VIT®
Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

School of Information Technology & Engineering

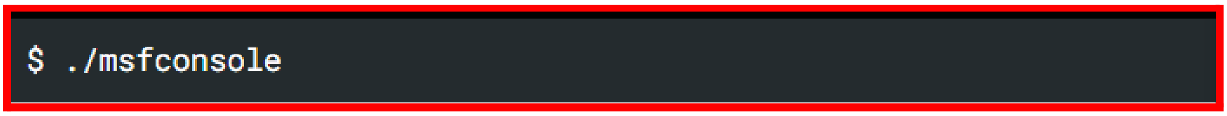
WINTER 2022 - 23

Programme : B.Tech **Due Date : 22-04-2022**
Course Title : Information Security Management **Course Code : CSE3502**

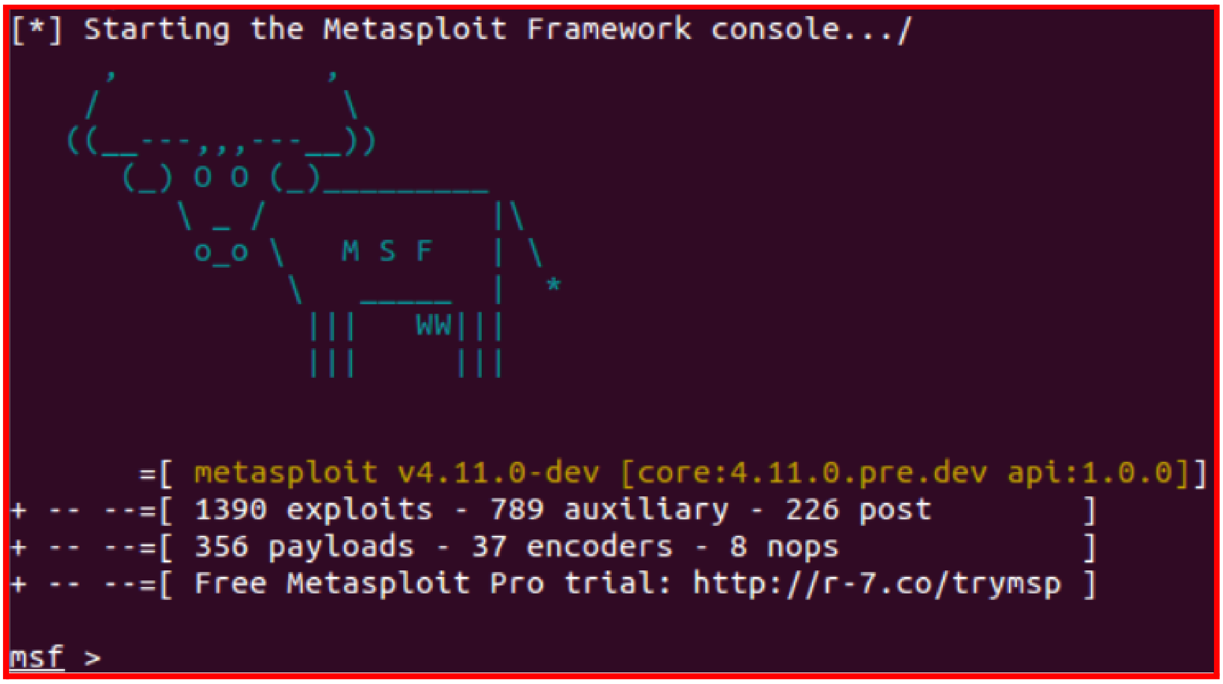
Name: SHUBHAM AGARWAL
RegNo: 19BIT0010

1. Exploring the Metasploit Framework

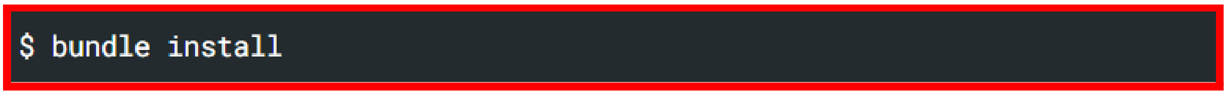
Ans:
Metasploit is a collection of tools, not just one. It's a full-fledged framework. It's a Ruby-based, modular penetration testing platform that lets you design, test, and executes exploit code. It's flexible and incredibly resilient, with a plethora of tools for performing both simple and sophisticated tasks.
Exploring:



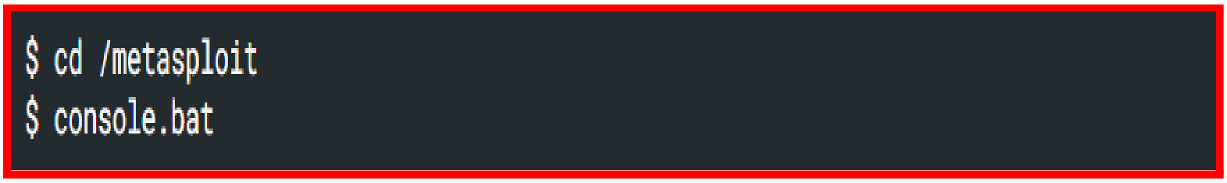
```
$ ./msfconsole
```



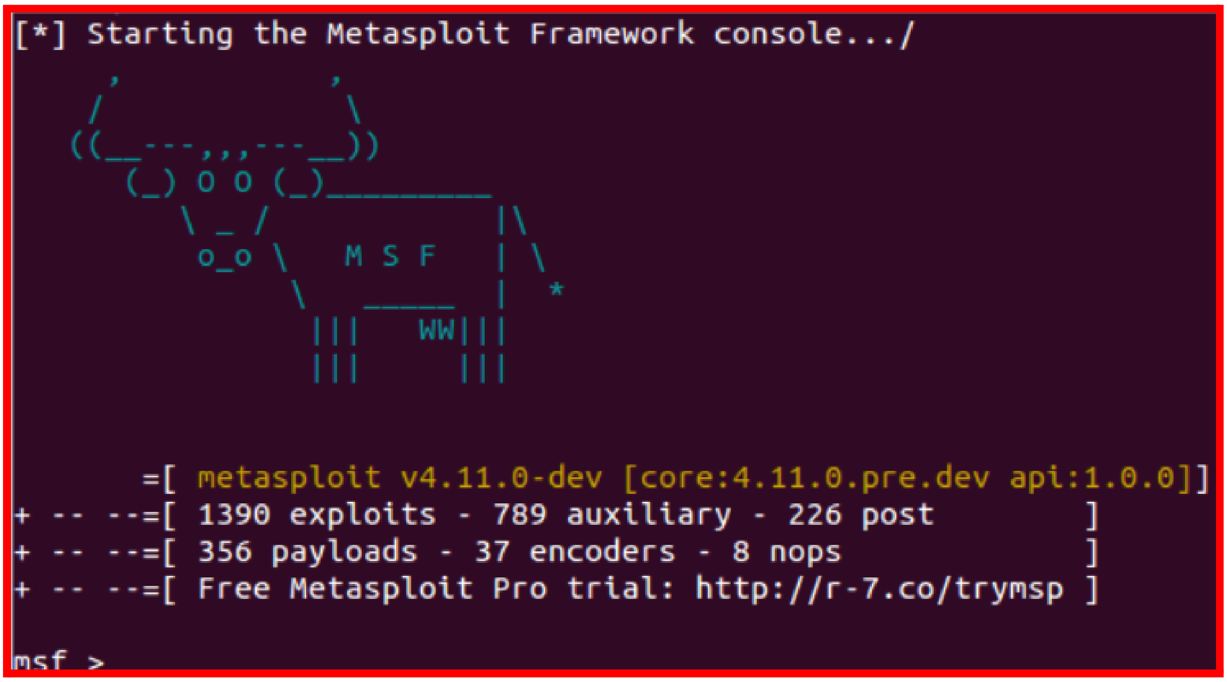
```
[*] Starting the Metasploit Framework console.../

      ,           ,
     /             \
    ((__---,,,---__))
       (_) O O (_)_________
          \ _ /            |\
           o_o \   M S F   | \
                \   _____  |  *
                 |||   WW|||
                 |||     |||


       =[ metasploit v4.11.0-dev [core:4.11.0.pre.dev api:1.0.0]]
+ -- --=[ 1390 exploits - 789 auxiliary - 226 post        ]
+ -- --=[ 356 payloads - 37 encoders - 8 nops             ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf >
```



```
$ bundle install
```



```
$ cd /metasploit
$ console.bat
```



```
[*] Starting the Metasploit Framework console.../
     ,           ,
    /             \
   ((__---,,,---__))
      (_) O O (_)__________
         \ _ /            |\
          o_o \   M S F   | \
               \   ______ |  *
                |||   WW|||
                |||     |||


       =[ metasploit v4.11.0-dev [core:4.11.0.pre.dev api:1.0.0]]
+ -- --=[ 1390 exploits - 789 auxiliary - 226 post        ]
+ -- --=[ 356 payloads - 37 encoders - 8 nops             ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf >
```

Component of MetasPloit:

Exploit - An exploit module is a programme that runs a series of commands in order to exploit a vulnerability in a system or application. An exploit module takes advantage of a flaw in the target system to gain access to it. Buffer overflow, code injection, and web application exploits are examples of exploit modules.

Auxiliary - A payload is not executed by an auxiliary module. It can be used for a variety of purposes that aren't necessarily related to exploitation. Scanners, fuzzers, and denial-of-service assaults are examples of auxiliary modules.

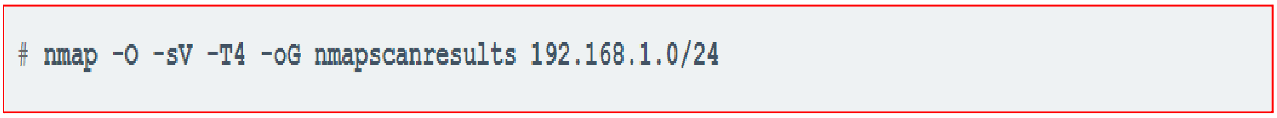
Post-Exploitation - A post-exploitation module allows you to obtain more information or gain access to a target system that has been compromised. Hash dumps and application and service enumerators are examples of post-exploitation modules.The shell code that executes after the payload is referred to as a payload.

Payload - The shell code that runs after an attack successfully compromises a system is referred to as a payload. You can use the payload to specify how you want to connect to the shell and what you want to do with the target system once you've gained control. A payload can be used to launch a Meterpreter or a command shell. Meterpreter is a sophisticated payload that allows you to dynamically generate new features by writing DLL files.

NOP generator - A NOP generator generates a series of random bytes that can be used to get around normal NOP sled signatures in IDS and IPS. Pad buffers with NOP generators.

2. Demonstrate website vulnerability analysis using Nessus and Nmap

Ans:
Step 1 - Run Nmap and output “grepable” results:
Code:

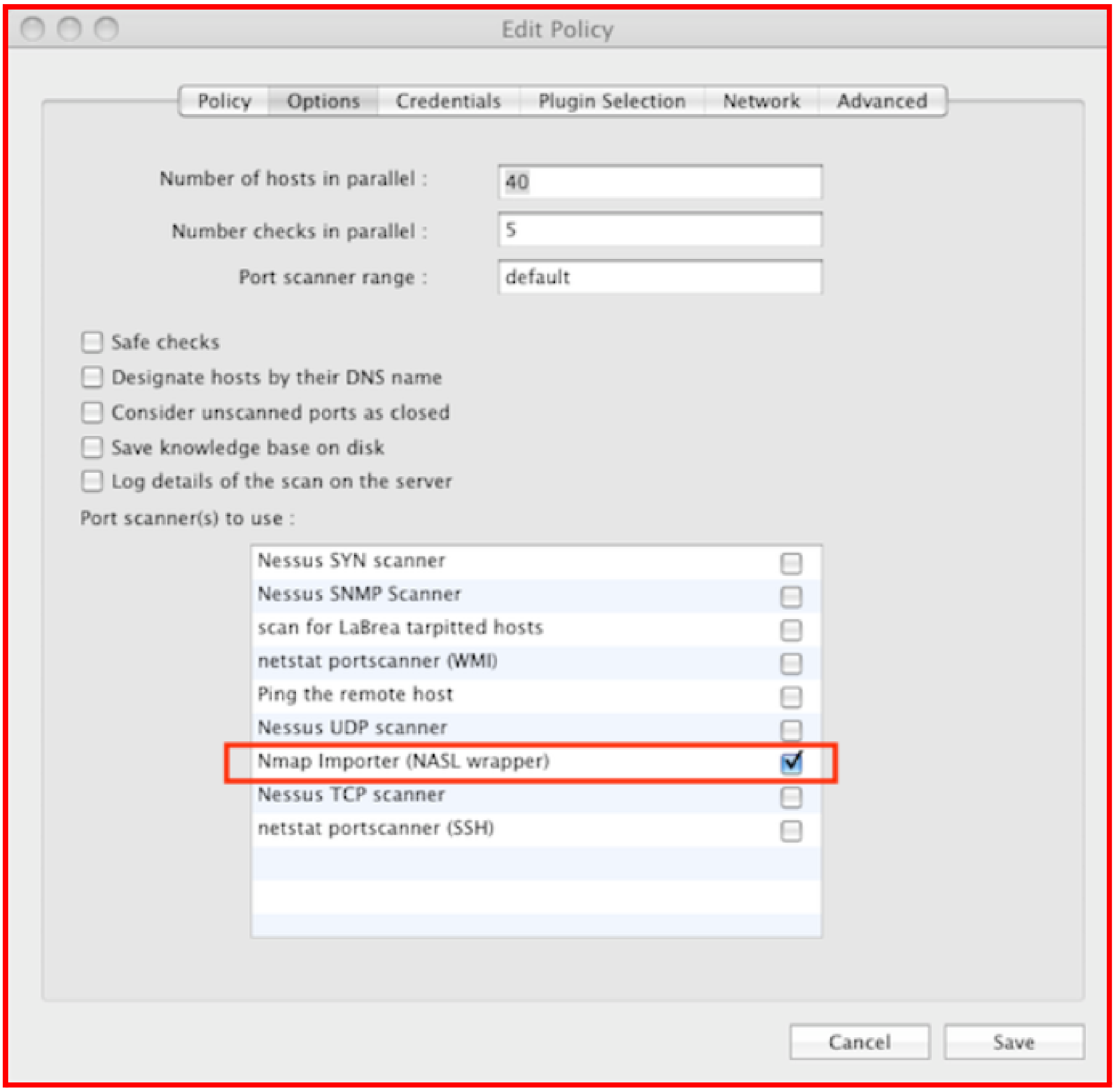


```
# nmap -O -sV -T4 -oG nmapscanresults 192.168.1.0/24
```

Explanation:
The Nmap command above will scan the target network (192.168.1.0/24), identify the remote operating system (-O), detect the services running on the ports discovered (-sV), and output Nmap grepable results (-oG) into the file called "nmapscanresults" using aggressive scan speeds (-T4).

Step 2 - We can now use NessusClient to set up a Nessus scan that uses the Nmap results. By establishing a /.nessusrc file with the scan policy information, you can create the Nessus configuration without utilising the NessusClient. It's easier to use the NessusClient for the initial configuration and vulnerability scan, then make changes to the /.nessusrc file later. For instructions on how to setup and configure nmap.nasl, see "When, how, and why (not) to utilise Nmap within Nessus," and make sure you're using the most recent version of nmap.nasl. Do not click the "share policy across several sessions" box when configuring the policy. The scan policy will not be incorporated in the.nessus file if you do so.

Step 3 -Only enable the Nmap Importer NASL wrapper in your scan policy configuration:



Number of hosts in parallel : 40

Number checks in parallel : 5

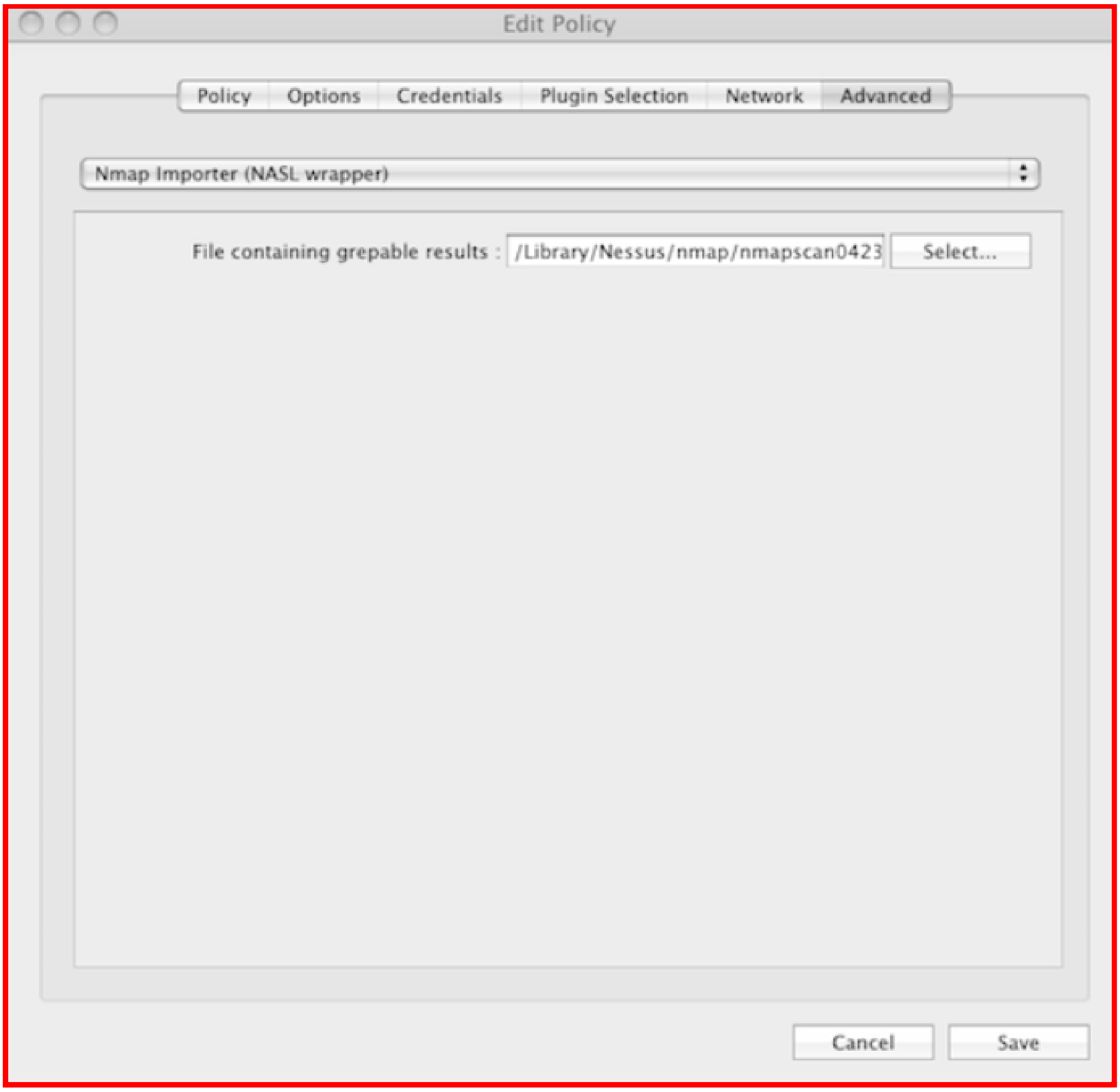
Port scanner range : default

□ Safe checks
□ Designate hosts by their DNS name
□ Consider unscanned ports as closed
□ Save knowledge base on disk
□ Log details of the scan on the server

Port scanner(s) to use :

Nessus SYN scanner	□
Nessus SNMP Scanner	□
scan for LaBrea tarpitted hosts	□
netstat portscanner (WMI)	□
Ping the remote host	□
Nessus UDP scanner	□
Nmap Importer (NASL wrapper)	☑
Nessus TCP scanner	□
netstat portscanner (SSH)	□

Step 4 - Select "Nmap Importer (Nasl wrapper)" from the pull-down option on the Advanced tab. You can use this option to select the Nmap grepable results file to utilise for the scan:

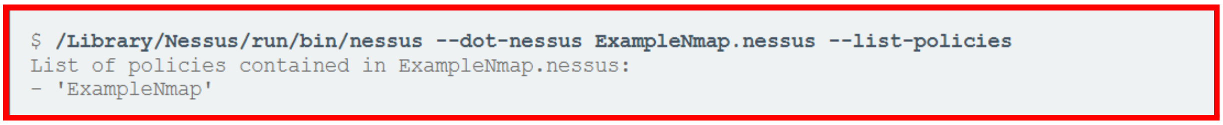


Nmap Importer (NASL wrapper)

File containing grepable results : /Library/Nessus/nmap/nmapscan0423

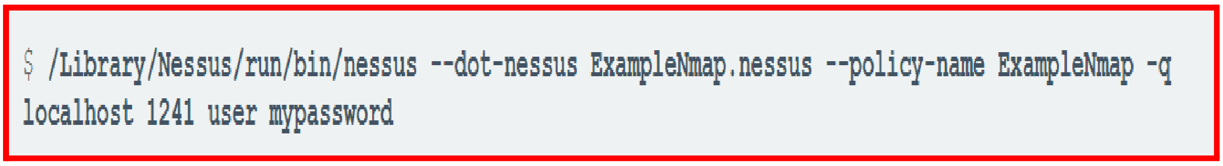
Step 5 - Execute your scan against the targets of your choice (which will also be saved in the.nessus file) and save the results by going to the menu and selecting "File-Save As...". The scan results and scan policies will be saved in the same.nessus file. We named the file "ExampleNmap.nessus" in this example and uploaded it to the Nessus service.

Step 6 - Use the Nessus client to read our scan policy and results. In this example, a Mac OS X machine was used. If you're using a Linux system, you'll need to change the path to /opt/nessus/bin/nessus:



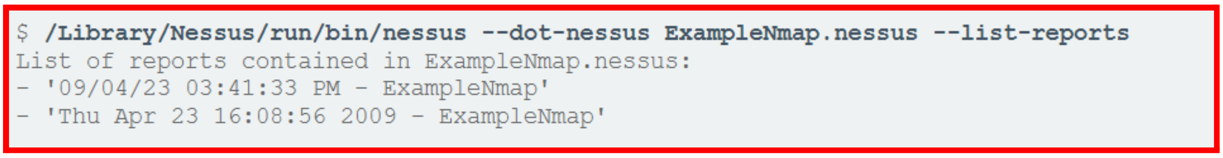
```
$ /Library/Nessus/run/bin/nessus --dot-nessus ExampleNmap.nessus --list-policies
List of policies contained in ExampleNmap.nessus:
- 'ExampleNmap'
```

Step 7 - Execute your scan in batch mode using the following command:

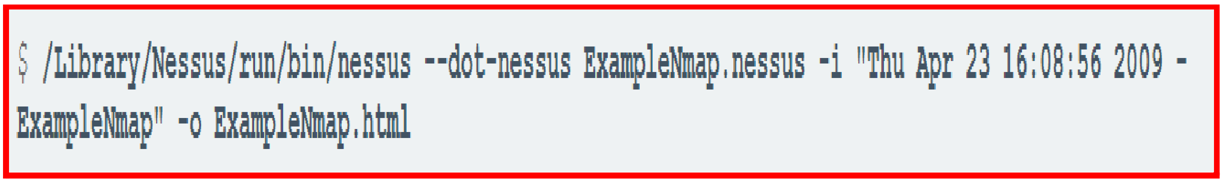


```
$ /Library/Nessus/run/bin/nessus --dot-nessus ExampleNmap.nessus --policy-name ExampleNmap -q
localhost 1241 user mypassword
```

Step 8 - When the scan has completed you can export and review the results using the following commands:



```
$ /Library/Nessus/run/bin/nessus --dot-nessus ExampleNmap.nessus --list-reports
List of reports contained in ExampleNmap.nessus:
- '09/04/23 03:41:33 PM - ExampleNmap'
- 'Thu Apr 23 16:08:56 2009 - ExampleNmap'
```



```
$ /Library/Nessus/run/bin/nessus --dot-nessus ExampleNmap.nessus -i "Thu Apr 23 16:08:56 2009 -
ExampleNmap" -o ExampleNmap.html
```