OST
Ostschweizer
Fachhochschule

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

Name Vorname

Cyber Defense HS2023

Hauptprüfung

15. Januar 2024

Document Name:	2023_HS2023_Cyber_Defense_Hauptprüfung_ohne_Musterlösung_V1.0.docx
Version:	V1.0
Author	Ivan Buetler
Classification:	EXAM

OST
Ostschweizer
Fachhochschule

Inhaltsverzeichnis

OST Ostschweizer Fachhochschule
Postfach 1475
CH-8640 Rapperswil
www.ost.ch

OST
Ostschweizer
Fachhochschule

Punkteverteilung

Aufgabe	Punkte
1.1 Security Jobs	6
1.2 End of Life	5
1.3 C2 Traffic	5
1.4 Inductive Automation Security Advisory	6
1.5 MISP	8
1.6 Memory Forensik	5
1.7 MitM am Flughafen	5
1.8 RAT	5
1.9 Cyber Kill Chain	7
1.10 Kerberos	8
1.11 Wie weiter?	10
1.12 Yara	7
1.13 MS Office Advisory und Whazu	14
1.14 Mimikatz	5
1.15 Forensic Readiness	3
1.16 Trusted Root CA	4
1.17 Spam Protectoin	4
1.18 GPO	5
Total	112

OST Ostschweizer Fachhochschule
Postfach 1475
CH-8640 Rapperswil
www.ost.ch

Sprache
Ihre Lösungen müssen in Blockschrift geschrieben werden (lesbar). Die Verwendung von Englischen Begriffen (aus den Folien, Vorlesung) ist absolut ok und erlaubt. Sie können Ihre Antworten in der Deutschen oder Englischen Sprache abgeben.

Abändern der Fragestellung
Bitte ändern Sie die Fragestellung nicht ab. Belassen Sie die Fragen wie sie sind und beantworten Sie, was gefragt ist. Wenn es für Sie Unklarheiten in der Fragestellung 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**.

Flugmodus
Die Verwendung von Ihrem Laptop oder Tablet ist während der Prüfung zu Nachschlage-Zwecken gestattet. Allerdings müssen Sie alle Ihre elektronischen Geräte in den Flugmodus setzten oder anders gesagt dafür sorgen, dass Sie während der Prüfung **keinen** Zugriff auf das Internet haben. **Die Nutzung des Internet während der schriftlichen Prüfung ist grundsätzlich untersagt**, egal mit welchem Device, Protokoll oder anderer kreativen Art und Weise, die hier nicht explizit ausgeschlossen ist.

Toilette während der Prüfung
Sie müssen nicht fragen, wenn Sie auf die Toilette gehen müssen. Stellen Sie einfach sicher, dass Sie warten, bis Ihr Vorgänger oder Vorgängerin zurück ist.

Vorzeitige Abgabe
Selbstverständlich dürfen Sie die Prüfung auch früher abgeben. Bitte verlassen Sie nach der Abgabe den Raum unmittelbar und packen Sie Ihr Material nach dem offiziellen Schluss der Prüfung zusammen. Es sollen keine Geräusche und Unruhe während der Prüfung für andere Personen entstehen, so dass diese sich bis zum Schluss voll konzentrieren können.

OST Ostschweizer Fachhochschule
Postfach 1475
CH-8640 Rapperswil
www.ost.ch

1 Cyber Defense HS2023

1.1 Security Jobs (6 Punkte)

In der Security Branche gibt es aktuell diverse Stellenangebote. Bitte beantworten Sie pro Security Job die folgenden Fragen

a) Was macht man bei diesem Job primär?

b) Was ist das primäre Ergebnis, das man bei diesem Job herstellt oder entwickelt?

c) Worin liegt der primäre Nutzen von diesem Ergebnis?

Frage	Antwort	Punkte
Penetration Tester	a) b) c)	1.5
Red Teamer	a) b) c)	1.5

OST Ostschweizer Fachhochschule
Postfach 1475
CH-8640 Rapperswil
www.ost.ch

Frage	Antwort	Punkte
Digitale Forensik bei der Polizei	a) b) c)	1.5
Incident Responder	a) b) c)	1.5

OST Ostschweizer Fachhochschule
Postfach 1475
CH-8640 Rapperswil
www.ost.ch

1.2 End of Life (5 Punkte)

Am 30. Juni 2024 ist der End of Life Termin von CentOS 7. Sie sind in der IT von einem Unternehmen und verwenden CentOS 7, aber ausschliesslich mit Docker Services. Sie haben keine native CentOS 7 Applikationen, alles läuft in Docker Container.

Frage	Antwort	Punkte
Sehen Sie einen Handlungsbedarf per 1. Juli 2024 ein anderes OS einzusetzen oder ist es vertretbar CentOS 7 auch länger zu nutzen? Antwort mit Begründung!		2
Nehmen wir an, Sie hätten 100 Virtuelle Maschinen auf Basis von CentOS 7. Welche dieser 100 VM's würden Sie zuerst auf ein neues OS migrieren oder anders gesagt, was sind die Kriterien für die Migration? Antwort mit Begründung	Mindestens 3 sicherheitsrelevante Kriterien werden erwartetet für 100% der Punkte	3

OST Ostschweizer Fachhochschule
Postfach 1475
CH-8640 Rapperswil
www.ost.ch

1.3 C2 Traffic (5 Punkte)

Im Unterricht wurde immer wieder das Thema APT und C2 angesprochen.

Frage	Antwort	Punkte
Was ist die Idee von einem C2 Server?		1
Worin sehen Sie den Vorteil aus Sicht von Cyber Defense, wenn der Payload des C2 Traffic mit einem symetrischen Key verschlüsselt ist?		2
Worin sehen Sie den Nutzen aus Sicht der Täter, wenn der Payload des C2 Traffic mit einem asymetrischen Schlüsselpaar verschlüsselt ist?		2

OST Ostschweizer Fachhochschule
Postfach 1475
CH-8640 Rapperswil
www.ost.ch

OST
Ostschweizer
Fachhochschule

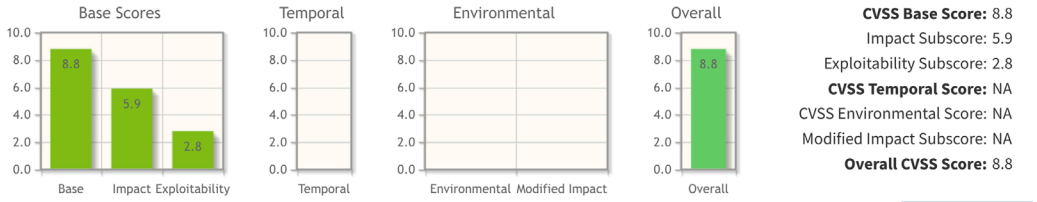
1.4 Inductive Automation Security Advisory (6 Punkte)

Bitte schauen Sie sich untenstehendes Advisory an. Es stammt von der Zero Day Initiative und wurde am 5.1.2024 aktualisiert.

Data Remote Code Execution Vulnerability

ZDI-24-018
ZDI-CAN-22127

CVE ID	CVE-2023-50223
CVSS SCORE	8.8, (AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)
AFFECTED VENDORS	Inductive Automation
AFFECTED PRODUCTS	Ignition
VULNERABILITY DETAILS	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Inductive Automation Ignition. Authentication is required to exploit this vulnerability. The specific flaw exists within the ExtendedDocumentCodec class. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data. An attacker can leverage this vulnerability to execute code in the context of SYSTEM.



CVSS Base Score: 8.8
Impact Subscore: 5.9
Exploitability Subscore: 2.8
CVSS Temporal Score: NA
CVSS Environmental Score: NA
Modified Impact Subscore: NA
Overall CVSS Score: 8.8

Show Equations

CVSS v3.1 Vector
AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Base Score Metrics

Exploitability Metrics

Attack Vector (AV)*
Network (AV:N) | Adjacent Network (AV:A) | Local (AV:L) | Physical (AV:P)

Attack Complexity (AC)*
Low (AC:L) | High (AC:H)

Privileges Required (PR)*
None (PR:N) | Low (PR:L) | High (PR:H)

User Interaction (UI)*
None (UI:N) | Required (UI:R)

Scope (S)*
Unchanged (S:U) | Changed (S:C)

Impact Metrics

Confidentiality Impact (C)*
None (C:N) | Low (C:L) | High (C:H)

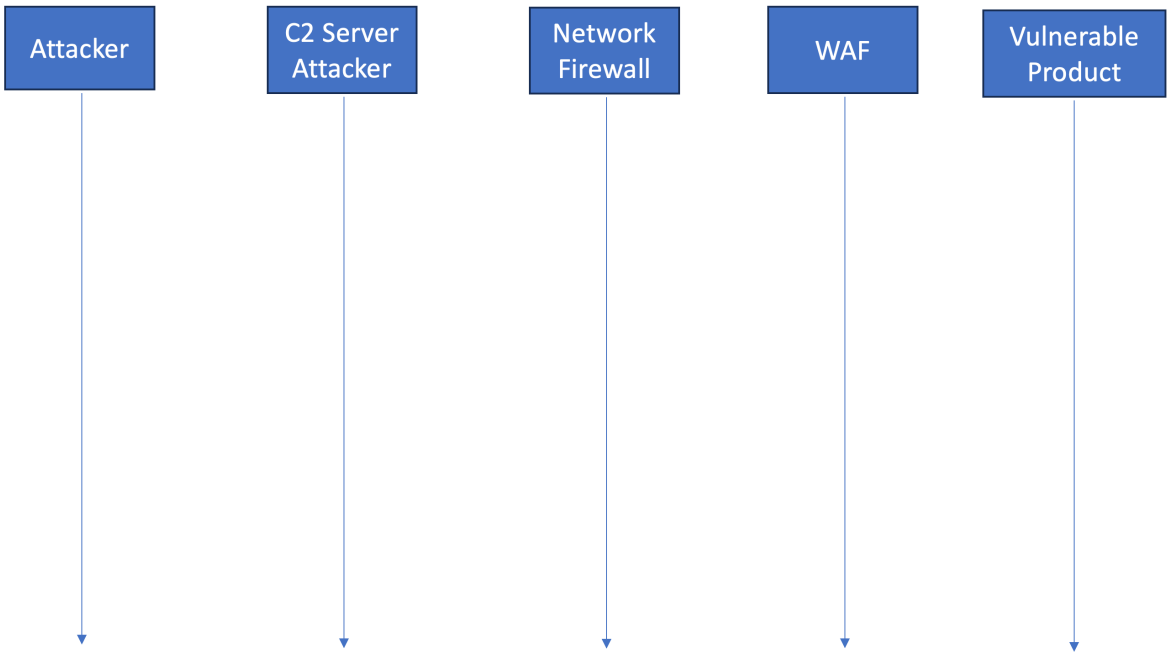
Integrity Impact (I)*
None (I:N) | Low (I:L) | High (I:H)

Availability Impact (A)*
None (A:N) | Low (A:L) | High (A:H)

* - All base metrics are required to generate a base score.

Frage	Punkte
Was bedeutet der CVSS SCORE von **8.8**? Antwort mit Begründung	2
Wo liegt der maximale Score?	1

Zeichnen Sie ein UML Sequenz-Diagramm das den erfolgreichen Angriff zeigt, inklusive RCE und einer Reverse Shell über TCP Port 443 zurück zum C2. Beginnen Sie mit dem ersten Verbindungsaufbau und beenden Sie Ihre Zeichnung mit dem Aufbau der Reverse Shell (4 Punkte)



OST Ostschweizer Fachhochschule
Postfach 1475
CH-8640 Rapperswil
www.ost.ch

Frage	Antwort	Punkte
Wie kann sich das Unternehmen schützen, bis der Hersteller einen Patch bereitgestellt hat? Es werden 2 Varianten erwartet. PS: Deaktivierung des Service gilt nicht als Lösung	Variante 1 Variante 2	2
Was bedeutet es, wenn im Advisory steht "*An attacker can leverage this vulnerability to execute code in the context of SYSTEM*»		1

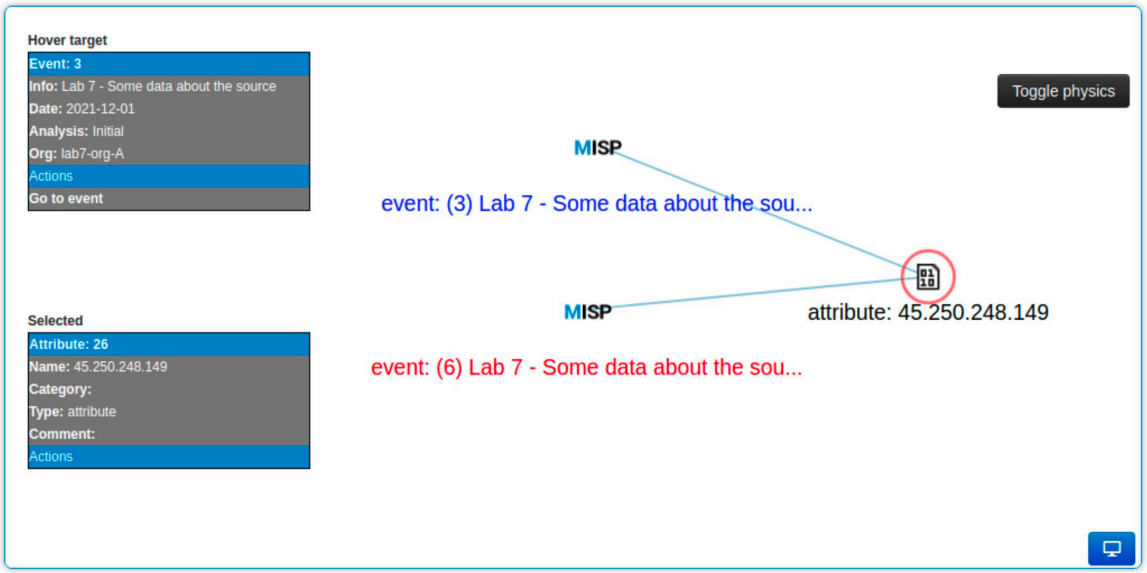
OST Ostschweizer Fachhochschule
Postfach 1475
CH-8640 Rapperswil
www.ost.ch

1.5 MISP (8 Punkte)

Frage	Antwort	Punkte
Worin liegt der Nutzen von MISP?		1
Welche Gefahr sehen Sie beim Einsatz von MISP für ein Unternehmen?	Gefahr 1 Gefahr 2	2
Beim Swisscom SOC Besuch wurde auf die Frage nach MISP der Begriff IOC als Antwort gebracht. Erklären Sie den Zusammenhang von MISP und IOC		2

OST Ostschweizer Fachhochschule
Postfach 1475
CH-8640 Rapperswil
www.ost.ch

Siehe folgendes Bild aus MISP und die Frage unterhalb des Bildes in der Tabelle.



Frage	Antwort	Punkte
Wie nennt man diese Art Grafik in MISP?		1
Interpretieren Sie die Grafik oben. Was lesen Sie daraus? Was interpretieren Sie?		1
Worin liegt der Nutzen in einer solchen visuellen Darstellung?		1

OST Ostschweizer Fachhochschule
Postfach 1475
CH-8640 Rapperswil
www.ost.ch

OST
Ostschweizer
Fachhochschule

1.6 Memory Forensik (5 Punkte)

Frage	Antwort	Punkte
Erklären Sie den Begriff Memory Forensik		1
Für welche Art von Vorfällen eignet sich die Analyse eines RAM-Abbildes besser, als wenn man das System zuerst stromlos macht und dann ein dd-Image zieht?		1
Was genau passiert, wenn man ein Executable von der Festplatte ausführt und daraus ein Prozess entsteht? Erklären Sie die Funktionsweise		1
Kann man anhand des Memory Abbild ein Executable wieder herstellen, respektive die Load Funktion umkehren?		1
Welche Tricks nutzen Viren, damit sie beim Start noch «harmlos» sind und dann zu Laufzeit «gefährlich werden»?		1

OST Ostschweizer Fachhochschule
Postfach 1475
CH-8640 Rapperswil
www.ost.ch

1.7 MitM am Flughafen (5 Punkte)

Ein Hacker betreibt am Flughafen Zürich einen Rogue Access Point. Er nennt die SSID «Free WiFi». Wer sich darauf verbindet, kann über den Access Point gratis das Internet nutzen. Damit hat der Hacker eine Man in the Middle (MitM) Situation geschaffen.

Danach verbindet sich der System Engineer Matthias Sorglos mit dem «Free WiFi».

Bitte beantworten Sie die Fragen in der Tabelle.

Frage	Antwort	Punkte
Matthias möchte kurz via SSH seinen Server checken. Wie kann sich Matthias vor dem MitM schützen?		1
Matthias möchte kurz über Outlook Web Access seine Mails checken. Wie kann sich Matthias vor dem MitM schützen?		1

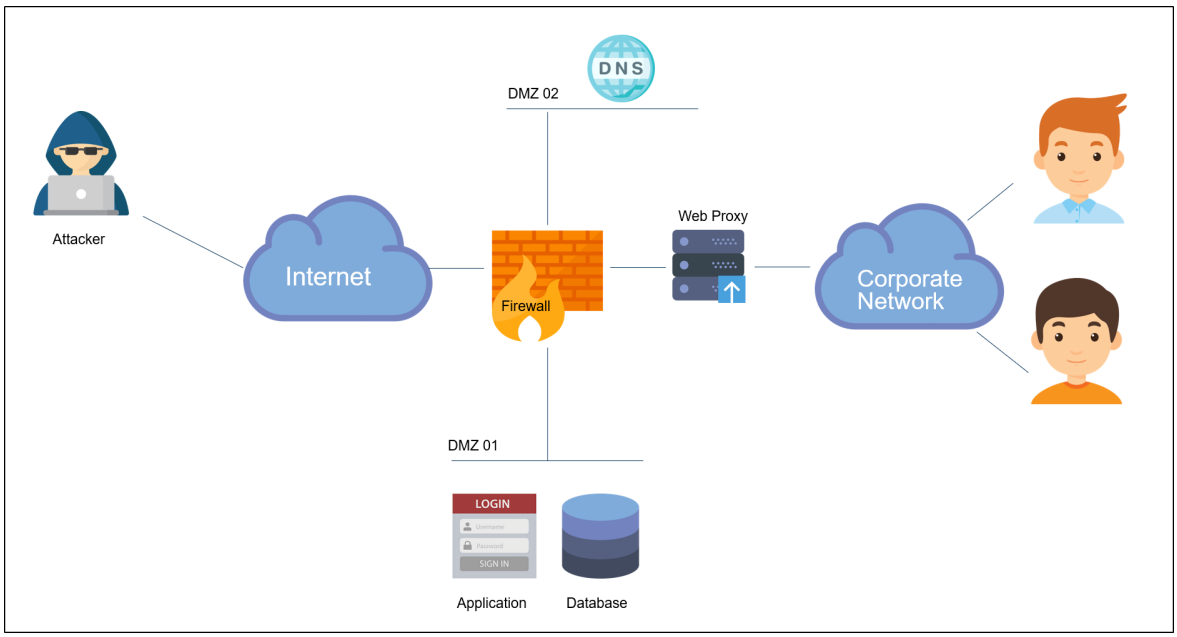
OST Ostschweizer Fachhochschule
Postfach 1475
CH-8640 Rapperswil
www.ost.ch

Frage	Antwort	Punkte
Matthias macht noch kurz eine E-Banking Zahlung Wie kann sich Matthias vor dem MitM schützen?		1
Matthias baut noch kurz zu seinem VPN Server zu Hause eine Session auf um die aktuelle Stromleistung seiner Smart Home Installation zu checken Wie kann sich Matthias vor dem MitM schützen?		1
Matthias greift über RDP auf einen Terminal Server zu den er administrieren muss. Wie kann sich Matthias vor der MitM schützen? s		1

OST Ostschweizer Fachhochschule
Postfach 1475
CH-8640 Rapperswil
www.ost.ch

1.8 RAT (5 Punkte)

Die untenstehende Topologie Zeichnung zeigt das Netzwerk Layout einer kleinen Firma. Die Firewall trennt das Internet vom Firmennetz. Die Firma betreibt zwei Demilitarisierte Zonen, die DMZ 01 mit einer Webanwendung und dazugehöriger Datenbank und eine zweite DMZ Zone mit dem Public DNS Server. Die End-User greifen über den Web Proxy (Port 80 und 443) auf das Internet zu. Der Web Proxy verwendet den Public DNS Server in der DMZ 02 für die Namensauflösung.



Frage	Antwort	Punkte
Geben Sie 3 Möglichkeiten an, wie der Hacker eine Reverse Shell aus dem Corporate Network zum Hacker im Internet aufbauen kann. Geben Sie das **Protokoll** an und eine kurze **Erklärung** wie der Hacker über dieses Protokoll eine Reverse Shell herstellen könnte.		3

OST Ostschweizer Fachhochschule
Postfach 1475
CH-8640 Rapperswil
www.ost.ch

Frage	Antwort	Punkte
Geben Sie 1 Möglichkeit an, wie der Hacker eine Reverse Shell von der DMZ 01 bekommen könnte.		1
Wie kann sich das Unternehmen generell vor Reverse Shells schützen?		1

OST Ostschweizer Fachhochschule
Postfach 1475
CH-8640 Rapperswil
www.ost.ch

1.9 Cyber Kill Chain (7 Punkte)

Sowohl Angreifer (Threat Actors, Red Team) als auch Verteidiger (Blue Team, SOC/CSIRT) verwenden u. A. die Cyber Kill Chain, um Cyber Attacken zu modellieren. Sie unterteilt einen Angriff in einzelne Phasen. Durch Detection & Response Massnahmen lassen sich Angriffe gezielt pro Phase erkennen und verhindern.

Bitte **benennen** sie in untenstehender Tabelle die sieben Phasen basierend auf den genannten Aktivitäten und listen sie mind. 1x **konkretes Beispiel** pro Aktivität (Phase) auf (welche Techniken werden seitens Angreifer in der entsprechenden Phase typischerweise eingesetzt?).s

Aktivität	Phase und Beispiel	Punkte
Kommunikationskanäle zu System des Angreifers suchen und öffnen, um die Malware resp. das System des Opfers aus der Ferne steuern zu können.	Phase: Beispiel:	1
Passenden Angriffswerkzeuge zusammenstellen.	Phase: Beispiel:	1

OST Ostschweizer Fachhochschule
Postfach 1475
CH-8640 Rapperswil
www.ost.ch

Aktivität	Phase und Beispiel	Punkte
Schwachstelle (Hardware, Software, Benutzer) ausnutzen, um Code/Befehle auf dem Zielsystem auszuführen.	Phase: Beispiel:	1
Mittels «Exploit» ausgeführter Code/Befehl lädt Payload nach und führt diesen auf dem System des Opfers aus. Bei Bedarf werden Persistenzen erstellt.	Phase: Beispiel:	1
Angriff starten, Malware verteilen.	Phase: Beispiel:	1

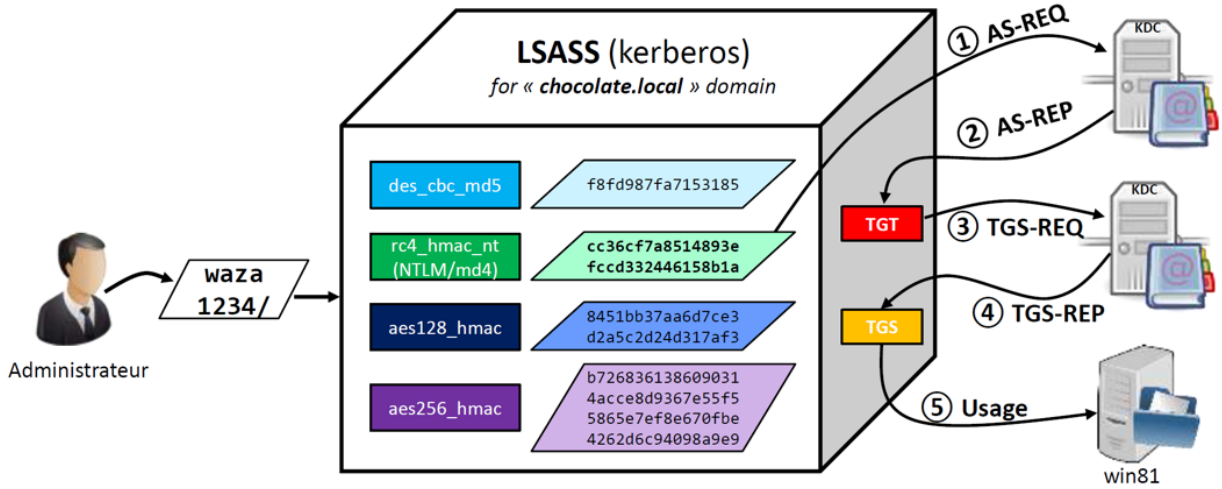
OST Ostschweizer Fachhochschule
Postfach 1475
CH-8640 Rapperswil
www.ost.ch

Aktivität	Phase und Beispiel	Punkte
Ziele identifizieren. Informationen über potenzielle Opfer sammeln.	Phase: Beispiel:	1
Zugang erlangen zu Systemen und Daten, um «Business Goals / Mission Objectives» zu erreichen.	Phase: Beispiel:	1

OST Ostschweizer Fachhochschule
Postfach 1475
CH-8640 Rapperswil
www.ost.ch

1.10 Kerberos (8 Punkte)

Kerberos ist das bevorzugte Authentisierungsprotokoll für Windows wenn Client und Server Teil einer Active Directoy Domain sind. Es basiert auf Tickets und bietet erhöhte Sicherheitsmerkmale im Vergleich zu NTLM. Trotzdem wird auch Kerberos von Angreifern auf verschiedene Arten für Lateral Movement ausgenutzt.



Hauptbestandteile der meisten Angriffstechniken sind NTLM Hashes, Ticket Granting Tickets (TGT) und Service Tickets (ST). Ordnen sie diese den verschiedenen Angriffstechniken zu, da wo sie **primär** zum Einsatz kommen. Mit «primär» sind nur die gemeint, die bspw. gestohlen oder manipuliert werden, also nicht alle, die im späteren Verlauf der Authentisierung auch noch zum Einsatz kommen (trotzdem mehrere Kreuze pro Angriff möglich).

Aussage	TGT	ST	NTLM Hash	Punkte
Over-Pass-the-Hash	[ ]	[ ]	[ ]	0.5
Kerberoasting	[ ]	[ ]	[ ]	0.5
Pass-the-Ticket	[ ]	[ ]	[ ]	0.5
Silver Ticket	[ ]	[ ]	[ ]	0.5
Golden Ticket	[ ]	[ ]	[ ]	0.5

OST Ostschweizer Fachhochschule
Postfach 1475
CH-8640 Rapperswil
www.ost.ch

Die wichtigsten Secrets im Kerberos-Protokoll sind der NTLM Hash eines x-beliebigen Benutzers (aka **«User Hash»**), des KRBTGT Accounts (aka **«KRBTGT Hash»**) und eines Maschinen/Service Accounts (aka **«Machine/Service Hash»**). Ordnen sie diese den verschiedenen Angriffstechniken zu, da wo sie benötigt werden (nur 1x Kreuz pro Angriff, also nur das Relevanteste).

Aussage	User Hash	KRBTGT Hash	Machine/Service Hash	Punkte
Over-Pass-the-Hash	[ ]	[ ]	[ ]	0.5
Silver Ticket	[ ]	[ ]	[ ]	0.5
Golden Ticket	[ ]	[ ]	[ ]	0.5

Bitte beantworten Sie die Fragen in der Tabelle.

Frage	Antwort	Punkte
Was ist der Unterschied zwischen Pass-the-Hash und Over-Pass-the-Hash?		0.5 0.5
Was geschieht bei einem Pass-the-Ticket Angriff genau?		0.5 0.5

OST Ostschweizer Fachhochschule
Postfach 1475
CH-8640 Rapperswil
www.ost.ch

Frage	Antwort	Punkte
Welche zwei Schwachstellen nutzen wir aus, wenn wir mit Kerberoasting erfolgreich sind?		0.5 0.5
Wie lange bleibt ein Golden Ticket gültig? (Bitte geben sie die Gültigkeitsdauer an und beschreiben sie was eine Organisation wie oft tun müsste, um das Ticket früher ungültig zu machen?)		0.5 0.5

OST Ostschweizer Fachhochschule
Postfach 1475
CH-8640 Rapperswil
www.ost.ch

1.11 Wie weiter? (10 Punkte)

Sie sind IT Forensiker und ermitteln in einem Cyber Vorfall. Die betroffene Firma wurde durch das Nationale Cyber Sicherheits Center (NCSC) über eine Viren-Infektion informiert. Daraufhin hat die Firma bereits eine Arbeitsstation ermitteln können, welche die rapportierten C2 Verbindungen verursacht hat. Vermutlich liegt die Infektion schon einige Zeit zurück. Die Arbeitsstation wurde isoliert.

Es besteht nun eine grosse Unsicherheit darüber, ob sich die Angreifer im Netz noch weiter ausgebreitet haben und noch immer aktiv sind. Besonders die Baupläne der "Combat Drones" auf dem Windows File Share "WRLDRGN-1" sind sowohl für Mitbewerber als auch global-politisch von hohem Wert. Der Benutzer der infizierten Arbeitsstation hatte zum Glück keine Berechtigungen für den Fileshare.

Sie haben bereits Zugriff auf das SIEM bekommen. Alle Clients und Server liefern die Logs dahin. Auch die Firewall und der Surf-Proxy liefern die Logs ins SIEM. Es gibt noch kein EDR Tool (bspw. Velociraptor) in der Umgebung. Die Authentisierung in dem Netzwerk ist in der Regel Kerberos-basiert.

Beantworten Sie die Fragen in der Tabelle.

Frage	Antwort	Punkte
Das Management will den Internetanschluss kappen. Nennen Sie je einen Vor- und Nachteil dieser Massnahme. Geben Sie eine Empfehlung ab	Vorteil Nachteil	3.0
Der "Initial Access" ist schon lange zurück und der Angreifer hat vermutlich Persistenz-Mechanismen eingerichtet. Sie untersuchen die isolierte Arbeitsstation. Nennen Sie **zwei** typische Möglichkeiten, um Persistenz zu erreichen und erklären Sie, nach was Sie suchen müssen.		2.0

OST Ostschweizer Fachhochschule
Postfach 1475
CH-8640 Rapperswil
www.ost.ch

Frage	Antwort	Punkte
Es erhärtet sich der Verdacht, dass von der infizierten Arbeitsstation doch auf eine Laufwerkfreigabe des Server "WRLDRGN-1" zugegriffen wurde. Welche Events im Active Directory Log sind dafür interessant? Nennen Sie **zwei** relevante Event IDs (4xxx) und was der jeweilige Event für Ihre Untersuchung bedeuten würde.		2.0
Das Nationale Cyber Sicherheits Center hat in Erfahrung gebracht, dass die Threat Actor auf den betroffenen Windows File Shares einen Service als Backdoor eingerichtet haben. Der Vorfall scheint nun aber so lange zurückzuliegen, dass nirgends mehr Logs dazu existieren. Beschreiben Sie, welche Möglichkeiten bestehen, trotzdem herauszufinden, ob und wann ein Backdoor Service allenfalls installiert wurde.		3.0

OST Ostschweizer Fachhochschule
Postfach 1475
CH-8640 Rapperswil
www.ost.ch

1.12 Yara (7 Punkte)

Frage	Antwort	Punkte
Was ist YARA und erklären Sie die Bedeutung in Cyber Security		1
Erklären Sie die Grundstruktur und wichtigsten Teile einer Yara Regel		2
Erklären Sie, wie man Conditions mit YARA abbildet. Erstellen Sie ein Beispiel wie man ein infiziertes File detektieren mittels Conditions erkennen könnte.		2

OST Ostschweizer Fachhochschule
Postfach 1475
CH-8640 Rapperswil
www.ost.ch

Frage	Antwort	Punkte
Erklären Sie, wie YARA einen polymorphic Virus erkennen könnte, was die Herausforderung darstellt und wie YARA diese adressiert.		2

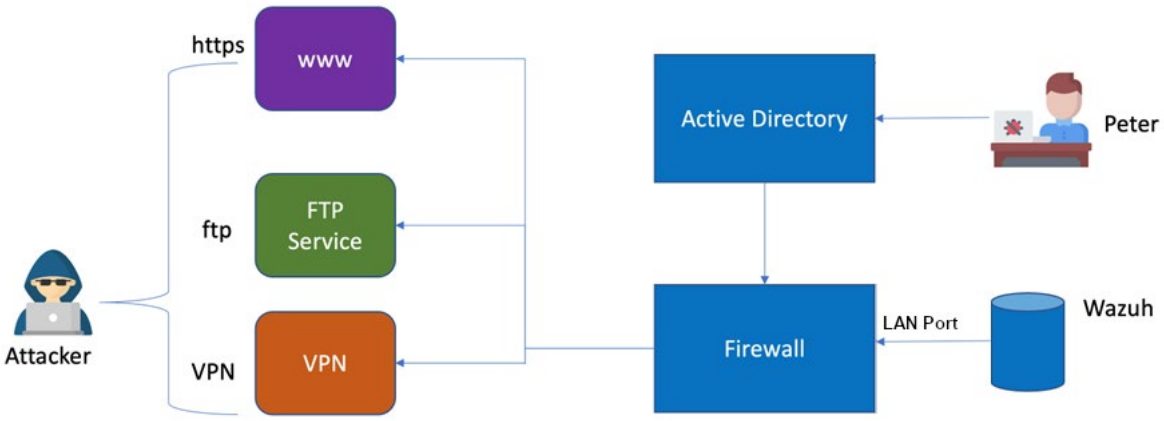
OST Ostschweizer Fachhochschule
Postfach 1475
CH-8640 Rapperswil
www.ost.ch

1.13 MS Office Advisory und Wazuh (14 Punkte)

Für diese Aufgabe basieren wir auf nachfolgender vereinfachten KMU Infrastruktur.

Aus dem Internet sind folgende 3 Dienste erkennbar:

- https Public Website
- ftp FTP für Kunden (In & Out)
- VPN Remote Access Gateway für Travelling User



Darüber hinaus hat es an einem LAN Port der Firewall eine Wazuh (SIEM) Instanz. Alle Komponente dieser IT Infrastruktur senden Ihre Logs an diese Wazuh Instanz.

Untenstehendes Advisory wird publiziert. Peter's Computer ist davon betroffen.

Microsoft Office: CVE-2024-20677: Microsoft Office Remote Code Execution Vulnerability

Severity	CVSS	Published	Created	Added	Modified
4	(AV:L/AC:M/Au:N/C:P/I:P/A:P)	01/09/2024	01/10/2024	01/09/2024	01/09/2024

Description

A security vulnerability exists in FBX that could lead to remote code execution. To mitigate this vulnerability, the ability to insert FBX files has been disabled in Word, Excel, PowerPoint and Outlook for Windows and Mac. Versions of Office that had this feature enabled will no longer have access to it. This includes Office 2019, Office 2021, Office LTSC for Mac 2021, and Microsoft 365. 3D models in Office documents that were previously inserted from a FBX file will continue to work as expected unless the Link to File option was chosen at insert time. This change is effective as of the January 9, 2024 security update.

OST Ostschweizer Fachhochschule
Postfach 1475
CH-8640 Rapperswil
www.ost.ch

Frage	Antwort	Punkte
Step 1 Wie könnte ein Angreifer das obige CVE für den Initial Access verwenden auf einen Windows Computer im Intranet?	Variante 1 Variante 2	2
Step 2 Zufälligerweise wird Ihr Initial Access (Schritt vorher) auf einem Computer ausgeführt, wo der User LOCAL ADMIN Rechte hat Was tun Sie nun als nächstes wenn es Ihr Ziel ist, im AD Enterprise Admin Rechte zu erlangen?		2
Step 3 Was tun Sie weiter, wenn der vorherige Schritt den Sie aufgeführt haben, erfolglos bleibt? PS: Muss was anderes sein als im vorherigen Schritt erklärt.		2

OST Ostschweizer Fachhochschule
Postfach 1475
CH-8640 Rapperswil
www.ost.ch

Frage	Punkte
Bitte Zeichnen Sie Ihre **Step 1 und Step 2** in die vereinfachte KMU Infrastruktur Grafik ein.	2

Fragestellungen zum Monitoring mit Wazuh:

Frage	Antwort	Punkte
Was müssen Sie tun, um Ihren Angriff von **Step 1** innerhalb des Wazuh SIEM zu erkennen?	Step 1	2
Was müssen Sie tun, um Ihren Angriff von **Step 2** innerhalb des Wazuh SIEM zu erkennen?	Step 2	2
Wie könnte man mit einem SIEM das Verschlüsseln von Files auf dem Fileserver erkennen? Antwort mit Begründung und im Kontext von einem AD und einem Fileserver, der dem AD joined ist.		2

OST Ostschweizer Fachhochschule
Postfach 1475
CH-8640 Rapperswil
www.ost.ch

1.14 Mimikatz (5 Punkte)

Frage	Antwort	Punkte
Wie kann man die Ausführung von Mimikatz mit einem SIEM erkennen?	Erklären Sie das Setup und Voraussetzungen am Beispiel von Wazuh	1
Woführ kann man folgendes Mimikatz Module verwenden? `sekurlsa::backupkeys` Was nützt das dem Angreifer und wie kann der Angreifer die Informationen für sich nutzen? Antwort mit Erklärung erwartet		2
Wofür kann man folgendes Modul einsetzen? `sekurlsa::dpapi` Was nützt das dem Angreifer und wie kann der Angreifer die Informationen für sich nutzen? Antwort mit Erklärung erwartet		2

OST Ostschweizer Fachhochschule
Postfach 1475
CH-8640 Rapperswil
www.ost.ch

1.15 Forensic Readiness (3 Punkte)

Frage	Antwort	Punkte
Erklären Sie das Konzept der unique-id im Kontext von Forensic Readiness in Web Anwendungen		1
Wer ist für die Erstellung oder Erzeugung der unique-id zuständig?		1
Ist es wichtig, dass diese unique-id wirklich random ist? Oder reicht es, wenn es einfach ne Zahl ist die raufzählt?		1

OST Ostschweizer Fachhochschule
Postfach 1475
CH-8640 Rapperswil
www.ost.ch

1.16 Trusted Root CA (4 Punkte)

Frage	Antwort	Punkte
Warum wollen manche Trojaner ein eigenes CA Cert in die Liste der Trusted Root CA beim Client installieren?		2
Wie könnte man mit einem SIEM solche Einträge oder Löschungen überwachen?		2

OST Ostschweizer Fachhochschule
Postfach 1475
CH-8640 Rapperswil
www.ost.ch

OST
Ostschweizer
Fachhochschule

1.17 Spam Protection (9 Punkte)

Frage	Antwort	Punkte
Sie sind der E-Mail Verantwortliche für die Domain «cybertycoon.ch» Ein E-Mail Spammer versucht über einen eigenen, persönlichen Mail Relay Server im Internet ein Mail im Namen von finance@cybertycoon.ch an ivan.buetler@compass-security.com zu senden. Was müssen Sie als Mail Verantwortlicher von cybertycoon.ch tun, damit sie von diesem Spamversuch automatisch **erfahren**?		2
Garantiert der von Ihnen beschriebene Lösungsansatz, dass Sie davon **erfahren**? Antwort mit **Begründung**		2
Das Mail enthält ein Word File mit einem Self-Signed Makro. Was können Sie tun, damit Ihre Mitarbeiter vor diesem Makro (Virus) geschützt sind?		1

OST Ostschweizer Fachhochschule
Postfach 1475
CH-8640 Rapperswil
www.ost.ch

Frage	Antwort	Punkte
Nehmen wir an ihr Schutz im vorherigen Schritt ist unwirksam und funktioniert nicht, welche zusätzliche Schutzmassnahmen gibt es?		1
Nehmen wir an, auch der obige zweite Schutz ist unwirksam, gemeinsam mit dem ersten. Welche Möglichkeit sehen Sie, dass Sie die Ausführung von diesem Makro im Unternehmen erkennen?		2
Nehmen wir an 38% von Ihren Mitarbeitern hätte auf das Makro geklickt und das Programm ausgeführt. Wie würden Sie herausfinden, wer in Ihrem Unternehmen das Word Makro ausgeführt hat?		1

OST Ostschweizer Fachhochschule
Postfach 1475
CH-8640 Rapperswil
www.ost.ch

1.18 GPO (5 Punkte)

Frage	Antwort	Punkte
Annahme; ein Windows basierter Client Computer des AD wurde erfolgreich gehackt. Sie wissen aber noch nicht, wie genau. Bitte definieren Sie die 5 wichtigsten Security Empfehlungen der GPO von Client Workstations, um im Falle von einem Incident eine sehr gute Log Ausgangslage für die Ermittlung zu haben.	Prio 1 Prio 2 Prio 3 Prio 4 Prio 5	5

OST Ostschweizer Fachhochschule
Postfach 1475
CH-8640 Rapperswil
www.ost.ch