

Vulnyx: Zone DNS Enumeration

DNS, the “phone directory” of the internet, is used to keep track of which domain names are associated with which IP addresses, and vice versa



Vulnyx: Zone DNS Enumeration

On a network, if we know the IP address of a DNS server and a domain name, we can query that DNS server for additional information



Vulnyx: Zone DNS Zone Transfer

```
└$ dig axfr securezone.nyx @192.168.212.19

; <>> DiG 9.20.11-4+b1-Debian <>> axfr se
;; global options: +cmd
securezone.nyx.          604800  IN      SOA
800 86400 2419200 604800
securezone.nyx.          604800  IN      NS
admin.securezone.nyx.    604800  IN      A
```

DNS servers can perform a **zone transfer**, which allows all DNS records held by the server to be copied

Vulnyx: Zone DNS Zone Transfer

```
└$ dig axfr securezone.nyx @192.168.212.19

; <>> DiG 9.20.11-4+b1-Debian <>> axfr se
;; global options: +cmd
securezone.nyx.          604800  IN      SOA
800 86400 2419200 604800
securezone.nyx.          604800  IN      NS
admin.securezone.nyx.    604800  IN      A
```

If a DNS allows zone transfer without use of a key,
that's a security misconfiguration

Privilege Escalation Sudo Ranger

Ranger is a text-based file manager program. For the purposes of privilege escalation, we need to pay attention to the following, from the official Github repo...



Privilege Escalation Sudo Ranger

Ranger is a console file manager with VI key bindings. It provides a minimalistic and nice curses interface with a view on the directory hierarchy. It ships with rifle , a

Since the program has VI key bindings, it's likely that we will be able to spawn a shell in Ranger, much like we can with VI or VIM

Privilege Escalation

Sudo Ranger

Shell

It can be used to break out from restricted

(a) vi -c ':!/bin/sh' /dev/null

This entry from the GTFObins website is similar to how we would start an interactive shell session inside of the Ranger program

Privilege Escalation

Sudo Lynx

Lynx is a text-based web browser, allowing web pages to be viewed without a graphic-user interface



Privilege Escalation

Sudo Lynx

!

When “!” is pressed your default shell will be spawned Lynx (usually *exit* under Unix and *logout* under VMS). This users. On VMS, “\$” normally is a synonym.

For privilege escalation purposes, the important thing we need to know is that the program can spawn an interactive shell. See the above documentation from the official Lynx website