RP:Red Primer

RP: Web Scanning

RP: Web Scanning

Title DVWA IP Address 10.10.66.30

Web scanning represents one of the core constructs of modern pen testing. Quite simply, most of what we interact with on a daily basis is the internet, and therein there is a
multitude of ever-widening number of vulnerabilities. Within this room, we will investigate two of the most common scanners: Nikto and Zap.

Deploy the machine!

[Task 1] Pull the lever, Kronk!

Web scanning represents one of the core constructs of modern pen testing. Quite simply, most of what we interact with on a daily basis is the internet, and therein there is a multitude of ever-widening number of vulnerabilities. Within this room, we will investigate two of the most common scanners: Nikto and Zap.

Enjoy the room! For future rooms and write-ups, follow @darkstar7471 on Twitter.

click me	click me
#1	Deploy the machir

No answer needed

[Task 2] ...I'm supposed to scan with that?

click me	click me
#1	First and foremost, what switch do we use to s target host?

-h

---

click me	click me
#2	Websites don't always properly redirect to the transport port and can sometimes have different issues depending on manner in which they are scanned. How do we disable secure transpo

-nossl

---

click me	click me
#3	How about the opposite, how do we force sec transport?

-ssl

---

click me	click me
#4	What if we want to set a specific port to scan

-p

---

click me	click me
#5	As the web is constantly evolving, so is Nikto of vulnerabilities represents a core component to this web scanner, ho verify that this database is working and free from error?

-dbcheck

---

click me	click me
#6	If instructed to, Nitko will attempt to guess a files within directories as well as usernames. Which switch and numer do we use to set Nikto to enumerate usernames in Apache? Keep in m option is deprecated in favor of plugins, however, it's still a great opti aware of for situational usage.

-mutate 3

---

click me	click me
#7	Suppose we know the username and passwo forum, how do we set Nikto to do a credentialed check? Suppose the u admin and the password is PrettyAwesomePassword1234

-id admin:PrettyAwesomePassword1234

---

click me	click me
#8	Let's scan our target machine, what web serv discover and what version is it?

Apache/2.4.7

---

click me	click me
#9	This box is vulnerable to very poor directory c to it's web server version, what directory is indexed that really shouldn

config

click me	click me
#10	Nikto scans can take a while to fully complet switch do we set in order to limit the scan to end at a certain time?

-until

click me	click me
#11	But wait, there's more! How do we list all of are available?

--list-plugins

click me	click me
#12	On the flip-side of the database, plugins rep another core component to Nikto. Which switch do we use to instruct plugin checks to find out of date software on the target host? Keep in when testing this command we need to specify the host we intend to against. For submitting your answer, use only the base command wit date option.

-plugins outdated

click me	click me
#13	Finally, what if we'd like to use our plugins to of standard tests against the target host?

-plugins tests

[Task 3] Zip ZAP!

A brief quiz and tutorial over using the OWASP Zap Scanner

click me	click me
#1	Let's start simple and launch zap. This can be number of ways (Commands: owasp-zap, zaproxy) or through launchin Kali gui.

No answer needed

click me	click me
#2	Launch ZAP, what option to we set in order to what we are attacking?

url to attack

click me	click me
#3	Launch the attack against our target! Throug course of this attack you may notice this is very similar to Nikto. Simil Nessus vs. OpenVAS, Nikto and ZAP and both offer different perspectiv host and, as such, it's useful to know how to leverage both scanning t order to maximize your own visibility in a situation wherein 'noise' doe particularly matter.

No answer needed

click me	click me
#4	ZAP will discover a file that typically contains which well-behaved web indexing engines will read in order to know w sections of a site to avoid. What is the name of this file? (Lucky for us scanner isn't what we would call 'well-behaved'!)

robots.txt

click me	click me
#5	One entry is included in the disallow section what is it?

/

click me	click me
#6	ZAP will find a directory that contains images application, what is the path for that directory? (This is what will follo ip of the website)

/dvwa/images/

click me	click me
#7	This website doesn't force a secure connectio and ZAP isn't pleased with it. Which related cookie is ZAP upset about

HttpOnly

click me	click me
#8	Featured in various rooms on TryHackMe, Cros Scripting is a vicious attack that is becoming ever more common on t web. What Alert does ZAP produce to let us know that this site is vulne XSS? Note, there are often a couple warnings produced for this, look fo so directly related to the web client.

Web Browser XSS Protection Not Enabled

click me	click me
#9	The ZAP proxy spider represents the compone responsible for 'crawling' the site. What site is found to be out of scope

http://www.dvwa.co.uk

---

click me	click me
#10	ZAP will use primarily two methods in order website, which of these two HTTP methods requests content?

GET

---

click me	click me
#11	Which option attempts to submit content to

POST

RP: Nmap

RP: Nmap

Part of the Red Primer series, intro to scanning.

[Task 1] Deploy!

Nmap is an incredibly valuable tool in the world of penetration testing. In this room, we will cover the basics of using Nmap to effectively scan a target, gaining insight for further attacks!

#1
Deploy the machine!

No answer needed

[Task 2] Nmap Quiz

A short quiz on the more useful switches that we can use with Nmap. All you'll need for this is the help menu for nmap. Include all parts of the switch unless otherwise specified, this includes -
----

Enjoy the room! For future rooms and write-ups, follow @darkstar7471 on Twitter.

#1

First, how do you access the help menu?

-h

#2

Often referred to as a stealth scan, what is the first switch listed for a 'Syn Scan'?

-sS

#3

Not quite as useful but how about a 'UDP Scan'?

-sU

#4

What about operating system detection?

-O

#5

How about service version detection?

-sV

#6

Most people like to see some output to know that their scan is actually doing things, what is the verbosity flag?

-v

#7

What about 'very verbose'? (A personal favorite)

-vv

#8

Sometimes saving output in a common document format can be really handy for reporting, how do we save output in xml format?

-oX

#9

Aggressive scans can be nice when other scans just aren't getting the output that you want and you really don't care how 'loud' you are, what is the switch for enabling this?

-A

#10

How do I set the timing to the max level, sometimes called 'Insane'?

-T5

#11

What about if I want to scan a specific port?

-p

#12
How about if I want to scan every port?

-p-

#13
What if I want to enable using a script from the nmap scripting engine? For this, just include the first part of the switch without the specification of what script to run.

--script

#14
What if I want to run all scripts out of the vulnerability category?

--script vuln

#15
What switch should I include if I don't want to ping the host?

-Pn

[Task 3] Nmap Scanning

Perform some basic nmap scanning and learn to read through the results

#1
Let's go ahead and start with the basics and perform a syn scan on the box provided. What will this command be without the host IP address?

nmap -sS

#2
After scanning this, how many ports do we find open under 1000?

2

#3
What communication protocol is given for these ports following the port number?

tcp

#4
Perform a service version detection scan, what is the version of the software running on port 22?

6.6.1p1

#5
Perform an aggressive scan, what flag isn't set under the results for port 80?

httponly

#6
Perform a script scan of vulnerabilities associated with this box, what denial of service (DOS) attack is this box susceptible to? Answer with the name for the vulnerability that is given as the section title in the scan output. A vuln scan can take a while to complete. In case you get stuck, the answer for this question has been provided in the hint, however, it's good to still run this scan and get used to using it as it can be invaluable.

http-slowloris-check

RP: Nessus

Part of the Red Primer series, learn how to set up and use Nessus

[Task 1] Deploy!

Deploy the vulnerable machine! This one, well, it has problems.

#1
Deploy the virtual machine!

No answer needed

[Task 2] Installation

Install Nessus on a system of your system of choice! For the sake of this guide, I'll be using Ubuntu. I highly recommend installing this on a dedicated VM just for Nessus scanning. Here's a link to the Nessus documentation online: https://docs.tenable.com/nessus/Content/GettingStarted.htm

---

Enjoy the room! For future rooms and write-ups, follow @darkstar7471 on Twitter.

#1

First, create a basic Ubuntu box (or any other system of your choice). Minimum 4 2GHz cores, 4 GB RAM (8 Recommended) and 30 GB of disk space.

No answer needed

#2

Next, go ahead and register for a Nessus Home license. This can be used to scan up to 16 IP addresses at a time. Be sure to keep this license information safe, you'll need it for any manual work. Here's the registration link: https://www.tenable.com/products/nessus-home

No answer needed

#3

Follow the installation instructions on Tenable's website, once Nessus is set up connect the machine that it lives on to the network using your VPN file.

No answer needed

[Task 3] Nessus Quiz

A short quiz on the features and functions of Nessus, this includes the Nessus 7 manual as well for any clarification.

#1

As we log into Nessus, we are greeted with a button to launch a scan, what is the name of this button?

New Scan

#2

Nessus allows us to create custom templates that can be used during the scan selection as additional scan types, what is the name of the menu where we can set these?

policies

#3

Nessus also allows us to change plugin properties such as hiding them or changing their severity, what menu allows us to change this?

plugin rules

#4

Nessus can also be run through multiple 'Scanners' where multiple installations can work together to complete scans or run scans on remote networks, what menu allows us to see all of these installations?

scanners

#5
Let's move onto the scan types, what scan allows us to see simply what hosts are 'alive'?

host discovery

#6
One of the most useful scan types, which is considered to be 'suitable for any host'?

basic network scan

#7
Following a few basic scans, it's often useful to run a scan wherein the scanner can authenticate to systems and evaluate their patching level. What scan allows you to do this?

credential patch audit

#8
When performing Web App tests it's often useful to run which scan? This can be incredibly useful when also using nitko, zap, and burp to gain a full picture of an application.

web application tests

[Task 4] Scanning!

Run a basic network scan and learn to read through the results!

#1
Deploy the machine and connect to the network

No answer needed

#2
Create a new 'Basic Network Scan' targeting the deployed VM. What option can we set under 'BASIC' to set a time for this scan to run? This can be very useful when network congestion is an issue.

schedule

#3
Under discovery set the scan to cover ports 1-65535. What is this type called?

port scan (all ports)

#4

As we are connected to the network via a VPN, it may be to our benefit to 'tone down' the scan a bit. What scan type can we change to under 'ADVANCED' for this lower bandwidth connection?

scan low bandwidth links

#5

With these options set (other than the time to run) save and launch the scan.

No answer needed

#6

After the scan completes, which 'Vulnerability' can we view the details of to see the open ports on this host?

Nessus SYN scanner

#7

There seems to be a chat server running on this machine, what port is it on?

6667

#8

Looks like we have a medium level vulnerability relating to SSH, what is this vulnerability named?

SSH weak algorithms supported

#9

What web server type and version is reported by Nessus?

Apache/2.4.99

[Task 5] Wait, there's mail?

Add SMTP functionality into your Nessus install!

#1

An optional but awesome additional step, link your Nessus box up to an SMTP server via the Settings panel. Google provides this for free if you already have a Gmail account. Adding 2-factor authentication on your account and create an app password, then link Nessus to the Gmail SMTP server via these following settings: https://www.siteground.com/kb/-google_free_smtp_server/

No answer needed

[Task 6] So you're telling me that's how you set up a web app...

Run a Web App scan against a *very* secure web application that has absolutely no problems!

#1
Run a web application scan against this new box.

No answer needed

#2
What is the plugin id of the plugin that determines the HTTP server type and version?

10107

#3
What authentication page is discovered by the scanner that transmits credentials in cleartext?

/login.php

#4
What is the file extension of the config backup?

.bak

#5
Which directory contains example documents? (This will be in a php directory)

/external/phpids/0.6/docs/examples/

#6
What vulnerability is this application susceptible to that is associated with X-Frame-Options?

clickjacking

#7
What version of php is the server using?

5.5.9-1ubuntu4.26

RP: tmux

[Task 1] Screens wishes it was this cool.

**tmux, the terminal multiplexer, is easily one of the most used tools by the Linux community (and not just pentesters!). While not a malicious tool,
tmux makes running simultaneous tasks throughout a pentest incredibly easy. In this primer room, we'll walk through the process of installing and
using some of the most common key combinations used in tmux. (Note, the installation process in this is geared towards Kali/Ubuntu.)**

Link to the above cheat sheet: Link
Original credit for the cheat sheet goes to Linux Academy
For another excellent resource on learning tmux, check out IppSec's video: Link
---
Enjoy the room! For future rooms and write-ups, follow @darkstar7471 on Twitter.

click me	**click me**
#1	First things first, let's go ahead and install tm be done on Ubuntu/Kali with the command: apt-get install tmux

No answer needed

click me	click me
#2	Once tmux is installe command do we use to launch a new session

tmux

click me	click me
#3	All tmux commands combination. What is the first key in this com

control

click me	click me
#4	How about the seco pressed at the same time and released befor combination.

B

click me	click me
#5	Lets go ahead and d session. What key do we need to add to the c

D

click me	click me
#6	Well shoot, we've de list all of our sessions?

tmux ls

click me	click me
#7	What did our session one without a set name?

0

click me	click me
#8	Now that we've found attach to it?

tmux a -t 0

click me	click me
#9	Let's go ahead and r What key do we add to the combo in order to

C

click me	click me
#10	Seems like we hav them up with. Let's remedy that problem by and nmap scan against it. Deploy the VM n

No answer needed

click me	click me
#11	Run the following s TARGET_IP

No answer needed

click me	click me
#12	Whew! Plenty of ou with a relatively small terminal like me, this once. To fix that, let's enter 'copy mode'. Wh enter copy mode?

[

click me	click me
#13	Copy mode is very up and down using the arrow keys. What if w

g

click me	click me
#14	How about the bott

G

click me	click me
#15	What key do we pre mode'?

q

click me	click me
#16	This window we're need an upgrade. What key do we add to th

%

click me	click me
#17	How about horizon

"

click me	click me
#18	We can now move b combo and arrow keys, try it out!

No answer needed

click me	click me
#19	We can also resize combo and pressing the arrow keys, try it ou

No answer needed

click me	click me
#20	Wait a minute, we' window! We can go back it using the key co Try going back to this original window and t one!

No answer needed

click me	click me
#21	Say one of these n unresponsive or we're just done working in i 'kill' the pane?

x

click me	click me
#22	Now that's we've fi close the session?

exit

click me	click me
#23	Last but now least, session named 'neat'?

tmux new -s neat