Pat Reference Docs

Windows Server 2008

Firewall

Inbound Ports:

```
# Explicitly Given
445/tcp  # SMB
1433/tcp # MSSQL
3389/tcp # RDP
```

Users

👀 look here for anything odd 👀

Patching, Downloads, & AV

```
Download
http://download.windowsupdate.com/c/msdownload/update/software/secu/2017/05/windows8-rt-kb4012598-x86_a0f1c953a24dd042acc540c59b339f55fb18f594.msu
Algorithm       Hash
---------       ----
SHA256          6589008F680328707AAAE689A396EE0FBCD180F797228E36CB7019E65EE735CA
MD5             AE3865F6D94F6A88C8CCF9D19B135820
```

Download https://www.clamav.net/downloads/production/ClamAV-0.101.1.exe

```
Algorithm       Hash
---------       ----
SHA256          4ADCB9AAA43D529D1E37AF57B291A5A7CEB5FEE0516D9469ECBA3661F577D273
MD5             092C7131898ED8A30B25B9B52C695386
```

and Definitions for Clam

```
http://database.clamav.net/main.cvd
Algorithm       Hash
---------       ----
MD5             A22E1B59C5E8B8EFF166271B08B4AD72
SHA256          081884225087021E718599E8458FF6C9EE3CDEBED8775DD8E445FC7B589D88A6
*Hashes may vary depending on when downloaded for staging server

http://database.clamav.net/daily.cvd
Algorithm       Hash
---------       ----
MD5             6FC20F69CD062AC6DF20F5020860FE71
SHA256          1B163F89E2A6CF47AB91646B7E33B4AB04742D0EF67D04A30434D5E1119F9ABB
*Hashes may vary depending on when downloaded for staging server
```

Download https://download.sysinternals.com/files/SysinternalsSuite.zip

```
Algorithm       Hash
---------       ----
SHA256          B14466C6BF3BE216EA71610A3F455030E791CD5AD1B42A283886194205D176B0
MD5             C8E2413DB5306C64309456C368848962
```

Pat Reference Docs

Windows XP

Firewall

wscui.cpl

Inbound Ports:

```
# Explicitly Given
445/tcp  # SMB
3306/tcp # MySQL
```

Users

lusrmgr.msc

👀 look here for anything odd 👀

1. Open the System Properties applet (filename: SYSDM.CPL) in the Control Panel. The System Properties window will appear.
2. Click on the Advanced tab to view the advanced settings for the system.
3. In the Performance section at the top of the Advanced tab, click on the Settings button. The Performance Options window will appear
4. In the Performance Options window, click on the Data Execution Prevention tab to view the settings for DEP.
5. Select Turn on DEP for all programs and services except those I select:. If you have any programs that are incompatible with DEP, click on the Addbutton and add them to the exclusion list. Click on the OK button when finished to make the changes to the system
6. A reboot will be required for these changes made to Windows XP to take effect.

Patching, Downloads, & AV

Download https://download.microsoft.com/download/D/B/4/DB4B0C90-0A7D-46C9-8988-8A5BE95B44A6/WindowsXP-KB4012598-x86-Custom-ENU.exe

```
Algorithm       Hash
---------       ----
SHA256          3530B7890C22096693FD473D8C6455B9992AC4AA400E1B8CE14D0049234C489D
MD5             3AD11C9883051E5A5EEC5A000DC4C37C
```

Download https://www.clamav.net/downloads/production/ClamAV-0.101.1.exe

```
Algorithm       Hash
---------       ----
SHA256          4ADCB9AAA43D529D1E37AF57B291A5A7CEB5FEE0516D9469ECBA3661F577D273
MD5             092C7131898ED8A30B25B9B52C695386
```

and Definitions for Clam

http://database.clamav.net/main.cvd

```
Algorithm       Hash
---------       ----
MD5             A22E1B59C5E8B8EFF166271B08B4AD72
SHA256          081884225087021E718599E8458FF6C9EE3CDEBED8775DD8E445FC7B589D88A6
```

http://database.clamav.net/daily.cvd

```
Algorithm       Hash
---------       ----
MD5             6FC20F69CD062AC6DF20F5020860FE71
SHA256          1B163F89E2A6CF47AB91646B7E33B4AB04742D0EF67D04A30434D5E1119F9ABB
```

*Hashes may vary depending on when downloaded for staging server

Download https://download.sysinternals.com/files/SysinternalsSuite.zip

```
Algorithm       Hash
---------       ----
SHA256          B14466C6BF3BE216EA71610A3F455030E791CD5AD1B42A283886194205D176B0
MD5             C8E2413DB5306C64309456C368848962
```

Download https://cdn.mysql.com//Downloads/MySQLGUITools/mysql-workbench-community-6.2.5-win32.msi

```
Algorithm       Hash
---------       ----
SHA256          1AFFABF39F2057B768DC1A0C932D1E76F6A80DEA489F0617E3E2C4765EF4AAF4
MD5             A631FCB1DC8257ECCA271A0841019C22
```

For when the red team is winning...