

Crack Password “Offline Attack”

iSECUR1TY
INTEGRATED SECURITY SOLUTIONS

Eng: Mahmoud Atef



Crack Password “Offline Attack”

Different Types of Password-Cracking

Passive online Eavesdropping on network password exchanges. Passive online attacks include sniffing, man-in-the-middle, and replay attacks.

Active online Guessing the Administrator password. Active online attacks include automated password guessing.

Offline Dictionary, hybrid, and brute-force attacks.

Nonelectronic Shoulder surfing, keyboard sniffing, and social engineering.

Crack Password “Offline Attack”

Passive Online Attacks

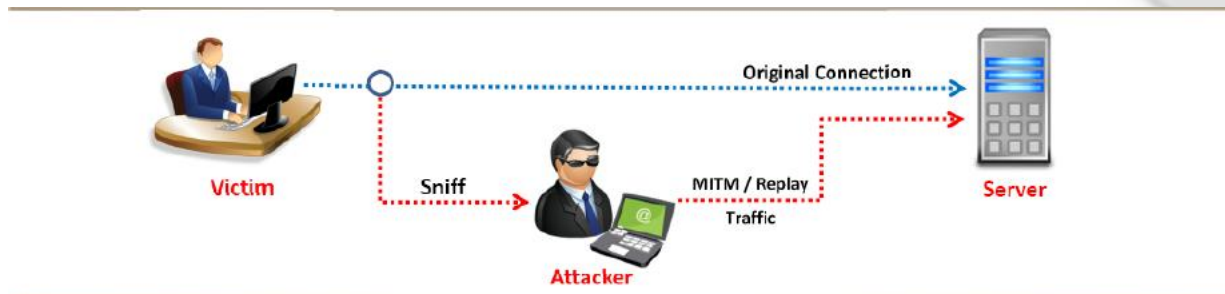
Sniffing

Man-in-the-middle and replay attack

Tools

Lophtcrack

cain



Crack Password “Offline Attack”

Active Online Attacks

Password guessing
Trojan / spyware / keylogger

Tools

THC-HYDRA

Ncrack



Crack Password “Offline Attack”

Nonelectronic Attacks

Shoulder surfing, keyboard sniffing
, and social engineering.



Crack Password “Offline Attack”

Offline attacks are only possible when you have access to the password hash(es). The attack is done on your own system or on systems that you have local access too. Unlike an online attack, there are no locks or anything else to stop you on an offline attack because you are doing it on your own machines. The only thing that could hold you back is the limits of your computer hardware because an offline attack takes advantage of its machine’s processing power and its speed is dependent on the speed of the actual machine. So the better the processor and nowadays even graphics card, the more password guessing attempts you can get per second.

Crack Password “Offline Attack”

Crack Administrator password In Windows O.S by Backtrack 5

fdisk -l

Mount /dev/sda1 /root/

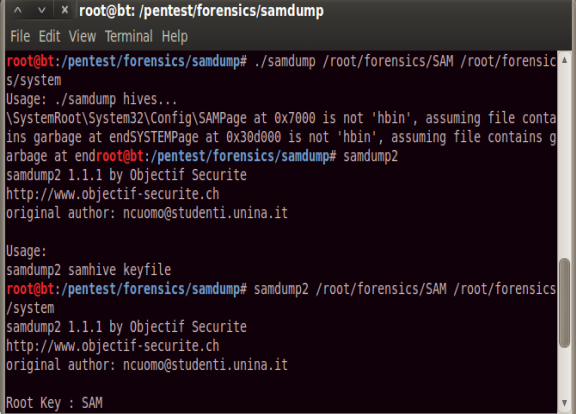
Cd /root/WINDOWS/system32/config

Bkhive system pass1.txt

Samdump2 SAM pass1.txt > Pass2.txt

Cd /pentest/password/john

./john /root/Windows/system32/config/pass2.txt



```
root@bt: /pentest/forensics/samdump
File Edit View Terminal Help
root@bt: /pentest/forensics/samdump# ./samdump /root/forensics/SAM /root/forensics/system
Usage: ./samdump hives...
\SystemRoot\System32\Config\SAMPage at 0x7000 is not 'hbin', assuming file contains garbage at endSYSTEMPage at 0x30d000 is not 'hbin', assuming file contains garbage at endroot@bt: /pentest/forensics/samdump# samdump2
samdump2 1.1.1 by Objectif Securite
http://www.objectif-securite.ch
original author: ncuomo@studenti.unina.it

Usage:
samdump2 samhive keyfile
root@bt: /pentest/forensics/samdump# samdump2 /root/forensics/SAM /root/forensics/system
samdump2 1.1.1 by Objectif Securite
http://www.objectif-securite.ch
original author: ncuomo@studenti.unina.it

Root Key : SAM
```

Crack Password “Offline Attack“

Crack Root Password In Linux O.S by Backtrack 5

Cat /etc/passwd

Save pass.txt

Cat /etc/shadow

Save shadow.txt

Cd /pentest/password/jhon

./unshadow /root/Desktop/pass.txt

/root/Desktop/shadow.txt > /root/Desktop/crack.txt

./jhon /root/Desktop/crack.txt

```
void send(PCB* from, PCB* to, char* buffer)
{
    // return error if process does not exist
    if(to == 0 || to->state == STOPPED)
    {
        from->syscall_ret = -1;
        return;
    }
    // if to is blocked waiting for this message, deliver it directly!
    if(to->state == BLOCKEDRECV && (to->waiting_for == from->pid || to->waiting_for == -1))
    {
        // if to is blocked & can recv msg, msg should be copied into recv buffer
        // and both pracs placed on the ready queue
        copy_buffer(buffer, to->buffer, 8);
        to->syscall_ret = 0;
        ready(to);

        from->syscall_ret = 0;
        ready(from);
    }
    else
    {
        // this condition should satisfy
        // - receiving process is blocked waiting for something else
        // - receiving process is not blocked

        ipc_msg *msg = kmalloc(sizeof(ipc_msg));
        msg->from = from->pid;
        msg->to = to->pid;
        msg->next_msg = 0;
    }
}
```