SSH Attacks

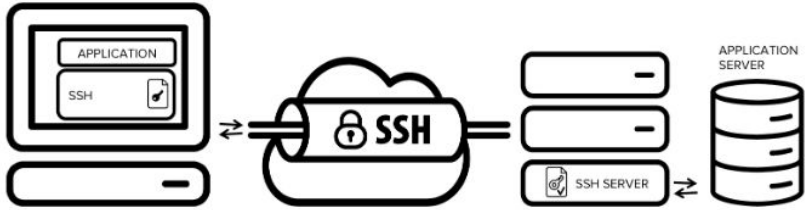
Técnicas de Percepção de Redes

MIECT

Ana Luísa Ferreira, Nº93301
João Gameiro, Nº93097

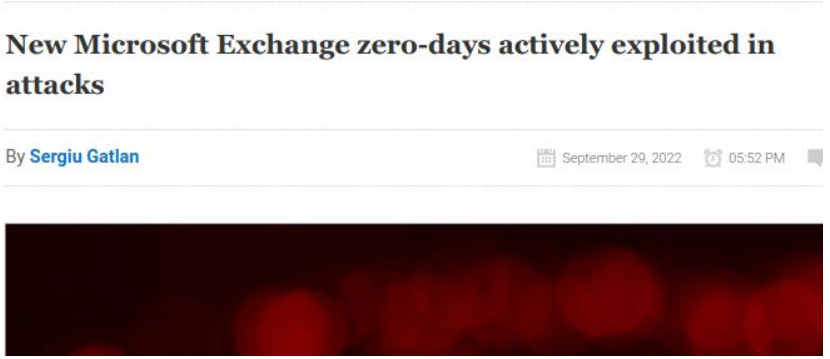
9 November 2022

What is SSH?



- SSH is a software package that enables system administration, file transfers and secure communications over insecure networks. It is used in nearly every data center and in every large enterprise.
- The SSH protocol uses encryption to secure the connection between a client and a server.
- All user authentication, commands, output, and file transfers are encrypted to protect against attacks in the network.

Real World Scenario



Microsoft Exchange Server is a mail server and calendaring server developed by Microsoft.

It contains two zero-days vulnerabilities:

- CVE-20022-41040 - an attacker can increase their privilege on the affected machine.
- CVE-2022-41082 - an attacker can get access to remote code execution.

Our Scenario

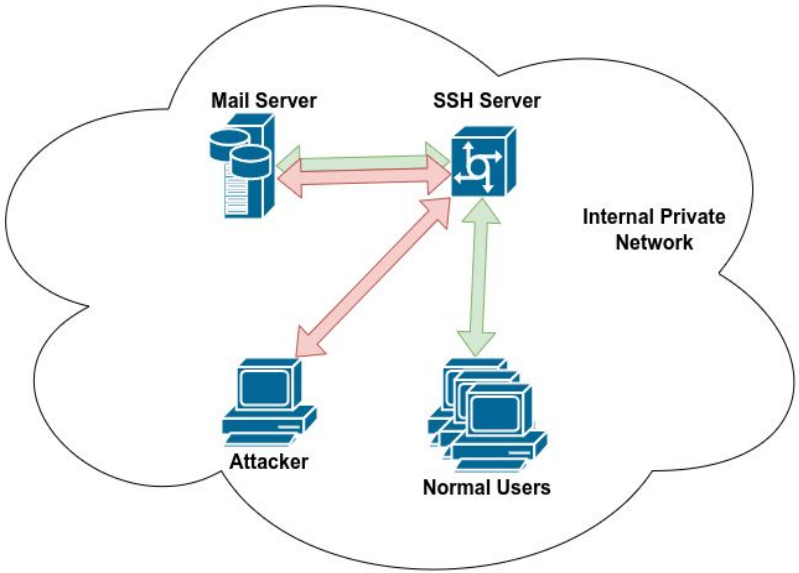
We assumed:

- Using SSH connections inside the company is a normal behaviour.
- Users use the ssh connection to open, close, edit files, travel through directories, etc…
- The attacker got access to a normal machine.
- He changed his permissions.

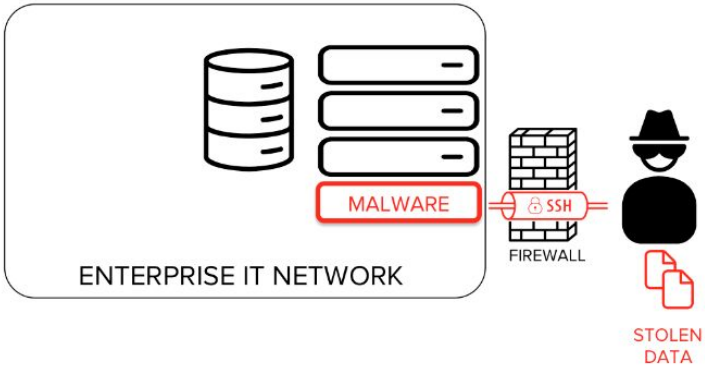
1º Scenario: begins to copy files (scp command) which incites abnormal behaviour.

2º Scenario: encrypts files that are on shared folders (ransomware).

- A normal user behaviour will be used to build a profile
- Deviations from the profile will be identified as abnormalities (Anomaly Detection)



Importance of the security issue/solution



- SSH traffic is protected with strong encryption, therefore is invisible which represents a problem in terms of detecting data exfiltration.
- Hackers can hide the source of the attack.
  - They can try several logins, run attack tools against company services and all is encrypted and untraceable.
- Anyone who is capable of logging in to the SSH server is capable of enabling port forwarding.
  - Hackers use it to leave a backdoor into an internal network.

Data sources

- Capture the SSH Traffic
- Check firewall logs
- SSH server logs
    - However this may be a non-viable option because the ssh server may be compromised by the attacker

Metrics to extract

- Number of TCP/SSH packets
  - Source and destiny IP addresses
    - Identify users and download/upload packets
    - Check for weird IPs
  - Source and destiny ports
    - Check for weird ports, others than 22
  - Packet size
    - Check for abnormalities in the size
  - Packet timestamp
    - To find relations between events and time
- SSH Server logins

Features

- Number of SSH/TCP packets
  - Mean, median, variance
  - Maximum number of packets in a certain time frame
  - Quantiles/Percentiles (98%, 95%, ...)
  - Periods of silence
  - Mean, median, variance of the silence periods
- Upload/Download packets
  - Mean, median and variance
  - Quantiles/Percentiles
  - Duration of the transfers

Features

- Packet size
  - Mean, median and variance
  - Quantiles/Percentiles
  - Maximum packet size
- SSH Logins
  - Duration of the session. Number of logins by a certain user
  - Mean, median and variance of the session duration
  - Users that are logged in

Observation Window

- Sliding window
  - So abnormalities can be detected as fast as possible
- Size of 2 / 3 minutes in order to detect abnormalities in normal behavior
  - Decision period of 5 seconds
- Considering a sampling period of 1 second to gather data

Bibliography

- SSH Tunneling: https://www.ssh.com/academy/ssh/tunneling
- SSH Home Page: https://www.ssh.com/academy/ssh
- Microsoft Server attack:
  - https://www.bleepingcomputer.com/news/security/microsoft-exchange-server-zero-day-mitigation-can-be-bypassed/
  - https://www.bleepingcomputer.com/news/security/new-microsoft-exchange-zero-days-actively-exploited-in-attacks/