Research Meeting Agenda

Marvin Newlin

17 Jul 19

**Updates/Discussion**

* DRB Presentation 17 Jul
* Signed up for research update in CyberAnimal on 26 Aug
* Problem scope concerns from Dr. Taylor

**This Week**

* DRB
* Putting together PEARC Presentation (shared on google slides)
* Familiarizing myself with SeqGAN, figuring out the layout and data input/output formats
* Log File format from Unified Host and Network dataset (2nd page)

**Next Week**

* PEARC presentation dry run at CyberAnimal, solidify presentation
* Figure out log file input into seqGAN

**Week After Next**

* PEARC

{"UserName": "Comp607982$", "EventID": 4688, "LogHost": "Comp607982", "LogonID": "0x3e7", "DomainName": "Domain001", "ParentProcessName": "services", "ParentProcessID": "0x2ac", "ProcessName": "svchost.exe", "Time": 1, "ProcessID": "0x1418"}

{"UserName": "Comp991643$", "EventID": 4688, "LogHost": "Comp991643", "LogonID": "0x3e7", "DomainName": "Domain001", "ParentProcessName": "services", "ParentProcessID": "0x334", "ProcessName": "rundll32.exe", "Time": 1, "ProcessID": "0xc0c"}

{"UserName": "Comp736087$", "EventID": 4688, "LogHost": "Comp736087", "LogonID": "0x3e7", "DomainName": "Domain001", "ParentProcessName": "services", "ParentProcessID": "0x2e8", "ProcessName": "svchost.exe", "Time": 1, "ProcessID": "0x2074"}

{"UserName": "Comp093128$", "EventID": 4688, "LogHost": "Comp093128", "LogonID": "0x3e7", "DomainName": "Domain001", "ParentProcessName": "services", "ParentProcessID": "0x2d4", "ProcessName": "vssvc.exe", "Time": 1, "ProcessID": "0x2200"}

{"UserName": "Comp006850$", "EventID": 4688, "LogHost": "Comp006850", "LogonID": "0x3e7", "DomainName": "Domain001", "ParentProcessName": "services", "ParentProcessID": "0x278", "ProcessName": "svchost.exe", "Time": 1, "ProcessID": "0x498"}

{"UserName": "system", "EventID": 4624, "LogHost": "Comp828729", "LogonID": "0x3e7", "DomainName": "nt authority", "LogonTypeDescription": "Service", "ProcessName": "services.exe", "AuthenticationPackage": "Negotiate", "Time": 1, "LogonType": 5, "ProcessID": "0x29c"}

{"UserName": "system", "EventID": 4672, "LogHost": "Comp828729", "LogonID": "0x3e7", "DomainName": "nt authority", "Time": 1}

{"UserName": "system", "EventID": 4672, "LogHost": "Comp423597", "LogonID": "0x3e7", "DomainName": "nt authority", "Time": 1}

{"UserName": "Comp466209$", "EventID": 4688, "LogHost": "Comp466209", "LogonID": "0x3e7", "DomainName": "Domain001", "ParentProcessName": "services", "ParentProcessID": "0x354", "ProcessName": "vssvc.exe", "Time": 1, "ProcessID": "0x2d20"}

{"UserName": "Comp688526$", "EventID": 4688, "LogHost": "Comp688526", "LogonID": "0x3e7", "DomainName": "Domain001", "ParentProcessName": "services", "ParentProcessID": "0x2b8", "ProcessName": "svchost.exe", "Time": 1, "ProcessID": "0x1ac0"}

{"UserName": "Comp107561$", "EventID": 4688, "LogHost": "Comp107561", "LogonID": "0x3e7", "DomainName": "Domain001", "ParentProcessName": "services", "ParentProcessID": "0x2cc", "ProcessName": "rundll32.exe", "Time": 1, "ProcessID": "0x18c"}

{"UserName": "system", "EventID": 4624, "LogHost": "Comp050550", "LogonID": "0x3e7", "DomainName": "nt authority", "LogonTypeDescription": "Service", "ProcessName": "services.exe", "AuthenticationPackage": "Negotiate", "Time": 1, "LogonType": 5, "ProcessID": "0x2ec"}

{"UserName": "Comp939275$", "EventID": 4624, "LogHost": "Comp661433", "LogonID": "0x23a8696", "DomainName": "Domain001", "LogonTypeDescription": "Network", "Source": "Comp939275", "AuthenticationPackage": "Kerberos", "Time": 1, "LogonType": 3}