

Lab 8.1 - Weeveily

💡 Webshells like simple-backdoor.php are effective but are not terribly stealthy. Basic IDS/IPS systems will be able to detect "shell-like" behavior by seeing content that looks like commands, prompts and sensitive files like /etc/passwd.

Wireshark Capture of traditional webshell

Target pippin with a traditional webshell (one without encryption or obfuscation). Capture a dump of /etc/passwd using Wireshark on your interface.

Deliverable 1. Provide a screenshot that shows the relevant tcp stream similar to the one below. Create a capture filter on port 80 when you do so.

```

Wireshark · Follow TCP Stream (tcp.stream eq 2) · wg0 (port 80)

X-Powered-By: PHP/7.3.31
Content-Length: 1402
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<!-- Simple PHP backdoor by DK (http://michaeldaw.org) -->

<pre>root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/www/html:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
systemd-network:x:192:192:systemd Network Management:/:/sb
dbus:x:81:81:System message bus:/:/sbin/nologin
1 client pkt, 2 server pkts, 1 turn.

```

3/18/2022

Deliverable 2. Investigate weeveily (a tool in kali). Create a php agent that is uniquely named, upload the agent to pippin and carry on a session similar to the one shown in the screenshot. Provide a screenshot of your session

```
[+] weeveily 4.0.1

[+] Target:      10.0.5.25
[+] Session:     /home/champuser/.weeveily/sessions/10.0.5.25/hermi
one_0.session

[+] Browse the filesystem or execute commands starts the connecti
on
[+] to the target. Type :help for more information.

weeveily> id
uid=48(apache) gid=48(apache) groups=48(apache)
pippin:/var/www/html/upload $ whoami
apache
pippin:/var/www/html/upload $
```

Deliverable 3. Provide a screenshot similar to the one below that displays the encoded tcp stream from a weeveily dump of /etc/passwd. Make sure to use a capture filter of port 80, to limit traffic.

Wireshark · Follow TCPStream (tcp.stream eq 1) · wg0 (port 80)

File Actions Edit View Help

inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 74 bytes 6612 (6.4 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 74 bytes 6612 (6.4 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0

pippin:/var/www/html/upload \$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/www/html:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
systemd-network:x:192:192:systemd Network Management
dbus:x:81:81:System message bus:/:/sbin/nologin

NAcKSzLBVe3odWKPweUZftwaDRGGuhYjDSn8ZiQpB1MwCpqd3cHANKdb
d7f8.C;C\)\xaG.a*-u{HTTP/1.1 200 OK
Date: Thu, 21 Oct 2021 13:37:18 GMT
Server: Apache/2.4.6 (CentOS) PHP/7.3.31
X-Powered-By: PHP/7.3.31
Content-Length: 784
Connection: close
Content-Type: text/html; charset=UTF-8

4TP4b0xF2TYoYN0C3b01bfeea7f4S6sDowv0vhU/t7lGPDkFft8T0/
ZtXV6ojduoe+V4ZS5RTKRqN0H+7mQ1wbz/
Rn08TldHPqpX5EvhAlKyHC8GD1n1VAqaJmRC0jpTJzHp01iX3iGI1CpN
GLdQQX03R1LVfzIjptKlWVp6J7y+0aN9ERqpdUmzeJUIP12fxXF0dEjS
BilF3nidMUAEMVPIZE6zFleTvK00W18/5J5ZoaPfchbzPKHnRKuPdAPL
PORBisD8EvUSUWUgkgRW4K8Y7pqPuul5oCoca+zTRN/
1FJsLcFhspcqFVYghTHIAHH+UOCTEIUun8IskGfdpo1tOucCCH0j+A4h
tdNamsXBfMTgatJj60n0t8aZWwn45dsIDo+S0hIP/pP/
XwKYu6ZVkfShZlREW1CabjfmSjBkwUFT06ZLvkUzmhrDUaAPYvK4ldw8
D8tjz8u3ij4QUQssVF1wIqcoqw6uTI90l6NjivTiJTgd8YbXXo9TGvYgl
v8Cl5xniAhDVY2NC8CBVzlg5dum3HqGAHE2gbj3+MxbSZlKgKo0ZrCM
FGMPryiJYpi+cXGuhP3FvpyeRwrNq4Ws3KeZj0GgFhWDGZRY3+QxaCDK
Dc8XN2w0+EdtoPwsJl4TibxJJAIwa9/42P4d7pSnedN3yyjh9CvqS436

Deliverable 4. Tech Journal

Provide a link to your usage documentation on weeveily and make sure to include reflections on this assignment.