**Name:erfan ahmadbeigi**

**Master :Mr.milad nourian nasab**

**Network scanning with Fierce**

Today, we will be introducing Fierce, a fantastic network mapping, and port scanning tool. Often used to locate non-contiguous IP space and hostnames across networks, Fierce is far more than just a simple IP scanner or a DDoS tool. It is a great reconnaissance tool that is used by whitehat communities all over the world.

Fierce is specifically designed for corporate networks and is used to discover likely targets in the networks of their systems. Capable of scanning for domains within minutes, Fierce is becoming the preferred tool for performing vulnerability checks in large networks.

### How Fierce performs Scanning

Despite being such a resourceful and effective recon tool, it’s working is relatively simple. It starts the scanning process with brute force attacks if it is not possible for it to readily perform zone transfer of the target domain. Fierce uses a predetermined wordlist that contains possible subdomains it can detect. If a subdomain isn’t on the list, it will not be detected.

### Performing a basic scan with Fierce

Let’s demonstrate how Fierce works with a simple scan with default settings. Here, we’re performing a basic scan on (websitename.com). To initiate scanning, type:

The scan inquires the names of the servers the target website is hosted on. Next, it will attempt a zone transfer against those servers, which is most likely to fail but, on rare occasions, may work. This is mostly because DNS queries made by the scan terminate against the third-party servers.

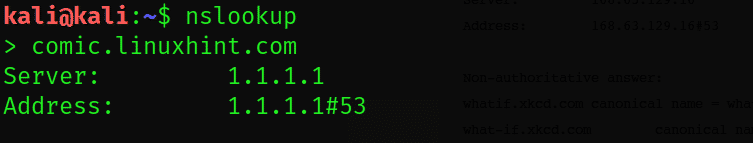
If the zone transfer fails, whe scan would attempt to locate the wildcard A record, which is relevant as it lists all the subdomains that are automatically assigned to an IP address. DNS A records look something like:

Notice how it shows the temp resolved to a.b.c.d. This is in part due to the fact that in DNS, a value of \*, resolve a subdomain to its IP address. The attempts at brute-forcing subdomains performed are usually endured and neutralized by this type of record. Still, we can procure some relevant data by searching for additional values.

For example, you can tell whether a subdomain is legit by looking at the IP it is resolved to. If several URLs resolve to a specific IP, they’re likely forfeited to protect the server from the scans such as the one we’re performing here. Usually, websites with unique IP values are real.

Moving on to other scan results, you’ll see that 11 entries were detected from the 1594 words we checked. In our case, we found one entry(c.xkcd.com ) that contained vital information after thoroughly checking. Let us see what this entry has for us.

*$*nslookup



The nslookup utility has checked the comic.linuxhint.com subdomain and failed to get any results. However, it’s the inquiry of checking the whatif.linuxhint.com subdomain has yielded some substantial results: namely a CN and A record response.