|  |
| --- |
| Project Report |
| Schedule |
|  |
| |  |  | | --- | --- | | **Professor:** | **Dr. Faghani** | |  |  | | **Students Name**: | Ali Reza Abedzadeh Anaraki (Ivan) Jin Huang  Moksh rajput | |  |  | | **Course** | DPI911 / Section A | |

Table of Contents

[1 Schedule 2](#_Toc1640854)

Project Report

# Schedule

|  |  |  |  |
| --- | --- | --- | --- |
| **Technique** | **ID** | **Date:** |  |
| Drive-by Compromise https://attack.mitre.org/techniques/T1189/ | T1189 | Mar21 |  |
| CMSTP https://attack.mitre.org/techniques/T1191 | **T1191** | Mar07 | ("cmstp.exe" AND "\*.inf") AND ("EventCode=1" OR "EventCode=3") OR ("EventCode=12" OR "EventCode=13")  --------------------------------------------  msctp.exe AND ( "eventcode=13" OR "eventcode=12" )  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ ("cmstp.exe" AND "EventCode=1" AND "\*.inf" ) OR ("cmstp.exe" AND (("EventCode=3"  OR "EventCode=1") OR ("EventCode=4688")) OR ("EventCode=12" OR "EventCode=13")) |
| Command-Line Interface https://attack.mitre.org/techniques/T1059/ | **T1059** | Mar07 | "CommandLine:\*" |
| Compiled HTML File https://attack.mitre.org/techniques/T1223/ | **T1223** | Mar07 | ("EventCode=1" AND "Image:\*hh.exe" AND "CommandLine:\*" AND "ParentImage:\*cmd.exe") OR ("EventCode=1" AND "Image:\*hh.exe" AND "\*.chm") ----------------------------------------------  "hh.exe" AND "EventCode=1" AND "cmd.exe" AND "\*.chm" |
| Time Providers  RegCreateKeyEx (handle to open registery key in c)  Dll requirement ? | T1209 | Mar19 | RegCreateKeyEx OR RegSetValueEx OR W32tm.exe  ---------------- audit system events enable ( audit time change) |
| Valid Accounts | T1078 | Mar19 | Audits enable , AND "CommandLine:\*"  Machine learning ? anomaly detection ?? |
| Web Shell | T1100 | Mar21 |  |
| Windows Management Instrumentation Event Subscription | **T1084** | Mar14 |  |
| Winlogon Helper DLL | **T1004** | Mar14 |  |
| Application Shimming | **T1138** | Mar14 |  |
| Bypass User Account Control | **T1088** | Mar14 |  |
| DLL Search Order Hijacking | T1038 | Apr 01 |  |
| Access Token Manipulation  [https://attack.mitre.org/techniques/T1134](https://attack.mitre.org/techniques/T1134/)  event 4688 new process created  search mimicats | **T1134** | March12 | "eventcode=4688" AND  Microsoft ATP defender ATP |
| BITS Jobs | **T1197** | March14 | "bitsadmin" AND ( "Transfer" OR "Create" OR "AddFile" OR "SetNotifyFlags" OR "SetNotifyCmdLine" OR "SetMinRetryDelay" OR "SetCustomHeaders" OR "Resume") |
| Binary Padding  [https://attack.mitre.org/techniques/T1009](https://attack.mitre.org/techniques/T1009/) | **T1009** | March12 | Padding technique can not be detected this way. Since the padding or garbage added to file can be anything at any size. Same problem exist for hashing scenario. Talk to Dr. Faghani |
| Bypass User Account Control  <https://attack.mitre.org/techniques/T1088>   * The eventvwr.exe bypass uses the [HKEY\_CURRENT\_USER]\Software\Classes\mscfile\shell\open\command Registry key. [[6]](https://enigma0x3.net/2016/08/15/fileless-uac-bypass-using-eventvwr-exe-and-registry-hijacking/) * The sdclt.exe bypass uses the [HKEY\_CURRENT\_USER]\Software\Microsoft\Windows\CurrentVersion\App Paths\control.exe and [HKEY\_CURRENT\_USER]\Software\Classes\exefile\shell\runas\command\isolatedCommand Registry keys. [[30]](https://enigma0x3.net/2017/03/14/bypassing-uac-using-app-paths/) [[31]](https://enigma0x3.net/2017/03/17/fileless-uac-bypass-using-sdclt-exe/) | **T1088** | March12 | Not possible with splunk forwarder, also require domain controller to monitor registry or splunk enterprise on local machine as well  <https://docs.splunk.com/Documentation/Splunk/7.2.4/Data/MonitorWindowsregistrydata>  C:\ProgramData\osquery\packs\ windows-registry-monitoring.conf |
| CMSTP  <https://attack.mitre.org/techniques/T1191> | **T1191** | March12 | ("cmstp.exe" AND "\*.inf") AND ("EventCode=1" OR "EventCode=3") -------------------------------------------- "cmstp.exe" AND "EventCode=1" AND "\*.inf"  "cmstp.exe" AND "EventCode=3" |
| Code Signing | T1116 | Mar26 |  |
| Account Manipulation  4720 A user account was created  4722 A user account was enabled  4725 A user account was disabled  4726 A user account was deleted  4738 A user account was changed  4740 A user account was locked out  4741 A computer account was created  4742 A computer account was changed  4743 A computer account was deleted  4767 A user account was unlocked  4797 An attempt was made to query the existence of a blank password for an account | **T1098** | Mar07 | "eventcode=4720" OR "eventcode=4722" OR "eventcode=4725" OR "eventcode=4726" OR "eventcode=4738" OR "eventcode=4740" OR "eventcode=4741" OR "eventcode=4742" OR "eventcode=4743" OR "eventcode=4767" OR "eventcode=4797"  ------------------------------------- |
| Brute Force 4625 An account failed to log on 4740 A user account was locked out  4797 An attempt was made to query the existence of a blank password for an account | **T1110** | Mar07 | "eventcode=4740" OR "eventcode=4625" OR "eventcode=4797" Or "eventype=4” AND IPC$ OR Net\*user\*/Domain\* |
| Network Sniffing | **T1040** | Mar07 | tshark.exe OR wireshark.exe OR tcpdump.exe OR npcap.exe OR windump.exe OR dumpcap.exe OR USBPcapCMD.exe OR rawshark |
| Password Policy Discovery | **T1201** | Mar07 | commandline:"net accounts\*" ----------------------------------- note there is two space between “net account” may use with \* |
| Application Deployment Software | T1017 | Mar26 |  |
| Distributed Component Object Model | T1175 | Mar 28 |  |
| Data from Information Repositories | T1213 | Mar 28 |  |
| Automated Exfiltration | T1020 | April 01 |  |
| Commonly Used Port | T1043 | April 04 |  |
| Communication Through Removable Media | T1092 | April 04 |  |