|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **System** | **Location** | **IP** | **OS** | **Services** |  |
| Router | Corp | .254 | Cisco | SSH, SNMP (Read only) |  |
| Switch | Corp | .1 | Cisco | SSH |  |
| Wireless AP | Corp | .9 | Cisco | -- |  |
| Caterpie | Corp | .40 | Windows | DNS, AD  Powershell Remoting | DNS  LDAP |
| Weedle | Corp | .2 | Linux | -- |  |
| Pidgy | Corp | .3 | Linux | -- |  |
| Rattata | Corp | .8 | Linux | -- |  |
| Spearow | Corp | .4 | Windows 10 | Powershell Remoting  OpenOffice  VSphere Client |  |
| Magikarp | Corp | .12 | Windows 2012(ESX) | SMB | SMB |
| Voltorb | Corp | .22 | CentOS | FTP | Vsftpd 2.3.4 |
| Ekans | Corp | .5 | Windows 10 | Powershell Remoting  OpenOffice  VSphere Client |  |
| Sandshrew | Corp | .6 | Windows 10 | Powershell Remoting  OpenOffice  VSphere Client |  |
| Clefairy | Corp | .7 | Windows 10 | Powershell Remoting  OpenOffice  VSphere Client |  |
| Zubat | Corp | .30 | ESX | SSH  ESXI | ESXi |
| Snorlax | Corp | 138 | VCenter | VCenter | VCenter |
| Machop | Corp | .37 | CentOS | Foreman, DHCP, TFTP | Score Foreman webapp |
| Bellsprout | Corp | .20 | Linux (ESX) | SSH, POP/SMTP/IMAP | SSH  POP3  SMTP  IMAP |
| Vulpix | Corp | -- | Android | F-Score Inc | F-Score Inc |
| Venonat | Dev | -- | ESX | -- |  |
| Diglett | Dev | .21 | Linux | GitLab, Jenkins, SSH | Gitlab  Jenkins - If build passed  SSH |
| Meowth | Dev | .22 | Linux | MySQL, Web, SSH | MySQL  Web  SSH |
| Abra | Prod | -- | Gentoo | SSH, Nginx  Ansible | Load balancer Redirect  SSH |
| Mankey | Prod | -- | Ubuntu (Docker) | SSH, Nginx, MySQL, VsFTP, webmin | MySQL  SSH |
| Growlithe | Prod | -- | Ubuntu (Docker) | SSH, Nginx (PHP), VsFTP. webmin | SSH |
| Poliwag | Prod | -- | Ubuntu(docker) | SSH, Nginx (PHP), VsFTP.webin | SSH |

Make a case for using docker versus not docker

Prod has a higher weight

Vulns -

Red team can grab SSH keys and pivot

Web vulnerabilities

Gentoo box will have SSH keys to

VsFTP - Guest user with slightly weaker

Weak Credentials on SSH in the switch/Router

WPA2 creds are stored in NExus 5x

Default Netsys123$

Port 8421 is check

SSH on phone open and forwarded

Terminal installed

Enable debugging

Firewall off on AP

Backdoor in the nexus

Easy password on WRT-110N

Backdoor on three of the windows boxes

Backdoor on 2 of the debian boxes

wiper with creds to all the -> we want this to be on three windows boxes

Load 5 isos onto external drives

**Team 1**

|  |  |  |
| --- | --- | --- |
| Ubuntu-14 | [ec2-204-236-210-251.compute-1.amazonaws.com](http://ec2-204-236-210-251.compute-1.amazonaws.com) | 204.236.210.251 |
| Ubuntu-14 | [ec2-54-204-141-218.compute-1.amazonaws.com](http://ec2-54-204-141-218.compute-1.amazonaws.com) | 54.204.141.218 |
| Ubuntu-14 | [ec2-52-205-70-89.compute-1.amazonaws.com](http://ec2-52-205-70-89.compute-1.amazonaws.com) | 52.205.70.89 |
| Gentoo | [ec2-107-20-53-231.compute-1.amazonaws.com](http://ec2-107-20-53-231.compute-1.amazonaws.com) | 107.20.53.231 |

**Team 2**

|  |  |  |
| --- | --- | --- |
| **Ubuntu-14** | [**ec2-54-145-183-218.compute-1.amazonaws.com**](http://ec2-54-145-183-218.compute-1.amazonaws.com) | **54.145.183.218** |
| **Ubuntu-14** | [**ec2-54-91-64-179.compute-1.amazonaws.com**](http://ec2-54-91-64-179.compute-1.amazonaws.com) | **54.91.64.179** |
| **Ubuntu-14** | [**ec2-34-207-103-248.compute-1.amazonaws.com**](http://ec2-34-207-103-248.compute-1.amazonaws.com) | **34.207.103.248** |
| **Gentoo** | [**ec2-52-54-80-14.compute-1.amazonaws.com**](http://ec2-52-54-80-14.compute-1.amazonaws.com) | **52.54.80.14** |

**Team 3**

|  |  |  |
| --- | --- | --- |
| **Ubuntu-14** | [**ec2-107-23-103-206.compute-1.amazonaws.com**](http://ec2-107-23-103-206.compute-1.amazonaws.com) | **107.23.103.206** |
| **Ubuntu-14** | [**ec2-54-236-232-16.compute-1.amazonaws.com**](http://ec2-54-236-232-16.compute-1.amazonaws.com) | **54.236.232.16** |
| **Ubuntu-14** | [**ec2-54-197-123-117.compute-1.amazonaws.com**](http://ec2-54-197-123-117.compute-1.amazonaws.com) | **54.197.123.117** |
| **Gentoo** | [**ec2-54-144-82-182.compute-1.amazonaws.com**](http://ec2-54-144-82-182.compute-1.amazonaws.com) | **54.144.82.182** |

**Team 4**

|  |  |  |
| --- | --- | --- |
| **Ubuntu-14** | [**ec2-52-91-88-114.compute-1.amazonaws.com**](http://ec2-52-91-88-114.compute-1.amazonaws.com) | **52.91.88.114** |
| **Ubuntu-14** | [**ec2-54-196-8-206.compute-1.amazonaws.com**](http://ec2-54-196-8-206.compute-1.amazonaws.com) | **54.196.8.206** |
| **Ubuntu-14** | [**ec2-184-73-59-200.compute-1.amazonaws.com**](http://ec2-184-73-59-200.compute-1.amazonaws.com) | **184.73.59.200** |
| **Gentoo** | [**ec2-54-221-136-10.compute-1.amazonaws.com**](http://ec2-54-221-136-10.compute-1.amazonaws.com) | **54.221.136.10** |

**Team 5**

|  |  |  |
| --- | --- | --- |
| **Ubuntu-14** | [**ec2-54-172-222-44.compute-1.amazonaws.com**](http://ec2-54-172-222-44.compute-1.amazonaws.com) | **54.172.222.44** |
| **Ubuntu-14** | [**ec2-54-196-34-134.compute-1.amazonaws.com**](http://ec2-54-196-34-134.compute-1.amazonaws.com) | **54.196.34.134** |
| **Ubuntu-14** | [**ec2-54-224-51-26.compute-1.amazonaws.com**](http://ec2-54-224-51-26.compute-1.amazonaws.com) | **54.224.51.26** |
| **Gentoo** | [**ec2-52-91-126-201.compute-1.amazonaws.com**](http://ec2-52-91-126-201.compute-1.amazonaws.com) | **52.91.126.201** |

**Team 6**

|  |  |  |
| --- | --- | --- |
| **Ubuntu-14** | [**ec2-54-242-40-219.compute-1.amazonaws.com**](http://ec2-54-242-40-219.compute-1.amazonaws.com) | **54.242.40.219** |
| **Ubuntu-14** | [**ec2-54-92-235-124.compute-1.amazonaws.com**](http://ec2-54-92-235-124.compute-1.amazonaws.com) | **54.92.235.124** |
| **Ubuntu-14** | [**ec2-54-86-85-117.compute-1.amazonaws.com**](http://ec2-54-86-85-117.compute-1.amazonaws.com) | **54.86.85.117** |
| **Gentoo** | [**ec2-52-86-90-235.compute-1.amazonaws.com**](http://ec2-52-86-90-235.compute-1.amazonaws.com) | **52.86.90.235** |

**Team 7**

|  |  |  |
| --- | --- | --- |
| **Ubuntu-14** | [**ec2-52-201-251-74.compute-1.amazonaws.com**](http://ec2-52-201-251-74.compute-1.amazonaws.com) | **52.201.251.74** |
| **Ubuntu-14** | [**ec2-54-89-242-216.compute-1.amazonaws.com**](http://ec2-54-89-242-216.compute-1.amazonaws.com) | **54.89.242.216** |
| **Ubuntu-14** | [**ec2-54-91-44-241.compute-1.amazonaws.com**](http://ec2-54-91-44-241.compute-1.amazonaws.com) | **54.91.44.241** |
| **Gentoo** | [**ec2-107-22-62-5.compute-1.amazonaws.com**](http://ec2-107-22-62-5.compute-1.amazonaws.com) | **107.22.62.5** |

**Team 8**

|  |  |  |
| --- | --- | --- |
| **Ubuntu-14** | [**ec2-54-210-251-103.compute-1.amazonaws.com**](http://ec2-54-210-251-103.compute-1.amazonaws.com) | **54.210.251.103** |
| **Ubuntu-14** | [**ec2-52-54-233-33.compute-1.amazonaws.com**](http://ec2-52-54-233-33.compute-1.amazonaws.com) | **52.54.233.33** |
| **Ubuntu-14** | [**ec2-54-167-187-223.compute-1.amazonaws.com**](http://ec2-54-167-187-223.compute-1.amazonaws.com) | **54.167.187.223** |
| **Gentoo** | [**ec2-54-163-176-189.compute-1.amazonaws.com**](http://ec2-54-163-176-189.compute-1.amazonaws.com) | **54.163.176.189** |

**Team 9**

|  |  |  |
| --- | --- | --- |
| **Ubuntu-14** | [**ec2-52-90-167-86.compute-1.amazonaws.com**](http://ec2-52-90-167-86.compute-1.amazonaws.com) | **52.90.167.86** |
| **Ubuntu-14** | [**ec2-54-82-139-162.compute-1.amazonaws.com**](http://ec2-54-82-139-162.compute-1.amazonaws.com) | **54.82.139.162** |
| **Ubuntu-14** | [**ec2-34-207-232-201.compute-1.amazonaws.com**](http://ec2-34-207-232-201.compute-1.amazonaws.com) | **34.207.232.201** |
| **Gentoo** | [**ec2-54-146-110-123.compute-1.amazonaws.com**](http://ec2-54-146-110-123.compute-1.amazonaws.com) | **54.146.110.123** |

**Team 10**

|  |  |  |
| --- | --- | --- |
| **Ubuntu-14** | [**ec2-54-172-147-128.compute-1.amazonaws.com**](http://ec2-54-172-147-128.compute-1.amazonaws.com) | **54.172.147.128** |
| **Ubuntu-14** | [**ec2-34-207-113-123.compute-1.amazonaws.com**](http://ec2-34-207-113-123.compute-1.amazonaws.com) | **34.207.113.123** |
| **Ubuntu-14** | [**ec2-54-172-147-128.compute-1.amazonaws.com**](http://ec2-54-172-147-128.compute-1.amazonaws.com) | **54.172.147.128** |
| **Gentoo** | [**ec2-52-87-175-213.compute-1.amazonaws.com**](http://ec2-52-87-175-213.compute-1.amazonaws.com) | **52.87.175.213** |

**AWS Misconfigurations**

* VSFTP anonymous upload/download to web directory on ubuntu hosts
* All SSH keys are available on jenkins build boxes and throughout local cloud Windows environment.
* Webmin (web admin panel to the box)
* Web application