assessment tools and topics:

- Nessus and its policies
- Scanning using Nessus
- Exporting Nessus results
- Analyzing Nessus results
- Using web application scanners

Technical requirements

The following are the technical requirements for this chapter:

- Kali Linux: <https://www.kali.org/>
- Nessus (Essentials): <https://www.tenable.com/products/nessus/nessus-essentials>
- WordPress Server: <https://www.turnkeylinux.org/wordpress>

Nessus and its policies

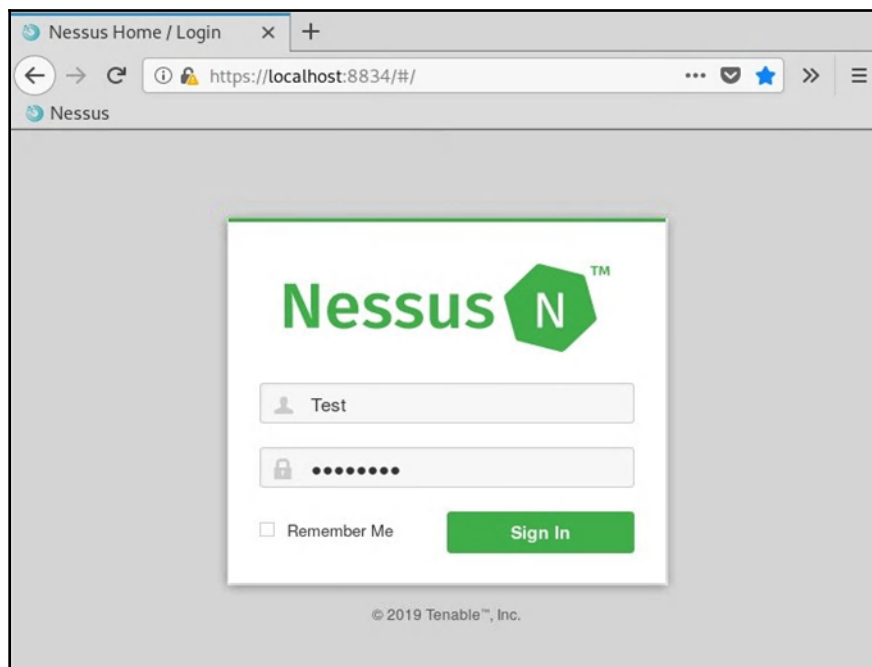
Nessus is one of the most popular and reputable vulnerability scanners in the industry and is used by many professionals within the field of cybersecurity. It has become the de facto industry standard for performing vulnerability assessments among cybersecurity professionals. Some of the benefits of using Nessus include the following:

- Discovery of over 45,000 **Common Vulnerabilities and Exposures (CVEs)**
- Contains over 100,000 plugins (used to discover vulnerabilities)
- Frequent updates of new plugins for newly disclosed vulnerabilities
- Able to identify over 100 zero-day vulnerabilities for the past three years

Let's log in to Nessus on our Kali Linux machine; firstly, you'll need to enable the Nessus service using the following command within a Terminal window:

```
service nessusd start
```

Once the service has been successfully enabled, open the web browser in Kali Linux, enter `https://localhost:8834` within the address bar, and hit *Enter*. You should see the following login portal:



Log in using your user account, which was created during the setup process. Once you are logged in, the main dashboard is available. Here you'll be able to configure and access policies and plugin rules, create new scans, and view results. The Nessus user interface is a very simple-to-use interface, and in a very short time you'll be very familiar with it.

Nessus policies

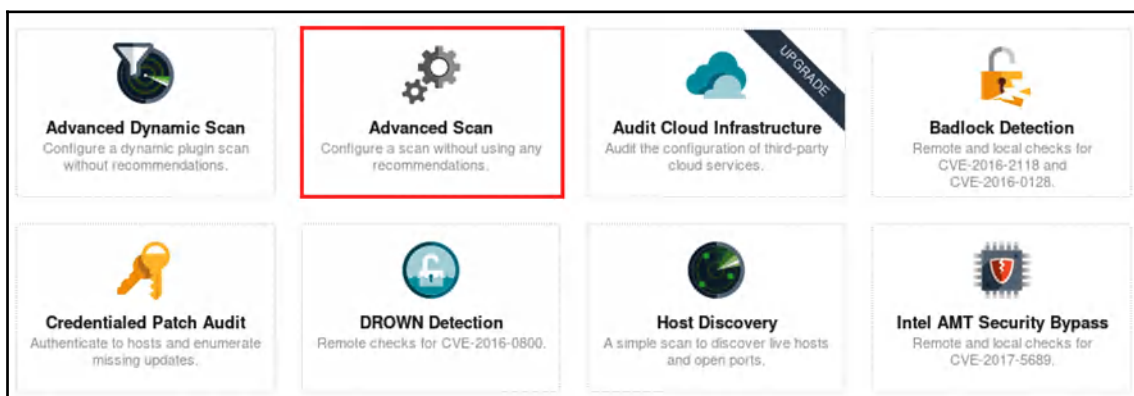
Within the Nessus application, there are many existing policies for various purposes, and new ones are added to the database quite often. Nessus policies are the parameters that control the technical aspects of a scan on a target system. To elaborate further, the technical aspects of a scan may include the number of host devices to scan, the port numbers and services, protocol type (TCP, UDP, and ICMP), the type of port scanner, and so on.

Nessus policies also allow the use of credentials (usernames and passwords) for local scanning on Windows-based operating systems, database applications such as Oracle platforms, and other application-layer protocols such as FTP, POP, and HTTP.

There are preinstalled policies that help security practitioners to perform compliance auditing on systems. An example is checking whether a network that handles payment card transactions is vulnerable, using an **internal PCI network scan**. This policy would check for any vulnerability according to the **Payment Card Industry Data Security Standard (PCI DSS)**.

The Nessus policies allow the scanning of malware infections on Windows operating systems by comparing the hash checksums against both good and malicious files on a target system. This policy is quite handy when determining the number of hosts infected with a type of malware on the network.

To get started with policies on Nessus, ensure you are currently logged in to Nessus. On the left pane, click on **Policies**. The following screenshot shows the currently available policies within the home edition of Nessus. However, if you would like to unlock the other plugins and policies, you'll need to acquire the professional edition:



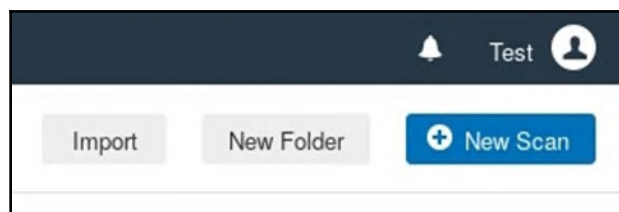
As mentioned before, a policy contains predefined configurations for scanning a target in search of specific vulnerabilities and to ensure a system meets the compliance standard. However, as a security professional, you will need to customize your own scanning policies to perform vulnerability assessments on various types of systems.

Scanning with Nessus

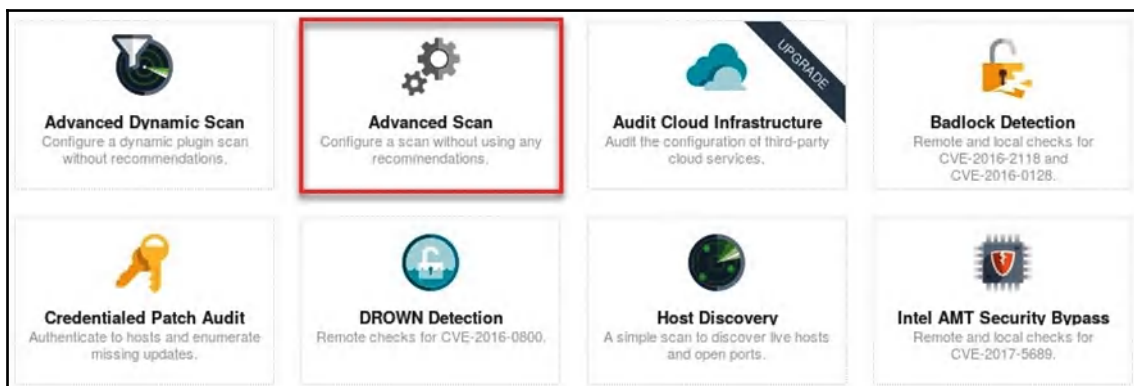
Performing a vulnerability scan using Nessus is quite simple. In this section, I will guide you through the process of creating a customized scan.

To create a new scan, use the following procedure:

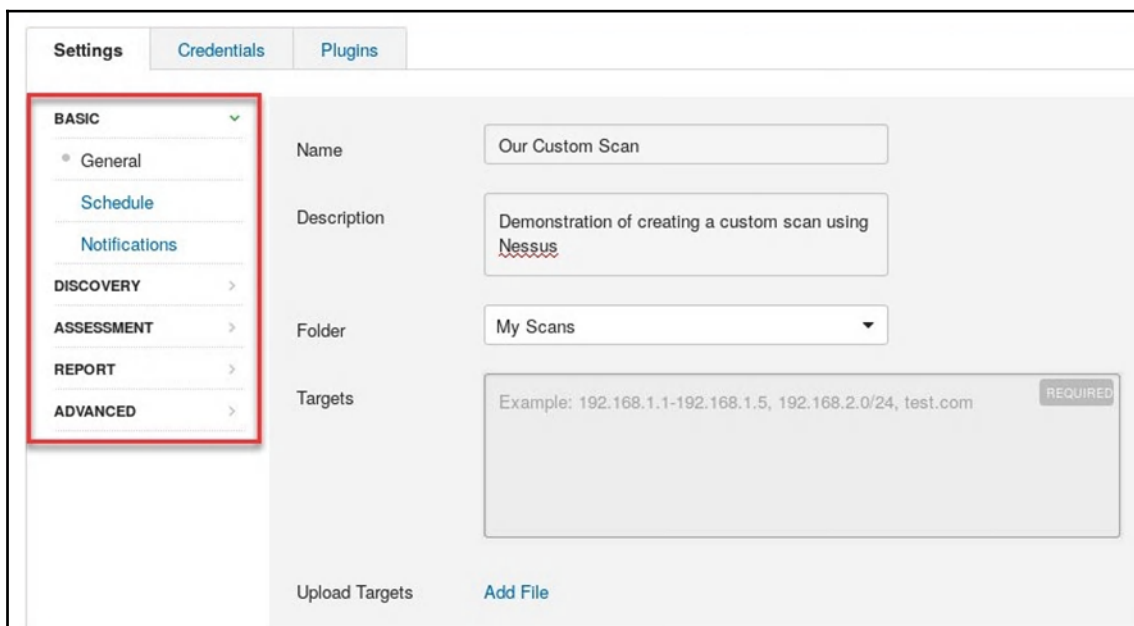
1. On the top-right corner, click on the **New Scan** button as shown in the following screenshot:



2. You'll have the option of using one of the predefined policies available. If you would like to create a custom scan for a target, select the **Advanced Scan** policy as shown in the following screenshot:



3. The policy/scan wizard will open, providing you with many options to customize your new scan. On the **General** tab, ensure you insert a name and description as they will aid in identifying the purpose of this new scan/policy; be sure to include your target(s):



The screenshot shows the 'Settings' interface for creating a new scan. The 'Credentials' and 'Plugins' tabs are visible at the top. On the left, a sidebar menu is highlighted with a red box, showing categories: BASIC (with a dropdown arrow), General (selected), Schedule, Notifications, DISCOVERY (with a right arrow), ASSESSMENT (with a right arrow), REPORT (with a right arrow), and ADVANCED (with a right arrow). The main area is the 'General' tab, which contains the following fields:

- Name:** A text input field containing 'Our Custom Scan'.
- Description:** A text input field containing 'Demonstration of creating a custom scan using Nessus'.
- Folder:** A dropdown menu showing 'My Scans'.
- Targets:** A large text area containing the example '192.168.1.1-192.168.1.5, 192.168.2.0/24, test.com'. A 'REQUIRED' label is in the top right corner of this field.

At the bottom of the main area, there are two buttons: 'Upload Targets' and 'Add File'.

4. You'll have the option to schedule how often the scan/policy should run: once, daily, weekly, monthly, or yearly. This feature allows the automation of running periodic vulnerability scans on target systems. Should you decide to create a schedule for the scan, you can use the options to set the date and time, the time zone, and how often to repeat:

The screenshot shows the 'Settings' page of a vulnerability scanner. The 'Notifications' tab is selected. On the left, a sidebar lists categories: BASIC (with sub-items General, Schedule, and Notifications), DISCOVERY, ASSESSMENT, REPORT, and ADVANCED. The main content area shows the 'Notifications' settings. A toggle switch is set to 'ON'. Below it, the 'Frequency' is set to 'Daily'. The 'Starts' date is '2019-04-28' and the time is '14:00'. The 'Timezone' is set to 'America/Virgin'. The 'Repeat Every' interval is set to 'Day'. A 'Summary' line at the bottom states: 'Daily at 2:00 PM, starting on Sunday, April 28th, 2019'.

5. If you'd like to receive email notifications of the status of a scan, simply click on the **Notifications** tab and enter the recipient's email address. However, ensure you've configured the SMTP server settings, which will handle the delivery of email notifications.
6. To access the SMTP server settings, go to <https://localhost:8834/#/settings/smtp-server>.

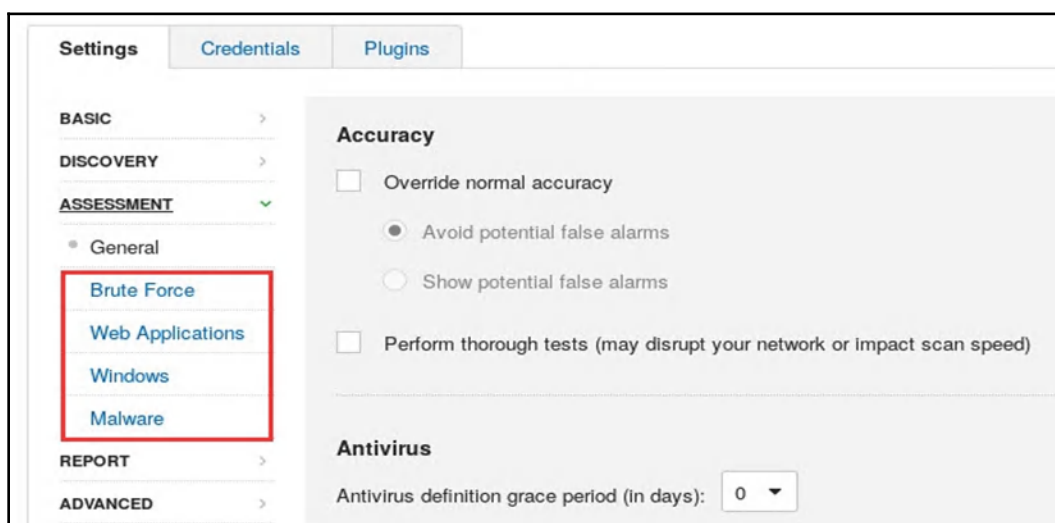
The **Discovery** tab contains the following options:

- **Host Discovery:** Provides options available to discover host devices on a network by using ping methods (ARP, TCP, UDP, and ICMP), discovering network printers, Novell NetWare hosts, and operational technology devices.
- **Port Scanning:** Provides customizable options for scanning a range of ports or a single port, performing enumeration of **Secure Shell (SSH)**, **Windows Management Instrumentation (WMI)** using the **netstat** tool and **Simple Network Management Protocol (SNMP)**. Performs network scanning on TCP and UDP ports and stealth scanning.
- **Service Discovery:** Allows the mapping of each found service to a port number.

The **Assessment** tab contains the following options:

- **Brute Force:** Performs brute force testing on the Oracle database, and attempts logins to websites using Hydra.
- **Web Application:** Web application vulnerability testing.
- **Windows:** Attempts to enumerate domain and local user accounts.
- **Malware:** Scans for malware.

The following screenshot displays the options as outlined in the preceding section:



7. Once you've completed customizing your policy, click on **Save**. The new policy/scan will be available in the **My Scans** folder (left panel). To launch the newly created policy/scan, click the scan and select **Launch**.

Now that you have an understanding of how to perform a scan using Nessus, let's take a deep dive into understanding the results Nessus produces in the next section.

Exporting Nessus results

Whenever a scan has been completed, we can simply click on it to access a very nice dashboard with the statistics. Exporting the results in various formats, such as PDF, HTML, CSV, and so on, is quite simple. Exporting the results will allow you to save the report offline. This will be beneficial as a penetration tester for either revisiting the vulnerability assessment details at a later time or providing the report to the people concerned (clients or team members).

To export the results of a Nessus scan, follow these steps:

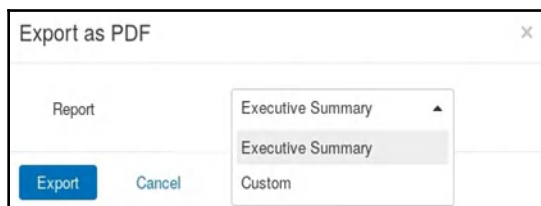
1. Open the scan and click on **Export**:

The screenshot displays the Nessus web interface for a scan titled "Our Custom Scan". The interface is divided into several sections:

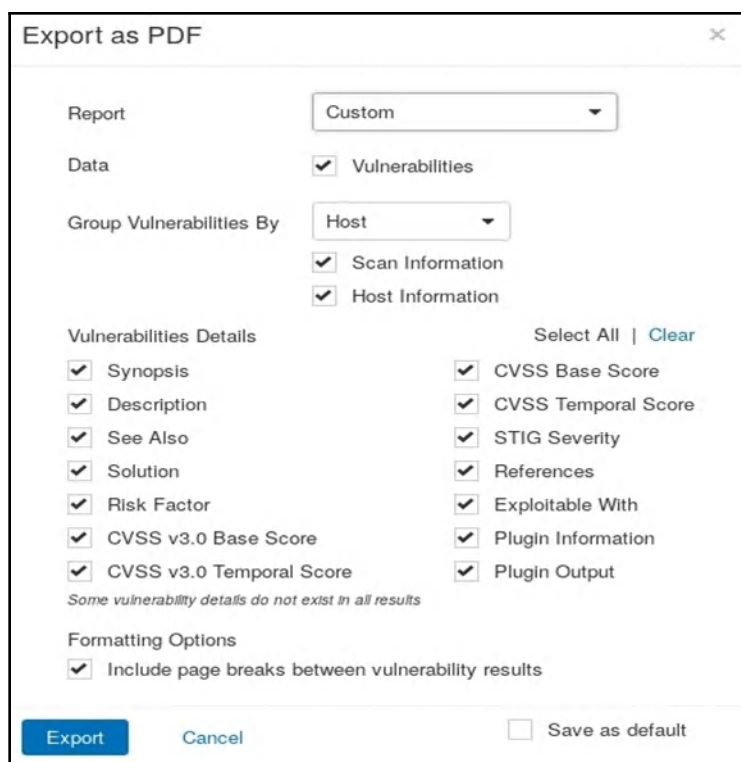
- Left Sidebar:** Contains "FOLDERS" (My Scans, All Scans, Trash) and "RESOURCES" (Policies, Plugin Rules, Scanners).
- Top Navigation:** Includes "Scans" and "Settings" tabs, and a user profile icon.
- Scan Overview:** Shows "Hosts: 1", "Vulnerabilities: 60", and "History: 1". A "Filter" dropdown and a "Search Hosts" input are present.
- Host Table:** A table with columns "Host" and "Vulnerabilities". It lists one host: "10.10.10.100" with a vulnerability count of 120. The count is broken down by severity: 6 Critical (red), 11 High (orange), 4 Medium (yellow), and 120 Low (blue).
- Scan Details:** A section on the right providing metadata:
 - Name: Our Custom Scan
 - Status: Completed
 - Policy: Basic Network Scan
 - Scanner: Local Scanner
 - Start: Today at 2:10 PM
 - End: Today at 2:24 PM
 - Elapsed: 14 minutes
- Vulnerabilities:** A donut chart showing the distribution of vulnerabilities by severity. The legend indicates: Critical (red), High (orange), Medium (yellow), Low (green), and Info (blue).

The "Export" dropdown menu is open, showing the following options: Nessus, PDF, HTML, CSV, and Nessus DB. The "Export" button is highlighted with a red box.

2. You'll have the option to select the output format. Then, the export wizard will provide another option to generate the final output as an **Executive Summary** or to customize a report to your personal preference:

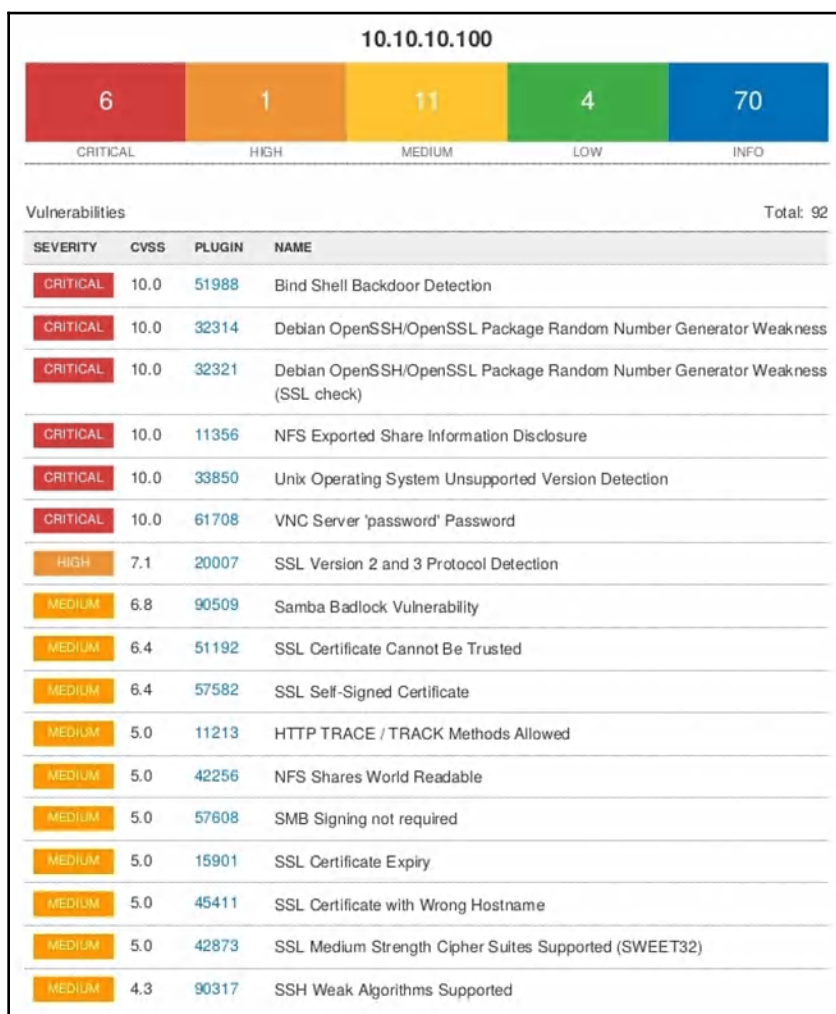


3. Should you choose to create a custom report, the following options are available:



The executive report is better suited for upper management staff who are not concerned about all the technical details of the vulnerability assessment but rather the main overview of the report. The custom report can be used to include or remove specific details, based on what is required and the reader's interest.

The following is a sample of the executive report generated for a vulnerability scan on the Metasploitable VM within our lab:



As you can see, a severity rating and a score are assigned to each vulnerability found on the target. The **Common Vulnerability Scoring System (CVSS)** is a quantitative vulnerability scoring system that helps security professionals to determine the severity of a threat, exploit, or even a security weakness.

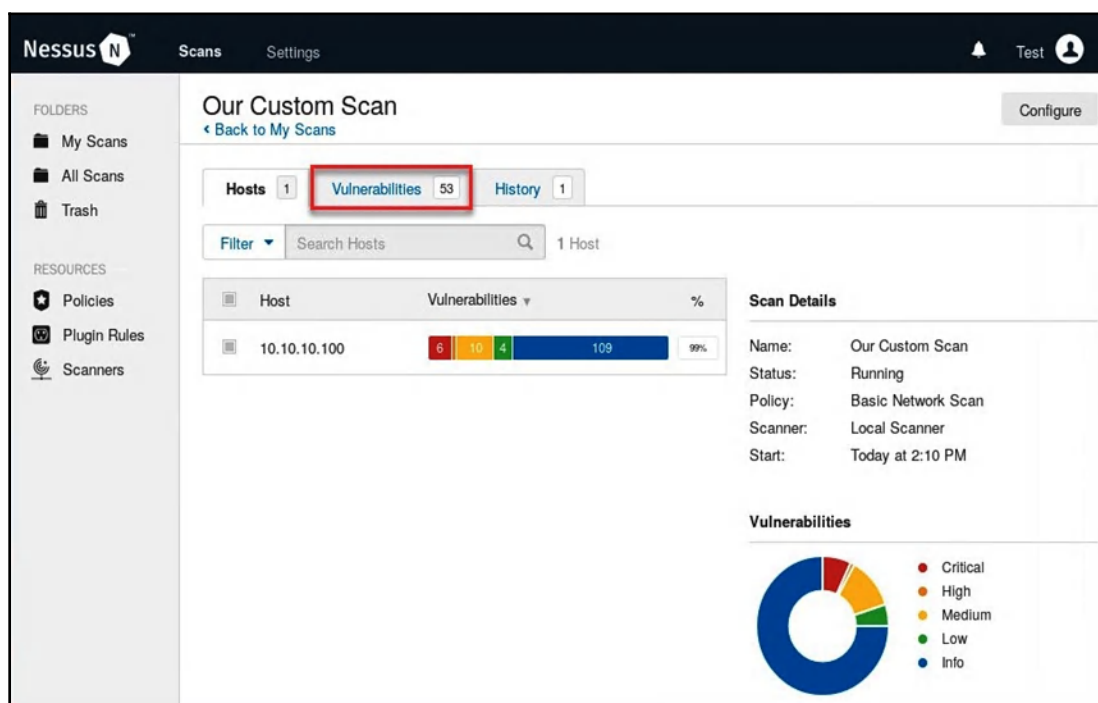


Further information on CVSS can be found on the FIRST website at <https://www.first.org/cvss/>.

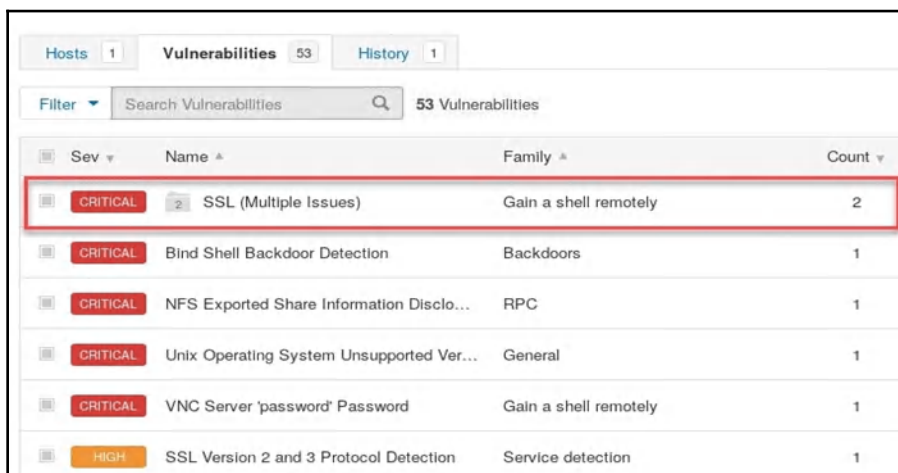
In this section, you have learned about the various formats for exporting Nessus results, the benefits of exporting reports offline, and types of reports. In the upcoming section, we will dive deep into analyzing the output/results provided by Nessus.

Analyzing Nessus results

Creating and performing a vulnerability scan with Nessus is quite easy; however, the mindset of a cybersecurity professional is most needed during the analysis phase. Nessus makes the analysis of the results easy. When a scan has been completed, you'll be able to view the list of vulnerabilities found by selecting the **Vulnerabilities** tab, as shown in the following screenshot:

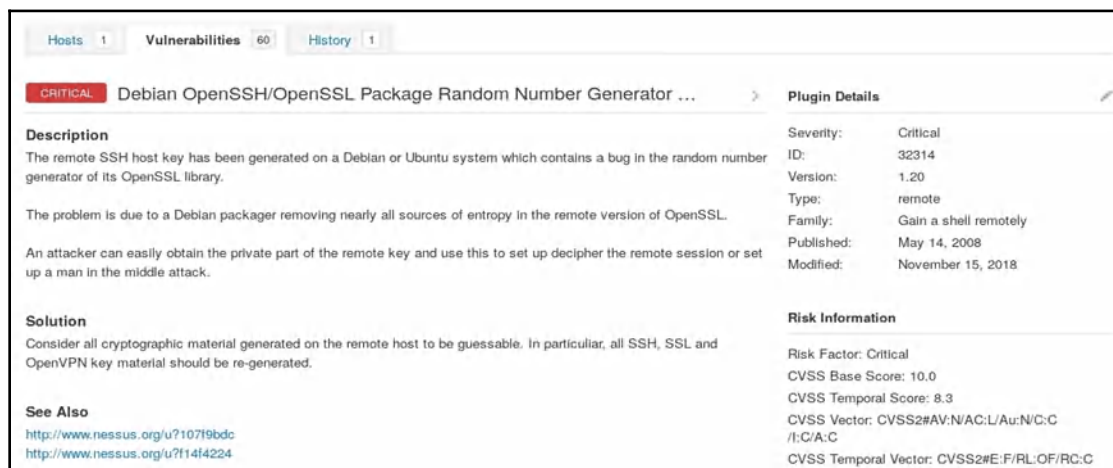


Now, we are able to see a list of vulnerabilities found on the target. Nessus provides us with the severity rating, name of the vulnerability, and the amount found:



Sev	Name	Family	Count
CRITICAL	SSL (Multiple Issues)	Gain a shell remotely	2
CRITICAL	Bind Shell Backdoor Detection	Backdoors	1
CRITICAL	NFS Exported Share Information Disclo...	RPC	1
CRITICAL	Unix Operating System Unsupported Ver...	General	1
CRITICAL	VNC Server 'password' Password	Gain a shell remotely	1
HIGH	SSL Version 2 and 3 Protocol Detection	Service detection	1

To get more details on a vulnerability, click on the specific vulnerability, such as the one highlighted in the preceding screenshot. Nessus will provide you with a detailed description of the selected vulnerability, the risk information, plugin details, remediation, and external referencing, as shown in the following screenshot:



CRITICAL Debian OpenSSH/OpenSSL Package Random Number Generator ...

Description

The remote SSH host key has been generated on a Debian or Ubuntu system which contains a bug in the random number generator of its OpenSSL library.

The problem is due to a Debian packager removing nearly all sources of entropy in the remote version of OpenSSL.

An attacker can easily obtain the private part of the remote key and use this to set up decipher the remote session or set up a man in the middle attack.

Solution

Consider all cryptographic material generated on the remote host to be guessable. In particular, all SSH, SSL and OpenVPN key material should be re-generated.

See Also

<http://www.nessus.org/u?107f9bdc>
<http://www.nessus.org/u?114f4224>

Plugin Details

Severity: Critical
ID: 32314
Version: 1.20
Type: remote
Family: Gain a shell remotely
Published: May 14, 2008
Modified: November 15, 2018

Risk Information

Risk Factor: Critical
CVSS Base Score: 10.0
CVSS Temporal Score: 8.3
CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C
CVSS Temporal Vector: CVSS2#E:F/RL:OF/RC:C

Using this information, a penetration tester can quickly identify the weakest points on a target, and narrow the scope when choosing payloads to exploit the target.

Now you have a firm understanding of Nessus and its capabilities. In the next section, we will use various web application scanners to assist us in detecting web vulnerabilities on a target server.

Using web application scanners

Web application scanners focus primarily on detecting and identifying vulnerabilities on web servers, websites, and web applications. In your career in cybersecurity, whether as a penetration tester or a security practitioner, you may be tasked to perform some sort of security auditing on a target website or web server.

However, as a penetration tester, we need to be able to discover security misconfigurations and weaknesses on a target website and web server. An organization may contract you to perform a penetration test on their website rather than on their network, or even both. Remember the goal of having a penetration test done on an object such as a website is to identify the vulnerabilities and remediate them as soon as possible before an actual hacker is able to compromise the system and exfiltrate data.

There are many web application scanners available on the market, from commercial to free and open source; here are some of them:

- Acunetix vulnerability scanner (commercial)
- w3af (free)
- Nikto (free)
- Burp Suite (commercial and free)
- IBM AppScan (commercial)

In the remaining sections of this chapter, we will cover various exercises using Nikto, WPScan, and Burp Suite to detect and identify security vulnerabilities on a target web server.

Let's take a deep dive into learning about Nikto in the next section.

Nikto

Nikto is a popular open source web vulnerability scanner and is preinstalled in Kali Linux. This command-line tool is capable of identifying security flaws on a target website and providing detailed referencing for each issue found. Nikto is not a stealth-oriented tool and can be a bit noisy while performing its scan.

Some of its features are as follows:

- Checking for any outdated components on a web server
- Capable of identifying installed applications via headers and files on a target
- SSL support
- Performs subdomain guessing
- Apache username enumeration

To get started with Nikto, we will perform a web vulnerability scan on our Metasploitable VM. If you recall, in the previous chapter, we performed a port scan on Metasploitable and saw that port 80 was open. By default, web servers open port 80 to allow inbound and outbound communication between a client and the web server.

Open a new Terminal window using the `nikto -h <target>` syntax, where `-h` specifies a host (hostname or IP address). We use the `nikto -h 10.10.10.100` command:

```
root@kali:~# nikto -h 10.10.10.100
- Nikto v2.1.6

-----
+ Target IP:          10.10.10.100
+ Target Hostname:    10.10.10.100
+ Target Port:        80
+ Start Time:         2019-04-28 12:18:31 (GMT-4)
-----

+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Uncommon header 'tcn' found, with contents: list
+ Apache mod negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. See http://www.wisec.it/sectou.php?id=4698ebdc59d15. The following alternatives for 'index' were found: index.php
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ /phpinfo.php: Output from the phpinfo() function was found.
+ OSVDB-3268: /doc/: Directory indexing found.
+ OSVDB-48: /doc/: The /doc/ directory is browsable. This may be /usr/doc.
+ OSVDB-12184: /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
```

If you provide a hostname, Nikto will be able to perform an IP lookup via the **Domain Name System (DNS)**. During the initial phase, Nikto attempts to perform an operating system and service version fingerprinting; our target is using Ubuntu as its operating system and Apache 2.2.8 as the web server application.



Nikto can be found under the **Applications | 02 – Vulnerability Analysis** tab in Kali Linux.

Each point on the output is an indication of an issue Nikto has detected, whether a configuration is missing, access to a sensitive directory or file was found, or even an application version is outdated. For each security issue found, an **Open Source Vulnerability Database (OSVDB)** reference ID is associated with the issue. The OSVDB is an independent and open source database that contains information about web application security vulnerabilities. Once Nikto is able to identify a security flaw on a target, it provides an associated OSVDB reference ID. Once the OSVDB ID has been obtained, you can head over to <http://cve.mitre.org/data/refs/refmap/source-OSVDB.html> to reference the OSVDB IDs with CVE entries.



Further information about Nikto can be found at <https://cirt.net/Nikto2> and <https://github.com/sullo/nikto>.

Now you have the essential skills to use Nikto, let's take a look at using WPScan in the next section.

WPScan

Creating a website for a company involves a lot of programming and work. There are many **Content Management Systems (CMSes)** that allow you to create, manage, and publish a website quite easily. Imagine having to statically code web languages for multiple pages of a website or multiple websites; this would be a daunting task requiring good knowledge of web languages. A CMS allows a web administrator to easily manage and update the contents of a website seamlessly while being able to integrate additional third-party web plugins, allowing more functionality to the users.

There are many CMSes available; here are some of them:

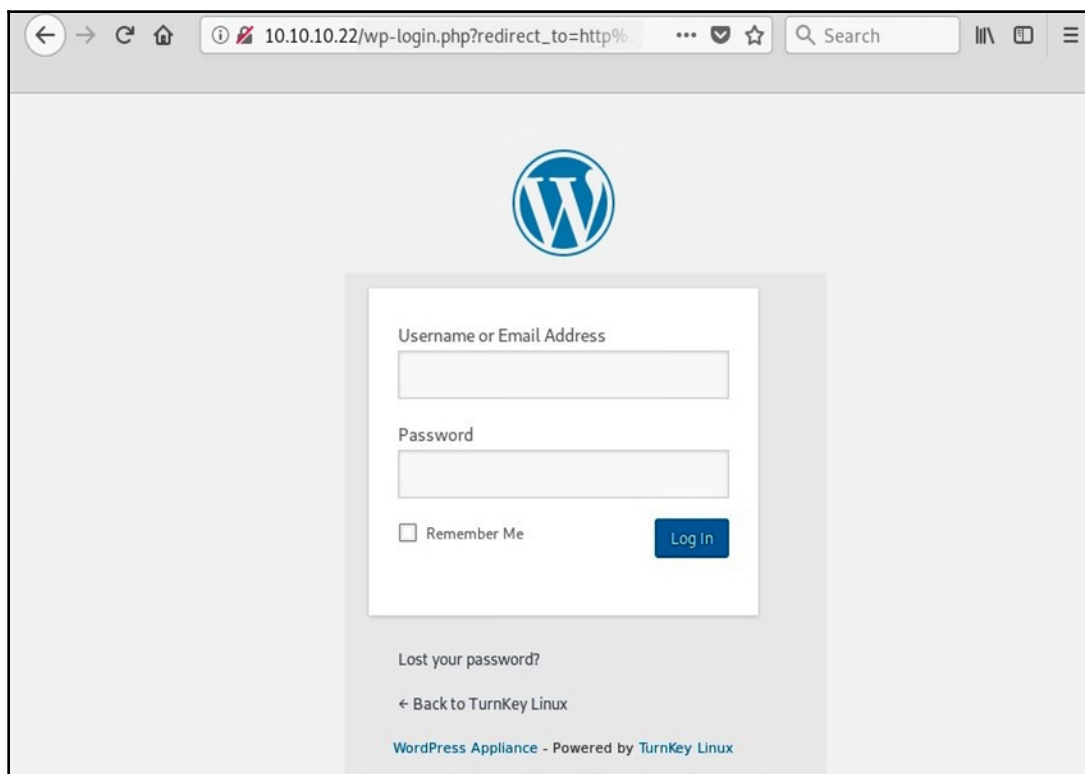
- WordPress
- Joomla
- Drupal
- Plone

On the internet, one of the most popular CMSes currently being used is WordPress. Whether you're a blogger, a freelancer, a start-up, or a large organization, many people are using WordPress as their preferred choice for a CMS. WordPress is an open source CMS that is based on MySQL and PHP. Since WordPress is very popular on the internet, we will use the **WPScan** tool within Kali Linux to scan for web vulnerabilities on a WordPress web server.

To begin, you'll need to install a WordPress server within your virtual lab environment. To do this, follow these steps:

1. Go to <https://www.turnkeylinux.org/wordpress> and download the ISO image or the VM file (using the virtual machine files is easier to set up the VM).
2. Once installed within your hypervisor, ensure the network configurations are enabled for the same network as your Kali Linux machine.
3. Power on the WordPress VM. It will receive an IP address automatically from the **Dynamic Host Configuration Protocol (DHCP)** service within the hypervisor.
4. Using your Kali Linux machine, perform a network and port scan to identify the WordPress server IP address.
5. Enter the IP address into the Kali Linux web browser, and you should see the WordPress default web page.

6. Using the `http://<ip address>/wp-login.php` URL will display the administrator login page as shown in the following screenshot:



This is the default login page for WordPress servers.



Optionally, the WPScan tool can be found under the **Applications | 03 – Web Application Analysis | CMS & Framework Identification** tab within the Kali Linux menu.

On your Kali Linux machine, we are going to perform a vulnerability scan on the WordPress web server by using the `wpscan --url <target IP or hostname>` command:

```
root@kali:~# wpscan --url 10.10.10.22
```

```

      _____
     /          \
    /             \
   /               \
  /                 \
 /                   \
/                     \
\                     /
 \                   /
  \                 /
   \               /
    \             /
     \           /
      \         /
       \       /
        \     /
         \___/
            ®

WordPress Security Scanner by the WPScan Team
Version 3.5.1

Sponsored by Sucuri - https://sucuri.net
 @_WPScan_, @ethicalhack3r, @erwan_lr, @FireFart_

```

```
[+] URL: http://10.10.10.22/
[+] Started: Sun Apr 28 14:55:06 2019
```

Interesting Finding(s):

```
[+] http://10.10.10.22/
 | Interesting Entry: Server: Apache
 | Found By: Headers (Passive Detection)
 | Confidence: 100%
```

WPScan will provide the server platform; in our case, it's Apache.

Next, it will attempt to discover and list all the known vulnerabilities found and provide fixes and references for each as shown in the following screenshot:

```
[*] 9 vulnerabilities identified:

[*] Title: WordPress <= 5.0 - Authenticated File Delete
Fixed in: 4.9.9
References:
- https://wpvulndb.com/vulnerabilities/9169
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-20147
- https://wordpress.org/news/2018/12/wordpress-5-0-1-security-release/

[*] Title: WordPress <= 5.0 - Authenticated Post Type Bypass
Fixed in: 4.9.9
References:
- https://wpvulndb.com/vulnerabilities/9170
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-20152
- https://wordpress.org/news/2018/12/wordpress-5-0-1-security-release/
- https://blog.ripstech.com/2018/wordpress-post-type-privilege-escalation/
```

WPScan is not only a vulnerability scanner for WordPress but has also the ability to perform user account enumeration. Let's attempt to extract the user accounts on our WordPress server; use the `wpscan --url 10.10.10.100 -e u vp` command to perform user enumeration:

```
[+] Enumerating Users (via Passive and Aggressive Methods)
Brute Forcing Author IDs - Time: 00:00:00 <=====

[i] User(s) Identified:

[+] admin
| Detected By: Author Posts - Display Name (Passive Detection)
| Confirmed By:
| Rss Generator (Passive Detection)
| Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Login Error Messages (Aggressive Detection)
```

As you saw in our results, the admin user was discovered. Next, we can attempt to perform password cracking on the admin account using the brute force technique.



To create a custom wordlist for password cracking, you can use the **crunch** tool with Kali Linux. Additionally, you can download a wordlist from the internet. A good source is <https://github.com/danielmiessler/SecLists>.

To perform password cracking using WPScan with an offline wordlist (ours is called `custom_list.txt`), we use the `wpscan --url 10.10.10.100 -e u --passwords custom_list.txt` command.

In the following snippet, we were able to crack the password for the user account:

```
[+] Enumerating Users (via Passive and Aggressive Methods)
Brute Forcing Author IDs - Time: 00:00:00 <=====

[i] User(s) Identified:

[+] admin
| Detected By: Author Posts - Display Name (Passive Detection)
| Confirmed By:
| Rss Generator (Passive Detection)
| Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Login Error Messages (Aggressive Detection)

[+] Performing password attack on Xmlrpc against 1 user/s
Trying admin / Admin456 Time: 00:00:00 <=====
[SUCCESS] - admin / Admin456

[i] Valid Combinations Found:
| Username: admin, Password: Admin456
```

As a penetration tester has obtained the username and password, the account is compromised. We can now log in to the control panel of the WordPress server to perform various malicious actions.



Password cracking can be a very time-consuming process and can take a few minutes or a few hours to complete.

Having completed this section, you have acquired the skills to perform a vulnerability assessment on a WordPress server using WPScan. In the next section, we will learn about another web vulnerability assessment tool, Burp Suite.

Burp Suite

Burp Suite (<https://portswigger.net/burp>) is a **graphical user interface (GUI)** web application vulnerability scanner that has the capability to identify over 100 generic vulnerabilities, such as all the vulnerabilities found in the OWASP top 10 list of critical web application security risks.



The OWASP top 10 list can be found at https://www.owasp.org/index.php/Category:OWASP_Top_Ten_2017_Project.

Burp Suite applications allow a penetration tester to intercept all HTTP and HTTPS requests and responses between the web server (web application) and the browser, via its HTTP proxy component. By intercepting web traffic, Burp Suite can test various types of vulnerabilities and attacks such as fuzzing, brute force password attacks, decoding, obtaining hidden URLs via spidering, and a lot more.

Before getting started with Burp Suite, ensure your OWASP **Broken Web Applications (BWA)** virtual machine (victim machine) is online and has received an IP address.

Once the OWASP BWA VM is online, you should be presented with the following screen; however, your IP address details may be different from what is shown:

```
Welcome to the OWASP Broken Web Apps VM

!!! This VM has many serious security issues. We strongly recommend that you run
it only on the "host only" or "NAT" network in the VM settings !!!

You can access the web apps at http://10.10.10.134/

You can administer / configure this machine through the console here, by SSHing
to 10.10.10.134, via Samba at \\10.10.10.134\, or via phpmyadmin at
http://10.10.10.134/phpmyadmin.

In all these cases, you can use username "root" and password "owaspbwa".

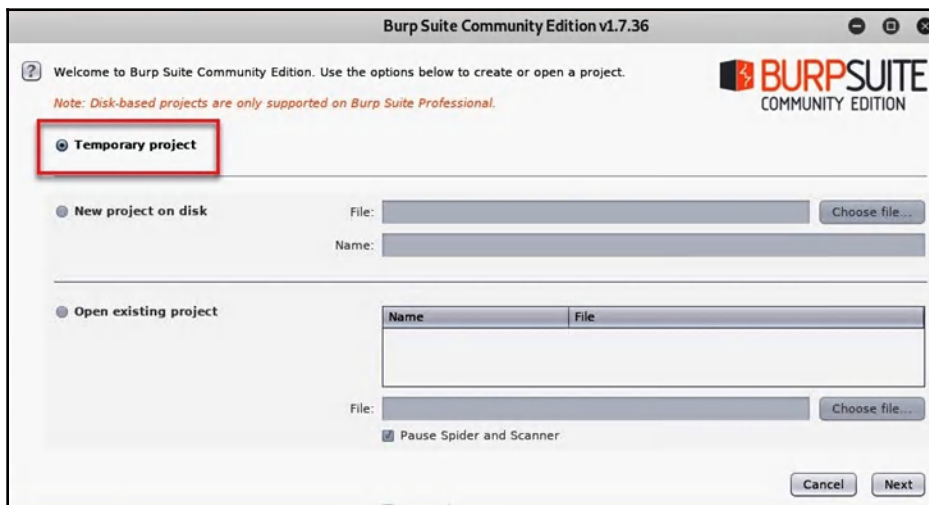
OWASP Broken Web Applications VM Version 1.2
Log in with username = root and password = owaspbwa

owaspbwa login:
```

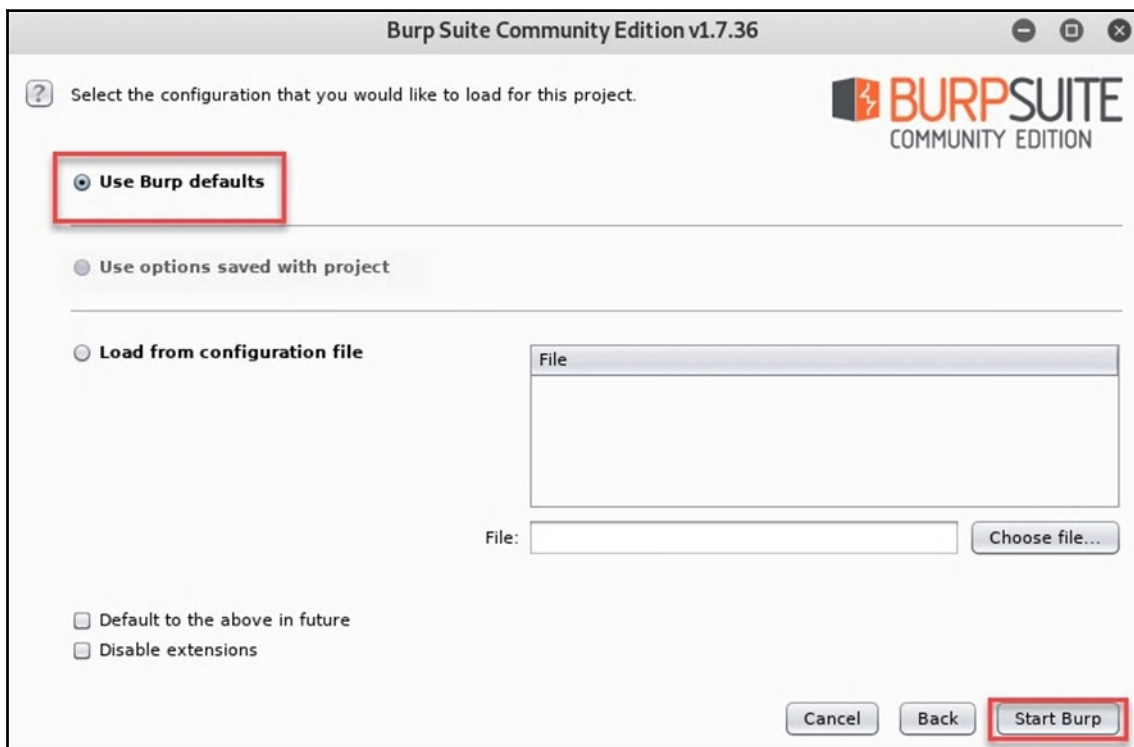
On your Kali Linux machine, ensure there is end-to-end connectivity by pinging the OWASP BWA virtual machine. Once you've verified connectivity, it's time to open the Burp Suite application.

To complete this task, use the following instructions:

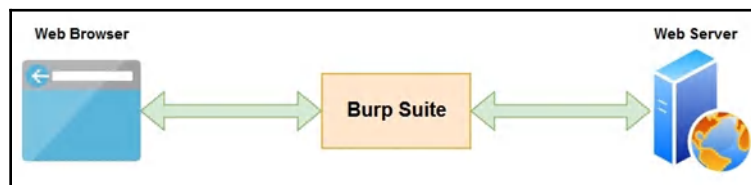
1. Go to **Applications | 03 – Web Application Analysis | Web Application Proxies | Burp Suite**.
2. Now the application is open, the wizard will ask whether you would like to create a **Temporary project**, a **New project on disk**, or **Open existing project**.
3. Select **Temporary project** and click **Next**:



4. The next window will ask whether Burp Suite should use the default setting or load configurations from a file. Select the **Use Burp defaults** option, and click **Start Burp** to launch the user dashboard:



Traffic sent between your web browser and the target web server is not monitored or intercepted by Burp Suite. Burp Suite contains an HTTP proxy that allows the application to intercept HTTP traffic between a web browser and a target web server. The web browser does not directly interact with the web server; traffic is sent from the web browser to the Burp Suite HTTP proxy, then the HTTP proxy forwards the traffic to the target web server and vice versa. The following is a diagram showing the flow of traffic between a web browser and a web server:



Burp Suite works as an intercepting proxy application. By default, Burp Suite is not able to intercept any traffic between our Kali Linux machine and the OWASP BWA virtual machine. To configure our web browser to work with Burp Suite, use the following instructions:

1. Open Firefox and click on the menu icon | **Preferences (Options)**.
2. On the default tab, scroll down until you see the **Network Proxy** settings (**Network Settings**) and click on **Settings**.
3. Select **Manual proxy configurations** and use the configurations displayed in the next screenshot:

The screenshot shows the 'Connection Settings' dialog box in Firefox. The 'Configure Proxy Access to the Internet' section has four radio buttons: 'No proxy', 'Auto-detect proxy settings for this network', 'Use system proxy settings', and 'Manual proxy configuration'. The 'Manual proxy configuration' option is selected and highlighted with a red rectangle. Below this, the 'HTTP Proxy' is set to '127.0.0.1' and the 'Port' is '8080'. A checkbox labeled 'Use this proxy server for all protocols' is checked. Below these, the 'SSL Proxy', 'FTP Proxy', and 'SOCKS Host' are all set to '127.0.0.1' with 'Port' '8080'. The 'SOCKS v4' and 'SOCKS v5' radio buttons are present, with 'SOCKS v5' selected. Below these is an 'Automatic proxy configuration URL' section with a text field and a 'Reload' button. At the bottom, there is a 'No proxy for' section with a text field. A red rectangle highlights this text field with the text 'Ensure this field is blank' inside it. Below the text field is an example: '.mozilla.org, .net.nz, 192.168.1.0/24'. At the bottom right are 'OK', 'Cancel', and 'Help' buttons.

Connection Settings

Configure Proxy Access to the Internet

☐ No proxy

☐ Auto-detect proxy settings for this network

☐ Use system proxy settings

☒ Manual proxy configuration

HTTP Proxy 127.0.0.1 Port 8080

☒ Use this proxy server for all protocols

SSL Proxy 127.0.0.1 Port 8080

FTP Proxy 127.0.0.1 Port 8080

SOCKS Host 127.0.0.1 Port 8080

☐ SOCKS v4 ☒ SOCKS v5

☐ Automatic proxy configuration URL

Reload

No proxy for

Ensure this field is blank

Example: .mozilla.org, .net.nz, 192.168.1.0/24

OK Cancel Help

Ensure the **No proxy for** field is blank.

4. Click on **OK** to save your settings in Firefox.

Now that we've configured our web browser to work with the Burp Suite HTTP proxy service, let's head back over to the Burp Suite application to allow the interception of traffic. To do so, follow these steps:

1. Click on **Proxy | Intercept**, and click on the **Intercept is on** icon to toggle enable/disable:

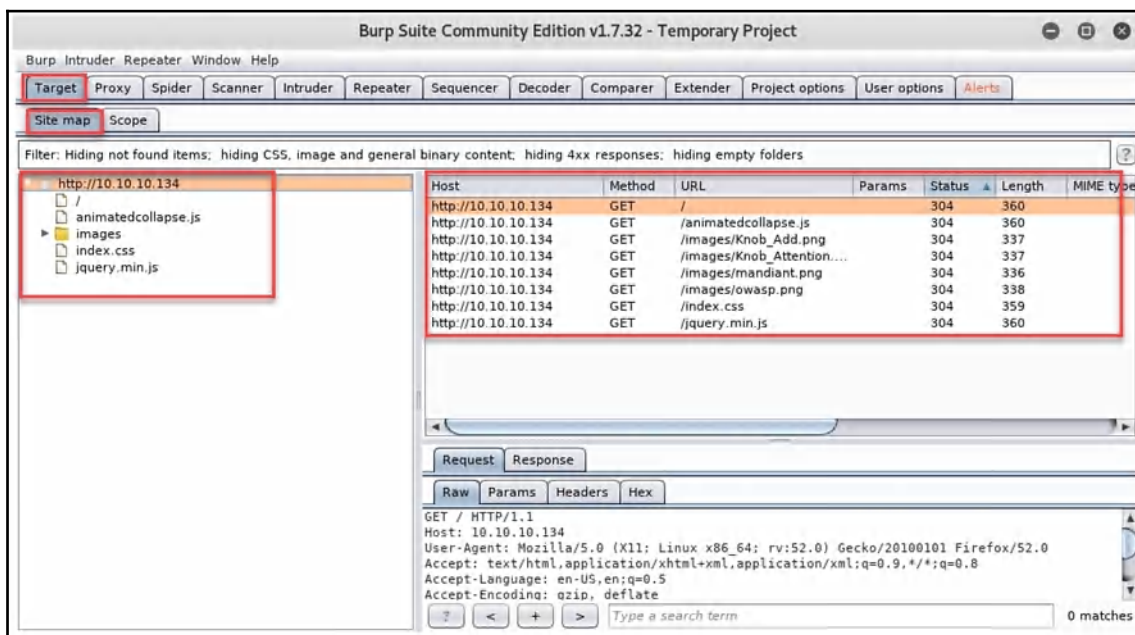


Ensure your configurations are set properly or the exercise won't work as it's intended to.



If the Intercept icon says on, Burp Suite is able to intercept traffic between the web browser and the web server. Additionally, be sure to forward requests; otherwise, they will stay within the interceptor and not be forwarded, and eventually the request will time out.

- Next, enter the IP address of the OWASP BWA virtual machine within the address bar in Firefox on your Kali Linux machine. The default web page should load perfectly. On Burp Suite, click on **Target | Site Map** to see the HTTP requests and responses:



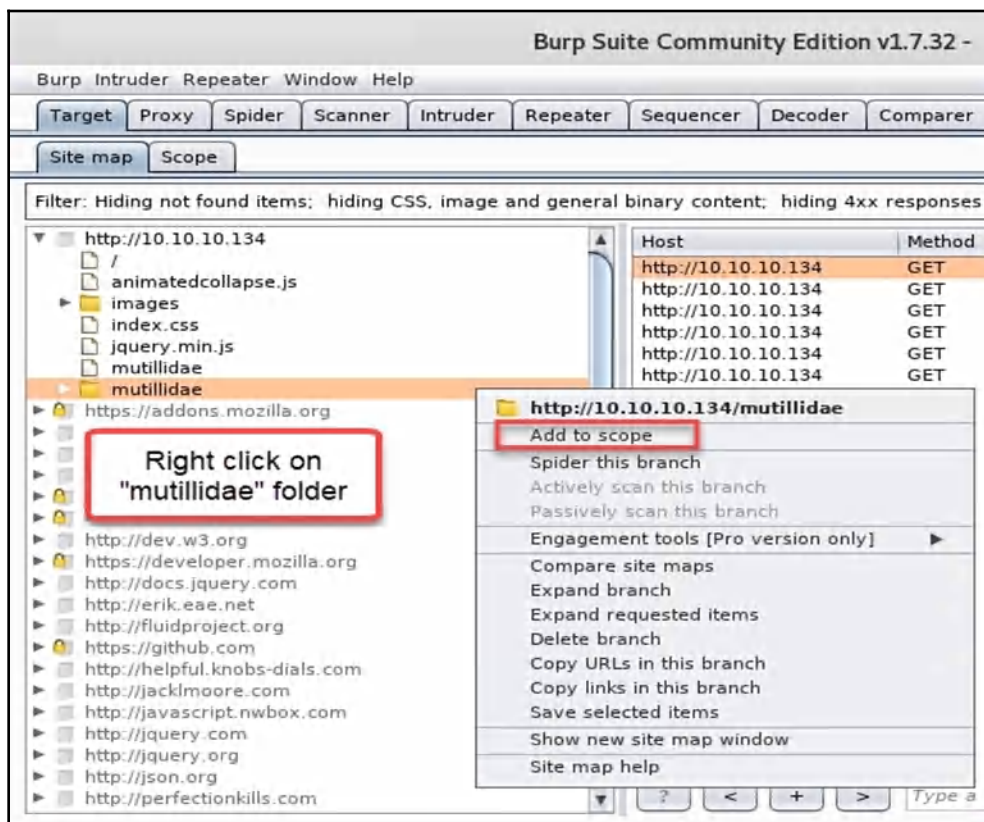
- On the web browser, enter the URL (or IP address) of the OWASP BWA virtual machine. The HTTP requests and responses will appear on the **Target | Site Map** tab on Burp Suite.

Now that we've outlined how to intercept web traffic using Burp Suite, let's go a step further to perform an offensive attack on our Metasploitable machine. In the next section, we will use Burp Suite to perform a brute force attack.

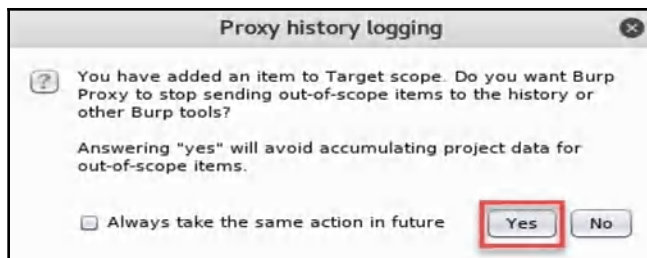
Using Intruder for brute force

The Intruder component/module within Burp Suite allows a penetration tester to perform online password attacks using the brute force method. Let's attempt to obtain the password to log in to the `http://<target ip addr>/mutillidae` URL:

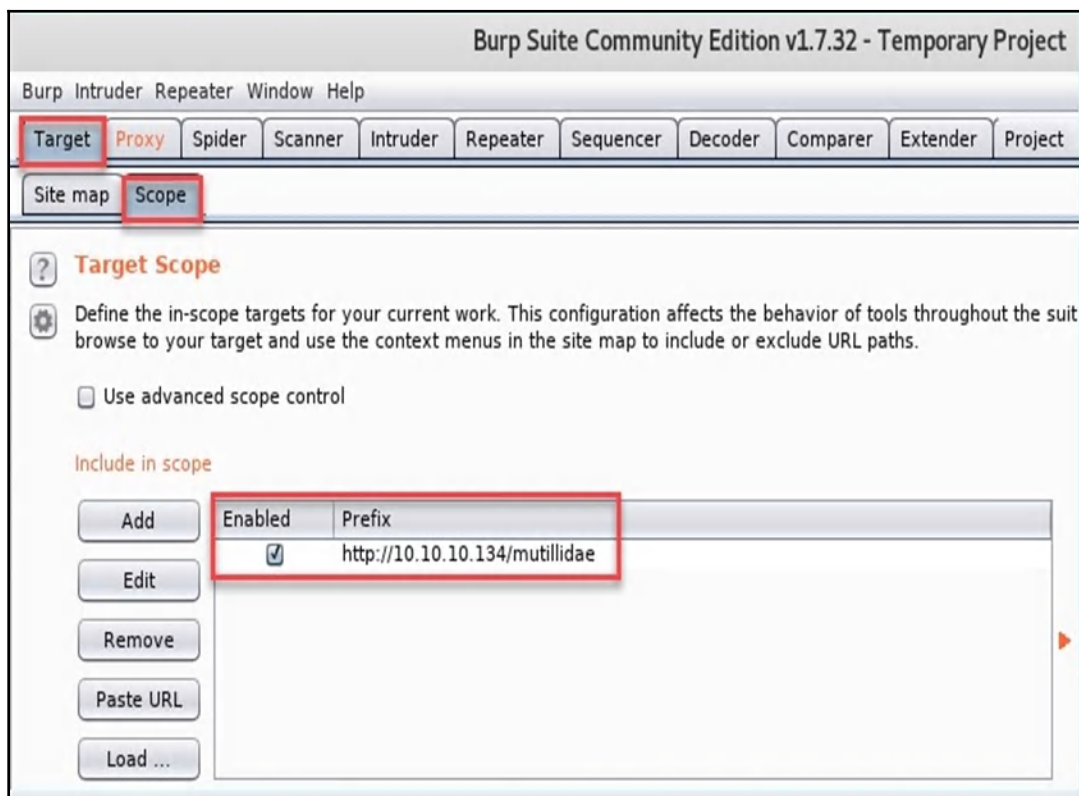
1. Using the Firefox web browser click on **Mutillidae II**. On Burp Suite, you should see the `mutillidae` folder appearing under the left pane of the **Site map** tab.
2. Next, right-click on the `mutillidae` folder, and select **Add to scope** as shown in the following screenshot:



3. The following **Proxy history logging** window will appear; simply click on **Yes**:



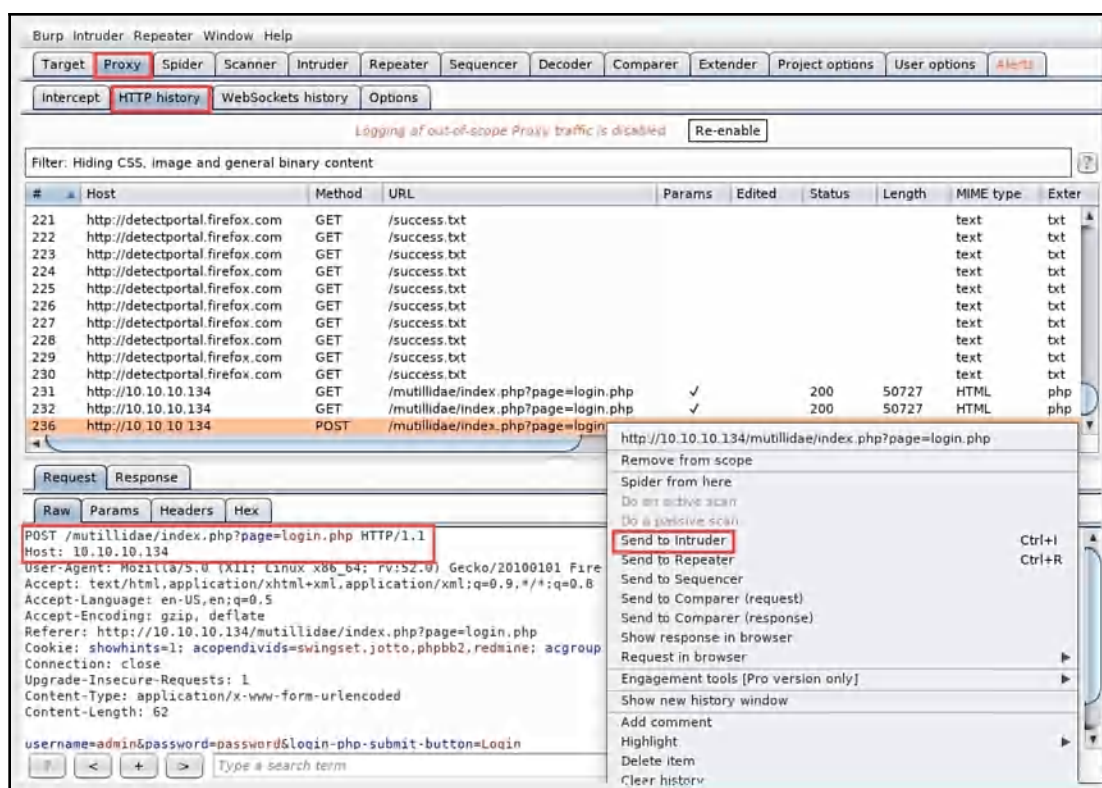
4. To verify our scope has been added successfully, go to the **Target | Scope** tab:



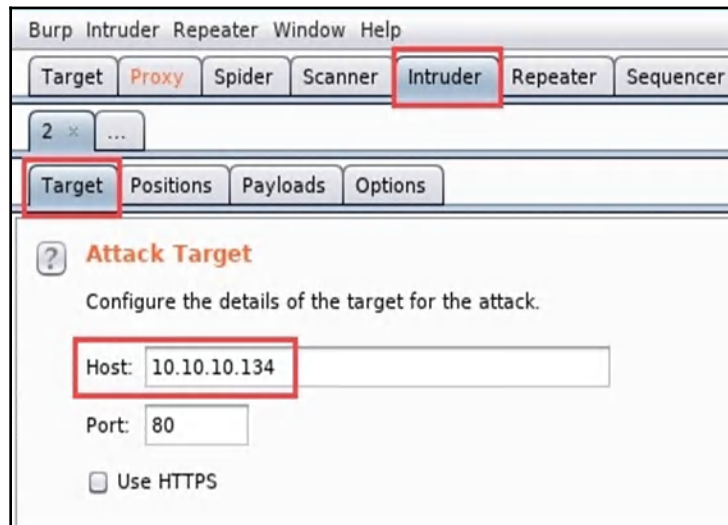
- Now your scope has been added, head back to your web browser. At the top of the Mutillidae web page, you'll see a link that allows a user to perform login attempts. Use `admin` for the username and `password` for the password. The login attempt should fail; however, we need Burp Suite to capture specific details about the login field on the web page.

Let's head back to Burp Suite to continue our exercise.

- On Burp Suite, click on the **Proxy | HTTP history** tab and select the HTTP **POST** message, which has the login attempt from our browser (your # message may be different from what is shown in the following snippet). Once selected, right-click and choose **Send to Intruder**:

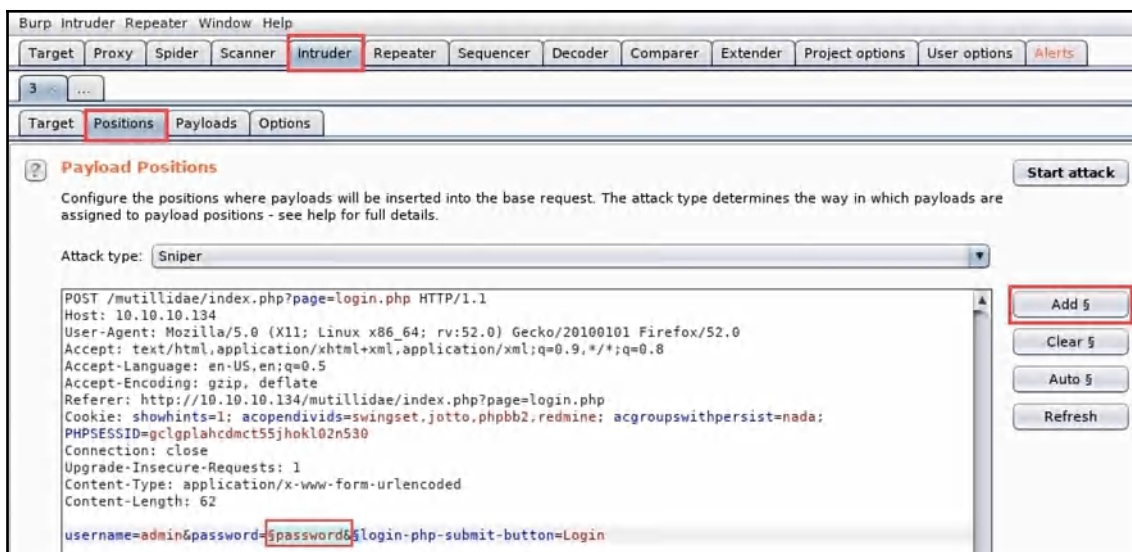


7. Next, click on the **Intruder** | **Target** tab to see the target IP address that has been set:



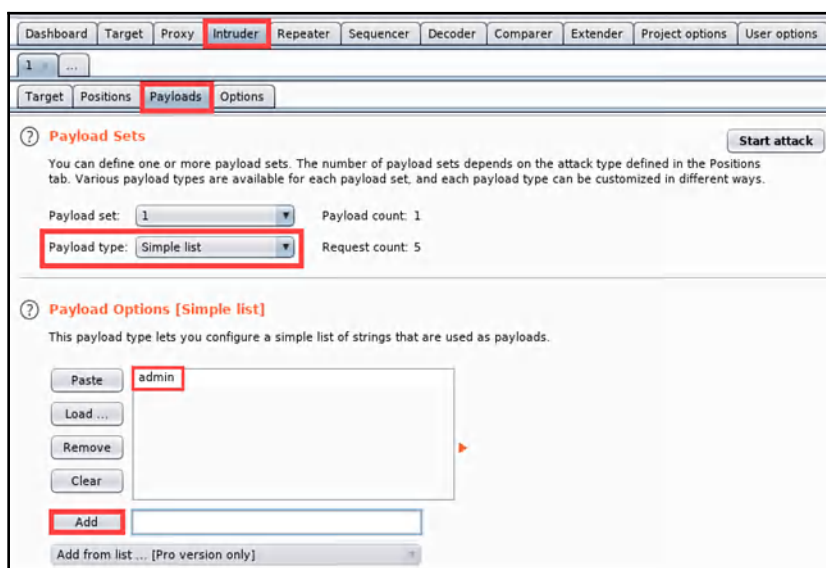
Within the **Intruder** tab, there are a few sub-tabs, including the following:

- **Target:** Allows you to set a specific target and port number.
 - **Positions:** Allows you to select where a payload will be inserted into the HTTP request.
 - **Payloads:** Provides the ability to configure the type of payload.
 - **Options:** Additional options can be set on this tab.
8. Select the **Positions** tab and click on the **Clear** button to clear all selections. By default, Burp Suite has selected certain areas of the HTTP request message to insert its payload. However, for our exercise, the payload is to be inserted in the password field.
 9. Highlight the word `password` and click on **Add**. This will allow Burp Suite to insert its payload on the selected field:



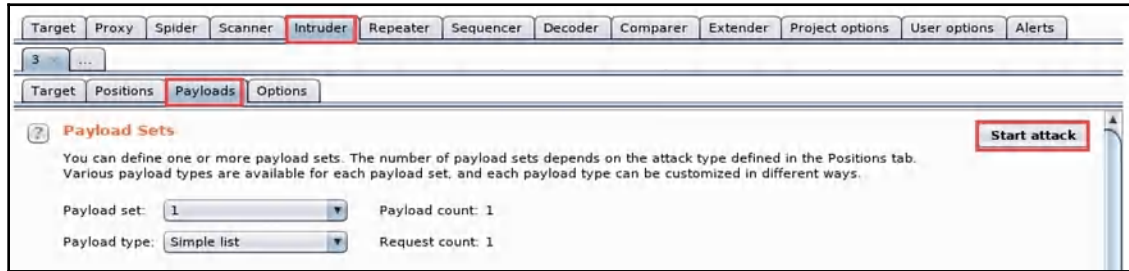
The red text is the data sent from the browser to the web server. As you can see, the word `password` is the value we used during our login attempt.

10. Click on the **Payloads** tab. Enter `admin` in the text field and click **Add**; this will be our custom payload:

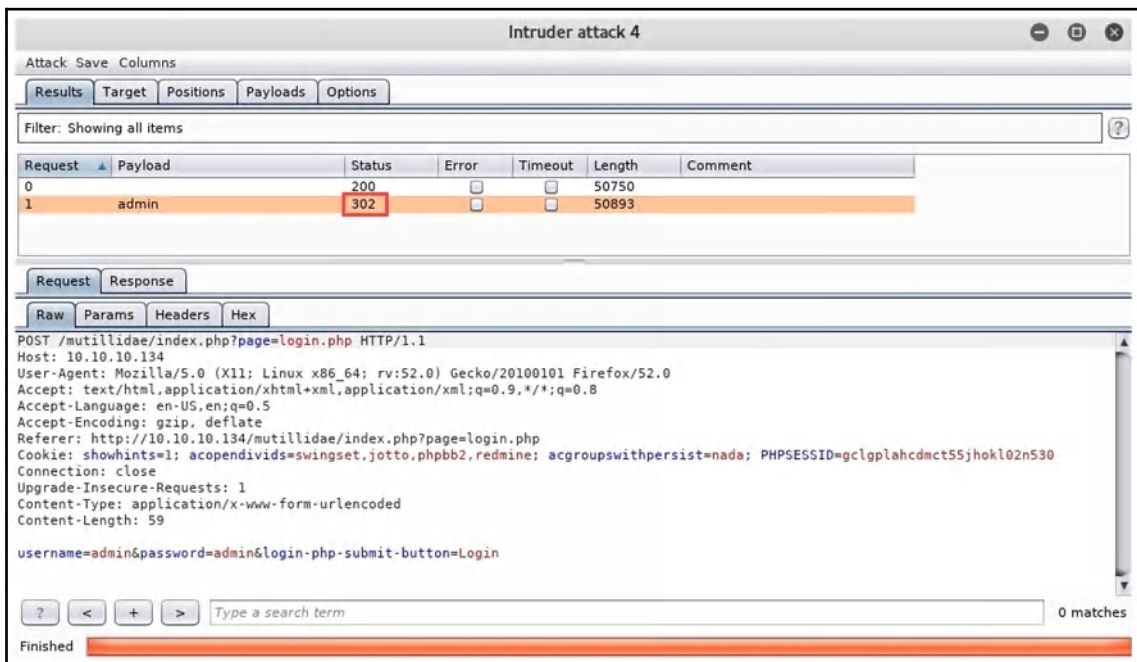


Ensure everything else is left as default in the remaining portions of the **Payloads** and **Options** tabs.

- When you're ready to launch the payload, click on **Start attack**:

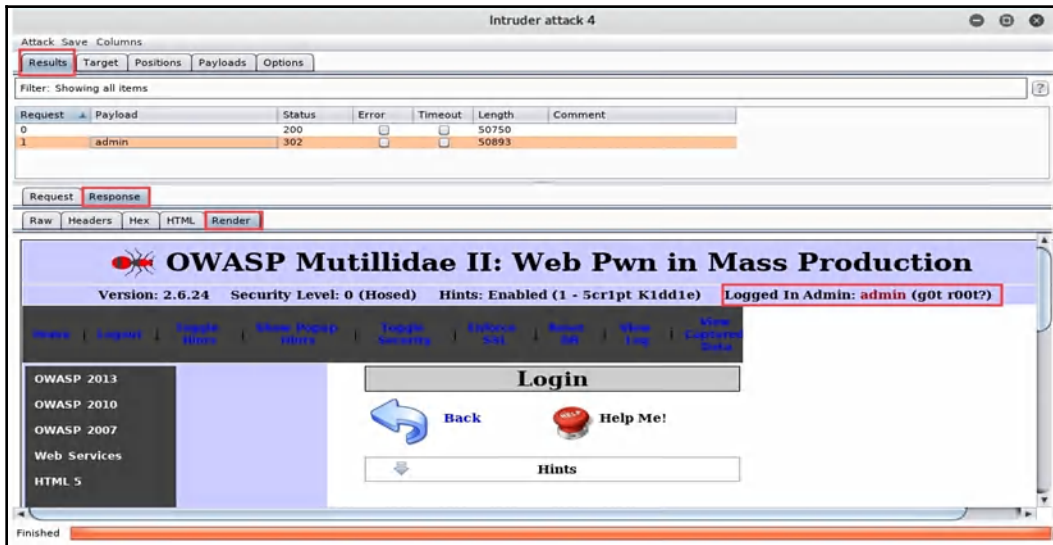


When the attack has been completed, Intruder will open a new window to provide a summary. On the **Results** tab, notice we have an HTTP request message with a **302** status code; this means an HTTP redirect took place. In other words, Intruder was able to successfully log in to Mutillidae. The details can be seen in the following screenshot with username and password:



Selecting the HTTP request message with the **302** status code, you see the username and password that were sent from the web browser on the **Request** tab.

12. To view the response from the web server, click on the **Response** | **Render** tab. Here you will be able to see how the web application responded to the payload:



Looking closely, you'll see the `admin` user account was successfully logged in. Please note that the user account shown in the preceding screenshot is the default administration account for the intentionally vulnerable Metasploitable virtual machine. Furthermore, do not try any sort of attack on devices or networks where you have not acquired legal permission to do so. This exercise was conducted in a lab environment.



The *Burp Suite Cookbook* by Sunny Wear contains a lot of recipes to perform web-based assessments. This title can be found at <https://www.packtpub.com/networking-and-servers/burp-suite-cookbook>.

As you saw, Burp Suite is a very powerful application for web penetration testing and vulnerability assessments. This tool should definitely be part of your go-to list of tools whenever you're tasked with performing security auditing on a web server and website.

Summary

During the course of this chapter, we discussed the need to discover security weaknesses on a system and even a web server. We took a look at performing vulnerability scanning, customizing policies, and reporting using Nessus. Additionally, we learned about Nikto, an open source web vulnerability scanner, and using WPScan to detect security misconfigurations and flaws in WordPress. Lastly, we closed the chapter by covering the fundamentals of using the Burp Suite applications and performing a brute force attempt to gain entry into a website.

Upon completing this chapter, you now have the ability to successfully perform a vulnerability assessment on a target network and system using Nessus, and to perform website penetration testing using Burp Suite, Nikto, and WPScan.

I do hope this chapter has been informative and will help on your journey in the field of cybersecurity. In the next chapter, we will explore the basic concepts of wireless penetration testing.

Questions

The following are some questions based on the topics we have covered in this chapter:

1. After installing Nessus in Kali Linux, what command is used to enable the Nessus service?
2. Many financial institutions provide their customers with card payment functionality. To ensure the institution is compliant with industry standards, what framework should be used?
3. What types of reports can be exported from Nessus?
4. Can you name two or three web vulnerability scanners that are preinstalled in Kali Linux?
5. What tool can be used to scan WordPress websites for security vulnerabilities?

Further reading

- For more information on Nessus, please visit <https://www.tenable.com/products/nessus/nessus-professional>.
- Further information on PCI DSS can be found on the Security Standards Council website at <https://www.pcisecuritystandards.org/>.

8

Understanding Network Penetration Testing

During the preparation phase of a network penetration test, it's essential to understand the objective of security testing on the target's systems and/or network infrastructure. Prior to launching any sort of attack simulation, it's important to be an anonymous user (or pretend to be a legitimate user) on the network by spoofing the MAC address of your device and configuring your wireless network adapter to monitor and capture wireless traffic on an IEEE 802.11 wireless network.

Network penetration testing focuses on gaining entry to a network and performing security auditing (penetration testing) on network security appliances, devices, and systems within the internal network of a target organization. In this chapter, you will learn about the various modes that can be configured on a wireless adapter in Kali Linux, how to spoof your MAC address, and how to capture packets on a wireless network.

In this chapter, we will cover the following topics:

- Introduction to network penetration testing
- Understanding the MAC address
- Connecting a wireless adapter to Kali Linux
- Managing and monitoring wireless modes

Technical requirements

The following are the technical requirements for this chapter:

- Kali Linux (<https://www.kali.org/>)
- VMware Workstation or Oracle VM VirtualBox
- A wireless **network interface card** (NIC) that supports packet injection

Not all wireless cards support monitor mode and packet injection. However, a minor revision in a chipset can cause the card to not work in monitor mode, and some cards may need the drivers to be compiled and may not work out of the box.

The following is a list of supported external wireless NICs for Kali Linux:

- Atheros: ATH9KHTC (AR9271, AR7010)
- Ralink: RT3070
- Realtek: RTL8192CU
- TP-Link TL-WN722N
- TP-Link TL-WN822N v1 - v3
- Alfa Networks AWUS036NEH
- Alfa Networks AWUS036NHA
- Alfa Networks AWUSO36NH

I would personally recommend using the **Alfa Networks AWUS036NHA** card.

Introduction to network penetration testing

The objective of network penetration testing is to discover any security vulnerabilities on a target's network infrastructure. This type of penetration test can be done either from outside the organization (external testing) or from the inside (internal testing). As a penetration tester, I would definitely recommend performing both internal and external security testing on the target's network.

The following are some objectives of network penetration testing:

- Bypassing the perimeter firewall
- Evading **Intrusion Detection System / Prevention System (IDS/IPS)**
- Testing for routing and switching misconfiguration
- Detecting unnecessarily open network ports and services
- Finding sensitive directories and information

Performing network penetration testing helps IT professionals close unnecessary network ports, disable services, troubleshoot issues, and configure security appliances in a better way to mitigate threats.

During an external network penetration test, the penetration tester attempts to access the target organization's network across the internet by breaching the firewall and any IDS/IPS. However, an internal network penetration test involves security testing from inside the organization's network, which is already behind the perimeter firewall appliance.

The following are the six steps that need to be followed in the network penetration testing process:

1. Information gathering
2. Port scanning
3. OS and service fingerprinting
4. Vulnerability research
5. Exploit verification
6. Reporting

In the following section, we will briefly cover the different approaches to penetration testing.

Types of penetration test

The following are three types of security testing that are usually done by penetration testers:

- **White box:** White-box testing involves having complete knowledge – including network diagrams, IP addressing schemes, and other information – about the network and systems prior to the network penetration test. This type of test is much easier than gray-box and black-box testing since the penetration tester does not need to perform any sort of information gathering on the target network and systems.
- **Gray box:** In gray-box testing, the penetration tester is given limited knowledge about the organization's network infrastructure and systems prior to the network penetration test.
- **Black box:** In black-box testing, the penetration tester is given no prior knowledge about the target organization or its network and system information. The information that's provided about the target is usually just the organization's name.

Now that we have completed this introductory section to network penetration testing, let's dive into the essentials of understanding the MAC address.

Understanding the MAC address

Within the field of networking, there are two models that network professionals often refer to during their troubleshooting. These models are known as the **Open Systems Interconnection (OSI)** reference model and the **Transmission Control Protocol/Internet Protocol (TCP/IP)** stack.

The following table outlines the layers of each model and displays the OSI model, **Protocol Data Units (PDUs)**, and the TCP/IP protocol suite:

OSI Model	PDU	TCP/IP Stack
Application	Data	Application
Presentation		
Session		
Transport	Segment	Transport
Network	Packet	Internet
Data Link	Frame	Network Access/Link
Physical	Bits	

Often, the terms **packets** and **frames** will be used interchangeably, but there is a difference between them. Let's focus a bit more on the characteristics of a frame and its composition.

In this section, we are going to focus on the data link layer (layer 2) of the OSI model. The data link layer is responsible for moving data between the software applications on devices to the physical layer of a network. This is done by the NIC. Additionally, before the data is placed on the physical layer, the data layer inserts the physical address of the NIC, that is, the **media access control (MAC)** address, into the frame. This address is sometimes referred to as the **burned-in address (BIA)**.

The MAC address of a device is 48 bits in length and is written in hexadecimal format; therefore, each character ranges between 0-9 and A-F. The first 24 bits are known as the **organizationally unique identifier (OUI)** and are assigned by the **Institute of Electrical and Electronics Engineers (IEEE)** to vendors and manufacturers. By having knowledge of the first 24 bits of any valid MAC address, you can determine the vendor/manufacturer of the NIC and/or device. The last 24 bits are unique and assigned by the vendor, thereby creating a unique MAC address for each device.

The following is a breakdown of a MAC address:

Organizationally Unique Identifier (OUI)	Assigned by the Vendor
3 Bytes	3 Bytes
24 Bits	24 Bits
00-E0-F7	58-1E-83
Cisco Systems	Device-Specific

To view the MAC address on Windows, use the `ipconfig /all` command:

```
C:\>ipconfig /all

FastEthernet0 Connection: (default port)

    Connection-specific DNS Suffix...:
    Physical Address.....: 0002.165D.5D20
    Link-local IPv6 Address.....: FE80::202:16FF:FE5D:5D20
    IP Address.....: 192.168.1.2
    Subnet Mask.....: 255.255.255.0
    Default Gateway.....: 192.168.1.1
    DNS Servers.....: 8.8.8.8
    DHCP Servers.....: 192.168.1.1
    DHCPv6 Client DUID.....: 00-01-00-01-A4-39-DB-87-00-02-16-5D-5D-20
```

However, on a Linux-based OS, you need to use the `ifconfig` command:

```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.2 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 2803:1500:1201:9991::2 prefixlen 64 scopeid 0x0<global>
    inet6 fe80::20c:29ff:fe37:58 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:7e:37:58 txqueuelen 1000 (Ethernet)
    RX packets 147 bytes 180942 (176.7 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 113 bytes 9511 (9.2 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

We now have a better idea of the purpose of the MAC address on a device and network. Now, let's take a deep dive into learning how to change (spoof) our MAC address in Kali Linux.

How to spoof the MAC address

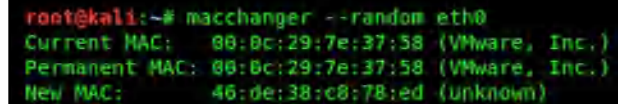
Spoofing is a form of impersonation on a network; it conceals your identity as a penetration tester. All the traffic leaving your Kali Linux machine will contain the source's newly configured MAC address.

In this exercise, we are going to change the MAC address of the LAN interface on our Kali Linux machine. Follow these simple steps to do so:

1. Turn off the network interface using the following command:

```
ifconfig eth0 down
```

2. Once the interface is down, we can use the `macchanger` tool to modify our MAC address on the interface. The `macchanger` tool allows you to customize your new (spoofed) address. To see all the available options, use the `macchanger --help` command.
3. To change the MAC address on our Ethernet (network) interface, we will use the `macchanger --random eth0` command, as shown in the following screenshot:



```
root@kali:~# macchanger --random eth0
Current MAC: 00:0c:29:7e:37:58 (VMware, Inc.)
Permanent MAC: 00:0c:29:7e:37:58 (VMware, Inc.)
New MAC: 46:de:38:c8:78:ed (unknown)
```

4. Once the MAC address has been changed successfully, it's time to turn on the Ethernet interface by using the following command:

```
ifconfig eth0 up
```

5. Finally, we can now use the `ifconfig` command to verify whether the new MAC address is registered on the interface, as shown in the following screenshot:



```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.1 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 2803:1500:1201:9991::1 prefixlen 64 scopeid 0x0<global>
    inet6 2803:1500:1201:9991::2 prefixlen 64 scopeid 0x0<global>
    inet6 fe80::44de:38:c8:78:ed prefixlen 64 scopeid 0x20<link>
    ether 46:de:38:c8:78:ed txqueuelen 1000 (Ethernet)
    RX packets 162 bytes 183839 (179.5 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 141 bytes 12729 (12.4 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```


Having completed this exercise, you are now capable of spoofing the MAC address on each network interface in Kali Linux. In the next section, we will learn about connecting a wireless adapter to a Kali Linux machine.

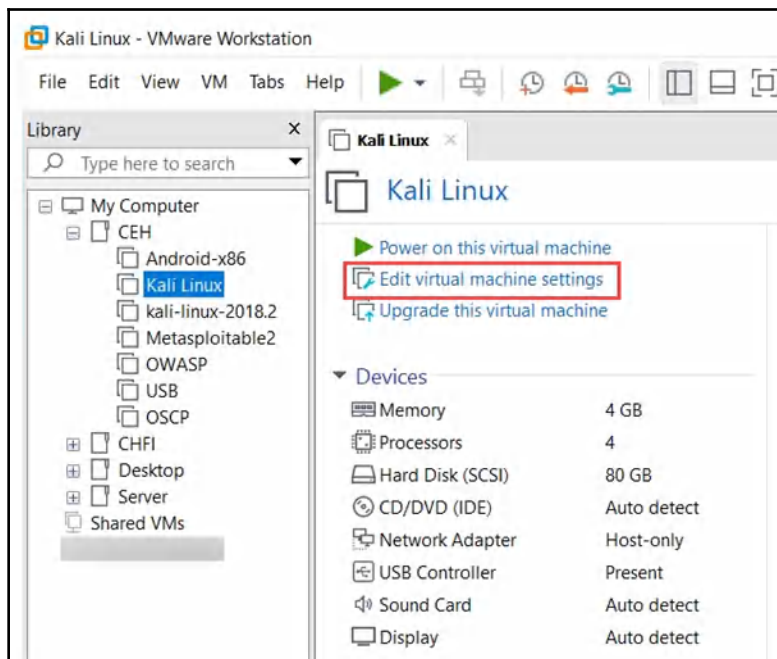
Connecting a wireless adapter to Kali Linux

During a wireless network penetration test, you will be required to attach an external wireless NIC to your Kali Linux machine. If you have Kali Linux installed directly on a disk drive, attaching a wireless NIC is as simple as connecting it via USB. The adapter will automatically be present within the network settings.

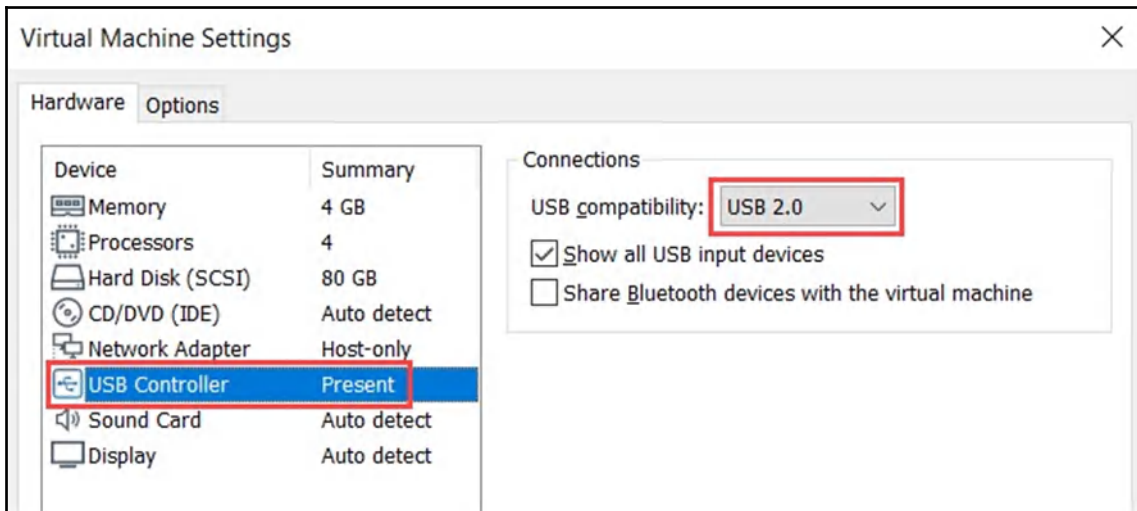
However, things can get a bit tricky when using virtual machines. In this section, I will demonstrate how to attach a wireless network adapter to both **VMware Workstation** and **Oracle VM VirtualBox**.

If you're using VMware Workstation, follow these steps:

1. First, select the Kali Linux virtual machine and click on **Edit virtual machine settings**:



- Then, the virtual machine settings will open, providing you with a number of options to add, remove, and modify the emulated hardware resources. Select the **USB Controller**; the options will appear to the right of the window. Select the appropriate USB version based on the physical USB controllers on your computer and ensure there is a tick in the checkbox for **Show all USB input devices**:



- Now that you're finished, click on **OK** to save the settings. Power on the Kali Linux virtual machine and plug your wireless adapter into an available USB port on your computer.

In the bottom-right corner of VMware Workstation, you'll see some icons. These icons represent a physical hardware component or device. The faded icons indicate that the hardware or device is not connected to the virtual machine, while the brightly colored icons indicate that the component or device is connected.

- Click on the USB icon highlighted in the following screenshot. A menu will appear, providing the option to attach a USB device from your host machine to the virtual machine. Select the wireless adapter:



5. Once the USB wireless adapter has been successfully attached, the icon should be bright. Now, it's time to verify whether Kali Linux is able to see the wireless adapter. Open a Terminal and execute the `ifconfig` command:

```
root@kali:~# ifconfig
eth0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    ether 00:0c:29:... txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

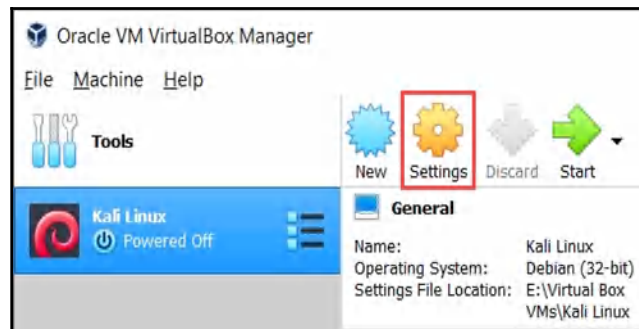
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 16 bytes 960 (960.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 16 bytes 960 (960.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

wlan0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    ether 9e:0f:8b:... txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

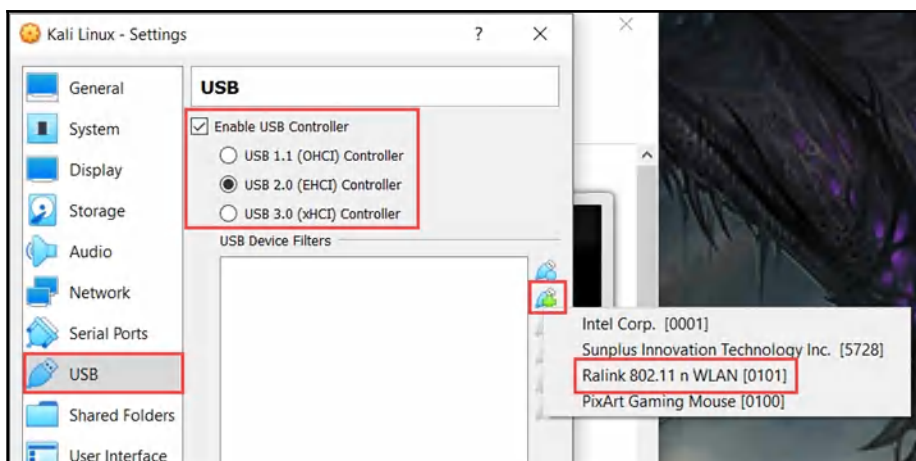
All wireless adapters are represented as `wlan`, followed by a number. Our wireless adapter is `wlan0`.

For those who are using **Oracle VM VirtualBox**, the process is a bit similar to what was mentioned previously for VMware. Use the following steps to complete this exercise of connecting a wireless adapter to Kali Linux through the hypervisor:

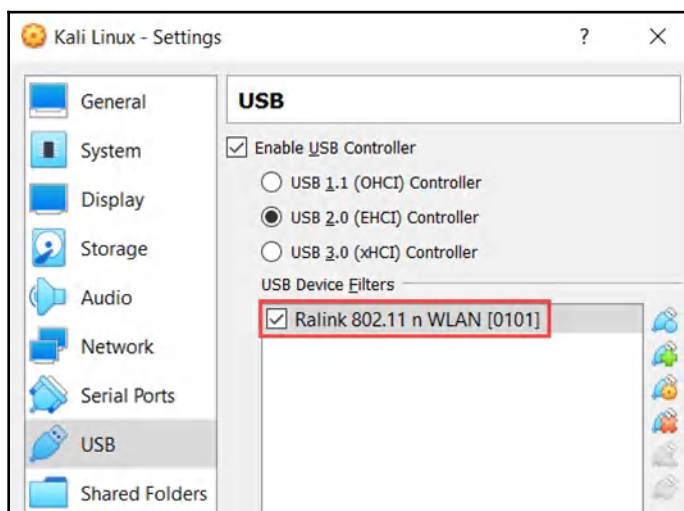
1. To get started, select the Kali Linux virtual machine within the dashboard and click on **Settings**:



2. Once the settings menu has opened, select the **USB** category on the left column. Ensure the wireless adapter is plugged into a USB port on your computer and, similar to what we did for VMware Workstation, select the **USB 2.0 (EHCI) Controller** version.
3. Next, click the **USB** icon with the + symbol next to it to attach a USB device to the virtual machine. Select the USB wireless adapter:



The wireless adapter will be inserted into the **USB Device Filters** field, as shown in the following screenshot:



4. Click on **OK** to save the settings of the virtual machine. Power on the Kali Linux virtual machine and use the `ifconfig` command to verify the status of the wireless adapter.

Completing this section has provided you with the necessary skills to successfully connect a wireless adapter to a Kali Linux virtual machine. In the next section, we will take a look at how to manage and monitor wireless modes in Kali Linux.

Managing and monitoring wireless modes

The Linux OS allows users to manually configure the mode of operation for wireless adapters.

The following are the different modes and explanations of what they entail:

- **Ad hoc** mode is used to interconnect multiple end devices, such as laptops, without the use of a wireless router or access point.
- The default mode of operation is **managed**. This mode allows the device (that is, the host) to connect to wireless routers and access points. However, at times, you may be required to perform a wireless penetration test on an organization's Wi-Fi network. A wireless adapter in managed mode is not suitable for such a task.
- **Master** mode allows the Linux device to operate as an access point to allow other devices to synchronize data.
- **Repeater** mode allows the node device to forward packets to other nodes on the network; repeaters are usually implemented to extend the range of a wireless signal.
- **Secondary** mode allows the device to function as a backup for the master or repeater.
- **Monitor** mode allows a device to pass monitor packets and frames on the frequencies of IEEE 802.11. This mode would allow a penetration tester to not only monitor traffic but also capture data and perform **packet injection** using a compatible wireless adapter.



The mode of operation depends on the network topology and the role of your Linux OS in your network.

There are two methods we can use to configure the wireless adapter in monitor mode: manually and by using the `airmon-ng` tool.

In the following section, we will take a look at doing the following:

- Enabling monitor mode manually
- Enabling monitor mode using airmon-ng

Let's look at each of these methods in more detail.

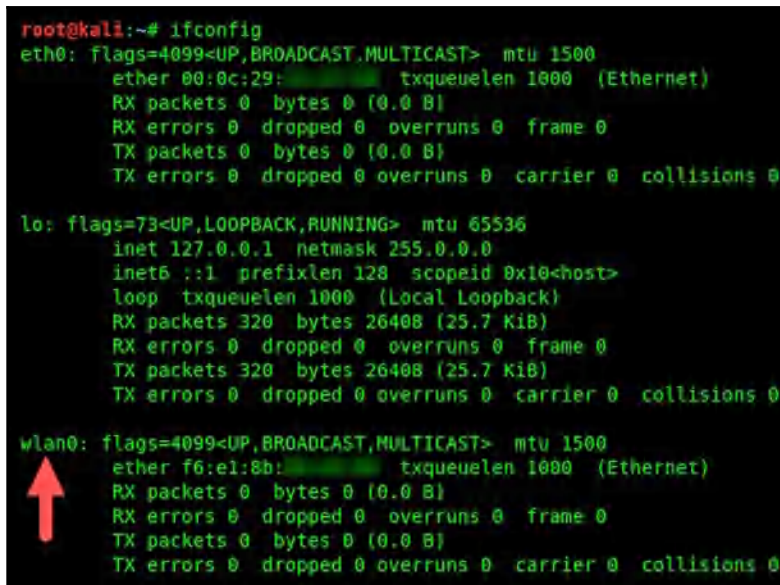
Enabling monitor mode manually

In this section, I'll guide you through the steps you need to take to manually enable monitor mode on the wireless NIC of your Kali Linux machine.

The following instructions will guide you through the process of enabling monitor mode manually on your Kali Linux machine.

To get started, open a new Terminal window and execute the following commands:

1. Execute the `ifconfig` command to determine whether the wireless adapter is connected and recognized by the Kali Linux OS. Additionally, take note of the interface ID. In the following screenshot, the interface is `wlan0`:

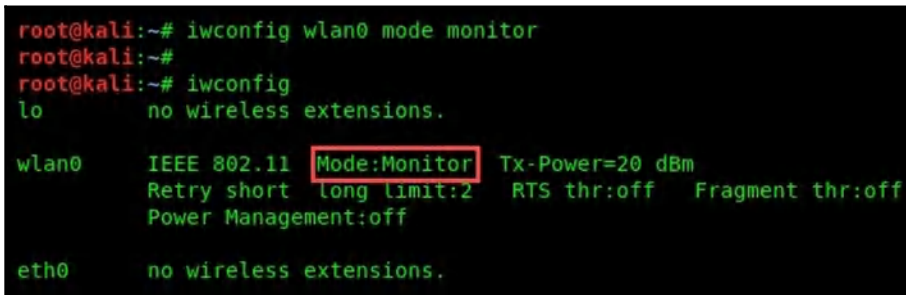


```
root@kali:~# ifconfig
eth0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    ether 00:0c:29:12:34:56 txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 320 bytes 26408 (25.7 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 320 bytes 26408 (25.7 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

wlan0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    ether f6:e1:8b:12:34:56 txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

2. Now that we have the interface ID, use `ifconfig wlan0 down` to logically turn down the interface via the OS. This is necessary prior to changing the mode of any interface.
3. Now that the interface is down, it's time to configure our `wlan0` interface for monitor mode. The `iwconfig wlan0 mode monitor` command will enable monitor mode. Once completed, we need to verify that the mode has been changed successfully on the interface. Execute the `iwconfig` command. You should see that the mode has changed to `Monitor`, as shown in the following screenshot:



```
root@kali:~# iwconfig wlan0 mode monitor
root@kali:~#
root@kali:~# iwconfig
lo        no wireless extensions.

wlan0     IEEE 802.11  Mode:Monitor Tx-Power=20 dBm
          Retry short  long limit:2   RTS thr:off   Fragment thr:off
          Power Management:off

eth0      no wireless extensions.
```

4. Lastly, we need to turn up our `wlan0` interface by using the `ifconfig wlan0 up` command.

Having completed this exercise, you have attained the required skills to enable monitor mode in Kali Linux. In the next section, we will take a look at using `airmon-ng` to configure the wireless adapter.

Enabling monitor mode using `airmon-ng`

`airmon-ng` is part of the `aircrack-ng` suite of wireless security auditing tools. `airmon-ng` is a tool that's used to configure a wireless adapter into (and out of) monitor mode.

Let's see how we can enable and disable monitor mode:

1. To get started, open a new Terminal window and execute either the `ifconfig` or `iwconfig` command to verify the wireless adapter status and ID:

```
root@kali:~# iwconfig
lo        no wireless extensions.

wlan0     IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated  Tx-Power=20 dBm
          Retry short long limit:2   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off

eth0      no wireless extensions.
```

2. Before enabling monitor mode, we need to kill any background processes that may prevent the adapter from being converted into monitor mode. By using the `airmon-ng check kill` command, the tool will check for any processes that may prevent the adapter from converting into monitor mode and kill them:

```
root@kali:~# airmon-ng check kill

Killing these processes:

PID Name
590 wpa_supplicant
```

3. Next, execute `airmon-ng start wlan0` to enable monitor mode. Additionally, a new logical interface will be created, as shown in the following screenshot:

```
root@kali:~# airmon-ng start wlan0

PHY      Interface      Driver      Chipset
phy0     wlan0           rt2800usb   Ralink Technology, Corp. RT5372

(mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0] wlan0mon)
(mac80211 station mode vif disabled for [phy0]wlan0)
```

4. The `wlan0mon` interface will be used to monitor IEEE 802.11 networks. To disable monitor mode, simply use the `airmon-ng stop wlan0mon` command.

By completing this exercise, you can now enable monitoring on a wireless adapter using both the manual method and the `airmon-ng` tool.

Summary

In this chapter, we discussed the fundamentals and concepts of network penetration testing and its importance. We covered hands-on information about connecting a wireless adapter to our Kali Linux machine, discussed the purpose of a MAC address and its composition, and talked about how to spoof our identity by modifying it. Furthermore, we took a look at changing the default mode of our wireless adapter to monitor mode, via both manual configuration and using the `airmon-ng` tool.

Now that you have completed this chapter, you know how to properly enable monitor mode using both the `airmon-ng` tool and manually through the Kali Linux OS. Additionally, you are now able to perform monitoring on wireless networks.

I hope this chapter has been informative and is able to assist and guide you through your journey in the field of cybersecurity. In the next chapter, *Chapter 9, Network Penetration Testing - Pre-Connection Attacks*, we will take a deeper look into network penetration testing with some hands-on exercises.

Questions

The following are some questions based on the topics we have covered in this chapter:

1. What tool can be used to change the MAC address in Kali Linux?
2. Can you name the different modes in which a wireless adapter can be configured to operate?
3. How do you view the MAC address of a network interface?
4. How do you kill any background processes that may prevent the adapter from converting into monitor mode?

Further reading

- Further details on the OSI model and the TCP/IP stack can be found in the *CompTIA Network+ Certification Guide* at <https://www.packtpub.com/networking-and-servers/comptia-network-certification-guide>.
- For additional information on aircrack-ng and airmmon-ng, please see <https://www.aircrack-ng.org/documentation.html>.