Assignment #3 (28th Dec 2020)

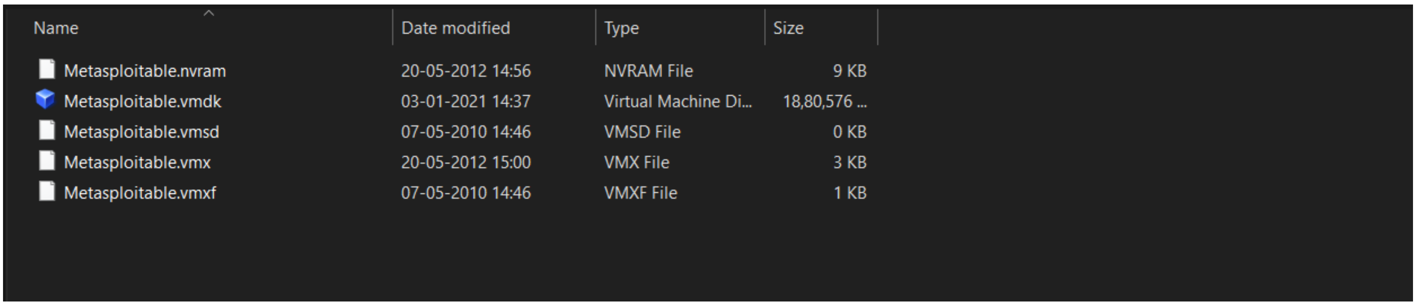
Metasploitable 2 Exploitability

The Metasploitable virtual machine is an intentionally vulnerable version of Ubuntu Linux designed for testing security tools and demonstrating common vulnerabilities. Version 2 of this virtual machine is available for download and ships with even more vulnerabilities than the original image. This virtual machine is compatible with *VMWare*, *VirtualBox*, and other common virtualization platforms. By default, Metasploitable's network interfaces are bound to the NAT and Host-only network adapters, and the image should never be exposed to a hostile network.

Metasploitable 2 is available at:

- https://information.rapid7.com/metasploitable-download.html
- https://sourceforge.net/projects/metasploitable/

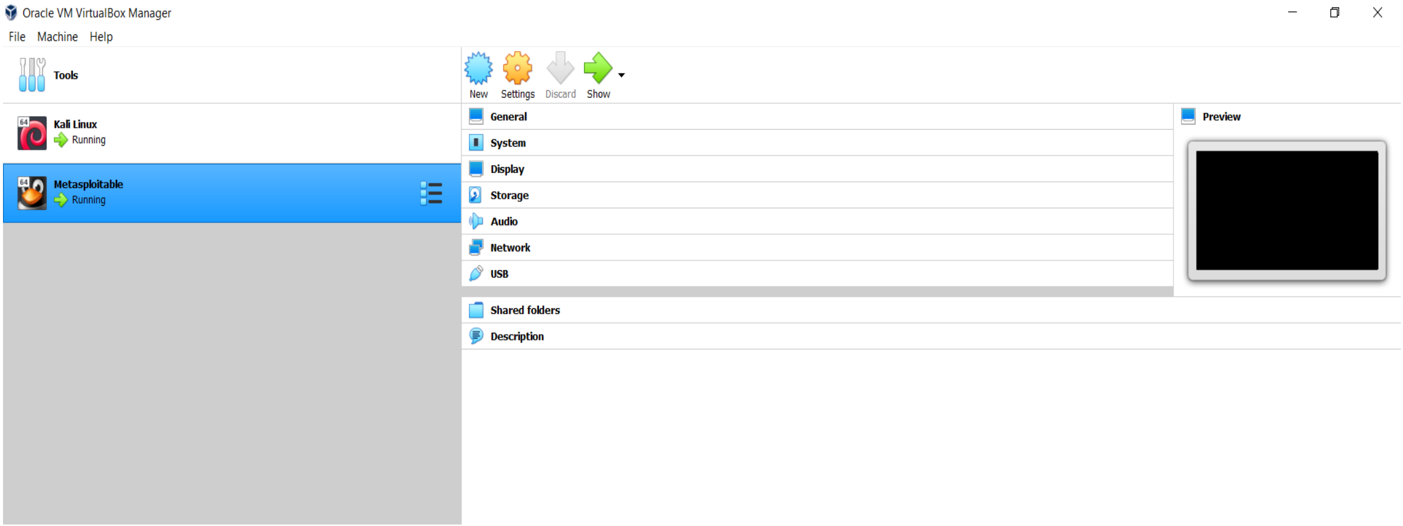
The compressed file is about 800 MB and can take up to 30 minutes to download. After you have downloaded the Metasploitable 2 file, you will need to unzip the file to see its contents.



Name	Date modified	Type	Size
Metasploitable.nvram	20-05-2012 14:56	NVRAM File	9 KB
Metasploitable.vmdk	03-01-2021 14:37	Virtual Machine Di...	18,80,576 ...
Metasploitable.vmsd	07-05-2010 14:46	VMSD File	0 KB
Metasploitable.vmx	20-05-2012 15:00	VMX File	3 KB
Metasploitable.vmxf	07-05-2010 14:46	VMXF File	1 KB

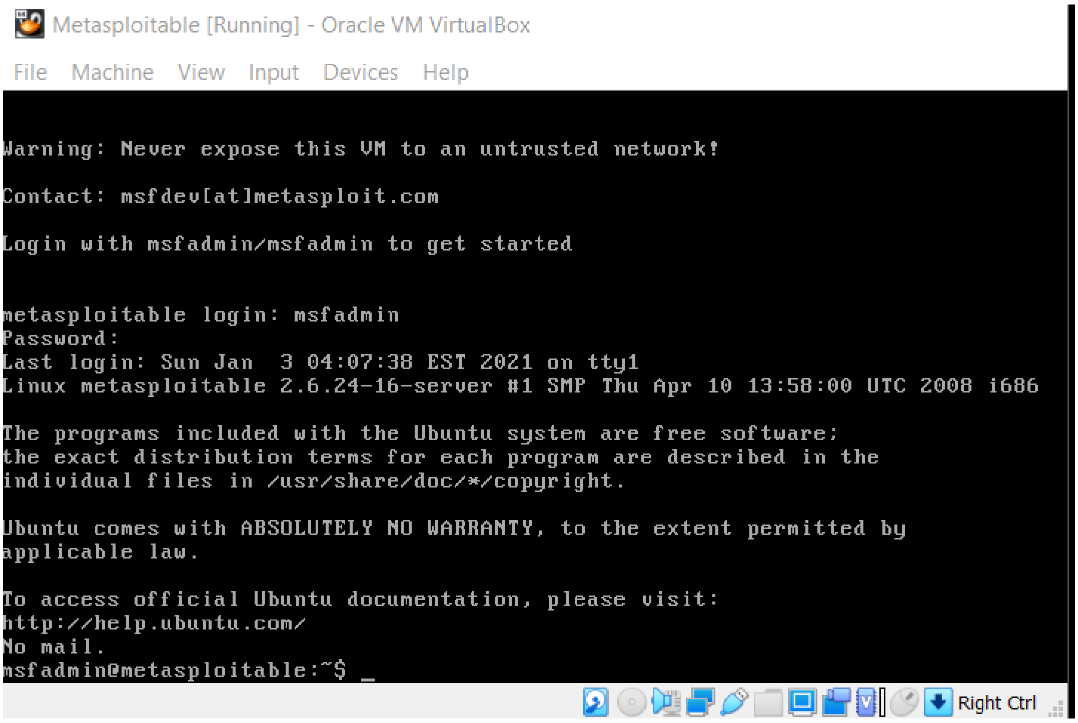
Powering on Metasploitable 2

Once the VM is available on your desktop, open the device, and run it with VMWare or VirtualBox.



Logging in to Metasploitable 2

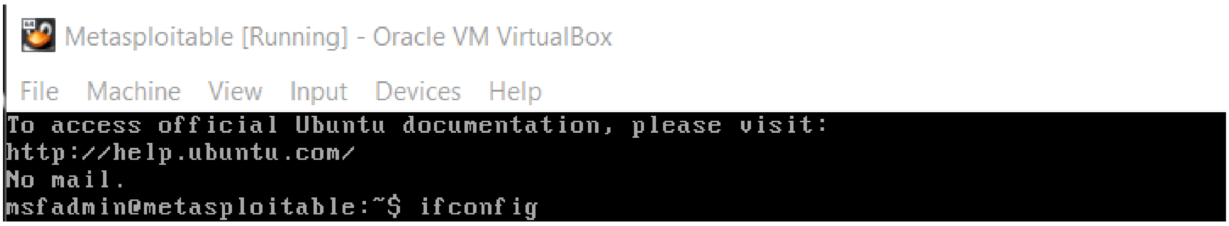
After the virtual machine boots, login to console with username msfadmin and password msfadmin.



```
Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: msfadmin
Password:
Last login: Sun Jan  3 04:07:38 EST 2021 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ _
```

Getting Started

From the shell, run the ifconfig command to identify the IP address. Services



```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
```

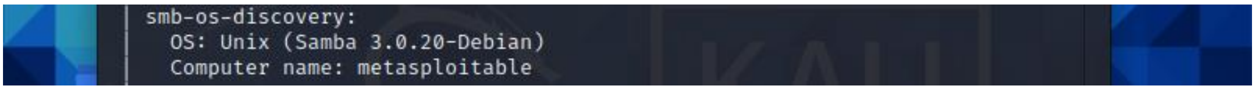
From our attack system (Linux, preferably something like Kali Linux), we will identify the open network services on this virtual machine using the Nmap Security Scanner.

CMD: nmap –A IP_Address

Gather following information:

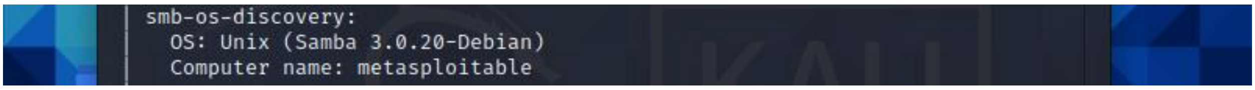
· The IP address : **find yours**

· The host name : metasploitable



```
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
```

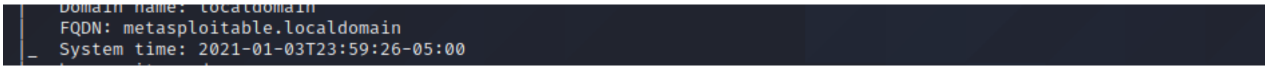
· The operating system : Unix (Samba 3.0.20-Debian)



```
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
```

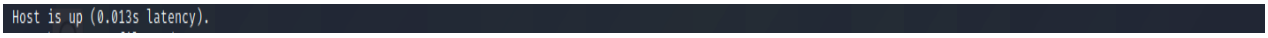
· The active services :

· The timestamp of the host :



```
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2021-01-03T23:59:26-05:00
```

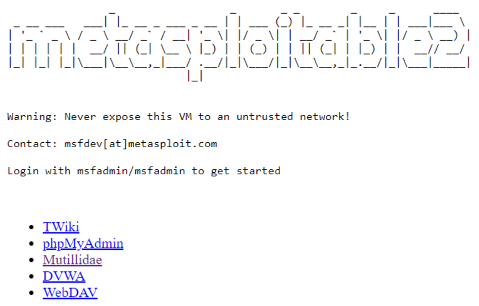
· The host status: Host is up (0.018s latency):



```
Host is up (0.013s latency).
```

Vulnerable Web Services

Metasploitable 2 has deliberately vulnerable web applications pre-installed. The web server starts automatically when Metasploitable 2 is booted. To access the web applications, open a web browser and enter the URL http://<IP> where <IP> is the IP address of Metasploitable 2. One way to accomplish this is to install Metasploitable 2 as a guest operating system in Virtual Box and change the network interface settings from "NAT" to "Host Only". For example, Metasploitable 2 is running at IP 192.168.56.101. Browsing to http://192.168.56.101/ shows the web application home page.



Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

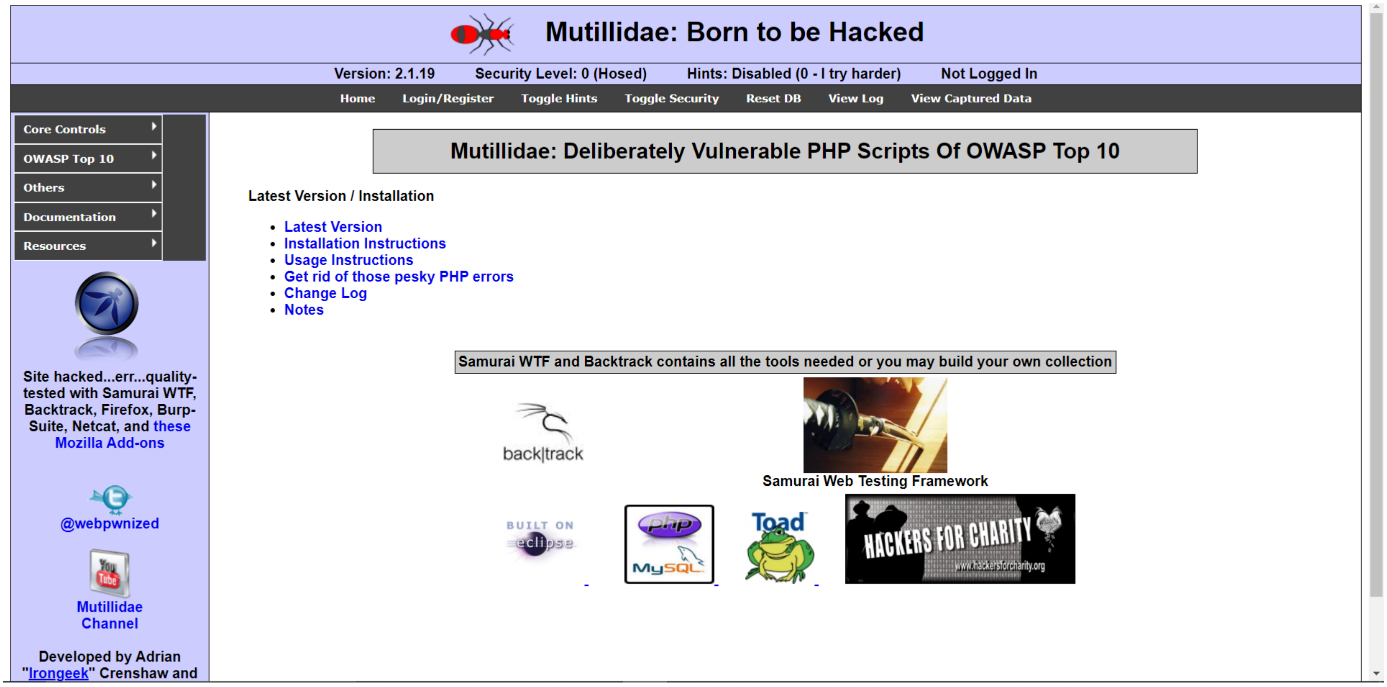
- TWiki
- phpMyAdmin
- Mutillidae
- DVWA
- WebDAV

To access a particular web application, click on one of the links provided. Individual web applications may additionally be accessed by appending the application directory name onto http://<IP> to create URL http://<IP>/<Application Folder>/. For example, the **Mutillidae** application may be accessed (for example) at address http://192.168.56.101/mutillidae/. The applications are installed in Metasploitable 2 in the /var/www directory. (Note: See a list with command ls /var/www.) In the current version as of this writing, the applications are

· mutillidae (NOWASP Mutillidae 2.1.19)
· dvwa (Damn Vulnerable Web Application)
· phpMyAdmin
· tikiwiki (TWiki)
· tikiwiki-old
· dav (WebDav)

1. Mutillidae

The Mutillidae web application (NOWASP (Mutillidae)) contains all of the vulnerabilities from the OWASP Top Ten plus a number of other vulnerabilities such as HTML-5 web storage, forms caching, and click-jacking. Inspired by DVWA, Mutillidae allows the user to change the "Security Level" from 0 (completely insecure) to 5 (secure). Additionally three levels of hints are provided ranging from "Level 0 - I try harder" (no hints) to "Level 2 - noob" (Maximum hints). If the application is damaged by user injections and hacks, clicking the "Reset DB" button resets the application to its original state. Enable hints in the application by click the **"Toggle Hints"** button on the menu bar.



Mutillidae: Born to be Hacked

Version: 2.1.19 Security Level: 0 (Hosed) Hints: Disabled (0 - I try harder) Not Logged In

Mutillidae: Deliberately Vulnerable PHP Scripts Of OWASP Top 10

Latest Version / Installation

- Latest Version
- Installation Instructions
- Usage Instructions
- Get rid of those pesky PHP errors
- Change Log
- Notes

Samurai WTF and Backtrack contains all the tools needed or you may build your own collection

Samurai Web Testing Framework

Site hacked...err...quality-tested with Samurai WTF, Backtrack, Firefox, Burp-Suite, Netcat, and these Mozilla Add-ons

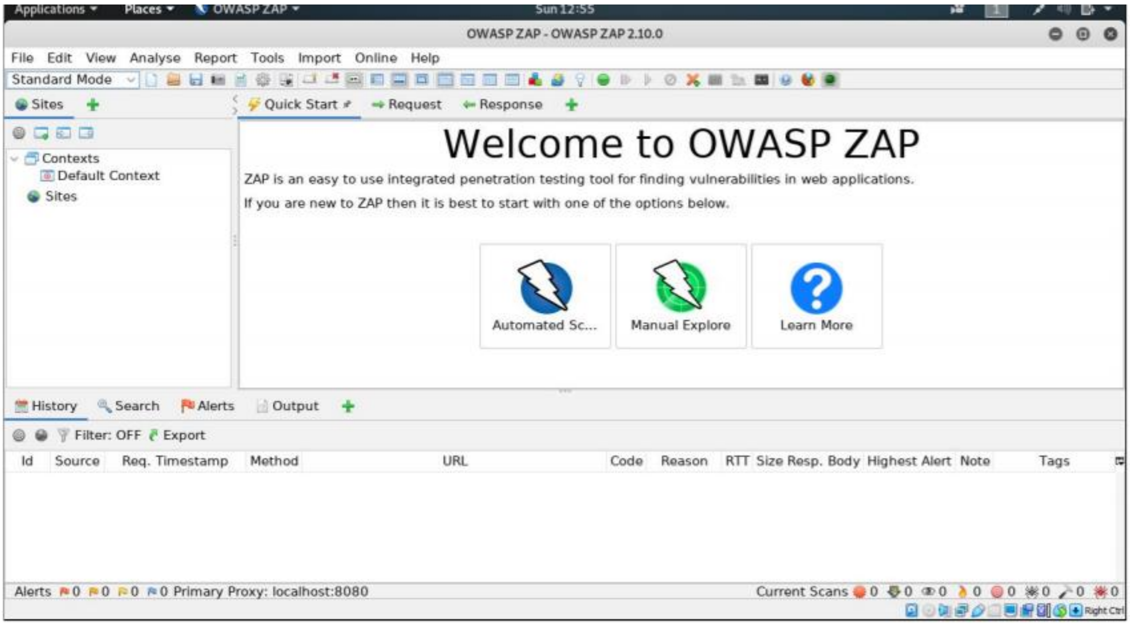
@webpwnized

Mutillidae Channel

Developed by Adrian "Irongeek" Crenshaw and

The Mutillidae application contains numerous vulnerabilities on these respective pages. You need to identify the web pages with following vulnerabilities using **ZAP** and/or **Nessus (**or any other tools **such as W3af, Wapiti etc.)**:

Using ZAP:



Welcome to OWASP ZAP

ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.

If you are new to ZAP then it is best to start with one of the options below.

** Steps to follow:

Start Automated Scan and also turn on ajax spider. In the link section put the multillidae link http://IP_address/mutillidae/ and start the scan.

Once the scan is over download the report in .json format and run the python script on that json file.

On running the script you will get an .txt file and you can find following answer in that file. **

i. SQL Injection on blog entry
ii. Cross-site request forgery
iii. JavaScript validation bypass
iv. XSS via referer HTTP header
v. Cross site scripting
vi. SQL injection
vii. JavaScript injection
viii. JSON injection
ix. Denial of Service if you fill up the log
x. Cascading style sheet injection xi. Any other known vulnerabilities

Attached File:

Result.txt: Contains all the urls.
