# Initial Steps

1. Install Wazuh Manager on an Ubuntu Workstation
   1. Install ubuntu agent on everything (Windows first)
2. Install SCAP and auto-remediate
3. Change all of the admin usernames and passwords
   1. Once this is done, consider reaching out to the white team and changing all normal credentials as well

# Administrator Account Passwords

| Username | Password | Changed? | Workstation |
| --- | --- | --- | --- |
| root | HungryGrouse17 | Yes | Splunk |
| sysadmin | SpongeBobMeBoy | Yes | Splunk |
| admin (web/UI) | UnfathomablyBased1 | Yes | Splunk |
| administrator | !Changeme123 | No | 2019 Docker |
| root | changeme | No | Debian |
| sysadmin | changeme | No | Debian |
| sysadmin | changeme | No | Ubuntu Web |
| administrator | !Password123 | No | 2019 AD |
| sysadmin | changeme | No | Ubuntu Wkst |
| root | changeme | No | CentOS |
| sysadmin | changeme | No | CentOS |
| root | !Password123 | No | Fedora |
| admin | Changeme123 | No | Palo Alto |
| minion | kingbob | No | Windows 10 |

172.20.241.20:8089

:8000

# 

# User Account Passwords

| User | Password |
| --- | --- |
| v3u1 | lolnicepassword!2 |
| v3u2 | greatDamnPasswd!3 |
| v3u3 | ? |
| v3u4 | NuPSSWD!4 |
| v3u5 | h8ZK2l2yfc52 |
| v3u6 |  |
| v3u7 | SmugBass1337 |
| v3u8 | 2Hm]E\*LAXh^V;tV |
| v3u9 |  |
|  |  |

# Ubuntu Workstation

## Wazuh Install (manager)

* sudo apt-get update
* sudo apt install curl tree
* curl -sO <https://packages.wazuh.com/4.10/wazuh-install.sh> && sudo bash ./wazuh-install.sh -a

Wazuh creds: admin:yuTebCX.1\*TGosW.E5iuQRkkG8qw+dQo

172.20.242.101

### Wazuh Install (Windows)

Invoke-WebReqeust -Uri <https://packages.wazuh.com/4.x/windows/wazuh-agent-4.10.1-1.msi> -OutFile $env:tmp\wazuh-agent; msiexec.exe /i $env:tmp\wazuh-agent /q WAZUH\_MANAGER=’172.20.242.101’

### Wazuh Install (Debian)

* apt-get install gnupg apt-transport-https
* curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | apt-key add -
* echo "deb https://packages.wazuh.com/4.x/apt/ stable main" | tee -a /etc/apt/sources.list.d/wazuh.list
* WAZUH\_MANAGER="172.20.242.101" apt-get install wazuh-agent
* systemctl daemon-reload
* systemctl enable wazuh-agent
* systemctl start wazuh-agent

### Zeek Install (Ubuntu)