

Forum:[Hack Forums](#)

Thread: [\[TUTORIAL\] Scan for vulnerabilities in a webserver](#)

SIM-2015410 - March 23, 2014, 9:30 pm

Hello Again HF!,

Welcome to another Hacking Tutorial by MeshCollider.

If you are interested, here are links to my other hacking tutorials: Spoiler ([Click to View](#))

Metasploit 1: <https://hackforums.net/showthread.php?tid=4124763>

Metasploit 2: <https://hackforums.net/showthread.php?tid=4124800>

Metasploit 3: <https://hackforums.net/showthread.php?tid=4124838>

Cracking WiFi - WEP: <https://hackforums.net/showthread.php?tid=4126315>

Remote view a webcam/microphone: <https://hackforums.net/showthread.php?tid=4126349>

Cracking WiFi - WPA/WPA2: <https://hackforums.net/showthread.php?tid=4127410>

Hacking/Crashing windows 7 with a shortcut file:

<https://hackforums.net/showthread.php?tid=4127314>

PDF backdoor: <https://hackforums.net/showthread.php?tid=4127426>

DNS Spoof password stealing: <https://hackforums.net/showthread.php?tid=4131834>

Hacking a website: a brief introduction.

Websites are hosted on a webserver - which is just a computer. if we can gain access to the webserver, we can steal or change the files (e.g. defacing), or move from there to attack an entire network.

To gain access, we can either guess/crack passwords for the FTP server on the computer, etc, or we could exploit vulnerabilities in the server or programs running there to gain access quickly and easily.

This tutorial will demonstrate a simple tool to find potential vulnerabilities in a web server, in order to exploit them. This tool is called Nikto. It is one of the most widely used website vulnerabilities tools for security (penetration) testing and black hat hacking.

WARNING: Although the tool is effective, it is very "noisy" - it is not stealthy and can easily be detected if the webserver being scanned has some sort of detection software installed or has a proactive administrator.

1) Run Nikto on Kali Linux

As usual, we will use Kali because it already has Nikto installed. Choose "Kali Linux -> Vulnerability Analysis -> Misc Scanners -> nikto" and run it.

2) Scan the target server

To simple scan for vulnerabilities, we will use this command:

Code `nikto -h example.com`Where example.com is the target's URL. We can also use an IP address, for example 192.168.1.8 which is the IP address of a server on my own network. To find the IP of a server, simple type this command into a terminal window:

Code `ping example.com`And it will tell you the IP address.

3) Analyse the detected vulnerabilities.

Nikto will give us a nice little report of potential vulnerabilities in the target server. For example, my

scan tells us the server is Apache 2.2.14, probably on Ubuntu, and gives a list of potential weaknesses we could try to exploit. Some vulnerabilities will be given with a OSVDB prefix, which stands for Open Source Vulnerability Database - a database of known vulnerabilities at www.osvdb.org. You can read more about the vulnerabilities there, by searching the vulnerability ID.

WATCH OUT FOR FALSE POSITIVES! Nikto merely scans to see if the server responds without error to known exploitable URLs, it does not attempt to execute the exploits itself. Some of the "vulnerabilities" nikto returns may not be vulnerable - this is called a false positive.

In future tutorials, I will demonstrate other ways to scan for vulnerabilities, and ways to exploit these vulnerabilities after you have found them.

Thanks for reading, please reply with your thanks if you enjoyed this and/or found it useful.

Watch out for future hacking tutorials from me - further wireless cracking, metasploit and other common hacking topics!

Written by MeshCollider ?

Ch1m4zz - March 24, 2014, 1:10 am

Thanks for this, might be useful one day!

SIM-2015410 - March 24, 2014, 1:37 am

(Mar 24, 2014 01:10 AM)Ch1m4zz Wrote: [\[CITE\]](#) Thanks for this, might be useful one day!

Congratz, first reply! Haha, it's not hard, none of my tutorials have been receiving much interest. I appreciate the fact that you have bothered replying, thank you ?

Od?y - August 19, 2014, 5:51 pm

This is actually a great tutorial. I think one of the reasons these tutorials don't get the credit they deserve is people want to just download magical software that does everything for them with little work from them.

SIM-2015410 - August 19, 2014, 10:08 pm

(Aug 19, 2014 05:51 PM)0day* Wrote: [\[CITE\]](#) This is actually a great tutorial. I think one of the reasons these tutorials don't get the credit they deserve is people want to just download magical software that does everything for them with little work from them.

Thanks man, yeah, there are a lot of LQ people around here. I appreciate your reply though!

CorsoConnected - August 21, 2014, 10:46 am

Looks good, Can't wait to try it mate. Just have to get all my protection in place, VPN, VM With Kali ect first lol. Pretty new to the scene =/ but not new to computing or programming.

Fruit Snacks - January 23, 2015, 2:57 pm

Nice tutorial man ! will definitely help people.

Furorem - January 24, 2015, 5:11 am

Nikto is one of the best tools to scan vulnerabilities, Linux distros have lots of stuff like this. But this is Vulnscanner #1 ?

BrokenMachine99 - May 12, 2015, 12:12 am

nice tut man. great work. keep it up.

janneman - May 12, 2015, 3:26 am

Thanks man, yeah i will try this

32x0LF - June 1, 2016, 10:45 pm

Could you make a TUT on stealthy scanners? thanks

testingon - June 7, 2016, 3:58 am

nice work done

thanks for sharing....

?BORNE? - June 7, 2016, 7:20 am

MeshCollider your tutorials are great never stop them coming!

Bouness - June 7, 2016, 2:44 pm

Nice tutorial man, giving the command to use on Kali, going to try this out now

Alterations - June 7, 2016, 2:48 pm

HQ tutorial, thank you very much!

super pl3b - June 7, 2016, 4:25 pm

thanks for the share dude. appreciate it

nuckle - June 7, 2016, 8:50 pm

Hey cool tutorial but these types of scanning is useless against some sites. That command to scan with will get you ip banned. Do you know how I can add a proxy list to this so it can be more effective and faster when scanning?

I've messed around in the help and didn't see anything related to a proxy list but maybe there was a proxy part but that proxy would only last a few seconds before banned.

R^ptor - June 8, 2016, 10:59 pm

Vouch for this user good TUT

Vhon - June 8, 2016, 11:37 pm

a very great tutorial and usefull

mgknight - March 19, 2018, 4:29 am

great thanks for you, said enough no less no more

Rootomi - March 20, 2018, 10:05 am

thank you nice tutorial please keep it up

Xcyber02 - March 31, 2018, 4:08 pm

good :) thanks man :) nice tut