3/18/2022

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.`

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

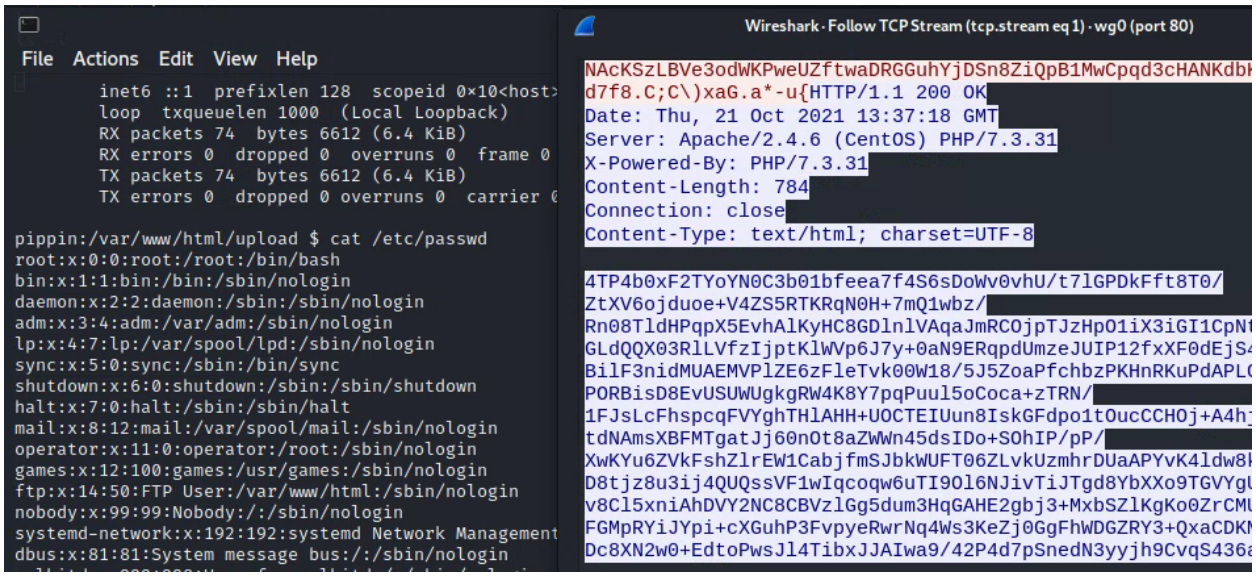
```
[+] weevely 4.0.1

[+] Target:     10.0.5.25
[+] Session:    /home/champuser/.weevely/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.

weevely> 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 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.