



Black Fox Bandits

Deontae | Geneva | Jordan | Sierra

Agenda

Team Member Introductions

Problem Domain & Project Overview

Team Process & Documentation

Application Demonstration

Q&A

Our Team

Deontae Carter

Geneva Knott

Sierra Maldonado

Jordan Marshall



Jordan Marshall

- USAF Medic
- Bodybuilding physique competitor
- Working in healthcare for the past 10 years
- I chose cybersecurity to learn a new skill



by
&



Connect with me
on LinkedIn!

Sierra Maldonado

- US Navy Veteran, Seabee
- ITF+, PCAP - Entry
- Six Sigma White belt in HR
- Accepted to ASU Pre-Vet Program
- Connect with me on linkedin!



LinkedIn



Deontae Carter

- Navy Veteran
- Dual Certified
- Passion for Cybersecurity Operations

Connect With Me





Geneva Knott

- Marine Corps Veteran- 0621 Communications
- 9 yo LE/Criminal Investigator -Violent Crimes w/ Bachelors in Criminal Justice
- Working on Associates in Cyber Defense

LinkedIn



by
&



Project Overview

Our team is tasked with conducting a network security assessment and penetration testing for Hermis network infrastructure. The objective is to identify vulnerabilities and weaknesses in the network's security defenses and provide recommendations for improvement.



Process and Documentation

This repository contains the scripts, and documentation for our Network Security Assessment.



This project is intended for educational and ethical purposes only.

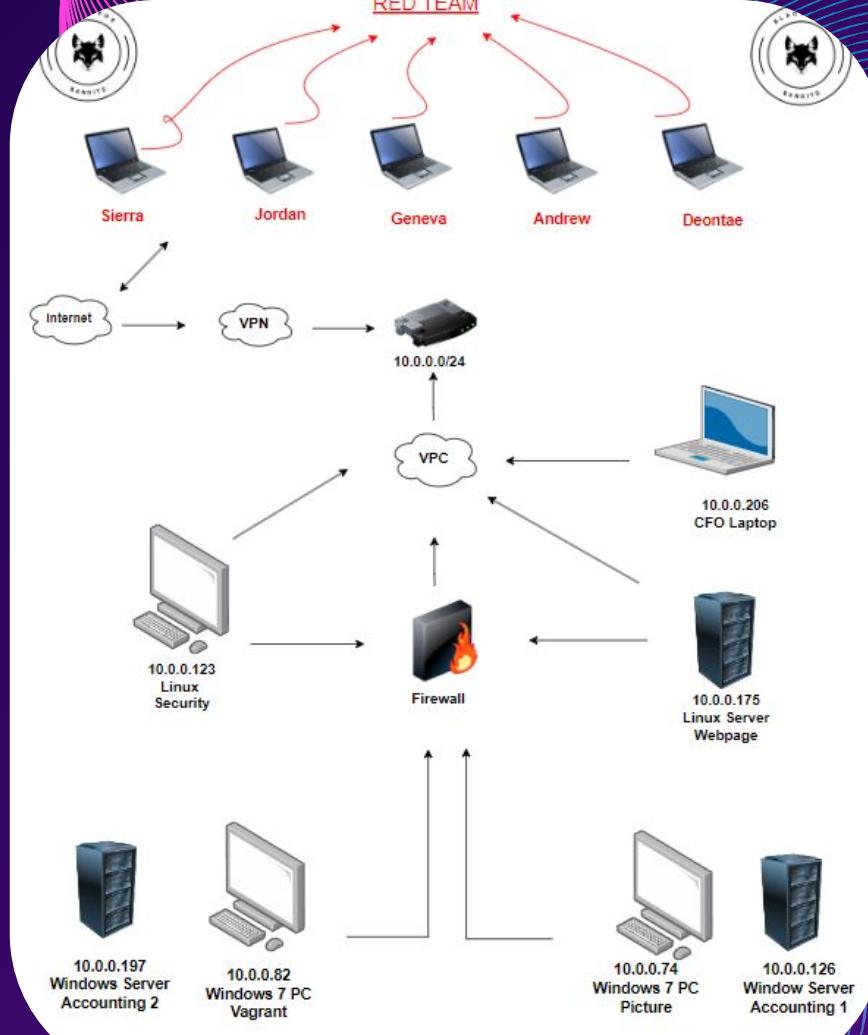
Screenshot of the GitHub repository page for "Black-Fox-Bandits".

The repository features a custom logo depicting a fox wearing a beret and holding a sword. The README file displays a creative graphic where the text "Data Thieves" is formed by a grid of numbers, with two red hand icons pointing towards it. Below the graphic, the text "Welcome to our team project" is followed by a thumbs-up emoji. A note states "We are Data Thieves. 🐱 The Black Fox Bandits 🎉🎉".

The "Description of our project" section explains the objective: "The objective of this project is to conduct a comprehensive penetration test on Company Hermes network infrastructure, systems, and applications. The purpose is to identify potential security vulnerabilities and weaknesses that could be exploited by unauthorized individuals. By simulating real-world attacks, the project aims to assess the company's security posture and provide recommendations for remediation."

On the right side of the repository page, there are sections for "View as: Public", "Discussions", "People", and "Top languages" (Python).

Network Topology





10.0.0.74 - Windows 7

Port	State / Service
135 / TCP	Open / MSRPC
139 / TCP	Open / NetBios-ssn
445 / TCP	Open / Microsoft-ds
554 / TCP	Open / RTSP
2869 / TCP	Open / HTTP
3389 / TCP	Open / SSL / Ms-wbt-server
5357 / TCP	Open / HTTP
8089 / TCP	Open / SSL HTTP

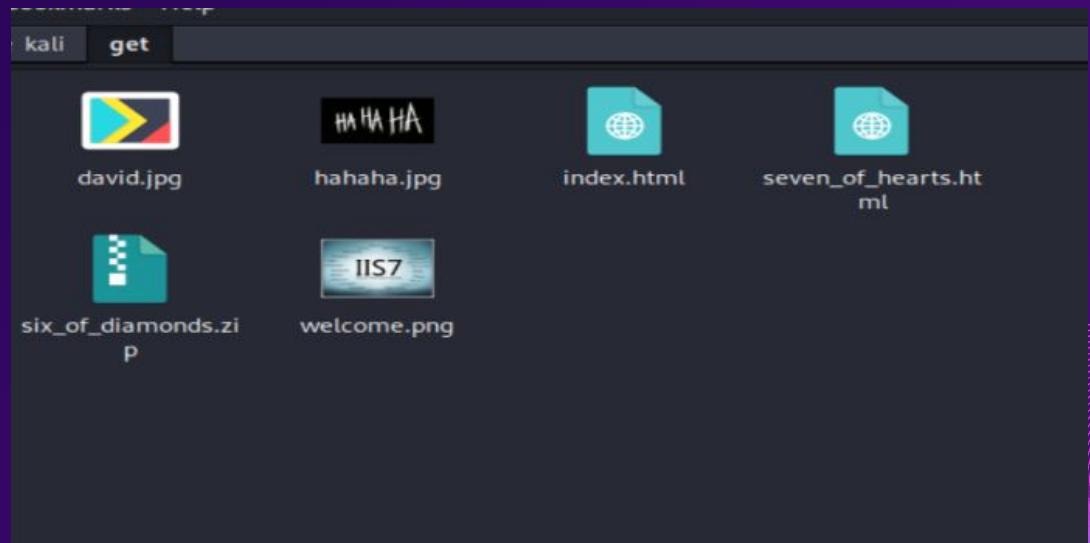
10.0.0.82 - Windows 7



Port	State / Service
21 / TCP	Open / FTP
80 / TCP	Open / HTTP
3389 / TCP	Open / Ms-wbt-server



10.0.0.82 - Windows 7



10.0.0.123 - Linux

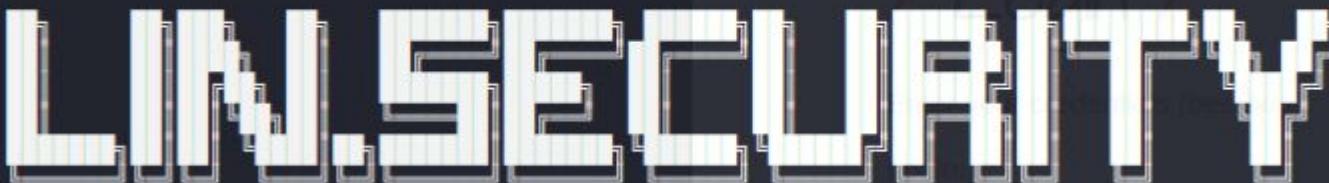


Port	State / Service
22 / TCP	Open / OpenSSH
111 / TCP	Open / Rpcbind
2049 / TCP	Open / Nfs_aci
8089 / TCP	Open / Ssl/http



10.0.0.123 - Linux

```
The authenticity of host '10.0.0.123 (10.0.0.123)' can't be established.  
ED25519 key fingerprint is SHA256:anPRcsI68yyyGmGTThL+wwTeplg+FcJcWjtzjkXxQG0.  
This key is not known by any other names.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '10.0.0.123' (ED25519) to the list of known hosts.
```



Welcome to lin.security | <https://in.security> | version 1.0

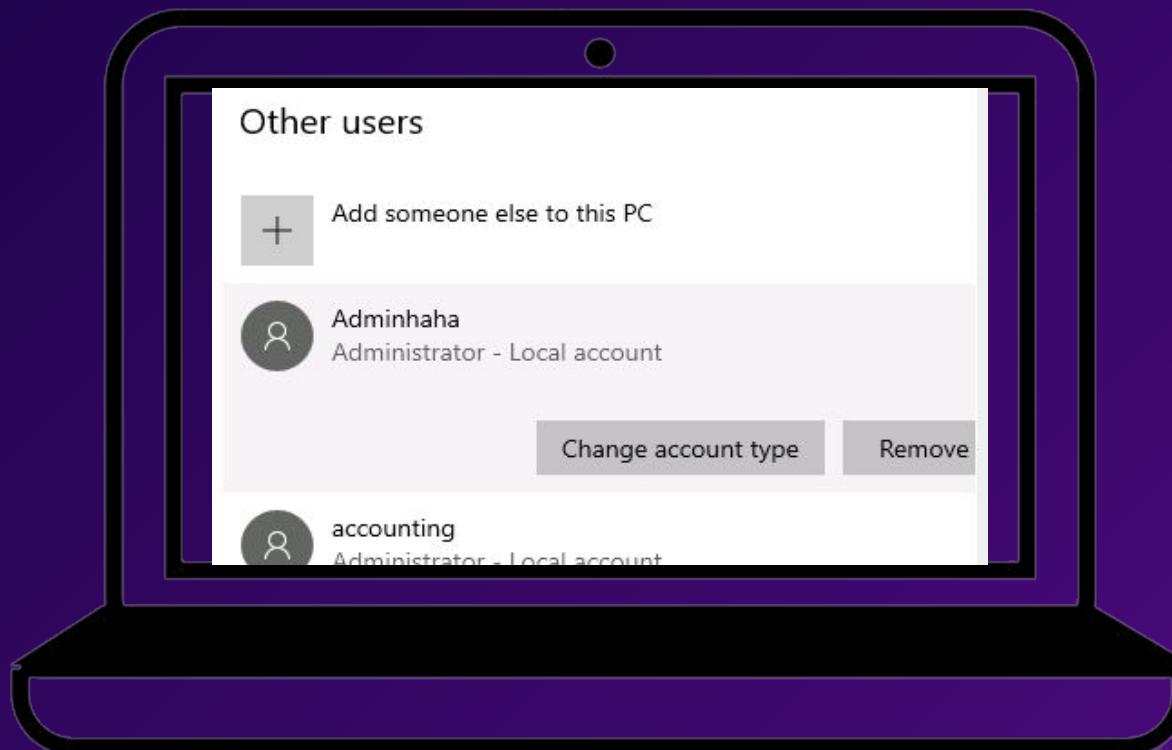
peter@linsecurity:~\$ █

Password:

10.0.0.126 - Windows Server 2019

Port	State / Service
135 / TCP	Open / Msrpc
139 / TCP	Open / NetBios-ssn
455 / TCP	Open / Microsoft-ds
3389 / TCP	Open / Ms-wbt-server
8089 / TCP	Open / unknown

10.0.0.126 - Windows Server 2019



10.0.0.175 - Linux



Port	State / Service
22 / TCP	Open / SSH
80 / TCP	Open / HTTP
8089 / TCP	Open / Unknown



10.0.0.175 - Linux



The image shows a web browser window displaying the SimCorp login page. The header features the SimCorp logo, which includes a stylized bee icon above the word "SimCorp" and the tagline "multi-asset investment management s". Below the header, there are two buttons: "Login" in yellow and "New User" in white. The main content area has a light gray background with the word "Login" in large, colorful, slanted letters. Below it, a sub-instruction reads "Enter your credentials (bee/bug)". There are two input fields: one for "Login:" containing a placeholder "username" and another for "Password:" containing a placeholder "password". In the bottom right corner of the page, there is a small logo for "NATIONAL CENTER F MISS EXP CHI".

SimCorp

multi-asset investment management s

Login New User

/ Login /

Enter your credentials (bee/bug).

Login:

Password:

10.0.0.197 - Windows Server 2019



Port	State / Service
135 / TCP	Open / Msrpc
139 / TCP	Open / NetBios-ssn
455 / TCP	Open / Microsoft-ds
3389 / TCP	Open / Ms-wbt-server
8089 / TCP	Open / unknown

10.0.0.197 - Windows Server 2019

Other users

+ Add someone else to this PC

-  FoxBandits
Administrator - Local account
-  Irwin
Local account
-  accounting
Local account
-  general-user
Local account
-  user
Local account

10.0.0.206 Window Server 2008

Port	State / Service
135	Open / Msrpc
139	Open / NetBios-ssn
445	Open / mircrosoft-ds
3389	Open / ms-wbt-server
5357	Open http
8089	ssl/http

10.0.0.206 Window Server 2008

Name	Full Name	Description
accounting	accounting	
Administrator		Built-in account for administering...
cfo	cfo	
DefaultAcco...		A user account managed by the s...
FluffyFox	FluffyFox	
general-user	general-user	
Guest		Built-in account for guest access t...
WDAGUtility...		A user account managed and use...

Hermis?



Demo

Resources and Thanks

ChatGPT

<https://chat.openai.com/>

Google

[https://www.google.com/
/](https://www.google.com/)



Stack Overflow

<https://stackoverflow.com/>

Our Classmates

Code Fellows



Questions?