Nikto Lab

Angad, Steve & Eden

Introduction to Lab:

We decided to make a lab to help introduce the basics of using Nikto, it's main features and some basic things it can do while also showing off other sides of computer security. I have some sections where I took important screenshots to understand certain steps better. You don't need to complete any of this yourself, but you can find all the screenshots in the "Lab Output" folder. (All Lab files, including Reflection Answers & screenshots are included in the Github Folder)

You can also look at our recording of the Lab which covers Standard Scan all the way to Ubuntu Scan. It does not show how to install the VMs and Servers required as they're labeled as pre-requisites for this lab. (https://youtu.be/VQbuBBYtfNI)

Pre-requisites

You will need the following software installed on your computer for this lab:

- Kali Linux VM
- Bad Store Server
- Ubuntu Server

Instructions

Install Bad Store Server

Get the Bad Store iso in

https://drive.google.com/file/d/1Ayj-vDxUHaZ2hbOMJZFjbAQCgQ6tzMZ5/view?usp=sharing

and make a new Virtual Machine.

- Name: BadstoreServer1
- Hardrive: 20 MB
- RAM: 20 MB
- Version: Linus 64x

Install Ubuntu Server

Get the Ubuntu iso in

https://drive.google.com/file/d/1Q0egBLVh4ZgwHl4DAomYcHufAmmFbESb/view?usp=sharing and make a new Virtual Machine.

- Name: UbuntuServer1
- Hardrive: 2 GB
- RAM: 2 GB
- Version: Ubuntu 64 bit

Do all settings as default, except make sure to enable Ubuntu as an SSL Server. That is all.

Startup both machines

- Remember the IP Address of the Bad Store Serve. Screenshot provided of this step in **badStoreIP.png**
- Open Terminal on Kali Linux VM

Standard Scan

- In the Kali Terminal, type

  ’nikto -h hackthissite.org’ (nikto -h scanme.nmap.org) Screenshot provided of this step in **standardScan.png**

- Read over the results and take a screenshot showing the Target IP & Port

Bad Store Scan

- In the Kali Terminal, type ‘nikto -h <badstore ip> -o badstoreOutput.csv’
- Using your Kali device, open your browser (Firefox)
- Type <badstore.ip>/images in the address bar and review what you’re seeing and what it is.
- Type <badstore.ip>/cgi-bin/test.cgi in the Firefox browser. Screenshot of the page provided in **testCgiEncoding.png**
- Try to Decode the Base64 message. You can find a Base64 decoder online.

Scanning Multiple Hosts

- Create a text file with IP addresses that you want to scan with Nikto.

  sudo vi IPlist

- You can copy the following lines into your IPlist file or have something of your own. (Press i to insert text.)

  <badstore IP address>

  hackthissite.org

- Remember to save it. (:w to save :q to quit)

- In the terminal type the following command to run the multiple hosts.

  nikto -h <filepath to the IPlist> (When Nikto is scanning multiple IP addresses you can press N to skip to the next IP.)
- Look over the scan result. Screenshot provided of this step in **multipleScan.png**

Ubuntu Scan

- Make sure Badstore, Ubuntu & Kali machine is running.
- Go to your ubuntu and use 'ip address'. Make sure to remember this ip address. Screenshot provided of this step in **ubuntuIP.png**
- Go to your Kali machine and put in

  nmap -p 80 <ubuntuIP address> -oG ubuntuList.txt
- do cat ubuntuList.txt and find all the IPs with "Ports: 80/open"
- make a file named ubuntuList2.txt and put in all the IPs that have "Port: 80/open"
- Type in nikto -h ubuntuList2.txt -o ubuntuOutput.csv -Format csv Screenshot provided of the output **ubuntuOutput.csv** **(**You can use Google Sheets to have a better view of the CSV file.)

Screenshots & Outputs provided for Lab:

Nikto Lab Output/

screenshots/

badStoreIP.png

standardScan.png

testCgiEncoding.png

multipleScan.png

ubuntuIP.png

badstoreOutput.csv

ubuntuOutput.csv

Nikto Lab Reflection Questions

1. What is the encrypted message of the Base64 and MD5 Hash string?

2. What is the port that the standard scan is scanning?

3. How can you scan other ports using Nikto?

4. What port is used for HTTPS?

5. What command could've been used to find IPs with "Ports: 80/open"

6. What command could've been used to make a text file for ipList2.txt

References for Lab

1. Staff, HackThisSite. org. (n.d.). Hackthissite. Hack This Site. https://www.hackthissite.org/
2. Shivanandhan, M. (2021, July 14). *Web Server Scanning With Nikto – A Beginner's Guide*. freeCodeCamp. Retrieved December 4, 2023, from
3. https://www.freecodecamp.org/news/an-introduction-to-web-server-scanning-with-nikto/
4. Chris Sullo, David Lodge (2021, Sep 16). *Nikto 2.5*. Retrieved December 5, 2023, from https://cirt.net/Nikto2
5. Nielsen Networking. (2022, December 22). Nikto and Kali Linux: The Ultimate Duo for Penetration Testing [Video]. YouTube. https://www.youtube.com/watch?v=ogUN8Nrr__g
6. Cyber Today Academy. (2022, March 13). What is Nikto Tool in Kali Linux and How to use it? [Video]. YouTube.

7. https://www.youtube.com/watch?v=zKpaD1Bi9DI

8. HackerSploit. (2018, January 31). Nikto Web Vulnerability Scanner - Web Penetration Testing - #1 [Video]. YouTube. https://www.youtube.com/watch?v=GH9qn_DBzCk

9. TigTec. (2022, February 10). Vulnerability Scanning with Nikto [Video]. YouTube. https://www.youtube.com/watch?v=a6hlUyMX968