**HEADS EMPTY**

**CPA (The Circle for the Protection of Antarctica)**

**INCIDENT RESPONSE REPORT**

**Contents:**

1. [Introduction](#nw38kerwngfl)
2. [ORCA - Rocky Desktop](#5uj0r8mb129)
3. [PENGUIN - Windows 10](#qi3f14igc84m)
4. [SQUID - Windows Server 2022](#btnkebganrkx)
5. [ALBATROSS - Arch Linux](#123uamly6dj7)
6. [Final Thoughts](#fpkc1sdaw3im)

**Introduction**:

Throughout our investigation there were several signs of SEAL within our network. This report outlines incidents that our team found and the several efforts we made to mitigate them. An incident is defined as “a cybersecurity event that has been determined to have an impact on the organization prompting the need for response and recovery.” Associated with each incident, we have:

* The affected host: who on the network was affected?
* The event: a description of what occurred
* Severity: how urgent and serious was the incident?
* Remediation: how quickly it was resolved (N/A if the incident was unresolved)
* Incident Identification: Screenshot proof
* Incident causes: what were the reasons for the incident occurring?
* Responses taken: what was done to address the issue (and if it wasn’t solved, what could have been done)
* Lessons learned

**Affected Host: Orca**

**Event:** Vulnerable local users

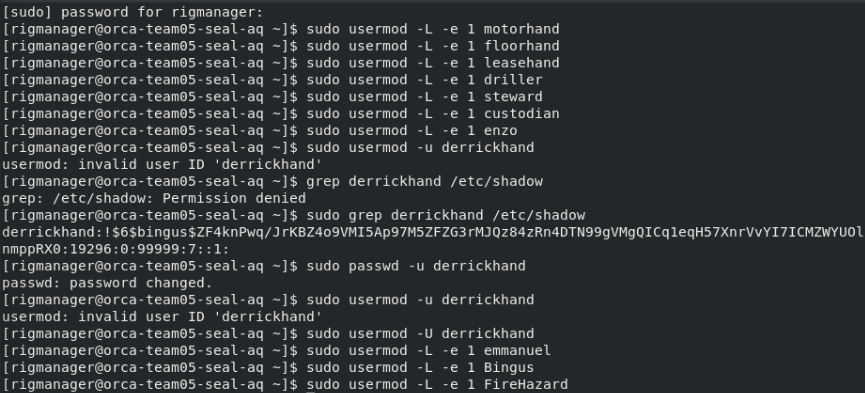
**Priority:** MEDIUM

**Initial Detection:** 9:42 AM EST

**Remediation:** Immediate

**Incident Identification:**

Using IRSeC packet, our team identified that there were many local users with default passwords.



**Incident Causes:**

Default setup by SEAL member

**Responses Taken:**

Locked/Disabled all of the local users and all but two local admins by using the sudo usermod -L -e 1 <username> command

**Lessons Learned:**

Have the least number of users necessary to use a box, since pre-existing users with permissions set by the SEAL member are dangerous.

**Event:** Vulnerable local users

**Priority:** MEDIUM

**Initial Detection:** 9:47 AM EST

**Remediation:** Immediate

**Incident Identification:** Using /etc/shadow, identification of additional users took place in which there was a “redteam” and “notredteam” malicious users.





**Incident Causes:**

Default setup by SEAL member

**Responses Taken:**

Locked/Disabled the local users that seemed malicious based on their naming conventions

**Lessons Learned:**

Have the least number of users necessary to use a box, since pre-existing users with permissions set by the SEAL member are dangerous.

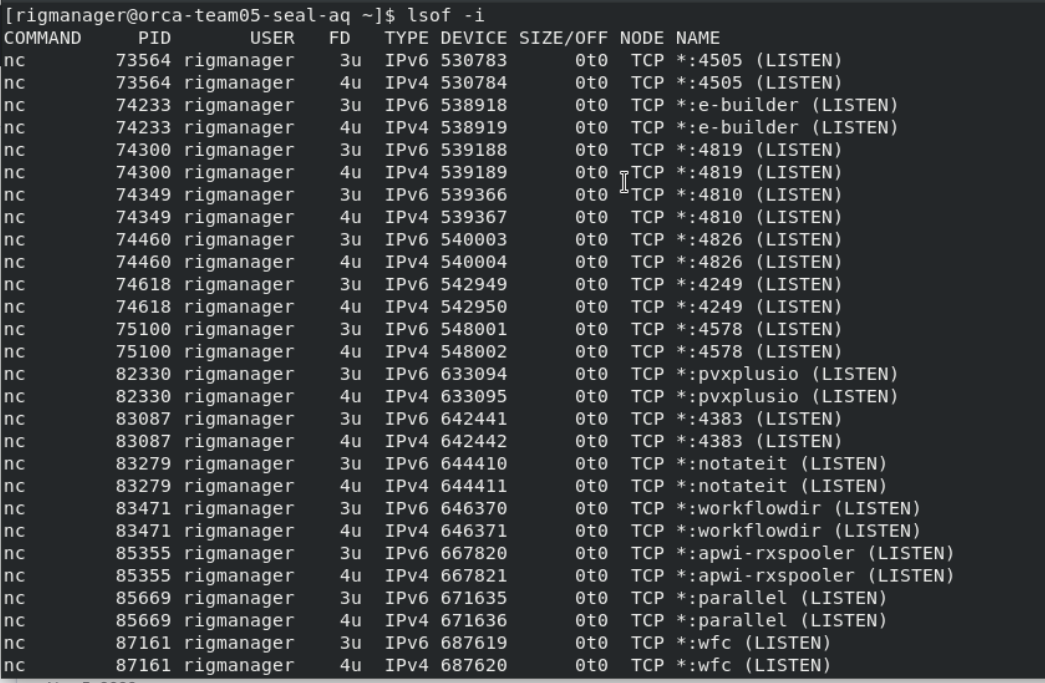
**Event:** Netcat backdoor installed by SEAL’s

**Priority: HIGH**

**Initial Detection:**  10:42 AM EST

**Remediation:** N/A

**Incident Identification:** Used “lsof -i” which lists open files in Linux and shows which processes are using them.



**Incident Causes:**

Default network configurations left this host susceptible.

**Responses Taken:**

Found binary file location for netcat/nc which was /usr/bin/nc, and tried to delete this file.

**Lessons Learned:**

Always check which processes are using certain open files.

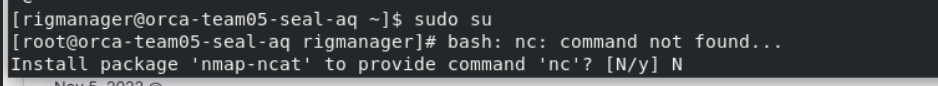
**Event:** Hook to get netcat installed

**Priority:** MEDIUM

**Initial Detection:** 11:02 AM EST

**Remediation:** N/A

**Incident Identification:**



**Incident Causes:**

Default network configuration.

**Responses Taken:**

Used control C since every time “N” was selected it would prompt the user again and start lagging the system.

**Lessons Learned:**

Always check which processes are using certain open files to mitigate potential issues that may arise later on, at the start of the competition.

**Event:** SSH is down

**Priority:** HIGH

**Initial Detection:** 11:30 AM EST

**Remediation:** Immediate

**Incident Identification:**



Unable to ssh into my own box albatross to find more info.

**Incident Causes:** Several files needed to run the ssh service were deleted

**Responses Taken:** Tried to restart ssh using systemctl restart “ssh”, tried to restart “sshd” the same way. It was deemed that certain files needed to run the ssh service were deleted, therefore, our team reverted the box with the help of the SEAL member.

**Lessons Learned:**

Be sure to clarify to all team members to be more careful of deleting essential files needed to run basic services.

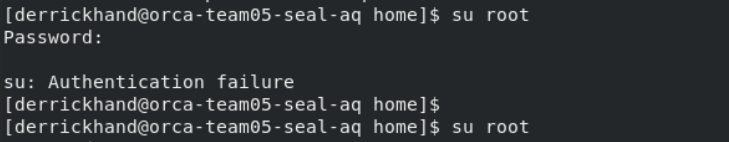
**Event:** Authentication failure

**Priority:** MEDIUM

**Initial Detection:** 1:17 PM EST

**Remediation:** Immediate

**Incident Identification:**



**Incident Causes:**

Malicious actors from SEAL’s team changed the root password which resulted in an authentication error since this password was also not updated on scorestack.

**Responses Taken:** used the “exit” command two times to get back to when I ssh’d into orca from orca to find more clarity on another error. This action took me back to root.

**Lessons Learned:**

When the default password for any user is changed, keep changing it every two hours to lessen the chances of the SEAL’s team identifying what the password for that user is, whether that password was changed already due to a team member following their 5-minute plan.

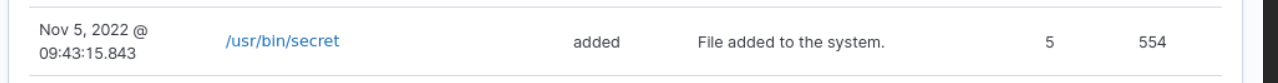
**Event:** File added to system

**Priority:** LOW

**Initial Detection:** 9:43 AM

**Remediation:** N/A

**Incident Identification:**



**Incident Causes:**

SEAL’s team added a file into the system early on in the competition before all local users were locked.

**Responses Taken:** N/A

**Lessons Learned:**

Continuously check Wazuh for logs of incidents, so responses can be taken as soon as an event that is deemed malicious can be resolved.

**Affected Host:** **Penguin**

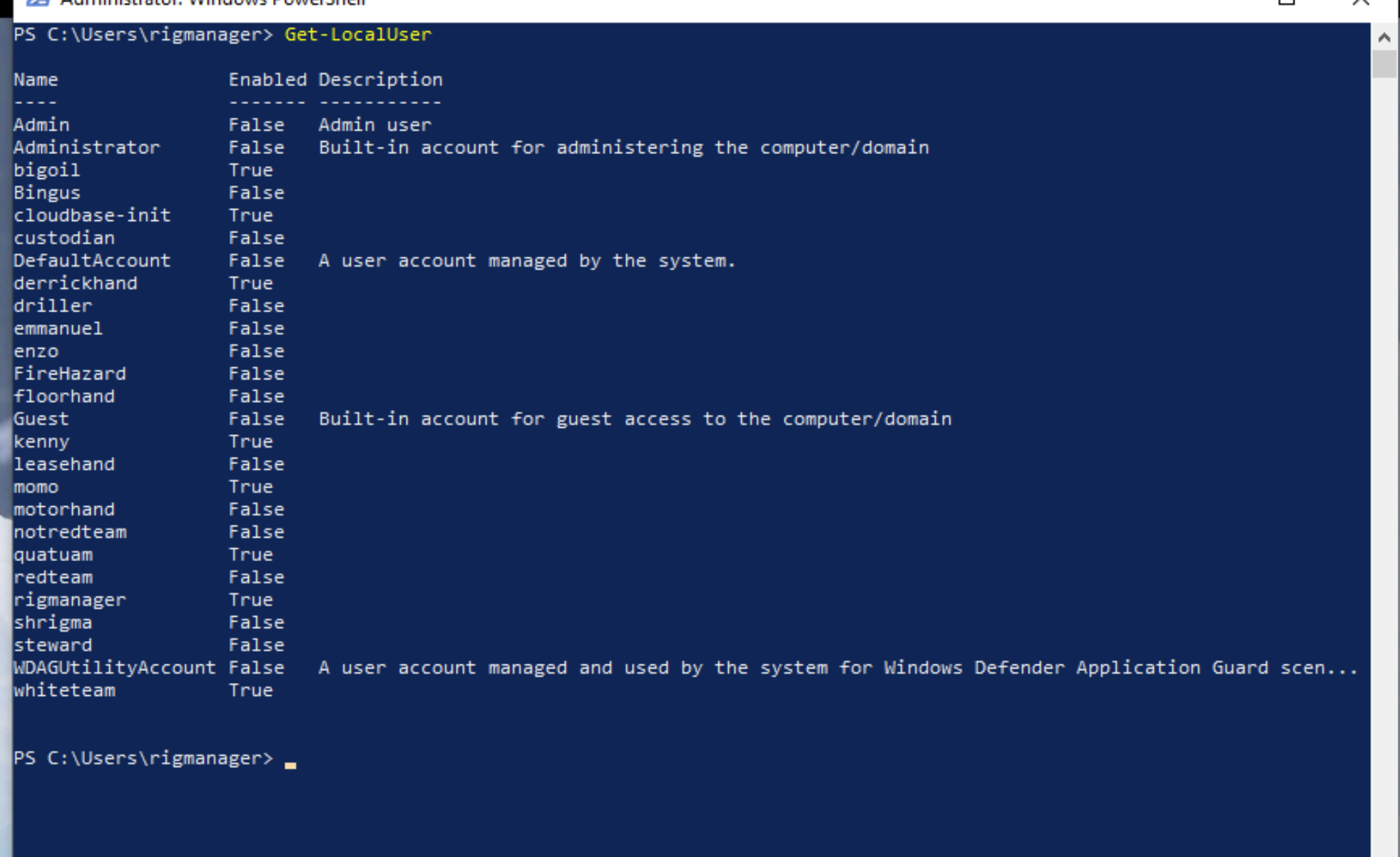
**Event:** Suspicious and Likely Malicious Users

**Priority:** High

**Initial Detection:** 9:42 AM ET

**Remediation:** Immediate

**Incident Identification:** As seen in the below screenshot, there are a lot of users on this box. This includes some with suspicious names like “redteam” and not “notredteam”. Additionally, to start the admin user was enabled



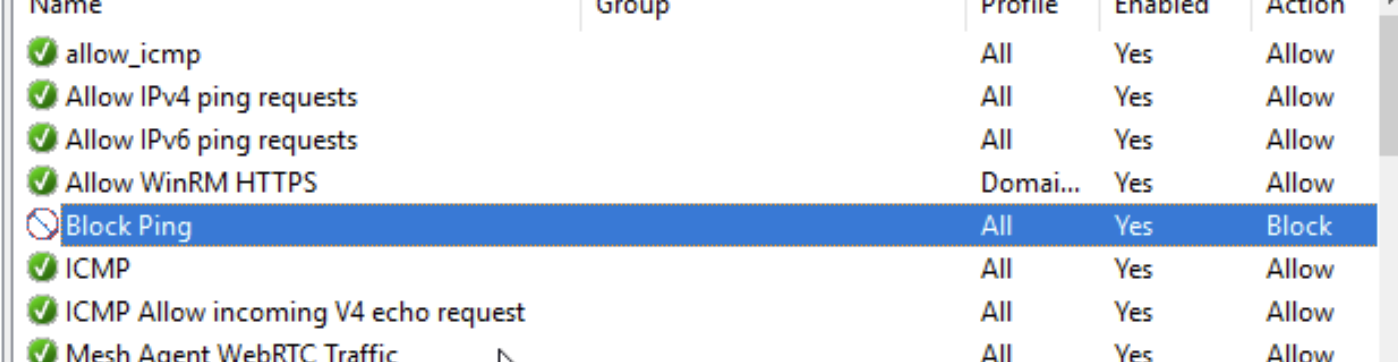
**Incident Causes:** Initial configuration of the box was set up for the SEAL member.

**Lessons Learned:** We must be careful about the starting configuration of the box and take immediate action to fix obvious security issues.

**Event:** Firewall rule blocking ICMP

**Priority: High**

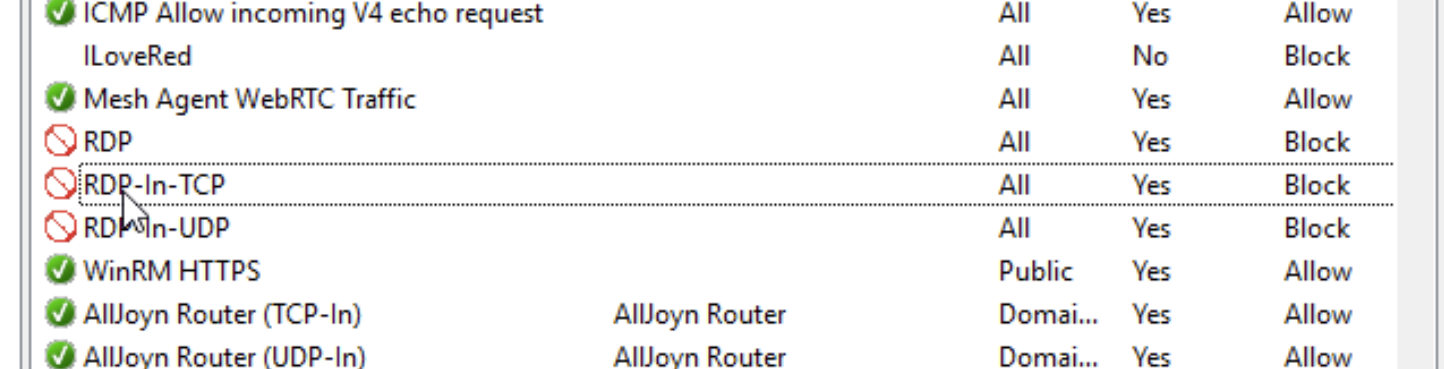
**Initial Detection:** 11:10 AM ET



**Remediation:** Immediate

**Response Taken:** Our team disabled this rule and also instituted another rule to implicitly allow ICMP, as shown at the top of the screenshot above. This is to better ensure that ICMP will always be allowed through our firewall and the scoring check will stay up.

**Incident Causes:** Seal members likely had access through something like RDP. After preventing RDP access to the box, the ICMP score check stayed up for the rest of the competition. These firewall rules blocking RDP are shown below.



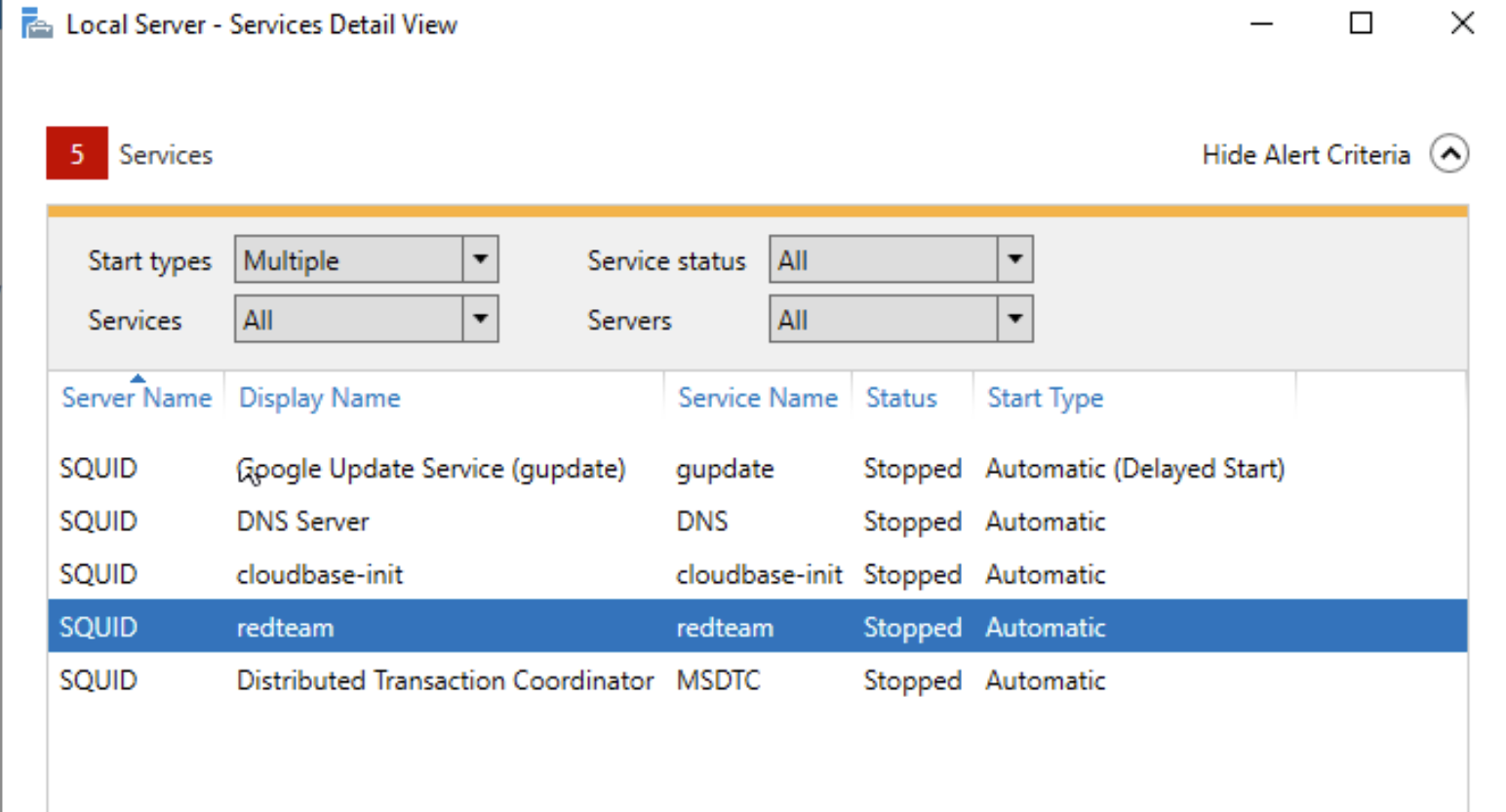
**Lessons Learned:** Firewalls are very powerful and an easy way to bring services down. However, they can also be used to prevent SEAL member access and to keep scoring checks up.

**Affected Host: Squid**

**Event:** DNS Repeatedly Goes Down

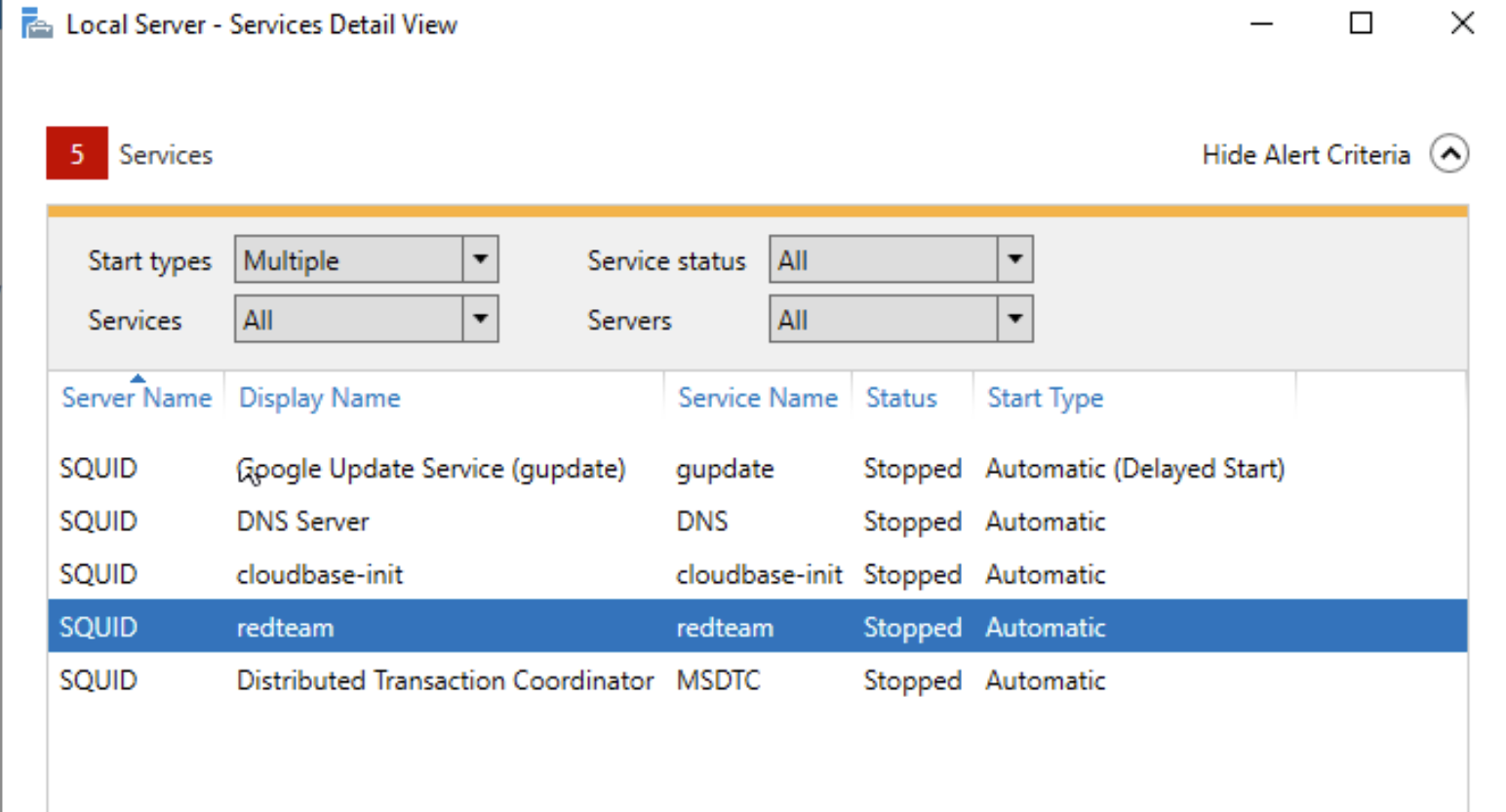
**Priority: MEDIUM**

**Initial Detection:** 11:00 AM ET



As seen above, DNS has been stopped by SEAL members.

**Remediation:** Restarting DNS/the machine would reliably bring back DNS in this scenario. In order to prevent SEAL members from messing with DNS in the future we needed to kick them off the box. As seen below, they had some sort of service running.



**Incident Causes:** This “redteam” service likely had something to do with it. By stopping this service, restarting the machine we could take back control of the machine from the SEAL members.

**Lessons Learned:** Sometimes the service is just simply stopped by the attacker - in this case it is usually just as simple to bring it back online. The challenge is then to identify how attackers were able to turn off the service and how we can kick those SEAL members off our box for the time being.

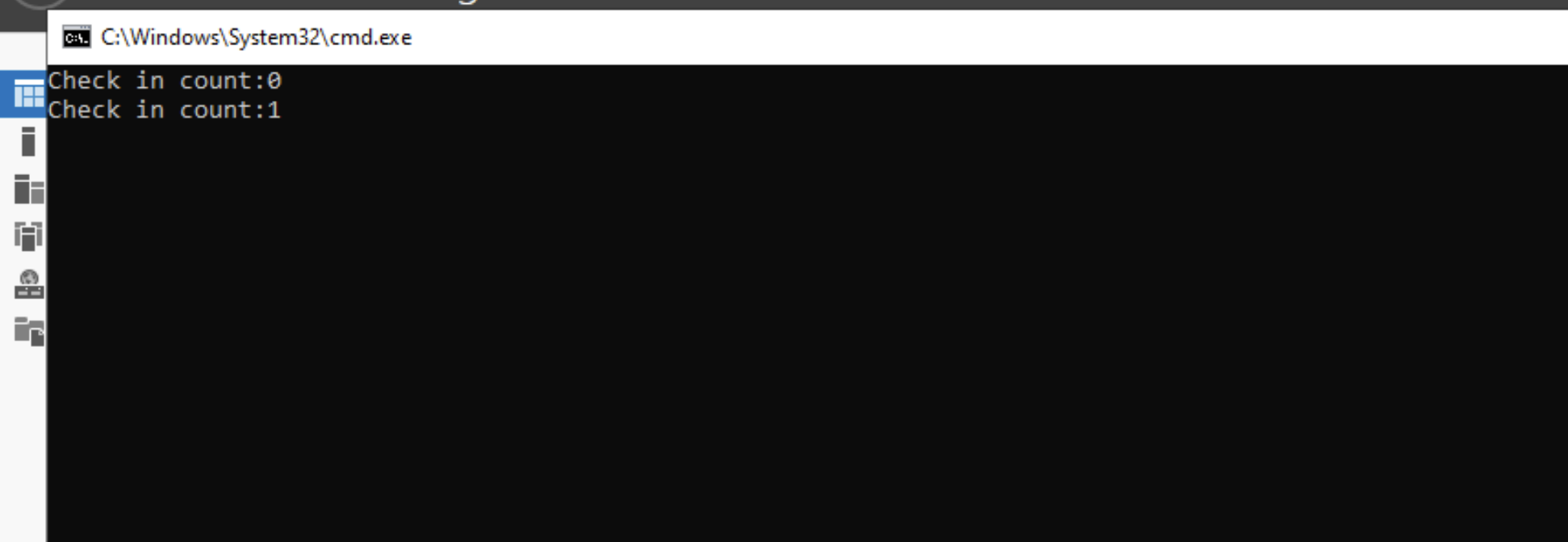
**Event:** Malicious Start up Process

**Priority:** MEDIUM

**Initial Detection:** 10:00 AM ET

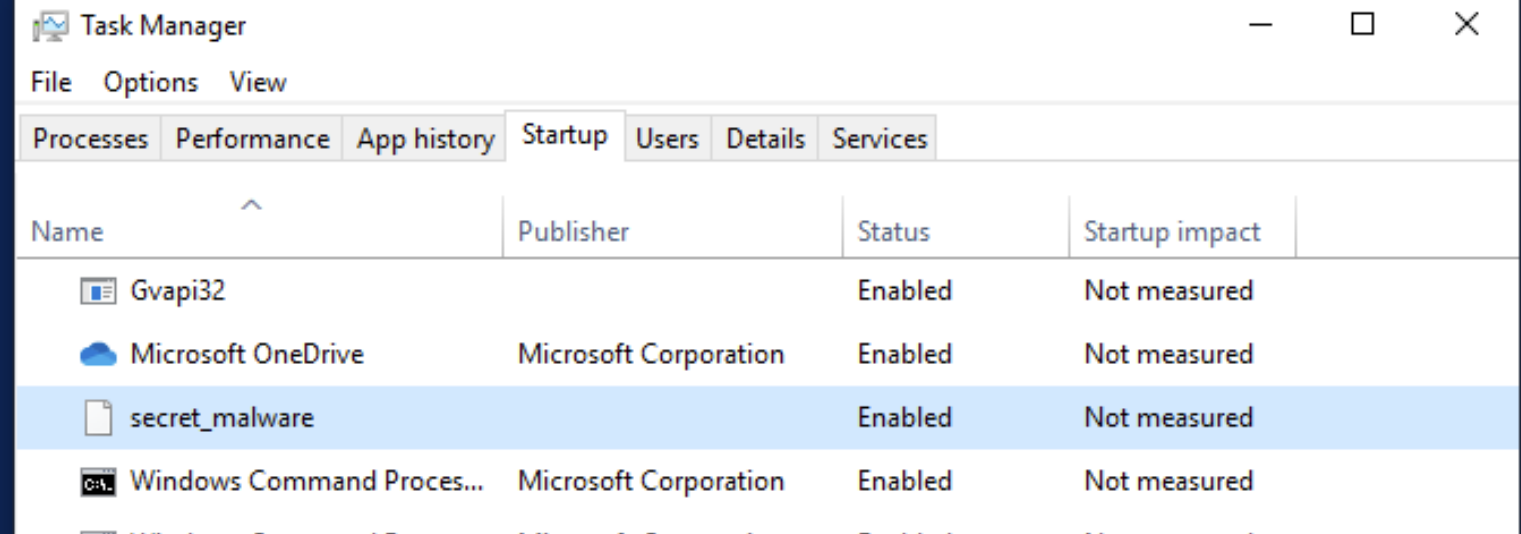
**Remediation:** Immediate

**Incident Identification:** Upon logging into the machine, it is clearly there are some malicious scripts being run in the background on startup (check screenshot below)



**Incident Causes:** Default malware installed in the machine by SEAL members.

**Responses Taken:** Check startup tasks on Windows to see what is being run.



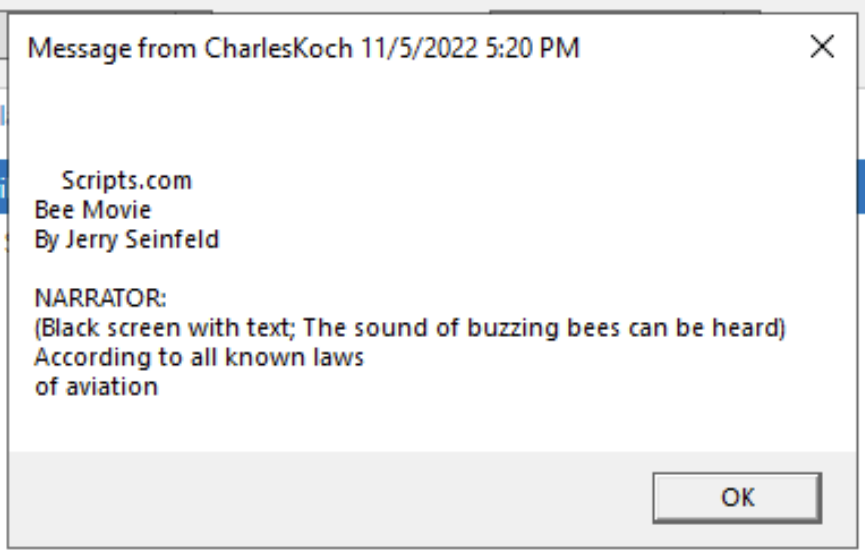
Clearly, as seen above, there is “secret\_malware” being run on startup. By simply disabling this we were able to make our box much safer for the remainder of the competition after a restart.

**Lessons Learned:** Startup processes are a very easy way for an attacker to have persistence on a machine. By removing this, it takes away persistence for the SEAL members and makes our services a lot safer.

**Event:** Repeated Bee Movie Messages

**Priority: LOW**

**Initial Detection:** 5:20 PM ET



As seen above, there is a message related to the Bee Movie popping up on many machines at this time.

**Remediation:** None

**Incident Causes:** This does not require action as it does not result in any score checks going down. However, it proves that SEAL members have access to this box somehow.

**Lessons Learned:** Somehow the SEAL members have access to the box and we need to do more threat hunting to figure out how.

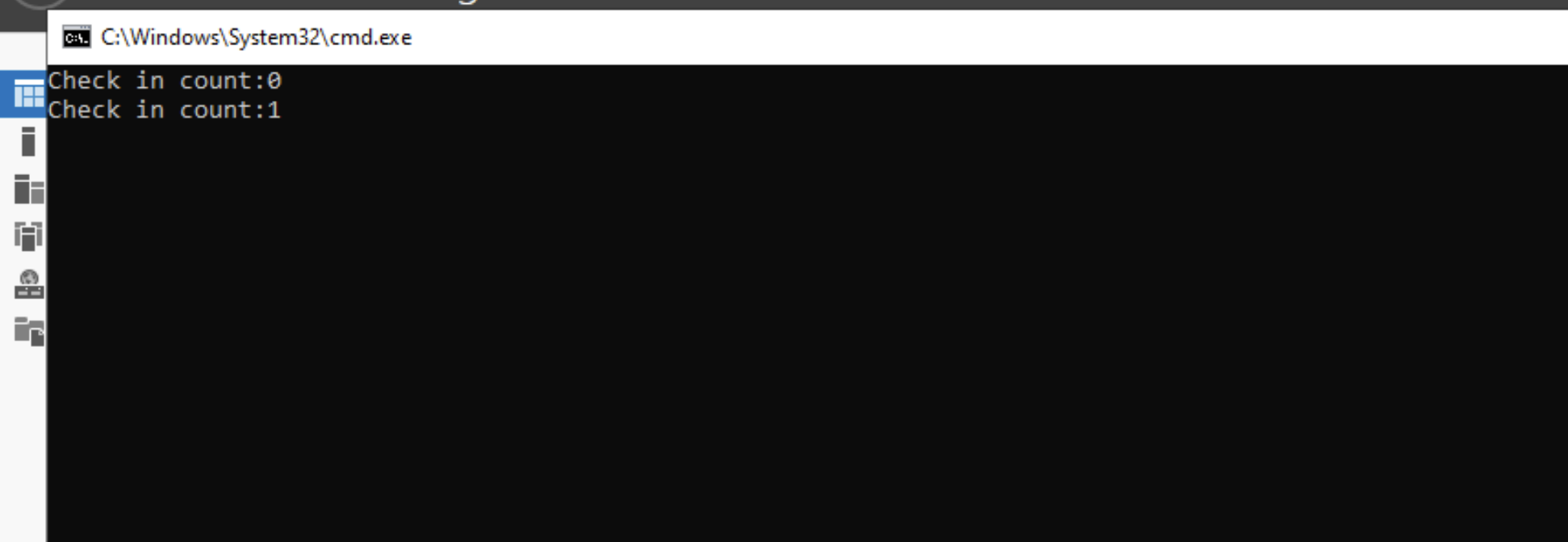
**Event:** Malicious Start up Process

**Priority:** MEDIUM

**Initial Detection:** 10:00 AM ET

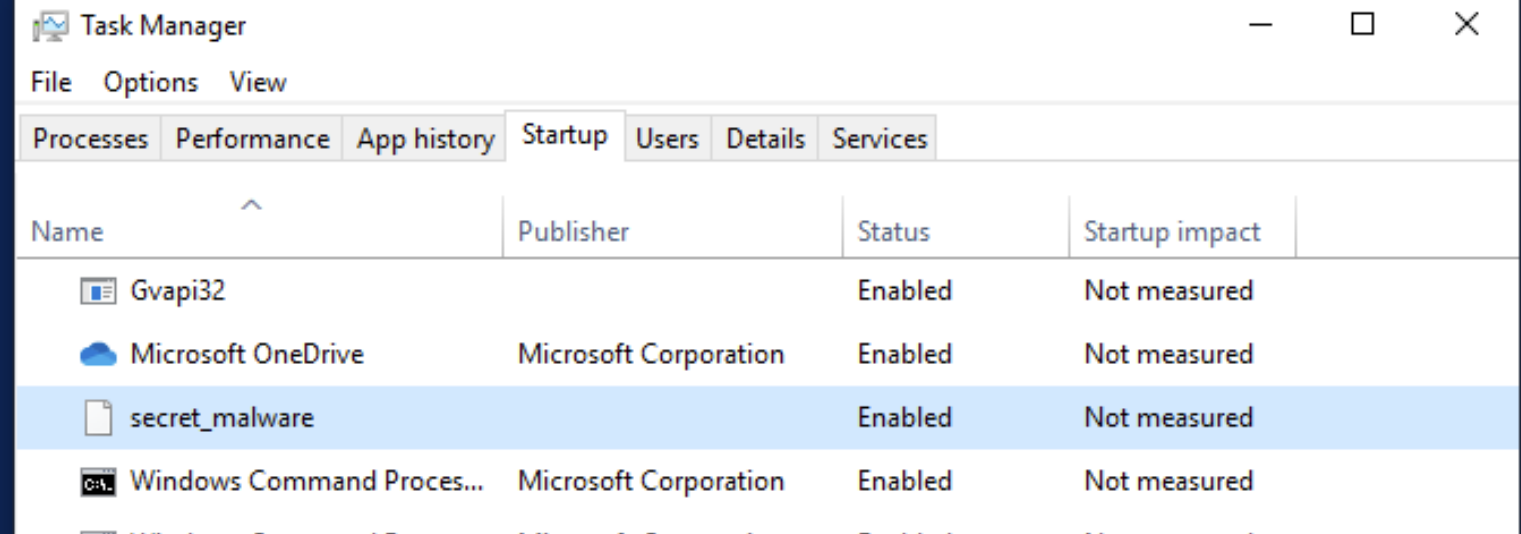
**Remediation:** Immediate

**Incident Identification:** Upon logging into the machine, it is clearly there are some malicious scripts being run in the background on startup (check screenshot below)



**Incident Causes:** Default malware installed in the machine by SEAL members.

**Responses Taken:** Check startup tasks on Windows to see what is being run.



Clearly, as seen above, there is “secret\_malware” being run on startup. By simply disabling this we were able to make our box much safer for the remainder of the competition after a restart.

**Lessons Learned:** Startup processes are a very easy way for an attacker to have persistence on a machine. By removing this, it takes away persistence for the SEAL members and makes our services a lot safer.

**Affected Host: Albatross**

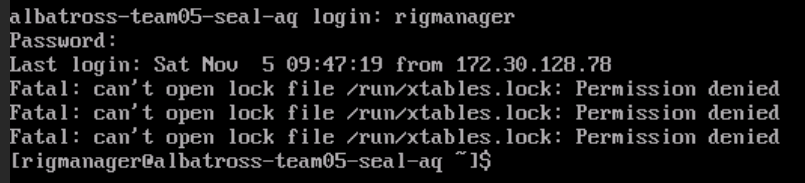
**Event:** SEAL member Login Attempt

**Priority:** MEDIUM

**Initial Detection:** 9:47 AM EST

**Remediation:** N/A

**Incident Identification:** We logged into the arch linux server as rigmanager and immediately noticed that the last login attempt was a few minutes before our log in was

****

**Incident Causes:** Not changing the password or setting up firewalls fast enough enabled SEAL member to get into the albatross box and lock files

**Responses Taken:** We immediately changed the password for both rigmanager and root users and also disabled every other user that we were not using

**Lessons Learned:** To not wait before logging into boxes at the start of a competition and to set up firewalls when we first log in

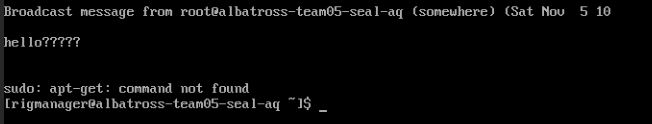
**Event:** SEAL member Broadcasted a message

**Priority:** LOW

**Initial Detection:** 10:46 AM EST

**Remediation:** Immediate

**Incident Identification:** Was typing in the Arch Linux terminal and was interrupted by a broadcast message from root that said “hello?????”



**Incident Causes:** Not setting up firewalls fast enough enabled a SEAL member to get into the albatross box as a root user and send out a broadcast message

**Responses Taken:** We changed the password for both rigmanager and root users again and checked our firewall configurations

**Lessons Learned:** To check the logs and pay attention to when the SEAL team infiltrates a server or system

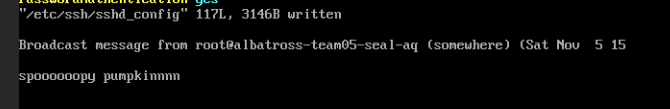
**Event:** SEAL member Broadcasted a message

**Priority:** LOW

**Initial Detection:** around 3 PM EST

**Remediation:** Immediate

**Incident Identification:** Was typing in the Arch Linux terminal and was interrupted by a broadcast message from root that said “spoooooopy pumpkinnnn”

****

**Incident Causes:** Not paying attention to logs and member access enabled a SEAL member to get into the albatross box as a root user and send out a broadcast message

**Responses Taken:** We changed the password for both rigmanager and root users again and checked our firewall configurations

**Lessons Learned:** To check the logs more often and pay attention to when the SEAL team infiltrates a server or system

**Final Thoughts:**

We are quite grateful for this experience. The environment also means a lot to us. It is important to preserve it to sustain our human race for future generations. It is unfortunate that organizations such as SEAL only keep their own priorities in mind instead of the future of the planet we call home. We are glad we were able to neutralize the oil rigs in Antarctica and stop SEAL’s malicious users from facilitating their corporate greed. Most of all, this experience was extremely valuable to each of the team members and has allowed us to reflect on our blue teaming tactics for future incidents. We hope to work with the CPA again soon.

Best regards,

Heads Empty (ma13c, Ghost225, Ribs, Christippert, poseidon)