CYBERSECURITY

EXPLOITATION: PASSWORD AND SHADOW

Purpose is to get passwords after gaining (root) access to a system.
These passwords can be used to hop to further machines.

Basically this comes down to a hash/unhash attack.
Make sure you create some users, preferably with their passwords from a wordlist you will use. (rockyou?)

FILES

A couple files of particular interest on Linux systems are the /etc/passwd and /etc/shadow files.

PASSWD

The /etc/passwd file contains basic information about each user account on the system, including the root user which has full administrative rights, system service accounts, and actual users.

Document an existing passwd file.
There are seven fields in each line of /etc/passwd.
What do they mean? Document this.

SHADOW

The /etc/shadow file contains the encrypted passwords of users on the system. While the /etc/passwd file is typically world-readable, the /etc/shadow is only readable by the root account.

The shadow file also contains other information such as password expiration dates.

Document a line from an existing shadow file.

JOHN THE RIPPER

We'll use John the Ripper to try to crack the passwords.

Copy the contents of /etc/passwd and /etc/shadow into their own text files on our local machine.
Document the names of these text files.

Before we can feed the hashes we obtained into John, we need to use a utility called unshadow to combine the passwd and shadow files into a format that John can read.
Run the following command to merge the data into a new text file called passwords.txt.

Type: unshadow your_passwd_file.txt your_shadow_shadow.txt > passwords.txt

We will use john with a wordlist file for fast encryption

Type: john --wordlist=/usr/share/wordlists/sqlmap.txt passwords.txt
The cracking can take a long time.
Document the result.
Note: remember that if you used john before for existing hashes, the results may already be present. Where? Check the FAQ!

To see the passwords,
Type: john --show passwords.txt
Document the result.

HASHCAT

This tool only needs the hashes.

Copy any hashes we want to crack into a new text file that we'll call hashes.txt:

Document the contents of hashes.txt

Use the hashid tool to identify the hash-type
Document this.

Run the following command to start cracking.

Type: hashcat -m YOURHASHID -a 0 -o cracked.txt hashes.txt /usr/share/wordlists/sqlmap.txt -O --forced

Make sure to replace YOURHASHID with the number suited for your hashtype.
Check what all of the options mean.

Document the findings. (If necessary use a shorter wordlist for faster unhashing.)

ONLINE

Check also if you can crack the hashes online. This might save you some time.
Document the sites which give the best solutions.