**Detection Rule Testing Document**

**Test 1**

**Rule Name:** Discovery - Account Discovery - Net - T1087

**Rule Goal:** Detects enumeration of account information via net.exe

**Attack Instructions**

1. Log on to test endpoint system
2. Run Cmd.exe
3. Execute the following commands
   1. Net user
   2. Net group
   3. Net localgroup
   4. Net accounts
   5. Net view
   6. Net share
4. Run FreeEDR to determine if appropriate alerts have been generated

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Test 2**

**Rule Name:** Discovery - File and Directory Discovery - Command Line Utilities - T1083

**Rule Goal:** Detects enumeration of files and directories using various command-line utilities

**Attack Instructions**

1. Log on to test endpoint system
2. Run Cmd.exe or Powershell.exe
3. Execute the following commands
   1. dir
   2. tree
   3. ls
   4. syteminfo
   5. ver
4. Run FreeEDR to determine if appropriate alerts have been generated

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Test 3**

**Rule Name:** Discovery - Network Share Discovery - Net - T1135

**Rule Goal:** Detects enumeration of network share information via net.exe

**Attack Instructions**

1. Log on to test endpoint system
2. Run Cmd.exe
3. Execute the following commands
   1. Net view
   2. Net share
4. Run FreeEDR to determine if appropriate alerts have been generated

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Test 4**

**Rule Name:** Discovery - Process Discovery - Tasklist - T1057

**Rule Goal:** Detects enumeration of processes using Tasklist.exe and other command-line utilities

**Attack Instructions**

1. Log on to test endpoint system
2. Run Powershell.exe
3. Execute the following commands
   1. tasklist
   2. ps
   3. get-process
4. Run FreeEDR to determine if appropriate alerts have been generated

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Test 5**

**Rule Name:** Discovery - System Network Configuration - Command Line Utilities - T1016

**Rule Goal:** Detects enumeration of System Network Configurations using various command-line utilities

**Attack Instructions**

1. Log on to test endpoint system
2. Run Cmd.exe
3. Execute the following commands
   1. Ipconfig
   2. Nbtstat /n
   3. route print
   4. arp /a
4. Run FreeEDR to determine if appropriate alerts have been generated

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Test 6**

**Rule Name:** Execution - Windows Management Instrumentation - WMIC Process Call Create - T1047

**Rule Goal:** Detects remote execution on hosts using WMIC Process Call Create

**Attack Instructions**

1. Log on to test endpoint system
2. Run Cmd.exe
3. Execute the following command
   1. Wmic process call create calc.exe
4. Run FreeEDR to determine if appropriate alerts have been generated

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Test 7**

**Rule Name:** Execution - Scheduled Task - Schtasks - T1053

**Rule Goal:** Detects creation, modification, and execution of scheduled tasks using Schtasks.exe

**Attack Instructions**

1. Log on to test endpoint system
2. Run Cmd.exe
3. Execute the following command
   1. Schtasks /run /tn (name of any sample scheduled task goes here)
4. Run FreeEDR to determine if appropriate alerts have been generated

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Test 8**

**Rule Name:** Initial Access - Spearphishing Attachment - Suspicious Office Activity - T1193

**Rule Goal:** Detects processes suspiciously launched by Microsoft Office applications

**Attack Instructions**

1. Log on to test endpoint system
2. Will require a sample Office document with macro scripts embedded to launch PowerShell, Cmd, Cscript, Wscript, Mshta, or Wmic.
3. Open the same document in Word, PowerPoint, or Excel
4. Enables macros/scripts so that the embedded script is executed
5. Run FreeEDR to determine if appropriate alerts have been generated

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Test 9**

**Rule Name:** Detects local user creation

**Rule Goal:** Detects local user creation on windows servers, which should not happen in an Active Directory environment. Apply this Sigma Use Case on your windows server logs and not on your DC logs.

**Attack Instructions**

1. Log on to test endpoint system
2. Launch Windows Settings and click on Accounts
3. Go to Family & Other Users, then create a new user account
4. Run FreeEDR to determine if appropriate alerts have been generated

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Test 10**

**Rule Name:** Persistence - Accessibility Features - Suspicious Accessibility Programs - T1015

**Rule Goal:** Detects Accessibility Features suspiciously launched by PowerShell or CMD

**Attack Instructions**

1. Log on to test endpoint system
2. Run Cmd.exe or Powershell.exe
3. Execute the following commands
   1. Narrator
   2. Utilman
   3. Magnify
   4. Osk
   5. DisplaySwitch
   6. Sethc
4. Run FreeEDR to determine if appropriate alerts have been generated

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Test 11**

**Rule Name:** Defense Evasion - File Deletion - Deletion of Malware - T1107

**Rule Goal:** Detects deletion of malware using the DEL or ERASE commands

**Attack Instructions**

1. Log on to test endpoint system
2. Create sample files to delete
3. Run Cmd.exe and navigate to the folder with the sample files
4. Execute the following commands
   1. Del (sample file name here)
   2. Erase (sample file name here)
5. Run FreeEDR to determine if appropriate alerts have been generated

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Test 12**

**Rule Name:** Disabling Windows Event Auditing

**Rule Goal:** Detects scenarios where system auditing is disabled

**Attack Instructions**

1. Log on to test endpoint system
2. Open Local Security Policy application
3. Navigate to Local Policies > Audit Policy
4. Change system audit policies to be disabled
5. Run FreeEDR to determine if appropriate alerts have been generated

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**