Detecting Web Shells

A web shell is a malicious program uploaded to a target web server, enabling adversaries to execute commands remotely.

- Run commands remotely through the web interface

Under the hood.

1) checks if the cmd parameter is present in the URL
?cmd=whoami

2) stores the user supplied command in the variable $cmd

3) Execute the command
4) Displays the output
5) HTML for the user interface
6) Command to execute
7) Output

Detection

- Remote log name field is typically represented by a hyphen (-)

- Repeated GET requests in quick succession means attacker is probing for a valid place to upload a shell

GET → Used for recon or interacting with a web shell
POST → Upload with a web shell
PUT → Upload a web shell
Delete → Cleanup
OPTIONS → Reconaissance HEAD → Detect files

Combining web access and error logs with auditd, a suspicious POST request in web logs can be linked to an audit event that includes a creat or execve syscall, showing a script wrote a file or ran commands.

An attacker's web shell must be stored somewhere

Common web server directories:

Apache : /var/www/html/
Nginx : /usr/share/nginx/html/