Client Side Attacks (Contd)

Tools in Kali Linux

Module #25

Kali Linux: Obtaining and cracking user passwords?

Password cracking by definition is recovering passwords from data that has been stored or transmitted by a computer system.

Host systems are usually Windows or Linux-based and have specific characteristics regarding how they store and protect user passwords. The easiest method to obtain user passwords is through social engineering.

A hacker could obtain passwords or clues to how passwords are created by posing as an authorized subject. For example, identifying that all passwords must be between 6-10 characters, start with a capital letter, and end with a number dramatically reduces the number of possible outcomes a hacker would need to attempt to crack a password.

Kali Linux: Obtaining and cracking user passwords?

There are a few ways hackers crack passwords. These are listed as follows:

- Guess: Manually guess using information obtained about a target
- Dictionary attack: Use an automated attack that tries all the possible dictionary words
- Brute-force: Try all the possible character combinations
- Hybrid: Combining dictionary with brute-force

Passwords must be stored so that the systems can verify a user's identity and access rights. Systems do not store passwords in plain text files for obvious security reasons. Most systems do not use encryption as the only means to protect passwords, because a key is required to unencrypt, which poses a weakness to protecting the encrypted files.

Kali Linux: Obtaining and cracking user passwords?

Hashing was invented as a means to transform a key or password, usually arithmetic, into a completely different value. Hashing is non-reversible and outputs the same value for an entered key, which means a hash can be stored and verified against an entered password to verify authenticity.

Changing one factor, such as making a letter capital or adding a space, generates a completely different hash output. Hashes can be brute-forced like a password if you know the formula for generating a Hash.

Many password cracking tools such as John the Ripper are capable of detecting a hash and brute-force attacking all hash output combinations with auto-generated hash outputs. Once a match is found, John the Ripper will print out the plain text password used to generate the matching hash.

Kali Linux: Windows passwords?

Windows stores passwords in the SAM (System Account Management) registry file. The exception to this is when Active Directory is used. An Active Directory is a separate authentication system that stores passwords in a LDAP database. The SAM file is located at C:\<systemroot>\sys32\config

The SAM file stores passwords in a hashed format using the LM and NTLM hash to add security to the protected file. The SAM file cannot be moved or copied while Windows is running.

The SAM file can be dumped, displaying the password hashes that can be moved offline for a brute-force tool to crack. A hacker can also get the SAM file by booting a different OS, mounting C:\ , booting a Linux distribution on a disk (such as Kali), or booting off of a CD/floppy drive.

Kali Linux: Windows passwords?

One common place to find a SAM file is in the C:\<systemroot>\repair folder. The backup SAM file is created by default and typically not deleted by system administrators.

The backup file is unprotected but compressed, meaning that you must decompress the file to obtain the hash files. You can use the expand utility to do this. The command is Expand [FILE] [DESTINATION] .

Here is an example of expanding the SAM file into the decompressed SAM file:
C:\> expand SAM uncompressedSAM

Kali Linux: Windows passwords?

Different methods available for capturing the Windows SAM and SYSKEY files. One such is mounting the target Windows system so that tools can access these files while Windows is not running.

One can use the fdisk -l command.
Device Boot Start End Blocks Id System
/dev/hdb1* 1 2432 19535008+ 86 NTFS
/dev/hdb2 2433 2554 979965 82 Linux swap/Solaris
/dev/hdb3 2555 6202 29302560 83 Linux

Create a mount point using the command mkdir /mnt/windows .
Mount the Windows system using the command as shown in the following example:
mount -t <WindowsType> <Windows partition> /mnt/windows

Kali Linux: Windows passwords?

Need to recover both the Bootkey and SAM files.
The Bootkey file is used to access the SAM file. Tools used to access the SAM file will require the Bootkey file.

bkreg and bkhive are popular tools that can obtain the Bootkey file, as shown in the following screenshot:

Kali Linux: Linux passwords?

Linux host systems are not as common as Windows and pose a different challenge for obtaining ROOT access. Olden days: Passwords stored in the clear when auto-login is enabled such as the .netrc files used for Telnet/FTP.

For most attacks, you will want to capture the passwd and shadow files commonly stored at /etc/passwd and /etc/shadow.

The shadow file is readable only by ROOT and typically an MD5 hash. It is harder to capture than a Window's SAM file.

Breaking a Linux password is similar to other systems such as Windows. Most hybrid automated cracking programs such as John the Ripper can identify the type of hash and brute-force attack the shadow passwords with the right dictionary.

Kali Linux: Kali password cracking tools?

Kali offers various utilities to bypass password security.

Password cracking tools can be found under Password Attacks and divided into tools used for offline and online attacks.

We will focus on tools used to compromise host systems during a web application Penetration Test.

Other tools also available in Kali, such as tools designed to crack passwords for wireless protocols

Thank You