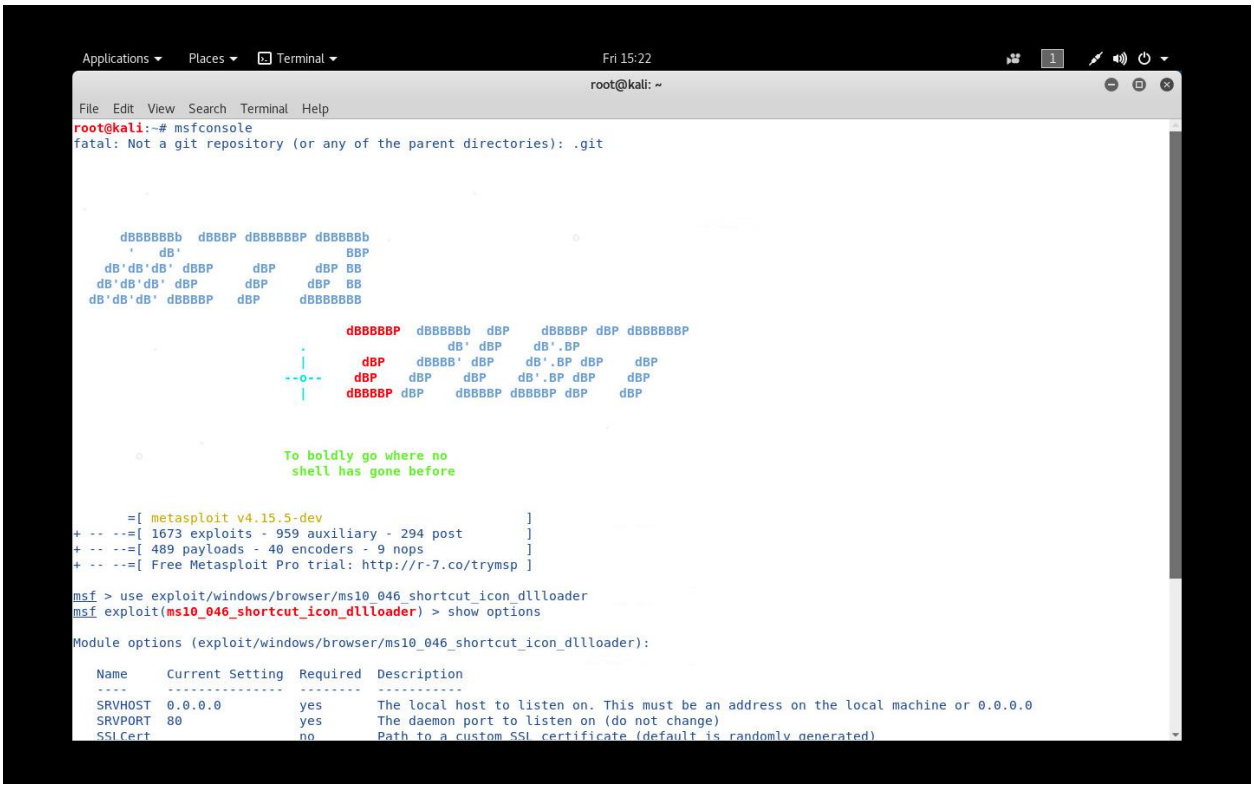
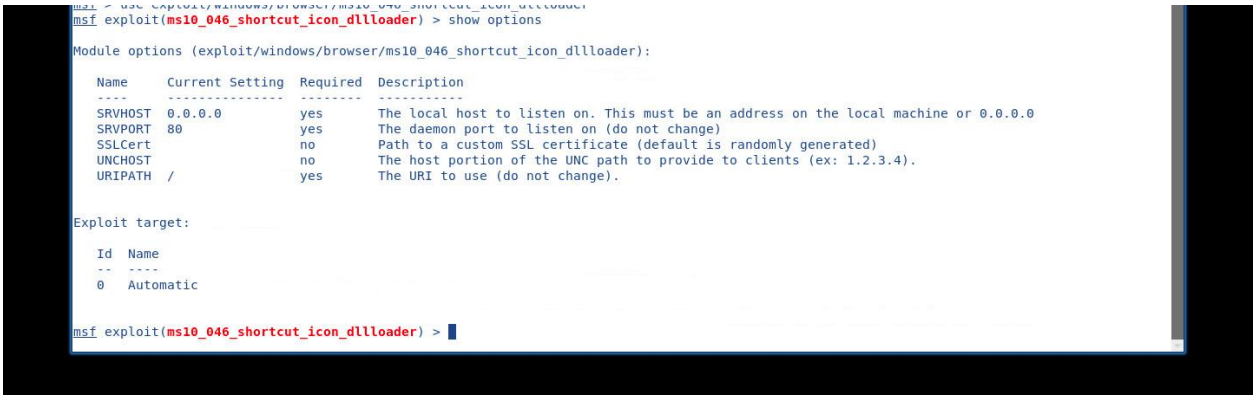
Lab 07 Report

Report by Joynal Abedin

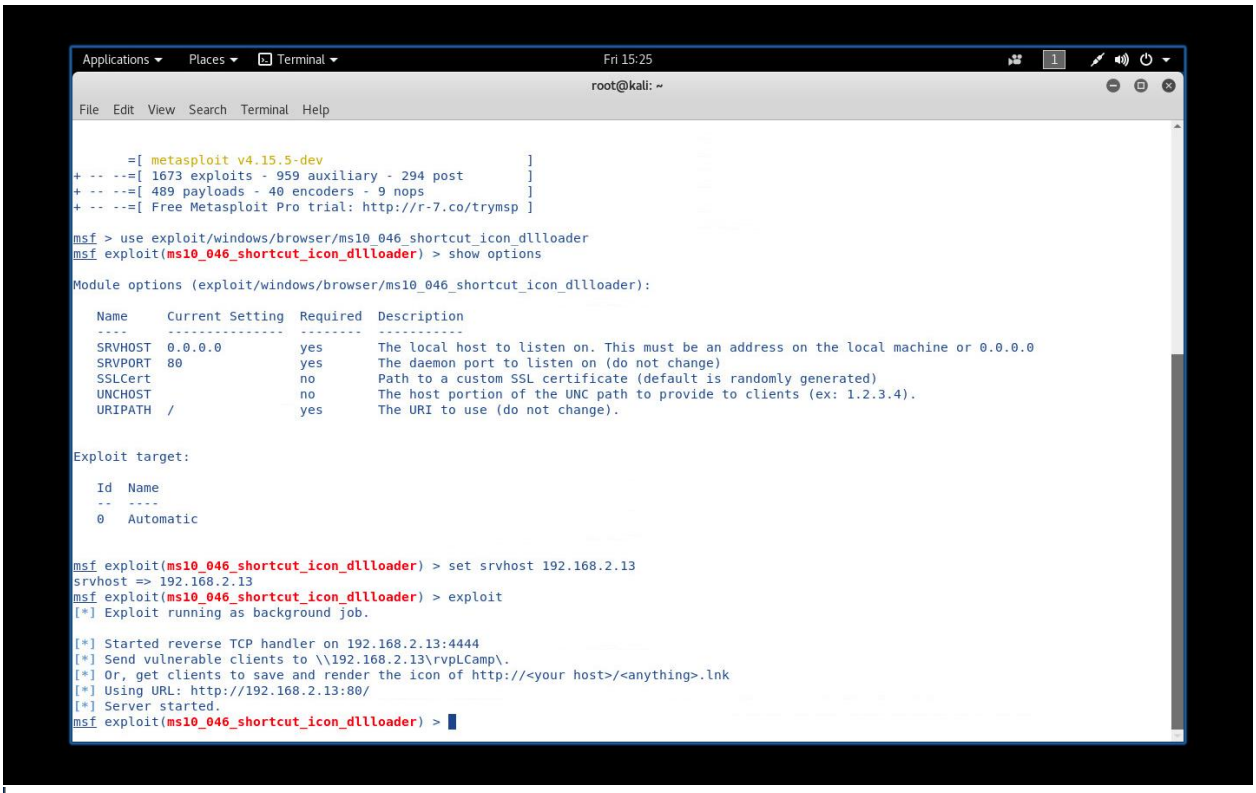
Documentation

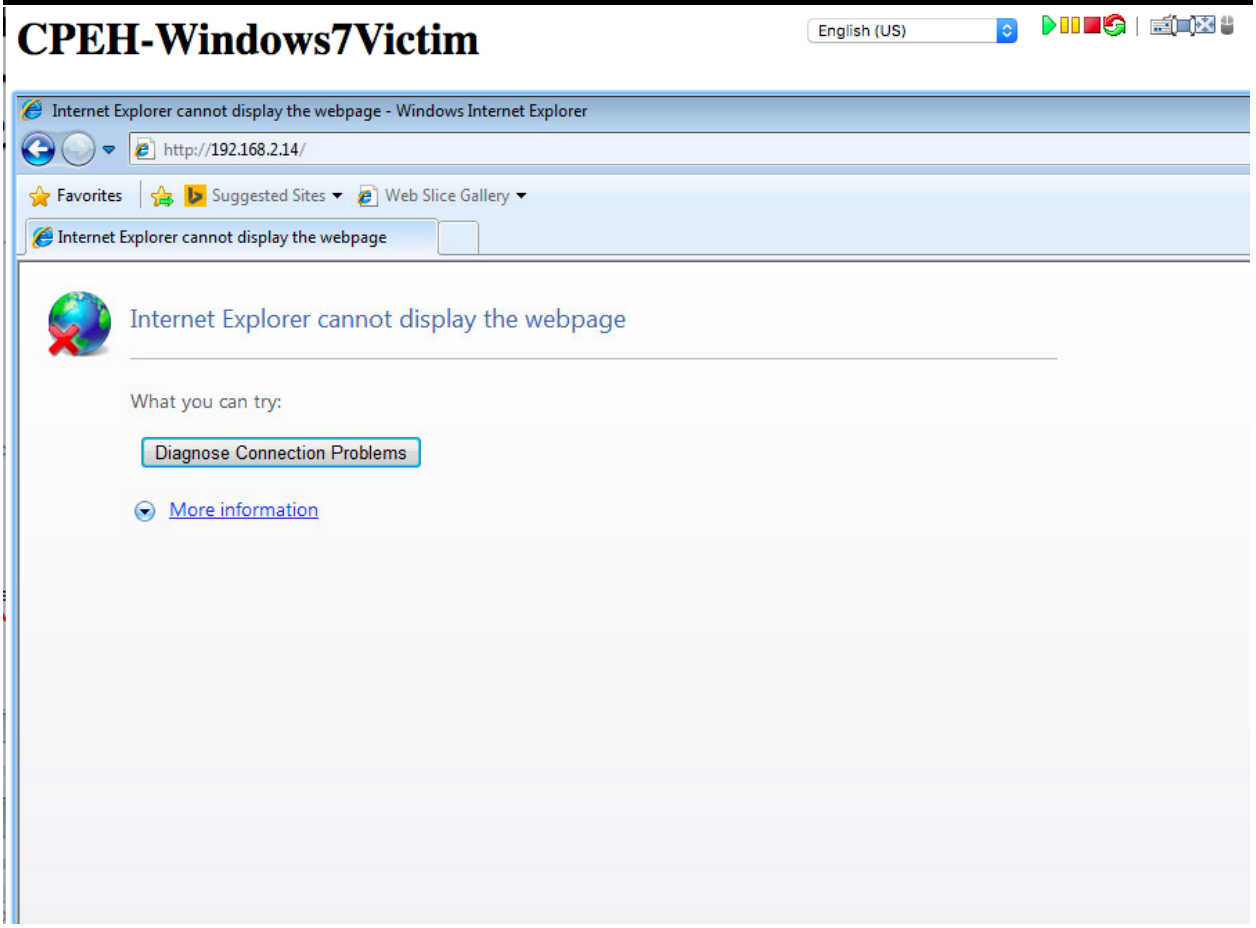
7.1 Using Metasploit





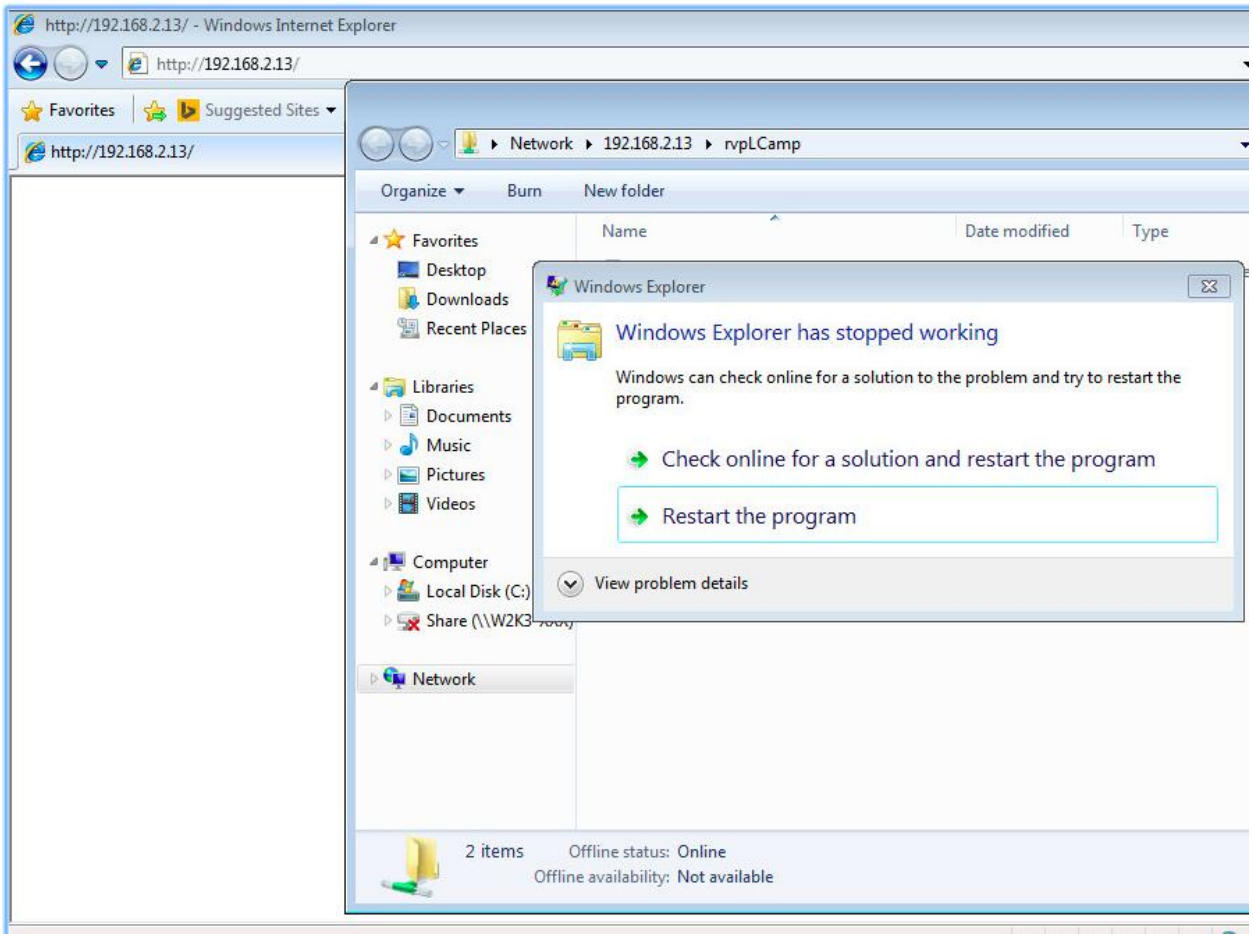
Lab 07 Report



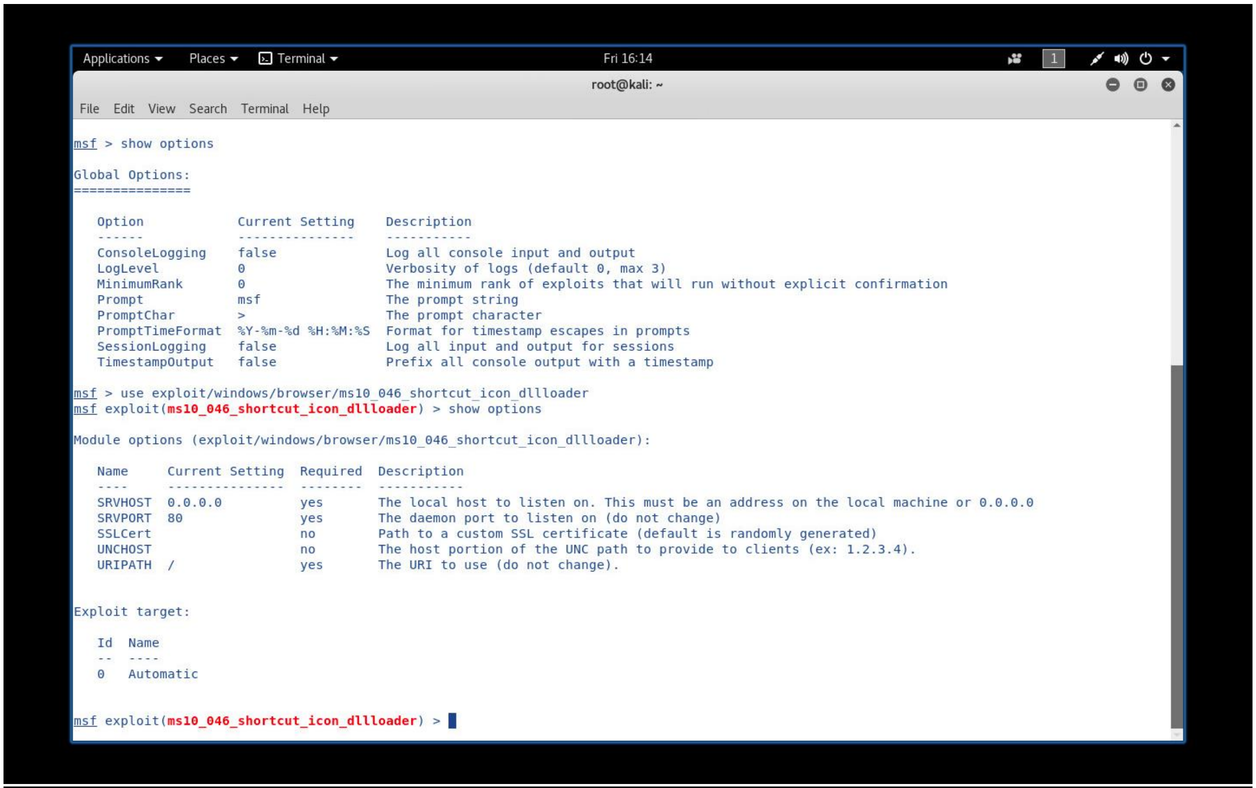


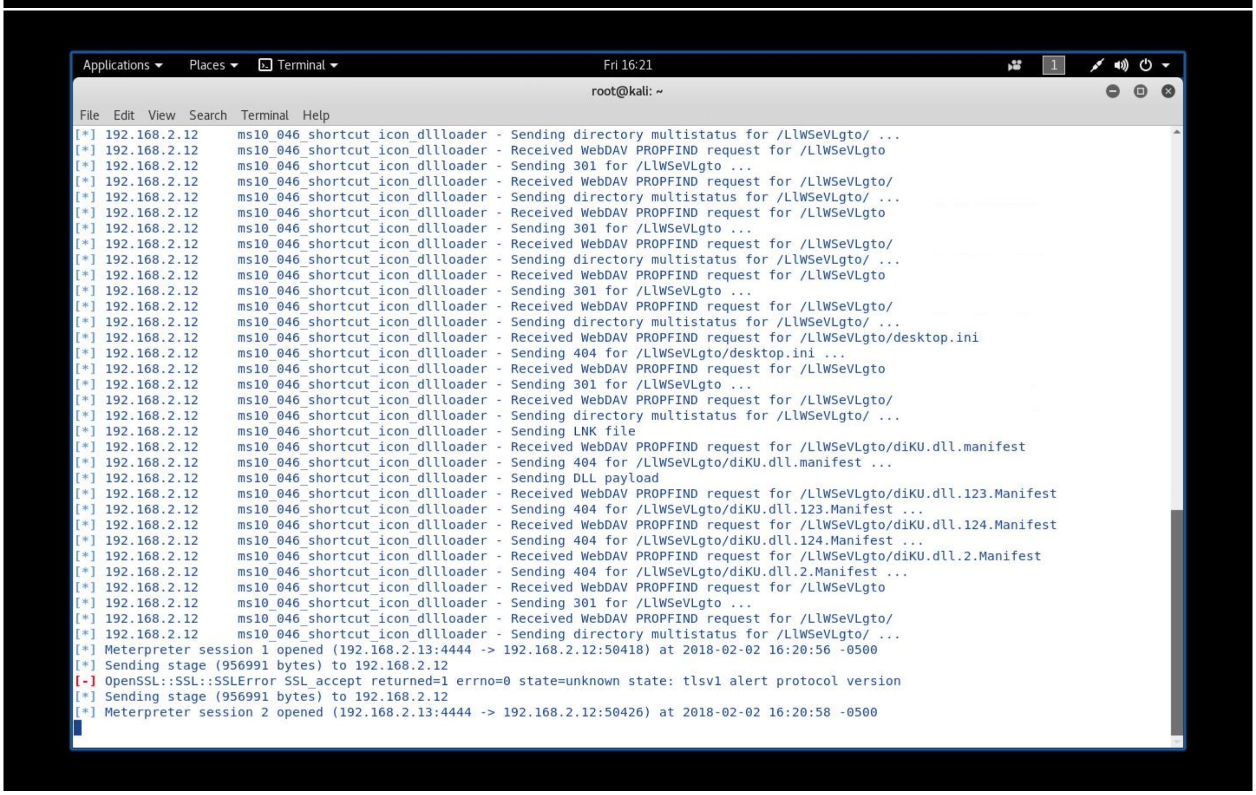
CPEH-Windows7Victim

English (US)

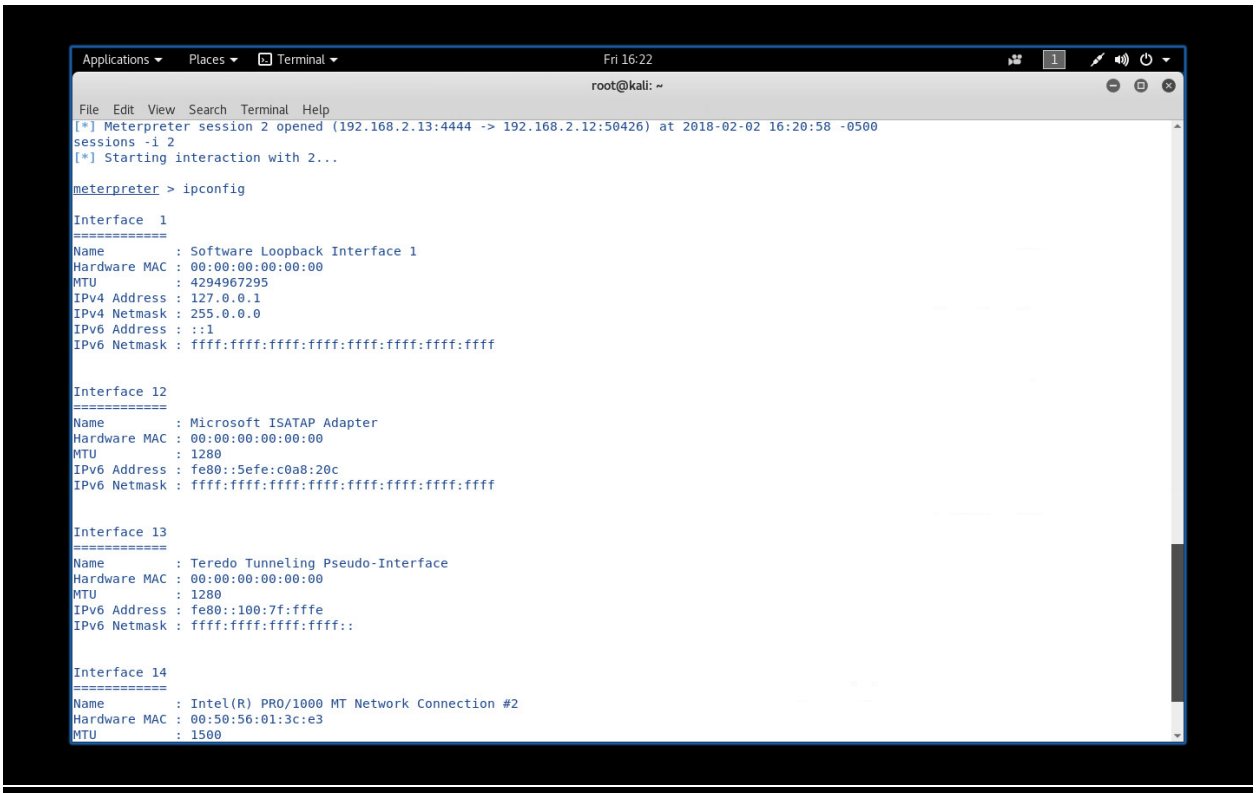


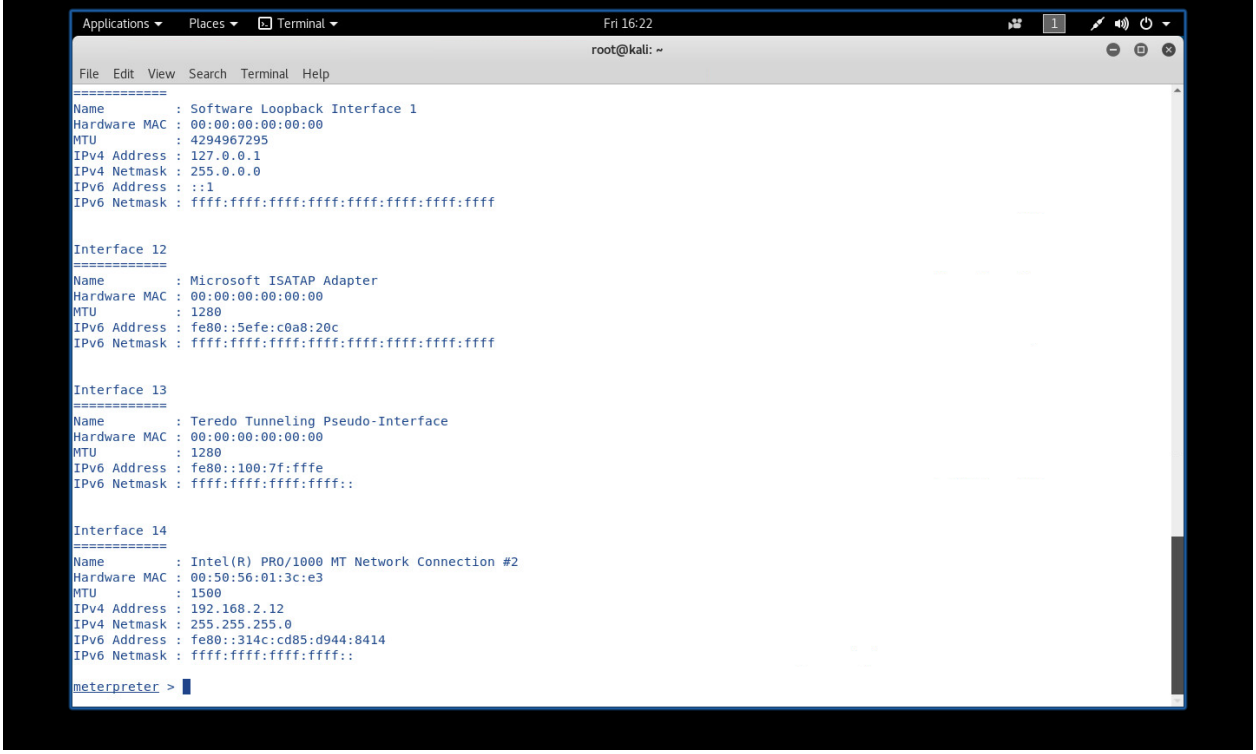
Lab 07 Report





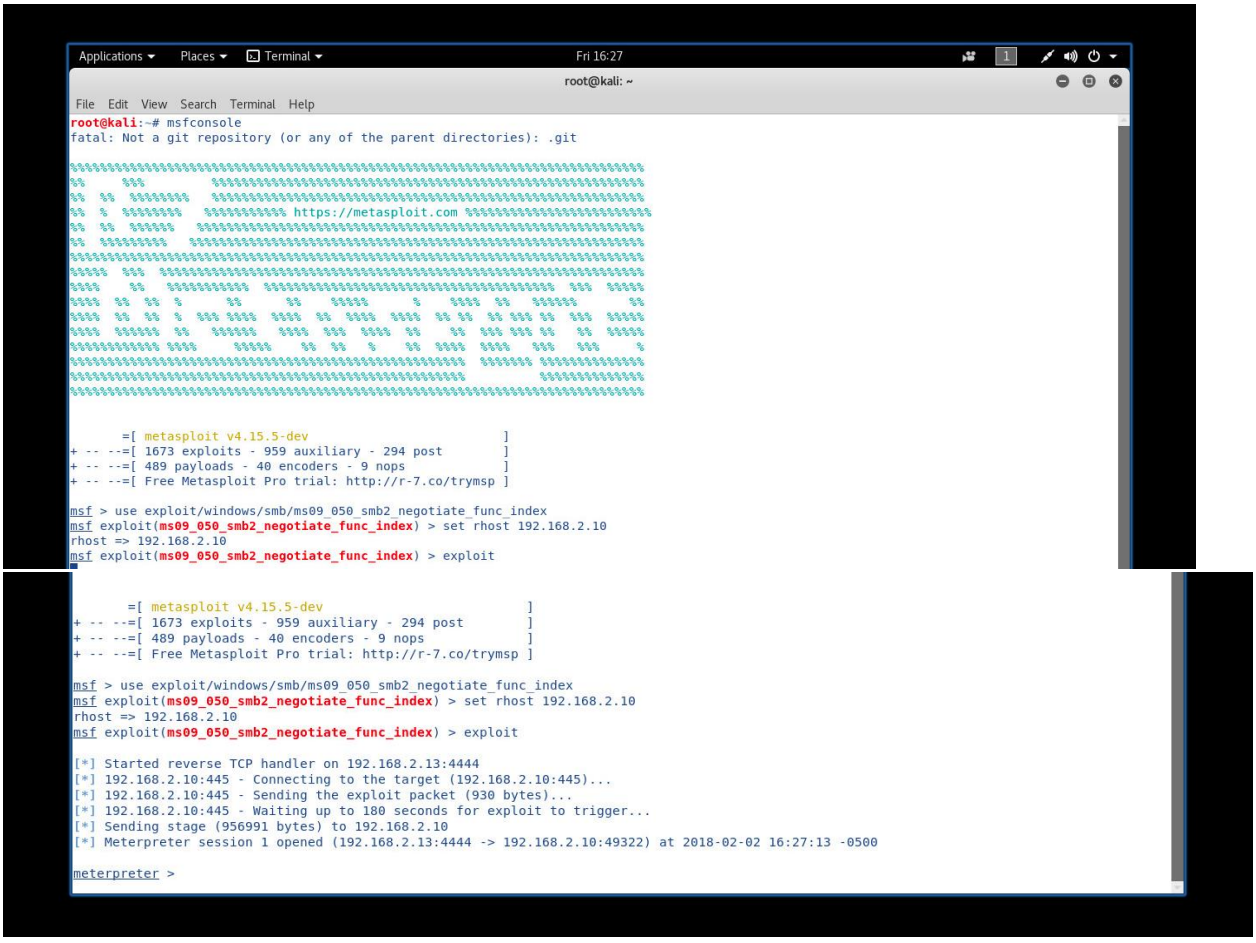
Lab 07 Report

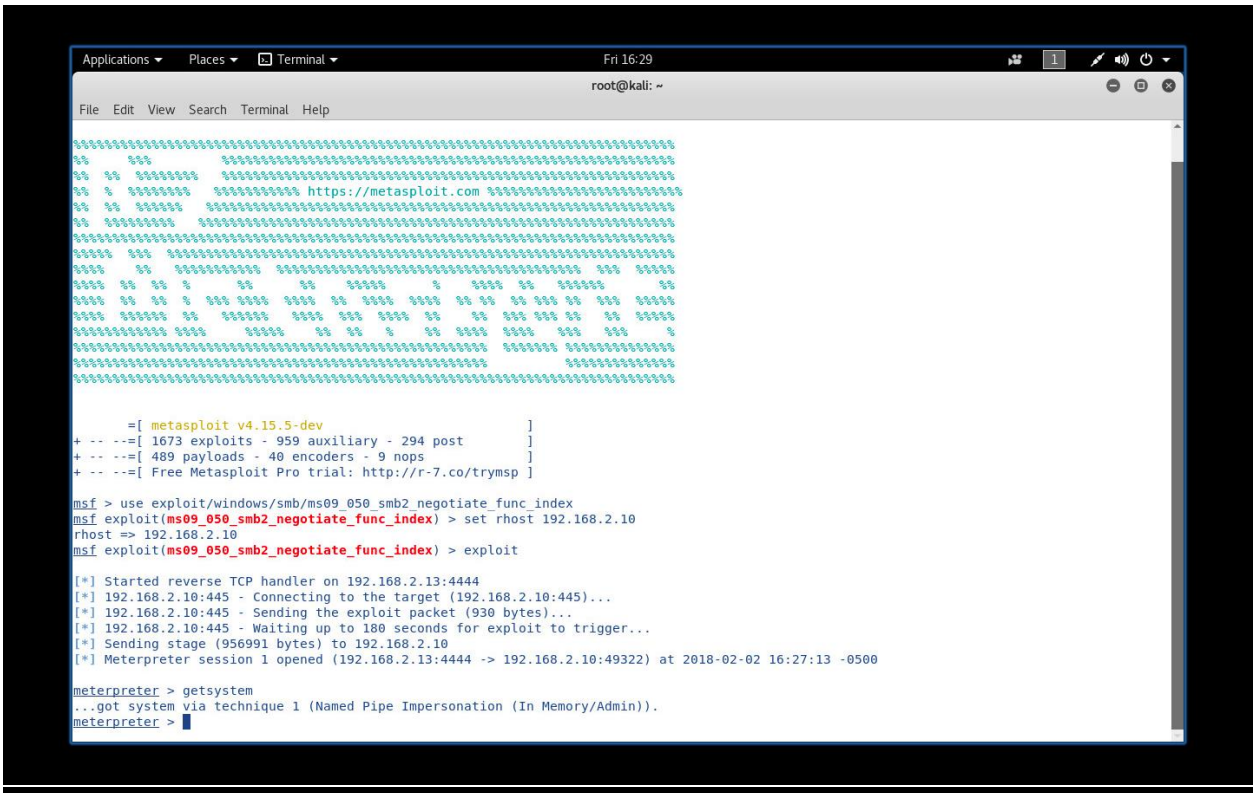


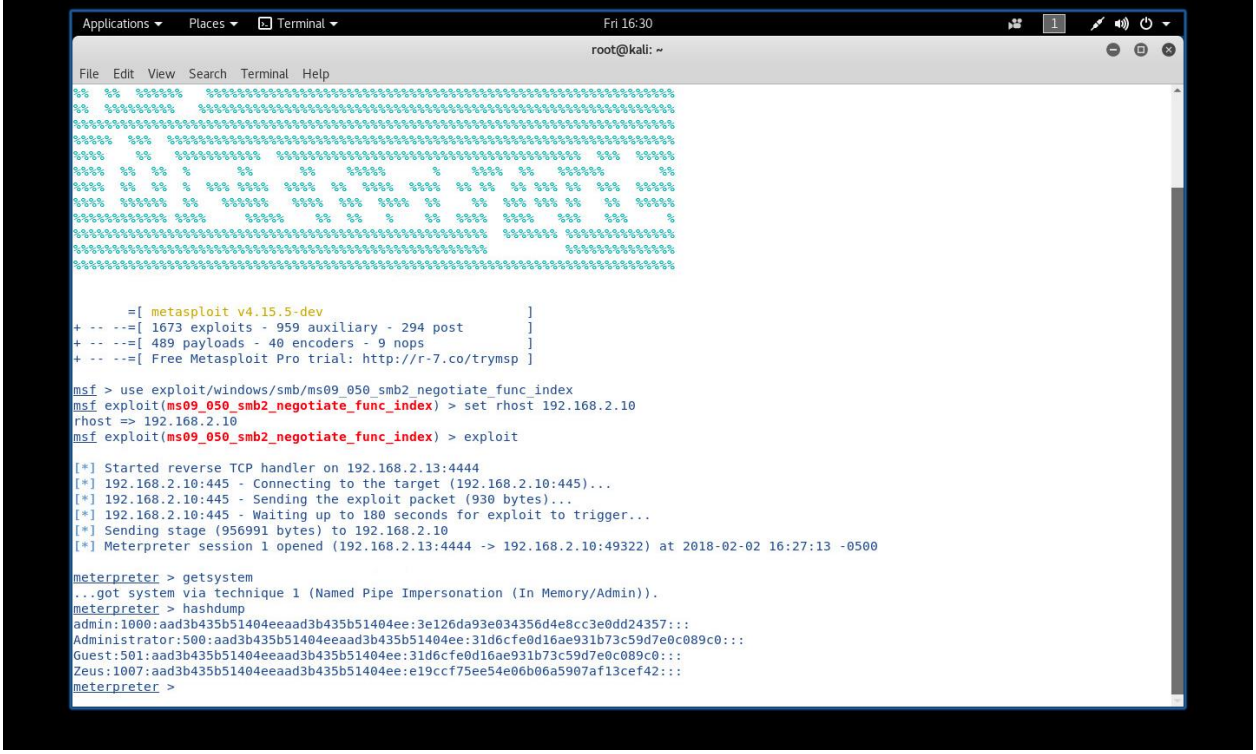


```
meterpreter > sysinfo
Computer        : WIN-CQR3UEPCPMH
OS              : Windows 7 (Build 7600).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 1
Meterpreter     : x86/windows
meterpreter >
```

7.2 Windows 2008 SMBv2 Exploit







7.3 Cracking with John the Ripper

```
root@kali:~# john --format=LM hashes.txt
Using default input encoding: UTF-8
Using default target encoding: CP850
Loaded 4 password hashes with no different salts (LM [DES 128/128 AVX-16])
Press 'q' or Ctrl-C to abort, almost any other key for status
                 (Zeus)
                 (Guest)
                 (Administrator)
                 (admin)
4g 0:00:00:00 DONE 2/3 (2018-02-02 16:52) 44.44g/s 15700p/s 15700c/s 62800C/s 123456..MARLEY
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@kali:~#
```

Vulnerabilities

Vulnerability 01

Description

Back in 2010, Microsoft openly admitted the vulnerability in Windows Shell that could allow remote code execution. It can allow remote execution when the user clicks on a file with the lnk extension. Basically, user that has account which is configured to have less user rights on its operating system could be less likely to be impacted than those who uses/operate on administrative user rights.

Overall, a bad person who successfully could exploit this vulnerability can gain the same user rights as the local user.

Relative Risk (High, Medium, Low)

- Medium
    - Approximately 10 times more expensive than a “low” risk
    - additional budget request may be required

Mitigation

Train employee or awareness training will help employee understand the vulnerability. Eventually, they’d be aware of those kinds of link and will not open them as it can cause harm.

Awareness training may cost a lot of money as they company may need to pay employees for their extra time on training sessions as well as training instructors.

Vulnerability 02

Description

System admins using weak password could make an attacker's job easier. It is always recommended to use password that meets complexity requirements.

Relative Risk

- Low
  - can be accomplished within the existing IT budget
  - no additional budget request required

Mitigation

Advise System Admins to user stronger password.