Ferhat Elmas
Przemyslaw Pietrzkiewicz
Javier Martín De Valmaseda Castro

Lab-8 Forensics Buffet

There are 3 directories in honey and we will examine them one by one:

Directory …/

In this directory, most important software is an ircBot with its configuration files and scripts to run it.

An ircBot is a set of scripts or an independent program that connects to Internet Relay Chat as a client and so appears to other IRC users as another user but it differs from classical client since it doesn't provide interactive access, instead it performs automated tasks.[Wikipedia]

When we run it, it tries to connect servers in sequence:

1. Tampa.FL.US.Undernet.org via port 6667
2. Diemen.NL.EU.Undernet.org via port 6667
3. Helsinki.FI.EU.Undernet.org via port 7000

Moreover, it tries to take **'FId2**' nickname which is already in use so it tries to different versions of it by appending 'underscore' such as 'FId2_', 'FId2__', 'FId2___', 'FId2____', etc.
When we check its capture, we see that it also connects another server via UDP, namely uptime.eggheads.org. There is a competition going on here to find the best ircBot that has the biggest up time so it sends its data(uptime) for this competition. For servers 2 and 3, TCP segments are divided and reassembled.

cyc.help, cyc.levels and m.help include documentation for the ircBot.

In r and randfiles directories, there are some sentences that can be used by the ircBot when it does some tasks such as going away, etc.

mech.dir is the result of pwd command and cat is the result of the ls command.

cyc.set and cyc.session are configuration files for mechs.

pico is a lightweight editor that provides much less features than vi or Emacs.

autorun, update, go, run, -bash are related to proper run of ircBot.

However, stealth and blah look somewhat different. When we run stealth, it says it is extremely dangerous so use in your own will. Since we are working virtual machine, we tried to run it but it prints no result and it is a binary file. Therefore, we couldn't exactly understand what it does. For blah, we can see what it tries since it is text file, in the enlightenment of blah we estimate that stealth can be used to bombard a port of an host with SYN and RST flooding.

For identity disclosure, we can see ircBot is written by Zetoo and ment0ru but this is for general use, we hope there is no relation between our hacker(s) with them.

.go/

In this directory, there are some user and password dictionaries to brute force, namely “1, 2, 3, 4, 5” files, these files slightly differ in format and complexity of user names and passwords. Moreover, these files are probably created by gen-pass.sh and its input file must be common file since it contains string that are permuted by gen-pass.sh to generate 1, 2, 3, 4, 5.

bios.txt includes initial guess of IP addresses of victims. mfu.txt and pass_file are files that are used on the fly(while scripts are running).

a seems the main brute forcer and finder of the actual victims and it utilizes of ss, ssh-scan and pscan2. secure is just a small script to make execution more secure.

Since there are some Romanian sentences and it is the main body of the attack to define actual victims, the writer of this script must be our hacker and he is Romanian and his name is IrcAngel. “SA VEDEM CE PULA MEA FACEM” is “see what the f**k do” in English.

.s/

This directory has more or less same structure with .go/ but at the end we can see IP addresses of victims in trueusers.txt.

Another important point is that we have the source code pscan2 in this directory.

When we look into trueusers.txt, we see bunch of IP addresses and they have common feature, owner of all IPs is same.

Recap

Attacker enter into IRC server by exploiting an IrcBot that is running under root privileges, then brute forces passwords of users that use this server to chat, bios.txt. Therefore, attacker must know in advance that his victims use this server. At the end, he can identify them in trueusers.txt with IP address, user and password information.

Malicious scripts and programs are tried to be explained above but here is their short list:

- pscan2
- ss
- scanner
- scanssh
- stealth
- a (this is dangerous in the context)
- gen-pass.sh (this is also)

Our hacker uses these tools but he didn't write all of them himself but a script is his artwork so his name should be IrcAngel. He should be originally from Romania but he prefers English since English is the must language of computers. We understand its origin from Romanian sentences: Incerc sa dau viatza cibernetici » I try to give life to cyber :->

Since determined IP addresses are owned a company, the goal of attack is much related to profit than pride.

We can see some slang but generally he is mature and doing his job.

Is he 1337 or n00b? We think he isn't n00b but he isn't also 1337. We wonder that why he brought source code of programs or why he permuted password on the server and didn't prepare before. We are n00b, maybe there is something that we don't know and he knows such as he brought the source code to make changes faster since he couldn't learn all properties of server.