Hack The Box
PEN-TESTING LABS

Technical report

Machine Mantis
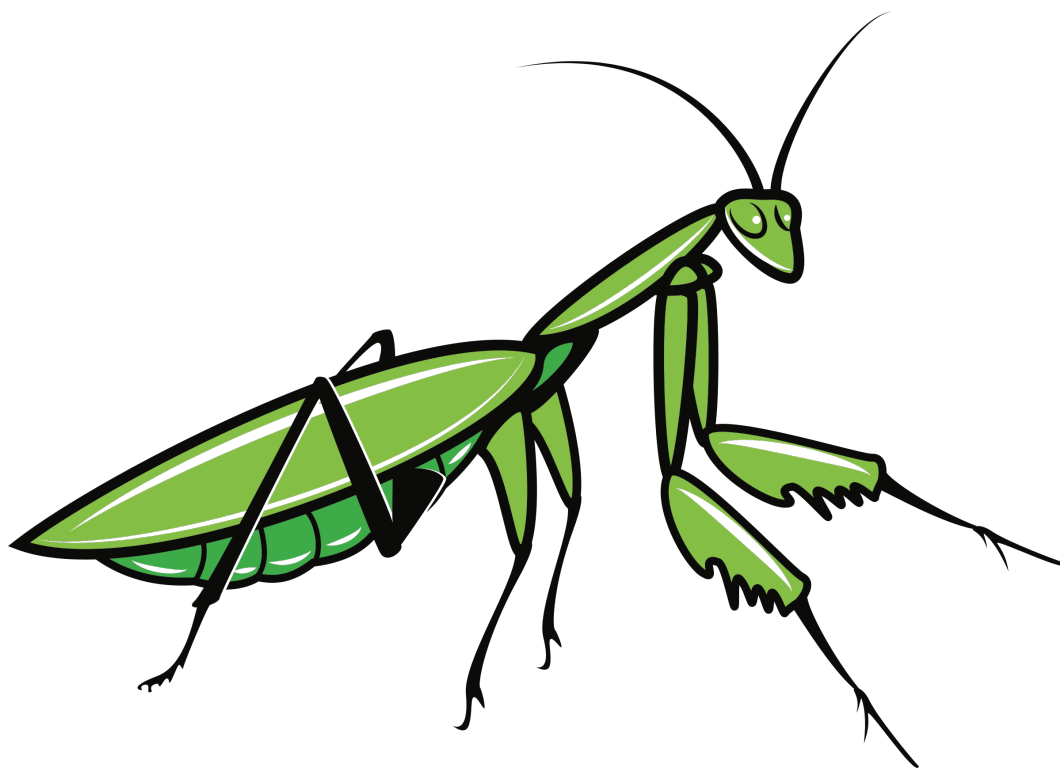
January 23 of 2022

Contents

1   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

1.1   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.

1.2   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.

2 Objectives

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

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 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.
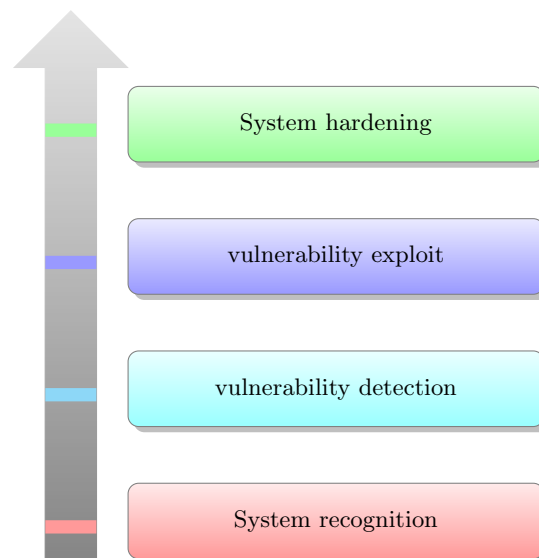

Figure 2: Workflow

3 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.

3.1 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.
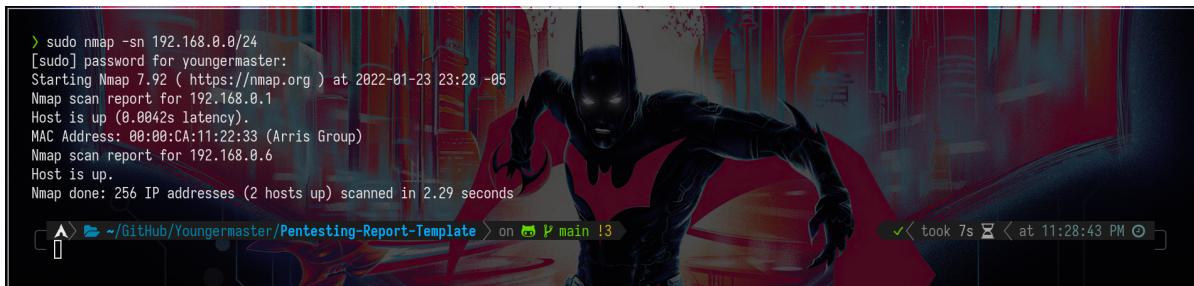
3.2 Improvement

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.

```
1  # This function is taken from S4vitar's blog.
2  # https://s4vitar.github.io/bspwm-configuration-files/
3
4  ports="$(cat $1 | grep -oP '\d{1,5}/open' | awk '{print $1}' FS='/' | xargs | tr ' ' ',')"
5  ip_address="$(cat $1 | grep -oP '\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}' | sort -u | head -n 1)"
6  echo -e "\n[*] Extracting information...\n" > extractPorts.tmp
7  echo -e "\t[*] IP Address: $ip_address"  >> extractPorts.tmp
8  echo -e "\t[*] Open ports: $ports\n"  >> extractPorts.tmp
9  echo $ports | tr -d '\n' | xclip -sel clip
10 echo -e "[*] Ports copied to clipboard\n"  >> extractPorts.tmp
11 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 5. Interdum et malesuada fames ac ante ipsum primis in faucibus.