QUIZZES

Created	@December 19, 2023 6:38 PM
Tags	

OSINT

What are "Google Dorks" and how are the used in OSINT?

- [ ] a. Google Dorks are a paid feature of Google Search. [Google Dorks sind eine bezahlte Funktion der Google-Suche.]
- [x] b. Google Dorks rely on Google Search features to gather OSINT information. [Google Dorks nutzen Google-Suchfunktionen, um OSINT-Informationen zu sammeln.]
- [ ] c. Google Dorks are employees of Google with special access to closed Google search data. [Google Dorks sind Mitarbeiter von Google mit speziellem Zugang zu nicht öffentlichen Google-Suchdaten.]
- [x] d. Google Dorks rely on public information of Google Search. [Google Dorks stützen sich auf öffentliche Informationen der Google-Suche.]

Public data from the Strava Fitness App enabled OSINT to ... [Öffentliche Daten aus der Strava-Fitness-App ermöglichten OSINT ...]

- [ ] a. Access heart rate information of well-known celebrities. [Zugriff auf die Herzfrequenzdaten bekannter Prominenter.]
- [x] b. Map walking paths of guards protecting critical infrastructure. [Kartierung der Routen von Wachleuten zum Schutz kritischer Infrastrukturen.]
- [x] c. Identify hidden military bases. [Verborgene Militärstützpunkte zu identifizieren.]
- [ ] d. Discover individuals with bad health habits. [Personen mit schlechten Gesundheitsgewohnheiten zu entdecken.]

Which of the following statements about OSINT are correct? [Welche der folgenden Aussagen über OSINT sind korrekt?]

- [ ] a. OSINT relies primarily on data from "Freedom of Information" requests. [OSINT stützt sich in erster Linie auf Daten aus "Freedom of Information"-Anfragen]
- [x] b. OSINT is the collection and analysis of data gathered from open sources. [OSINT beschreibt das Sammeln und die Analyse von Information aus offenen Quellen.]
- [ ] c. OSINT is an exclusive military strategy that relies on closed source data. [OSINT ist eine exklusive militärische Strategie, die sich auf geschlossene Datenquellen stützt.]
- [x] d. OSINT is used to de-anonymize individuals in criminal investigations. [OSINT wird verwendet um Individuen in strafrechtliche Ermittlungen zu identifizieren.]

Nym

The Nym Network ... [Das Nym-Netzwerk ...]

- [x] a. hinders timing analysis by employing cover traffic. [erschwert Zeitanalysen durch den Einsatz von Cover Traffic.]
- [ ] b. builds upon mix nodes exclusively operated by Nym Technologies S.A. [baut auf Mix-Knoten auf, die ausschließlich von Nym Technologies S.A. betrieben werden.]
- [ ] c. is a high-latency mix network for sending anonymous messages. [ist ein Mix Netzwerk mit hoher Latenz für den Versand anonymer Nachrichten.]
- [ ] d. enables one-way communication without the possibility of replying to messages. [ermöglicht Einwegkommunikation ohne die Möglichkeit, auf Nachrichten zu antworten.]

Verbleibende Zeit 0:02:08

Which of the following technologies are building blocks of the Nym Privacy Infrastructure? [Welche der folgenden Technologien sind Bausteine der Nym Privacy Infrastructure?]

- [x] a. Anonymous credentials.
- [ ] b. Tor hidden services.
- [x] c. Cryptocurrencies.
- [ ] d. I2P services.

Censorship

The Firewall of China works with the following methods ... [Die Firewall von China arbeitet mit den folgenden Methoden ...]

Wählen Sie eine oder mehrere Antworten:

- [x] a. DNS modification [DNS-Modifikationen]
- [ ] b. Manual verification using checklists. [Manueller Abgleich mit Checklisten]
- [x] c. Active probing to detect and block Tor bridges. [Aktives testen, detektieren und blockieren von Tor-Bridges.]
- [ ] d. Breaking the symmetric AES encryption in TLS1.3. [Brechen von symmetrischer AES Verschlüsselung innerhalb von TLS1.3.]

Which of the following statements about Domain Fronting are correct? [Welche folgenden Aussagen über Domain-Fronting sind korrekt?]

Wählen Sie eine oder mehrere Antworten:

- [ ] a. Domain Fronting does not work anymore because it is possible for censors to detect the hidden content. [Domain-Fronting funktioniert nicht mehr weil Zensoren den versteckten Inhalt entdecken können.]
- [x] b. Domain Fronting works because it creates collateral damage if blocked. [Domain-Fronting funktioniert weil es Kollateralschaden verursacht wenn es blockiert wird.]
- [x] c. Domain Fronting hides the censored endpoint in legitimate traffic. [Domain-Fronting versteckt den zensierten Endpunkt in legitimen Traffic]
- [x] d. Domain Fronting can be used in Tor. [Domain-Fronting kann in Tor verwendet werden.]

Messaging

According to the talk: What are properties that many people think of when they argue for decentralized messaging systems? [Gemäß des Vortrags: Was sind Eigenschaften an die Personen denken, wenn sie für dezentralisierte Messaging Systeme argumentieren?

- [ ] a. Easy of use
- [ ] b. Less complex systems
- [x] c. Censorship resistance
- [x] d. Privacy

TLS

Which statements regarding DoH and DoT are true?

Wählen Sie eine oder mehrere Antworten:

- [ ] a. DoH is a more complex protocol, so it is harder to implement. (DoH ist ein komplexeres Protokoll und deshalb schwerer zu implementieren)
- [x] b. DoT can be easily blocked. [DoT kann leicht blockiert werden.]
- [x] c. DoH allows DNS resultion on application level. (DoH erlaubt DNS Auflösung auf Applikationslevel).
- [ ] d. DoH uses the TCP port 853 [DoH verwendet den TCP Port 853]

Tor

What is Arti? [Was ist Arti?]

- [ ] a. Arti is already available and used en-large. [Arti ist bereits verfügbar und wird im großen Stil eingesetzt.]
- [ ] b. The name of the Tor implementation in C. [Der Name für die Tor Implementierung in C.]
- [ ] c. The name of one of the developers of Tor. [Der Name eines Tor Entwicklers.]
- [x] d. A complete reimplementation of the Tor codebase in Rust. [Eine komplette Reimplementierung von Tor in Rust]

Which statement about "Snowflakes" in the context of Tor is/are true ? [Welche der folgenden Aussage(n) über Snowflakes trifft im Kontext von Tor zu?]

- [x] a. There are currently about 150.000 available. [Es gibt ca. 150.000]
- [x] b. Snowflakes are browser extensions that are used to facilitate access to the Tor network in case of Internet censorship. [Snowflakes sind Browser Erweiterungen die den Zugang zum Tornetzwerk bei zensiertem Internet ermöglichen.]
- [ ] c. Snowflakes are the exit relays of the Tor browser [Snowflakes sind die Ausgänge aus dem Tornetzwerk im Torbrowser]
- [ ] d. There are currently about 15 million Snowflakes. [Es gibt im Moment ca. 15 Millionen Snowflakes]

VPN

What is the gist of the "bypassing tunnels" paper which was published at USENIX Security 2023? [Worum geht es im "Bypassing Tunnels" Paper von der USENIX Security 2023?]

- [x] a. An attacker can trick a client device into thinking the target server is on the same local network, thus bypassing the VPN connection to that server. [Der Trick ist das der Client glaubt er ist im gleichen Netzwerk wie der Zielserver, und umgeht die VPN Verbindung zu dem einen Server]
- [ ] b. Only macOS and iOS devices were found to be immune against the described attacks. [Nur macOS und iOS Geräte waren immun gegen die gezeigten Angriffe]
- [ ] c. They broke the used cryptography in VPN implementations. [Sie haben die Kryptografie in VPN Implementierungen geknackt]
- [ ] d. The described attack requires the attacker to have root permissions on the victim device to change the routing table. [Der beschriebene Angriff beschreibt wie ein Angreifer mit Root Rechten auf dem Opfergerät die Routing Tabelle ändern kann]

What information is used in fingerprinting TLS connections using JA3? [Welche Informationen werden verwendet um einen JA3 Fingerabdruck auf TLS Verbindungen zu erstellen?]

- [ ] a. The browser user agent string. [Der Identifizierungsstring des Browsers]
- [ ] b. The ip address of the server. [Die IP Adresse vom Zielserver]
- [x] c. The offered elliptic curves & their points in the client handshake. [Die im Verbindungsaufbau angebotetenen elliptischen Kurven und die darauf verwendeten Punkte]
- [x] d. The accepted CipherSuites from the client device. [Die angebotenen CipherSuites]

Which statementent regarding the differences between JA3 and JA4 is/are true? [Welche Aussagen zu den Unterschiede zwischen JA3 und JA4 ist/sind wahr?]

- [x] a. JA4 can work with QUIC and encrypted client handshakes (ECH). [JA4 kann mit QUIC und verschlüsselten Verbindungsaufbauten umgehen]
- [x] b. JA3 is MD5, JA4 is 3 part modular encoding. [JA3 verwendet MD5, JA4 eine 3-geteilte modulare Darstellung]
- [ ] c. JA3 could already handle QUIC and encrypted client handshakes. [JA3 konnte auch schon mit QUIC und verschlüsselten Verbindungsaufbauten umgehen]
- [ ] d. JA3 is 3 part modular encoding, JA4 is MD5. [JA3 verwendet eine 3-geteilte modulare Darstellung, JA4 verwendet MD5]