# NMAP Scan Details

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Machine Name | Version | IP Address | Ports Open | Services Running | Version |
| Phantom | 4.1.94 | 172.20.240.10 | 22  80  443  8088  8089  8300 (closed) | ssh  http  http  http  http  tmi | OpenSSH 7.4  nginx 1.13.7  nginx 1.13.7  Splunkd httpd  Splunkd httpd |
| Debian MySQL | 7.8 | 172.20.240.20 | 22  80  111  3306 | ssh  http  rpcbind  mysql | OpenSSH 6.0p1  Apache httpd 2.2.22  MySQL 5.5.44-0 |
| Ubuntu DNS | 12.04 | 172.20.242.10 | 21  22 | ftp  ssh | ProFTPD 1.3.3c  OpenSSH 5.9p1 |
| Windows  AD/DNS/Exchange | 2008 R2 | 172.20.242.200 | 53  80  88  111  135  139  389  445  464  593  636  3268  3269  3389  49154  49155  49157  49158  49161 | domain  http  Kerberos  rpcbind  msrpc  netbios  ldap  Microsoft-ds  kpasswd5  ncacn\_http  tcpwrapped  ldap  tcpwrapped  ms-wbt-server  msrpc  msrpc  ncacn\_http  msrpc  msrpc | DNS 6.1.7600  IIS httpd 7.5  Kereros  Windows RPC  Windows netbios-ssn  AD LDAP  RPC over HTTP 1.0  AD LDAP  RPC  RPC  RPC over HTTP 1.0  RPC  RPC |
| Windows | 8.1 | 172.20.242.100 | 135  139  445  1025  1026  1027  1028  1029  1052  1054  1059 | msrpc  netbios-ssn  Microsoft-ds  msrpc  msrpc  msrpc  msrpc  msrpc  msrpc  msrpc  msrpc | Windows RPC  netbios-ssn  workgroup: FROG  Windows RPC  Windows RPC  Windows RPC  Windows RPC  Windows RPC  Windows RPC  Windows RPC  Windows RPC |
| Splunk  (CentOS) | 8.0  6.4 | 172.20.241.20 | 22  8000  8008(closed)  8089 | ssh  http  http  http | OpenSSH 5.3  Splunkd httpd  Splunkd httpd |
| CentOS Ecomm | 6.0 | 172.20.241.30 | 22  80 | ssh  http | OpenSSH 5.3  Apache httpd 2.2.15 |
| Fedora Webmail/WebApps | 21 | 172.20.241.40 | 22  9090 | ssh  http | OpenSSH 6.6.1  Cockpit MGMT console |

# Quick Reference List

Update/upgrade commands for Linux Machines

* Fedora/CentOS: *sudo dnf update && dnf upgrade*
* Ubuntu/Debian: *sudo apt-get update && apt-get upgrade –yy*
* Check for updates to Splunk and Phantom
* Run Windows Update

PW base for machines/admins: ##WhatsTheWeather04

* ## = machine number (refer to table above)

PW for scoring users – refer to Scoring User List

Windows AD: Change all user passwords, both local and domain

* Use script for domain users

1. Download script and userlist
2. Move both files to C drive
3. Open Powershell in “Run as Administrator” mode
4. Run command **Import-Module “c:\ResetPassword.psm1”** to import the script (enter exactly)
5. Run command **Set-OSCADAccountPassword -path “c:\Userlist.csv”**
6. Enter **A** for yes to all option
7. Send memo to scoring judges with the result file attached
8. Once sent, delete file and empty Recycle Bin
   * will not change administrator or mysql user password

* Create new user, make administrator
  + Username: rthunter
  + Password: \*use password base minus machine number\*
* Change Administrator password
  + Use password base above minus machine number
* Change local admin password
  + Use password base above
* Windows Firewall
  + Remove exceptions that are not needed
  + Enable firewall
  + Enable alert when new program is blocked