Penetration Testing for FCM 745—Michael Fernez

I. Executive Summary

Our class was tasked with a sample penetration test on servers set up at John Jay College by Professor Obaidat.

The goals of this penetration test are as follows:

- 1) to identify if an attacker can compromise the Ubuntu Server in question at IP 10.5.62.84
- 2) determine the impact in the event the system is compromised on
 - a) confidentiality and integrity of system information
 - b) availability of the server

Penetration testing was conducted following the specifications in NIST SP 800-115 with recommendations from the InfoSec Institute [1] and Offensive Security [2].

- A. Summary of Results
- II. Vulnerability Analysis
- A. Vulnerability Scans with Nmap and Nikto

Given a specific host to probe host was discovered using Nmap and analyzed further with a Sparta vulnerability scan, which utilized nmap, nikto, and various connection services.

The result revealed ftp, ssh, apache, and mySQL services running on ports 21, 22, 80, and 3306 respectively.

				SPARTA 1	.0.3 (BE	TA) - untitled - /roc	ot/			0	• •
File Help											
Scan Brute											
Hosts Services	Tools	Services	Scripts	Information	Notes	nikto (80/tcp) 🗵	screensh	not (80/tcp) 🗵	mysql-defa	ult (3306/to	:p) ⊲ ►
OS Ho	ost	Por	rt	Protocol	Sta	ate Name		١	/ersion		
10.5.65.84			tc	р	open	ftp	vsftpd 3	3.0.3			
		● 22	tc	р	open	ssh	OpenSS	SH 7.6p1 Ubunti	u 4ubuntu0.1	(Ubuntu Lin	านx
		● 80	tc	р	open	http	Apache	httpd 2.4.29 ((l	Jbuntu))		
		330	06 tc	р	open	mysql	MySQL	5.7.24-0ubuntu	0.18.04.1		
Log											
Progress		Tool		Host		Start time		End time		Status	
	mysql-defaul	t (3306/tcp) 1	10.5.65.84		08 Dec 2018 12:48:1	.9 08 De	08 Dec 2018 12:48:26 F			
	nmap (stage	3)	1	L0.5.65.84	0	08 Dec 2018 12:48:1	.9 08 De	c 2018 12:50:15	5 Finished		
	screenshot (8	80/tcp)	1	10.5.65.84	0	08 Dec 2018 12:46:4	2 08 De	c 2018 12:46:42	2 Finished		v

B. Brute Force Connection attempts

Following the Sparta scan, I attempted to brute force each connection using the default word lists provided by metasploit utilizing the "Brute" tab in Sparta.

i. Apache Server

Entering the IP address in a browser reveals the default Apache2 Ubuntu page, suggesting that this server may be using default passwords and usernames Using the http_default_pass and users files with THCHydra via Sparta revealed the site is using several default usernames and passwords

SPARTA 1.0.3 (BETA) - scan1.sprt - /root/Desktop/	•	•
File Help		
Scan Brute		
IP 10.5.65.82 Port 80 Service http-get 🛊 Run		
🗌 Try blank password 👿 Try login as password 👿 Loop around users 🗌 Exit on first valid 🗌 Verbose 🗌 Additional Options		
○ Username root		
O Password password	16	A V
[DATA] attacking http-get://10.5.65.82:80//		4
[80][http-get] host: 10.5.65.82 login: admin password: admin		
[80][http-get] host: 10.5.65.82 login: manager password: manager		
[80][http-get] host: 10.5.65.82 login: root password: root		1
[80][http-get] host: 10.5.65.82 login: cisco password: cisco		
[80][http-get] host: 10.5.65.82 login: apc password: apc		
[80][http-get] host: 10.5.65.82 login: pass password: pass		
_[80][http-get] host: 10.5.65.82 _login: securitypassword: security		V

Using the tomcat default lists additional logins were revealed, detailed in Appendix A. (Note: IP is different here because the test was conducted before the new server was in place. A second test confirmed the logins were still valid on the 10.5.62.84 server)

ii. FTP and SSH Server

Using a publicly available password list and cycling through the default unix_users list, the login to the ftp serve was found relatively quickly. It was found this account could read files on the server and even transfer files to the server (such as simple text files).

		SPARTA 1.0.3	(BETA) - untitled - /root/		c		8
File Help							
Scan Brute							
1 × 2 × 3	×						
IP 10.5.65.84	Port 21 Service	ftp	Run				
🗹 Try blank pas	ssword 🛛 🐨 Try login as passw	vord 🛛 🗹 Loop around	users 🛛 🗹 Exit on first valid	🗌 🗌 Verbose 📄 Additio	onal Options		
○ Username	root 💿 Userna	me list eloit/unix_user	s.txt Browse O Fou	ind usernames			
○ Password	password Passwo	ord list rdlists/rockyo	u.txt Browse O Fou	nd passwords	Threads	16	×
[DATA] max 16 [DATA] attackin [21][ftp] host: 1 [STATUS] attacl 1 of 1 target su Hydra (http://w	tasks per 1 server, overall 16 t g ftp://10.5.65.84:21/ 10.5.65.84 login: ftp passwo k finished for 10.5.65.84 (valid ccessfully completed, 1 valid p ww.thc.org/thc-hydra) finished	asks, 1606572912 log rd: ftp pair found) assword found I at 2018-12-08 14:05:	in tries (l:112/p:14344401) :19	, ~100410807 tries per ta	sk		v
Log							
Progress	Tool	Host	Start time	End time	Status		
	hydra (21/tcp)	10.5.65.84	08 Dec 2018 14:04:40	08 Dec 2018 14:05:24	Finished		
	hydra (3306/tcp)	10.5.65.84	08 Dec 2018 13:58:20	08 Dec 2018 13:59:39	Killed		
	hydra (3306/tcp)	10.5.65.84	08 Dec 2018 13:28:36	08 Dec 2018 13:29:08	Finished		v

The ssh server proved to be a more time-consuming task, but using the password list as the username list as well eventually found a username, "sam," using an easily guessable password. It was found this user has root privileges and can read and write files at will.



iii. MySQL database

Using the same method as the FTP brute force, the login to the SQL server was found very quickly as it is currently using a default username and password. With this login, a user can execute arbitrary SQL commands to read, write, and delete data from the server.

			SPARTA 1.0.3	(BETA) - untitled - /root/			•	E
Help								
n Brute								
× 2 ×								
10.5.65.84	Port 3306	Service my	sql	♦ Run				
🕈 Try blank p	assword 👿 Try log	jin as password	👿 Loop around	users 👿 Exit on first valid	🗌 🗆 Verbose 🔲 Additi	onal Options		
Username	root	Username	list vloit/unix_user	rs.txt Browse O Fou	ind usernames			
	[Password I	ist rdlists/rockyg	Browse O Fou	ind passwords	Threads	16	-
) Password /hydra.restore DATA] max 4 DATA] attack 3306][mysql]	tasks per 1 server, o ing mysql://10.5.65.8	verall 4 tasks, 1 34:3306/	606572912 login	tries (l:112/p:14344401), ~	401643228 tries per task		10	
Password /hydra.restorr DATA] max 4 DATA] attack 3306][mysql] STATUS] atta . of 1 target s łydra (http://	password tasks per 1 server, o ing mysqL://10.5.65.8 host: 10.5.65.84 lc ck finished for 10.5.0 successfully complete www.thc.org/thc-hyd	verall 4 tasks, 1 34:3306/ ogin: root pass 55.84 (valid pair ed, 1 valid passv dra) finished at 2	606572912 login word: root found) vord found 2018-12-08 13:29	tries (l:112/p:14344401), ~	401643228 tries per task			
Password /hydra.restor DATA] max 4 DATA] attack 3306][mysql] STATUS] atta of 1 target s 4ydra (http://	password tasks per 1 server, o ing mysql://10.5.65.8 host: 10.5.65.84 lc ck finished for 10.5.4 uccessfully complete www.thc.org/thc-hyd	verall 4 tasks, 1 34:3306/ ggin: root pass 55.84 (valid pair ed, 1 valid passv dra) finished at 2	606572912 login word: root found) vord found 2018-12-08 13:29	tries (l:112/p:14344401), ~	401643228 tries per task			
Password /hydra.restorn DATA] max 4 DATA] attack 3306][mysql] STATUS] attack . of 1 target s łydra (http:// Progress	password tasks per 1 server, o ing mysqL//10.5.65.8 host: 10.5.65.84 lc ck finished for 10.5.4 uccessfully complete www.thc.org/thc-hyd	verall 4 tasks, 1 34:3306/ ggin: root pass 55.84 (valid pair ed, 1 valid pass dra) finished at 2	606572912 login word: root found) vord found 2018-12-08 13:29 Host	tries (l:112/p:14344401), ~ :03	401643228 tries per task End time	Status		
 Password /hydra.restor DATA] max 4 DATA] attack DATA] attack 3306][mysql] STATUS] atta dydra (http:// Progress 	assword tasks per 1 server, o ing mysqL//10.5.65.84 lo ck finished for 10.5.4 uccessfully complete www.thc.org/thc-hyd Too hydra (3306/tcp)	verall 4 tasks, 1 34:3306/ ggin: root pass 55.84 (valid pair ed, 1 valid pass dra) finished at 2	606572912 login word: root found) vord found 2018-12-08 13:29 Host 10.5.65.84	tries (l:112/p:14344401), ~ :03 Start time 08 Dec 2018 13:28:36	401643228 tries per task End time 08 Dec 2018 13:29:08	Status Finished		
Password /hydra.restor DATA] max 4 DATA] attack 3306[msvgl] STATUS] atta of 1 target s 4ydra (http:// Progress	a tasks per 1 server, o ing mysqL//10.5.65.84 lc ck finished for 10.5.4 uccessfully complete www.thc.org/thc-hyd Too hydra (3306/tcp) hydra (22/tcp)	verall 4 tasks, 1 34:3306/ ogin: root pass 55.84 (valid pair cd, 1 valid pass dra) finished at 2 bl	606572912 login word: root found) vord found 2018-12-08 13:29 Host 10.5.65.84 10.5.65.84	tries (l:112/p:14344401), ~ :03 Start time 08 Dec 2018 13:28:36 08 Dec 2018 13:24:36	401643228 tries per task End time 08 Dec 2018 13:29:08	Status Finished Running		



III. Classification of Vulnerabilities and Recommendations

Vulnerability: SSH Login with weak password

Risk: Critical

Impact: A user with access to this SSH server can read and write files and execute programs. Since the account found has root privileges, an attacker who finds it has full access to the machine.

Remediation: Revoke Sam's root privileges and/or have him change both the username and the password. A user's account should never have a password that matches the username, especially one so easily guessable with publicly available word lists. Passwords should be at least 15 characters in length containing a combination of letters, numbers and special characters.

Vulnerability: SQL databse login with default credentials

Risk: High

Impact: A user with access to this MariaDB server can execute SQL commands that read, write, and drop tables from the SQL database. This can potentially compromise other systems if the databases contain account info.

Remediation: Disable default logins and considering disabling the database if it is not being used.. Default usernames passwords are a common vulnerability on fresh installations of MariaDB. It is recommended that each user have a unique username and password, with passwords at least 15 characters in length containing a combination of letters, numbers and special characters.

Vulnerability: FTP Login with default credentials

Risk: Medium

Impact: A user with access to this FTP server can read and transfer files on the server. This could enable an attacker to read sensitive data, change sensitive data, and transfer malicious executables to the server.

Remediation: Change both the username and the password. Default usernames passwords are a common vulnerability on fresh installations of FTP. It is recommended that each user of the FTP server have a unique username and password, with passwords at least 15 characters in length containing a combination of letters, numbers and special characters.

Vulnerability: Apache Login with default credentials

Risk: Medium

Impact: A user with access to this web server can make changes to webpages and read potentially sensitive data.

Remediation: Disable default logins and limit the users who can access the server and change the Apache default webpage. Default usernames passwords are a common vulnerability on fresh

installations of Apache. It is recommended that each user have a unique username and password, with passwords at least 15 characters in length containing a combination of letters, numbers and special characters.

IV. Appendix A: Tools Used and References

Kali Linux Penetration Testing OS Sparta – Comprehensive Vulnerability Suite using nmap and nikto Nikto – Vulnerability scanner Nmap – port scanner Metaploit – Penetration Testing Framework Password lists from <u>https://wiki.skullsecurity.org/Passwords</u>

1. <u>https://resources.infosecinstitute.com/writing-penetration-testing-reports/</u>

2. <u>https://www.offensive-security.com/reports/sample-penetration-testing-report.pdf</u>

V. Appendix B: Login Credentials for Apache Web Server

[80][http-get] host: 10.5.65.82 login: admin password: admin [80][http-get] host: 10.5.65.82 login: manager password: manager [80][http-get] host: 10.5.65.82 login: root password: root [80][http-get] host: 10.5.65.82 login: cisco password: cisco [80][http-get] host: 10.5.65.82 login: apc password: apc [80][http-get] host: 10.5.65.82 login: pass password: pass [80][http-get] host: 10.5.65.82 login: security password: security [80][http-get] host: 10.5.65.82 login: system password: system [80][http-get] host: 10.5.65.82 login: sys password: sys [80][http-get] host: 10.5.65.82 login: wampp password: wampp [80][http-get] host: 10.5.65.82 login: newuser password: newuser [80][http-get] host: 10.5.65.82 login: manager password: admin [80][http-get] host: 10.5.65.82 login: user password: user [80][http-get] host: 10.5.65.82 login: xampp-dav-unsecure password: xampp-dav-unsecure [80][http-get] host: 10.5.65.82 login: vagrant password: vagrant [80][http-get] host: 10.5.65.82 login: root password: admin [80][http-get] host: 10.5.65.82 login: cisco password: admin [80][http-get] host: 10.5.65.82 login: xampp-dav-unsecure password: admin [80][http-get] host: 10.5.65.82 login: vagrant password: admin [80][http-get] host: 10.5.65.82 login: user password: password [80][http-get] host: 10.5.65.82 login: xampp-dav-unsecure password: password [80][http-get] host: 10.5.65.82 login: vagrant password: password [80][http-get] host: 10.5.65.82 login: xampp-dav-unsecure password: manager [80][http-get] host: 10.5.65.82 login: vagrant password: manager [80][http-get] host: 10.5.65.82 login: user password: admin [80][http-get] host: 10.5.65.82 login: xampp-dav-unsecure password: letmein

[80][http-get] host: 10.5.65.82 login: vagrant password: letmein

[80][http-get] host: 10.5.65.82 login: manager password: manager [80][http-get] host: 10.5.65.82 login: root password: admin [80][http-get] host: 10.5.65.82 login: role1 password: manager [80][http-get] host: 10.5.65.82 login: role1 password: role1 [80][http-get] host: 10.5.65.82 login: manager password: admin [80][http-get] host: 10.5.65.82 login: role1 password: admin [80][http-get] host: 10.5.65.82 login: tomcat password: admin [80][http-get] host: 10.5.65.82 login: both password: admin [80][http-get] host: 10.5.65.82 login: admin password: manager [80][http-get] host: 10.5.65.82 login: both password: manager [80][http-get] host: 10.5.65.82 login: admin password: admin [80][http-get] host: 10.5.65.82 login: root password: root [80][http-get] host: 10.5.65.82 login: tomcat password: tomcat [80][http-get] host: 10.5.65.82 login: root password: manager [80][http-get] host: 10.5.65.82 login: tomcat password: manager [80][http-get] host: 10.5.65.82 login: both password: both [80][http-get] host: 10.5.65.82 login: admin password: role1 [80][http-get] host: 10.5.65.82 login: tomcat password: role1