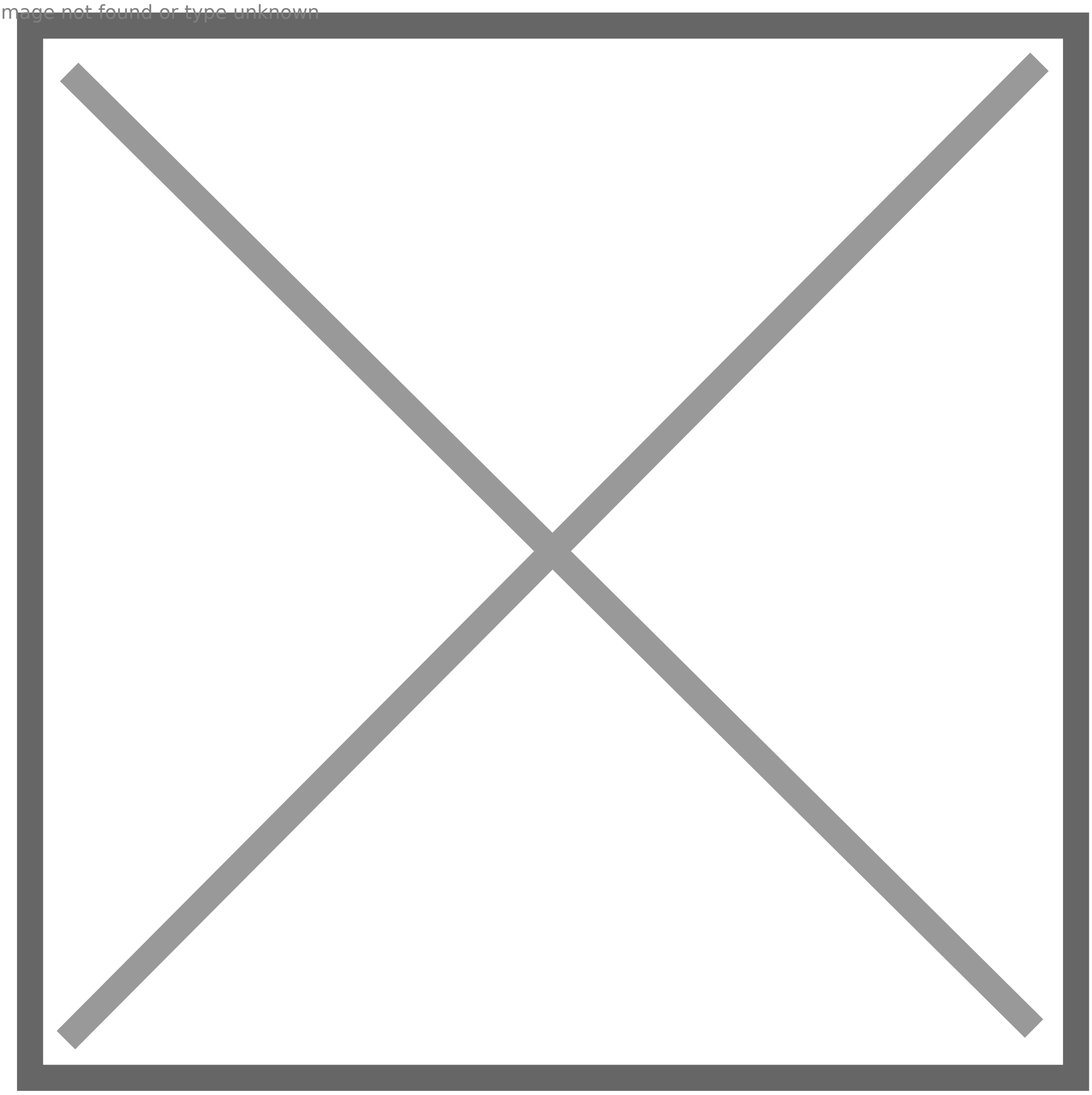
[Backup] How Did I Take Over CobaltStrike Servers

Hi folks, today I would like to share how I take over some Cobalt Strike TeamServers with Quake and Password Spray Attack. From the perspective of a threat hunter, it is good to track C2 servers on the Internet. From the perspective of a hacker, it is good to compromise a host, but it is better to compromise a C2 team server and then take over all compromised hosts connected to the team server : D

Recon
Before exploitation, we need to recon. Here I use Quake(https://quake.360.net) to find a list of Cobalt Strike with weak credentials. Quake is something which is similar to Shodan. The query sentence should be **response:“\x00\x00\xca\xfe” AND port: “50050”**
What does it mean? Quake will try some very simple passwords to connect to Cobalt Strike Team Server. If the authentication is successful, Cobalt Strike Team Server will return “\x00\x00\xca\xfe” in response. According to search results, there are 417 records, 191 unique IPs currently. Of course, if you do not specify the default port, you could get more results. To get complete and detailed information, a subscription of Quake is recommended.



After getting these results, then export IP of these Team Servers as a file. So, let’s use Password Spray Attack against these Team Servers!

Exploitation

Just a disclaimer, it is unethical and even illegal to actually take over those Team Servers. The article is just a proof of concept, it does not encourage anyone to pwn those servers, even they may belong to unethical hackers.

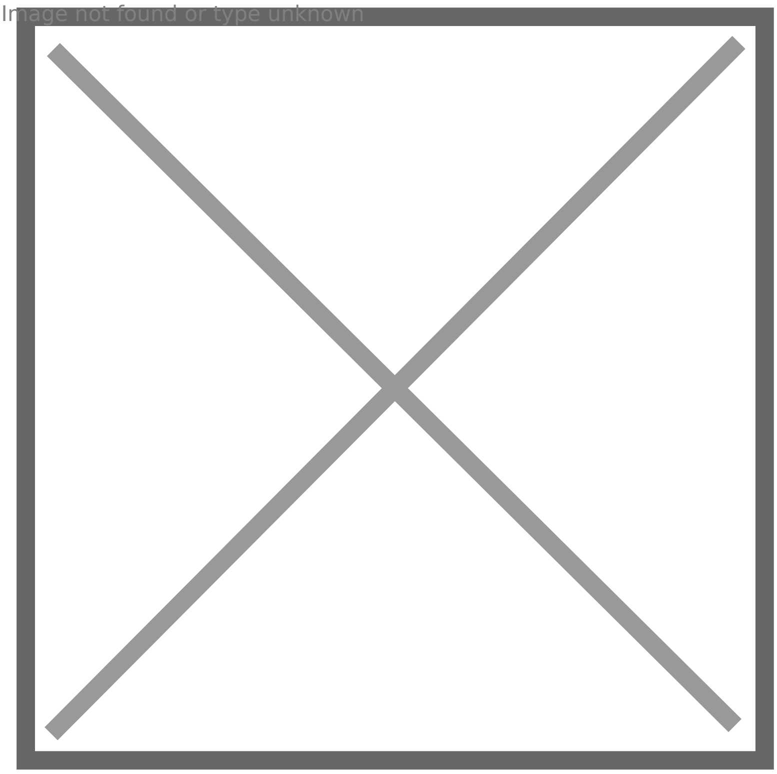
Because Cobalt Strike Team Server has rate limit, it is not wise to brute force a single Team Server with a big password list. Instead, we can use spray a single simple password to a list of Team Servers.

I download and modify a script from https://github.com/ryanohoro/csbruter to enable it to launch Password Spray Attack.

Image not found or type unknown

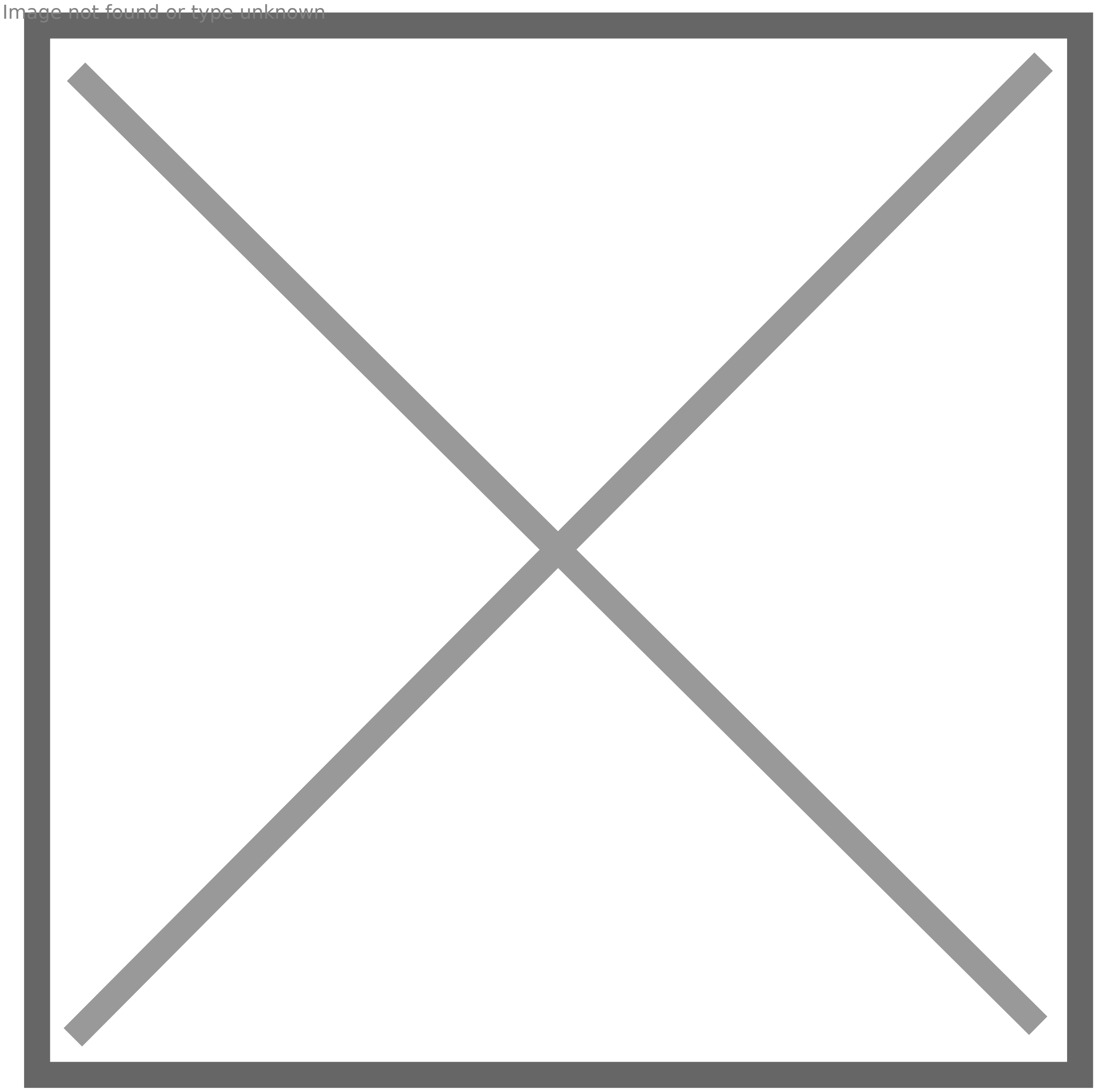
Image not found or type unknown

Oh, among these 158 Team Servers, 24 of them use the same simple password! Just select one and try to log in!



Oh no! The version of your client should match target Team Server's! Actually most of these Team Servers' version are 4.0 lol.

Try another one, cool, there are a lot of bots controlled by the Team Server! By this way we are able to successfully find and take over some Cobalt Strike Team Servers!



Tips

The list I used is absolutely not an exhaustive list of Team Server with a weak password. If you want to find more Team Servers with a weak password, here are some tips

1: Remove the specified port and modify the script.

2: If a Team Server does not show up in previous search results, it does not mean the Team Server has a strong password, since Quake will only try some simplest passwords like 123123, 123456, password, etc.

3: Just try different fingerprinting methods to get a large list of Cobalt Strike Team Servers, and then spray a single simple password to them. If you are lucky, you will take over many Team Servers from the list : P

Thanks for reading! Happy hacking!

Revision #1
Created 28 February 2024 19:38:16 by winslow
Updated 28 February 2024 19:38:48 by winslow