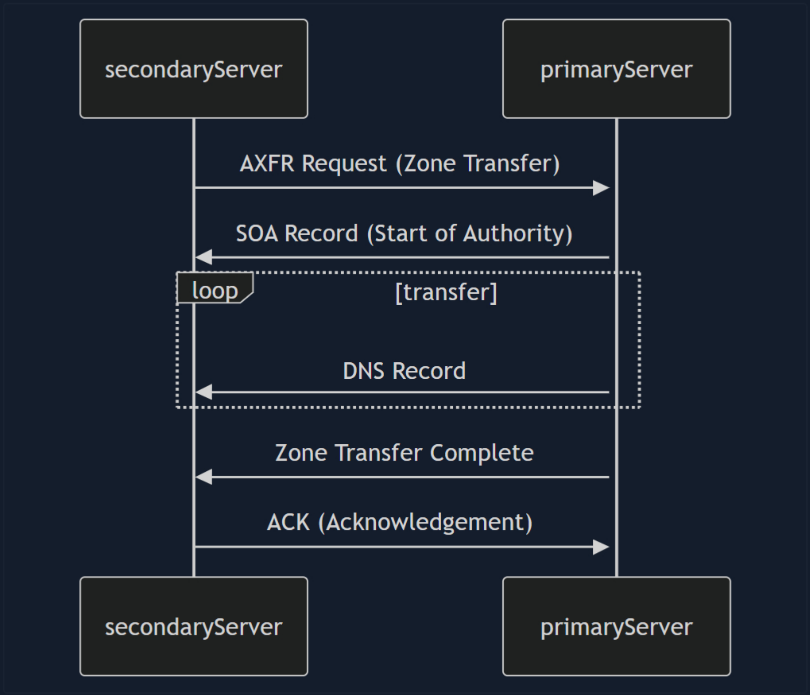
DNS Zone Transfers

While brute-forcing can be a fruitful approach, there's a less invasive and potentially more efficient method for uncovering subdomains – DNS zone transfers. This mechanism, designed for replicating DNS records between name servers, can inadvertently become a goldmine of information for prying eyes if misconfigured.

What is a Zone Transfer

A DNS zone transfer is essentially a wholesale copy of all DNS records within a zone (a domain and its subdomains) from one name server to another. This process is essential for maintaining consistency and redundancy across DNS servers. However, if not adequately secured, unauthorised parties can download the entire zone file, revealing a complete list of subdomains, their associated IP addresses, and other sensitive DNS data.



1. `Zone Transfer Request (AXFR)`: The secondary DNS server initiates the process by sending a zone transfer request to the primary server. This request typically uses the AXFR (Full Zone Transfer) type.
2. `SOA Record Transfer`: Upon receiving the request (and potentially authenticating the secondary server), the primary server responds by sending its Start of Authority (SOA) record. The SOA record contains vital information about the zone, including its serial number, which helps the secondary server determine if its zone data is current.
3. `DNS Records Transmission`: The primary server then transfers all the DNS records in the zone to the secondary server, one by one. This includes records like A, AAAA, MX, CNAME, NS, and others that define the domain's subdomains, mail servers, name servers, and other configurations.
4. `Zone Transfer Complete`: Once all records have been transmitted, the primary server signals the end of the zone transfer. This notification informs the secondary server that it has received a complete copy of the zone data.
5. `Acknowledgement (ACK)`: The secondary server sends an acknowledgement message to the primary server, confirming the successful receipt and processing of the zone data. This completes the zone transfer process.

The Zone Transfer Vulnerability

While zone transfers are essential for legitimate DNS management, a misconfigured DNS server can transform this process into a significant security vulnerability. The core issue lies in the access controls governing who can initiate a zone transfer.

In the early days of the internet, allowing any client to request a zone transfer from a DNS server was common practice. This open approach simplified administration but opened a gaping security hole. It meant that anyone, including malicious actors, could ask a DNS server for a complete copy of its zone file, which contains a wealth of sensitive information.

The information gleaned from an unauthorised zone transfer can be invaluable to an attacker. It reveals a comprehensive map of the target's DNS infrastructure, including:

- `Subdomains`: A complete list of subdomains, many of which might not be linked from the main website or easily discoverable through other means. These hidden subdomains could host development servers, staging environments, administrative panels, or other sensitive resources.
- `IP Addresses`: The IP addresses associated with each subdomain, providing potential targets for further reconnaissance or attacks.
- `Name Server Records`: Details about the authoritative name servers for the domain, revealing the hosting provider and potential misconfigurations.

Cheat Sheet
? Go to Questions

Table of Contents

My Workstation

OFFLINE

Start Instance

∞ / 1 spawns left

Remediation

Fortunately, awareness of this vulnerability has grown, and most DNS server administrators have mitigated the risk. Modern DNS servers are typically configured to allow zone transfers only to trusted secondary servers, ensuring that sensitive zone data remains confidential.

However, misconfigurations can still occur due to human error or outdated practices. This is why attempting a zone transfer (with proper authorisation) remains a valuable reconnaissance technique. Even if unsuccessful, the attempt can reveal information about the DNS server's configuration and security posture.

Exploiting Zone Transfers

You can use the `dig` command to request a zone transfer:

DNS Zone Transfers

```
MisaelMacias@htb[/htb]$ dig axfr @nsztm1.digi.ninja zonetransfer.me
```

This command instructs `dig` to request a full zone transfer (`axfr`) from the DNS server responsible for `zonetransfer.me`. If the server is misconfigured and allows the transfer, you'll receive a complete list of DNS records for the domain, including all subdomains.

DNS Zone Transfers

```
MisaelMacias@htb[/htb]$ dig axfr @nsztm1.digi.ninja zonetransfer.me

; <<>> DiG 9.18.12-1~bpo11+1-Debian <<>> axfr @nsztm1.digi.ninja zonetransfer.me
; (1 server found)
;; global options: +cmd
zonetransfer.me.    7200    IN  SOA nsztm1.digi.ninja. robin.digi.ninja. 2019100801 172800 900 1209600 3600
zonetransfer.me.    300 IN  HINFO   "Casio fx-700G" "Windows XP"
zonetransfer.me.    301 IN  TXT "google-site-verification=tyP28J7JAUHA9fw2sHXMgcCC0I6XBmmoVi04VlMewxA"
zonetransfer.me.    7200    IN  MX  0 ASPMX.L.GOOGLE.COM.
...
zonetransfer.me.    7200    IN  A   5.196.105.14
zonetransfer.me.    7200    IN  NS  nsztm1.digi.ninja.
zonetransfer.me.    7200    IN  NS  nsztm2.digi.ninja.
_acme-challenge.zonetransfer.me. 301 IN TXT "6Oa05hbUJ9xSsvYy7pApQvwCUSSGgxvrbdizjePEsZI"
_sip._tcp.zonetransfer.me. 14000 IN SRV 0 0 5060 www.zonetransfer.me.
14.105.196.5.IN-ADDR.ARPA.zonetransfer.me. 7200 IN PTR www.zonetransfer.me.
asfdbauthdns.zonetransfer.me. 7900 IN   AFSDB   1 asfdbbox.zonetransfer.me.
asfdbbox.zonetransfer.me. 7200  IN  A   127.0.0.1
asfdbvolume.zonetransfer.me. 7800 IN    AFSDB   1 asfdbbox.zonetransfer.me.
canberra-office.zonetransfer.me. 7200 IN A  202.14.81.230
...
;; Query time: 10 msec
;; SERVER: 81.4.108.41#53(nsztm1.digi.ninja) (TCP)
;; WHEN: Mon May 27 18:31:35 BST 2024
;; XFR size: 50 records (messages 1, bytes 2085)
```

`zonetransfer.me` is a service specifically setup to demonstrate the risks of zone transfers so that the `dig` command will return the full zone record.

VPN Servers

⚠ **Warning:** Each time you "Switch", your connection keys are regenerated and you must re-download your VPN connection file.

All VM instances associated with the old VPN Server will be terminated when switching to a new VPN server.

Existing PwnBox instances will automatically switch to the new VPN server.

US Academy 3 — Medium Load ▾

PROTOCOL

● UDP 1337 ○ TCP 443

DOWNLOAD VPN CONNECTION FILE

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

Pwnbox Location

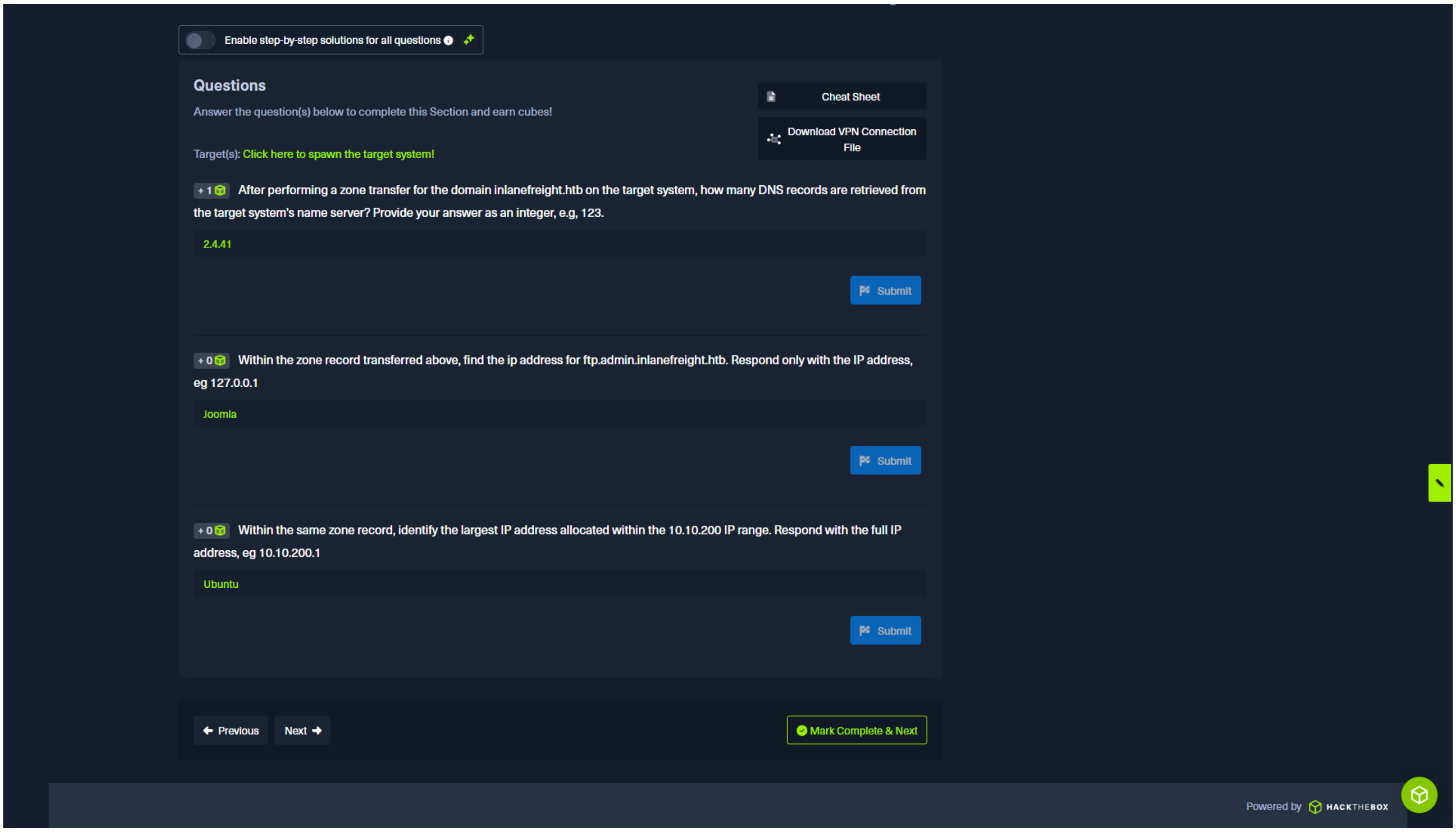
UK — 137ms ▾

ⓘ Terminate Pwnbox to switch location

Start Instance

∞ / 1 spawns left

Waiting to start...



Enable step-by-step solutions for all questions

Questions

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

Target(s): Click here to spawn the target system!

+ 1 After performing a zone transfer for the domain inlanefreight.htb on the target system, how many DNS records are retrieved from the target system's name server? Provide your answer as an integer, e.g, 123.

2.4.41

+ 0 Within the zone record transferred above, find the ip address for ftp.admin.inlanefreight.htb. Respond only with the IP address, eg 127.0.0.1

Joomla

+ 0 Within the same zone record, identify the largest IP address allocated within the 10.10.200 IP range. Respond with the full IP address, eg 10.10.200.1

Ubuntu