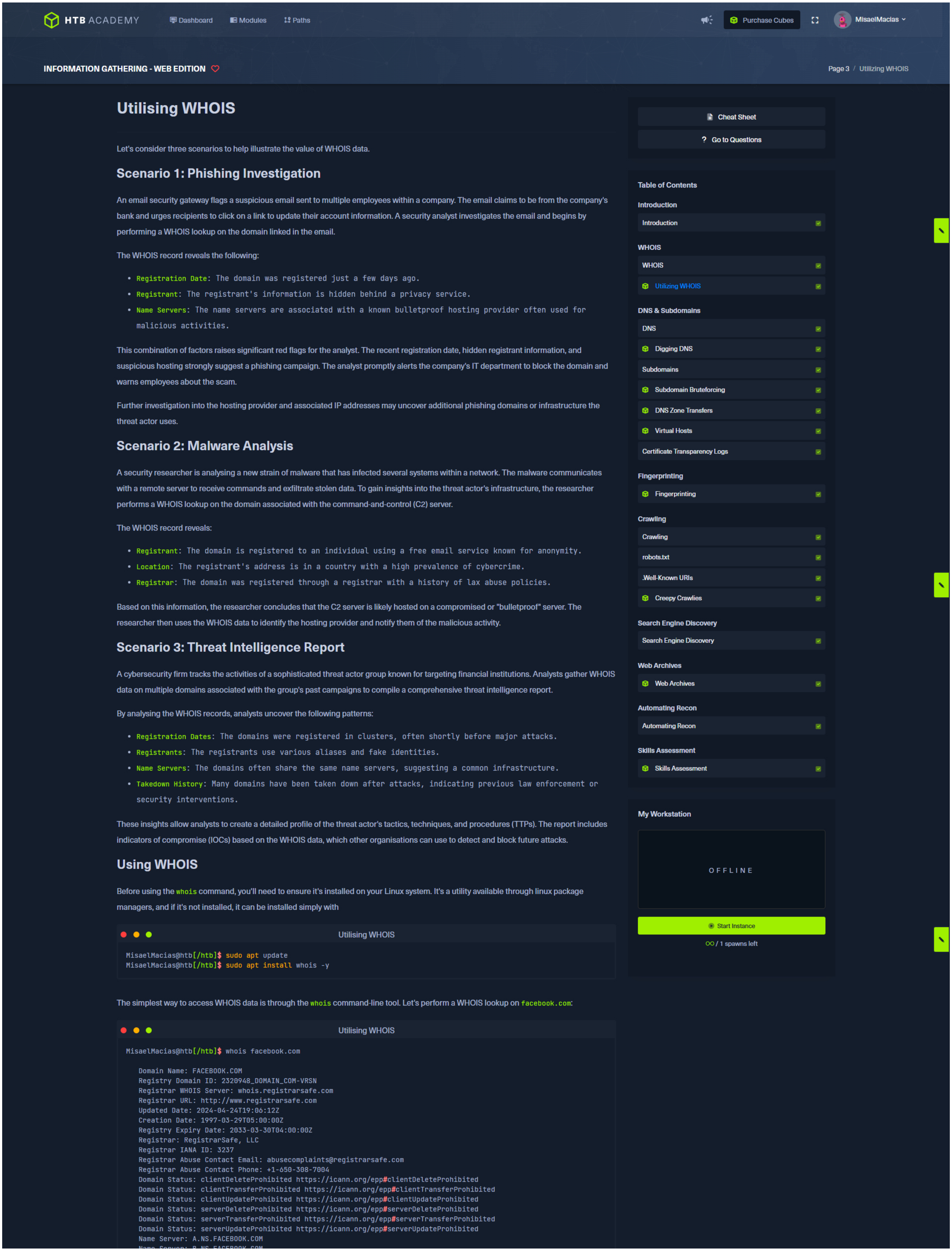


Utilising WHOIS

Let's consider three scenarios to help illustrate the value of WHOIS data.

Scenario 1: Phishing Investigation

An email security gateway flags a suspicious email sent to multiple employees within a company. The email claims to be from the company's bank and urges recipients to click on a link to update their account information. A security analyst investigates the email and begins by performing a WHOIS lookup on the domain linked in the email.

The WHOIS record reveals the following:

- `Registration Date`: The domain was registered just a few days ago.
- `Registrant`: The registrant's information is hidden behind a privacy service.
- `Name Servers`: The name servers are associated with a known bulletproof hosting provider often used for malicious activities.

This combination of factors raises significant red flags for the analyst. The recent registration date, hidden registrant information, and suspicious hosting strongly suggest a phishing campaign. The analyst promptly alerts the company's IT department to block the domain and warns employees about the scam.

Further investigation into the hosting provider and associated IP addresses may uncover additional phishing domains or infrastructure the threat actor uses.

Scenario 2: Malware Analysis

A security researcher is analysing a new strain of malware that has infected several systems within a network. The malware communicates with a remote server to receive commands and exfiltrate stolen data. To gain insights into the threat actor's infrastructure, the researcher performs a WHOIS lookup on the domain associated with the command-and-control (C2) server.

The WHOIS record reveals:

- `Registrant`: The domain is registered to an individual using a free email service known for anonymity.
- `Location`: The registrant's address is in a country with a high prevalence of cybercrime.
- `Registrar`: The domain was registered through a registrar with a history of lax abuse policies.

Based on this information, the researcher concludes that the C2 server is likely hosted on a compromised or "bulletproof" server. The researcher then uses the WHOIS data to identify the hosting provider and notify them of the malicious activity.

Scenario 3: Threat Intelligence Report

A cybersecurity firm tracks the activities of a sophisticated threat actor group known for targeting financial institutions. Analysts gather WHOIS data on multiple domains associated with the group's past campaigns to compile a comprehensive threat intelligence report.

By analysing the WHOIS records, analysts uncover the following patterns:

- `Registration Dates`: The domains were registered in clusters, often shortly before major attacks.
- `Registrants`: The registrants use various aliases and fake identities.
- `Name Servers`: The domains often share the same name servers, suggesting a common infrastructure.
- `Takedown History`: Many domains have been taken down after attacks, indicating previous law enforcement or security interventions.

These insights allow analysts to create a detailed profile of the threat actor's tactics, techniques, and procedures (TTPs). The report includes indicators of compromise (IOCs) based on the WHOIS data, which other organisations can use to detect and block future attacks.

Using WHOIS

Before using the `whois` command, you'll need to ensure it's installed on your Linux system. It's a utility available through linux package managers, and if it's not installed, it can be installed simply with

Utilising WHOIS

```
MisaelMacias@htb[/htb]$ sudo apt update
MisaelMacias@htb[/htb]$ sudo apt install whois -y
```

The simplest way to access WHOIS data is through the `whois` command-line tool. Let's perform a WHOIS lookup on `facebook.com`:

Utilising WHOIS

```
MisaelMacias@htb[/htb]$ whois facebook.com

   Domain Name: FACEBOOK.COM
   Registry Domain ID: 2320948_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.registrarsafe.com
   Registrar URL: http://www.registrarsafe.com
   Updated Date: 2024-04-24T19:06:12Z
   Creation Date: 1997-03-29T05:00:00Z
   Registry Expiry Date: 2033-03-30T04:00:00Z
   Registrar: RegistrarSafe, LLC
   Registrar IANA ID: 3237
   Registrar Abuse Contact Email: abusecomplaints@registrarsafe.com
   Registrar Abuse Contact Phone: +1-650-308-7004
   Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
   Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
   Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
   Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
   Name Server: A.NS.FACEBOOK.COM
   Name Server: B.NS.FACEBOOK.COM
```

Table of Contents

Introduction

WHOIS

DNS & Subdomains

Fingerprinting

Crawling

Search Engine Discovery

Web Archives

Automating Recon

Skills Assessment

My Workstation

```
   Name Server: B.NS.FACEBOOK.COM
   Name Server: C.NS.FACEBOOK.COM
   Name Server: D.NS.FACEBOOK.COM
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2024-06-01T11:24:10Z <<<

[...]
Registry Registrant ID:
Registrant Name: Domain Admin
Registrant Organization: Meta Platforms, Inc.
[...]
```

The WHOIS output for `facebook.com` reveals several key details:

1. `Domain Registration`:
   - `Registrar`: RegistrarSafe, LLC
   - `Creation Date`: 1997-03-29
   - `Expiry Date`: 2033-03-30

   These details indicate that the domain is registered with RegistrarSafe, LLC, and has been active for a considerable period, suggesting its legitimacy and established online presence. The distant expiry date further reinforces its longevity.
2. `Domain Owner`:
   - `Registrant/Admin/Tech Organization`: Meta Platforms, Inc.
   - `Registrant/Admin/Tech Contact`: Domain Admin

   This information identifies Meta Platforms, Inc. as the organization behind `facebook.com`, and "Domain Admin" as the point of contact for domain-related matters. This is consistent with the expectation that Facebook, a prominent social media platform, is owned by Meta Platforms, Inc.
3. `Domain Status`:
   - `clientDeleteProhibited`, `clientTransferProhibited`, `clientUpdateProhibited`, `serverDeleteProhibited`, `serverTransferProhibited`, and `serverUpdateProhibited`

   These statuses indicate that the domain is protected against unauthorized changes, transfers, or deletions on both the client and server sides. This highlights a strong emphasis on security and control over the domain.
4. `Name Servers`:
   - `A.NS.FACEBOOK.COM`, `B.NS.FACEBOOK.COM`, `C.NS.FACEBOOK.COM`, `D.NS.FACEBOOK.COM`

   These name servers are all within the `facebook.com` domain, suggesting that Meta Platforms, Inc. manages its DNS infrastructure. It is common practice for large organizations to maintain control and reliability over their DNS resolution.

Overall, the WHOIS output for `facebook.com` aligns with expectations for a well-established and secure domain owned by a large organization like Meta Platforms, Inc.

While the WHOIS record provides contact information for domain-related issues, it might not be directly helpful in identifying individual employees or specific vulnerabilities. This highlights the need to combine WHOIS data with other reconnaissance techniques to understand the target's digital footprint comprehensively.

Connect to Pwnbox

Your own web-based Parrot Linux instance to play our labs.

Pwnbox Location

UK 138ms

Terminate Pwnbox to switch location

Start Instance

∞ / 1 spawns left

Waiting to start...

Enable step-by-step solutions for all questions

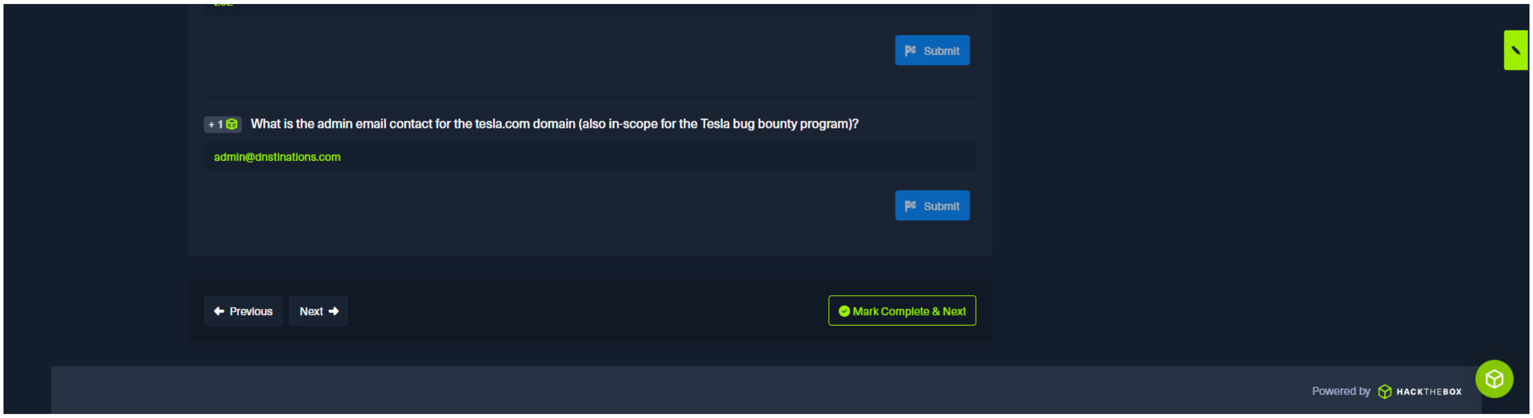
Questions

Cheat Sheet

Answer the question(s) below to complete this Section and earn cubes!

+ 1 Perform a WHOIS lookup against the paypal.com domain. What is the registrar Internet Assigned Numbers Authority (IANA) ID number?

292



+1 What is the admin email contact for the tesla.com domain (also in-scope for the Tesla bug bounty program)?

admin@dnstinations.com