**PA Firewall Hardening Plan (v.8.0.5)** [**https://drive.google.com/open?id=13n4ZqfBoAHOS0d8Pt3DxAEt5S-QeWaPq**](https://drive.google.com/open?id=13n4ZqfBoAHOS0d8Pt3DxAEt5S-QeWaPq)

**<https://file.io/92zhZA>**

*PA Firewall Information:*

|  |  |
| --- | --- |
| IP address for MGT port: | 172.20.242.150 |
| Netmask: | 255.255.255.0 |
| Default Gateway: | 172.20.242.1 |
| DNS server address: | [primary=Ubuntu 12.04] [secondary=2008 R2] |

1. Change Admin Password: Use PuTTY to sign in.

**configure**

**set mgt-config users admin password**

yellow monkey face (default = admin/admin) (admin/changeme)

**commit**

**exit**  (to leave configuration mode)

1. Past configuration script: <https://file.io/hPrtpX>

**set cli scripting-mode on** (make sure you’re not in configuration mode)

**configure**

(paste contents)

**commit**

1. Update default rules if present:
   1. In WebGUI, default rules: intrazone-default, interzone-default
   2. Click the Name of the policy and then “Override” in the bottom toolbar. Set both to Deny and Log at Session End.
2. Backup Configuration: (Manual: <https://file.io/wKFbBE> )
   1. Use GUI/Web Interface
3. Check for Updates:
   1. Download the base 6.0.1 (Do not install) and then the latest. (Install this one)
4. Update virus/threat definitions:
   1. In WebGUI, go to **Device > Dynamic Updates** and click “**Check now**.” After the new update is listed, download and install it.
   2. You can also manually download the updates from: <https://support.paloaltonetworks.com/Support/Index>
      1. Requires a valid Support Account
      2. Instructions: <https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000PMZuCAO>

*Potential Injects:*

* Forward logs to splunk:
  + <https://splunkbase.splunk.com/app/491/>
* Marking packets as AF42
* Static IP NAT. (i.e. External IP 77.33.22.11 to internal 172.20.242.100 port 3389)
* After creating new user accounts on domain, sync users
* Custom URL blocking (i.e. facebook.com)

**Windows 8**

1. Change password (Default: binddn / !Password123 )
2. Download updates:
   1. <https://www.catalog.update.microsoft.com>
   2. Servicing Stack Update (SSU): Win. 8 – KB4524445 – (~11 MB)
   3. Security Only: Win. 8 - KB4525250 – (~30 MB)
   4. Monthly Rollup: Win. 8 - KB4525243 – (~320-500 MB)
3. Check for other accounts
4. Firewall:
   1. Turn on
5. Ensure Windows Defender is on and Updated
6. Download Microsoft Baseline Configuration Manager 2.0
   1. <https://www.microsoft.com/en-us/download/details.aspx?id=16475>

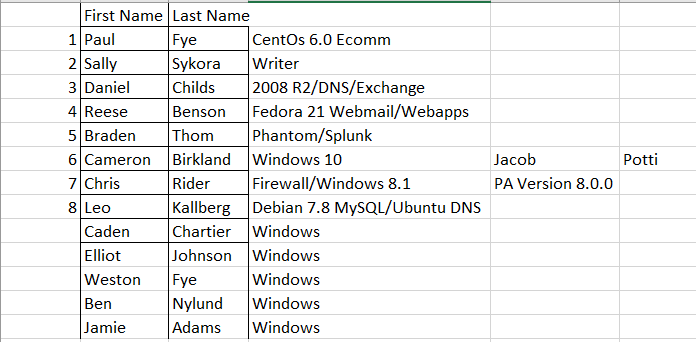
*Potential Injects:*

* Set login banner
  + **HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\winlogon\**
  + **Edit the LegalNoticeCaption and put a title text like “Warning” and,**
  + **edit the LegalNoticeText and put a message like “I have the owner ship!”**
  + **Could also be:**
    - **POLICY\_KEY = “HKLM\Software\Microsoft\Windows\CurrentVersion\policies\system\”**
    - **Const LEGAL\_CAPTION\_VALUENAME = “legalnoticecaption”**
    - **Const LEGAL\_TEXT\_VALUENAME = “legalnoticetext”**
  + **Or:** 
    - Run -> secpol.msc -> Local Policies -> Security Options -> "Interactive logon: Message text for users attempting to log on" and change/remove the text here.
* Set ntp
  + Right click clock > Adjust Date/Time
  + Tab: Internet Time > Change Settings…(admin)
  + Type server name, click update then ok.
* Forward logs to splunk
  + <https://splunkbase.splunk.com/app/3067/>

**NTP Servers:** <https://www.ntppool.org/en/use.html>

1.north-america.pool.ntp.org

2.pool.ntp.org

Team: 

Topology: 

*Private IP Range Used in Competition*

172.20.240.0/24 - 172.20.242.0/24

172.25.29.0/24 [Team 9 Public IPs]

172.31.29.0-7 [Team 9 to Core]

*Private IP Range NOT used in Competition*

10.0.0.0 – 10.255.255.255

172.16.0.0 – 172.20.239.255

172.20.243.0 – 172.25.20.255

172.25.22.0- 172.31.20.255

172.31.21.8 – 172.31.255.255

192.168.0.0 – 192.168.255.255

**Other:**

**Awesome Security Lists**

<https://github.com/sbilly/awesome-security>

<https://github.com/meirwah/awesome-incident-response>

**Basically any tool in the ADHD toolkit is useful:**

<https://github.com/adhdproject/adhdproject.github.io/blob/master/index.md>

**File Hosting:**

pastebin.com

transfer.sh

ghostbin.com

**Linux Malware Detect**

<https://www.rfxn.com/projects/linux-malware-detect/>

**Lynis Auditing Tool**

<https://cisofy.com/lynis/>

**Useful blogs and talks that cover CCDC related material.**

General CCDC:

<https://www.reddit.com/r/ccdc/>

<https://sites.google.com/site/howtoccdc/tips>

<https://jordanpotti.com/ccdc/>

<https://scout.wisc.edu/cyberwatch/downloads/62/NCC_Press_How_To_Prepare_For_the_CCDC.pdf>

<https://www.trustwave.com/Resources/SpiderLabs-Blog/Web-Application-Defender-s-Cookbook--CCDC-Blue-Team-Cheatsheet/>

<http://www.hackingtheuniverse.com/infosec/isnews/ccdc-tips>

<http://hackersvanguard.com/ccdc-tips-and-tricks/>

Red Team CCDC Stuff:

<https://blog.cobaltstrike.com/2016/02/23/cobalt-strike-tips-for-2016-ccdc-red-teams/>

<https://blog.cobaltstrike.com/2014/03/04/ccdc-red-teams-ten-tips-to-maximize-success/>

<http://www.hecfblog.com/2015/04/national-ccdc-2015-red-team-debrief.html>

<https://alexlevinson.wordpress.com/2015/04/27/ccdc-2015-debrief-red-team-identity/>

Previous Topologies:

<https://www.reddit.com/r/ccdc/comments/5czu7v/previous_ccdc_topologies/da1175r/>