Team Texas Offense Report 3/27

Overview:

In our offensive operation, Operation Lateral, our goal is to gain access to as many of our adversaries Linux systems as possible by exploiting back door accounts used by red team.

Objective:

The objective is to abuse two accounts, "weblclient", which was discovered to be an attack used by red team (discussed in our previous incident response report), and "cron", an account that gives access to a nologin shell with some administrative privileges, to install persistence on as many Linux systems of our adversaries that still contain the account. When discussing with our alliance team New York, we discovered that this account is a reoccurring attack plaguing multiples system.

Recently, to recover root privileges on our Auto workstation, we were able to crack the password hash of this account, giving us access to this user. Upon further investigation, it was found that the password used is the same password across all Linux systems.

We were also able to discover a back door with in the account "cron" found inside the shadow file of all of our linux systems.

We believe these accounts have the same passwords on all infected systems, including our adversaries, which we plan to abuse to obtain escalated privileges onto their system.

Targeted Machines:

Since the attack has been found to plague all linux systems, the goal is to target as many Linux systems as possible to increase the odds of success of this attack. Below is a list of all Linux system IP's (discovered by nmap) we plan to initiate the attack on:

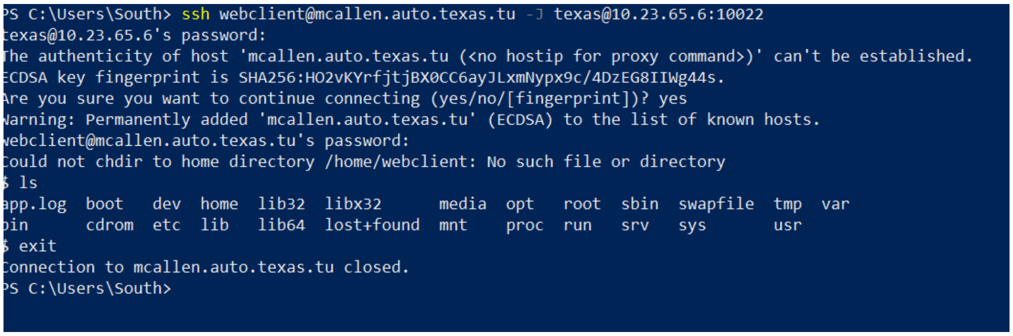
Team	IP Address
California	172.17.71.56
California	172.17.71.59
California	172.17.71.93
California	172.17.71.114
California	172.17.71.145
California	172.17.159.7
California	172.17.159.197

Team	System IP
Florida	172.19.229.17
Florida	172.19.229.79
Florida	172.19.229.162
Florida	172.19.229.229
Florida	172.19.229.248
Florida	172.19.203.122
Florida	172.19.203.138
Florida	172.19.203.34
Florida	172.19.114.13
Florida	172.19.114.4
Florida	172.19.101.29

Team	IP Address
Illinois	172.21.11.139
Illinois	172.21.43.153
Illinois	172.21.155.95
Illinois	172.21.155.134
Illinois	172.21.190.38
Illinois	172.21.190.51
Illinois	172.21.190.52
Illinois	172.21.190.144
Illinois	172.21.190.146
Illinois	172.21.190.206

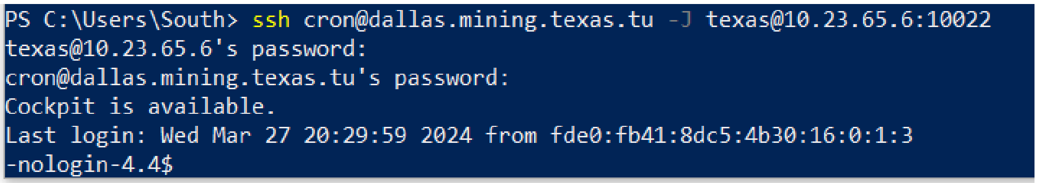
Phase1: Initial Access:

Initial Access will be received by abusing two accounts. The first is a user account called “webclient”. Upon being prompted for the password, we will use the password used for the account on our system. The screenshot below shows we can access the account:



```
PS C:\Users\South> ssh webclient@mcallen.auto.texas.tu -J texas@10.23.65.6:10022
texas@10.23.65.6's password:
The authenticity of host 'mcallen.auto.texas.tu (<no hostip for proxy command>)' can't be established.
ECDSA key fingerprint is SHA256:HO2vKYrfjtjBX0CC6ayJLxmNypx9c/4DzEG8IIWg44s.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'mcallen.auto.texas.tu' (ECDSA) to the list of known hosts.
webclient@mcallen.auto.texas.tu's password:
Could not chdir to home directory /home/webclient: No such file or directory
$ ls
app.log  boot   dev  home  lib32  libx32      media  opt   root  sbin  swapfile  tmp  var
bin      cdrom  etc  lib   lib64  lost+found  mnt    proc  run   srv   sys       usr
$ exit
Connection to mcallen.auto.texas.tu closed.
PS C:\Users\South>
```

The second is cron, what we believe to be a backdoor planted by red team inside shadow. Logging into the account gives us a nologin shell, however, we have permissions to edit sensitive files like passwd and shadow and has the ability to change passwords with passwd. An example is shown accessing the account from our mining system:



```
PS C:\Users\South> ssh cron@dallas.mining.texas.tu -J texas@10.23.65.6:10022
texas@10.23.65.6's password:
cron@dallas.mining.texas.tu's password:
Cockpit is available.
Last login: Wed Mar 27 20:29:59 2024 from fde0:fb41:8dc5:4b30:16:0:1:3
-nologin-4.4$
```

If successful, we will have obtained initial access on the targets system. If it fails, then we will know that the Team has either deleted the accounts or changed their passwords, in which we will switch the target to the next Linux system.

Phase 2: Escalation:

In all records of attacks, the Red Team has given these accounts administrative privileges and configured them to be included in the group sudoers. If configured similarly on other systems, no privilege escalation should be needed as we will already have the highest level of authority.

If escalated privileges has been revoked, the system will be noted and the next system in the list will be attacked. After attacking all the systems, all noted systems will be circled back to and attempts will be made to find misconfigurations to escalate to root.

Phase 4: Persistence:

Persistence will be like our previous attack, planting public keys in multiple administrative accounts, including root. This way, if the password of the account is ever changed, we will still have a way to access their system.

Another method that will be attempted is planting a bash script call inside the .bashrc file of their root user. This way, every time root is logged into, the bash script will replace our public key inside the file in the event it's deleted.

(Conditional) Phase 5: Execution:

The core goal is to obtain access to as many Linux systems as possible. That makes it tough to determine what data to exfiltrate/target. However, there are some general rules of data exfiltration that we will follow:

1. du command will be run on the home directories of all users to search for accounts that are abnormally sized, likely sensitive data stored in their local accounts to exfiltrate.

2. Mozilla contains roaming data for each user's browser history. We can exfiltrate this data and determine if this is a system the adversaries use to access sensitive websites like Nagios and the bank. There is also a chance that credentials are saved within the

files and can be directly exfiltrated. Otherwise, future operation plans can then be made to install keyloggers on the system to attempt to steal their passwords.

3. Passwd and shadow are also valuable targets to exfiltrate as the password hashes can be cracked. This could give us access to the adversaries' IT accounts or the passwords to one of their users, in which case we would need to crack their password prefix and have access to every system.

4. If the system is a samba file share, then we can exfiltrate sensitive data found within the file share section, including flags, operation plans, and incident responses.

5. If the system is a bind server, then we can exfiltrate their zone data or potentially create a new operation plan to redirect one of their zones to a malicious site.

Phase 6: Evasion:

Evasion for this attack is very limited. The initial attack will be loud, since attempting to access multiple machines from the same account will be logged by graylog. Therefore, the goal will be to hide the persistence of the attack, renaming any bash scripts to mimic system processes and deleting any logs of local commands as much as possible.

All these phases will be repeated for every system listed. A post operations plan will contain all systems accessed and all the data we were able to exfiltrate.

Benefits of this attack:

The biggest benefit of this attack is it's simplicity and effectiveness. No initial setup must be created on our end and due the nature of the attack and almost every linux system of our adversary can be attacked. If the initial access fails, we can simply move onto the next system in the list.

Once we obtain initial access, escalated privledges should already be obtained, meanining in most cases we can move straight to persistence and data exfiltration.

Finally, this attack allows for a high yield of systems to be compromised. If the malicious account hasn't been discovered on one linux system, theres a high chance it hasn't been deleted on the rest, creating a domino affect of compromised systems. This also means that our adversaries will have to find every planted on every compromised system to kick us out.

Consequences with this attack:

This attack relies heavily on the back doors still being present on our adversaries' systems. While we have the benefit of numbers, being able to attack multiple systems, theres also a chance that every discovered linux system from our adversaries have patched or deleted the accounts, making our operations plan a failure.

Due to how loud the attack is, it could also be discovered by our adversaries and revealed within the indicators of compromise. This could put us on a timer, or potentially cause our attack to be compromised.

Summary:

This attack has the potential to compromise many systems, but relies on Red teams persistence and our adversaries negligence to remove the accounts. Due to the nature of the attack, this should be completed very easily, allowing us to move onto a backup operation in the event it fails.