MetaSploit Pro Labs

Table of Contents

Credentials……3

LAB 1 – Quick Pentest ……4

LAB 2 – Discovering Targets…… 10

LAB 3 – Importing Scan Data…… 15

LAB 4 – Working with Credentials……23

LAB 5 – Web App Test……30

LAB 6 – Phishing Campaign……38

LAB 7 – Exploits and Payloads……46

LAB 8 –Reporting……53

Virtual Machine Credentials

Windows Server 2012 R2
username: Administrator
password: infosec458$%*

Windows 7 Client
no credentials are required to login
Metasploit Credentials:
username: student
password: infosec458$%*

Metasploit Pro Labs

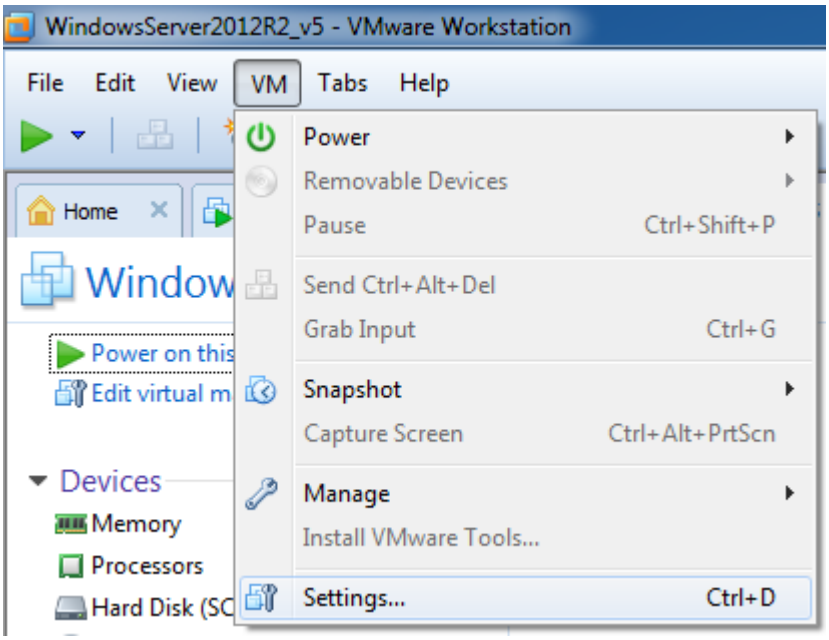
Lab 1 - Quick Pentest

Exercise 0 – Setting up Virtual Machines

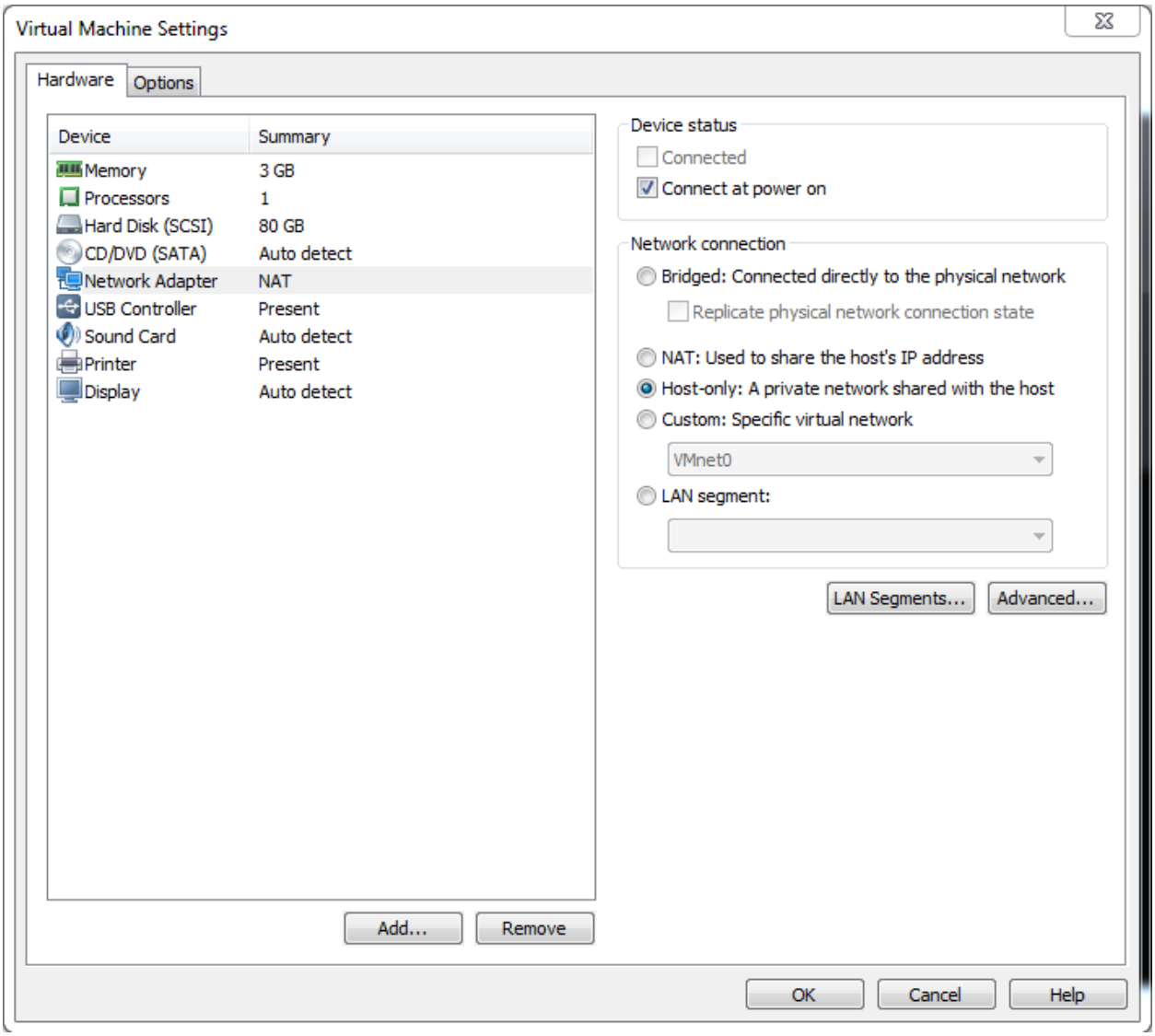
Before starting this lab, shut down all virtual machines that you have running at the moment.

We will be working with a trial version of Metasploit Pro for Windows, installed on the Metasploit Pro VM. Launch this VM from the shortcut on your Desktop.

As our target system, we will use the windows Server 2012 R2 VM. Before powering it on, change its Network Adapter setting to Host-only: in VMware Workstation, go to VM->Settings.



Then click Network Adapter in the Device list and select the “Host-only” radio button.



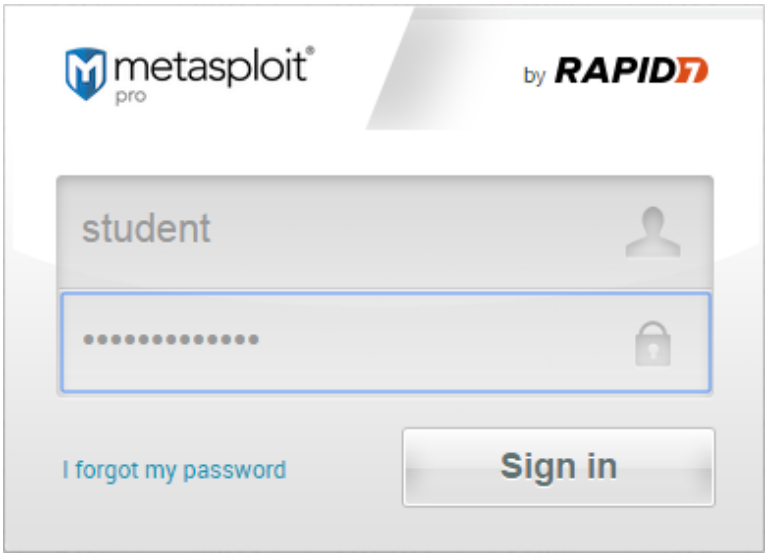
Click OK and power on the VM. Keep all other VMs powered off, otherwise you may experience significant performance issues. After logging on, run the **ipconfig** command in Command Prompt and record the new IP address for Windows Server 2012 R2 VM.

Exercise 1 – Getting started with Metasploit Pro

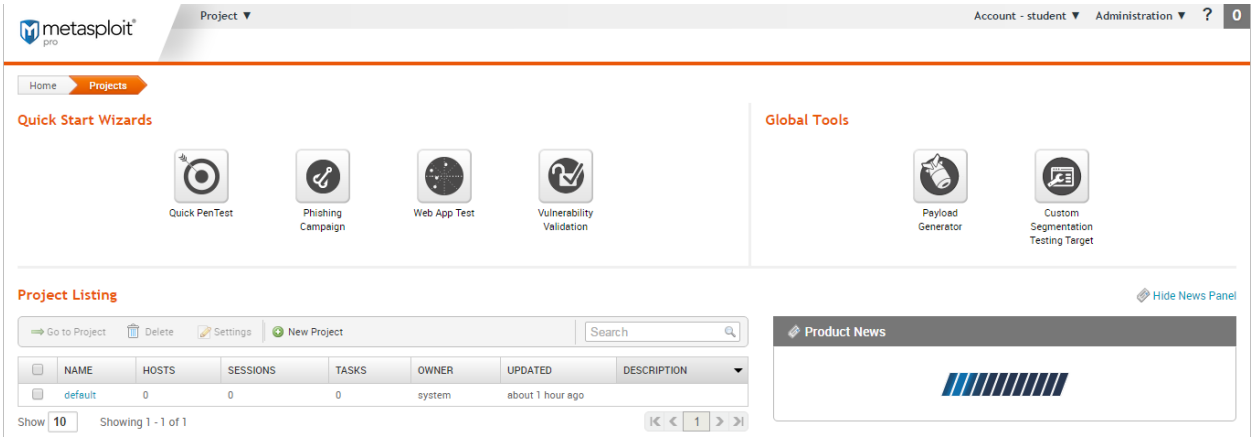
Metapsploit Pro includes a command line interafce (Metasploit Console), however, it is very similar to msfconsole, and does not support all Metasploit Pro features, which is why we will be working with the browser-based GUI. After your Metasploit Pro VM is started up, wait about 3-5 minutes, then double-click the “Access Metasploit Web UI” shortcut on the Metasploit Pro VM desktop to access the Web UI.

The Metasploit Pro login screen should open in a browser. Sign in with the following credentials:

username: **student**
password: **infosec458$%***



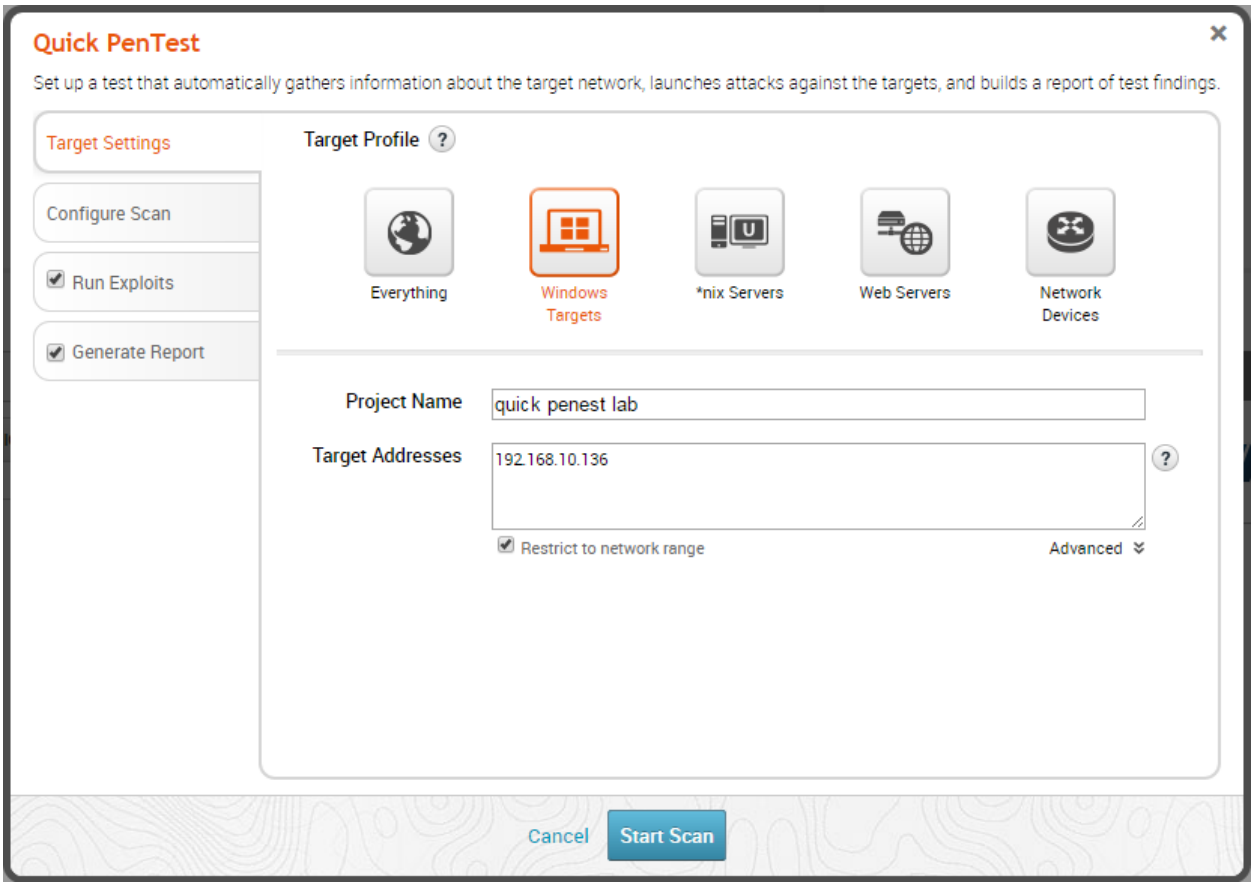
You will be taken to the Home->Projects page.



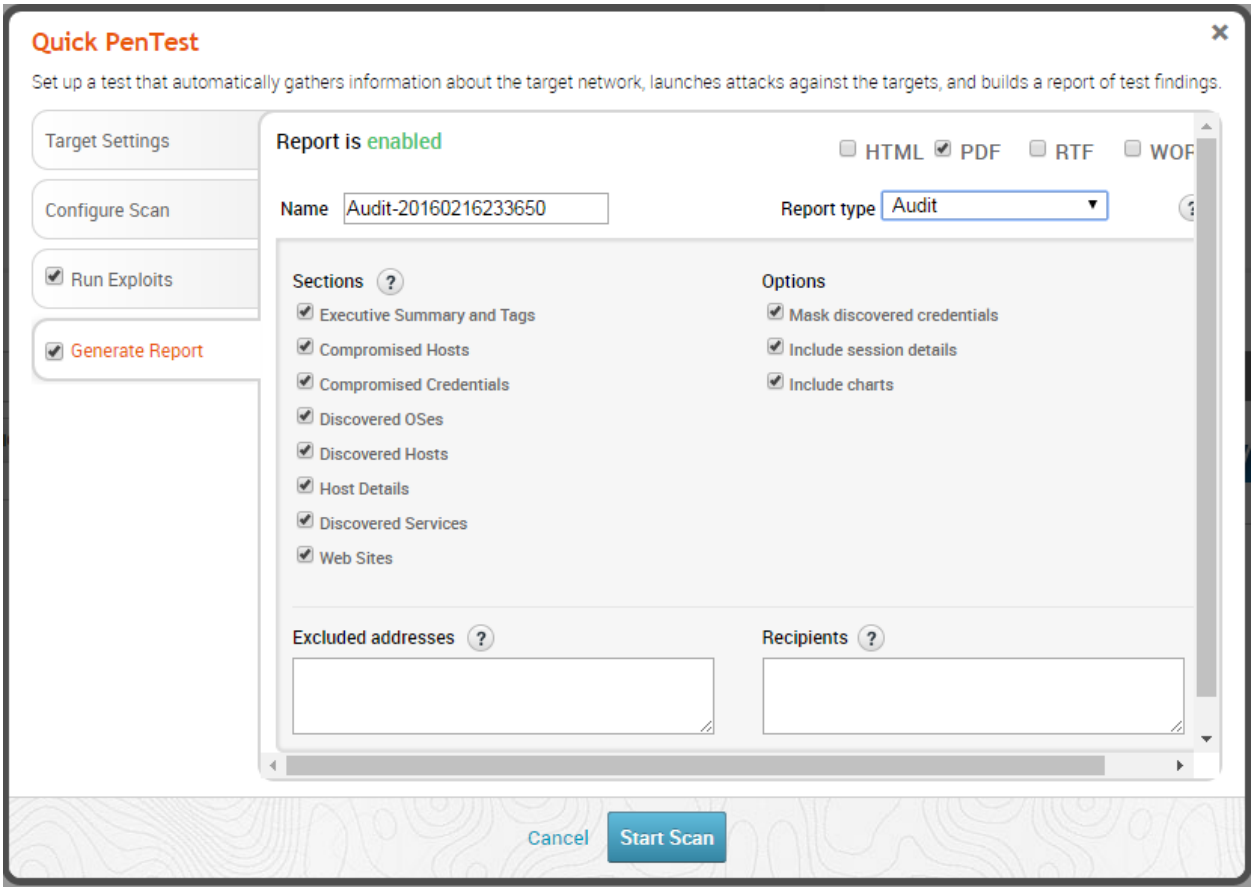
Projects in Metasploit Pro (as well as tasks within each projects) can be ran simultaneously. This feature will come in handy for this lab.

Exercise 2 – Using Quick PenTest Wizard

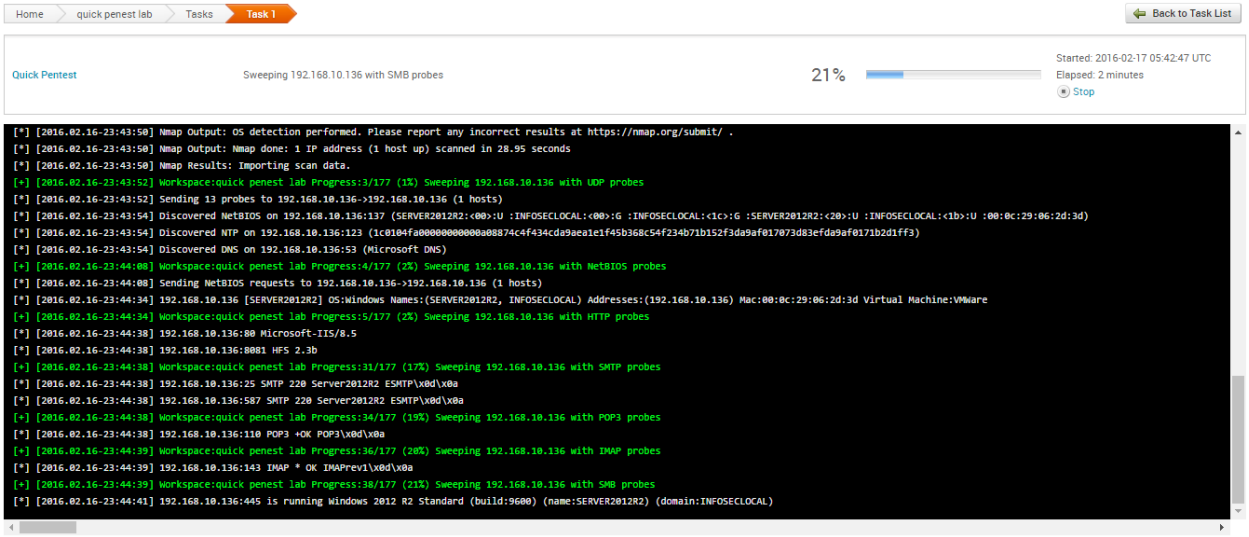
Select the “Quick PenTest” button from the Quick Start Wizards. In the dialog that opens, select “Windows Targets” as Target Profile, enter “quick pentest lab” as the Project Name, and the IP address of your Windows Server 2012 R2 VM as your Target Address.



Those are the only required options for Quick PenTest. Click through the remaining three tabs on the left and look at the options. For Generate Report, let’s check all three boxes under Options.

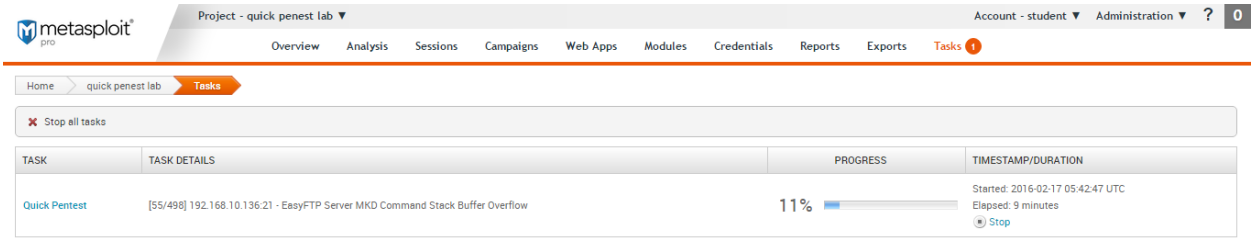


Click Start Scan. The dialog will close and the current task window will open, where you will see the progress of the Quick PenTest task.

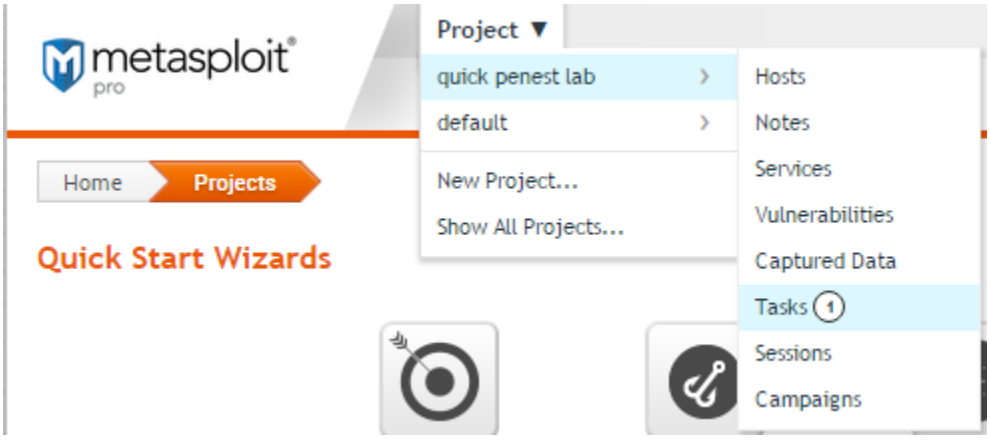


The “quick” in the Quick PenTest does not mean that this task will be quickly completed, it just requires minimal effort to setup. In fact, it will take a while to complete, depending on

configuration. So we will let it run for now and return to it in our last Metasploit Pro lab. For now, select “Back to Task List” on the top right. The list of tasks will be displayed, and you should also see the number of running tasks on the top, next to the “Tasks” menu item.



We can take another step back and click on the “quick pentest lab” link, which would display the Dashboard for our current project, with data gathered so far and results of successfully performed actions. This dashboard looks the same for all projects, so let’s just skip it for now and go back to Home. We can see that Project Listing now includes our “quick pentest lab” project with some stats. We can click on the project name to go to it, or we can select Project from the top menu and navigate to a specific section:



Let the Quick PenTest run and move on to the next lab[2].

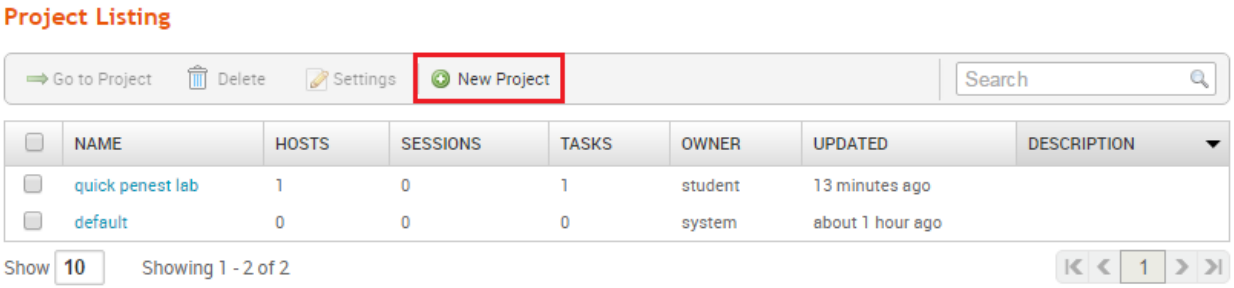
End of Lab

[2] Do not reboot, shut down, or revert your Metasploit Pro VM until Quick PenTest is finished. If you had to do it, follow the same steps to re-launch Quick PenTest.

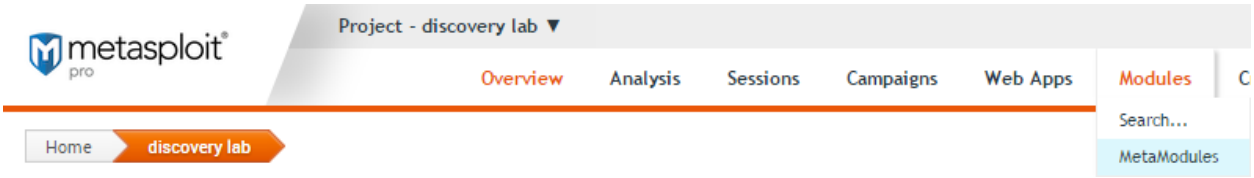
Lab 2 - Discovering Targets

Exercise 1 – Passive Network Discovery MetaModule

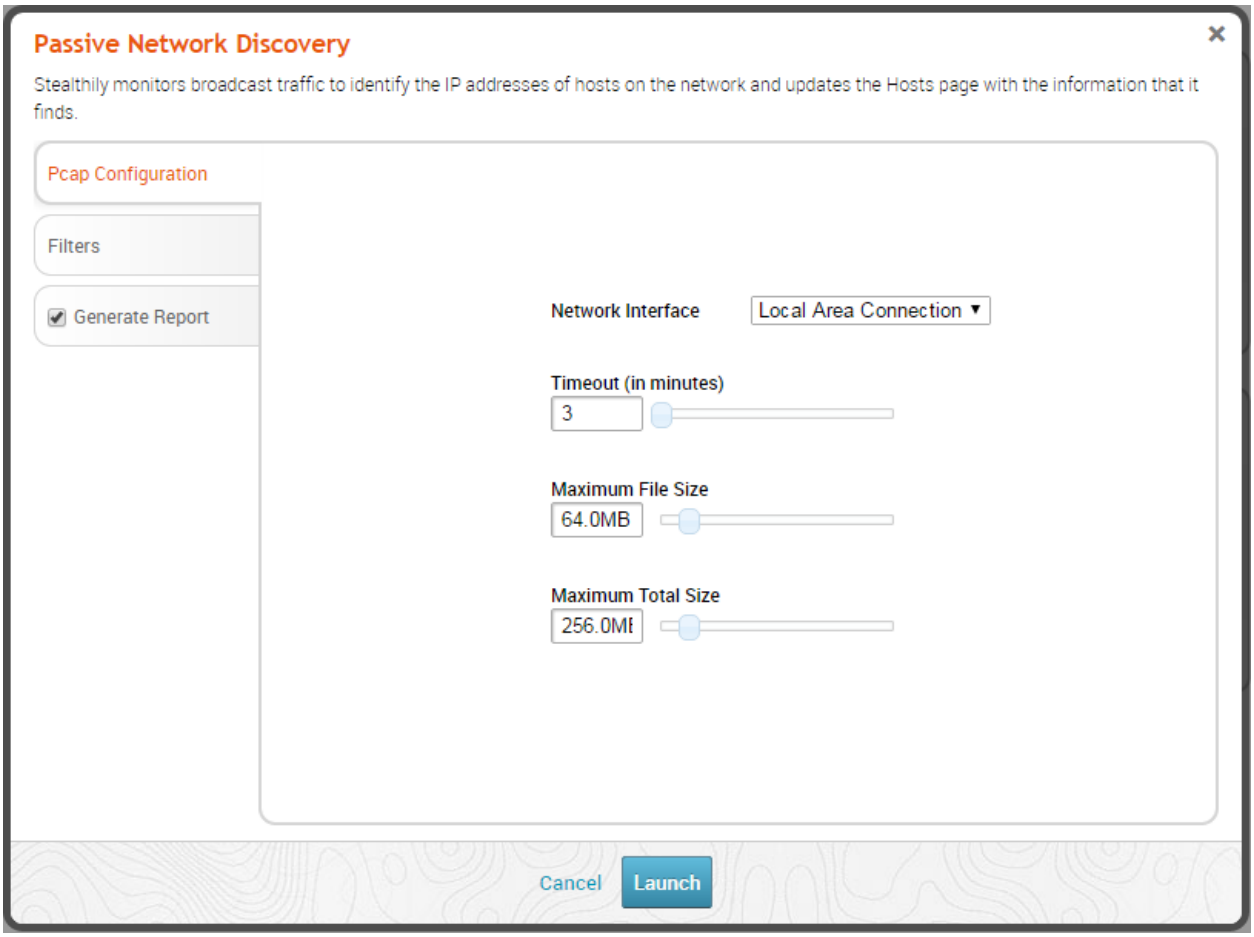
First, let's create a new project for this lab. On the Metasploit Pro Home screen, click the New Project button in the Project Listing section.



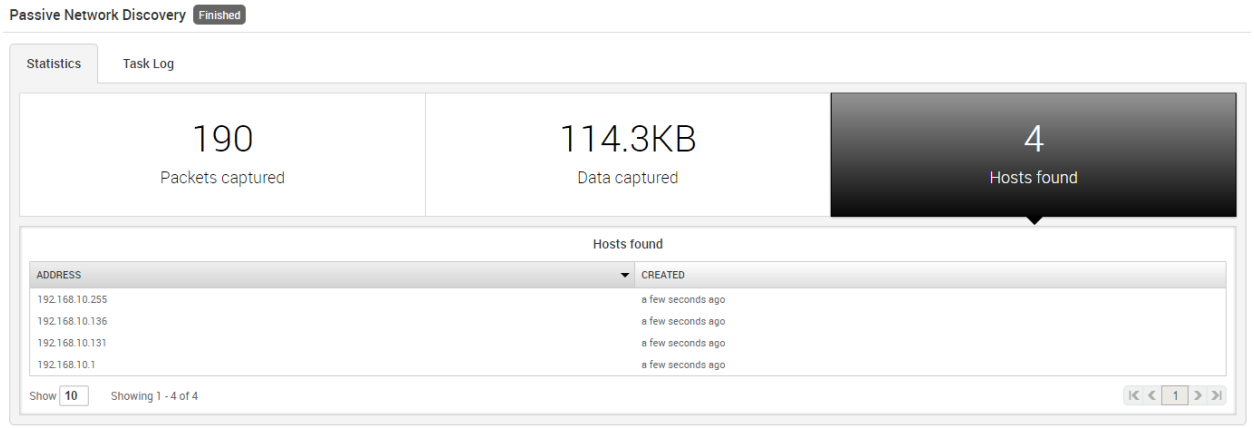
Alternatively, you can select Project->New Project from the menu on top. In the Project Settings dialog, name your project "discovery lab", add some description if you want, and click the Create Project button. You will be taken to the Overview page for the newly created project. As our first task, we will run the Passive Network Discovery MetaModule. MetaModules in Metasploit Pro are yet another efficiency feature: they provide a quick and simple way to perform common pentesting tasks than may be time consuming when completed manually. To access the MetaModules Overview Page, select Modules->MetaModules from the menu bar on top.



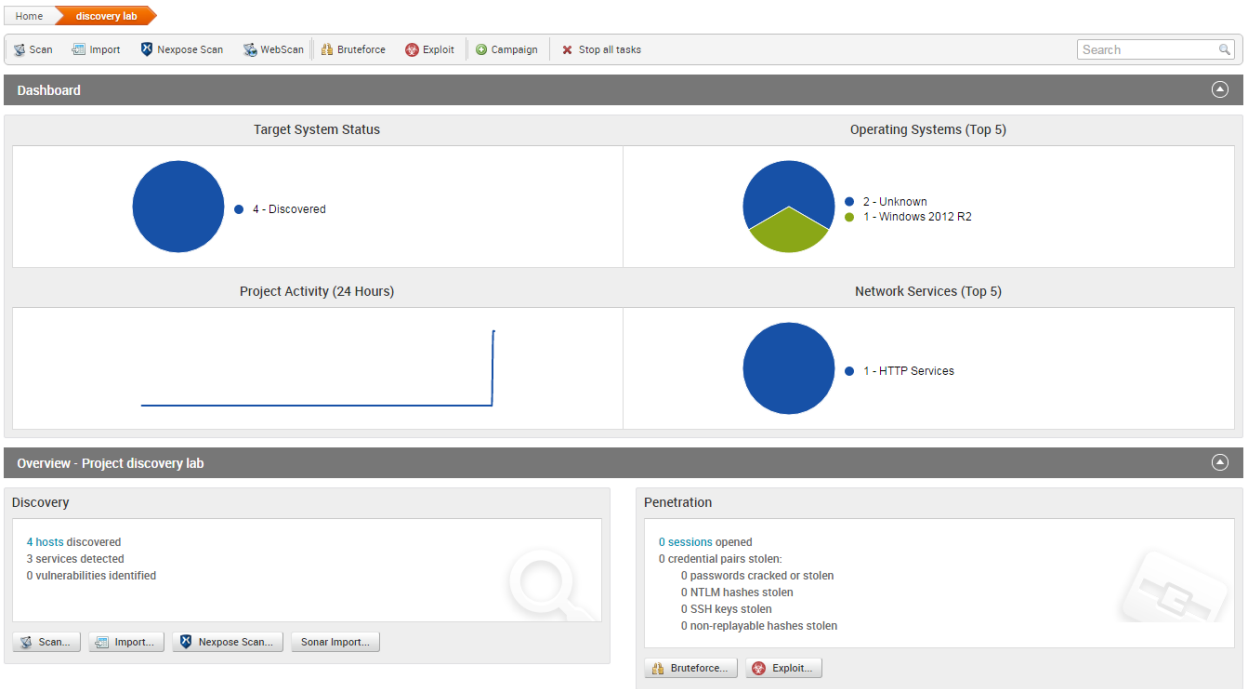
You will see seven small windows with short descriptions for each MetaModule. Find Passive Network Discovery and click the Launch button. As the name suggests, this is a passive technique, so no packets are sent: the MetaModule just sniffs traffic from the network. In the configuration window, select "Local Area Connection" as your Network Interface. Reduce the Timeout value to 3 minutes. We know that there is a Quick PenTest in progress, so there should be plenty of traffic for us to sniff. Click Launch to start the MetaModule.



You may not see any numbers displayed in the Statistics window: it is not updated immediately as new results come in. Don't worry, packets are being captured. After 3 minutes, the MetaModule will stop and the window will refresh. You may still see a zero for "Hosts found", but in a few seconds the window will refresh again and there should be a list of hosts on the bottom. The updated window should look something like the image below (your results will be different).



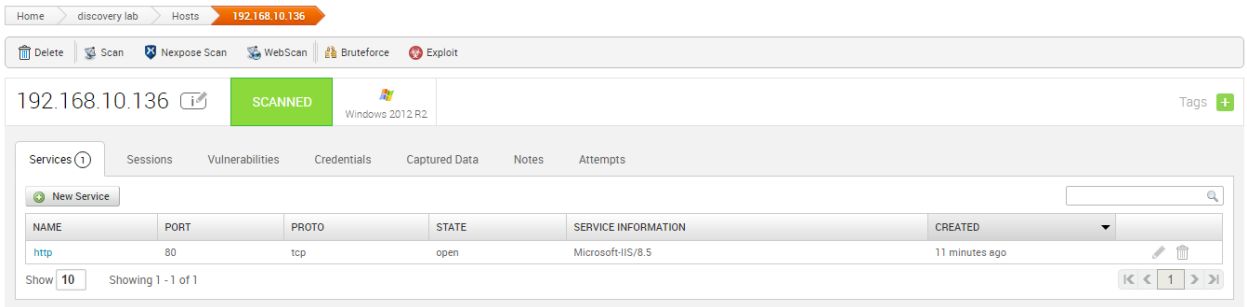
Close the Statistics window (click the “Close” button on the bottom right or the “X” on the top right) and select the “discovery lab” link on top to go to the Project Dashboard. You should see that Passive Network Discovery MetaModule discovered several IPs and was able to identify the Operating Systems for some of them. You may also see some services that were discovered, such as HTTP.



Click on the blue link with the number of discovered hosts in the Discovery pane. Now that we have a list of live hosts, we can focus on one of targets and gather more information.

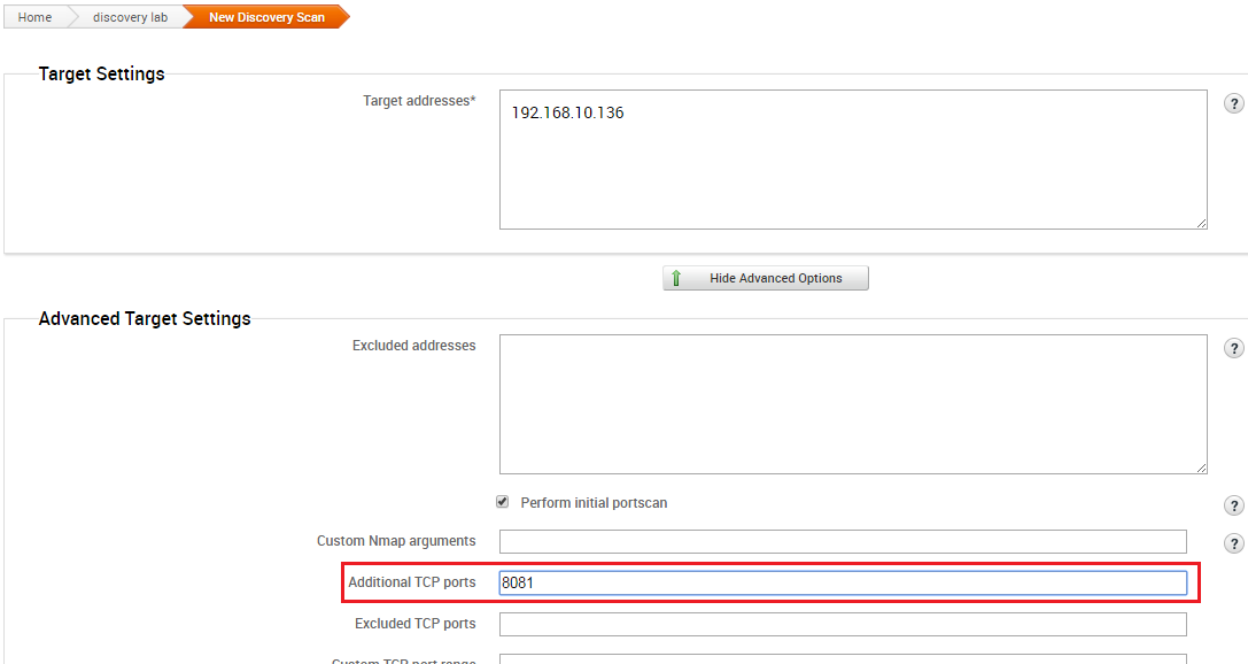
Exercise 2 – Discovery Scan

Select the IP address of the Windows Server 2012 R2 VM.

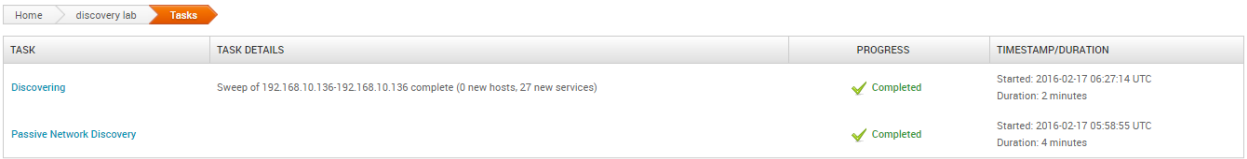


There are several options in the menu right above the IP address. Select the “Scan” button. In the “New Discovery Scan” window, the target address will be automatically filled out. This is the only required option. Click the “Show Advanced Options” button and look through the available

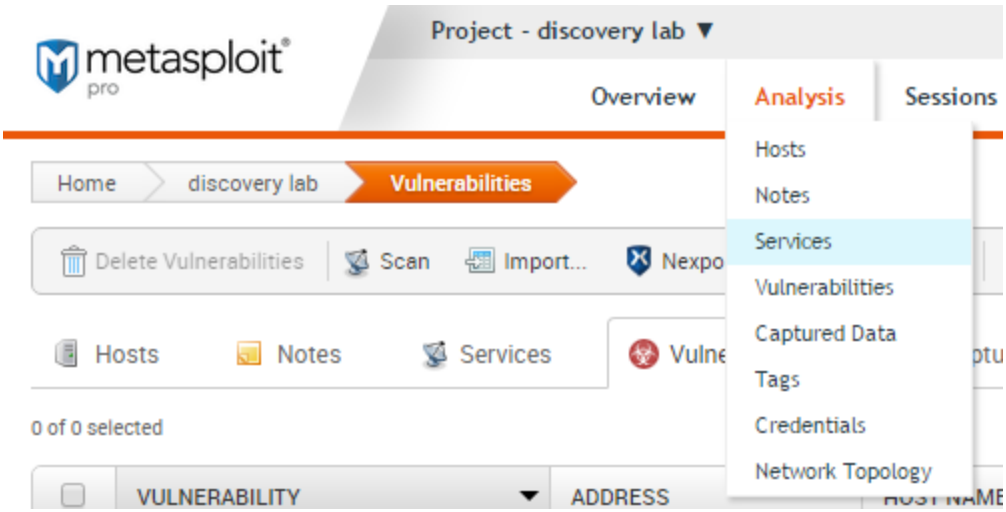
settings. We want to make sure that the port for our vulnerable HTTP File Server is scanned, so enter “8081” into the Additional TCP ports field.



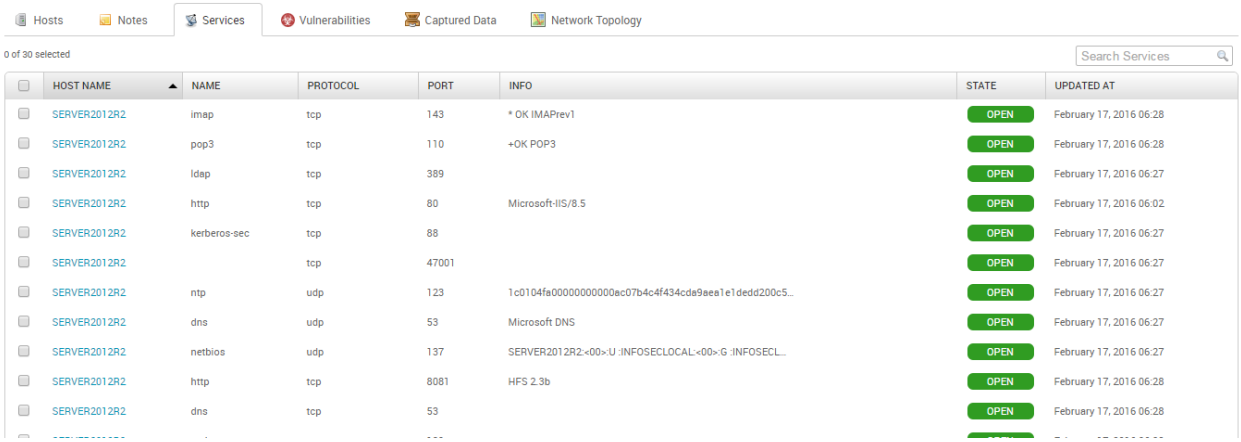
Scroll all the way to the bottom and click “Launch Scan”. Now if you click on the Tasks link on top or select Tasks->Show Tasks from the top menu bar, you should see the list of tasks for our current project, which now includes 2 tasks.



You may click on the Discovering link in the list, but this will not take you to results but rather to the logged scan process, which allows you to scroll through and see what exactly your scan was doing. To see the information we gathered with the scan, we can return to the Project Dashboard again, or we can go straight to a specific category of data that we are interested in. We can see that quite a few services were discovered, so let’s take a closer look at those. From the navigation menu on top, select Analysis->Services.



We will see a long list of open services, along with associated ports, and, in some cases, associated application. Results should include our vulnerable Rejetto HFS application, and we can clearly see the version.



HOST NAME	NAME	PROTOCOL	PORT	INFO	STATE	UPDATED AT
SERVER2012R2	imap	tcp	143	* OK IMAPrev1	OPEN	February 17, 2016 06:28
SERVER2012R2	pop3	tcp	110	+OK POP3	OPEN	February 17, 2016 06:28
SERVER2012R2	ldap	tcp	389		OPEN	February 17, 2016 06:27
SERVER2012R2	http	tcp	80	Microsoft-IIS/8.5	OPEN	February 17, 2016 06:02
SERVER2012R2	kerberos-sec	tcp	88		OPEN	February 17, 2016 06:27
SERVER2012R2		tcp	47001		OPEN	February 17, 2016 06:27
SERVER2012R2	ntp	udp	123	1c0104fa00000000000ec07b4c4f434cda9aea1e1dedd200c5...	OPEN	February 17, 2016 06:27
SERVER2012R2	dns	udp	53	Microsoft DNS	OPEN	February 17, 2016 06:27
SERVER2012R2	netbios	udp	137	SERVER2012R2:<00>:U :INFOSECLOCAL:<00>:G :INFOSECL...	OPEN	February 17, 2016 06:27
SERVER2012R2	http	tcp	8081	HFS 2.3b	OPEN	February 17, 2016 06:28
SERVER2012R2	dns	tcp	53		OPEN	February 17, 2016 06:28

This certainly would give a pentester a lot of useful information. But even with this data gathered, Metasploit hadn't provided us with any specific information regarding the target system's vulnerabilities. If you click on the Vulnerabilities tab on top, you won't see any results. Remember, Metasploit is not a vulnerability scanner[3], it is more about exploiting vulnerabilities than finding them. However, Metasploit Pro includes features that make the process of discovering or mapping vulnerabilities a lot easier. We will look at them in the next lab.

End of Lab

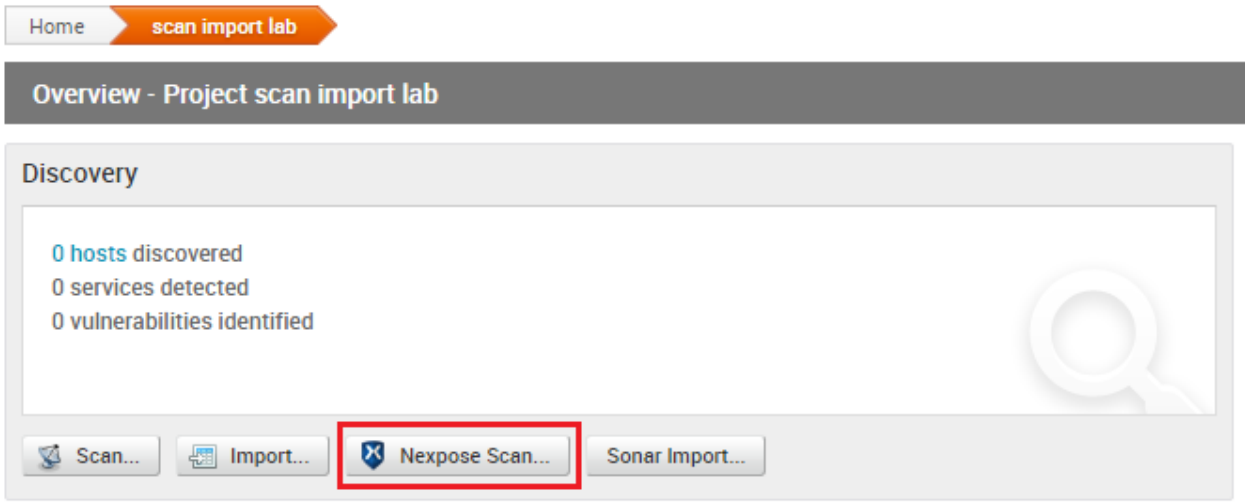
[3] However, the Web Scan feature can find Web application vulnerabilities.

Lab 3 - Importing Scan Data

Exercise 1 – Nexpose Integration

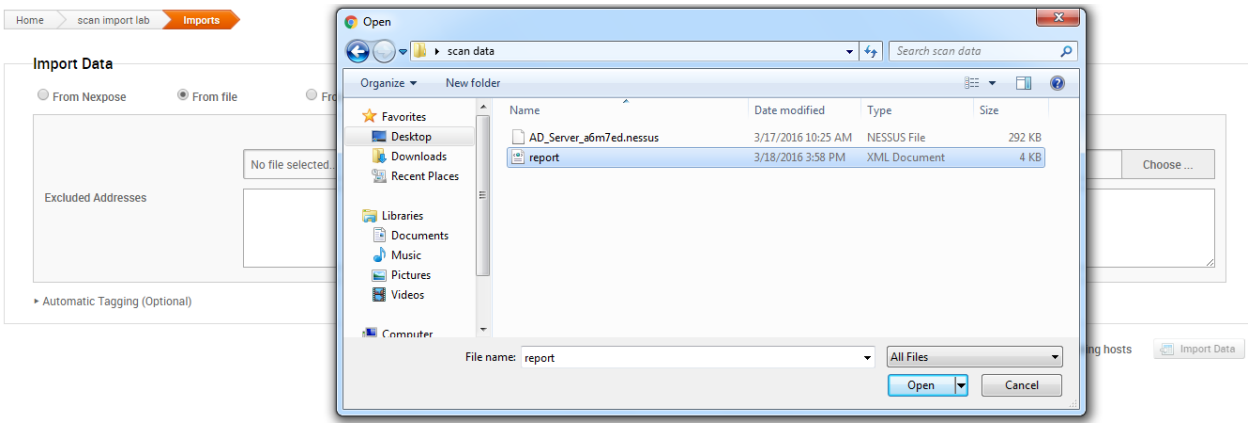
As we mentioned in the previous lab, Metasploit Pro cannot perform vulnerability scans on its own, but can use scan results produced by other tools. It can also work together with Nexpose, a vulnerability scanner from Rapid7. In this lab we will take a look at importing scan data.

First, let's create a new project. Go back to the Home screen and add a project (the "New Project" button or Project->New Project from the top menu). Name your project "scan import lab". Once at the Project Overview page, select the "Nexpose Scan" button from the Discovery pane[4].

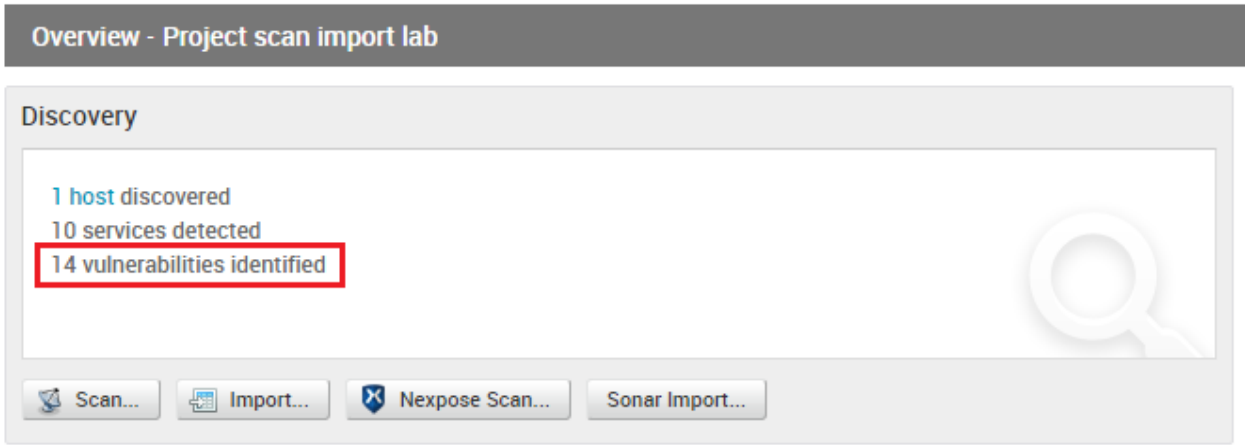


If we had a Nexpose console running, we could have run a vulnerability scan from within Metasploit Pro and imported the results right away. Since we don't have a connected Nexpose console, we can just import scan results gathered by Nexpose earlier. In the Import Data pane, change the selection to "From file", then click "Choose", browse to the **report** file located in the **Desktop/scan data** folder and click Open.

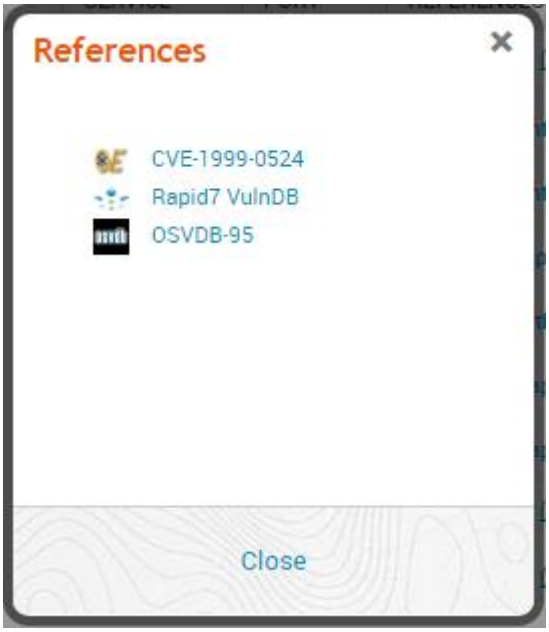
[4] Note that clicking the "Import" button would take you to the same screen, only with different options selected.



Select the “Import Data” button. It will only take a second to complete. Now go back to the Project Dashboard. You will see results similar to the ones gathered by the Discovery Scan in the previous lab, however, if you look at the Discovery pane, you will see that the number of identified vulnerabilities is not zero in this case.

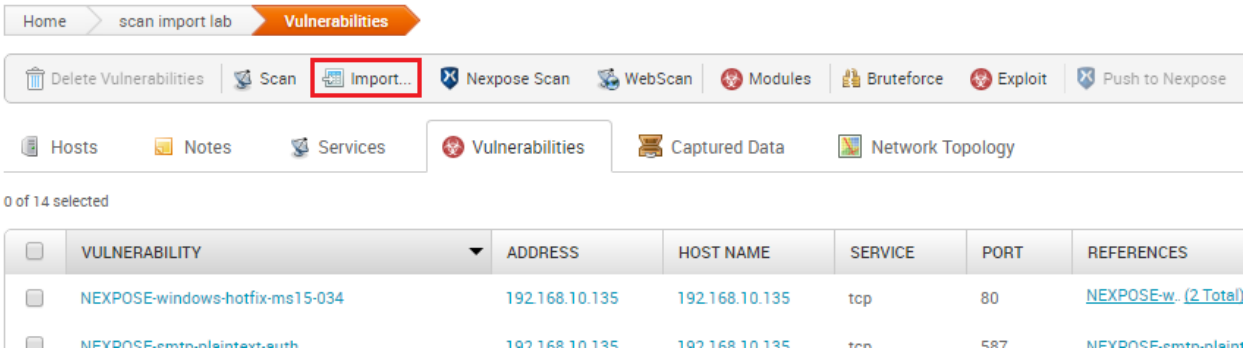


To examine the identified vulnerabilities, we can click on the blue “1 host” link and then select the “Vulnerabilities” tab, or go to Analysis->Vulnerabilities from the navigation menu on top. You will see the list of vulnerabilities with associated host IP addresses, services/ports, reference links, and other information. You can see that all of the vulnerabilities have the “Not Tested” status. Vulnerability Validation is yet another feature that requires a connected Nexpose console, so we won’t worry about it for this lab. You can see that some of vulnerabilities have several reference links for them (the ones that are underlined). Click on any of those links. A small window will open with links pointing to corresponding entries on various sources, including Rapid7 VulnDB, CVE, OSVDB, ForensicsWiki, and others.

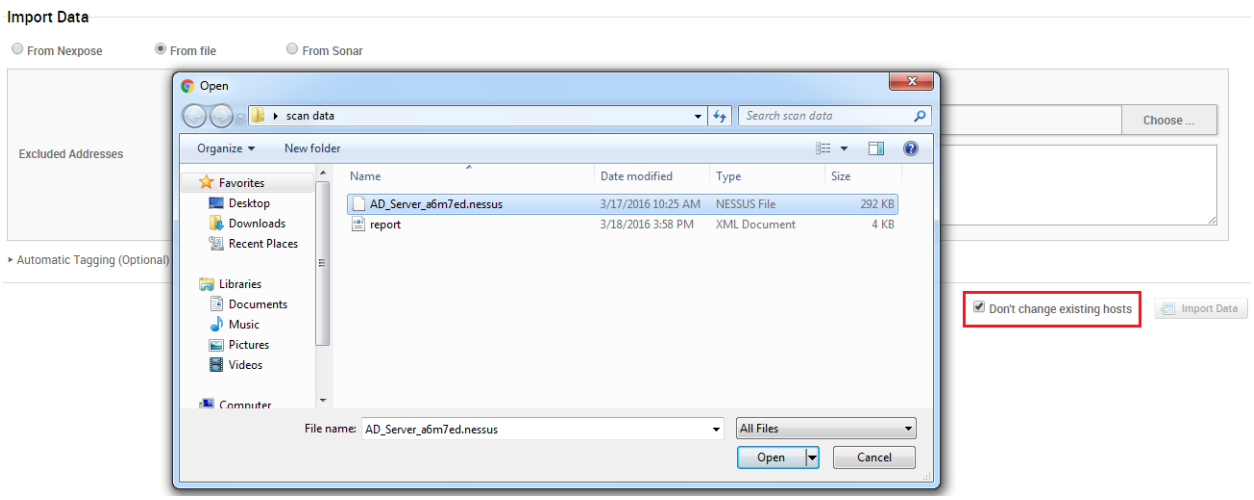


Exercise 2 – Importing Nessus scans

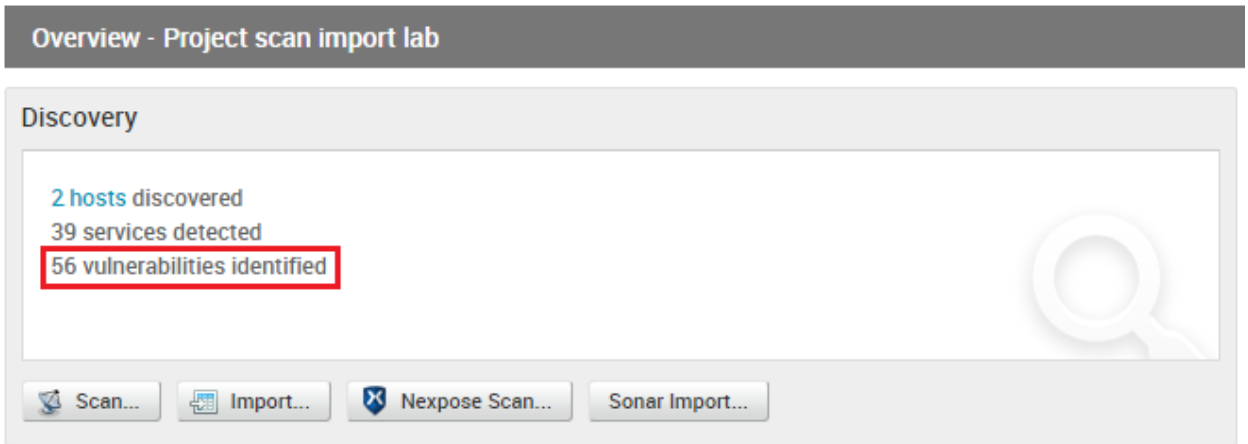
It is just as easy to import scan results gathered by other tools. In this exercise we are going to import a copy of the Nessus scan we performed earlier in our Vulnerability Identification lab. If you are still on the Vulnerabilities page, just select the "Import" button from the menu bar.



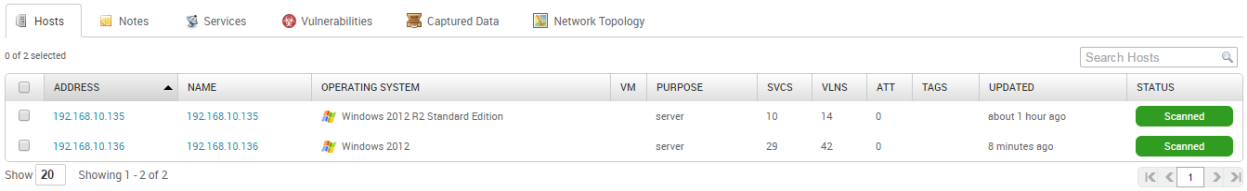
This time we want to check the "Don't change existing hosts" box, so the data we have already gathered/imported would not be overwritten. Click the "Choose" button, browse to the **AD_Server_a6m7ed.nessus** file located in the **Desktop/scan data** folder, and click Open.



Click “Import Data”. After the import is completed, go to the Project Dashboard. You can see that we have 2 hosts now, but, more importantly, the number of identified vulnerabilities is now much bigger!



We can now go to Analysis->Vulnerabilities again now and look at the Nessus scan results. Remember, that even though the IP addresses are different, those are two scans of the same host. Now switch to the “Hosts” tab. Now we can look the results separately. We can see that Nexpose found 14 vulnerabilities, while the Nessus scan found 42 vulnerabilities.



Click on the IP address for the Nessus scan (it should be 192.168.10.136). We can see that some tabs have numbers next to them. We know what Services and Vulnerabilities are, let’s take a look at Notes.

192.168.10.136
[192.168.10.136]
SCANNED
Windows 2012

Services (29) Sessions Vulnerabilities (42) Credentials Captured Data Notes (2) Attempts Modules (2)

NAME	DATA
host.os.nessus_fingerprint	{ os : Microsoft Windows Server 2012 R2 Standard }
host.imported	{ filename : C:/Windows/Temp/import20160217-1920-1x91ckw, type : Nessus XML (v2), time : 2016-02-17T08:15:35Z }

You can click on the note to expand it. First is the result of host fingerprinting and the second is the details of our scan file import. Now let's look at the Modules tab.

Services (29) Sessions Vulnerabilities (42) Credentials Captured Data Notes (2) Attempts Modules (2)

Auxiliary: MS15-034 HTTP Protocol Stack Request Handling Denial-of-Service (Launch)

Description

This module will check if scanned hosts are vulnerable to CVE-2015-1635 (MS15-034), a vulnerability in the HTTP protocol stack (HTTP.sys) that could result in arbitrary code execution. This module will try to cause a denial-of-service.

Module Details

Name	MS15-034 HTTP Protocol Stack Request Handling Denial-of-Service
Fullname	auxiliary/dos/http/ms15_034_ulonglongadd
Rank	★★
Stance	aggressive

Auxiliary: MS15-034 HTTP Protocol Stack Request Handling HTTP.SYS Memory Information Disclosure (Launch)

Description

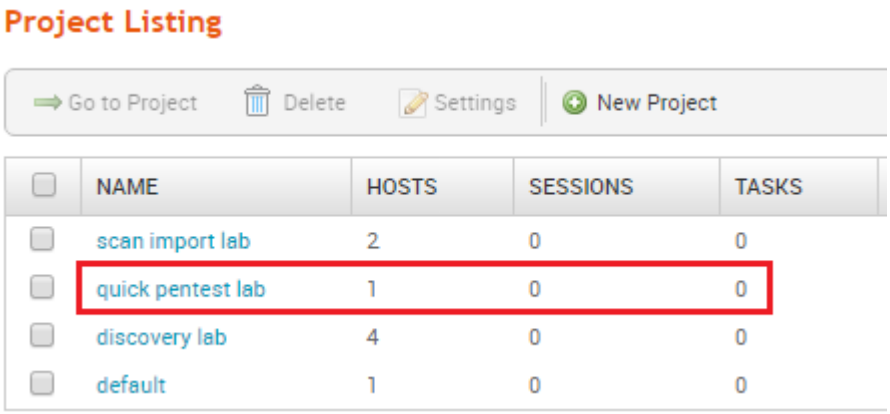
This module dumps memory contents using a crafted Range header and affects only Windows 8.1, Server 2012, and Server 2012R2. Note that if the target is running in VMware Workstation, this module has a high likelihood of resulting in BSOD; however, VMware ESX and non-virtualized hosts seem stable. Using a larger target file should result in more memory being dumped, and SSL seems to produce more data as well.

We can see that Metasploit found 2 modules based on the imported vulnerability scan. Both of them are Denial-of-Service modules. One of them, Auxiliary: MS-15-034 HTTP Protocol Stack Request Handling HTTP.SYS Memory Information Disclosure, may result in BSOD if target runs on VMware Workstation, so maybe let's not do that! The other, Auxiliary: MS-15-034 HTTP Protocol Stack Request Handling Denial-of-Service, seems a bit less dangerous, so we can try running it.

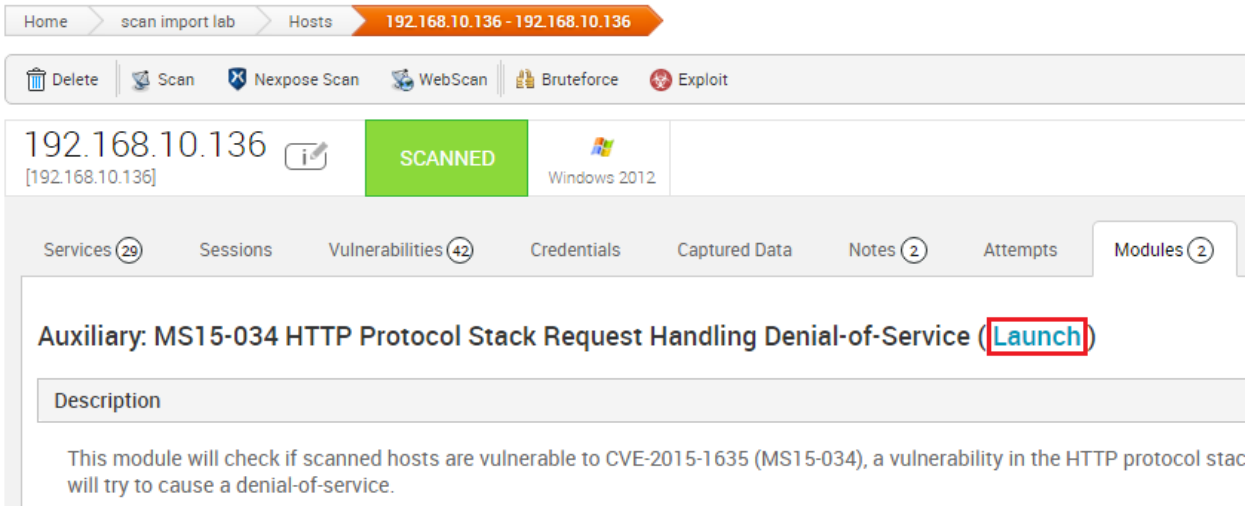
Exercise 3 – Manual Vulnerability Validation

WARNING: Running this module **WILL** crash your Windows Server 2012 R2 VM. Be sure that you are OK with it and check with your instructor before proceeding. If crashing the VM is not something you want to do at the moment, just read through the next section.

First, we need to make sure that our Quick PenTest is completed (it may be at this point). Go to the Home page and look at the Project Listing. If you see 0 tasks for the "quick pentest lab", you can proceed, if there's still a task running, you should move on to the next lab for now and return to this exercise later.



Now go back to the Modules page. The easiest way to do it would be by using the browser's Back button. Select the "Launch" link next to the module name.



The target address would be filled out automatically but you may need to change it to match the actual IP of your Windows Server 2012 R2 VM. We don't need to configure anything else, but feel free to look at the available Advanced and Evasion options.

MS15-034 HTTP Protocol Stack Request Handling Denial-of-Service

auxiliary/dos/http/ms15_034_ulonglongadd

This module will check if scanned hosts are vulnerable to CVE-2015-1635 (MS15-034), a vulnerability in the HTTP protocol stack (HTTP.sys) that could result in arbitrary code execution. This module will try to cause a denial-of-service.

Target Systems

Target Addresses	Excluded Addresses
192.168.10.136	

Exploit Timeout (minutes)

5

Module Options

Proxies		A proxy chain of format type:host:port[,type:host:port][...] (string)
RPORT	80	The target port (port)
SSL	☐	Negotiate SSL/TLS for outgoing connections (bool)
TARGETURI	/	URI to the site (e.g /site/) or a valid file resource (e.g /welcome.png) (string)
THREADS	1	The number of concurrent threads (integer)
VHOST		HTTP server virtual host (string)

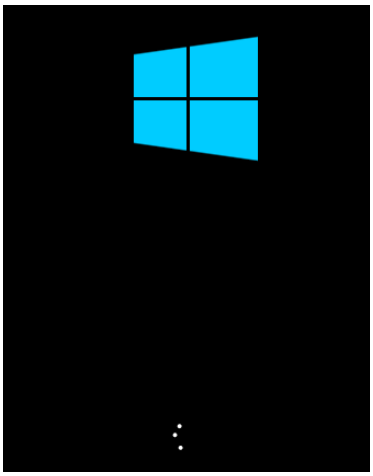
Advanced Options show

Evasion Options show

Run Module

Click “Run Module”. After the task is completed, take a look at your Windows Server 2012 R2 VM[5].

[5] You may actually get a VMware error message instead. In either case, the VM will crash.



Oops!

DoS is fun, but in most cases what we would really want is to find a vulnerability that could allow us to do more than that. We will get closer to this objective in our next lab.

Re-login to the Windows Server 2012 R2 VM before proceeding.

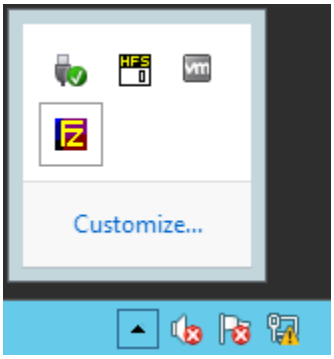
End of Lab

Lab 4 - Working with Credentials

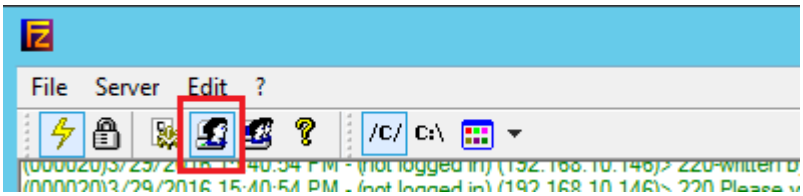
In this lab we are going to learn how to add credentials in a project and then use them in a Bruteforce attack.

Exercise 0 – Setting up the Target

First, let's configure an account that we will target with our Bruteforce attack. On your Windows Server 2012 R2 VM, open the FileZilla FTP Server user interface by double-clicking its icon in the notification area.



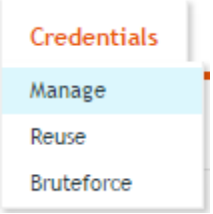
Next, select the Users icon.



In the Users dialog, change the Password value to **password!!!** and click OK.

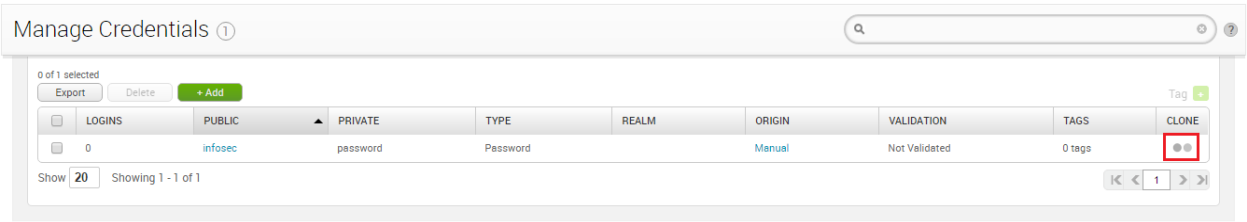
Exercise 1 – Adding Credentials

There are several ways credentials can be added in Metasploit Pro. First we will look at adding credential pairs manually. Create a new project from the Home screen and name it "credentials lab". On the Project Overview page select Credentials->Manage from the top navigation bar.



On the Manage Credentials page, select the green “+Add” button. Leave the Realm Type as “None” and switch to the “Public” tab (“public” is the Metasploit Pro term for username). Enter **infosec** into the Public field. Finally, switch to the “Private” tab (“private” is what Metasploit Pro calls passwords), select “Plaintext Password” for Private type and enter password for Password. Click OK.

You will see that our credential pair was added to the list. Now, if wanted to add another pair of similar, but slightly modified credentials, we can use the Clone options. Select the two gray dots icon under CLONE in the credentials list.



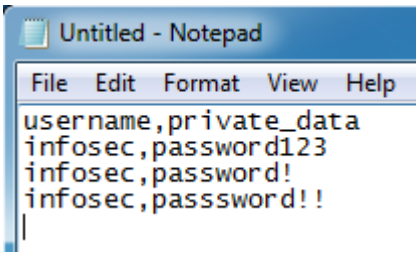
A new credential pair is created, now we can easily modify the private and public values. Add "1" to the end of credentials and click "Save" in the CLONE column. This is the process of manually adding credentials. Now let's create a list of credentials in CSV format and import it. The easiest way to create a CSV file would be by using a spreadsheet editor, such as Microsoft Excel. But notepad would also work. From the Start menu, type in **notepad** into the Search field and hit Enter to open Notepad. Now let's create a short list of credentials. To be able to import our list to Metasploit Pro, it needs to have the following header:

```
username,private_data
```

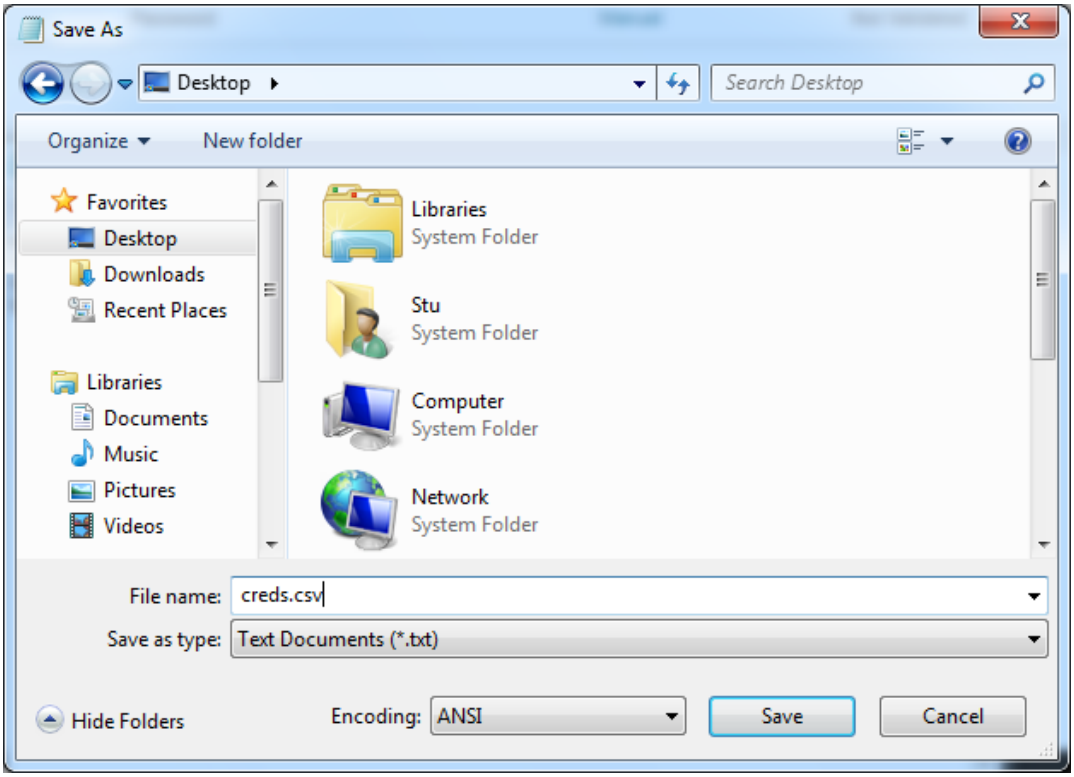
Enter the header and start adding credential pairs:

```
infosec,password123
infosec,password!
infosec,password!!
```

Your finished list will look like the image below.



Select File->Save As and save the list on the Desktop as creds.csv (don't forget to change the extension!)



Now go back to Metasploit Pro Credential Management page and click Add again. In the “Add Credential(s)” dialog, change the selection from Manual to Import, then click “Choose” to browse to our **creds.csv** file. Click OK.

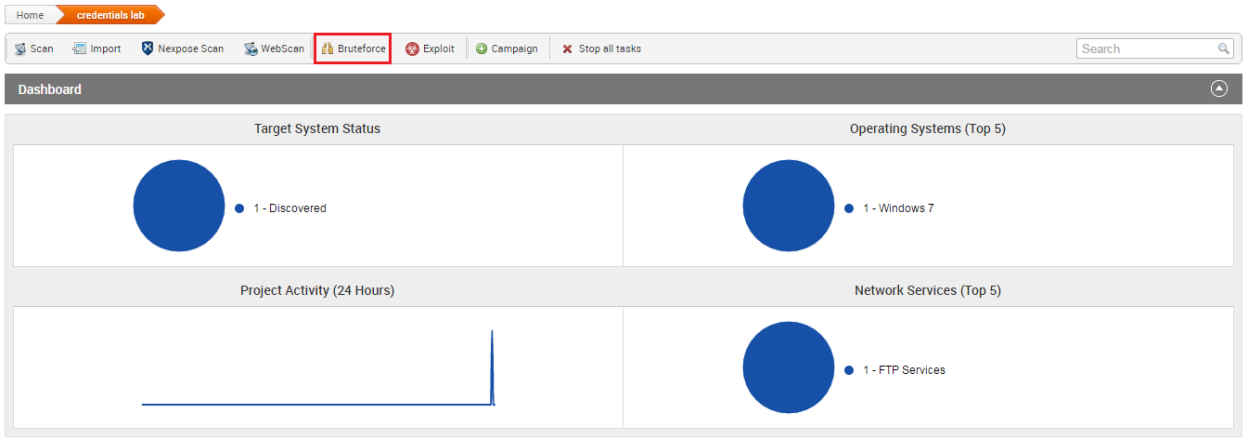
You will see that credentials were successfully added to our list. Note the ORIGIN tab: it identifies the method by which credentials were obtained. OK, we have our credential pair ready, let's do some bruteforcing!

Exercise 2 – Bruteforce attack

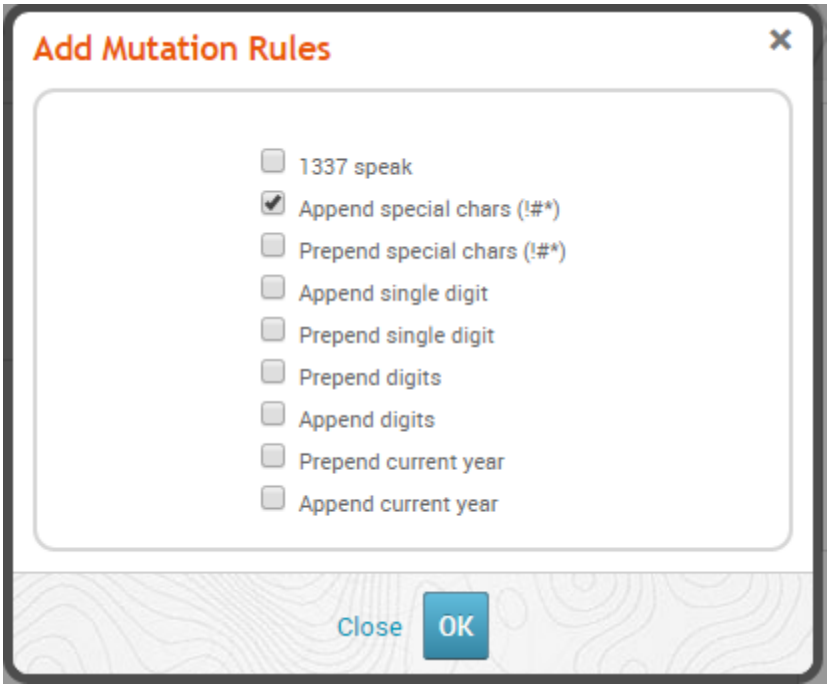
At the moment we don't have any hosts/services to bruteforce. Let's do a quick scan to add a host to our project. Go to the Overview tab and select "Scan" from the Discovery options. Enter the IP address of the Windows Server 2012 R2 VM as Target. This time, let's configure some advanced settings to save us some time. Click "Show Advanced Options" and configure it as follows:

- Enter **21** for "Custom TCP port range"
- Un-check all boxes in the Discovery Settings

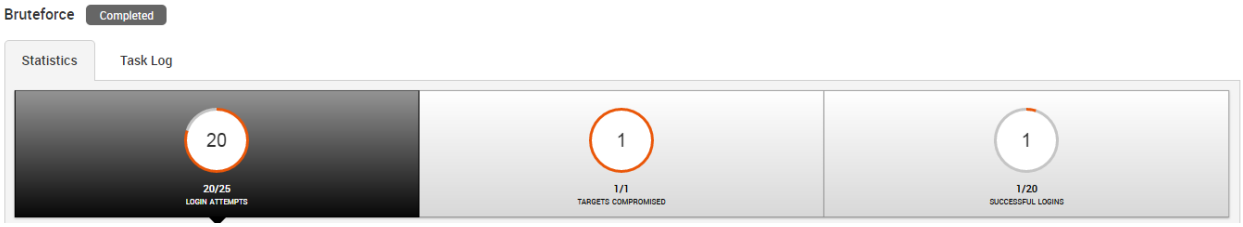
Click "Launch Scan" when done. The scan will be finished in a few seconds. Return to the Overview tab. You should see 1 host discovered and 1 service (FTP) detected. Select "Bruteforce" from the menu on top.



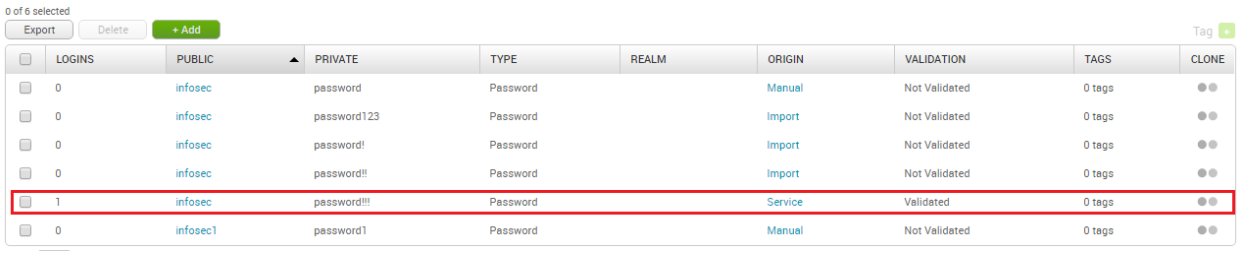
On the Bruteforce page, uder TARGETS, leave "All hosts" selected (we only have one) and check the box for FTP in "Select services" section. Under CREDENTIALS, check "All credentials in this project". Our 5 credential pairs will be added. Now, for the OPTIONS, leave all the timing selections at default, then select "Apply mutation(s)". Remember that we didn't enter the correct credential pair for our account. Mutations will modify the credentials we supplied, thus extending our list. In the "Add Mutations Rules" dialog, check the box for "Append special chars (!#*)" and click OK.



Notice that the number of possible combinations changed from 5 to 5+. Check the box for "Stop bruteforcing a target when a credential is guessed", then scroll down and click LAUNCH.[6] Click "Yes" to confirm and enjoy the show.

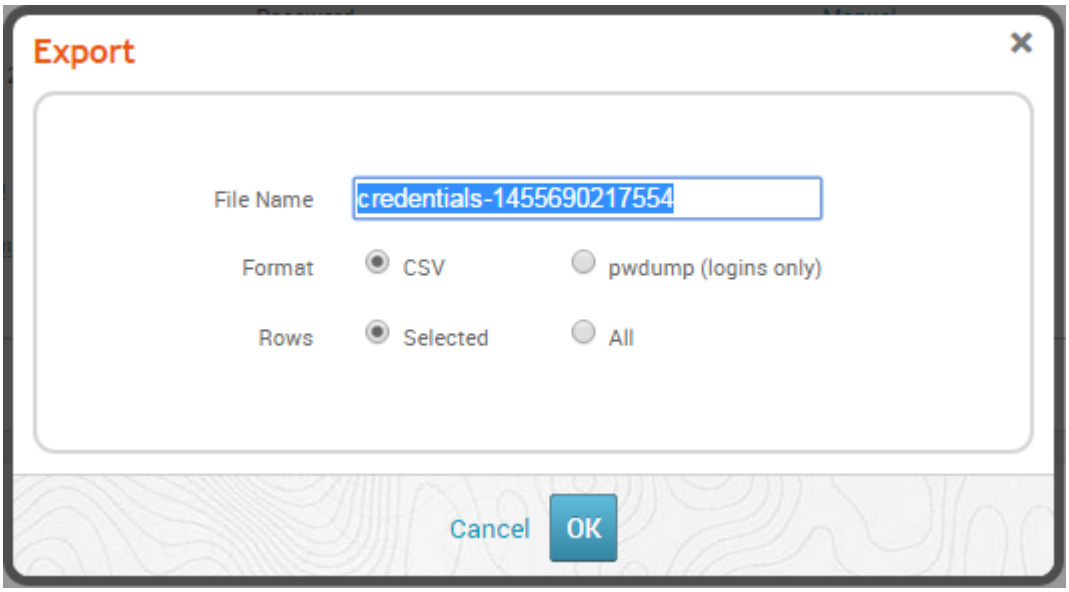


The attack won't take long with our short credentials list and only one mutation rule applied. After Bruteforce is successfully completed, return to the Credentials tab. Now we can see that our bruteforced credential pair is added to the list. It is listed as "Service" for ORIGIN, meaning that it was obtained by actually trying to login to a service, and was also Validated.



[6] Note that, if selected, Bruteforce can attempt to get session for MSSQL, MySQL, PostgreSQL, SMB, SSH, telnet, WinRM, and HTTP.

If we wanted to, we could now Export all or some of the credentials to a CSV or pwdump file and use in a different project.

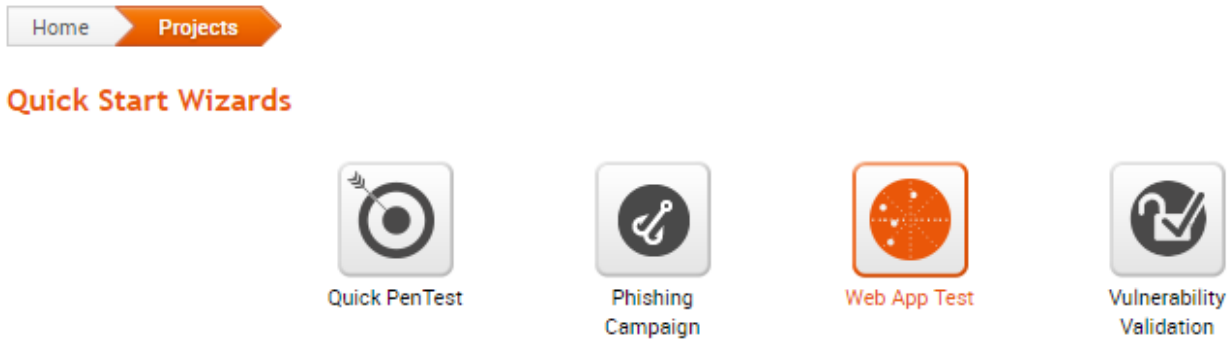


End of Lab

Lab 5 - Web App Test

Exercise 1 – Finding and Exploiting Web Vulnerabilities

Even though Metasploit isn't designed to find OS vulnerabilities, identifying vulnerabilities in Web application is something that it certainly can do. In this lab we will use the Web App Test Quick Start Wizard to perform a quick Web application vulnerability assessment. To start the wizard, select its button from the Quick Start Wizards menu on the home page.



Name the new project "web app test lab". For "Web Application Target URLs" enter the URL of Juggy Bank that we used in our SQL injection lab earlier (using the IP address of the Windows Server 2012 R2): http://192.168.x.x/sql/client2.htm

Next, switch to the "Find Vulnerabilities" tab and increase the value for "Time limit/form in minutes" to **10**.[7] Your configuration should look like the image below.

Feel free to look at other configuration tabs, but let's not change anything else for now. Click "Start Scan". After about 2-3 minutes you should see a notification about found vulnerabilities displayed in the Task window.

[7] Ten minutes should be sufficient for the test to succeed, but if it times out, try running it again with a bigger value.

```
[+] [2016.02.16-23:28:12]       VULNERABLE(PRO: SQL injection module) URL(http://192.168.10.136:80/sql/login.asp) PARAMETER(username) VALUES({"username"=>"'", "password"=>"", "B1"=>"Submit", "B2"=>"Reset"})
[+] [2016.02.16-23:28:12]               PROOF(ial" size=2> <p>Microsoft OLE DB Provider for ODBC Drivers</font> <font fa)
[+] [2016.02.16-23:28:12]       VULNERABLE(PRO: SQL injection module) URL(http://192.168.10.136:80/sql/login.asp) PARAMETER(password) VALUES({"username"=>"", "password"=>"'", "B1"=>"Submit", "B2"=>"Reset"})
[+] [2016.02.16-23:28:12]               PROOF(ial" size=2> <p>Microsoft OLE DB Provider for ODBC Drivers</font> <font fa)
```

Another 3-4 minutes later you should see the “Compromised” notification, meaning that Metasploit was able to not only find, but successfully exploit SQL injection vulnerabilities in our target Web application.

```
[+] [2016.02.16-23:56:38] Compromised 192.168.10.136:80 with exploit exploit/pro/web/sqli_mssql.
```

The completed task should result in 2 open sessions.

```
[+] [2016.02.17-00:14:50] Workspace:web app test lab Progress:3/3 (100%) Complete (2 sessions opened)
```

Before we jump to sessions, let’s look at the vulnerabilities found by the Web App Test. Go to the “web app test” Project Dashboard and select Analysis->Vulnerabilities from the navigation menu on top. One vulnerability will be displayed, which is the one that was exploited by Web App Test.

Hosts | Notes | Services | Vulnerabilities | Captured Data | Network Topology

0 of 1 selected

VULNERABILITY	ADDRESS	HOST NAME	SERVICE	PORT	REFERENCES	STATUS
SQL injection exploit for MSSQL	192.168.10.136	SERVER2012R2	tcp	80		Exploited

But didn’t we see 5 vulnerabilities found? Correct, Metasploit separates Web application vulnerabilities into a different category. To view them, switch to the “Hosts” tab, click on the IP of our target, and then select the Vulnerabilities tab.

Home > web app test lab > Hosts > 192.168.10.136 - SERVER2012R2

Delete | Scan | Nexpose Scan | WebScan | Bruteforce | Exploit

192.168.10.136
[SERVER2012R2]

SHELLED

Windows 2012 R2

Services (1) | Sessions (2) | Vulnerabilities (1) | Credentials | Captured Data | Notes (2) | Attempts (2)

New Vuln

NAME	REFERENCES	EXPLOIT
SQL injection exploit for MSSQL		exploit/pro/web/sqli_mssql

Show 10 Showing 1 - 1 of 1

Web Application Vulnerabilities

RISK	CATEGORY	NAME	BLAME	URL	PARAMETER	PROOF
High (75%)	SQLi	SQL Injection	App Developer	http://192.168.10.136/sql/login.asp)	username	ial" size=2> <p>Microsoft OLE DB Prov...
High (75%)	SQLi	SQL Injection	App Developer	http://192.168.10.136/sql/login.asp)	password	ial" size=2> <p>Microsoft OLE DB Prov...
High (75%)	SQLi	SQL Injection (blind)	App Developer	http://192.168.10.136/sql/login.asp)	username	Manipulatable response times.
High (75%)	SQLi	SQL Injection (blind)	App Developer	http://192.168.10.136/sql/login.asp)	password	Manipulatable response times.

Click on the URL value for either of the two vulnerabilities on top of the list. A new page will open, with detailed information about the vulnerability, including clickable URL, description, proof (you can see that the same error message was triggered for the test as in our SQL Injection lab), and the option to replay the vulnerability. If you click the “Replay SQLi Attack” button, you will be taken to a page containing a familiar error message.

192.168.10.136/sql/login.a

192.168.10.136/sql/login.asp

Microsoft OLE DB Provider for ODBC Drivers error '80040e14'

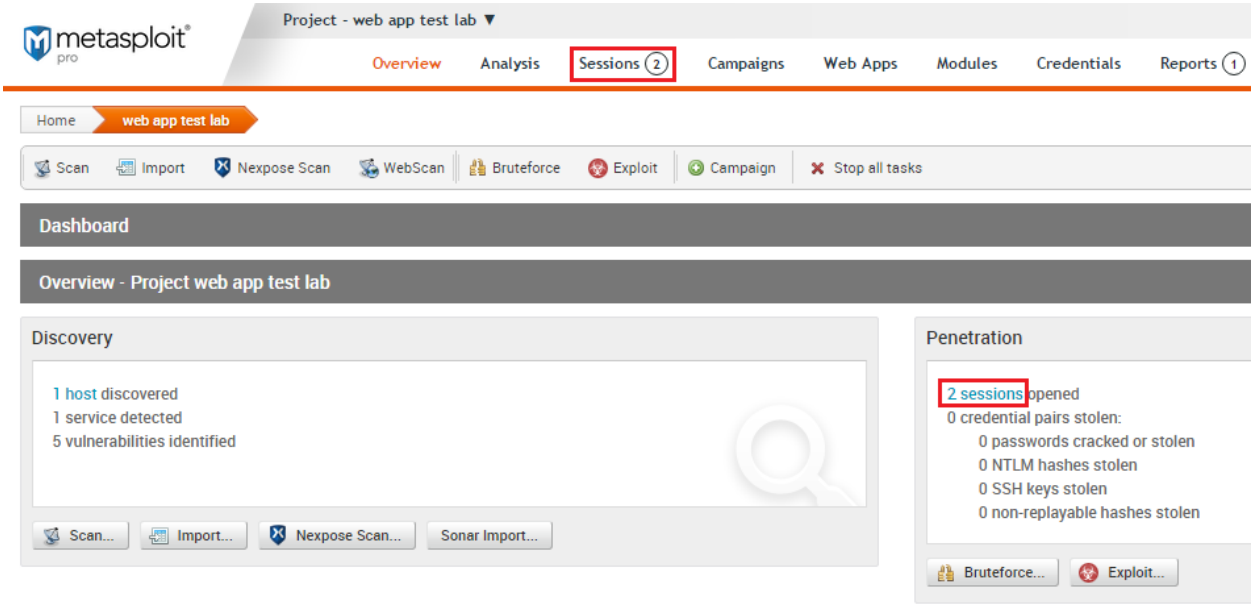
[Microsoft][ODBC SQL Server Driver][SQL Server]Unclosed quotation mark after the character string '' and password = ''.

/sql/login.asp, line 5

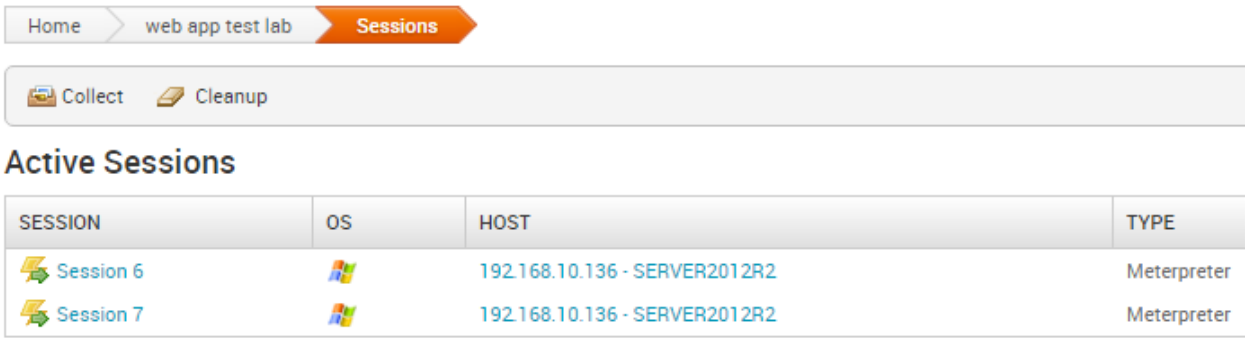
Hit the Back button and select either of the bottom two vulnerabilities. Read the description. Now, in the Replay Vulnerability section, try changing the “waitfor delay” value from 13 to something else, then hit “Replay SQLi Attack”. Go back again and try yet another value. Try some values that are very different, for example, you can try 2 first, then change it to 20. You will easily notice the difference in the time before the page loads. Now let’s move on to our opened sessions.

Exercise 2 – Working with Sessions

You can access opened sessions by either selecting Sessions from the navigation menu on top, or clicking the blue “2 sessions” link in the Penetration pane on the project Dashboard.



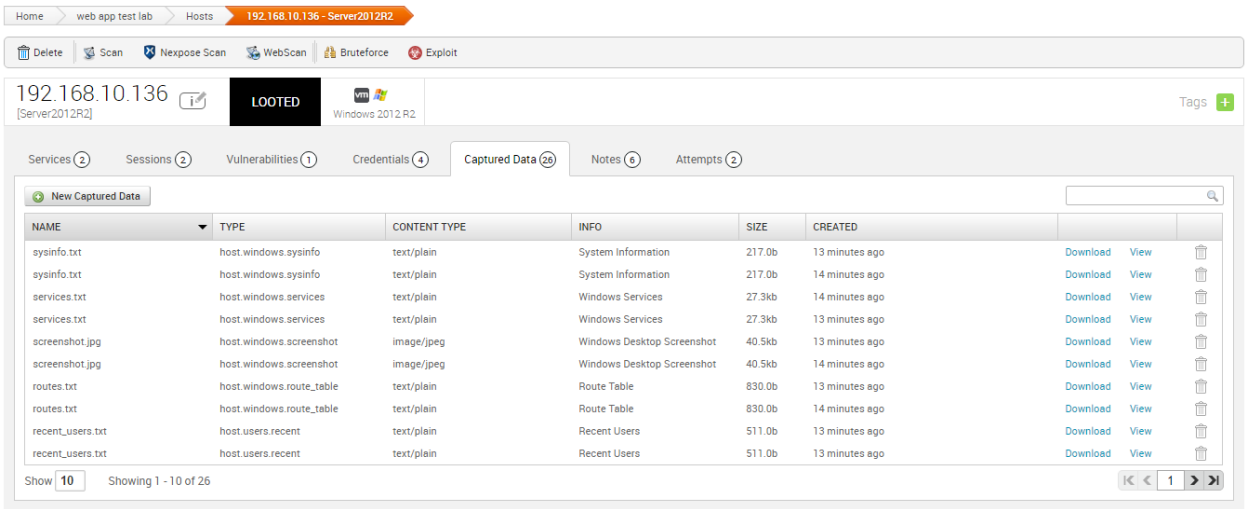
We can see that we have 2 active Meterpreter sessions.



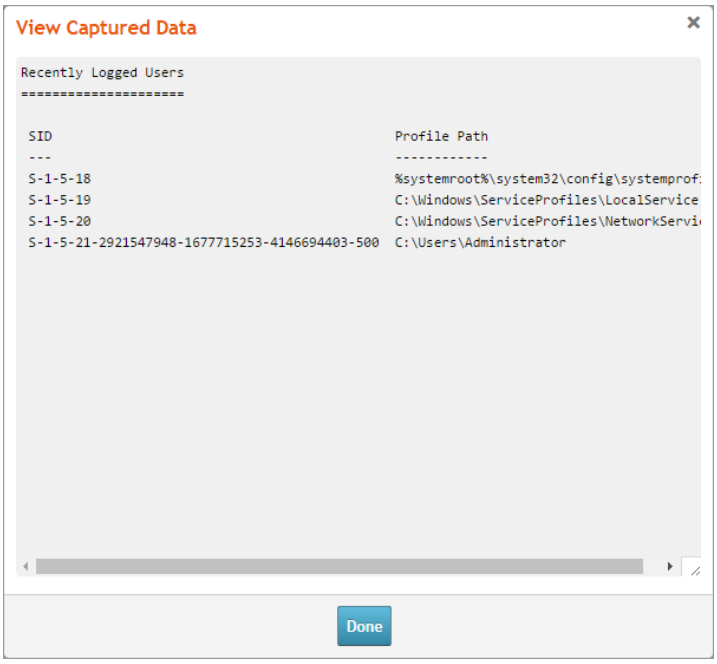
Click on either of them. You should see the list of available actions. Read the descriptions next to buttons to see what they are. Let’s click on “Collect System Data” first. Examine the available options for “Evidence to collect”. Let’s not change anything now, but note the “Collect other files” option, which allows collecting files with names that match a certain pattern (e.g., we can enter ***.doc** to collect all Microsoft Word documents). But for now let’s just run it with default options. Scroll all the way to the bottom and click the “Collect System Data” button. You may want to observer the output as the task runs, it’s pretty interesting. It will take only a couple of minutes to complete.

```
[+] [2016.02.17-00:52:52] Workspace:web app test lab Progress:4/4 (100%) Obtained 39 loots; Found 4 creds; Cracked 2 new hashes
```

As with many things in Metasploit Pro, we can access the captured data in a couple different ways: either by going to Analysis->Captured Data, or by clicking the host link in the Project Overview / Discovery pane, and then clicking the target's IP and selecting the Captured Data tab.



Click "View" for some of the items to see what data was captured.



And this is just one of the actions that can be performed with sessions. Let's examine some more. Select Sessions again from the navigation menu on top and click on the same sessions you used before. If look at the bottom of the page, you will see all the captured data, including screenshots, displayed there. Now select the "Access Filesystem" button. We can now easily browse the target's filesystem, download or delete the contents, or upload new files if we need to.

Home > web app test lab > Sessions > #6

Current Directory C:\ (↑ UPLOAD FILE ↑)

Downloaded 26 file(s) (show)

NAME	SIZE	LAST MODIFIED	AVAILABLE ACTIONS
$Recycle.Bin		2013-08-22 15:50:45 UTC	
Back to Parent Directory		1970-01-01 00:00:00 UTC	
Documents and Settings		2013-08-22 14:48:41 UTC	
PerfLogs		2013-08-22 15:52:33 UTC	
Program Files		2015-05-17 22:19:04 UTC	
Program Files (x86)		2016-02-29 22:24:54 UTC	
ProgramData		2015-05-17 22:19:04 UTC	
Snort		2015-04-17 22:22:28 UTC	
System Volume Information		2015-04-17 15:50:50 UTC	
Temp		2015-04-17 22:56:17 UTC	
Users		2015-04-17 15:38:39 UTC	
Windows		2016-03-22 17:38:03 UTC	
inetpub		2015-04-17 22:59:51 UTC	
BOOTNXT	1	2013-06-18 12:18:29 UTC	(↓ STORE ↓) | (× DELETE ×)
bootmgr	427680	2013-08-22 05:31:45 UTC	(↓ STORE ↓) | (× DELETE ×)
pagefile.sys	3221225472	2016-03-22 20:21:02 UTC	(↓ STORE ↓) | (× DELETE ×)

Go back to the Available Actions list. In the middle you should see the “Command Shell” button. In the description it says “advanced users”. That’s us! Let’s click on it. Now we are back to the command line interface (sort of). Scroll all the way to the bottom to see the Meterpreter > prompt. Enter some Meterpreter commands that you learned earlier, such as **getuid**.

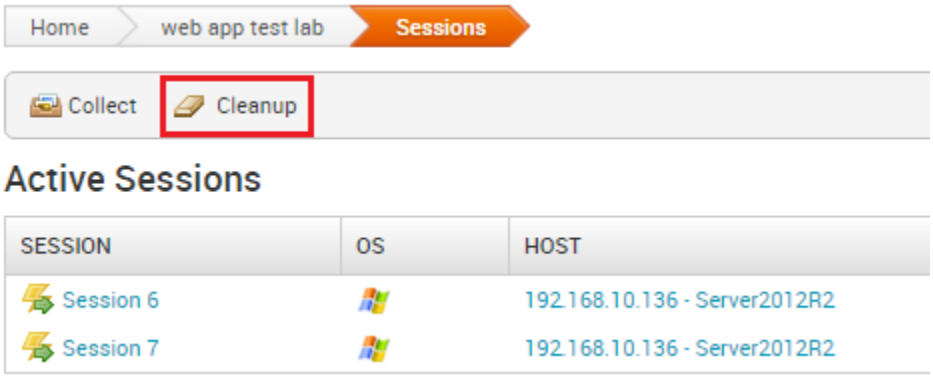
```
Metasploit - Mdm::Session ID # 6 (192.168.10.136)

  [*] Host process notepad.exe has PID 2560
  [*] Allocated memory at address 0x004e0000, for 285 byte stager
  [*] Writing the VNC stager into memory...
  [*] Starting the port forwarding from 53879 => TARGET:53879
  [*] Local TCP relay created: 127.0.0.1:53879 <-> 127.0.0.1:53879

 getuid

  Server username: NT AUTHORITY\SYSTEM
```

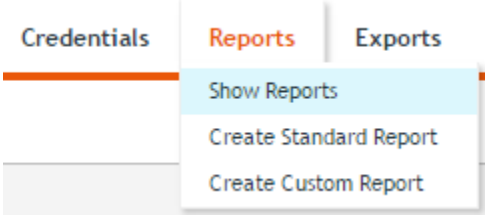
To close sessions, select Sessions from the navigation menu on top, then click the “Cleanup” button.



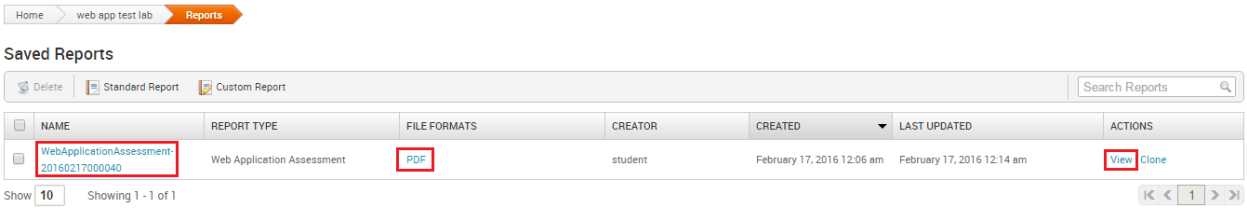
Leave boxes checked for both sessions and click “Cleanup Sessions”. In a few seconds, sessions will be closed.

Exercise 3 – Viewing the Report

By default, Metasploit Pro creates a report as part of the Web App Test Quick Start Wizard. We can view the generated report by selecting Reports->Show Reports from the navigation menu on top.



We will look into creating a different types of reports later, for now just click on the report name, file format, or the “View” link to view it.



Look through the report. You can see that it references OWASP Top 10 list.

OWASP 2013 Top 10 Web Application Security Risk Summary - Failures

A1 - Injection	Injection flaws, such as SQL, OS, and LDAP injection occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing unauthorized data.

Which sections would you customize if you could?

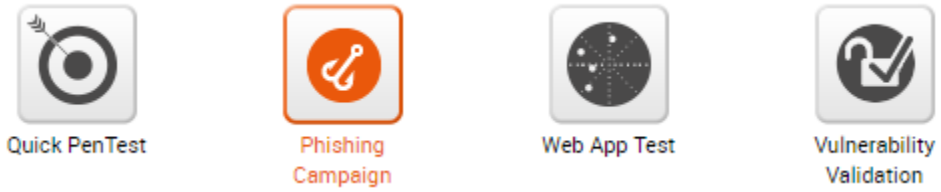
End of Lab

Lab 6 - Phishing Campaign

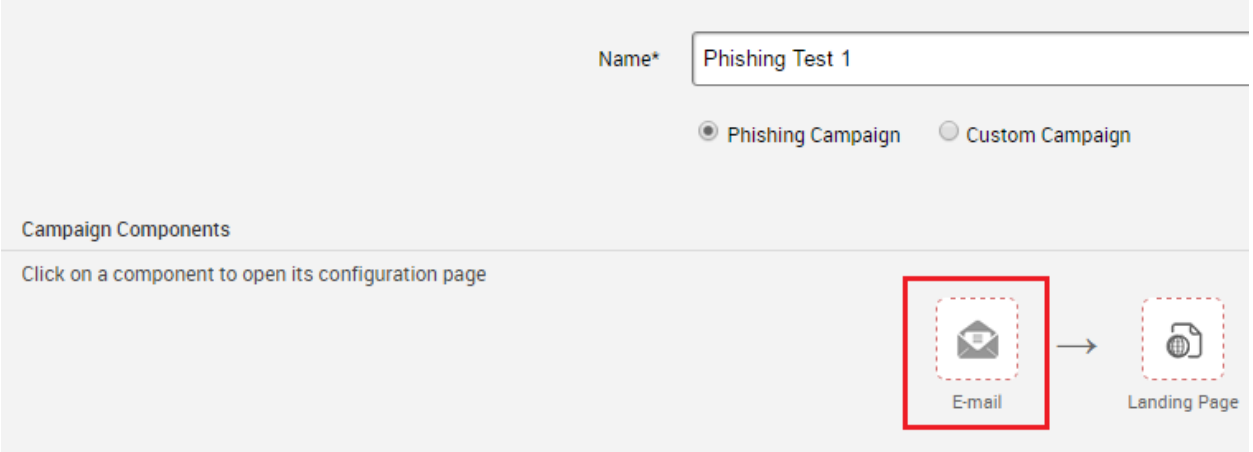
Exercise 1 – Setting Up a Campaign

So far we've talked about using Metasploit Pro to exploit OS vulnerabilities and Web application vulnerabilities. In this lab, we will see how Metasploit Pro can be used to exploit the weakest link in information security systems – the human factor. Metasploit Pro has a feature for performing one of the most effective social engineering attacks – phishing.

Go to Metasploit Pro Home page and select the Phishing Campaign Quick Start Wizard[8].



Name your project "phishing lab" and click "Next". The campaign configuration page will open. Let's name our campaign "Phishing Test 1". Now click on the E-mail icon in the Campaign Components section.



This is where we conjure our "bait" – the phishing email message. Let's make this email look like an urgent message to a Juggy Bank customer. Change the header entries so they look like the image below.

[8] Note that you can create a phishing campaign as a task in an existing project by selecting Campaigns from the navigation menu.

Configure E-mail Header

Subject	URGENT: Suspisious account activity detected
From address	security@juggybank.com
From name	Juggy Bank Secuity

Next, we need to choose a Target List. We haven't created any email lists yet, so click on the dropdown and select "Create a new Target List". When the "New Target List" dialog opens, name our list "email list 1". Note that there is an option to import a list. Then add a target manually, using the same email address we used in the SET Attack lab earlier: jsmith@infoseclocal.com.

New Target List

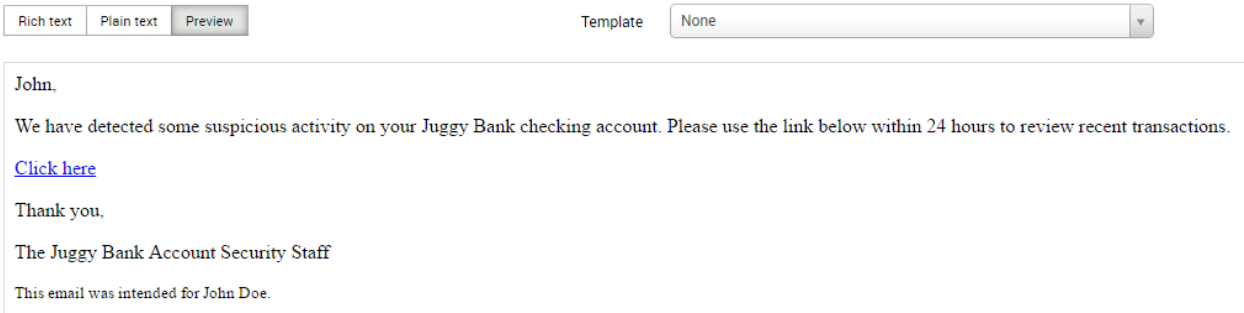
List Name*	email list 1
Import Target List (CSV format)	Choose File No file chosen

Manually Add Targets:

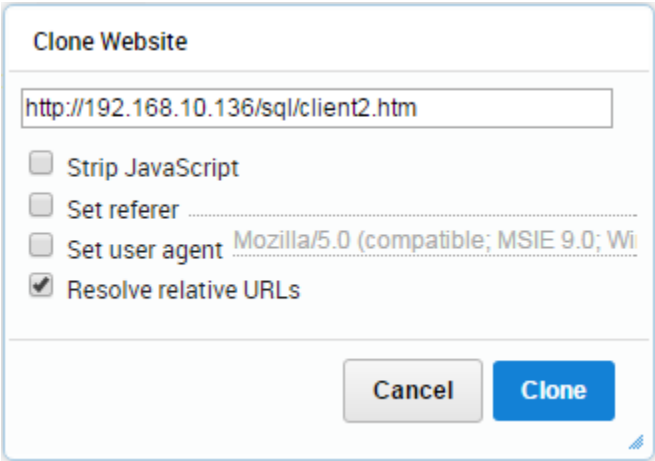
jsmith@infoseclocal.com	John	Smith

Submit

Click "Submit". Our target list is added now. Click "Next" (you may need to scroll down to see the button) to move on to configuring the email content. If you want, modify the message text to make it look somewhat like a real bank notification. Click "Preview" button to see what your message will look like to a recipient. Note that there is an option to select a template. We will look at templates later.

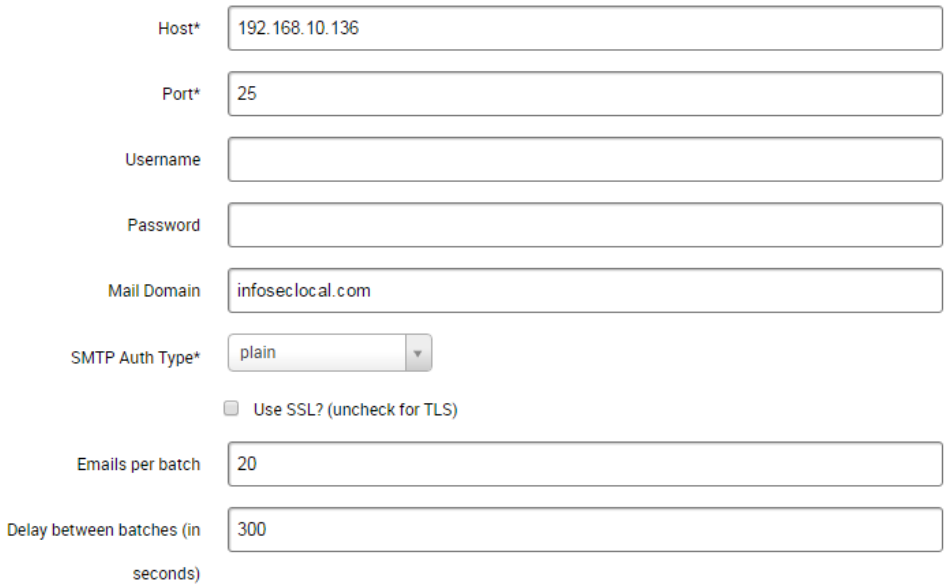


When you are satisfied with the content, click “Save”. We are back to the campaign configuration page. Notice that the E-mail icon has a solid outline now, meaning that this component has been configured. Click on the “Landing Page” icon. We can see that we can configure a path for our landing page, and have an option to either redirect to a custom URL or to the Campaign Redirect Page. Let’s leave all settings at default here and click “Next”. On the Content page we have options of using a pre-configured landing page, modify the HTML code, choosing a saved template, or cloning a website. Let’s clone our Juggy Bank login page! Click the “Clone Website” button. In the configuration dialog enter the Juggy Bank URL (using your Windows Server 2012 R2 VM IP address): http://192.168.x.x/sql/client2.htm, and click “Clone”.

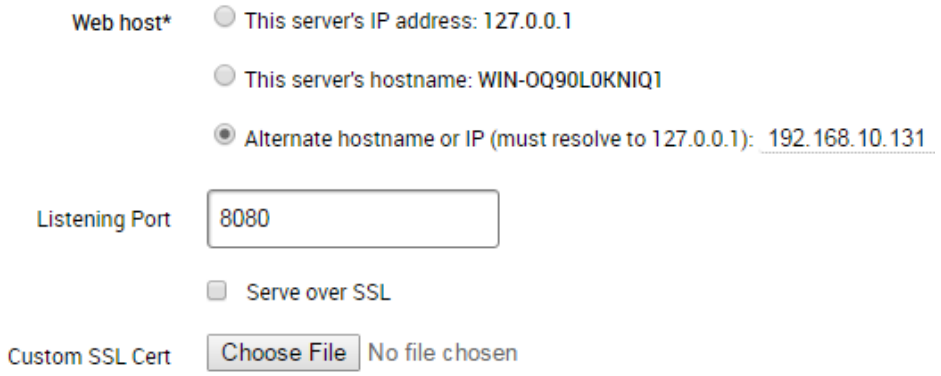


Now, if we click “Preview”, we will see that our landing page looks identical to the Juggy Bank login page.

Click “Save”. One last step for the Campaign Components: the Redirect Page. Click on the icon, then click “Next” and “Save” to accept the default settings. Now select the “E-mail Server” icon in the Server Configuration section. Enter the Windows Server 2012 R2 VM IP address for “Host”, and change “Mail Domain” to **infoseclocal.com**.



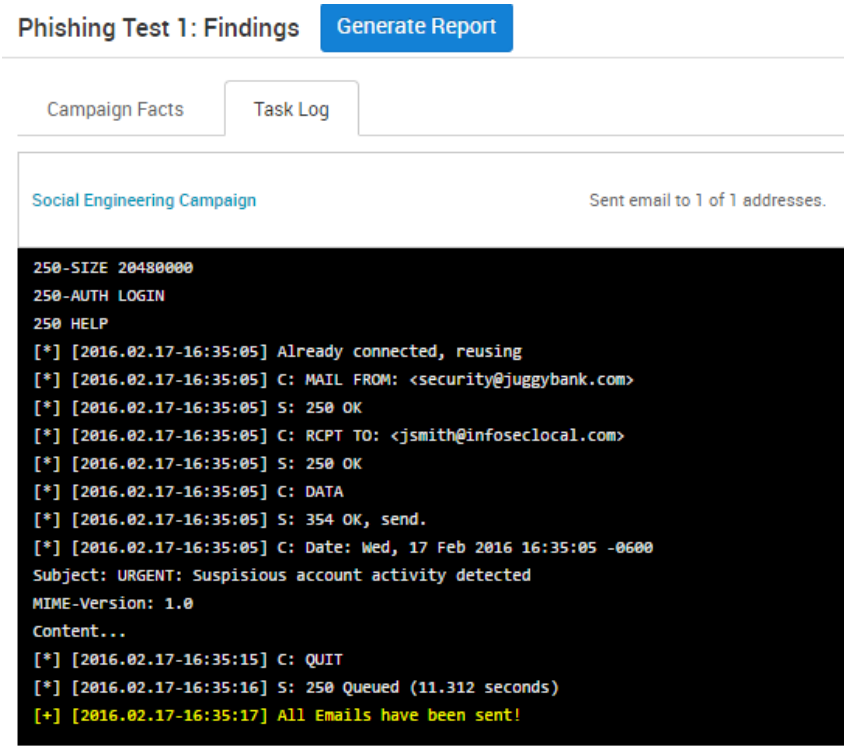
Click “Save”. The last thing we need to configure is the Web Server. Click the “Web Server” icon. Change the selection for “Web host” to “Alternative hostname or IP” and enter the IP address of your Metasploit Pro VM.



Click “Save”. We are ready to launch our phishing campaign.

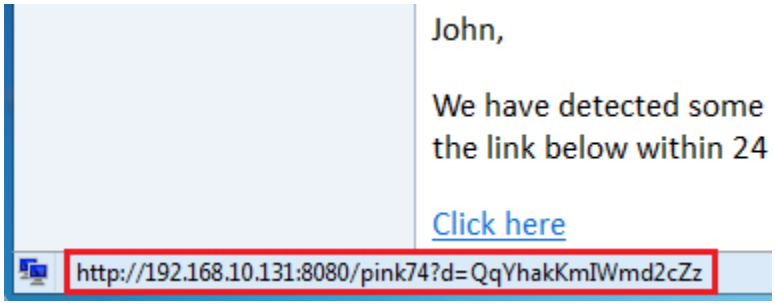
Exercise 2 – Running and Managing Campaigns

To run our newly configured campaign, click the “Launch Campaign” button. Click “OK” to confirm. It will take about half a minute for the email to be sent. You can check the progress by switching to the “Task Log” tab.



Now let's play the role of a security unaware employee and open the phishing email. On your Metasploit Pro VM, open the Thunderbird email client by double-clicking the desktop shortcut icon.

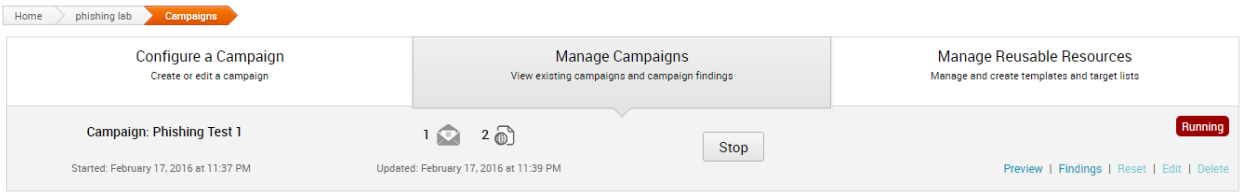
You should see our message in the Inbox (allow a few seconds for it to load). If you hover over the "malicious" link, you will see that it does, in fact, point to our landing page.



Click the link in the email. Our fake Juggy Bank login page should open in the browser. Enter some credentials and click "Submit". You should see the Warning message displayed on our redirect page. Go back to the Metasploit Pro VM. In your Task Log you should now see some output similar to the image below.

```
[*] [2016.02.17-17:17:38] 192.168.10.139   web_phish - Hook: pro/social_engineering/web_phish - 192.168.10.139:49170
[+] [2016.02.17-17:17:38] 192.168.10.139   web_phish - Request is of type :tracking_request -- set cookie and redirect
[*] [2016.02.17-17:17:39] 192.168.10.139   web_phish - Hook: pro/social_engineering/web_phish - 192.168.10.139:49170
[*] [2016.02.17-17:17:39] 192.168.10.139   web_phish - This human target is already tracked
[*] [2016.02.17-17:18:47] 192.168.10.139   web_phish - Hook: pro/social_engineering/web_phish - 192.168.10.139:49175
[*] [2016.02.17-17:18:47] 192.168.10.139   web_phish - POST request with data from 192.168.10.139
[*] [2016.02.17-17:18:47] 192.168.10.139   web_phish - Sending redirect to http://192.168.10.131:8080/yellow26
[*] [2016.02.17-17:18:47] 192.168.10.139   web_phish - Hook: pro/social_engineering/web_phish - 192.168.10.139:49175
[*] [2016.02.17-17:18:47] 192.168.10.139   web_phish - This human target is already tracked
```

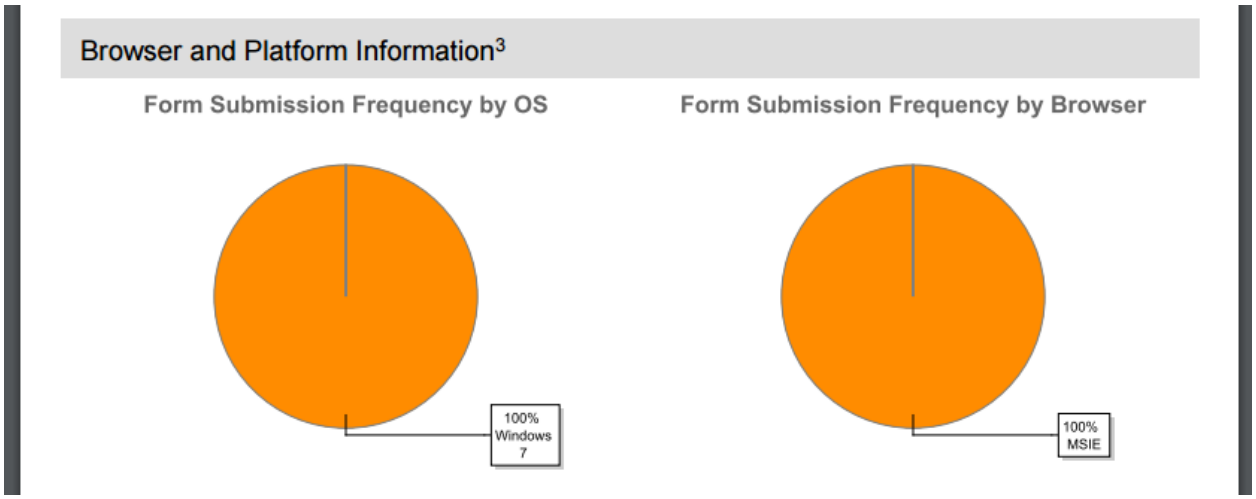
Click "Done". We are now redirected to the Manage Campaign section, where we can see our Phishing Test 1 campaign labeled as "Running".



Note that we can Preview our campaign (view the phishing email and landing and redirect pages) or view Findings, but cannot Reset, Edit, or Delete the campaign while it's running. Click the "Stop" button. The campaign is now labeled as "Finished" and the Reset, Edit, and Delete options are now available.

Exercise 3 – Generating Reports

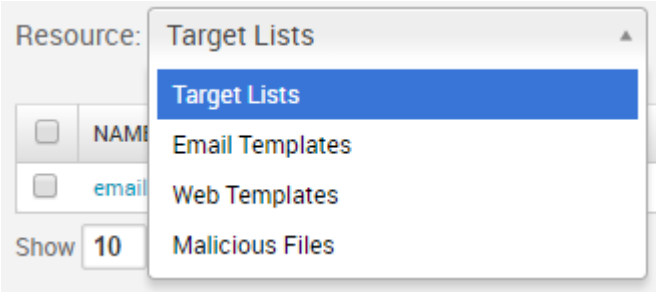
We can get some information about campaign results from viewing the Findings, but what we really want to do here is generate a report. Click the Findings link and then select the blue "Generate Report" button. On the New Report page, look through the available options, note that we can upload a custom logo, replace email addresses with target IDs, and email the report directly from within Metasploit. Leave all settings as default and click "Generate Report". Wait a few seconds for the report to be created, the Reports page will reload a few times before showing the result. Again, we can click on the name, file format, or the "View" link to view the report.



Look through the report. How would you customize it?

Exercise 4 – Managing Reusable Resources

Finally, let's switch to the Manage Reusable Resources section of the Campaigns page and see what we can do here. There are for categories of resources that we can manage: Target Lists, Email Templates, Web Templates, and Malicious Files.



Look at each category to see what options are available. After you build a library of reusable resources, you can make the process of creating new phishing campaigns more efficient.

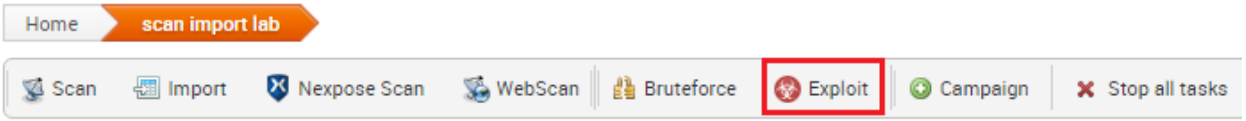
End of Lab

Lab 7 - Exploits and Payloads

Exercise 1 – Automated and Manual Exploits

We've already seen how Metasploit Pro can automate the process of finding and executing exploits. In this lab we will take a quick look at Automated exploits and then will go through the process of performing a Manual exploit.

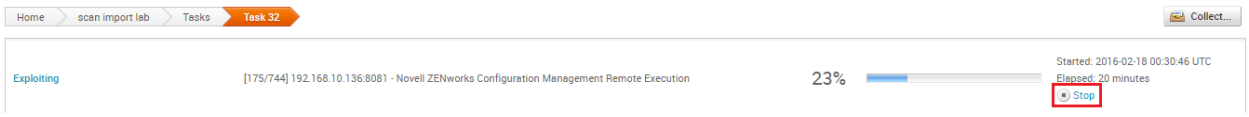
We will go back to our "scan import lab" project for this Exercise. Go to the Metasploit Pro Home page and select it from the Project Listing. Once at the Project Overview page, select "Exploit" from the top menu bar.



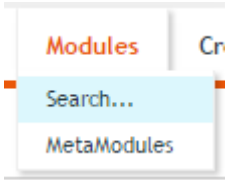
Modify the Target Addresses so the field only contains the actual IP address of your Windows Server 2012 R2 VM. Look through the Advanced Options and click "Exploit". Metasploit will now select exploits with minimum reliability of "Great" (default setting) based on vulnerabilities and services/ports identified for the target. Observe the Task output as it runs to see which exploits Metasploit is attempting to run. In the example below we can see that Metasploit selected 744 (!) exploits to try against the target.

```
[*] [2016.02.17-18:30:46] Minimum rank: great, transport evasion level: 0, application evasion level: 0
[*] [2016.02.17-18:30:46] Target hosts: 192.168.10.136
[+] [2016.02.17-18:30:47] Workspace:scan import lab Progress:1/100 (1%) Starting analysis
[+] [2016.02.17-18:30:47] Workspace:scan import lab Progress:2/100 (2%) Analyzing exploits: filtering by vulnerability, port
[+] [2016.02.17-18:30:51] Workspace:scan import lab Progress:3/100 (3%) Building exploit map: matching by vulnerability, port
[*] [2016.02.17-18:30:51] Matching exploits: 0 hosts processed (0 potential actions)
[+] [2016.02.17-18:30:52] Workspace:scan import lab Progress:4/100 (4%) Building attack plan
[*] [2016.02.17-18:30:52] Finalizing attack plan: 744 total exploits
[+] [2016.02.17-18:30:52] Workspace:scan import lab Progress:5/749 (0%) [1/744] 192.168.10.136:445 - Samba "username map script" Command Execution
```

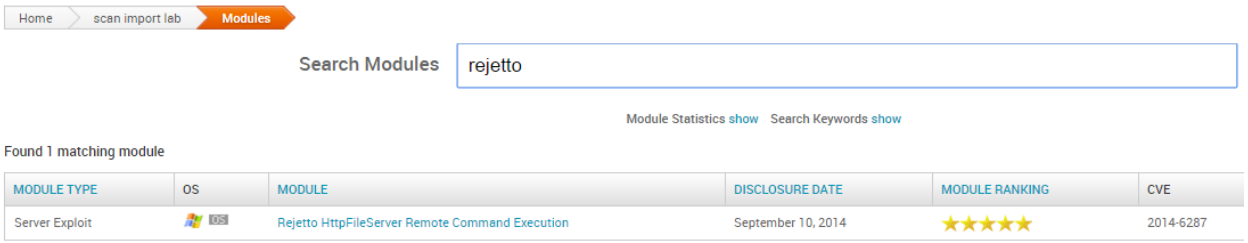
Let the task run for a little while. You will see that despite trying tons of exploits, Metasploit failed to open a single session. Such approach may work in some pentesting scenarios, but in most cases we would want something more effective (and probably a bit more stealthy as well). Click "Stop" to terminate the automated exploit task, and "OK" to confirm.



Naturally, we can select and run a specific exploit in Metasploit Pro, just as we did in Metasploit Framework, only with less typing and more mouse clicking. From the top navigation menu, select Modules->Search.



Lets' run our trusted Rejetto exploit. Enter **rejetto** into the "Search Modules" field.

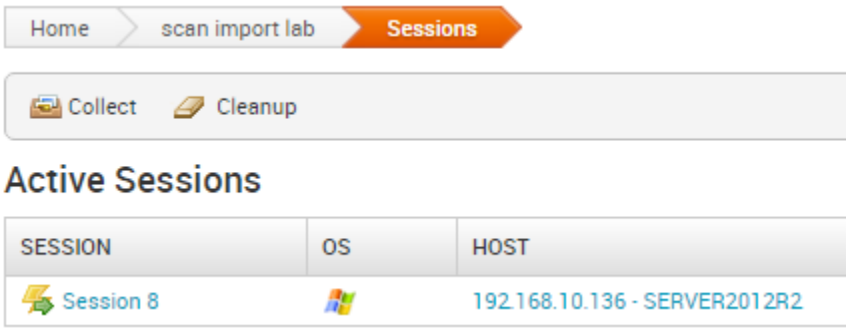


Click on the module name. On the configuration page, enter the IP address of our Windows Server 2012 R2 VM as the target address, un-check the DynamicStager box (we know that there's no AV program running on the target, so this would just save us some time), and change the RPORT value to **8081**. Then click the "Run Module" button. The task should take less than a minute to complete.

```
[+] [2016.02.17-19:01:03] Workspace:scan import lab Progress:1/2 (50%) Exploiting 192.168.10.136
[*] [2016.02.17-19:01:06] Started reverse TCP handler on 0.0.0.0:1024
[*] [2016.02.17-19:01:06] Using URL: http://0.0.0.0:8080/bMVj4CktBHjyN
[*] [2016.02.17-19:01:06] Local IP: http://127.0.0.1:8080/bMVj4CktBHjyN
[*] [2016.02.17-19:01:06] Server started.
[*] [2016.02.17-19:01:06] Sending a malicious request to /
[*] [2016.02.17-19:01:16] 192.168.10.136   rejetto_hfs_exec - 192.168.10.136:8081 - Payload request received: /bMVj4CktBHjyN
[*] [2016.02.17-19:01:19] Server stopped.
[!] [2016.02.17-19:01:19] This exploit may require manual cleanup of '%TEMP%\CSYWChPS.vbs' on the target
[+] [2016.02.17-19:01:19] Workspace:scan import lab Progress:2/2 (100%) Complete (0 sessions opened) exploit/windows/http/rejetto_hfs_exec
```

You may see that despite the "0 session opened" message, a number 1 appears next to the Sessions tab in the navigation menu.

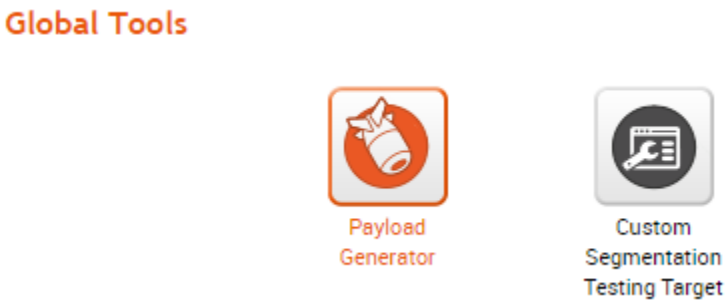
If we click on Sessions, we will see that there is, indeed, an active Meterpreter session we can use.



You can connect to this session if you want, or just select “Cleanup” to close it.

Exercise 2 – Generating Payloads

Next we will look at the Payload Generator tool provided by Metasploit Pro. To use it, click the icon on the Home page, in the Global Tools section.



When the Payload Generator window opens, let’s change the selection to “Classic Payload” first. Enter the Metasploit Pro VM IP address for “LHOST”, leave the rest of the settings unchanged, and click “Generate”.

Payload Generator Classic Payload Dynamic Payload (AV evasion)

Builds a customized payload. (All platforms)

Payload Options

Encoding

Output Options

Platform: Windows

Architecture: x86

Stager: reverse_tcp

Stage: windows/meterpreter

LHOST*: 192.168.10.131

LPORT*: 4444

EXITFUNC*: Process

Added Shellcode: No file selected Choose File...

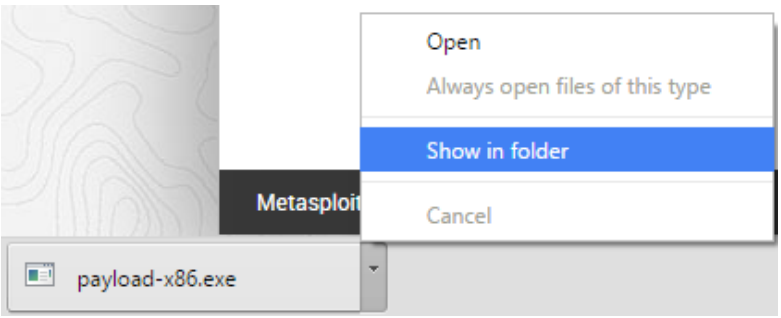
Size of NOP sled: (bytes)

Advanced

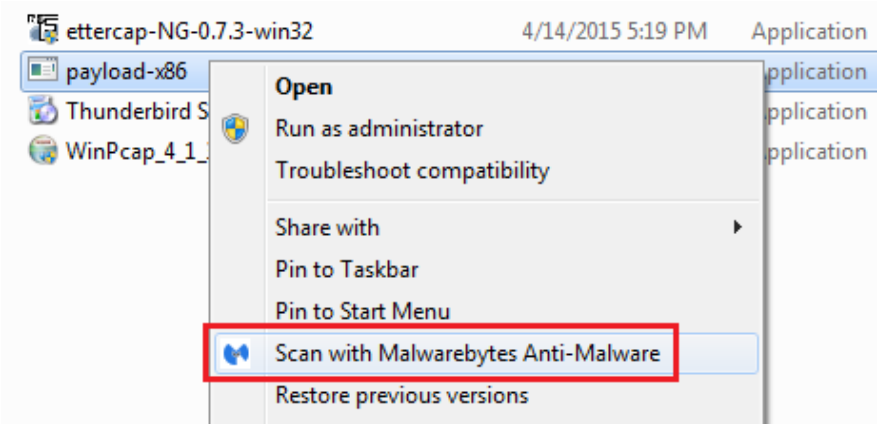
Cancel Generate

When the “Payload generated” dialog appears, click “Download”. Chrome will download the file to default location (/Downloads folder). Next, launch Malwarebytes, a popular anti-malware program, from the desktop shortcut.

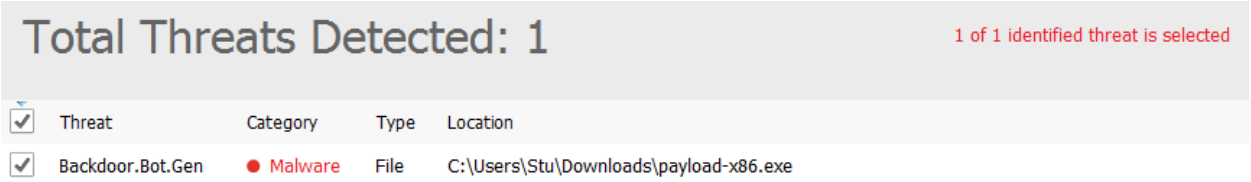
Once Malwarebytes has started, go back to the browser, find your downloaded payload executable, click the little arrow on the right and select “Show in folder” (alternatively you can just browse to the file with Windows Explorer).



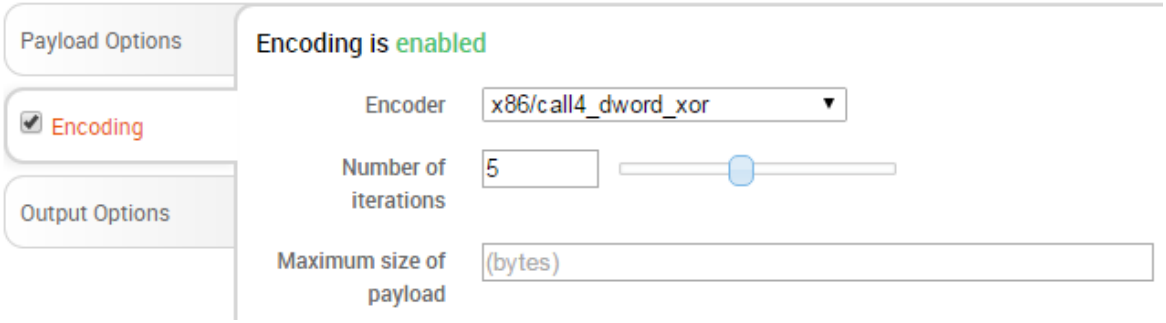
Right-click the file and select “Scan with Malwarebytes Anti-Malware”.



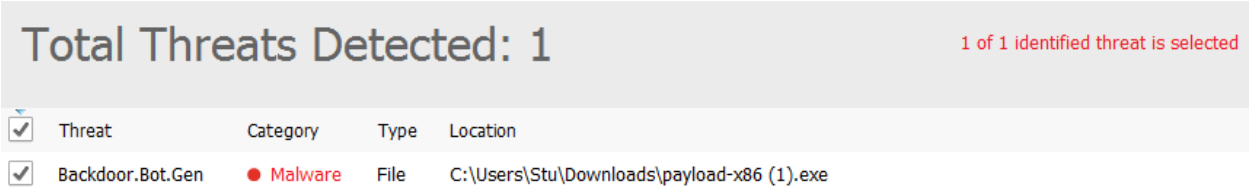
Malwarebytes will identify our payload as malware.



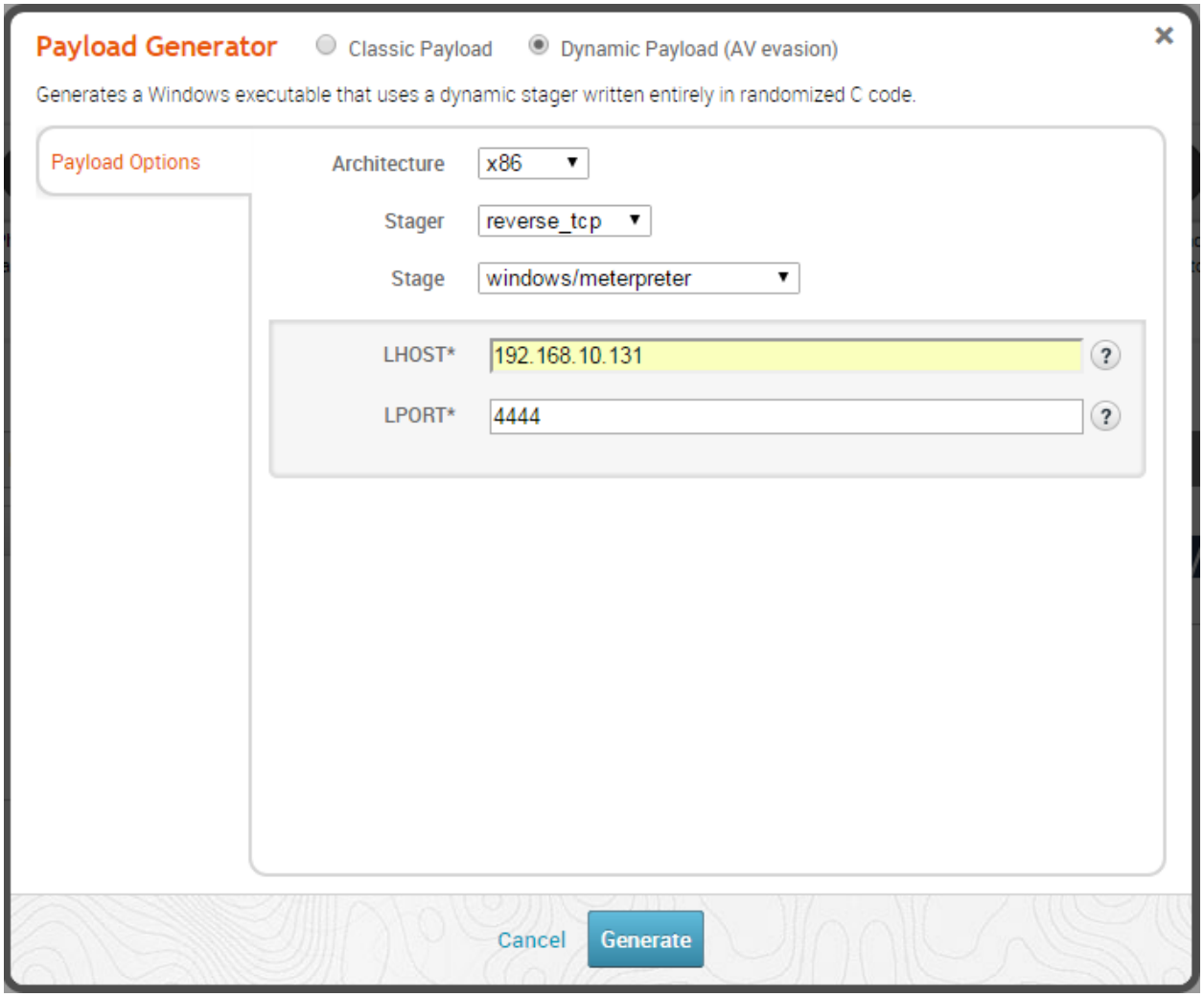
Now go back to Metasploit Pro Payload Generator and create another Classic Payload, this time selecting a different encoder in the Encoding options, and increasing the number of iterations.



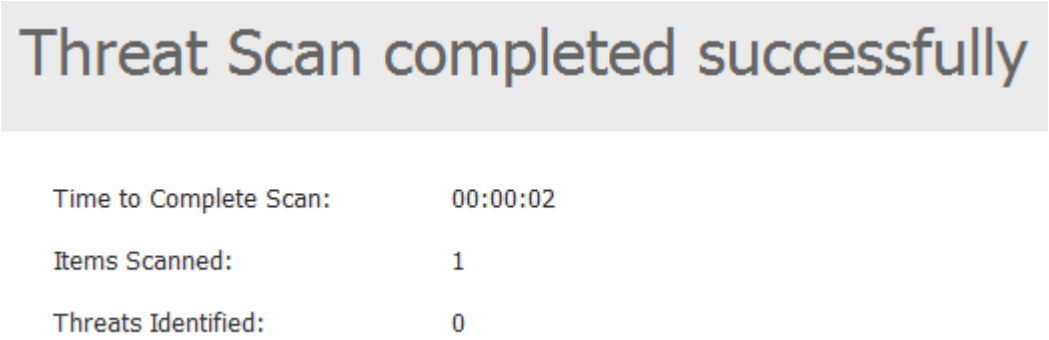
Generate the payload, download it, and scan with Malwarebytes. Looks like changing the Encoding settings didn't help much.



Well, let's see if Dynamic Payload really provides AV evasion as it claims. Open Payload Generator again, leave Dynamic Payload selected this time, enter the "LHOST" value and click "Generate".



Download the new payload file and scan it with Malwarebytes. No threats will be identified this time[9].



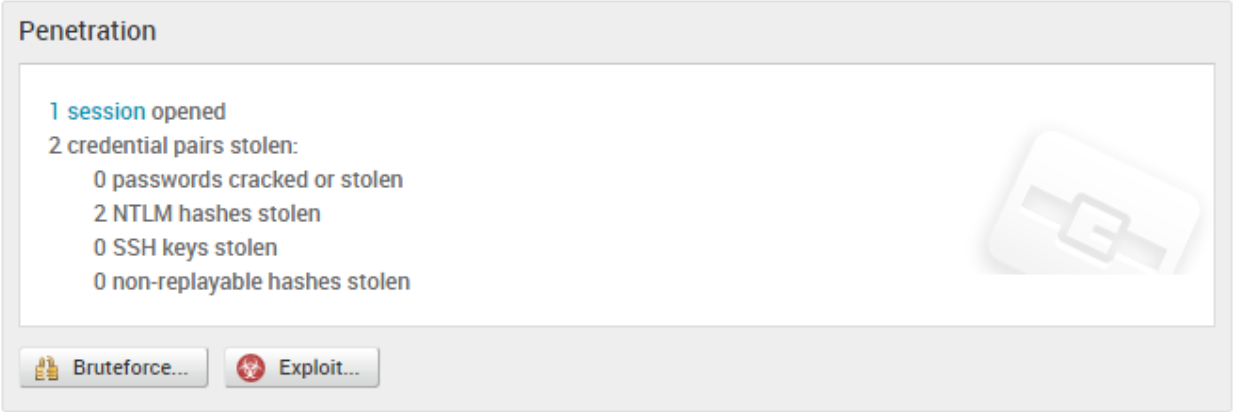
End of Lab

[9] In our Advanced Ethical Hacking course we learn how to create such undetectable payloads.

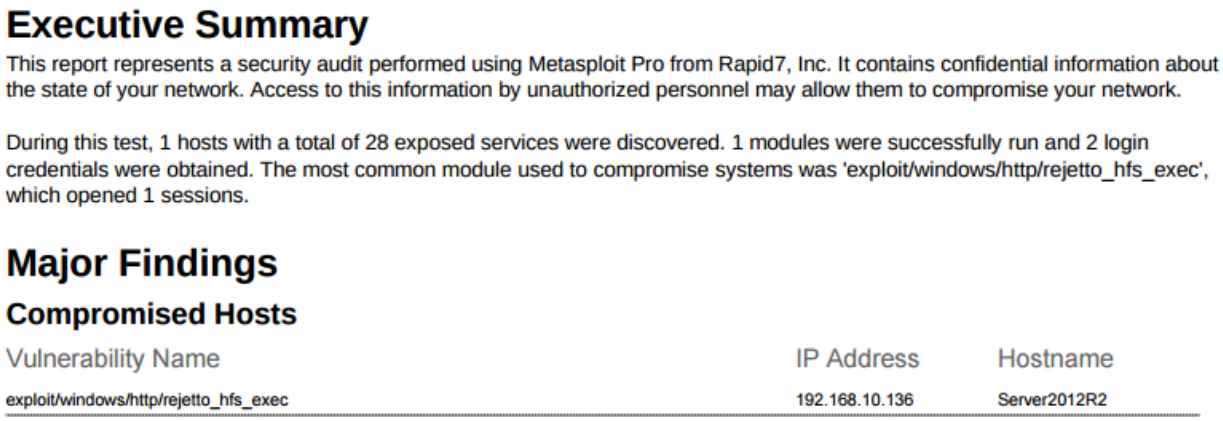
Lab 8 - Reporting

Exercise 1 – Creating Standard Reports

Now we can finally go back to our first project, “quick pentest lab”, and see how effective it was. Select the project from the Project Listing on the Metasploit Home page. Look at the Overview. Looks like we had some success here: opened a session and stole some credentials.



There was also a report created for the project. If we look through the report, we will see that the Quick PenTest ended up using the Rejetto HFS exploit to penetrate the system.



Executive Summary

This report represents a security audit performed using Metasploit Pro from Rapid7, Inc. It contains confidential information about the state of your network. Access to this information by unauthorized personnel may allow them to compromise your network.

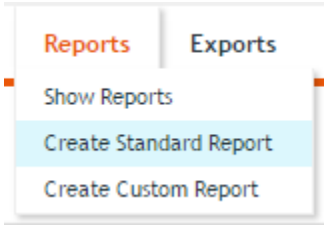
During this test, 1 hosts with a total of 28 exposed services were discovered. 1 modules were successfully run and 2 login credentials were obtained. The most common module used to compromise systems was 'exploit/windows/http/rejetto_hfs_exec', which opened 1 sessions.

Major Findings

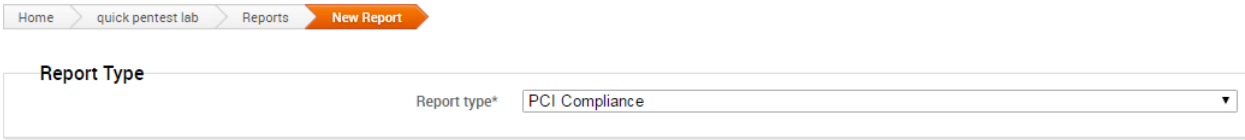
Compromised Hosts

Vulnerability Name	IP Address	Hostname
exploit/windows/http/rejetto_hfs_exec	192.168.10.136	Server2012R2

To create Custom Reports, custom report templates should be uploaded first. We won’t do it in this lab, instead, we will look at different types of Standard Reports we can generate with Metasploit Pro. Select Reports->Create Standard Report from the navigation menu on top.



By default, Metasploit Pro generates Audit reports. Let's change the Type to something different, such as PCI Compliance.



Feel free to modify some other settings. Click "Generate Report" when you're done. Wait for the new report to appear on the list, it will take a few seconds. View the report. As you can see, Metasploit Pro broke down the findings according to specific PCI Requirements, and determined whether these requirements were met.

Requirements Status Summary

PCI Requirement	Result
2.2.1	**FAIL**
2.3	**PASS**
6.1	**FAIL**
8.2	**PASS**
8.4	**PASS**
8.5.8	**PASS**
8.5.10	**PASS**
8.5.11	**PASS**

Hosts Status Summary

Host	Test status
192.168.10.136 (Server2012R2)	FAIL

Detailed information about each of the listed requirements with reasons for failure is also provided.

PCI Requirement 6.1

FAIL

Description: Ensure that all system components and software have the latest vendor-supplied security patches installed. Deploy critical patches within a month of release.

Results: The following hosts failed to satisfy this requirement.

Host: 192.168.10.136 (Server2012R2) OS: Windows 2012 R2 Standard

Successful Exploits:

Vulnerability	Metasploit module	Exploited on
Rejetto HttpFileServer Remote Command Execution	exploit/windows/http/rejetto_hfs_exec	2016-02-17 07:02:14 UTC

Feel free to generate other types of reports and compare the contents. You can see that even with standard options, Metasploit Pro offers a lot of flexibility for reporting, which will help in meeting some specific objectives of your pentesting activities.

End of Lab