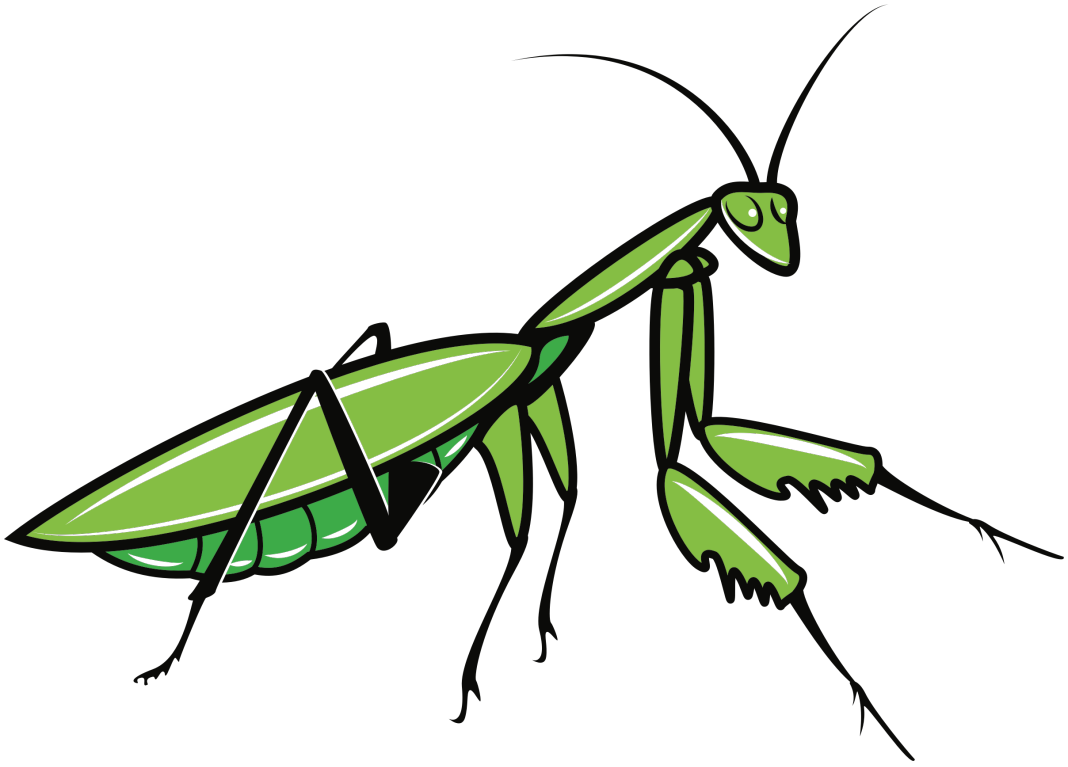
Hack The Box
PEN-TESTING LABS

Technical report

Machine Mantis



January 23 of 2022

Contents

1 Disclaimer

A penetration test is considered a snapshot in time. The findings and recommendations reflects the information gathered during the assessment and not any changes or modifications made outside of that period.

Time-limited engagements do not allow for a full evaluation of all security controls. **Your Company Name** prioritized the assessment to identify the weakest security controls an attacker would exploit. **Your Company Name** recommends conducting similar assessments on an annual basis by internal or third-party assessors to ensure the continued success of the controls.

1.1 Confidentiality Statement

This document is the exclusive property of Demo Company (DC) and **Your Company Name**. This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent of both DC and TCMS.

TCMS may share this document with auditors under non-disclosure agreements to demonstrate penetration test requirement compliance.

1.2 Contact info

Your Company Namecontact			
Name	Title	Email	Contact
Juan	Cybersecurity Lead	juan@test	(99) 9999 9999
Manuel	Junior Pentester	manuel@test	(99) 9999 9999
Young	Junior Pentester	young@test	(99) 9999 9999

1.3 Assesment overview

From *Date 1* to *Date 2*, **Your Company Name** engaged Penetration tests to evaluate the security posture of its infrastructure compared to current industry best practices. All testing performed is based on the NIST SP 800-115 Technical Guide to Information Security Testing and Assessment, OWASP Testing Guide (v4), and customized testing frameworks.

Phases conducted for penetration testing are the following:

- Planning and preparation.
- Reconnaissance / Discovery.
- Vulnerability Enumeration / Analysis.
- Initial Exploitation.
- Expanding Foothold / Deeper Penetration.
- Cleanup.
- Report Generation.

2 Antecedents

The following document takes all the processes and results given by the audit made to the machine **Mantis** from the platform **HackTheBox**.

Figure 1: Details of the machine

URL

https://app.hackthebox.com/machines/98

2.1 considerations

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Curabitur molestie nulla nec hendrerit blandit. Aenean euismod tincidunt sapien at lacinia. Praesent at tortor nec nunc sodales posuere in eu mi. Fusce ac fringilla velit. Nam libero leo, consequat sit amet est varius, imperdiet iaculis massa. Suspendisse scelerisque eu erat eu cursus. Vivamus ac euismod ex. Integer euismod sem et euismod mattis. Integer vel rutrum velit, eu dictum nisi. Pellentesque venenatis et nisi a sodales. Integer pretium ut nisi at fringilla. Quisque nunc dui, consequat id turpis non, dignissim consectetur nunc.

2.2 examples

Morbi id turpis bibendum, ultrices turpis eu, molestie nunc. Duis aliquet aliquam turpis, vitae ultricies turpis. Ut tristique elementum nunc ac euismod. Proin viverra ultrices enim, et bibendum sem dignissim venenatis. Pellentesque non lectus nec erat congue viverra feugiat a urna. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia curae; Nam vel ex sit amet nulla mollis lacinia. Nulla vehicula orci sit amet fermentum egestas. Mauris blandit ultricies sem, id convallis nunc malesuada non. Morbi venenatis ultricies leo, vel ullamcorper ligula mattis a.

3 Objectives

The idea is to check the machine state of the machine **images/mantis.png**.

3.1 considerations

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Curabitur molestie nulla nec hendrerit blandit. Aenean euismod tincidunt sapien at lacinia. Praesent at tortor nec nunc sodales posuere in eu mi. Fusce ac fringilla velit. Nam libero leo, consequat sit amet est varius, imperdiet iaculis massa. Suspendisse scelerisque eu erat eu cursus. Vivamus ac euismod ex. Integer euismod sem et euismod mattis. Integer vel rutrum velit, eu dictum nisi. Pellentesque venenatis et nisi a sodales. Integer pretium ut nisi at fringilla. Quisque nunc dui, consequat id turpis non, dignissim consectetur nunc.

3.2 results

Morbi id turpis bibendum, ultrices turpis eu, molestie nunc. Duis aliquet aliquam turpis, vitae ultricies turpis. Ut tristique elementum nunc ac euismod. Proin viverra ultrices enim, et bibendum sem dignissim venenatis. Pellentesque non lectus nec erat congue viverra feugiat a urna. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia curae; Nam vel ex sit amet nulla mollis lacinia. Nulla vehicula orci sit amet fermentum egestas. Mauris blandit ultricies sem, id convallis nunc malesuada non. Morbi venenatis ultricies leo, vel ullamcorper ligula mattis a.

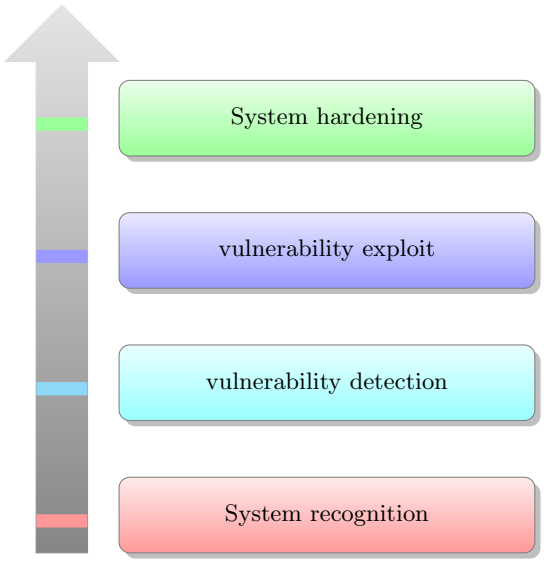


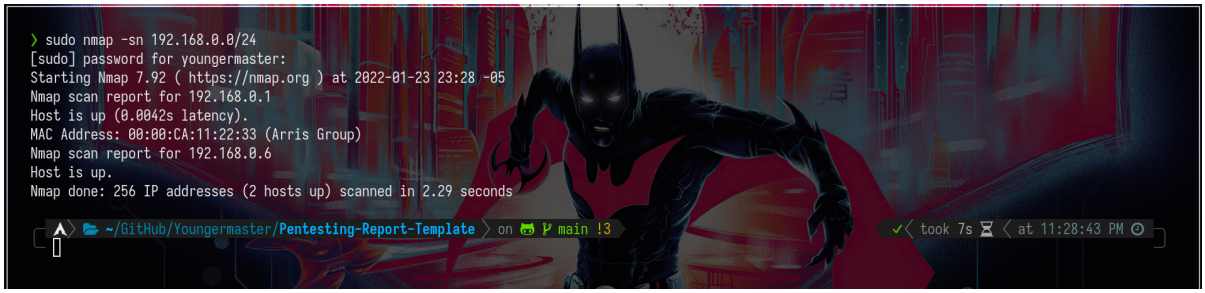
Figure 2: Workflow

4 Vulnerability analysis

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Curabitur molestie nulla nec hendrerit blandit. Aenean euismod tincidunt sapien at lacinia. Praesent at tortor nec nunc sodales posuere in eu mi.

4.1 Initial Recognition

Fusce ac fringilla velit. Nam libero leo, consequat sit amet est varius, imperdiet iaculis massa. Suspendisse scelerisque eu erat eu cursus. Vivamus ac euismod ex. Integer euismod sem et euismod mattis. Integer vel rutrum velit, eu dictum nisi. Pellentesque venenatis et nisi a sodales. Integer pretium ut nisi at fringilla. Quisque nunc dui, consequat id turpis non, dignissim consectetur nunc.



4.2 Improvement

Morbi id turpis bibendum, ultrices turpis eu, molestie nunc. Duis aliquet aliquam turpis, vitae ultricies turpis. Ut tristique elementum nunc ac euismod. Proin viverra ultrices enim, et bibendum sem dignissim venenatis. Pellentesque non lectus nec erat congue viverra feugiat a urna. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia curae; Nam vel ex sit amet nulla mollis lacinia. Nulla vehicula orci sit amet fermentum egestas. Mauris blandit ultricies sem, id convallis nunc malesuada non. Morbi venenatis ultricies leo, vel ullamcorper ligula mattis a.

```
# This function is taken from S4vitar's blog.
# https://s4vitar.github.io/bspwm-configuration-files/

ports="$(cat $1 | grep -oP '\d{1,5}/open' | awk '{print $1}' FS='/' | xargs | tr ' ' ',')"
ip_address="$(cat $1 | grep -oP '\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}' | sort -u | head -n 1)"
echo -e "\n[*] Extracting information...\n" > extractPorts.tmp
echo -e "\t[*] IP Address: $ip_address"  >> extractPorts.tmp
echo -e "\t[*] Open ports: $ports\n"  >> extractPorts.tmp
echo $ports | tr -d '\n' | xclip -sel clip
echo -e "[*] Ports copied to clipboard\n"  >> extractPorts.tmp
cat extractPorts.tmp; rm extractPorts.tmp
```

Code 1: This script allow us to extract nmap generated info

Donec ut tincidunt dolor. Curabitur sit amet porttitor magna, nec consectetur mi. Praesent quis congue tellus, a tincidunt mauris. Aenean sed luctus enim. Donec ut maximus nisi, sed malesuada erat. Aliquam sollicitudin ullamcorper sem vitae ultrices. Sed iaculis enim egestas, suscipit arcu ac, lacinia risus. Proin scelerisque mi eu feugiat euismod:

TCP
Ports
593, 1337

Vivamus vitae elit porta, tempor justo tincidunt, accumsan ligula. Proin nec magna sit amet leo dignissim sollicitudin sit amet ut quam:

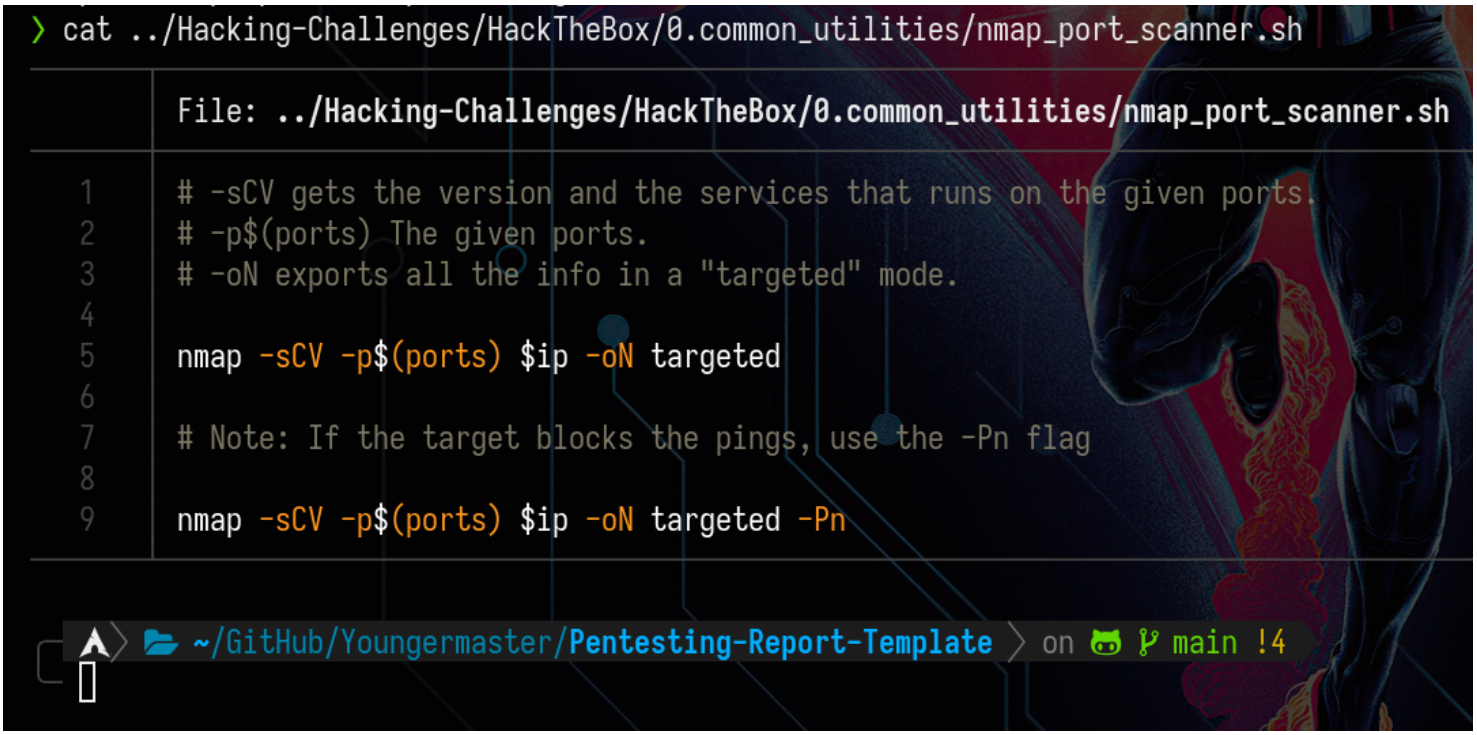


Figure 3: These are the results of lorem ipsum

Ut vulputate fermentum scelerisque 3 and 6. Interdum et malesuada fames ac ante ipsum primis in faucibus.