

Bitte beschriften Sie die Cyber Defense Prüfung mit Ihrem Namen und Vornamen. Ich wünsche Ihnen viel Erfolg!

Name

Vorname

Cyber Defense HS2021

Hauptprüfung

18. Januar 2022

Document Name: 2021_HS21_Cyber_Defense_Hauptprüfung_ohne_Musterlösung_V1.0.docx
Version: V1.0
Author: Ivan Buetler
Classification: EXAM

Inhaltsverzeichnis

1 CYBER DEFENSE HAUPTPRÜFUNG	4
1.1 MITRE ATT&CK FRAMEWORK (6 PUNKTE)	4
1.2 YARA (6 PUNKTE)	6
1.3 VELOCIRAPTOR (8 PUNKTE)	7
1.4 MEMORY FORENSICS (7 PUNKTE)	9
1.5 RED TEAMING (4 PUNKTE)	11
1.6 MUTUAL AUTH (3 PUNKTE)	12
1.7 WEBAPP IN DMZ (12 PUNKTE)	13
1.8 INFORMATIKER STREIT (2 PUNKTE)	15
1.9 DNS OVER HTTP (DOH) (12 PUNKTE)	16
1.10 RANSOMWARE (8 PUNKTE)	19
1.11 RDP BRUTE FORCE ATTACK (2 PUNKTE)	20
1.12 IP BLOCKLIST (3 PUNKTE)	21
1.13 FORENSIK (6 PUNKTE)	22
1.14 GPO (6 PUNKTE)	23
1.15 SIGMA RULES (5 PUNKTE)	24
1.16 ADVISORY (6 PUNKTE)	25
1.17 SSH AUDIT (6 PUNKTE)	27
1.18 NLA (6 PUNKTE)	28
1.19 LARGE SCALE (6 PUNKTE)	29
1.20 SPF/DKIM/DMARC (6 PUNKTE)	30
2 ANHANG	31
2.1 Log4j ADVISORY	31

Punkteverteilung

Aufgabe	1	MITRE	6	Punkte
Aufgabe	2	Yara	6	Punkte
Aufgabe	3	Velociraptor	8	Punkte
Aufgabe	4	Memory Forensics	7	Punkte
Aufgabe	5	Red Teaming	4	Punkte
Aufgabe	6	Mutual Auth	3	Punkte
Aufgabe	7	Web App in DMZ	12	Punkte
Aufgabe	8	Informatiker Streit	2	Punkte
Aufgabe	9	DNS over HTTP	12	Punkte
Aufgabe	10	Ransomware	8	Punkte
Aufgabe	11	RDP Brute Force	2	Punkte
Aufgabe	12	IP Blocklist	3	Punkte
Aufgabe	13	Forensik	6	Punkte
Aufgabe	14	GPO	6	Punkte
Aufgabe	15	SIGMA Rules	5	Punkte
Aufgabe	16	Advisory	6	Punkte
Aufgabe	17	SSH Audit	6	Punkte
Aufgabe	18	NLA	6	Punkte
Aufgabe	19	Large Scale	6	Punkte
Aufgabe	20	SPF/DKIM/DMARC	6	Punkte
TOTAL			120	Punkte

Sprache

Ihre Lösungen müssen in Blockschrift geschrieben werden (lesbar). Die Verwendung von Englischen Begriffen (aus den Folien, Vorlesung) ist absolut ok und erlaubt.

Abändern der Fragestellung

Bitte ändern Sie die Fragestellung der Fragen nicht ab. Belassen Sie die Fragen wie sie sind. Wenn es für Sie Unklarheiten gibt, dann treffen Sie Annahmen. Kennzeichnen Sie ihre Annahmen deutlich.

Zuwenig Platz für Ihre Antworten

Falls Sie zu wenig Platz für Ihre Lösung/Antwort haben, dann nutzen Sie bitte die Rückseite des vorherigen Blattes und machen eine deutlich und klar ersichtliche Referenz darauf (Pfeil, Buchstabe)

Kugelschreiber / Filzstift

Bitte beantworten Sie die Fragen mit einem Kugelschreiber, Füllfederhalter oder Filzstift.

***NICHT* mit Bleistift.**

1 Cyber Defense Hauptprüfung

1.1 MITRE ATT&CK Framework (6 Punkte)

Frage	Antwort	Punkte
Was ist eine Cyber Kill Chain?		1
Erklären Sie was der Begriff "Technique" im MITRE ATT&CK Framework bedeutet.		1
Welchen Zweck verfolgen Angreifer, wenn wie " T1053 Scheduled Task/Job" anwenden?		1

Frage	Antwort	Punkte
Erklären Sie was der Begriff "Tactic" im MITRE ATT&CK Framwork bedeutet.		1
Nennen Sie eine "Tactic" und erklären Sie, was damit gemeint ist.		2

1.2 YARA (6 Punkte)

Frage	Antwort	Punkte
<p>Erklären Sie, inwiefern sich ein Scan mittels YARA Rules von einem Virens Scanner unterscheidet.</p> <p>Nennen Sie dabei je einen Vorteil und einen Nachteil.</p>		2
<p>Sie untersuchen einen Vorfall.</p> <p>Ihr Kollege hat endlich die Malware entdeckt und davon gleich einen SHA256 Hash erstellt.</p> <p>Er will nun alle 5000 Server und Clients in der Infrastruktur auf den Hash durchsuchen.</p> <p>Erklären Sie, warum dies eine gute oder schlechte Idee ist.</p>		2
<p>Wir wollen das Memory eines aktuellen Windows 10 nach einem String durchsuchen und verwenden die YARA Regel nebenan.</p> <p>Leider verläuft die Suche erfolglos. Nennen Sie Gründe, warum die Suche gescheitert ist, und korrigieren Sie die Regel.</p>	<pre>rule Gotham { strings: \$a = "Batman" \$b = "Robin" condition: \$a or \$b }</pre>	2

1.3 Velociraptor (8 Punkte)

Frage	Antwort	Punkte
<p>Sie sind Incident Handler und werden zu einem Notfall gerufen. Die infizierte Firma betreibt über hundert Server und rund tausend Workstations darunter viele Laptops. Für die Analyse deployen Sie einen Velociraptor Server und via GPO die Velociraptor Agents auf die jeweiligen Server und Workstations. Nach rund 30min haben sich aber erst wenige Agents beim zentralen Server gemeldet.</p> <p>Nennen Sie 3 mögliche Ursachen.</p>		3
<p>Sie analysieren ein Fall und haben herausgefunden, dass sich die Angreifer mittels PSEXEC von System zu System bewegen.</p> <p>Sie möchten nun mit Hilfe von Velociraptor herausfinden, welche Systeme betroffen sind.</p> <p>Zählen Sie vier Aktionen auf, die Sie dafür im GUI des Velociraptors ausführen müssen?</p>		2

Frage	Antwort	Punkte
<p>Leider passt keines der vorgefertigten Artefakte für Ihre aktuelle Untersuchung.</p> <p>Sie verwenden das Velociraptor Notebook, um eine neue Query zu programmieren und es werden auch gleich erste Ergebnisse dargestellt.</p> <p>Von welchem System stammen die Ergebnisse des Notebook Output, welche bei der ausgeführten Query angezeigt werden?</p>		1
<p>Wenn ein Benutzer nicht interaktiv am System angemeldet ist, dann ist sein Registry Hive bzw. dann sind seine User spezifischen Registry Einträge nicht in der Registry ersichtlich.</p> <p>Nennen Sie eine Methode, wie man mit Velociraptor trotzdem auf die Registry-Einträge von nicht angemeldeten Benutzern zugreifen kann.</p>		2

1.4 Memory Forensics (7 Punkte)

Frage	Antwort	Punkte
<p>Die Akquisition von flüchtigem Speicher (RAM) braucht Zeit und Platz und macht deshalb nicht für jede Untersuchung Sinn.</p> <p>Nennen Sie 2 Situationen, Verdächtige bzw. Vorfälle wo die Akquisition von RAM zwingend notwendig ist.</p>	-	2
<p>Erklären Sie den Begriff "Memory Smear" und was dies für die forensische Analyse von flüchtigem Speicher (RAM) bedeutet.</p>		1
<p>Nennen Sie zwei Beispiele, wie bzw. wo Sie beim Sammeln von flüchtigem Speicher den "Memory Smear" verhindern können.</p>		2

Frage	Antwort	Punkte
Nennen Sie den Unterschied zwischen den Volatility commands pslist und psscan.		2

1.5 Red Teaming (4 Punkte)

Frage	Antwort	Punkte
Erklären Sie den Begriff "Lateral Movement"		1
Geben Sie 3 Unterschieden zwischen "Penetration Test" und "Red Teamings" an.	1 2 3	3

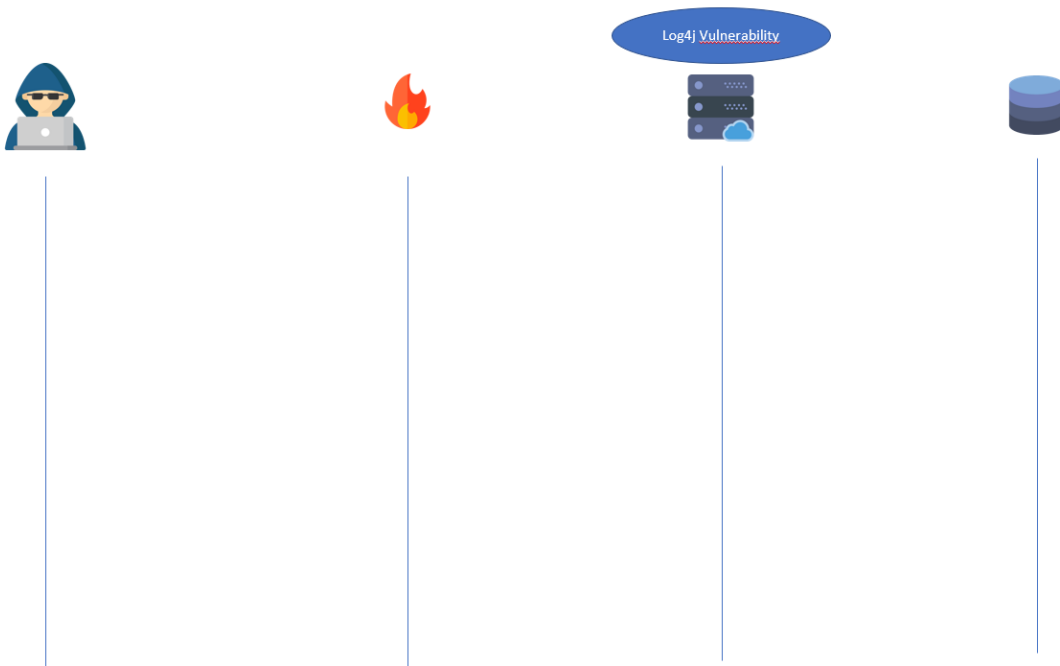
1.6 Mutual Auth (3 Punkte)

Frage	Antwort	Punkte
Erklären Sie wie Mutual Auth mit Zertifikaten funktioniert und begründen Sie, warum damit kein MitM möglich ist. Argumentieren Sie mittels Krypto Knowhow.	<p>Erklärung</p> <p>Begründung</p> <p>Krypto Know-How</p>	3

1.7 WebApp in DMZ (12 Punkte)

Eine selbst entwickelte und betriebene WebApp mit DB Anbindung in der DMZ einer Firma ist verwundbar gegenüber der Log4j Sicherheitslücke. Zeichnen Sie in untenstehendes Diagramm ein, wie ein Hacker diese Sicherheitslücke ausnützen könnte. Sie finden das Security Advisory der Log4j Sicherheitslücke ganz am Ende der Prüfung im Anhang unter Kapitel 2.1.

Zeichnung: 4 Punkte



Der CEO der Firma möchte den verwundbaren Log4j Service auf keinen Fall ausser Betrieb nehmen. Um einen Code Change in der Produktion einzuspielen, dauert es sicher 10 Tage. Welche Schritte machen Sie mit dieser Rahmenbedingung in welcher Reihenfolge, damit niemand die Sicherheitslücke ausnützen kann?

Reihenfolge	Antwort	Punkte
Sofortmassnahme (gleicher Tag)	<div>1</div> <div>2</div> <div>3</div>	3
Mittelfristige Massnahme (innerhalb 1 Woche)	<div>1</div> <div>2</div>	2
Längerfristige Massnahme (innerhalb nächstem Monat)	<div>1</div> <div>2</div> <div>3</div>	3

1.8 Informatiker Streit (2 Punkte)

Zwei SOC Mitarbeiter streiten sich in der Kaffee Pause über den Nutzen von Yara. Einer der Kollegen, der primär Windows Event Logs analysiert (EVT) argumentiert, dass er mit Yara überhaupt keinen Erfolg hatte und das Projekt «Yara» überbewertet wird.

Fragen	Antwort	Punkte
Beurteilen Sie die obige Aussage. Begründen Sie Ihre Antwort.		2

1.9 DNS over HTTP (DoH) (12 Punkte)

Ein neuartiger Trojaner soll im Rahmen eines Red-Teaming Engagement über HTTPS DoH Kontakt zu seinem C2 Server (Command & Control) aufnehmen.

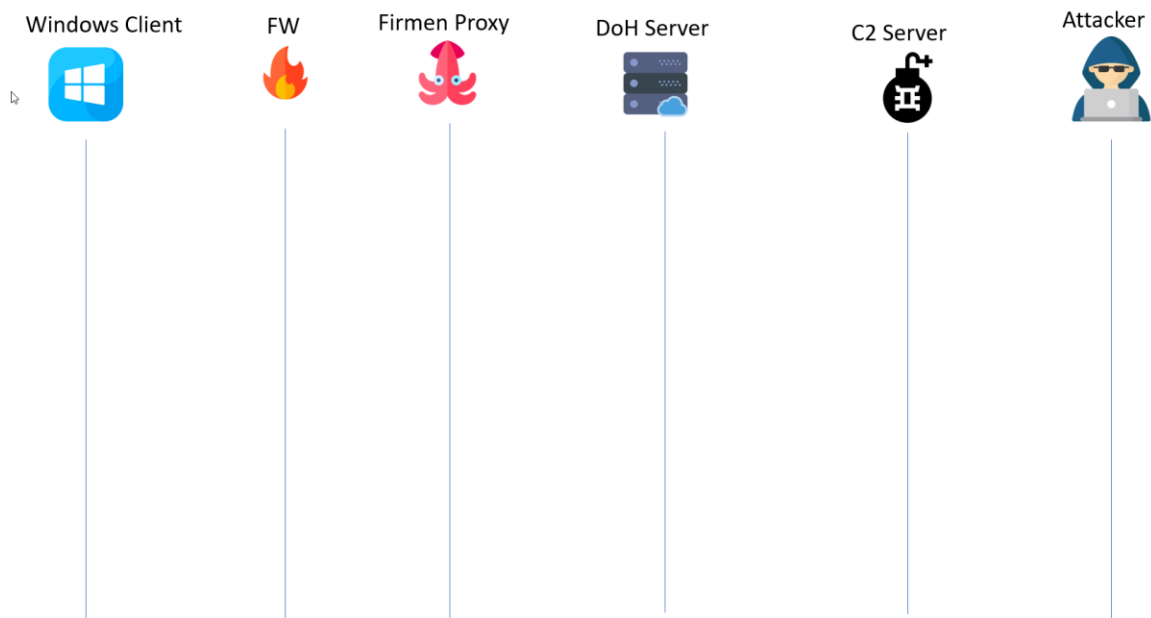
Kriterien für Bewertung (Zeichnung)

- Richtung der Pfeile
- Angabe des Protokolls und Port
- Beschriftung pro Pfeil (Bedeutung)

Polling des Trojaner zum C2 (polling for commands)

Zeichnen Sie nur das «Polling» des Windows Client zum C2 Server ein

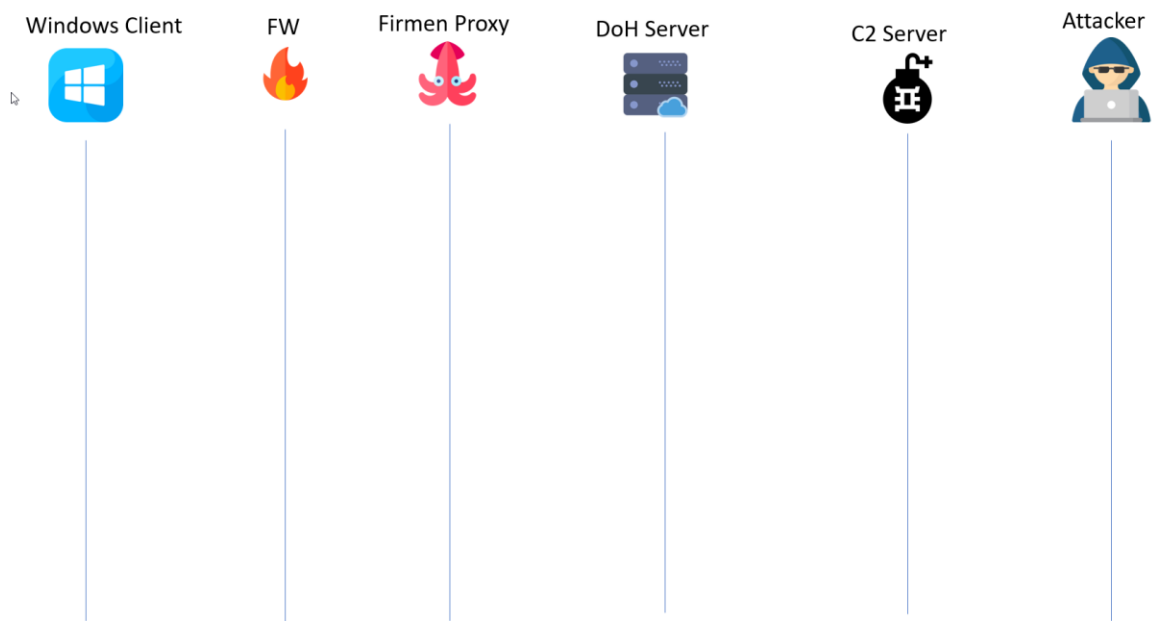
Zeichnung: 4 Punkte



Download EXE vom C2 zum Windows Client

Zeichnen Sie ein, wie das trojanische Pferd auf dem Windows Client vom C2 Server ein weiteres EXE downloaded.

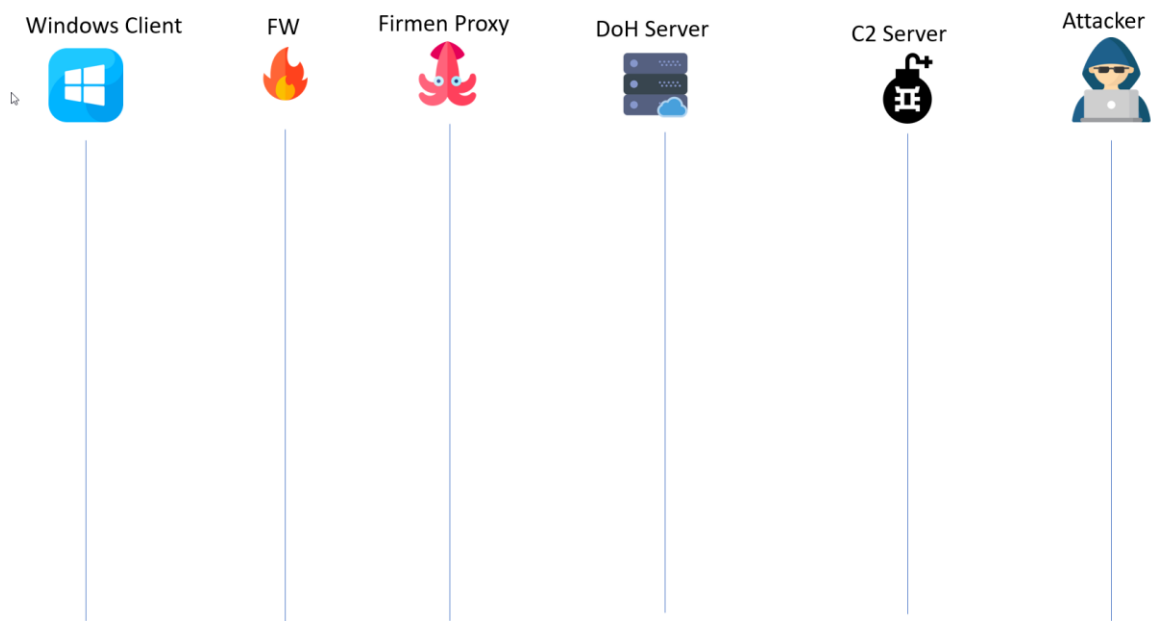
Zeichnung: 4 Punkte



Datei-Upload vom Windows Client zum C2 Server

Zeichnen Sie den Ablauf, wie das trojanische Pferd auf dem Windows Client eine Datei (z.B. C:\geheim\passworte.txt) vom Windows Client zum C2 Server uploaded.

Zeichnung: 4 Punkte



1.10 Ransomware (8 Punkte)

Eine Firma wird Opfer einer Ransomware Attacke. Niemand hat den Angriff bemerkt und alle Daten sind übers Wochenende verschlüsselt worden. Der erste Mitarbeiter am Montag in der früh konnte sich nicht mehr am PC anmelden. Alle Files sind verschlüsselt, auf allen Clients und Server (Active Directory). Das Backup ist jedoch Gott sei Dank noch in Ordnung und die Netzwerk-Geräte und Firewalls sind nicht betroffen. Sie werden als Cyber Security Spezialist angefragt, was man nun der Reihe nach tun soll.

Geben Sie in untenstehende Tabelle 4 Schritte an, was der Kunde der Reihenfolge (Priorität) nach tun muss und was man besonders achten muss, um wieder in den «Normalbetrieb zu kommen». Verzichten Sie auf organisatorische Massnahmen und fokussieren Sie sich auf technische Massnahmen.

Reihenfolge	Antwort	Punkte
1		2
2		2
3		2
4		2

1.11 RDP Brute Force Attacke (2 Punkte)

Während der Wazuh-Übung im Hacking-Lab war es etwas frustrierend zu sehen, dass man im Wazuh die RDP Brute Forcing Attacken nicht finden konnte.

Frage	Antwort	Punkte
<p>Beschreiben Sie die Lösung für das Problem, so dass sämtliche RDP Brute Forcing Attacken auf allen Systemen in Wazuh erkannt wird</p> <p>PS: Wir haben dies in der HL Übung gemacht.</p>		2

1.12 IP Blocklist (3 Punkte)

Der Spezialist von Wazuh und der Spezialist von MISP treffen sich in der Kaffee Pause. Sie tauschen sich aus. Dabei erzählen beide Spezialisten, dass Sie externe Quellen für ihr Tool einsetzen (IP Blacklist, IP-Reputation, Tor Exit Nodes, C2 Server Listen, Spam Listen, etc.)

Beide Spezialisten benutzten zum Teil die gleichen Feeds in MISP und Wazuh und zahlen natürlich auch doppelt (für die kostenpflichtigen Feeds)

Frage	Antwort	Punkte
Wofür zieht man in Wazuh oder MISP externe Quellen an?	<p>Grund 1</p> <p>Grund 2</p>	2
Beschreiben Sie eine Methode, mit welcher die Feeds nur noch 1x bezahlt werden müssen.		1

1.13 Forensik (6 Punkte)

Ein Forensiker erstellt ein Memory Abbild von einem «kompromittierten» Windows 10 Client, auf dem man vermutet, dass ein Trojaner aktuell läuft. Sie bekommen das Memory Abbild und sollen es analysieren.


Frage	Antwort	Punkte
Mit welchem Tool analysieren Sie das Memory Abbild?		1
Welche 5 Schritte unternehmen Sie, um das Abbild zu untersuchen?	1 2 3 4 5	5

1.14 GPO (6 Punkte)

Im Rahmen des Unterrichtes haben Sie das Active Directory und die GPO (Group Policy Object) kennen gelernt.

Frage	Antwort	Punkte
Welche Voraussetzungen müssen auf einem Win10 Client erfüllt sein, damit man diesen über die GPO steuern kann? `		1
<p>Beschreiben Sie 5 notwendige Teilschritte die nötig sind, um via GPO den Wazuh Agent auf allen Windows Clients zu installieren.</p> <p>Das AD hat alle Clients in der Gruppe «ALL CLIENTS» gespeichert.</p>	<p>1</p> <p>2</p> <p>3</p> <p>4</p> <p>5</p>	5

1.15 SIGMA Rules (5 Punkte)

Frage	Antwort	Punkte
<p>Erklären Sie den Nutzen von SIGMA Rules</p> 	<p>Nutzen 1</p> <p>Nutzen 2</p>	2

```

win_susp_lsass_dump.yml x  win_susp_failed_logons_single_source.yml  win_susp_failed_logon_reas
1  title: Password Dumper Activity on LSASS
2  description: Detects process handle on LSASS process with certain access mask and object type SAM_DOMAIN
3  status: experimental
4  reference: https://twitter.com/jackcr/status/807385668833968128
5  logsource:
6    product: windows
7  detection:
8    selection:
9      EventLog: Security
10     EventID: 4656
11     ProcessName: 'C:\Windows\System32\lsass.exe'
12     AccessMask: '0x705'
13     ObjectType: 'SAM_DOMAIN'
14    condition: selection
15  falsepositives:
16    - Unkown
17  level: high
18

```

Frage	Antwort	Punkte
<p>Was kann der SOC Spezialist, der bei sich selbst Wazuh einsetzt mit obiger SIGMA Rule machen (Nutzen) und wofür ist die Rule?</p>	<p>Nutzen (1 Punkt)</p> <p>Erklärung Rule (2 Punkte)</p>	3

Frage	Antwort	Punkte
<p>Um welche Art von Angriff handelt es sich und wie kann sich das Unternehmen davor schützen?</p> <p>Begründen Sie Ihre Antwort. Abschalten des Systems gilt nicht als Lösung.</p>	<p>Art des Angriff</p> <p>Begründung</p>	2

1.17 SSH Audit (6 Punkte)

Eine Firma hat viele SSH Services in der DMZ. Der Login ist nur mit SSH PubKey Auth erlaubt. Username/Passwort Auth ist überall deaktiviert. Die SSH Dienste werden auch von einer externen Firma für die IT-Support Unterstützung benutzt. Sie vertrauen aber dem externen Dienstleister nicht 100% und möchten die Aktivitäten des externen Dienstleisters überwachen. Sie wollen jeden Befehl sehen und protokollieren, welcher der externe Dienstleister via SSH auf ihren Systemen eingibt.

Frage	Antwort	Punkte
<p>Ein Mitarbeiter aus dem eigenen Unternehmen schlägt vor, hierfür den SSH MitM Docker zu verwenden, den Sie in der Übung kennen gelernt haben. Bewerten Sie diesen Lösungsansatz.</p> <p>Erklären Sie den Sachverhalt. Begründen Sie ihre Gedanken. Denken Sie auch an SSH Tunneling.</p>	<p>Erklärung Sachverhalt</p> <p>Begründung</p>	3
<p>Das Konzept mit dem SSH MitM ist in der Firma sehr umstritten. Man will das letztlich nicht.</p> <p>Erklären Sie ein Konzept, mit welchem Sie sämtliche SSH Befehle des externen Dienstleisters auf allen Systemen überwachen können (ohne SSH MitM Proxy)</p> <p>Ist sowas möglich? Begründen Sie Ihre Antwort.</p>	<p>Konzept</p> <p>Begründung</p>	3

1.18 NLA (6 Punkte)

Bei der RDP MitM Übung haben wir gesehen, dass RDP MitM mit aktiviertem NLA verhindert wird.

Frage	Antwort	Punkte
Erklären Sie auf Basis von kryptografischen Argumenten, warum NLA vor MitM schützt	Erklärung	3
Könnte die Methode von NLA nicht auch auf Form-based Authentisierungssysteme bei Web-Apps genutzt werden? Begründen Sie Ihre Antwort.		3

1.19 Large Scale (6 Punkte)

In einem Unternehmen mit 20'000 Windows Clients will man herausfinden, wer alles ein Tool gestartet hat, das einen bestimmten Registry Key schreibt (wie in der Übung SysInternals in die Registry)

Man könnte dies via GPO über ein PowerShell Script lösen. Das SOC Team nutzt jedoch eine SOAR Lösung für diesen Zweck.

Frage	Antwort	Punkte
Worin liegt der Unterschied zwischen einem SIEM und SOAR?	1 2 3	3
Welches SOAR System haben Sie während den HL Übungen kennen gelernt?		1
Wie muss man mit SOAR Methoden vorgehen, um die Antwort auf die Frage zu erhalten, auf welchen Clients das Tool gelaufen ist. Annahme, ein SOAR Tool ist installiert.		2

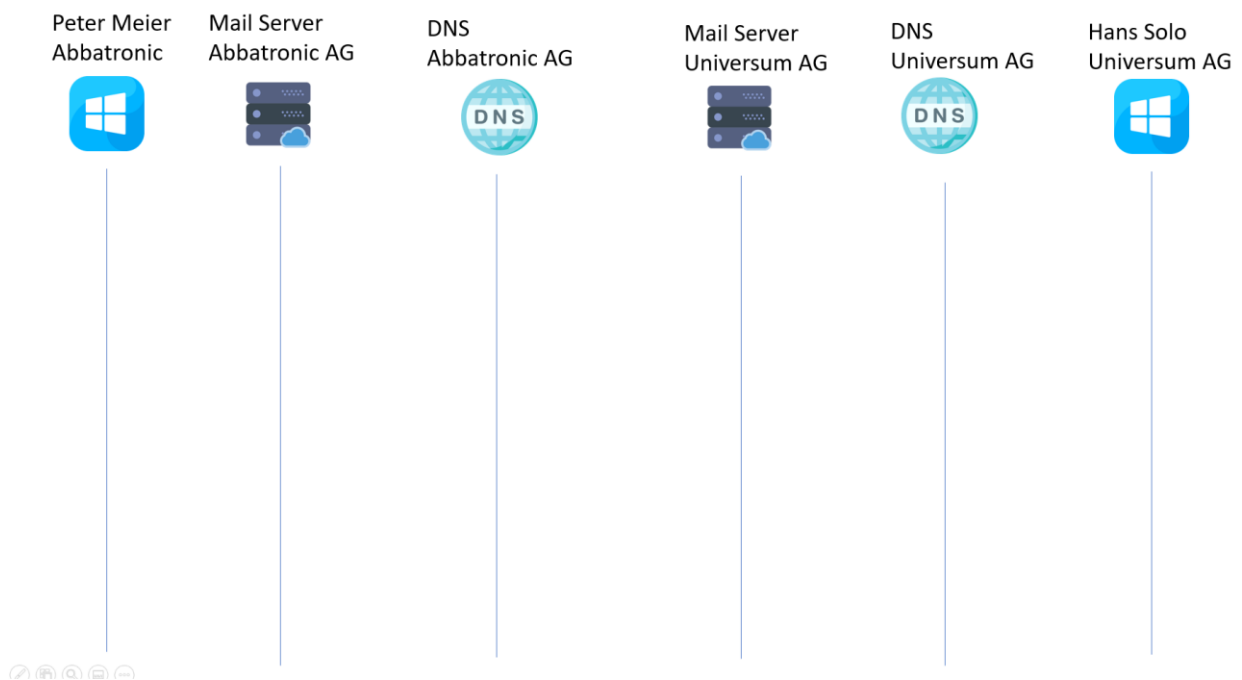
1.20 SPF/DKIM/DMARC (6 Punkte)

Peter Meier der Firma Abbatronic sendet von seinem PC via Mail Server von Abbatronic AG als peter.meier@abbatronic.ch ein Mail an Hans Solo von Universum AG hans.solo@universum.com.

Zeichnen Sie in untenstehendes Diagramm ein, wie SPF, DKIM und DMARC angewendet wird in der Annahme, dass Sender und Empfänger SPF/DKIM und DMARC unterstützen. Zeichnen Sie folgende Protokolle ein

- SMTP
- DNS

Machen Sie Pfeile mit einer Richtung und beschriften Sie die Pfeile mit Protokoll



2 Anhang

2.1 Log4j Advisory

← → ↻ cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44832 🔍 🖨️ ☆ 👤 ⋮

[Printer-Friendly View](#)

CVE-ID	
CVE-2021-44832	Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information
Description	
Apache Log4j2 versions 2.0-beta7 through 2.17.0 (excluding security fix releases 2.3.2 and 2.12.4) are vulnerable to a remote code execution (RCE) attack when a configuration uses a JDBC Appender with a JNDI LDAP data source URI when an attacker has control of the target LDAP server. This issue is fixed by limiting JNDI data source names to the java protocol in Log4j2 versions 2.17.1, 2.12.4, and 2.3.2.	
References	
<p>Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.</p> <ul style="list-style-type: none">• CISCO:20211210 Vulnerabilities in Apache Log4j Library Affecting Cisco Products: December 2021• URL:https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-apache-log4j-gRuKNEbd• CONFIRM:https://security.netapp.com/advisory/ntap-20220104-0001/• CONFIRM:https://cert-portal.siemens.com/productcert/pdf/ssa-784507.pdf• URL:https://cert-portal.siemens.com/productcert/pdf/ssa-784507.pdf• FEDORA:FEDORA-2021-1bd9151bab	