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_mit_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) Suche nach Schwachstellen in IT Systeme, meist ohne Exploitation b) Erklären der Schwachstelle und Empfehlungen für die Behebung aussprechen c) Schwachstellen werden gefunden und Unternehmen kann Risiko minimieren	1.5
Red Teamer	a) Simulation «Echter Angriff» mit Exploitation b) Testen ob es das Monitoring der Firma merkt c) Empfehlungen für die Verbesserung der Incident Prozesse	1.5

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

Frage	Antwort	Punkte
Digitale Forensik bei der Polizei	a) Erstellen von digitalen Beweisen (dd-image, memory dumps von laufenden Systemen) b) Analyse von forensischen Artefacts um zu beweisen, was auf dem Artefact passiert ist (wer, was wann, wie, wo) c) Erstellen Bericht zuhanden Gericht oder Kunde das aufzeigt, was die Ergebnisse der forensischen Untersuchung sind	1.5
Incident Responder	a) Durchführung von Sofort-Massnahmen, beispielsweise bei Ransomware Case b) Consulting Kunde für Datensicherung und Datenerhebung c) Empfehlungen Kunde wie die Log Qualität verbessert werden kann, Attacken besser erkannt werden	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!	Ja, man muss trotzdem reagieren, da der Docker Daemon selbst ja nicht aktualisiert wird. Zudem werden die meisten Unix Maschinen über SSH gewartet, welches ja dann auch keine Updates mehr erhält. Also JA	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 Prio 1: Internet Facing Systeme Prio 2: Systeme mit vertraulichen Daten oder sensitiven Funktionen Prio 3: Systeme die von jedem Computer im Intranet erreichbar sind	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?	Ein Server im Internet der darauf warten von Clients kontaktiert zu werden. Damit eröffnet der Client die TCP/IP Verbindung aus dem Intranet auf den C2 Server im Internet, was viel einfacher ist als umgekehrt. Der C2 Admin kann Befehle bereitstellen, welche beim nächsten Poll des infizierten Clients geholt, ausgeführt und das Ergebnis dem C2 gesendet werden.	1
Worin sehen Sie den Vorteil aus Sicht von Cyber Defense, wenn der Payload des C2 Traffic mit einem symetrischen Key verschlüsselt ist?	Der Netzwerkverkehr des C2 Traffic lässt sich damit relativ einfach entschlüsseln.	2
Worin sehen Sie den Nutzen aus Sicht der Täter, wenn der Payload des C2 Traffic mit einem asymetrischen Schlüsselpaar verschlüsselt ist?	Der Täter hat einen besseren Schutz, dass der C2 Traffic nicht durch Ermittler entschlüsselt werden können.	2

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

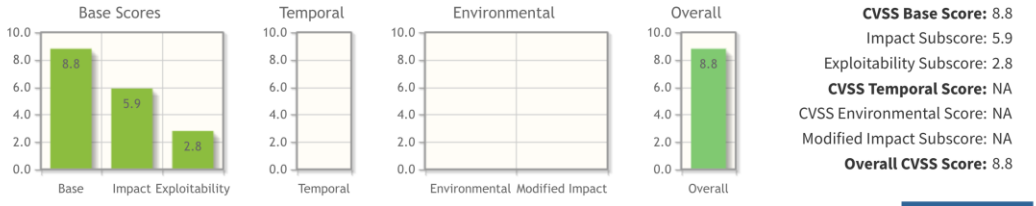
1.4 Inductive Automation Security Advisory (6 Punkte)

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)

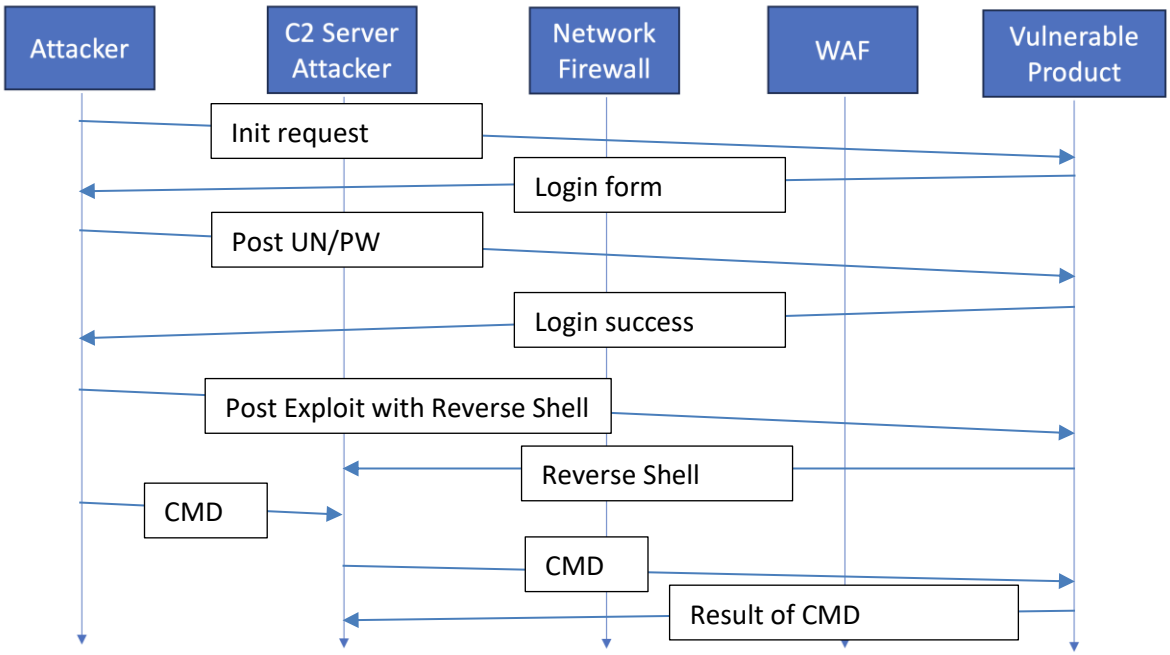
Integrity Impact (I)*
None (I:N) | Low (I:L) | High (I:H)

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 Kritische Sicherheitslücke (HIGH) aber nicht ganz 10, weil der Angreifer gültige Credentials haben muss. Ohne gültige Credentials lässt sich der Angriff nicht realisieren.	2
Wo liegt der maximale Score? Der maximale Score liegt bei 10 Punkten	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

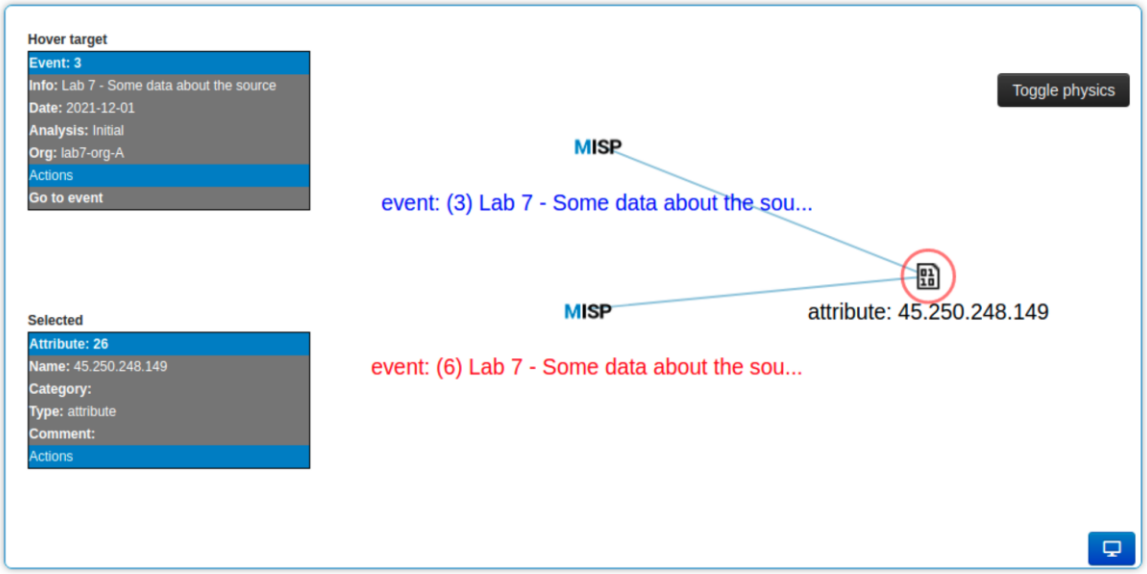
Frage	Antwort	Punkte
Wie kann sich das Unternehmen schützen, bis der Hersteller einen Patch bereitgestellt hat? Es werden 2 Varianten erwartet. PS: Deaktivierung des Service gilt nicht als Lösung	Variante 1 Mit der WAF den Exploit Request erkennen und blockieren, so dass dieser nicht zum verwundbaren System gelangt Variante 2 Firewall Rules so gesetzt, so dass das verwundbare System keine Verbindungen nach Aussen zulässt.	2
Was bedeutet es, wenn im Advisory steht "*An attacker can leverage this vulnerability to execute code in the context of SYSTEM*»	Das bezieht sich auf Microsoft Systeme. Dort gibt es noch einen mächtigeren User als Local Admin, den man System nennt. Das ist der entsprechende Hinweis bei diesem Advisory, dass es sich offensichtlich um ein Windows System handelt wo man maximale Rechte bekommt, wenn der Angriff erfolgreich ist.	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?	Austausch von IOC mit Dritten. Input von Dritten erhalten nach was man im eigenen SIEM System suchen könnte	1
Welche Gefahr sehen Sie beim Einsatz von MISP für ein Unternehmen?	Gefahr 1 Aus Versehen vertrauliche Daten mit Dritten sharen Gefahr 2 Aus Versehen eine Viren Infektion im eigenen Hause auslösen durch Samples von MISP	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	IOC sind Indicator of Compromize und diese warden über MISP ausgetauscht. Das bedeutet, dass Swisscom nicht primär Daten bereitstellt, aber von den MISP Feeds Anhaltspunkte sucht, nach denen Sie in lookup Tables ebenfalls suchen könnte. Damit man möglichen Gefahren und Attacken auf die Spur kommt, von denen man bisher noch nichts wusste. MISP wird als eine Art Threat Intelligence verwendet.	2

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?	Correlation Graph	1
Interpretieren Sie die Grafik oben. Was lesen Sie daraus? Was interpretieren Sie?	Das zwei Events die gleiche IP Adresse teilen. Das man diese IP Adresse genauer untersuchen sollte.	1
Worin liegt der Nutzen in einer solchen visuellen Darstellung?	Der Mensch kann anhand von Bildern besser die Zusammenhänge erkennen als in einer Tabellen-Form. Für den Mensch einfacher die Sachlage zu verstehen.	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	Damit wird die forensische Analyse von Memory Artefakten gemeint. Das sind Daten die von einem Live System stammen und etwas besonders angeschaut werden, weil man darin Prozess, User, Berechtigungen etc. einsehen kann. Man kann auch Binaries in Memory Dumps extrahieren und untersuchen, ob es ein bekannter Virus ist.	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?	Ransomware für das Auslesen des Encryption Key. Im stromlosen Zustand sind diese Daten oft nicht verfügbar.	1
Was genau passiert, wenn man ein Executable von der Festplatte ausführt und daraus ein Prozess entsteht? Erklären Sie die Funktionsweise	Der Loader stellt einen Memory Bereich für das Binary bereit und stellt die Import Adress Tables und Export Adress Tables zum Kernel und den bereitgestellten API bereit. Der Prozess selbst hat das Gefühl, er sei alleine auf dem System und das bedeutet, dass das Binary im Memory verteilt wird, so dass eine Rückführung des Prozess Memory zum Binary mitunter schwierig ist. Aber Tools wie Volatility stellen trotzdem solche Funktionalitäten bereit.	1
Kann man anhand des Memory Abbild ein Executable wieder herstellen, respektive die Load Funktion umkehren?	Ja, wie oben beschrieben nicht ganz einfach, aber man man kann anhand der Memory Adressen ein Binary wieder rekonstruieren. Aka Volatility	1

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

Frage	Antwort	Punkte
Welche Tricks nutzen Viren, damit sie beim Start noch «harmlos» sind und dann zu Laufzeit «gefährlich werden»?	Sie laden die gefährliche Funktion mittels Dynamic Loading aus dem Internet oder einer eigenen verschlüsselten Partition des Binary nach, so dass der Viren Scanner beim Durchforsten des initialen Binary keine Anzeichen von Viren findet.	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?	Sicher mit PubKey Auth arbeiten SSH Server Key überprüfen beim Verbindungsaufbau Falls der SSH Fingerprint ändert beim SSH Verbindungsaufbau, dann kein SSH machen Alternativ VPN aufbauen und darüber SSH machen	1
Matthias möchte kurz über Outlook Web Access seine Mails checken. Wie kann sich Matthias vor dem MitM schützen?	Prüfen des TLS Zertifikates und der Domain. HSTS und HSTS Pre-Loading funktionieren dann gut, wenn die Original Domain verwendet wird. Bei einem Phishing Versuch über einen Reverse Proxy und einer anderen Domain hilft nur die Prüfung der FQDN des Menschen, ausser mit FIDO2, wo ein MitM nicht möglich ist. Alternativ VPN aufbauen und darüber OWA machen	1

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

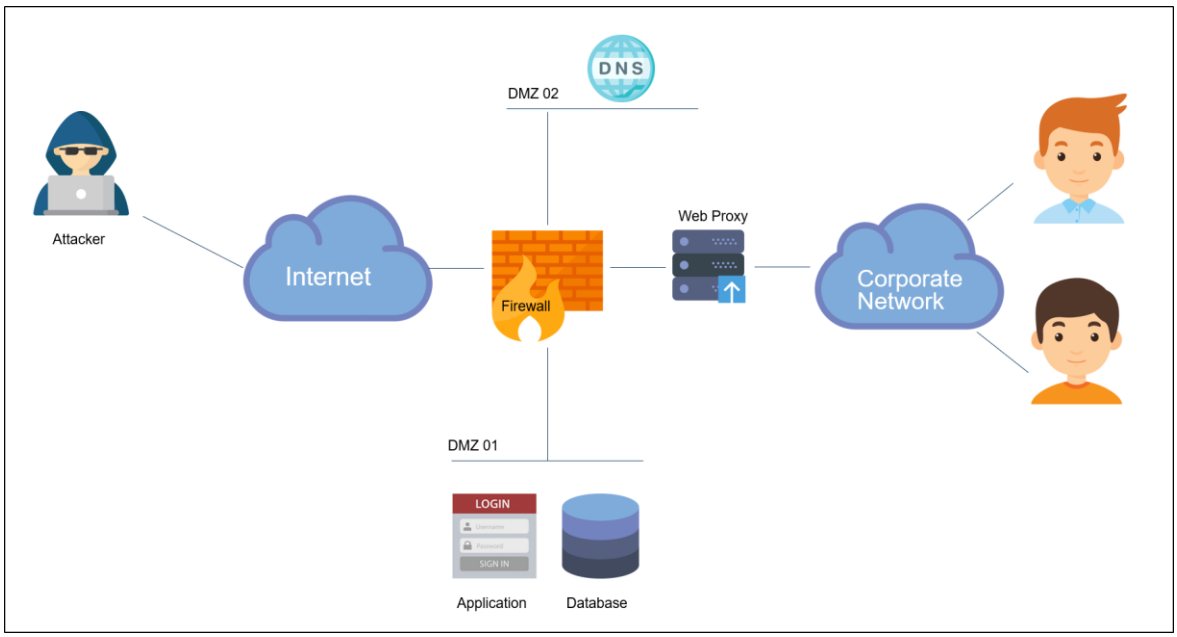
Frage	Antwort	Punkte
Matthias macht noch kurz eine E-Banking Zahlung Wie kann sich Matthias vor dem MitM schützen?	Analog E-Mail. Prüfen des TLS Zertifikates und der Domain. HSTS und HSTS Pre-Loading funktionieren dann gut, wenn die Original Domain verwendet wird. Bei einem Phishing Versuch über einen Reverse Proxy und einer anderen Domain hilft nur die Prüfung der FQDN des Menschen, ausser mit FIDO2, wo ein MitM nicht möglich ist. Alternativ VPN aufbauen und darüber E-Banking machen	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?	Einsatz von Asymetrischer Schlüssel mit Mutual Authentication. Prüfen des VPN Fingerprint	1
Matthias greift über RDP auf einen Terminal Server zu den er administrieren muss. Wie kann sich Matthias vor der MitM schützen? s	Ein zusätzliches VPN aufsetzen und darüber RDP machen, aber zumindest NLA aktivieren und TLS Zert überprüfen	1

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

OST
Ostschweizer
Fachhochschule

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.	Via Web Proxy (aka Covenant) Via DNS over HTTP (DoH) Via DNS Tunneling Port 53 direkt, falls der FW von Innen nach Aussen (via DMZ DNS) DNS Auflösung erlaubt.	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.	RCE auf Webserver. Exploit macht a) Bind Shell b) Reverse Shell c) Web Shell Am Wahrscheinlichsten ist die Reverse Shell von der DMZ über http oder HTTPS, da diese Protokolle oft von der DMZ ins Internet funktionieren (OS Update)	1
Wie kann sich das Unternehmen generell vor Reverse Shells schützen?	Präventiv • Updates aller OS, Apps, Services, Libraries • Least Privileges, Hardening • WAF Incident • Ausgehende Verbindungen sperren oder zumindest monitoren und blocken	1

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

1.8.1 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: Command & Control C&C C2 Beispiel: • http, https, dns, icmp	1
Passenden Angriffswerkzeuge zusammenstellen.	Phase: Weaponize Beispiel: • Malware / Payloads entwickeln oder beschaffen • Exploits entwickeln/beschaffen	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: Exploitation Beispiel: • Benutzer öffnet Link, lädt Malware herunter und führt diese aus • Browser Schwachstelle wird ausgenutzt mittels Exploit (Drive-by) um Malware auszuführen	1
Mittels «Exploit» ausgeführter Code/Befehl lädt Payload nach und führt diesen auf dem System des Opfers aus. Bei Bedarf werden Persistenzen erstellt.	Phase: Installation Beispiel: • Detonation: LOLBins wie Certutil, Bitsamin, HTS • Persistence Registry, Scheduled Task, Windows Service, DCOM, WMI	1
Angriff starten, Malware verteilen.	Phase: Delivery Beispiel: • E-Mail mit Attachment oder Link zur Malware versenden • Malware via kompromittierte Webseite verteilen • Malware via Advertising Netzwerk verteilen	1

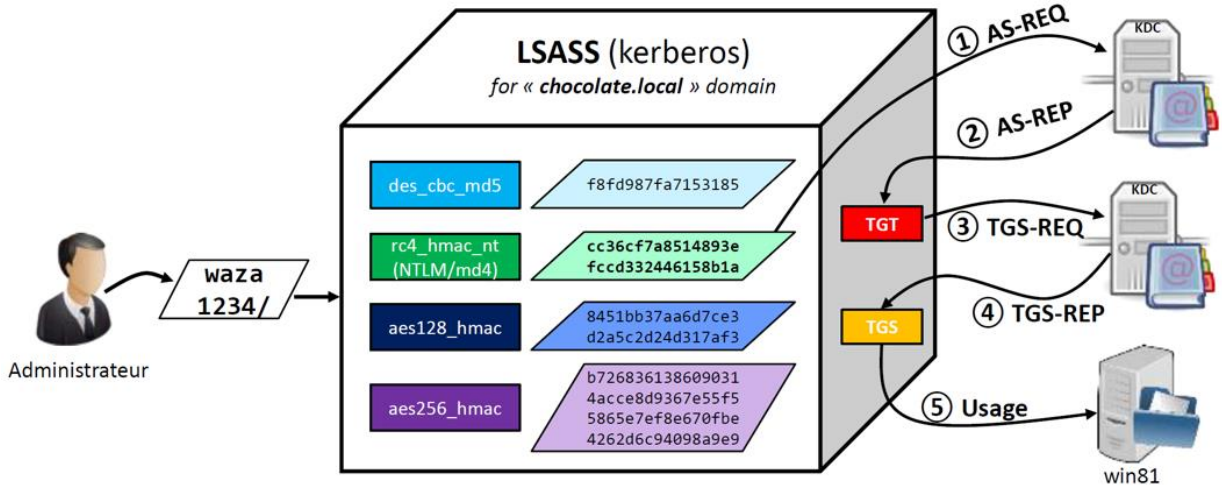
OST Ostschweizer Fachhochschule
Postfach 1475
CH-8640 Rapperswil
www.ost.ch

Aktivität	Phase und Beispiel	Punkte
Ziele identifizieren. Informationen über potenzielle Opfer sammeln.	Phase: Reconnaissance Beispiel: • E-Mail Adressen für Phishing sammeln • Daten aus Social Media sammeln • Informationen über Systeme und Anwendungen sammeln (Shodan)	1
Zugang erlangen zu Systemen und Daten, um «Business Goals / Mission Objectives» zu erreichen.	Phase: Action on Objectives Beispiel: • Informationen stehlen (Spionage) • Manipulation von Systemen (Sabotage) • Daten und Systeme verschlüsseln (Ransomware)	1

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

1.9 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	[ ]	[ ]	[X]	0.5
Kerberoasting	[ ]	[X]	[ ]	0.5
Pass-the-Ticket	[X]	[X]	[ ]	0.5
Silver Ticket	[ ]	[X]	[X]	0.5
Golden Ticket	[X]	[ ]	[X]	0.5

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	[X]	[ ]	[ ]	0.5
Silver Ticket	[ ]	[ ]	[X]	0.5
Golden Ticket	[ ]	[X]	[ ]	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?	Bei Pass-the-Hash wird der NTLM Hash im Authentication Package für NTLM in LSASS Memory ausgetauscht. Bei Over-Pass-the-Hash wird der NTLM Hash im Authentication Package für Kerberos in LSASS Memory ausgetauscht. In der Praxis macht Mimikatz bei PTH direkt beides auf einmal. Über das Netz geht aber erst einmal gar nichts.	0.5 0.5
Was geschieht bei einem Pass-the-Ticket Angriff genau?	Von einem kompromittierten System werden TGT und/oder ST Kerberos Tickets gestohlen und von einem anderen System aus bei Bedarf erneut zur Anmeldung mit der gestohlenen Identität genutzt.	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?	1.) User/Service Account (anstatt Machine Account) finden, der einen Service Principal Name (SPN) gesetzt hat 2.) Für den Account ein Service Ticket (ST) bestellen und dabei RC4_HMAC_MD5 Encryption wünschen 3.) Versuchen das Passwort des Accounts zu knacken mit hashcat oder John the Ripper	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?)	Gültigkeitsdauer kann von Angreifer frei gewählt werden (bis zu 10 Jahre) und bis Organisation den KRBTGT Hash resp. bis das Passwort des Accounts 2x nacheinander geändert hat.	0.5 0.5

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

1.10 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	Vorteile: - Es fliessen keine Daten mehr ab. Nachteile: - Der Angreifer bemerkt, dass er bemerkt wurde - Der Angreifer beginnt Spuren zu verwischen - Die Firma ist extern nicht erreichbar - Mitarbeiter können allenfalls nicht arbeiten Empfehlung: Es handelt sich um ein APT und es ist deshalb sinnvoll, erst alle "Unsicherheiten" zu beseitigen, bevor Containment betrieben wird. Der Angreifer könnte sonst seine Taktiken anpassen und die Aufklärung des Vorfalls wäre gefährdet.	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.	1) Scheduled Tasks Bspw. folgenden Logs weisen auf die Erstellung von neuen Scheduled Tasks hin - Security Log 4698 – Scheduled task created - Task Scheduler Log 106 – Scheduled task created 2) Run/RunOnce keys Die folgenden Registry Keys sollten nach unbekannten Einträgen durchsucht werden. - Jeweils HKLM und HKCU \Software\Microsoft - \Windows\CurrentVersion\Run - \Windows\CurrentVersion\Run - \Windows\CurrentVersion\RunOnce - \Windows\CurrentVersion\RunOnce	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.	1) Event ID: 4768…… Erläuterung: 4768 TGT granted bedeutet, dass mittels Kerberos authentisiert wurde und der TGS dem Benutzer ein TGT ausgestellt hat. Im Event ist das Quellsystem der Anfrage sowie der User, welcher das TGT gelöst hat ersichtlich. Somit kann die Zeit und das damit verbundene, gültige Login in der Domäne ermittelt werden. Es bedeutet aber noch nicht, dass der Benutzer auf den Share zugegriffen hat. 2) Event ID: 4769…….. Erläuterung: 4769 Service Ticket Granted beinhaltet das Zielsystem, die Quell-IP und den Logon User. Damit kann bewiesen werden, dass der User mindestens ein gültiges Ticket für den File Share bekommen hat. In der Regel werden Service Tickets ja nicht auf Halde bestellt sondern es erfolgt damit typischerweise auch ein Zugriff.	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	Artefakte in der Registry - Neuer Service in \CurrentControlSet\Services\ - ShimCache für .EXEs aber nicht für .DLLs - AmCache.hve – erste Ausführung von evil.exe Artefakte im File System - File Creation evil.exe or evil.dll malicious service executable or service DLL - Prefetch – C:\Windows\Prefetch\ evil.exe-{hash}.pf Keine Logs	3.0

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

1.11 Yara (7 Punkte)

Frage	Antwort	Punkte
Was ist YARA und erklären Sie die Bedeutung in Cyber Security	YARA ist ein Tool um nach Informationen in Binaries zu suchen. Es ist sowas wie «grep» für Binaries. In Yara kann man Regeln definieren, nach denen in Binary Daten gesucht werden, und diese mit AND oder OR Verknüpfungen verbinden.	1
Erklären Sie die Grundstruktur und wichtigsten Teile einer Yara Regel	1. Name der Regel 2. Meta Section für allgemeine Infos und Beschreibung über den Autor der Regel 3. Strings um Pattern zu beschreiben 4. Conditions um AND,OR von Strings zu beschreiben	2
Erklären Sie, wie man Conditions mit YARA abbildet. Erstellen Sie ein Beispiel wie man ein infiziertes File detektieren mittels Conditions erkennen könnte.	Die Suchbegriffe liegen in den Strings In den Conditions kann definiert werden, in welcher Kombination und wo der Suchbegriff vorkommen kann, mit AND und OR Operatoren und vielen weiteren Operatoren	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.	Grundsätzlich kann man mit Yara sowohl Binaries als auch Prozesse durchsuchen. Bei Polymorphic Malware ist das Problem, dass man im Binary keine Anhaltspunkte findet, höchstens die Load Funktion für das Laden von weiterer Funktionalität aus dem Internet. Bei Prozessen kann man ebenfalls die importierten API durchforsten, stellt sich aber trotzdem als schwierig dar. Mit Yara polymorphic Viren zuverlässig zu erkennen ist schwierig.	2

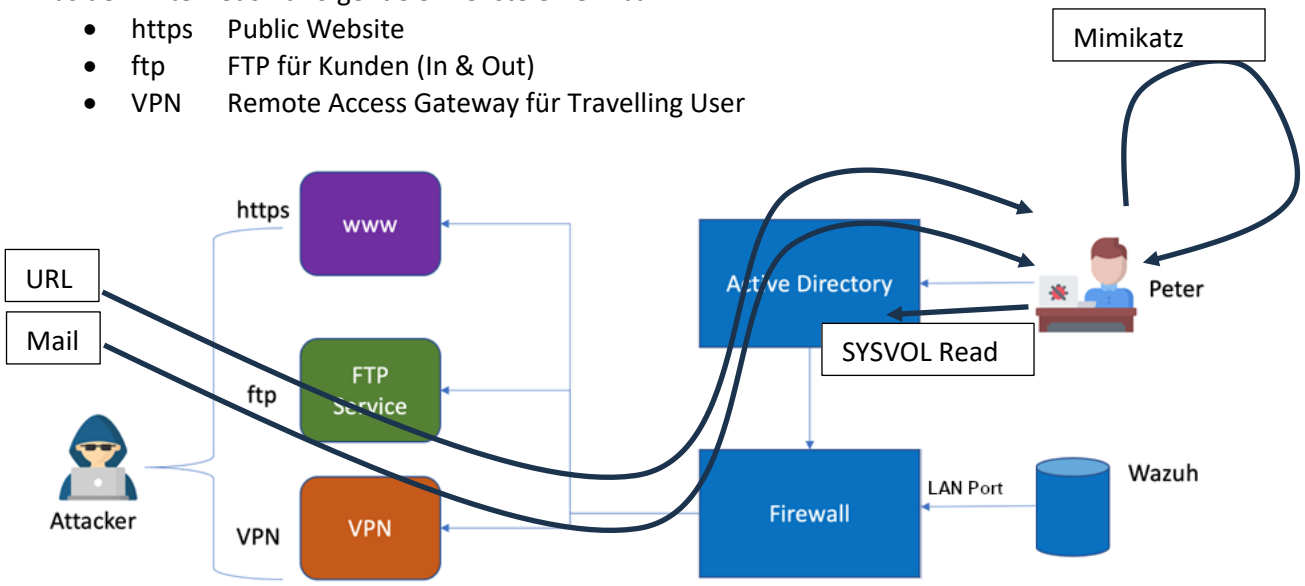
OST Ostschweizer Fachhochschule
Postfach 1475
CH-8640 Rapperswil
www.ost.ch

1.12 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 Malicious Word Dokument via E-Mail an Peter senden und mit einer gut gemachten Story Peter auffordern, das File zu öffnen. Variante 2 Malicious Word Dokument via Web Download anbieten und Peter auffordern, das Word File zu öffnen	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?	Post Exploitation Tool nutzen. Zuerst die Anti Viren Software ausschalten und Mimikatz ausführen. Mit Mimikatz hoffen, dass es dort Tickets zu stehlen gibt, die einem ein Lateral Movement ermöglichen.	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.	Installation Persistenz und Keystroke Sniffer und hoffen, dass in Zukunft über diesen Computer jemand mit Enterprise Admin Rechten einloggt Alternativ über SYSVOL AD Verzeichnis nach Informationen im AD suchen, über welche man Enterprise Admin erreichen könnte. Beispielsweise über das in der Vorlesung gezeigte XML mit dem Backup User und dem Passwort, das man mit dem Key von Microsoft entschlüsseln kann.	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. siehe Zeichnung oben.	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 Mimikatz Detection auf lsass.exe Prozess. Oder generell lsass.exe Prozess Monitoring	2
Was müssen Sie tun, um Ihren Angriff von **Step 2** innerhalb des Wazuh SIEM zu erkennen?	Step 2 Überwachung vom User gestartete Prozesse und deren Argumente	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.	Monitoring File Zugriff und Lesen/Schreiben von Files pro Zeiteinheit als Alert ausgeben. Wird heute so gemacht in Produkten wie NetApp und deren Ransomware Protection Über AD und GPO Policy für File Zugriffe monitoren	2

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

OST
Ostschweizer
Fachhochschule

1.13 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 Installation EDR Lösung oder mit sysmon.exe, lässt sich jeder Zugriff auf lsass.exe überwachen. Zusätzliche Überwachung auf Files wo Prozessdaten gespeichert werden (Hybernate, Caching)	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	listet die bevorzugten Backup-Master-Schlüssel auf Damit kann der Angreifer auf Backup Daten zugreifen um von dort an weitere vertrauliche Daten zu gelangen	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	listet DPAPI-gepufferte Masterkeys auf (dumping DPAPI secrets) Für diesen Befehl sind erhöhte Rechte erforderlich (durch vorherige Ausführung von privilege::debug oder durch Ausführung von Mimikatz als NT-AUTHORITY\SYSTEM-Konto). Die DPAPI (Data Protection API) ist eine interne Komponente des Windows-Systems. Sie ermöglicht es verschiedenen Anwendungen, sensible Daten (z. B. Passwörter) zu speichern. Die Daten werden im Benutzerverzeichnis gespeichert und sind durch benutzerspezifische Hauptschlüssel gesichert, die aus dem Kennwort des Benutzers abgeleitet werden.	2

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

1.14 Forensic Readiness (3 Punkte)

Frage	Antwort	Punkte
Erklären Sie das Konzept der unique-id im Kontext von Forensic Readiness in Web Anwendungen	Eindeutige Zahl pro http Request, die das erste System, üblicherweise eine WAF generiert, loggt und im Request Header ins Backend weiterleitet. Wenn alle Systeme in einer kaskadierten IT Landschaft diese Zahl zur Action loggen, dann weiss man immer wer wann welchen Request ausgeführt hat.	1
Wer ist für die Erstellung oder Erzeugung der unique-id zuständig?	Das vorderste System in einer Web Kaskade, üblicherweise die WAF. Wenn es keine WAF gibt, dann der Server der TLS terminiert.	1
Ist es wichtig, dass diese unique-id wirklich random ist? Oder reicht es, wenn es einfach ne Zahl ist die raufzählt?	Randomness ist nicht wichtig. Kann auch eine Zahl sein die raufzählt.	1

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

1.15 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?	Die Idee hierbei ist, dass ein Trojaner eine Art Inspection Proxy wie Burp oder ZAP enthält, über welchen der Verkehr dann aufgezeichnet und Passwörter oder ähnliches ausgelesen werden können. Damit dies ohne Warnung für den User funktioniert, muss der Angreifer ein CA Cert im Trusted Store haben, sonst gäbe es beim TLS Verkehr über die Malware eine TLS Error Meldung .	2
Wie könnte man mit einem SIEM solche Einträge oder Löschungen überwachen?	Ein modernes DER System hat die Möglichkeit, Manipulationen im Keystore zu erkennen, sprich im System das die CA Certs verwaltet.	2

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

OST
Ostschweizer
Fachhochschule

1.16 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**?	Zum einen muss der MX von Compass Security das sogenannte DMARC unterstützen, das ist eine Policy die bestimmt, was im Falle von einer Policy Violation passiert Der DNS von cybertycoon.ch muss eine Policy im DNS ablegen die besagt, wie man in einem solchen Fall umzugehen hat. Dann macht der MX von Compass Security eine DNS Abfrage bei cybertycoon.ch und anhand der Response weiss der MX, ob und wer von cybertycoon zu informieren sei.	2
Garantiert der von Ihnen beschriebene Lösungsansatz, dass Sie davon **erfahren**? Antwort mit **Begründung**	Nein, wenn der Mailserver der das Mail bekommt keine DMARC Unterstützung hat, dann bringt dieser Lösungsansatz nichts. Etwas anderes gibt es aber auch nicht.	2

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

Frage	Antwort	Punkte
Das Mail enthält ein Word File mit einem Self-Signed Makro. Was können Sie tun, damit Ihre Mitarbeiter vor diesem Makro (Virus) geschützt sind?	Gemäss Policy nur Word Files mit trusted signed Makros zulassen (oder Makros generell sperren) Ein Self-Signed Makro würde dann nicht gestartet werden durch MS Word.	1
Nehmen wir an ihr Schutz im vorherigen Schritt ist unwirksam und funktioniert nicht, welche zusätzliche Schutzmassnahmen gibt es?	Nutzung eines EDR, das die Ausführung vom Makro verhaltensgesteuert unterbindet. Auch kein 100% Schutz natürlich.	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?	Das Makro wird mit hoher Wahrscheinlichkeit mit dem Internet kommunizieren wollen (C2). Im Unternehmen könnte man also ein Pattern auf der Firewall oder Proxy oder Endpoint einrichten, dass die Malware keinen Dynamischen Content downloaden kann. Oder aber ein Blackholing der DNS Einträge, wo die C2 Server stehen.	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?	Durch Hunting mit einem SOAR Tool wie beispielsweise Velociraptor. Eine Suche erstellen und auf allen Clients nach Spuren des Virus suchen. Jeder Virus hat eine Signatur, einen Registry Key, ein Temp File oder ähnlich. Danach im Unternehmen suchen.	1

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

1.17 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 Event 4688: Via GPO das Logging von Prozessen und deren Argumente zu aktivieren Prio 2 Via GPO die Logs remote zu loggen, so dass diese vom Angreifer nicht geändert werden können Prio 3 Loggen von 4648(S) Explicit Credential Logon Prio 4 Loggen von 4672(S) Special Privileges Logon Prio 5 Loggen von Account Creation Check for 4728 / 4732 / 4756 events weitere Loggen, wenn Services eingerichtet werden: 7045 = once a service gets installed Loggen von Scheduled Tasks 4698: A scheduled task was created 4700: A scheduled task was enabled	5

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