Metasploit Pro

Detailed Audit Report

Report generated:

Sat, 10 Jan 2015 19:28:44 +0800

Total Pages: 7

Executive Summary

This report represents a security audit performed using Metasploit Pro from Rapid7, Inc. It contains confidential information about the state of your network. Access to this information by unauthorized personnel may allow them to compromise your network.

During this test, 1 hosts with a total of 32 exposed services were discovered. 2 modules were successfully run and 5 login credentials were obtained. The most common module used to compromise systems was 'exploit/multi/misc/java_rmi_server', which opened 1 sessions.

Major Findings

Compromised Hosts

Vulnerability Name	IP Address	Hostname
exploit/multi/samba/usermap_script	172.16.162.128	metasploitable
exploit/multi/misc/java_rmi_server	172.16.162.128	metasploitable

Discovered Operating Systems

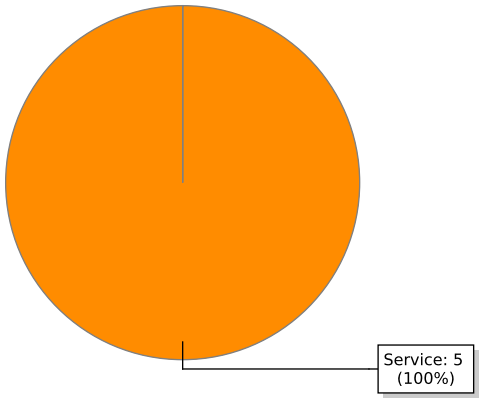
Operating System	Hosts	Services	Vulnerabilities
Linux	1	32	2

Discovered Hosts

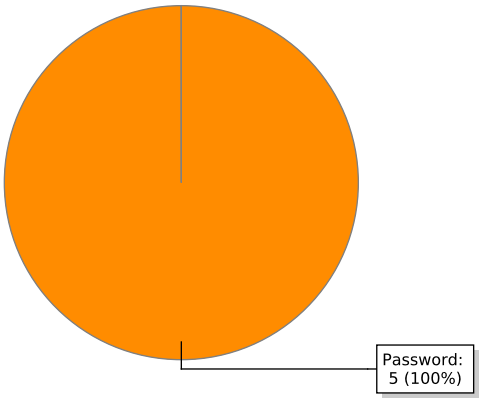
Discovered	IP Address	Hostname	OS	Services	Vulns
1/10/15 8:31 AM	172.16.162.128	metasploitable	Linux	32	2

Credentials (5 total)

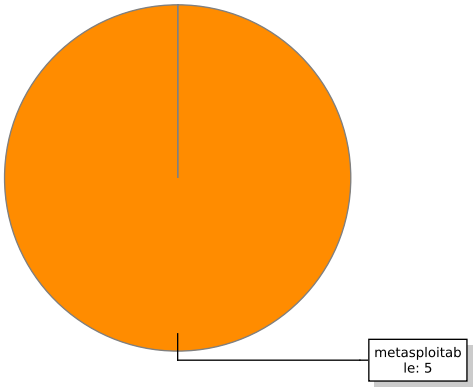
Credential Origins



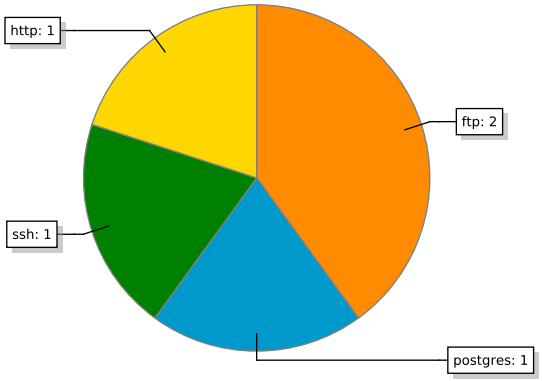
Private Types



Credentials by Host



Credentials by Service



Plaintext Passwords

Public	Private	Realm Type	Realm Value	Origin	Hosts	Services
postgres	postgres	PostgreSQL Database	template1	Service	1	1
tomcat	tomcat	None		Service	1	1
user	user	None		Service	1	1

Public	Private	Realm Type	Realm Value	Origin	Hosts	Services
anonymous	1234	None		Service	1	1
ftp	1234	None		Service	1	1

Detailed Findings

172.16.162.128 - metasploitable

Discovered: 2015-01-10 08:31:38.308298

Operating System: Linux

Credentials

Type	Origin	Logins	Service/Port	Public	Private
Password	Service	1	postgres/5432	postgres	postgres
Password	Service	1	http/8180	tomcat	tomcat
Password	Service	1	ftp/21	anonymous	1234
Password	Service	1	ftp/21	ftp	1234
Password	Service	1	ssh/22	user	user

Successful Attacks

Vulnerability Name	Exploit Module
Java RMI Server Insecure Endpoint Code Execution Scanner	exploit/multi/misc/java_rmi_server
Samba "username map script" Command Execution	exploit/multi/samba/usermap_script

Active Services

<table>
<tr><th>Port</th><th>Protocol</th><th>Name</th><th>Info</th></tr>
<tr><td>21</td><td>tcp</td><td>ftp</td><td>220 (vsFTPd 2.3.4)\x0d\x0a</td></tr>
<tr><td>22</td><td>tcp</td><td>ssh</td><td>SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1</td></tr>
<tr><td>23</td><td>tcp</td><td>telnet</td><td>_ _ _ _ _ _ ____ \x0a _ __ ___ ___| |_ __ _ ___ _ __ | | ___ (_) |_
__ _| |__ | | ___|___ \ \x0a| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |\x0a| | | | |
| __/ || (_| __ \ |_) | | (_) | | || (_| | |_) | | __// __/ \x0a|_| |_| |_|___|____,_|___/
.__/|_|___/|_|____,_|_.__/|_|___|_____|\x0a |_|
\x0a\x0a\x0aWarning: Never expose this VM to an untrusted network!\x0a\x0aContact: msfdev[at]metasploit.com\x0a\x0aLogin with msfadmin/msfadmin to get started\x0a\x0a\x0ametasploitable login:</td></tr>
<tr><td>25</td><td>tcp</td><td>smtp</td><td>220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
</td></tr>
<tr><td>53</td><td>udp</td><td>dns</td><td>BIND 9.4.2</td></tr>
<tr><td>53</td><td>tcp</td><td>dns</td><td></td></tr>
<tr><td>80</td><td>tcp</td><td>http</td><td>Apache/2.2.8 (Ubuntu) DAV/2 (Powered by PHP/5.2.4-2ubuntu5.10)</td></tr>
<tr><td>111</td><td>udp</td><td>portmap</td><td>100000 v2 TCP(111), 100000 v2 UDP(111), 100024 v1 UDP(42839), 100024 v1 TCP(37334), 100003 v2 UDP(2049), 100003 v3 UDP(2049), 100003 v4 UDP(2049), 100021 v1 UDP(58816), 100021 v3 UDP(58816), 100021 v4 UDP(58816), 100003 v2 TCP(2049), 100003 v3 TCP(2049), 100003 v4 TCP(2049), 100021 v1 TCP(42623), 100021 v3 TCP(42623), 100021 v4 TCP(42623), 100005 v1 UDP(43762), 100005 v1 TCP(35285), 100005 v2 UDP(43762), 100005 v2 TCP(35285), 100005 v3 UDP(43762), 100005 v3 TCP(35285)</td></tr>
<tr><td>111</td><td>tcp</td><td>sunrpc</td><td>100000 v2</td></tr>
<tr><td>137</td><td>udp</td><td>netbios</td><td>METASPLOITABLE:<00>:U :METASPLOITABLE:<03>:U :METASPLOITABLE:<20>:U :&#x01;&#x02;__MSBROWSE__&#x02;:<01>:G :WORKGROUP:<00>:G :WORKGROUP:<1d>:U :WORKGROUP:<1e>:G :00:00:00:00:00:00</td></tr>
<tr><td>139</td><td>tcp</td><td>smb</td><td></td></tr>
<tr><td>445</td><td>tcp</td><td>smb</td><td>Unix (Samba 3.0.20-Debian)</td></tr>
<tr><td>512</td><td>tcp</td><td>exec</td><td></td></tr>
</table>

Port	Protocol	Name	Info
513	tcp	login	
514	tcp	shell	
1099	tcp	java-rmi	Class Loader: Enabled
2049	udp	nfsd	NFS Daemon 100005 v1
2049	tcp	sunrpc	100003 v4
2121	tcp	ftp	220 ProFTPD 1.3.1 Server (Debian) [::ffff:172.16.162.128]\x0d\x0a
3306	tcp	mysql	5.0.51a-3ubuntu5
3632	tcp	distccd	
5432	tcp	postgres	8.3.8
5900	tcp	vnc	
6000	tcp	x11	
6667	tcp	irc	
8180	tcp	http	Apache-Coyote/1.1
35285	tcp	sunrpc	100005 v3
37334	tcp	sunrpc	100024 v1
42623	tcp	sunrpc	100021 v4
42839	udp	sunrpc	100024 v1
43762	udp	sunrpc	100005 v3
58816	udp	sunrpc	100021 v4

Web Vulnerabilities

Discovered Vulnerabilities

Vulnerability	Description
Java RMI Server Insecure Endpoint Code Execution Scanner	Module auxiliary/scanner/misc/java_rmi_server confirmed remote code execution via this RMI service
Samba "username map script" Command Execution	Exploited by exploit/multi/samba/usermap_script to create Session 27

Session Activity

Session #26

Opened: 2015-01-10 08:38:28.773435 | Closed: null

> load stdapi

Session #27

Opened: 2015-01-10 08:38:29.873311 | Closed: 2015-01-10 11:24:22.187325

> uname -a

> uname -a

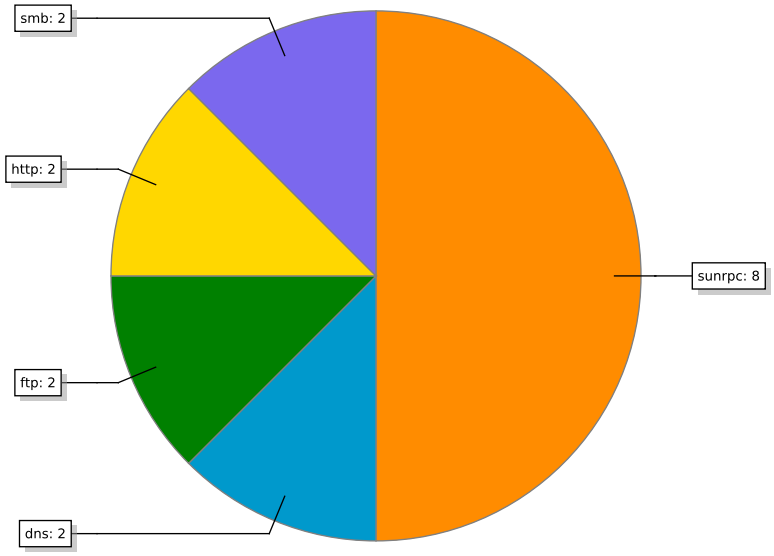
> module_run post/pro/device/gather/device_info

> show config
show version
help

Service Table

Service/Port
ftp/21
ssh/22
telnet/23
smtp/25
dns/53
dns/53
http/80
portmap/111
sunrpc/111
netbios/137
smb/139
smb/445
exec/512
login/513
shell/514
java-rmi/1099
sunrpc/2049
nfsd/2049
ftp/2121
mysql/3306
distccd/3632
postgres/5432
vnc/5900
x11/6000
irc/6667
http/8180
sunrpc/35285
sunrpc/37334
sunrpc/42623
sunrpc/42839
sunrpc/43762
sunrpc/58816

Multiple Service Instance Frequency
(all services with multiple running instances)



Total Service Instance Frequency
(32 total service instances open)