Elek Thomas-Toth

Part 1: Webshell

a. By going to the url below. Adding the ?command=[command] takes in input to the php webshell

http://danger.jeffondich.com/uploadedimages/thomastothe-php.php?command=whoami

b. The <pre> tags format the response to the request so you don't just get a big block of text when doing something like "ls"

Part 2: Looking around

a. /var/www/

b. We can get all of the users by running the command getent passwd

   i. root:x:0:0:root:/root:/bin/bash
   ii. daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
   iii. bin:x:2:2:bin:/bin:/usr/sbin/nologin
   iv. sys:x:3:3:sys:/dev:/usr/sbin/nologin
   v. sync:x:4:65534:sync:/bin:/bin/sync
   vi. games:x:5:60:games:/usr/games:/usr/sbin/nologin
   vii. man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
   viii. lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
   ix. mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
   x. news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
   xi. uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
   xii. proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
   xiii. www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
   xiv. backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
   xv. list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
   xvi. irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
   xvii. gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
   xviii. nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
   xix. systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
   xx. systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
   xxi. messagebus:x:102:105::/nonexistent:/usr/sbin/nologin
   xxii. systemd-timesync:x:103:106:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
   xxiii. syslog:x:104:111::/home/syslog:/usr/sbin/nologin
   xxiv. _apt:x:105:65534::/nonexistent:/usr/sbin/nologin

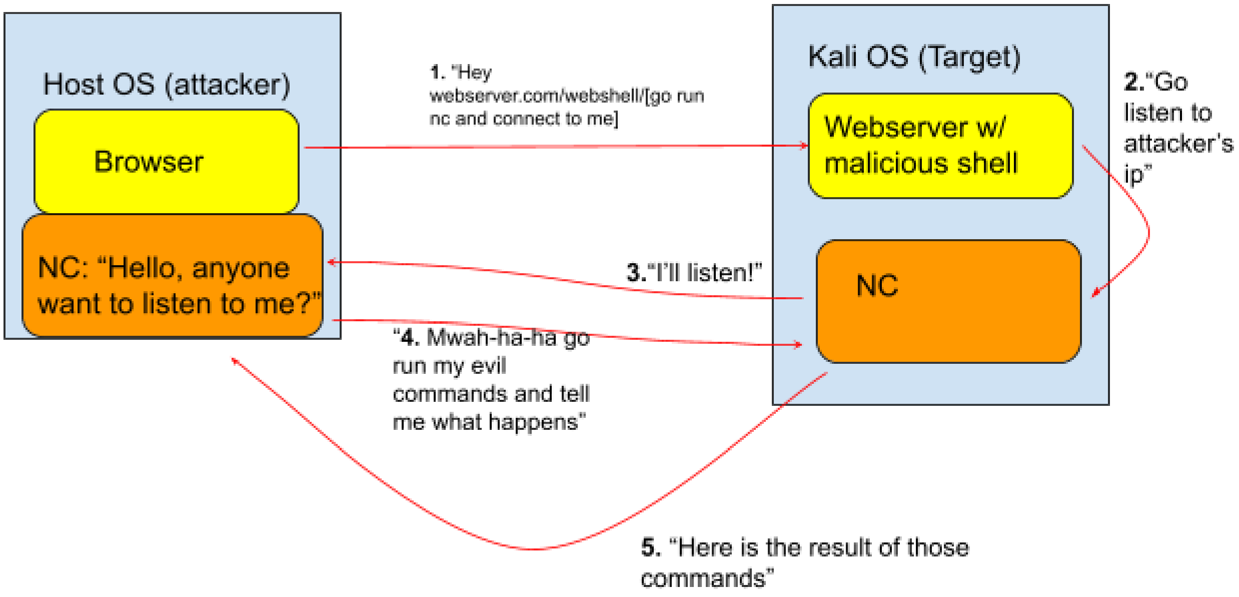
    xxv. tss:x:106:112:TPM software stack,,,:/var/lib/tpm:/bin/false
    xxvi. uuidd:x:107:113::/run/uuidd:/usr/sbin/nologin
    xxvii. tcpdump:x:108:114::/nonexistent:/usr/sbin/nologin
    xxviii. usbmux:x:109:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
    xxix. sshd:x:110:65534::/run/sshd:/usr/sbin/nologin
    xxx. pollinate:x:111:1::/var/cache/pollinate:/bin/false
    xxxi. landscape:x:112:116::/var/lib/landscape:/usr/sbin/nologin
    xxxii. fwupd-refresh:x:113:117:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nologin
    xxxiii. jeff:x:1000:1000:Jeff Ondich,,,:/home/jeff:/bin/bash
    xxxiv. postgres:x:114:119:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
    xxxv. bullwinkle:x:1001:1001:Bullwinkle J. Moose,,,:/home/bullwinkle:/bin/bash

c. /etc/passwd/ contains the same info as above. I think that I do technically have access but I was running into the issue of the server resetting when I tried to access it normally.
d. I don't have access but the internet says the /etc/shadow stores the hashed passwords for the linux account and other relevant password information. Only the root user can access these.
e. There are two secret files in at /danger.jeffondich.com/secrets and /danger.jeffondich.com/youwontfindthiswithgobuster/kindasecret which contain ascii animals.

Part 4: Reverse Shell

a. The Ip address of the kali machine is 192.168.219.128 which I got from running ifconfig
b. I got the ip address for the host machine by running ifconfig on WSL. Running a ipconfig on the windows terminal also provided more ip addresses but none of those worked so I went with the one from ifconfig.
c. N/A
d. N/A
e. I can run ipconfig to confirm that the ip address of the machine I am connected to is the correct instance of kali. I can also run 'cat /etc/os-release' to get the operating system information and confirm that everything matches.
f. The % codes are how the url accepts characters like spaces and dashes which would otherwise have a special meaning.
g.

Once the webshell is installed on the server, the attacker can run a command sent through a url request (1). In this case, the command causes the target to run nc, listening on the same port that the attacker is running nc on. Then the attacker can execute commands through nc and have a shell on the target computer.



Host OS (attacker)
Browser
NC: “Hello, anyone want to listen to me?”
1. "Hey webserver.com/webshell/[go run nc and connect to me]
Kali OS (Target)
Webserver w/ malicious shell
2.“Go listen to attacker's ip”
3.“I'll listen!”
NC
“4. Mwah-ha-ha go run my evil commands and tell me what happens”
5. “Here is the result of those commands”