CIS 375

Lab 7

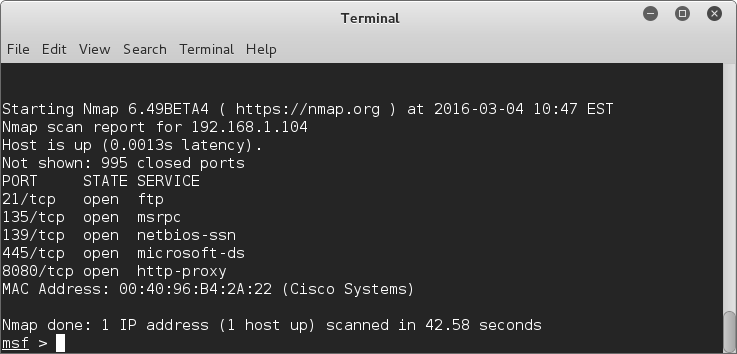
3 March 2016

Rodney Fulk

Jason Carr

1. **Information Gathering using the Attach Machine (Kali Linux)**

**Q-1: Submit a screenshot for the nmap output.**

****

**Q-2: What does the -sV option do? Are you able to determine the FTP service fingerprint?**

-sV enables version detection of the port services.

-sV did not but “banner grabbing” did

**Q-3: What is the FTP service fingerprint?**

BigFoolCat FTP Server 1.0

**2. Service Exploitation**

**Q-4: Are you able to find any Exploit?**

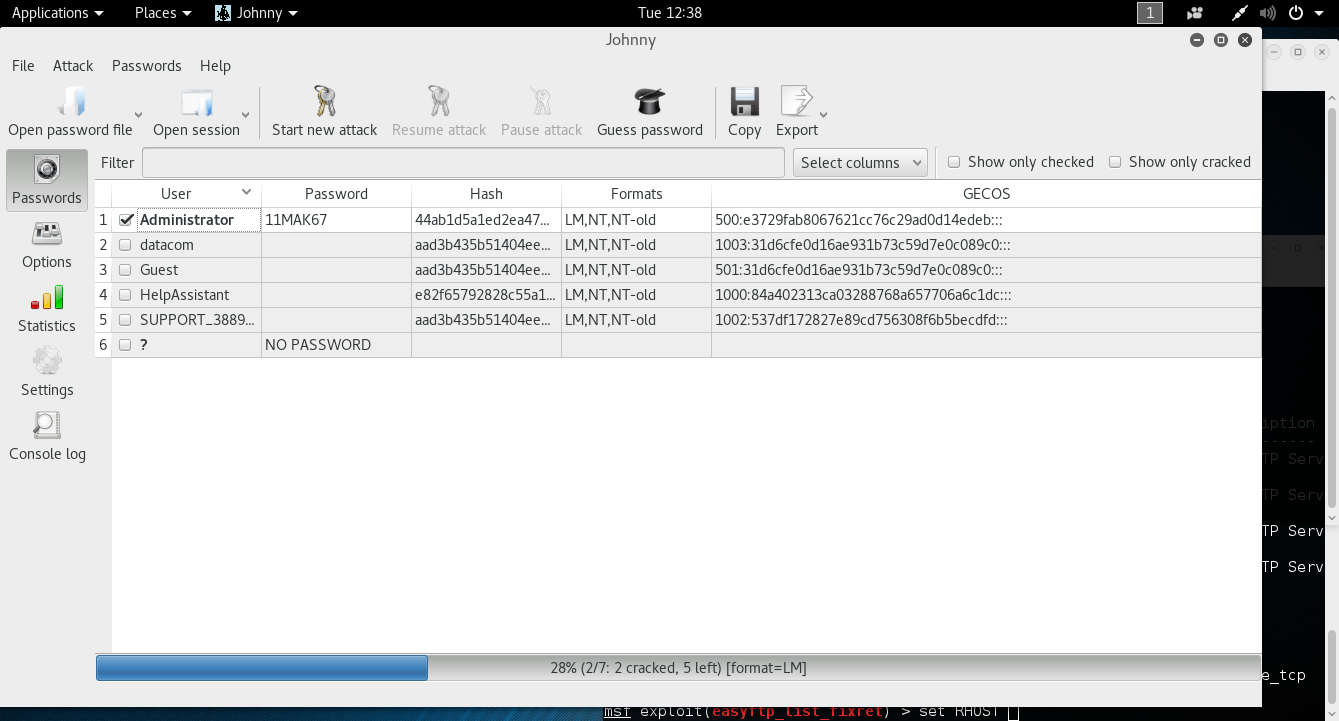
Had to google search what the server name actually was then we were able to find 4 exploits.

**Q-5: Which exploit was successful in attacking the target machine? Submit a screenshot for this meterpreter prompt that you get.**

easyftp\_list\_fixret

**Q-6: What is the administrator's’ password? Submit a screenshot for John-the-Ripper’s output.**

Actually used Jonny which is a Gui for John-the-Ripper



**Q-7: How to defend the victim machine against this attack?**

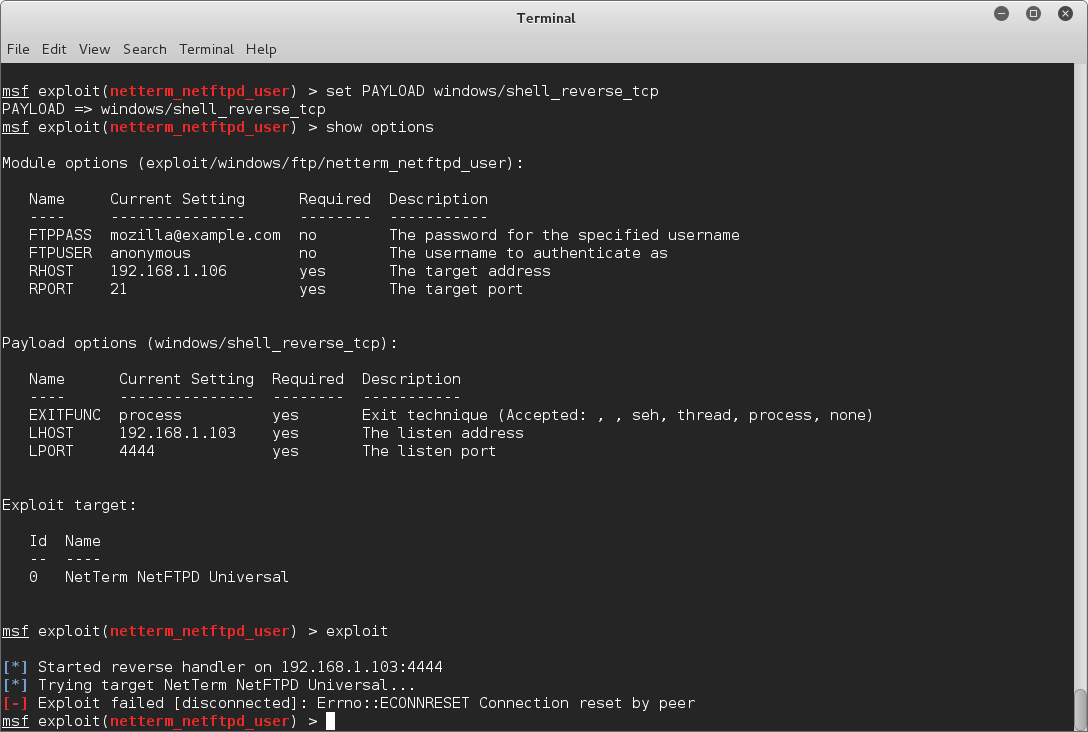
Make sure to update to the latest version of the program with no known vulnerabilities and try exploiting it again. If this does not work then you will need to use a different program.

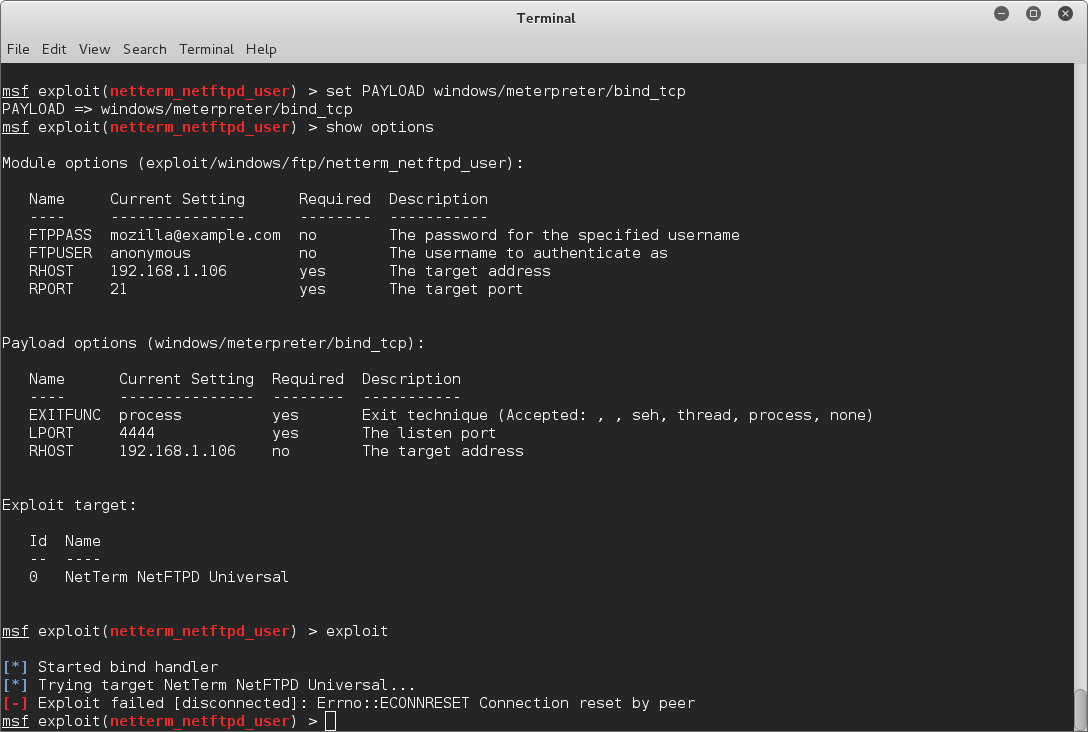
**Q-8: Are you able to get a meterpreter command prompt? If not, why? Submit a screenshot for the exploit(s) output that you tried on the victim**

**machine.**

We were not successful with getting a meterpreter prompt. The best we could do was get an anonymous connection one time, but was unable to replicate it. Also, we didn’t notice that this occurred until after looking at the ftp log.

According to several security sites, the only exploit that Quick N Easy 3.0 was vulnerable to were DoS attacks using a buffer overflow.

****

****

Administrator:500:44ab1d5a1ed2ea47aad3b435b51404ee:e3729fab8067621cc76c29ad0d14edeb:::

datacom:1003:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

HelpAssistant:1000:e82f65792828c55a129873d9eb714946:84a402313ca03288768a657706a6c1dc:::

SUPPORT\_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:537df172827e89cd756308f6b5becdfd:::