Penetration Test Exercise 03

Esteban Calvo

2023-10-25

Contents

1 Technical Report

1.1 Finding: *Private IP Subdomains*

Severity Rating

During network scanning, several private subdomains were discovered visible to users without the required privileges. This vulnerability can lead to the exposure of internal infrastructure, internal network scanning, and exploitation of user data.

CVSS Base Severity Rating: 3.3 AV:L AC:L PR:L UI:N S:U C:L I:N A:N

Vulnerability Description

This vulnerability can be present on various machines within the organization, typically those responsible for DNS configuration and management. Specifically, it may affect DNS servers and related services responsible for resolving domain names to IP addresses.

Confirmation method

To confirm these vulnerabilities, the use of CeWl and fierce in the kali command line can be used. Running the command ”cewl http://www.artstailor.com -d 3 -o -w list.txt” and then using this list to run ”fierce --domain artstailor.com --subdomain-file list.txt” will reveal several subdomains with IP addresses starting with 10. This IP address is generally reserved for private internal networks and should not be exposed to the public.

Mitigation or Resolution Strategy

To resolve this issue, the client can carefully review the companies DNS configuration to figure out where this information is being exposed from. From here, ensure that only public facing subdomains are shown in the DNS records. Also, figure out why these were available to begin with and see if more checks need to be implemented on who can change this configuration.

2 Attack Narrative

To find the private subdomains, there were several different steps. Firstly, I ran ”fierce --domain artstailor.com” and got a list of some subdomains, but all of these were public domains. From here, I wanted to find where this list was coming from to confirm how it was found. Running ”locate fierce | grep '\.txt'” showed me that where the default list was and running grep on this list along with the outcome of fierce showed me how these subdomains were found. From inside the fierce source code, I was also able to see that running --subdomain-file changes what file it reads. The blocks found up this point are

$$
\begin{gathered}
172.70.184.3 : mail.artstailor.com \\
172.70.184.3 : innerouter.artstailor.com. \\
172.70.184.133 : ns.artstailor.com. \\
172.70.184.3 : pop.artstailor.com. \\
10.70.184.90 : pdc.artstailor.com. \\
10.70.184.91 : books.artstailor.com.
\end{gathered}
$$

After this, I ran CeWL and used the list generated as an argument for fierce using the previous flag. From here, I was able to see several private subdomains that should have been hidden but were not such as

$$
\begin{gathered}
10.70.184.39 : costumes.artstailor.com \\
10.70.184.40 : KEY005 - hKku4/qTxNsmJIG0iT8pSQ.artstailor.com.
\end{gathered}
$$

On a similar note, running ”fierce --domain artstailor.com --wide” also revealed several other private networks such as

$$
\begin{gathered}
10.70.184.133 : linuxserver.artstailor.com \\
10.70.184.100 : devbox.artstailor.com
\end{gathered}
$$

that were not visible simply by using the CeWL list.

2.1 MITRE ATT&CK Framework TTPs

TA0043: Reconnaissance
    T1595: Active Scanning
        .001: Scanning IP Blocks

TA0043: Reconnaissance

- **T1595:** Active Scanning
  - **.003:** Wordlist Scanning