## Lab 8.1 - Weevely

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

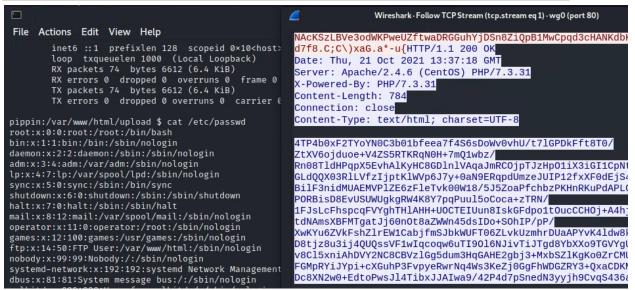
Target pippin with a traditional webshell (one without encryption or obfuscation). Capture a dump of /etc/passwd using Wireshark on your interface.

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)
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
dhus:v:81:81:System message hus:/:/shin/nologin
1 <mark>client</mark> pkt, 2 <mark>server</mark> pkts, 1 turn.
```

Deliverable 2. Investigate weevely (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

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



Deliverable 4. Tech Journal

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