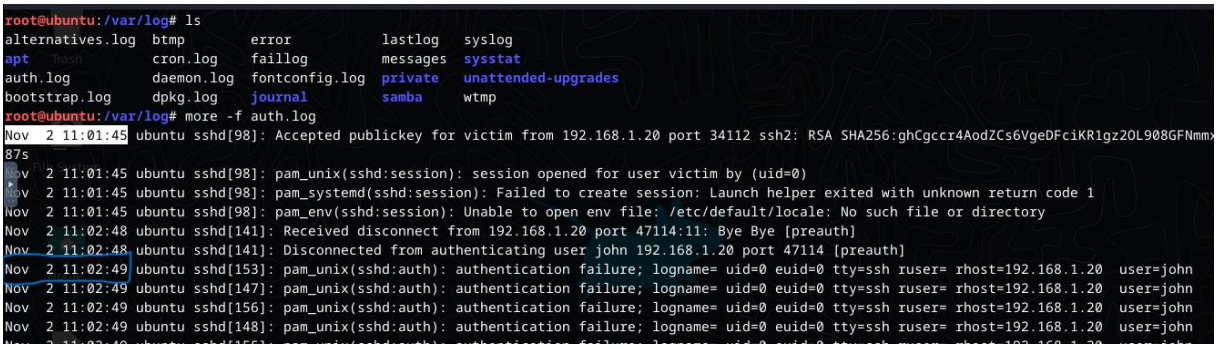
BLUETEAM INCIDENT ANALYSIS GAME REPORT

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.

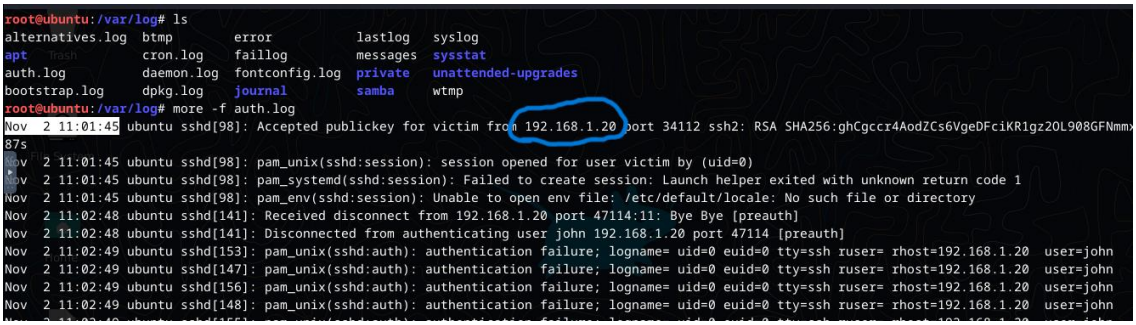


Şekil 1

- 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



Şekil 2

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

Flag 3

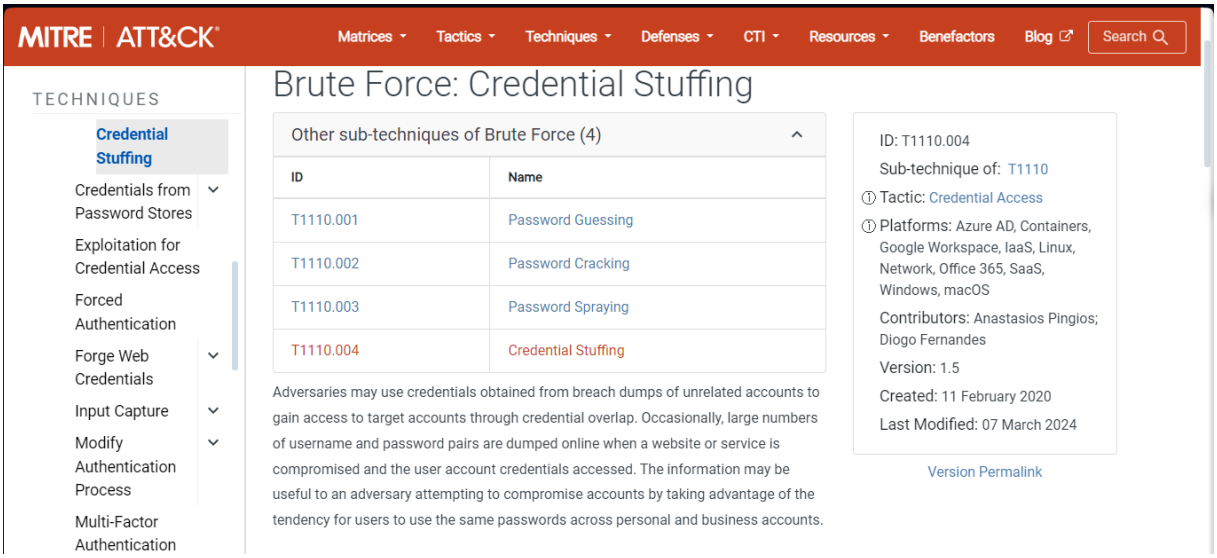
Şekil 3

- **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



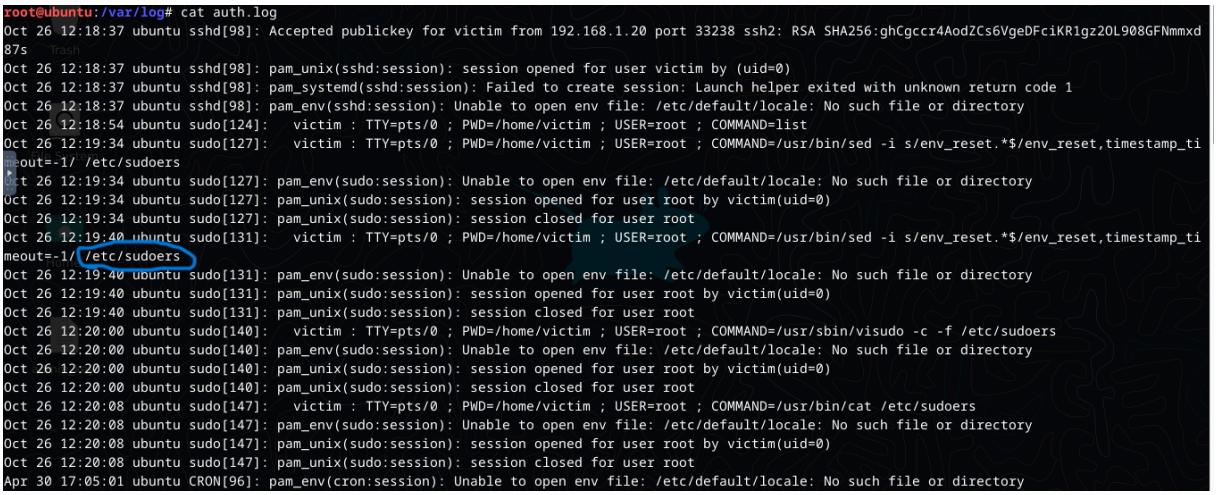
Şekil 4

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

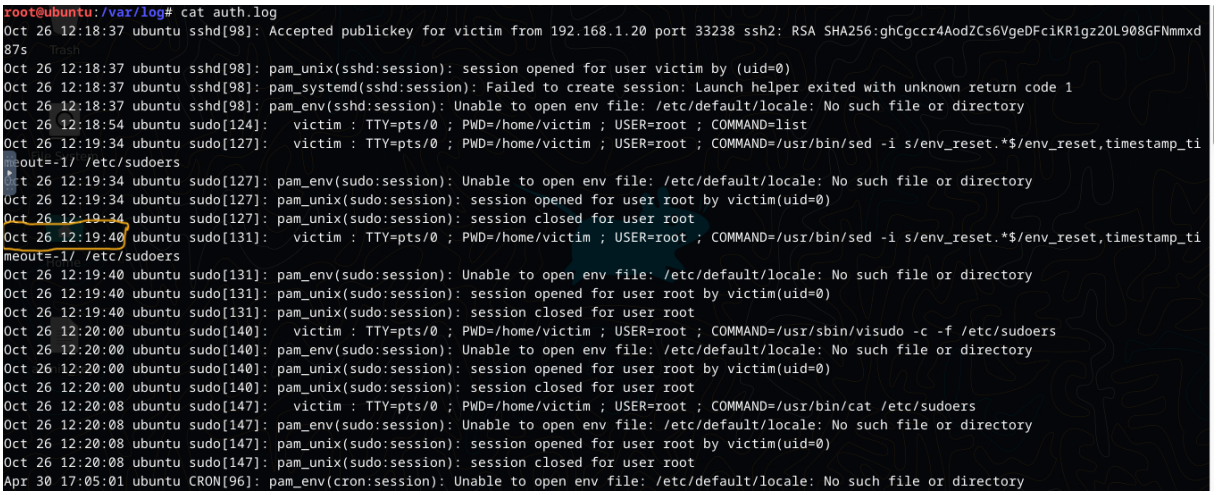
İkinci makineye bağlanmak için yukarıdaki komutu kullanıyoruz. Daha sonra sistemde kimlik doğrulama bilgileri ve kullanılan komutları da görüntüleyebilmek için tekrardan **/var/log** dizini altında bulunan **auth.log** dosyasını okuyoruz.



Şekil 5

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

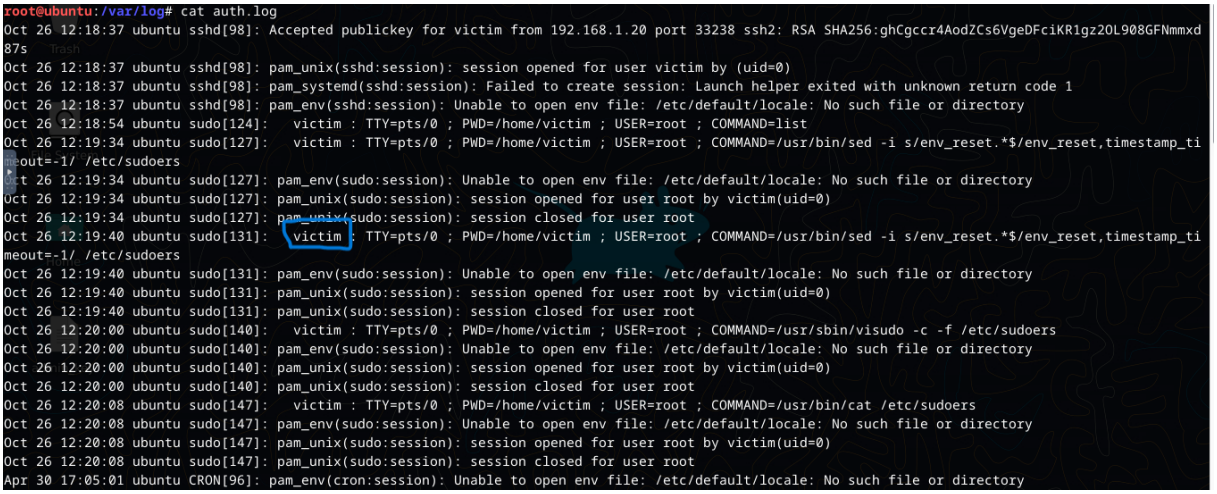
Flag 6



Şekil 6

Şekil 6'ya bakıldığında **Oct 26 12:19:40** tarihinde /etc/sudoers dosyasının son olarak değiştirildiği görülür.

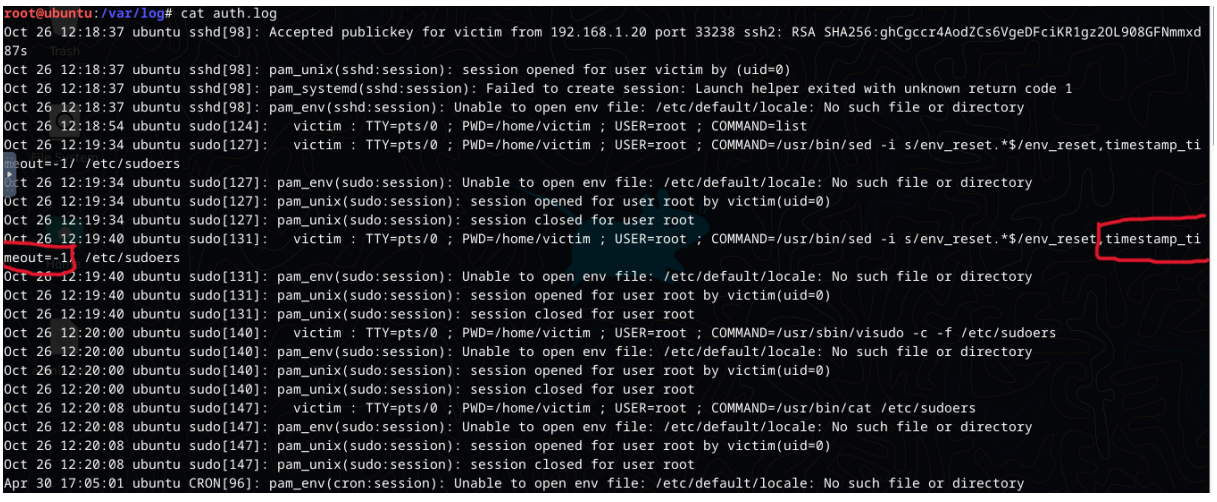
Flag 7



Şekil 7

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

Flag 8

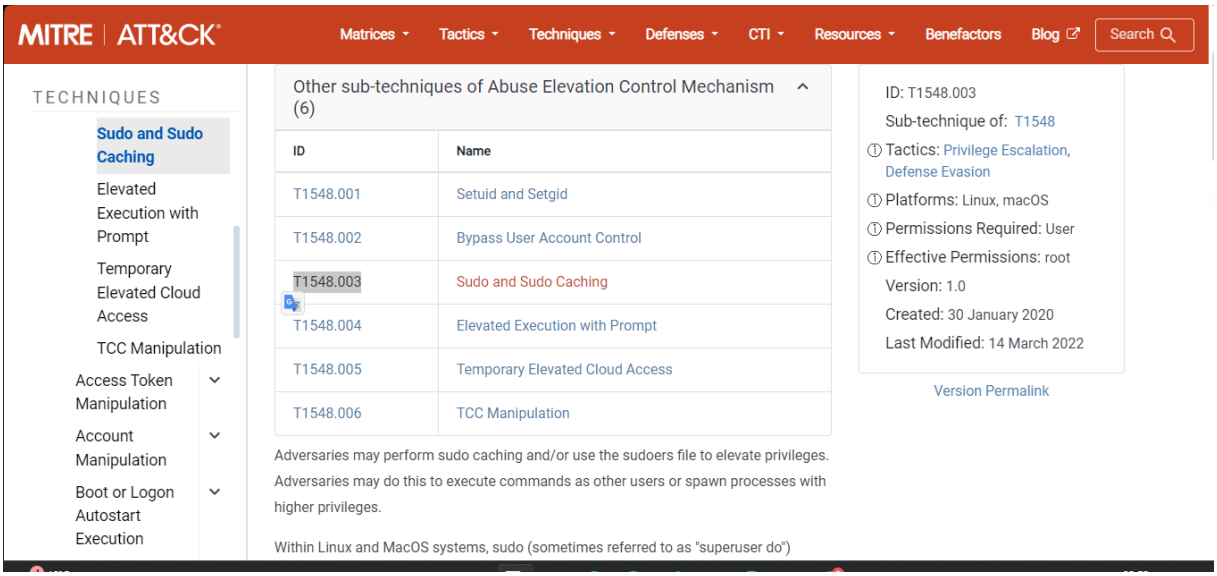


Şekil 8

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

Flag 9

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



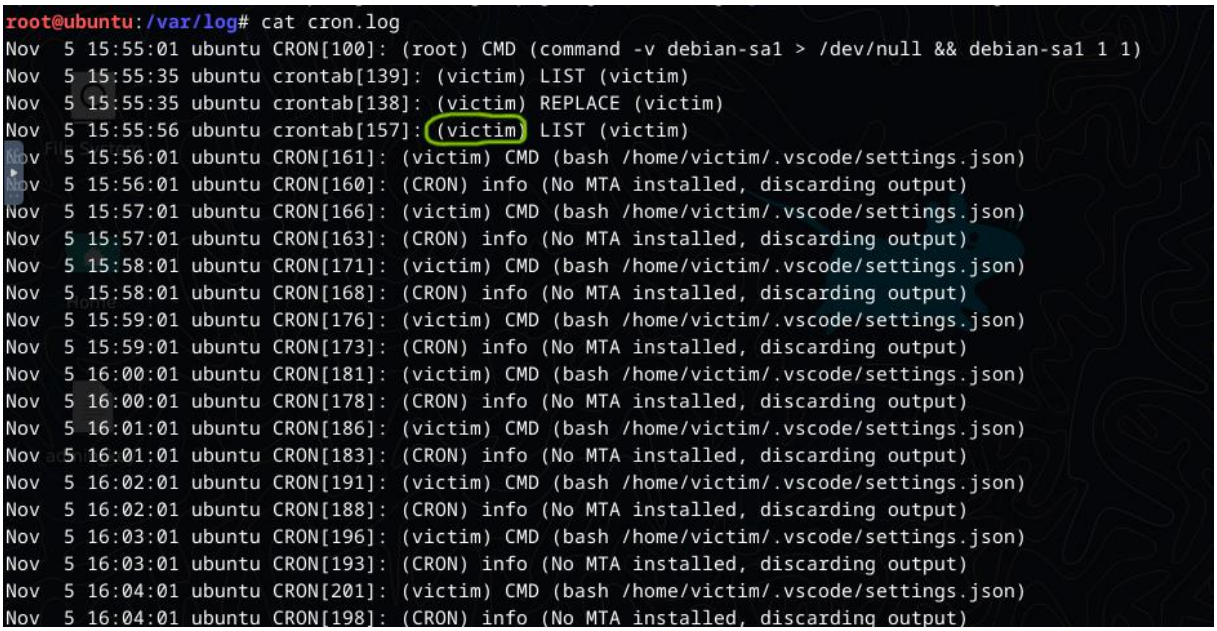
Şekil 9

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

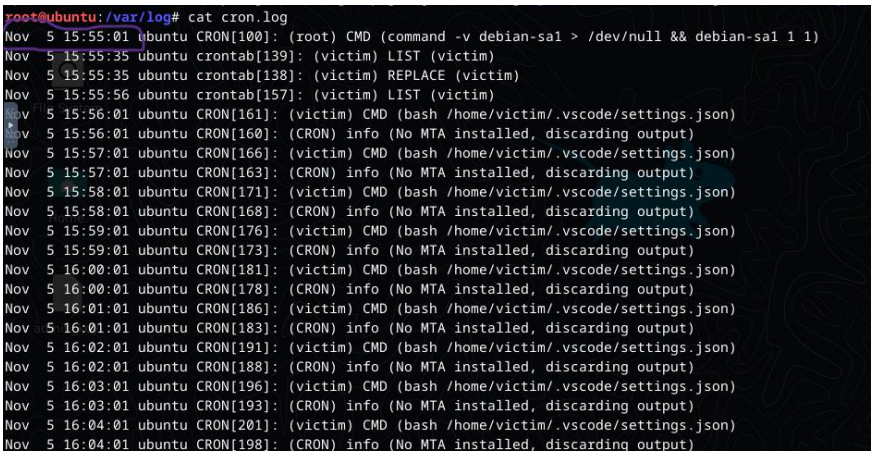
Üçüncü makineye bağlanmak için yukarıdaki komut kullanılır. *Cron* bir görevi ilerleyen bir zamanda tekrarlamak için kullanılan bir programdır. Belirli bir görevi belirli bir zamanda tekrarlamak için komut verme eylemine ise *Cron job* adı verilir. *Cron job* kayıtlarına */var/log* dizini altında bulunan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



Şekil 10

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

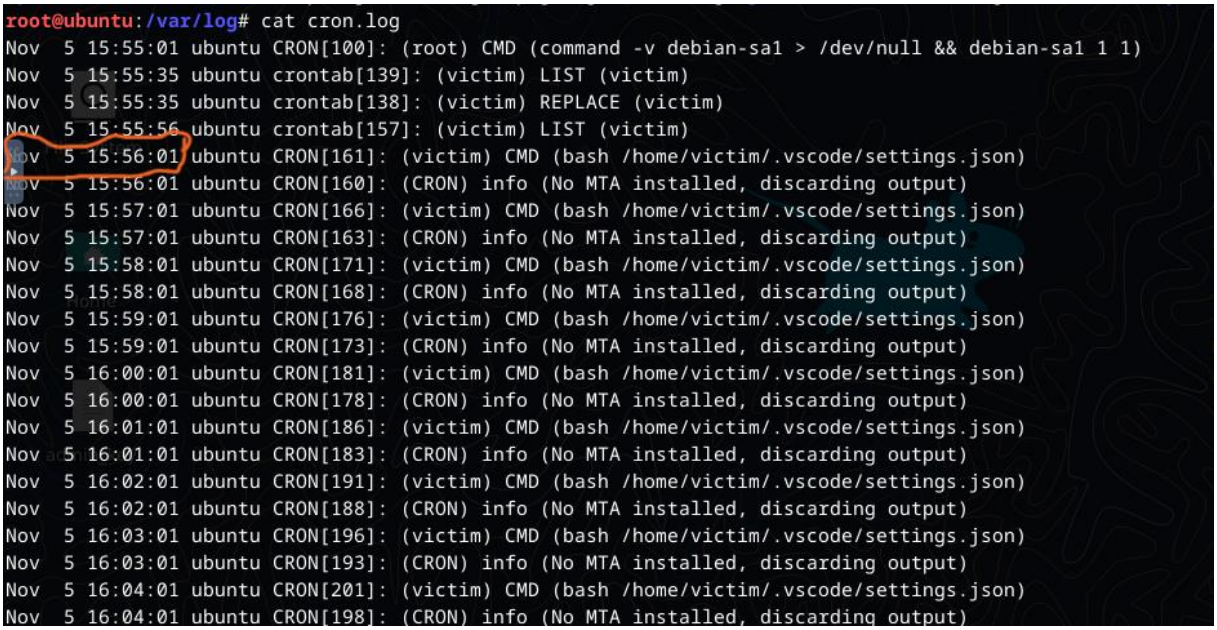
Flag 11



Şekil 11

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

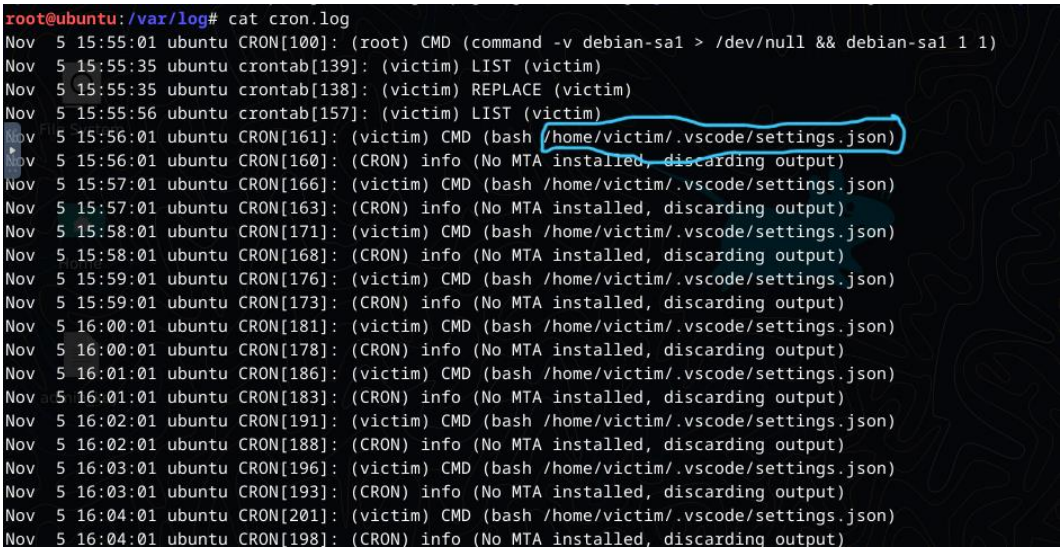
Flag 12



Şekil 12

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

Flag 13



Şekil 13

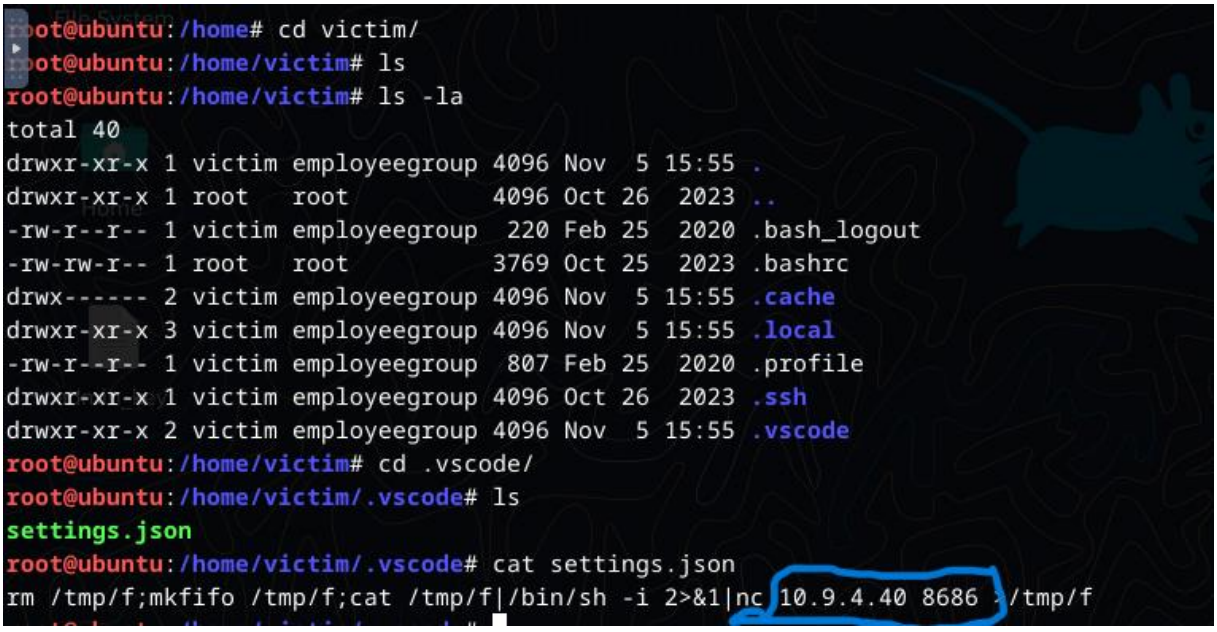
Şekil 13'te de görüldüğü üzere *cron job*'ın kullanıldığı dosya **/home/victim/.vscode/settings.json** dosyasıdır.

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.)

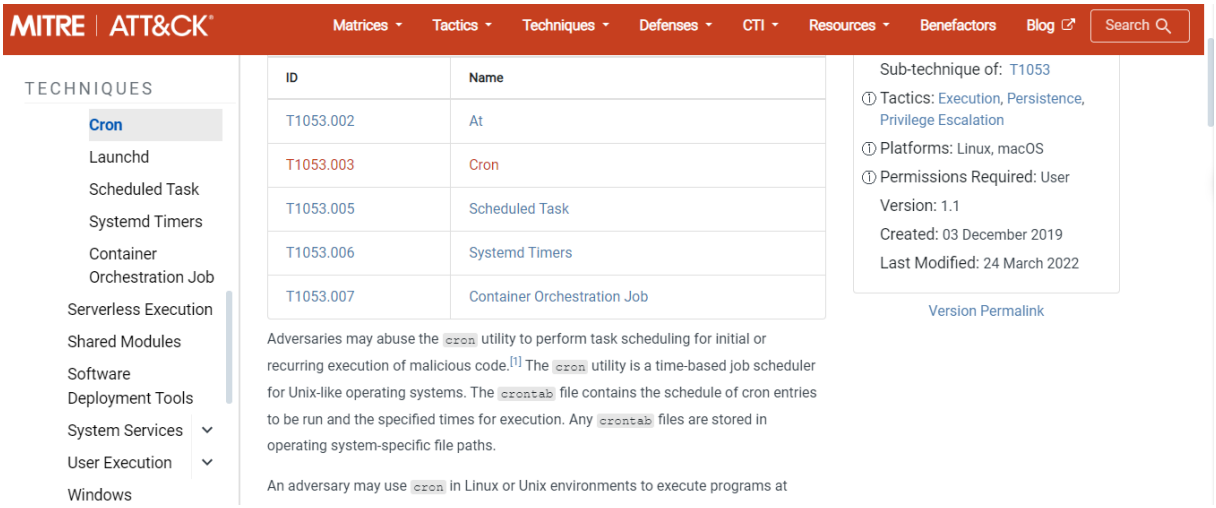
Flag 15



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



Şekil 15

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

(Platform cevabı Flag Değeri olarak Kabul Etmedi.)