GETTING TO THE SOUL OF INCIDENT RESPONSE
Attacks on Software Publishing Infrastructure and Windows Detection Capabilities

Imran Islam & Dave Jones
June 2016
Attacks on Software Publishing Infrastructure
5% of SySAdmin accounts or their laptops may be compromised at any moment

• Ask dave
From the recent news:

“Juniper said that someone managed to get into its systems and write "unauthorized code" that "could allow a knowledgeable attacker to gain administrative access."

“LANDESK has found remnants of text files with lists of source code and build servers that the attackers compiled,” John said. “They know for a fact that the attackers have been slowly [archiving] data from the build and source code servers, uploading it to LANDESK’s web servers, and downloading it.”
Infestation & Lateral Movement

1. User desktop infected WCE or Mimikatz is started
2. Privileged user or Application logs in - WCE hijacks credentials
3. Rootkit remotely installed on server in datacenter
4. Super user performs task on datacenter server, malware hijacks credentials
5. Malware spreads throughout datacenter

Malware details
- Targeting older software (Flash, Word, Acrobat Reader, Java)
- Malware customized to avoid AV signatures
- Higher they get – the more unique the malware
Infestation Abuses Applied
Software Publishing Infrastructure

1. Engineer desktop infected. Access to source code and Build server available
2. SysAdmin targeted for access to systems and/or the Distribution Creds.
3. SysAdmin laptop infected
4. Either way Customers are infected
Windows Detection Capabilities
AGENDA

- Scope & References
- Why Another Audit Document
- Auditing Quick Overview
- Need For A Partnered Approach.
- Review Auditing & Associated Events.
- Review Registry Auditing.
- Dashboard & Queries.
- Next Steps.
SCOPE & REFERENCES

- Focus Is On Windows 2008 (& Newer) systems.
- More Details: iIslam@cisco.com
WHY ANOTHER AUDIT DOCUMENT

- Red Team Lessons Learnt.
- Audit Category/Sub Category <> Event ID Mapping
AUDITING QUICK OVERVIEW

1. **ENABLE AUDITING**
   - Suggested minimum list of audit entries is provided in the “Windows Auditing” document.

2. **ENABLE REGISTRY SACL**
   - Instructions on which keys to monitor and how to enable this are in the document.

3. **CAPTURE LOGS**

4. **PRESENT DATA**
   - Reference queries have been provided in the auditing document.

5. **OPERATIONS TEAM**
   - Lots of interesting data to hunt with

   - MALWARE HUNTING
   - ESCALATE
   - CSIRT
   - CSIRT

   **STEP 1**
   **STEP 2**
   **STEP 3**
   **STEP 4**
   **STEP 5**

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential 13
NEED FOR A PARTNERED APPROACH

- Increasing Number Of Systems & Applications.
- Security Teams - Limited Ops Awareness
- Ops Teams - Limited Security Awareness.
- Raise Security Awareness!
REVIEW AUDITING & ASSOCIATED EVENTS

- Open GPMC
- Audit Policy
- Once Done...
- It Should Look Something Like.
# REVIEW AUDITING & ASSOCIATED EVENTS

<table>
<thead>
<tr>
<th>CATEGORY</th>
<th>SUBCATEGORY</th>
<th>MEMBER SERVER SETTING</th>
<th>DOMAIN CONTROLLER SETTING</th>
<th>EVENTS TO MONITOR</th>
</tr>
</thead>
<tbody>
<tr>
<td>System</td>
<td>Security System Extension</td>
<td>Success</td>
<td>Success and Failure</td>
<td>4651 (trusted login - success)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>4957 (service installation)</td>
</tr>
<tr>
<td></td>
<td>System Integrity</td>
<td>Success and Failure</td>
<td>Success and Failure</td>
<td>8086 (code integrity - hash of file is invalid)</td>
</tr>
<tr>
<td></td>
<td>iSCSI Driver</td>
<td>An Auditing</td>
<td>An Auditing</td>
<td>4063 (iSCSI dropped an inbound packet failed a replay check. It could indicate an replay attack against this computer)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>4062 (iSCSI dropped an inbound packet failed a replay check. Too low a sequence number to ensure it was not a replay)</td>
</tr>
<tr>
<td></td>
<td>Other System Events</td>
<td>Success</td>
<td>Success and Failure</td>
<td>5024 (Rew ind started)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>5025 (Rew ind stopped)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>5030 (Rew ind failed to start)</td>
</tr>
<tr>
<td></td>
<td>Security State Change</td>
<td>Success and Failure</td>
<td>Success and Failure</td>
<td>4608 (system start up)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>4609 (system shutdown)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>4620 (line change)</td>
</tr>
<tr>
<td>Login/Logoff</td>
<td>Legon</td>
<td>Success and Failure</td>
<td>Success and Failure</td>
<td>4624 (login success)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>4625 (login fail)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>4626 (Failure Reason- &quot;Account locked out&quot;)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>4640 (explicit password used for example: $pass$)</td>
</tr>
<tr>
<td></td>
<td>Legon</td>
<td>Success and Failure</td>
<td>Success and Failure</td>
<td>4642 (user logout)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>4654 (account logoff)</td>
</tr>
<tr>
<td></td>
<td>Account Lockout</td>
<td>An Auditing</td>
<td>An Auditing</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>iPsac Main Mode</td>
<td>An Auditing</td>
<td>An Auditing</td>
<td>4664 (IKE DLP: prevention mode started)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>4650 (An IKE security association was established. Certificate auth was not used)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>4651 (An IKE main mode security association was established. Cert used for auth.)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>4652 (An IKE main mode negotiation was failed.)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>4653 (An IKE main mode negotiation was failed.)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>4654 (An IKE main mode security association ended)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>4076 (During main mode negotiation, IPSec received an invalid negotiation packet. If this problem persists, it could indicate a network issue or an attempt to modify or replay this negotiation.)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>5649 (An IKE security association was deleted.)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>5642 (An IKE quick mode security association was established.)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>4075 (During quick mode negotiation, IPSec received an invalid negotiation packet. If this problem persists, it could indicate a network issue or an attempt to modify or replay this negotiation.)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>5643 (An IKE quick mode security association was established.)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>5644 (An IKE quick mode security association was established.)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>4078 (During extended mode negotiation, IPSec received an invalid negotiation packet.)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>4979 (IPSec mainmode and extended mode security associations were established.)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>4980 (IPSec mainmode and extended mode security associations were established.)</td>
</tr>
</tbody>
</table>
REVIEW REGISTRY AUDITING


<table>
<thead>
<tr>
<th>Object Access</th>
<th>File System</th>
<th>Registry</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Access</td>
<td>Access</td>
</tr>
<tr>
<td></td>
<td>4660 (object deleted)</td>
<td>4660 (object deleted)</td>
</tr>
<tr>
<td></td>
<td>4662 (object accessed)</td>
<td>4663 (registry access)</td>
</tr>
<tr>
<td></td>
<td>4665 (registry modifications)</td>
<td>4667 (registry modifications)</td>
</tr>
</tbody>
</table>

2. Enable SACL (audit)
### REVIEW AUDITING & ASSOCIATED EVENTS

<table>
<thead>
<tr>
<th>AD SERVERS</th>
<th>Windows Servers</th>
</tr>
</thead>
<tbody>
<tr>
<td>~258 Hosts*</td>
<td>~4500 Hosts</td>
</tr>
<tr>
<td>~587 Million Event</td>
<td>~171 Million Event</td>
</tr>
<tr>
<td>~142GB Storage</td>
<td>~44GB Storage</td>
</tr>
</tbody>
</table>

**Data Collection:** 24 Hour Period

---

**AD SERVERS**

- ~258 Hosts*
- ~587 Million Event
- ~142GB Storage

**WINDOWS SERVERS**

- ~4500 Hosts
- ~171 Million Event
- ~44GB Storage
DASHBOARD & QUERIES

- Dashboards
- Key Differences:
  - Drop Down Selection Boxes.
  - Admin Accounts/Privileged Groups
- Standard Operational View.
- Change “Index” For Queries
- Tags & Macros
  - Remove Known Good Behaviour
- Due To Time – Windows Only
DASHBOARD & QUERIES

- Event Summary By Task Category
- Event Summary By Host
- Host Support Details
- System Shutdown & Restart
- Local Security Group Change Monitoring
- Authorizations
  - Successful Authorizations
  - Successful Authorizations Grouped By User
  - Failed Authorizations
  - Failed Authorizations Grouped By User
- MSI Package Installations
- Suspect PowerShell Commands
- Process Execution Monitored Commands
- Process Execution
  - Most Common
  - Least Common
- Process Tracking By User
- New Service Installations
- Suspicious Services
- Registry Persistence Key Monitoring
- Scheduled Task Monitoring
- Firewall Change Monitoring
- Application Crashes
- Shares Remotely Accessed
- Local Account Password Changes.
- Event Category Activity Spikes Over Time
- Cross Reference To System/s Responsible

```
$search index=win | timechart count(EventCode) by TaskCategory
```

```
$search index=win | eval host=lower(host) | chart count over host by TaskCategory
```
index=win source=WinEventLog:Security EventCode=4624 | eval "Activity Time"=(_time) | eval User=mvindex(Account_Name,1) | eval User_Domain=mvindex(Account_Domain,1) | eval Sub_Status=lower(Sub_Status) | eval Status=lower(Status) | eval ComputerName=upper(ComputerName) | eval Workstation_Name=upper(Workstation_Name) | search NOT ((Status=0xc000006d Sub_Status=0xc0000321) OR (User=*$) OR (User_Domain="nt authority")) | lookup logon_types_explained.csv Logon_Type as Logon_Type output Summary as Logon_Summary | lookup Windows_Event_Status_Codes.csv Error_Code as Status output Error_Message AS Status_Message | lookup Windows_Event_Status_Codes.csv Error_Code as Sub_Status output Status_Description AS SubStatus_Message | rename Workstation_Name AS Source_Computer, ComputerName AS Destination_Computer, Caller_Process_Name AS Process_Name, Source_Network_Address AS Originating_Source_IP | transaction mvlist=t User | table "Activity Time" User User_Domain Originating_Source_IP Source_Computer Destination_Computer Process_Name Keywords EventCode Logon_Summary Status_Message SubStatus_Message Authentication_Package

SUCCESSFUL AUTHORIZATION ACTIVITY GROUPED BY USERNAME

<table>
<thead>
<tr>
<th>Activity Time</th>
<th>User</th>
<th>User_Domain</th>
<th>Originating_Source_IP</th>
<th>Source_Computer</th>
<th>Destination_Computer</th>
<th>Process_Name</th>
<th>Keywords</th>
<th>EventCode</th>
<th>Logon_Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>05/23/2015 01:10:05 CDT</td>
<td>DefaultUser</td>
<td>is (app)</td>
<td>-</td>
<td>NULL</td>
<td>NULL</td>
<td>MSH:14-A01-V1:CISCO.COM</td>
<td>NULL</td>
<td>Audit Success</td>
<td>46.24 Service</td>
</tr>
<tr>
<td>05/23/2015 02:13:36 CDT</td>
<td>DefaultUser</td>
<td>is (app)</td>
<td>-</td>
<td>NULL</td>
<td>NULL</td>
<td>MSH:14-A01-V2:CISCO.COM</td>
<td>NULL</td>
<td>Audit Success</td>
<td>46.24 Service</td>
</tr>
<tr>
<td>05/23/2015 02:37:42 CDT</td>
<td>DefaultUser</td>
<td>is (app)</td>
<td>-</td>
<td>NULL</td>
<td>NULL</td>
<td>MSH:14-A01-V3:CISCO.COM</td>
<td>NULL</td>
<td>Audit Success</td>
<td>46.24 Service</td>
</tr>
</tbody>
</table>

Show Log On Activity To Service Grouped By User

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential 23
DASHBOARD & QUERIES – SUSPECT POWERSHELL ACTIVITY

- **Suspect PowerShell Commands**
  - Identify Bypass, Hidden or Encoded Command Lines

```powershell
index=win EventCode=4688 powershell.exe (unrestricted OR bypass OR hidden OR Enc OR encodecommand) NOT power_shell_macro | eval User=mvindex(Account_Name,0) | eval Activity_Time=(_time) | search NOT User=*$ | decrypt f=PCL_Encoded_String atob emit('Decoded_Stager') | transaction host User mvlist=t | table Activity_Time User host Creator_Process_Name New_Process_Name Process_Command_Line Decoded_Stager | convert timeformat="%m/%d/%Y %H:%M:%S %Z" ctime(Activity_Time)
```

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential
- Identify Admin Commands Being Run
  - Only List If 4 Or More Unique Commands Have Been Run
  - Leveraging sub searches & Lookup Tables

```plaintext
index=win source=WinEventLog:Security EventCode=4688 NOT `proc_mon_macro` [search index=win
source=WinEventLog:Security EventCode=4688 NOT `proc_mon_macro` rex field=New_Process_Name
"(?P<Process_Name>[^\\]+)$" | search [inputlookup suspect_proc_mon.csv | fields + Process_Name] | stats
Values(New_Process_Name), dc(New_Process_Name) AS New_Process_Count BY ComputerName | where (New_Process_Count
>=4) | fields + ComputerName] | rex field=New_Process_Name "(?P<Process_Name>[^\\]+)$" | search [inputlookup
suspect_proc_mon.csv | fields + Process_Name] | dedup ComputerName New_Process_Name Process_Command_Line | eval
Activity_Time=(_time) | transaction ComputerName mvlist=t | table Activity_Time, ComputerName,
Account_Domain, Account_Name, Logon_ID, Process_Name, New_Process_Name, Process_Command_Line Token_Elevation_Type eventcount |
convert timeformat="%m/%d/%Y %H:%M:%S %Z" ctime(Activity_Time)
```
`proc_mon_macro`
DASHBOARD & QUERIES – PROCESS EXECUTION MONITORED CMDS

- Commands Being Looked For.
DASHBOARD & QUERIES – PROCESS EXECUTION MONITORED CMDS

- If 4 Or More Unique Commands Ran.
- Show Results Of Each Command & Command Line Together With User & Time.
**Show Who Is Running What...**

index=win source=WinEventLog:Security EventCode=4688 NOT ("NT AUTHORITY\SYSTEM" OR Account_Name="\$") eval PID=tonumber(New_Process_ID, 16) eval PPID=tonumber(Creator_Process_ID, 16) eval "Activity Time"=(_time) transaction ComputerName Account_Name Account_Domain mvlist=keepevicted=true table "Activity Time", ComputerName,Security_ID Account_Name, Logon_ID, Account_Domain, PID, New_Process_Name, Process_Command_Line, Token_Elevation_Type, PPID convert timeformat=%m/%d/%Y %H:%M:%S %Z" ctime("Activity Time") | sort Account_Name -"Activity Time"

---

**DASHBOARD & QUERIES**

---

<table>
<thead>
<tr>
<th>Activity Time</th>
<th>ComputerName</th>
<th>Security_ID</th>
<th>Account_Name</th>
<th>Logon_ID</th>
<th>Account_Domain</th>
<th>PID</th>
<th>New_Process_Name</th>
<th>Process_Command_Line</th>
<th>Token_Elevation_Type</th>
<th>PPID</th>
<th>&quot;Activity Time&quot;</th>
<th>ComputerName</th>
<th>Account_Name</th>
<th>Logon_ID</th>
<th>Account_Domain</th>
<th>PID</th>
<th>New_Process_Name</th>
<th>Process_Command_Line</th>
<th>Token_Elevation_Type</th>
<th>PPID</th>
<th>&quot;Activity Time&quot;</th>
</tr>
</thead>
</table>
### SUSPICIOUS SERVICES

<table>
<thead>
<tr>
<th>Time</th>
<th>Account_Name</th>
<th>Account_Domain</th>
<th>Logon_ID</th>
<th>ComputerName</th>
<th>EventCode</th>
<th>Process_Name</th>
<th>Operation_Type</th>
<th>Object_Name</th>
<th>Old_Value_Type</th>
<th>Old_Value</th>
<th>New_Value_Type</th>
<th>New_Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016-05-04 09:20</td>
<td>Administrator</td>
<td>NEMI-Lab1.v1</td>
<td>06/07/55</td>
<td>NEMI-Lab1.v1.cisco.com</td>
<td>4657</td>
<td>C:\Windows\regedit.exe</td>
<td>Registry Value modif</td>
<td>&quot;\REGISTRY\MACHINE\SYSTEM\ControlSet*&quot;</td>
<td>REG_EXPAND_SZ</td>
<td>C:\Windows\regedit.exe</td>
<td>REG_EXPAND_SZ</td>
<td>C:\Windows\regedit.exe</td>
</tr>
<tr>
<td>2016-05-04 09:16</td>
<td>Administrator</td>
<td>NEMI-Lab1.v1</td>
<td>06/07/55</td>
<td>NEMI-Lab1.v1.cisco.com</td>
<td>4657</td>
<td>C:\Windows\regedit.exe</td>
<td>Registry Value modif</td>
<td>&quot;\REGISTRY\MACHINE\SYSTEM\ControlSet*&quot;</td>
<td>REG_EXPAND_SZ</td>
<td>C:\Windows\regedit.exe</td>
<td>REG_EXPAND_SZ</td>
<td>C:\Windows\regedit.exe</td>
</tr>
<tr>
<td>2016-05-04 09:15</td>
<td>Administrator</td>
<td>NEMI-Lab1.v1</td>
<td>06/07/55</td>
<td>NEMI-Lab1.v1.cisco.com</td>
<td>4657</td>
<td>C:\Windows\regedit.exe</td>
<td>Registry Value modif</td>
<td>&quot;\REGISTRY\MACHINE\SYSTEM\ControlSet*&quot;</td>
<td>REG_EXPAND_SZ</td>
<td>C:\Windows\regedit.exe</td>
<td>REG_EXPAND_SZ</td>
<td>C:\Windows\regedit.exe</td>
</tr>
<tr>
<td>2016-05-04 09:15</td>
<td>Administrator</td>
<td>NEMI-Lab1.v1</td>
<td>06/07/55</td>
<td>NEMI-Lab1.v1.cisco.com</td>
<td>4657</td>
<td>C:\Windows\regedit.exe</td>
<td>Registry Value modif</td>
<td>&quot;\REGISTRY\MACHINE\SYSTEM\ControlSet*&quot;</td>
<td>REG_EXPAND_SZ</td>
<td>C:\Windows\regedit.exe</td>
<td>REG_EXPAND_SZ</td>
<td>C:\Windows\regedit.exe</td>
</tr>
</tbody>
</table>

**Shows Us If The Service Executable/Driver Is Not In \SYSTEM32\**

```sql
search index=windows source=WinEventLog:Security TaskCategory="Registry" EventCode=4657 Object_Name="\REGISTRY\MACHINE\SYSTEM\ControlSet*"
Object_Value_Name=ImagePath (Old_Value!="system32" OR New_Value!="system32") | table _time Account_Name Account_Domain Logon_ID ComputerName EventCode Process_Name Operation_Type Object_Name Old_Value_Type Old_Value New_Value_Type New_Value | sort -time
```
# DASHBOARD & QUERIES – REGISTRY PERSISTENCE KEY

- Identify Persistence Key Modifications.

```sql
index=windows source=WinEventLog:Security TaskCategory="Registry" EventCode=4657 NOT (Object_Name="\REGISTRY\MACHINE\SYSTEM\ControlSet001\services\*") | table _time Account_Name Account_Domain ComputerName EventCode Process_Name Operation_Type Object_Name Old_Value New_Value | dedup Account_Name, ComputerName, Process_Name, Operation_Type, Object_Name, Old_Value, New_Value | rename Account_Name AS "User", Account_Domain AS "User Domain", Process_Name AS "Process Making Change", Operation_Type AS "Registry Operation", Object_Name AS "Registry Service Path", Old_Value AS "Old Registry Value", New_Value AS "New Registry Value"
```

<table>
<thead>
<tr>
<th>_time</th>
<th>User</th>
<th>User Domain</th>
<th>ComputerName</th>
<th>EventCode</th>
<th>Process Making Change</th>
<th>Registry Operation</th>
<th>Registry Service Path</th>
<th>Old Registry Value</th>
<th>New Registry Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>2018-05-23 02:27:54</td>
<td>Administrator</td>
<td>MEM1-LAB1-V1</td>
<td>MEM1-LAB1-V1.cisco.com</td>
<td>4657</td>
<td>C:\Windows\System32\reg.exe</td>
<td>Registry value deleted</td>
<td>\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run</td>
<td>C:\UserEvil\Binary.exe</td>
<td>-</td>
</tr>
<tr>
<td>2018-05-23 02:07:31</td>
<td>Administrator</td>
<td>MEM1-LAB1-V1</td>
<td>MEM1-LAB1-V1.cisco.com</td>
<td>4657</td>
<td>C:\Windows\System32\reg.exe</td>
<td>New registry value created</td>
<td>\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run</td>
<td>-</td>
<td>C:\UserEvil\Binary.exe</td>
</tr>
<tr>
<td>2018-05-23 01:08:37</td>
<td>NEM1-LAB1-V1</td>
<td>CISCO</td>
<td>MEM1-LAB1-V1.cisco.com</td>
<td>4657</td>
<td>C:\Windows\System32\wininit.exe</td>
<td>Existing registry value modified</td>
<td>\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon</td>
<td>19</td>
<td>5</td>
</tr>
</tbody>
</table>

Registry Persistence

Dashboards & Queries – Shares Accessed

- Identify Shares Being Remotely Accessed

```
index=win  EventCode=5140 NOT (Account_Name=*$ OR Account_Name="ANONYMOUS LOGON" OR "SYSVOL" OR "IPC") | eval "Activity Time"=(_time) | transaction Source_Address mvlist=t | table "Activity Time" Account_Name Source_Address Account_Domain host Share_Name EventCode | convert timeformat="%m/%d/%Y %H:%M:%S %Z" ctime("Activity Time") | sort "Activity Time"
```

### Shares Remotely Accessed

<table>
<thead>
<tr>
<th>Activity Time</th>
<th>Account_Name</th>
<th>Source_Address</th>
<th>Account_Domain</th>
<th>Host</th>
<th>Share_Name</th>
<th>EventCode</th>
</tr>
</thead>
<tbody>
<tr>
<td>05/23/2016 01:22:30 CDT</td>
<td>Administrator</td>
<td>173.38.02.34</td>
<td>NEMI-LAB1-M2</td>
<td>mem-Hub1-v2</td>
<td>NEMI-LAB1-M2</td>
<td>5140</td>
</tr>
<tr>
<td>05/23/2016 01:44:44 CDT</td>
<td>Administrator</td>
<td>10.220.24.45</td>
<td>CISCO</td>
<td>mem-Hub1-v1</td>
<td>MEMI-LAB1-M1</td>
<td>5140</td>
</tr>
<tr>
<td>05/23/2016 02:23:23 CDT</td>
<td>Administrator</td>
<td>127.30.0.1</td>
<td>NEMI-LAB1-M1</td>
<td>mem-Hub1-v2</td>
<td>NEMI-LAB1-M1</td>
<td>5140</td>
</tr>
<tr>
<td>05/23/2016 02:48:18 CDT</td>
<td>islam</td>
<td>10.220.24.45</td>
<td>CISCO</td>
<td>mem-Hub1-v1</td>
<td>MEMI-LAB1-M1</td>
<td>5140</td>
</tr>
<tr>
<td>05/23/2016 02:48:18 CDT</td>
<td>islam</td>
<td>10.220.24.45</td>
<td>CISCO</td>
<td>mem-Hub1-v1</td>
<td>MEMI-LAB1-M1</td>
<td>5140</td>
</tr>
<tr>
<td>05/23/2016 02:48:18 CDT</td>
<td>islam</td>
<td>10.220.24.45</td>
<td>CISCO</td>
<td>mem-Hub1-v1</td>
<td>MEMI-LAB1-M1</td>
<td>5140</td>
</tr>
<tr>
<td>05/23/2016 02:48:18 CDT</td>
<td>islam</td>
<td>10.220.24.45</td>
<td>CISCO</td>
<td>mem-Hub1-v1</td>
<td>MEMI-LAB1-M1</td>
<td>5140</td>
</tr>
<tr>
<td>05/23/2016 03:56:40 CDT</td>
<td>Administrator</td>
<td>10.65.06.185</td>
<td>NEMI-LAB1-M1</td>
<td>mem-Hub1-v2</td>
<td>NEMI-LAB1-M1</td>
<td>5140</td>
</tr>
<tr>
<td>05/23/2016 04:49:44 CDT</td>
<td>Administrator</td>
<td>10.65.06.185</td>
<td>NEMI-LAB1-M1</td>
<td>mem-Hub1-v2</td>
<td>NEMI-LAB1-M1</td>
<td>5140</td>
</tr>
</tbody>
</table>

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential 32
NEXT STEPS

- **POWERSHELL (version requirement)**
  - EXPLOIT TOOLS
    - [https://github.com/PowerShellMafia/PowerSploit](https://github.com/PowerShellMafia/PowerSploit)
    - [https://github.com/PowerShellEmpire/PowerTools/tree/master/PowerUp](https://github.com/PowerShellEmpire/PowerTools/tree/master/PowerUp)
  - LOGGING
    - [https://www.petri.com/enable-powershell-logging](https://www.petri.com/enable-powershell-logging)
    - [https://logrhythm.com/blog/powershell-command-line-logging/](https://logrhythm.com/blog/powershell-command-line-logging/)

- **WMI**

- **SYSMON (FILE HASH)**

- **FIREWALL**
  - Audit Category: Object Access, Subcategory: Filtering Platform Connections  (high event volume)
NEXT STEPS

- Useful Sources... (Thank You)
  
  http://eventopedia.cloudapp.net/Events/?/Operating+System/Microsoft+Windows
  https://helgeklein.com/download/
  https://www.404techsupport.com/2010/05/rsop-and-gpresult-must-know-tools-when-using-group-policy/
  http://www.computerstepbystep.com/turn-off-multicast-name-resolution.html
  https://support.microsoft.com/en-us/kb/299656

- Download “Windows Auditing Guide”
  
  Download: https://cisco.box.com/v/15062016 (pwd: first_seoul)