Searcher's cheat

Set the index

```
index="main" earliest=0
```

make a list of values

```
index="main" | stats count by sourcetype
```

See 00 - Event-Logs > ^b52217 for sysmon event id's

Filter for values

```
index="main" sourcetype="WinEventLog:Sysmon" EventCode=1 (Image="*cmd.exe"
OR Image="*powershell.exe") | stats count by ParentImage, Image
```

search for stuff

```
index="main" 10.0.0.229 | stats count by sourcetype
```

Dosen't equl

```
index="main" CallTrace="*UNKNOWN*" | where SourceImage!=TargetImage | stats
count by SourceImage
```

Detecting Attacker Behavior With Splunk Based On TTPs

Detection Of Reconnaissance Activities Leveraging Native Windows Binaries

```
index="main" sourcetype="WinEventLog:Sysmon" EventCode=1
Image=*\\ipconfig.exe OR Image=*\\net.exe OR Image=*\\whoami.exe OR
Image=*\\netstat.exe OR Image=*\\nbtstat.exe OR Image=*\\hostname.exe OR
Image=*\\tasklist.exe | stats count by Image,CommandLine | sort - count
```

Detection Of Requesting Malicious Payloads/Tools Hosted On Reputable/Whitelisted Domains (Such As githubusercontent.com)

```
index="main" sourcetype="WinEventLog:Sysmon" EventCode=22
QueryName="*github*" | stats count by Image, QueryName
```

Detection Of PsExec Usage

```
index="main" sourcetype="WinEventLog:Sysmon" EventCode=13
Image="C:\\Windows\\system32\\services.exe"
TargetObject="HKLM\\System\\CurrentControlSet\\Services\\*\\ImagePath" | rex
field=Details "(?<reg_file_name>[^\\\]+)$" | eval reg_file_name =
lower(reg_file_name), file_name =
if(isnull(file_name),reg_file_name,lower(file_name)) | stats values(Image)
AS Image, values(Details) AS RegistryDetails, values(_time) AS EventTimes,
count by file_name, ComputerName
```

OR

```
index="main" sourcetype="WinEventLog:Sysmon" EventCode=11 Image=System |
stats count by TargetFilename
```

OR

```
index="main" sourcetype="WinEventLog:Sysmon" EventCode=18 Image=System |
stats count by PipeName
```

Detection Of Utilizing Archive Files For Transferring Tools Or Data Exfiltration

```
index="main" EventCode=11 (TargetFilename="*.zip" OR TargetFilename="*.rar"
OR TargetFilename="*.7z") | stats count by ComputerName, User,
TargetFilename | sort - count
```

Detection Of Utilizing PowerShell or MS Edge For Downloading Payloads/Tools

```
index="main" sourcetype="WinEventLog:Sysmon" EventCode=11
Image="*powershell.exe*" |  stats count by Image, TargetFilename |  sort +
count
```

msEdge

```
index="main" sourcetype="WinEventLog:Sysmon" EventCode=11
Image="*msedge.exe" TargetFilename=*"Zone.Identifier" |  stats count by
TargetFilename |  sort + count
```

Detection Of Execution From Atypical Or Suspicious Locations

```
index="main" EventCode=1 | regex
Image="C:\\\\Users\\\\.*\\\\Downloads\\\\.*" |  stats count by Image
```

Detection Of Executables or DLLs Being Created Outside The Windows Directory

```
index="main" EventCode=11 (TargetFilename="*.exe" OR TargetFilename="*.dll")
TargetFilename!="*\\windows\\*" | stats count by User, TargetFilename | sort
+ count
```

Detection Of Misspelling Legitimate Binaries

```
index="main" sourcetype="WinEventLog:Sysmon" EventCode=1
(CommandLine="*psexe*.exe" NOT (CommandLine="*PSEXESVC.exe" OR
CommandLine="*PsExec64.exe")) OR (ParentCommandLine="*psexe*.exe" NOT
(ParentCommandLine="*PSEXESVC.exe" OR ParentCommandLine="*PsExec64.exe")) OR
(ParentImage="*psexe*.exe" NOT (ParentImage="*PSEXESVC.exe" OR
ParentImage="*PsExec64.exe")) OR (Image="*psexe*.exe" NOT
(Image="*PSEXESVC.exe" OR Image="*PsExec64.exe")) |  table Image,
CommandLine, ParentImage, ParentCommandLine
```

Detection Of Using Non-standard Ports For Communications/Transfers

```
index="main" EventCode=3 NOT (DestinationPort=80 OR DestinationPort=443 OR
DestinationPort=22 OR DestinationPort=21) | stats count by SourceIp,
DestinationIp, DestinationPort | sort - count
```

Detecting Recon By Targeting Native Windows Executables

```
index=main source="XmlWinEventLog:Microsoft-Windows-Sysmon/Operational"
EventID=1
| search process_name IN
```

```
(arp.exe,chcp.com,ipconfig.exe,net.exe,net1.exe,nltest.exe,ping.exe,systemin
fo.exe,whoami.exe) OR (process_name IN (cmd.exe,powershell.exe) AND process
IN
(*arp*,*chcp*,*ipconfig*,*net*,*net1*,*nltest*,*ping*,*systeminfo*,*whoami*)
)
| stats values(process) as process, min(_time) as _time by parent_process,
parent_process_id, dest, user
| where mvcount(process) > 3
```

Detecting Recon By Targeting BloodHound

```
index=main  source="WinEventLog:SilkService-Log"
| spath input=Message
| rename XmlEventData.* as *
| table _time, ComputerName, ProcessName, ProcessId, DistinguishedName,
SearchFilter
| sort 0 _time
| search SearchFilter="*(samAccountType=805306368)*"
| stats min(_time) as _time, max(_time) as maxTime, count,
values(SearchFilter) as SearchFilter by ComputerName, ProcessName, ProcessId
| where count > 10
| convert ctime(maxTime)
```

Detecting Password Spraying

```
index=main  source="WinEventLog:Security" EventCode=4625
| bin span=15m _time
| stats values(user) as Users, dc(user) as dc_user by src,
Source_Network_Address, dest, EventCode, Failure_Reason
```

Detecting Responder-like Attacks

```
index=main  SourceName=LLMNRDetection
| table _time, ComputerName, SourceName, Message
```

To make sure

```
index=main  EventCode=22
```

```
| table _time, Computer, user, Image, QueryName, QueryResults
```

After they crack the password

```
index=main  EventCode IN (4648)
| table _time, EventCode, source, name, user, Target_Server_Name, Message
| sort 0 _time
```

Detecting Kerberoasting

```
index=main  EventCode=4648 OR (EventCode=4769 AND service_name=iis_svc)
| dedup RecordNumber
| rex field=user "(?<username>[^@]+)"
| table _time, ComputerName, EventCode, name, username, Account_Name,
Account_Domain, src_ip, service_name, Ticket_Options,
Ticket_Encryption_Type, Target_Server_Name, Additional_Information
```

Detecting Kerberoasting - SPN Querying

```
index=main  source="WinEventLog:SilkService-Log"
| spath input=Message
| rename XmlEventData.* as *
| table _time, ComputerName, ProcessName, DistinguishedName, SearchFilter
| search SearchFilter="*(&(samAccountType=805306368)
(servicePrincipalName=*)*"
```

Detecting Kerberoasting - TGS Requests

```
index=main  EventCode=4648 OR (EventCode=4769 AND service_name=iis_svc)
| dedup RecordNumber
| rex field=user "(?<username>[^@]+)"
| bin span=2m _time
| search username!=*$
| stats values(EventCode) as Events, values(service_name) as service_name,
values(Additional_Information) as Additional_Information,
values(Target_Server_Name) as Target_Server_Name by _time, username
| where !match(Events,"4648")
```

Detecting Kerberoasting Using Transactions - TGS Requests

```
index=main  EventCode=4648 OR (EventCode=4769 AND service_name=iis_svc)
| dedup RecordNumber
| rex field=user "(?<username>[^@]+)"
| search username!=*$
| transaction username keepevicted=true maxspan=5s endswith=(EventCode=4648)
startswith=(EventCode=4769)
| where closed_txn=0 AND EventCode = 4769
| table _time, EventCode, service_name, username
```

Detecting AS-REPRoasting - Querying Accounts With Pre-Auth Disabled

```
index=main  source="WinEventLog:SilkService-Log"
| spath input=Message
| rename XmlEventData.* as *
| table _time, ComputerName, ProcessName, DistinguishedName, SearchFilter
| search SearchFilter="*(samAccountType=805306368)
(userAccountControl:1.2.840.113556.1.4.803:=4194304)*"
```

Detecting AS-REPRoasting - TGT Requests For Accounts With Pre-Auth Disabled

```
index=main  source="WinEventLog:Security" EventCode=4768
Pre_Authentication_Type=0
| rex field=src_ip "(\:\:ffff\:)?(?<src_ip>[0-9\.]+)"
| table _time, src_ip, user, Pre_Authentication_Type, Ticket_Options,
Ticket_Encryption_Type
```

Detecting Pass-the-Hash With Splunk

```
index=main source="WinEventLog:Security" EventCode=4624 Logon_Type=9
Logon_Process=seclogo
| table _time, ComputerName, EventCode, user, Network_Account_Domain,
Network_Account_Name, Logon_Type, Logon_Process
```

With Lsass

```
index=main (source="XmlWinEventLog:Microsoft-Windows-Sysmon/Operational"
EventCode=10 TargetImage="C:\\Windows\\system32\\lsass.exe"
SourceImage!="C:\\ProgramData\\Microsoft\\Windows
Defender\\platform\\*\\MsMpEng.exe") OR (source="WinEventLog:Security"
EventCode=4624 Logon_Type=9 Logon_Process=seclogo)
| sort _time, RecordNumber
| transaction host maxspan=1m endswith=(EventCode=4624) startswith=
(EventCode=10)
| stats count by _time, Computer, SourceImage, SourceProcessId,
Network_Account_Domain, Network_Account_Name, Logon_Type, Logon_Process
| fields - count
```

Detecting Pass-the-Ticket With Splunk

```
index=main  source="WinEventLog:Security" user!=*$ EventCode IN
(4768,4769,4770)
| rex field=user "(?<username>[^@]+)"
| rex field=src_ip "(\:\:ffff\:)?(?<src_ip_4>[0-9\.]+)"
| transaction username, src_ip_4 maxspan=10h keepevicted=true startswith=
(EventCode=4768)
| where closed_txn=0
| search NOT user="*$@*"
| table _time, ComputerName, username, src_ip_4, service_name, category
```

Detecting Overpass-the-Hash With Splunk (Targeting Rubeus)

```
index=main  source="XmlWinEventLog:Microsoft-Windows-Sysmon/Operational"
(EventCode=3 dest_port=88 Image!=*lsass.exe) OR EventCode=1
| eventstats values(process) as process by process_id
| where EventCode=3
| stats count by _time, Computer, dest_ip, dest_port, Image, process
| fields - count
```

Detecting Golden Tickets With Splunk (Yet Another Ticket To Be Passed Approach)

```
index=main  source="WinEventLog:Security" user!=*$ EventCode IN
(4768,4769,4770)
| rex field=user "(?<username>[^@]+)"
```

````
| rex field=src_ip "(\:\:ffff\:)?(?<src_ip_4>[0-9\.]+)"
| transaction username, src_ip_4 maxspan=10h keepevicted=true startswith=
(EventCode=4768)
| where closed_txn=0
| search NOT user="*$@*"
| table _time, ComputerName, username, src_ip_4, service_name, category
````

Detecting Silver Tickets With Splunk By Targeting Special Privileges Assigned To New Logon

~~~
index=main  EventCode=4672
| stats min(_time) as firstTime, values(ComputerName) as ComputerName by
Account_Name
| eval last24h = 1690451977
```| eval last24h=relative_time(now(),"-24h@h") ```
| where firstTime > last24h
| table firstTime, ComputerName, Account_Name
| convert ctime(firstTime)
~~~

Detecting Unconstrained Delegation Attacks With Splunk

````
index=main  source="WinEventLog:Microsoft-Windows-PowerShell/Operational"
EventCode=4104 Message="*TrustedForDelegation*" OR
Message="*userAccountControl:1.2.840.113556.1.4.803:=524288*"
| table _time, ComputerName, EventCode, Message
````

Detecting Constrained Delegation Attacks - Leveraging PowerShell Logs

````
index=main  source="WinEventLog:Microsoft-Windows-PowerShell/Operational"
EventCode=4104 Message="*msDS-AllowedToDelegateTo*"
| table _time, ComputerName, EventCode, Message
````

Detecting Constrained Delegation Attacks - Leveraging Sysmon Logs

```
index=main  source="XmlWinEventLog:Microsoft-Windows-Sysmon/Operational"
| eventstats values(process) as process by process_id
| where EventCode=3 AND dest_port=88
| table _time, Computer, dest_ip, dest_port, Image, process
```

Detecting DCSync With Splunk

```
index=main  EventCode=4662 Message="*Replicating Directory Changes*"
| rex field=Message "(?P<property>Replicating Directory Changes.*)"
| table _time, user, object_file_name, Object_Server, property
```

Detecting DCShadow With Splunk

```
index=main  EventCode=4742
| rex field=Message "(?P<gcspn>GC\/[a-zA-Z0-9\.\-\/]+)"
| table _time, ComputerName, Security_ID, Account_Name, user, gcspn
| search gcspn=*
```

Change the index if possible

Detecting RDP Brute Force Attacks With Splunk & Zeek Logs

```
index="rdp_bruteforce" sourcetype="bro:rdp:json"
| bin _time span=5m
| stats count values(cookie) by _time, id.orig_h, id.resp_h
| where count>30
```

Detecting Beaconing Malware With Splunk & Zeek Logs

```
index="cobaltstrike_beacon" sourcetype="bro:http:json"
| sort 0 _time
| streamstats current=f last(_time) as prevtime by src, dest, dest_port
| eval timedelta = _time - prevtime
| eventstats avg(timedelta) as avg, count as total by src, dest, dest_port
| eval upper=avg*1.1
| eval lower=avg*0.9
| where timedelta > lower AND timedelta < upper
| stats count, values(avg) as TimeInterval by src, dest, dest_port, total
| eval prcnt = (count/total)*100
| where prcnt > 90 AND total > 10
```

Detecting Nmap Port Scanning With Splunk & Zeek Logs

```
index="cobaltstrike_beacon" sourcetype="bro:conn:json" orig_bytes=0 dest_ip
IN (192.168.0.0/16, 172.16.0.0/12, 10.0.0.0/8)
| bin span=5m _time
| stats dc(dest_port) as num_dest_port by _time, src_ip, dest_ip
| where num_dest_port >= 3
```

Detecting Kerberos Brute Force Attacks With Splunk & Zeek Logs

```
index="kerberos_bruteforce" sourcetype="bro:kerberos:json"
error_msg!=KDC_ERR_PREAUTH_REQUIRED
success="false" request_type=AS
| bin _time span=5m
| stats count dc(client) as "Unique users" values(error_msg) as "Error
messages" by _time, id.orig_h, id.resp_h
| where count>30
```

Detecting Kerberoasting With Splunk & Zeek Logs

```
index="kerberoast"  sourcetype="bro:kerberos:json"
request_type=TGS cipher="rc4-hmac"
forwardable="true" renewable="true"
| table _time, id.orig_h, id.resp_h, request_type, cipher, forwardable,
renewable, client, service
```

Detecting Golden Tickets With Splunk & Zeek Logs

```
index="golden_ticket_attack" sourcetype="bro:kerberos:json"
| where client!="-"
| bin _time span=1m
| stats values(client), values(request_type) as request_types,
dc(request_type) as unique_request_types by _time, id.orig_h, id.resp_h
| where request_types=="TGS" AND unique_request_types==1
```

Detecting Cobalt Strike's PSExec With Splunk & Zeek Logs

```
index="cobalt_strike_psexec"
sourcetype="bro:smb_files:json"
action="SMB::FILE_OPEN"
name IN ("*.exe", "*.dll", "*.bat")
path IN ("*\\c$", "*\\ADMIN$")
size>0
```

Detecting Zerologon With Splunk & Zeek Logs

```
index="zerologon" endpoint="netlogon" sourcetype="bro:dce_rpc:json"
| bin _time span=1m
| where operation == "NetrServerReqChallenge" OR operation ==
"NetrServerAuthenticate3" OR operation == "NetrServerPasswordSet2"
| stats count values(operation) as operation_values dc(operation) as
unique_operations by _time, id.orig_h, id.resp_h
| where unique_operations >= 2 AND count>100
```

Detecting HTTP Exfiltration With Splunk & Zeek Logs

```
index="cobaltstrike_exfiltration_http" sourcetype="bro:http:json"
method=POST
| stats sum(request_body_len) as TotalBytes by src, dest, dest_port
| eval TotalBytes = TotalBytes/1024/1024
```

Detecting DNS Exfiltration With Splunk & Zeek Logs

```
index=dns_exf sourcetype="bro:dns:json"
| eval len_query=len(query)
| search len_query>=40 AND query!="*.ip6.arpa*" AND query!="*amazonaws.com*"
AND query!="*._googlecast.*" AND query!="_ldap.*"
| bin _time span=24h
| stats count(query) as req_by_day by _time, id.orig_h, id.resp_h
| where req_by_day>60
| table _time, id.orig_h, id.resp_h, req_by_day
```

Detecting Ransomware With Splunk & Zeek Logs (Excessive Overwriting)

```
index="ransomware_open_rename_sodinokibi" sourcetype="bro:smb_files:json"
| where action IN ("SMB::FILE_OPEN", "SMB::FILE_RENAME")
| bin _time span=5m
| stats count by _time, source, action
| where count>30
| stats sum(count) as count values(action) dc(action) as uniq_actions by
_time, source
| where uniq_actions==2 AND count>100
```

Detecting Ransomware With Splunk & Zeek Logs (Excessive Renaming With The Same Extension)

```
index="ransomware_new_file_extension_ctbl_ocker"
sourcetype="bro:smb_files:json" action="SMB::FILE_RENAME"
| bin _time span=5m
| rex field="name" "\.(?<new_file_name_extension>[^\.]*$)"
| rex field="prev_name" "\.(?<old_file_name_extension>[^\.]*$)"
| stats count by _time, id.orig_h, id.resp_p, name, source,
old_file_name_extension, new_file_name_extension,
| where new_file_name_extension!=old_file_name_extension
| stats count by _time, id.orig_h, id.resp_p, source,
new_file_name_extension
| where count>20
| sort -count
```