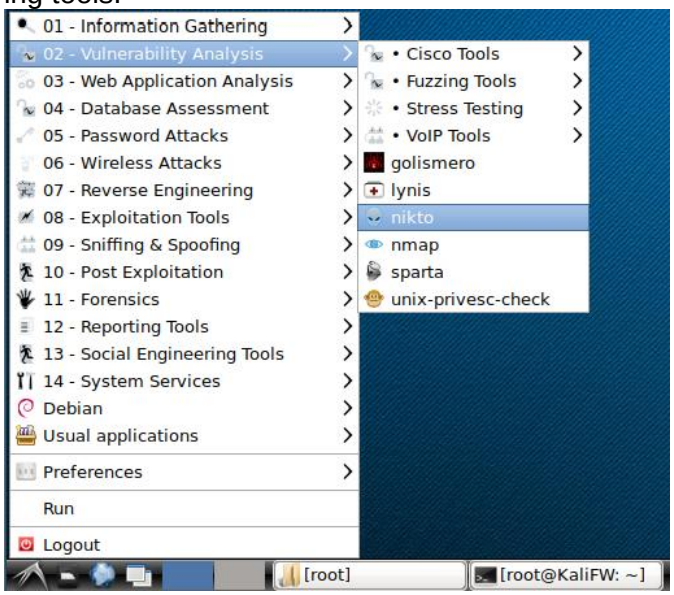
Lab5 – Pen Testing Example

Pen Testing

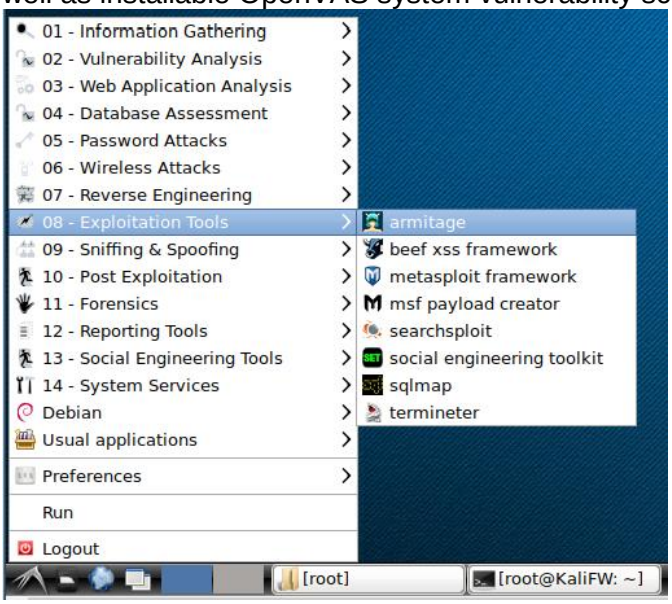
Penetration testing is a simulated attack aimed at identifying exploitable vulnerabilities of the system.
Pen testing involves the following stages: planning and reconnaissance (the scope and goals are defined, testing methods are picked, research is conducted); scanning and vulnerability detection (analysis of the system's state and code); gaining and maintaining access (exploiting detected vulnerability); report and analysis (compiling and assessing the collected data). There are also different pen testing methods, such as external and internal tests, blind tests (simulates and actual attack), double-blind tests (the security team is not notified of the upcoming attack), and targeted tests (cooperative work of the tester and the security team).

Kali Linux Pen Testing Tools

Kali Linux has a wide range of preinstalled and installable penetration testing tools.



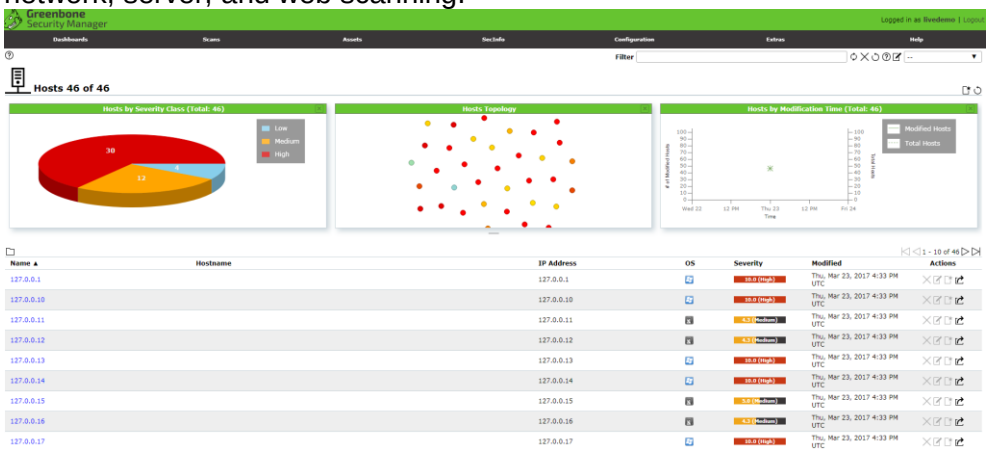
In this report I will cover the preinstalled Nikto web vulnerability scanner and Armitage cyber attack management GUI for Metasploit framework, as well as installable OpenVAS system vulnerability scanner.



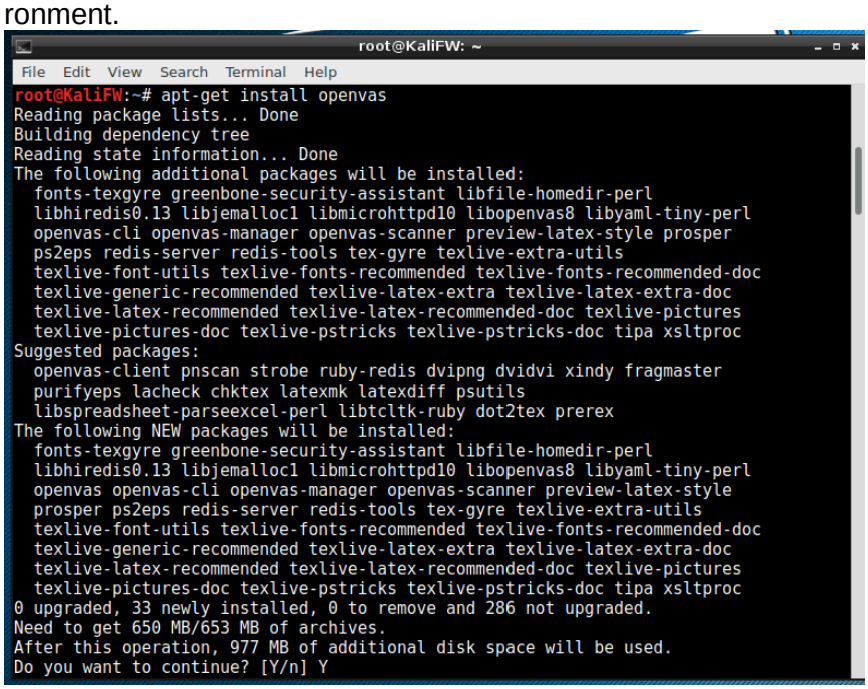
OpenVAS

Initially I have chosen the third-party OpenVAS software framework which deploys multiple vulnerability scanning and management tools that can be used for penetration testing. Since 2019, OpenVAS refers only to the scanner element of the Greenbone Security Manager architecture.

The functionality of the Greenbone applications includes scanning for security vulnerabilities, authenticated and unauthenticated testing, risk assessment reports, vulnerability alerts, and various customizable options for network, server, and web scanning.



Unfortunately, due to version incompatibility it was impossible to install the software on the Kali version that we are using as a part of the testing environment.



```
root@KaliFW: ~
File  Edit  View  Search  Terminal  Help
root@KaliFW:~# apt-get install openvas
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  fonts-texgyre greenbone-security-assistant libfile-homedir-perl
  libhiredis0.13 libjemalloc1 libmicrohttpd10 libopenvas8 libyaml-tiny-perl
  openvas-cli openvas-manager openvas-scanner preview-latex-style prosper
  ps2eps redis-server redis-tools tex-gyre texlive-extra-utils
  texlive-font-utils texlive-fonts-recommended texlive-fonts-recommended-doc
  texlive-generic-recommended texlive-latex-extra texlive-latex-extra-doc
  texlive-latex-recommended texlive-latex-recommended-doc texlive-pictures
  texlive-pictures-doc texlive-pstricks texlive-pstricks-doc tipa xsltproc
Suggested packages:
  openvas-client pnscan strobe ruby-redis dvipng dvidvi xindy fragmaster
  purifyeps lacheck chktex latexmk latexdiff psutils
  libspreadsheet-parseexcel-perl libtcltk-ruby dot2tex prerex
The following NEW packages will be installed:
  fonts-texgyre greenbone-security-assistant libfile-homedir-perl
  libhiredis0.13 libjemalloc1 libmicrohttpd10 libopenvas8 libyaml-tiny-perl
  openvas openvas-cli openvas-manager openvas-scanner preview-latex-style
  prosper ps2eps redis-server redis-tools tex-gyre texlive-extra-utils
  texlive-font-utils texlive-fonts-recommended texlive-fonts-recommended-doc
  texlive-generic-recommended texlive-latex-extra texlive-latex-extra-doc
  texlive-latex-recommended texlive-latex-recommended-doc texlive-pictures
  texlive-pictures-doc texlive-pstricks texlive-pstricks-doc tipa xsltproc
0 upgraded, 33 newly installed, 0 to remove and 286 not upgraded.
Need to get 650 MB/653 MB of archives.
After this operation, 977 MB of additional disk space will be used.
Do you want to continue? [Y/n] Y
```

```
root@KaliFW: ~
File  Edit  View  Search  Terminal  Help

E: Failed to fetch http://http.kali.org/kali/pool/main/t/texlive-base/texlive-latex-r
ecommended-doc_2015.20160320-1_all.deb  404  Not Found

E: Failed to fetch http://http.kali.org/kali/pool/main/t/texlive-base/texlive-picture
s-doc_2015.20160320-1_all.deb  404  Not Found

E: Failed to fetch http://http.kali.org/kali/pool/main/t/texlive-extra/texlive-pstric
ks-doc_2015.20160320-1_all.deb  404  Not Found

E: Failed to fetch http://http.kali.org/kali/pool/main/libx/libxslt/xsltproc_1.1.28-2
.1_amd64.deb  404  Not Found

E: Failed to fetch http://http.kali.org/kali/pool/main/o/openvas-cli/openvas-cli_1.4.
2-0kali1+b1_amd64.deb  404  Not Found

E: Failed to fetch http://http.kali.org/kali/pool/main/o/openvas/openvas_8.0+kali3_al
l.deb  404  Not Found

E: Unable to fetch some archives, maybe run apt-get update or try with --fix-missing?
root@KaliFW:~#
```

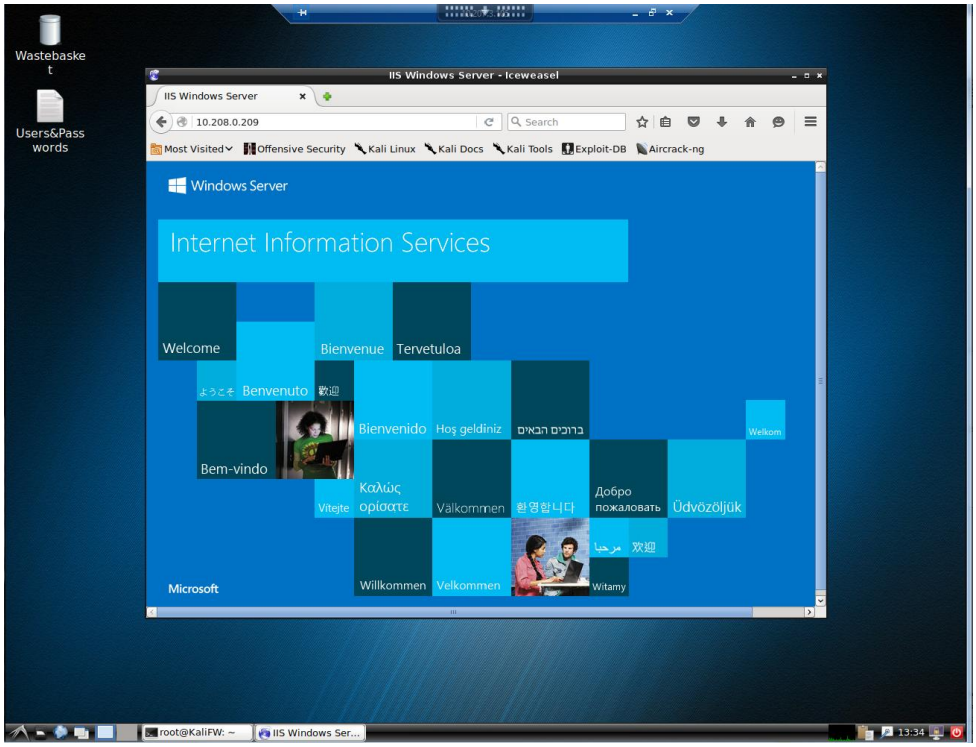
Since trying to update Kali did not fix the issue, I had to roll back to the initial version and switch to using preinstalled Kali tools.

Nikto

Nikto is an open source web vulnerability scanning tool. It allows to detect potentially dangerous files and programs, outdated and misconfigured services, vulnerable scripts. Scanning options can also be enhanced by additional plugins allowing more customization.
To start working with Nikto, first of all I checked the basic commands with Nikto Help.
nikto -h (for the short version) or *nikto -H* (for the full version)

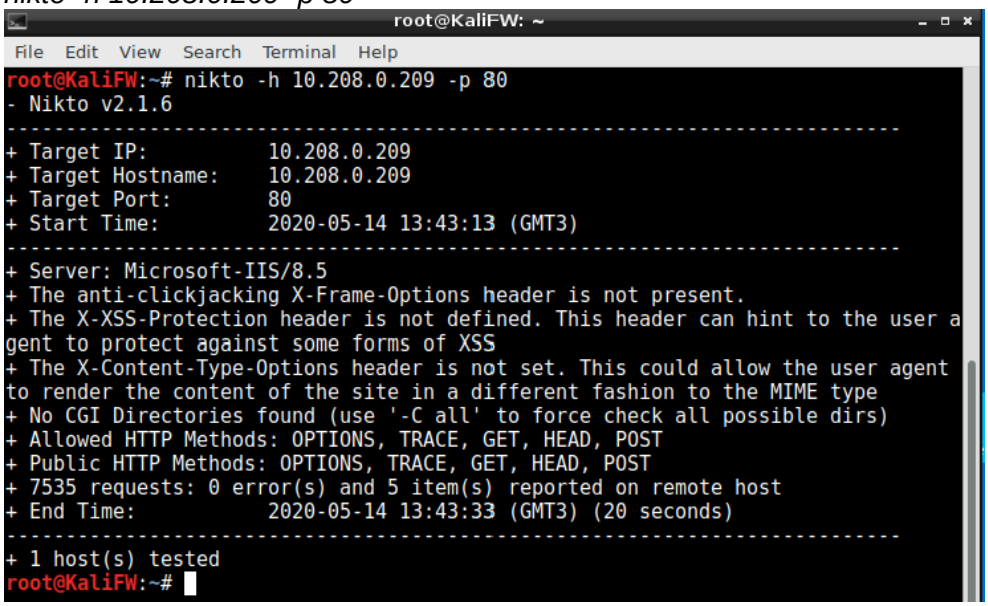
```
root@KaliFW: ~
File  Edit  View  Search  Terminal  Help
root@KaliFW:~# nikto -h
Option host requires an argument

       -config+            Use this config file
       -Display+           Turn on/off display outputs
       -dbcheck            check database and other key files for syntax errors
       -Format+            save file (-o) format
       -Help               Extended help information
       -host+              target host
       -id+                Host authentication to use, format is id:pass or id:pass:r
ealm
       -list-plugins       List all available plugins
       -output+            Write output to this file
       -nossl              Disables using SSL
       -no404              Disables 404 checks
       -Plugins+           List of plugins to run (default: ALL)
       -port+              Port to use (default 80)
       -root+              Prepend root value to all requests, format is /directory
       -ssl                Force ssl mode on port
       -Tuning+            Scan tuning
       -timeout+           Timeout for requests (default 10 seconds)
       -update             Update databases and plugins from CIRT.net
       -Version            Print plugin and database versions
       -vhost+             Virtual host (for Host header)
                + requires a value

        Note: This is the short help output. Use -H for full help text.

root@KaliFW:~# nikto -H
```

For testing purposes, I have preinstalled IIS on my Windows Server 1 and set up a test web page. It is accessible withing the network by the server IP (10.208.0.209).



To define the target for scanning we are giving the IP address of the host and the port, which is by default port 80.

nikto -h 10.208.0.209 -p 80

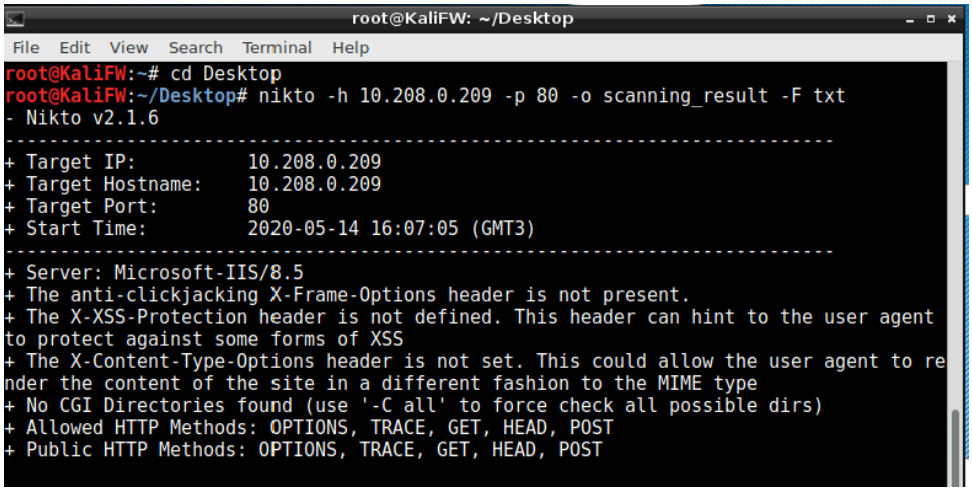


```
root@KaliFW: ~
File  Edit  View  Search  Terminal  Help
root@KaliFW:~# nikto -h 10.208.0.209 -p 80
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.208.0.209
+ Target Hostname:    10.208.0.209
+ Target Port:        80
+ Start Time:         2020-05-14 13:43:13 (GMT3)
---------------------------------------------------------------------------
+ Server: Microsoft-IIS/8.5
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user a
gent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent
to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Allowed HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST
+ Public HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST
+ 7535 requests: 0 error(s) and 5 item(s) reported on remote host
+ End Time:           2020-05-14 13:43:33 (GMT3) (20 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
root@KaliFW:~#
```

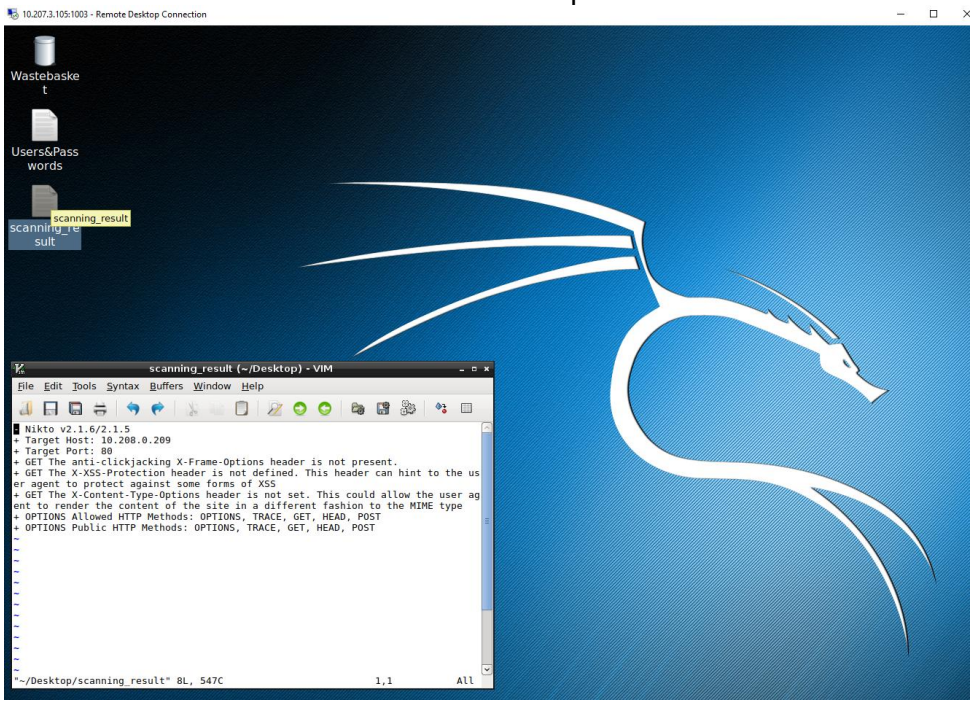
We can see that it is a Microsoft-IIS web server. Then we can also see vulnerability threats, for example, the X-XSS-Protection header is not defined, which means it is vulnerable to cross-site scripting.

We can also save the output to a file. For instance, it can be saved to the Desktop directory with the name “scanning_results” using txt file format.

nikto -h 10.208.0.209 -p 80 -o scanning_results -F txt



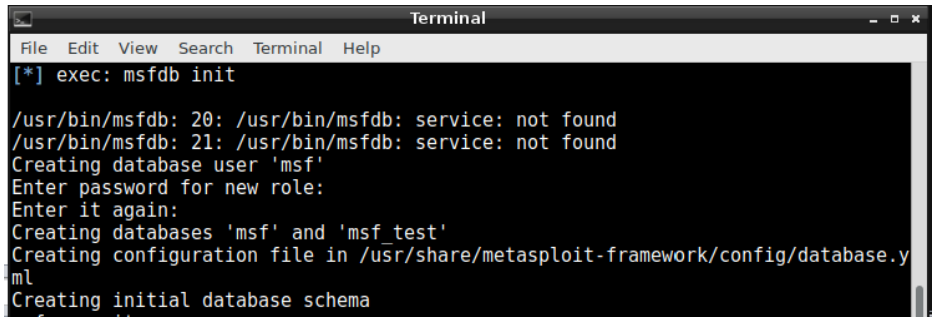
We can now access the file from the desktop.



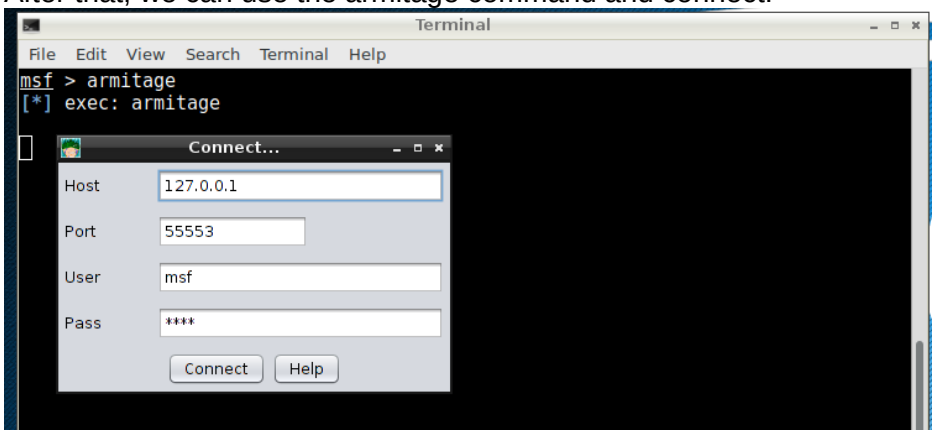
The information obtained during the scanning can be used for penetration testing to attack the system using the detected exploits. These results can also be exported and are compatable with Metasploit, which will be discussed further on in this report. To export the file into the Metasploit-readable format we use the command -Format msf+.

Armitage

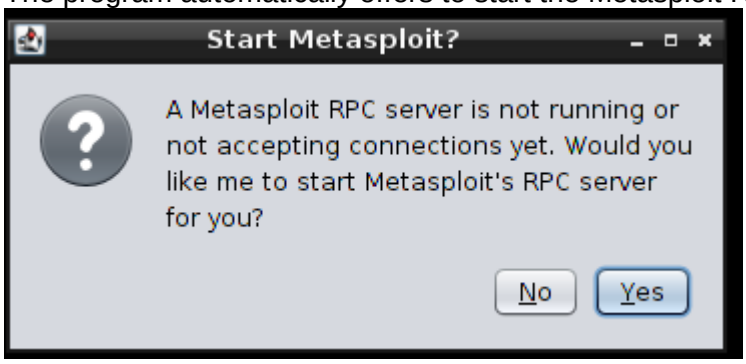
Armitage is a graphical user interface for the Metasploit framework. Metasploit is a penetration testing framework designed for detecting vulnerabilities of the network or server. It includes numerous applications and exploits. Armitage is an open source network security tool that visualizes targets and recommends exploits. It also allows the security team to collaborate on the Metasploit session.
Armitage can be accessed by using msf console (Metasploit Terminal).
First of all, a database file should be setup.
msfdb init



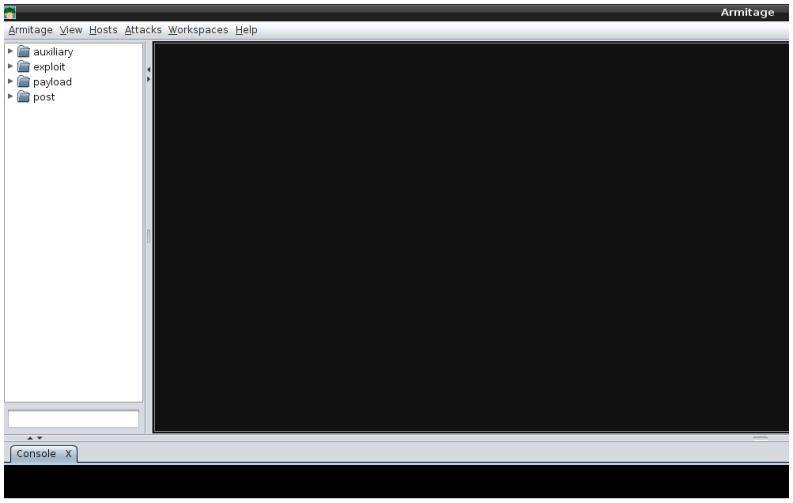
After that, we can use the armitage command and connect.



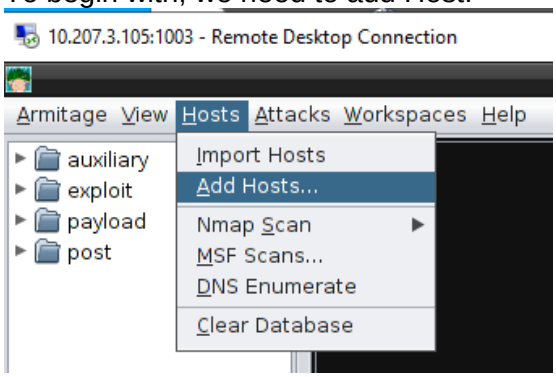
The program automatically offers to start the Metasploit RPC server.



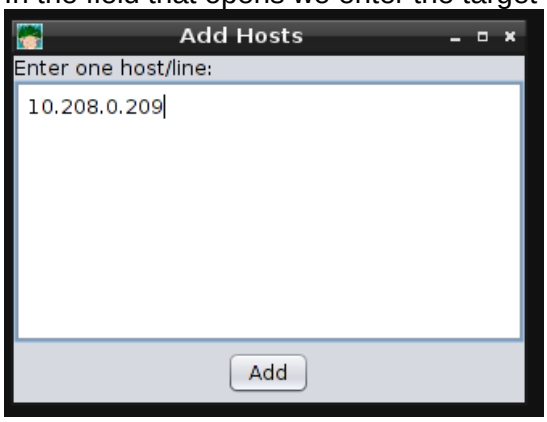
The Armitage interface is now accessable. The modules include auxiliary, exploit, payload, and post.



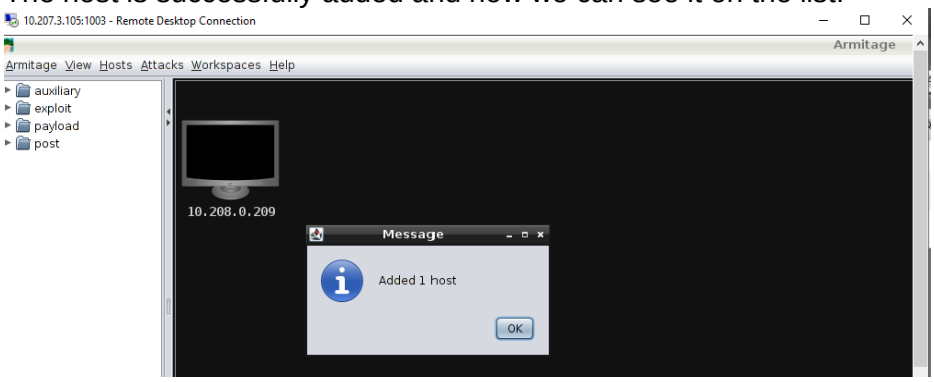
To begin with, we need to add Host.



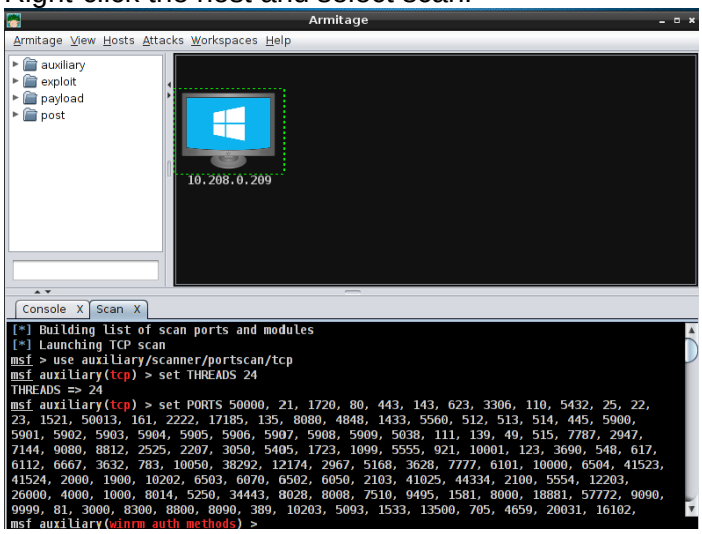
In the field that opens we enter the target IP address.



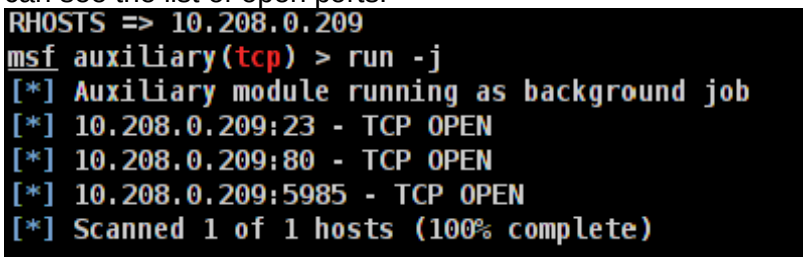
The host is successfully added and now we can see it on the list.



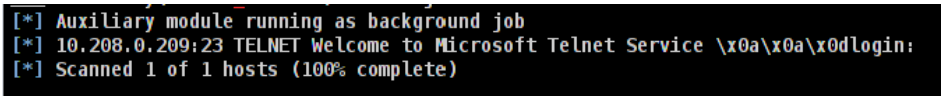
Right-click the host and select scan.



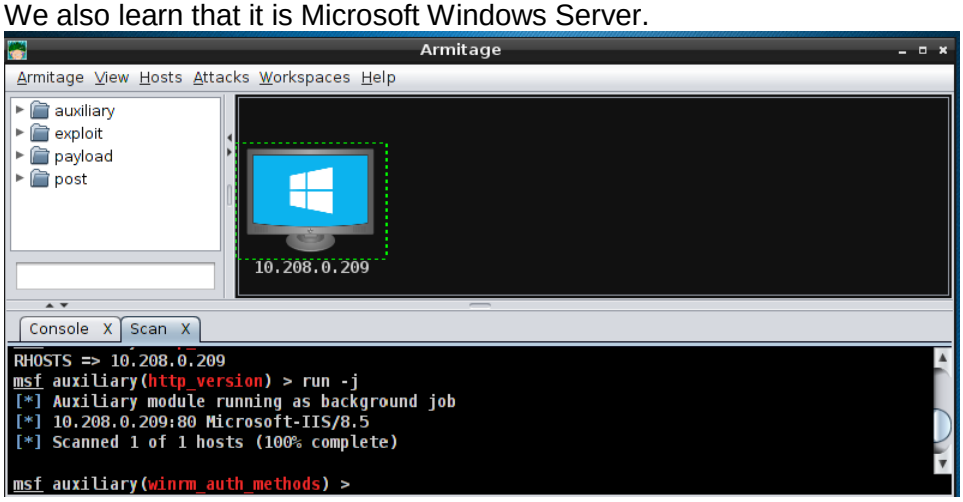
The obtained information will be displayed in the console. For example, we can see the list of open ports.



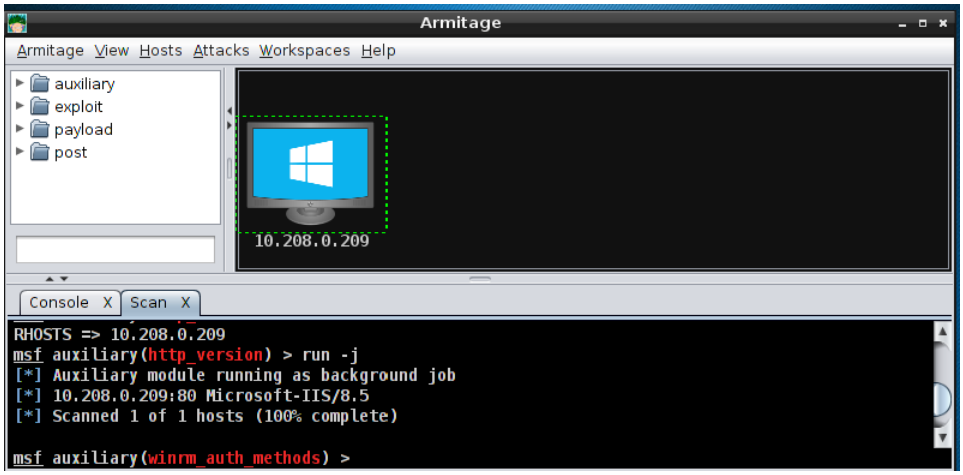
Basic auxiliary scan also identifies the running services, for example, Telnet.



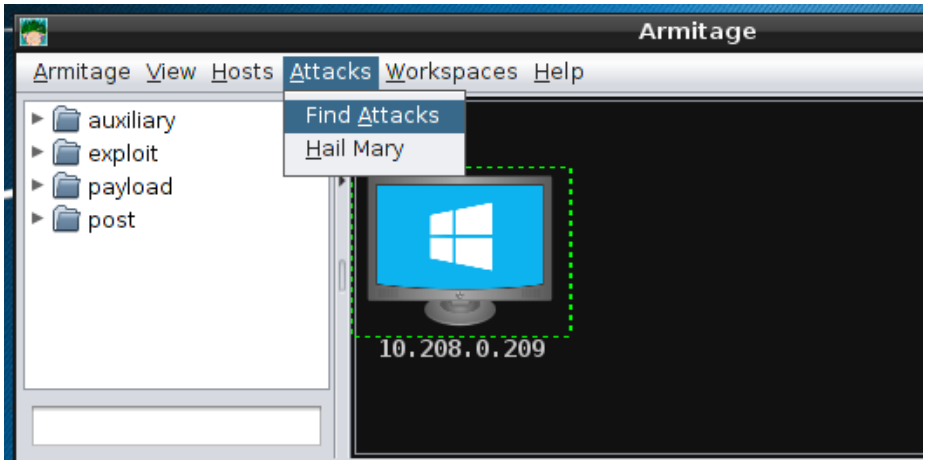
We also learn that it is Microsoft Windows Server.



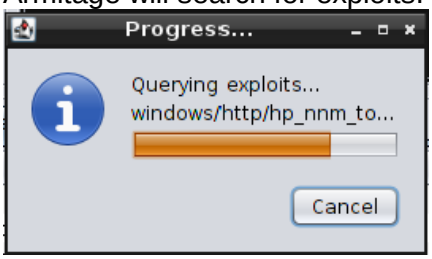
After the scan is complete, if we right-click the host, we can pick the Services option to get a report on all the running services.



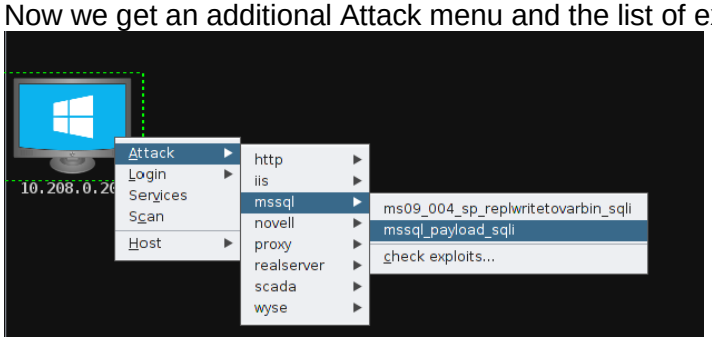
In order to find exploits we need to go to the Attaks tab and pick the Find Attaks option.



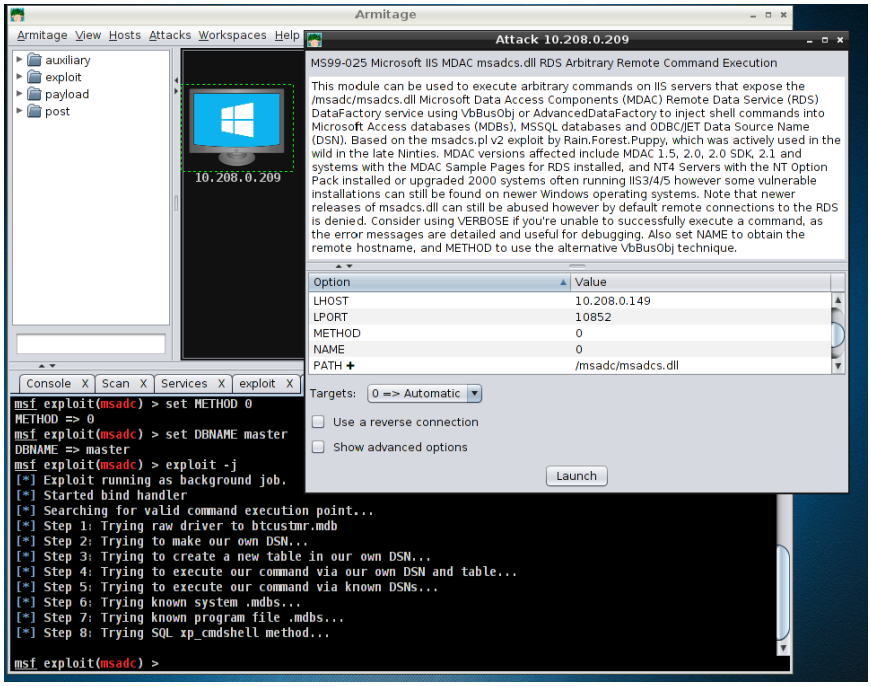
Armitage will search for exploits.



Now we get an additional Attack menu and the list of exploits.



We can pick an exploit from the list, and try launching an attack. For example, we can insert shell commands by using iis msadc exploit. Detailed description of the exploit that I used is provided on the screenshot.



There are numerous other exploits available for all kinds of services, for instance, IIS, databases, telnet, ftp, http, and ssh connections.

Resources

Greenbone Networks. 2020. The Greenbone Security Manager at Work. URL: https://www.greenbone.net/en/live-demo/. Accessed: 6 May 2020.

Infosec. 2018. Introduction to the Nikto Web Application Vulnerability Scanner. URL: https://resources.infosecinstitute.com/introduction-nikto-web-application-vulnerability-scanner/#gref. Accessed: 8 May 2020.

Imperva. 2020. Penetration Testing. URL: https://www.openvas.org/. Accessed: 8 May 2020.

Kali by Offensive Security. 2015. OpenVAS 8.0 Vulnerability Scanning. URL: https://www.kali.org/penetration-testing/openvas-vulnerability-scanning/. Accessed: 6 May 2020.

OffSec Services, 2020. Armitage Exploitation. URL: https://www.offensive-security.com/metasploit-unleashed/armitage-exploitation/. Accessed: 13 May 2020.

OffSec Services, 2020. Kali Linux Tools Listing. URL: https://tools.kali.org/tools-listing. Accessed: 13 May 2020.

OffSec Services, 2020. Nikto. https://tools.kali.org/information-gathering/nikto. Accessed: 8 May 2020.

OffSec Services, 2020. Working with Active and Passive Exploits in Metasploit. URL: https://www.offensive-security.com/metasploit-unleashed/exploits/. Accessed: 13 May 2020.

OpenVAS. 2020. OpenVAS – Open Vulnerability Assessment Scanner. URL: https://www.openvas.org/. Accessed: 6 May 2020.

Strategic Cyber, 2014. Armitage Manual. URL: http://www.fastandeasyhacking.com/manual. Accessed 13 May 2020.