RECON (Reconnaissance)

RECON or Reconnaissance in web security is the first and one of the most important stages of security assessment. This stage includes gathering information about the target in order to identify and exploit possible weaknesses.

Running the Reconnaissance stage in a hidden and silent way can reduce the risk of detection by the target's security systems. This allows hackers to collect the information they need without attracting attention. In fact, the more time you spend at this stage, the more likely you are to discover vulnerabilities and **critical** assets!

RECON CATEGORIES

RECON is divided into two general categories: **EXTERNAL RECON** & **INTERNAL RECON**.

EXTERNAL RECON

This step include gathering information that is done without internal access to the systems and from the outside of target network. This type of identification takes place without direct interaction with the target and uses public sources and available information. The purpose of

this step is to obtain basic information for planning the next steps of penetration testing. In this section we have two main phases that include: **Vertical** & **Horizontal**.

Vertical Phase

The vertical phase is one of the most common phases of RECON and everyone, even beginners have done this phase. In this phase, we gather information about the main target subdomains. For example if we are working on `Google.com`, our Vertical phase will only include Google subdomain such as: `docs.google.com` & `mail.google.com`.

Vertical Phase Workflow

- **Domain Information Gathering** → `Whois` …
- **DNS Enumeration** → `DNS Records Discovery`
- **Subdomain Enumeration** → `Subfinder & Amass` …
- **DNS Brute Force** → `Puredns`, `ShuffleDNS`
- **SSL Certificate Search** → `Nmap`
- **Search Engine** → `Shodan`, `Censys` …
- **Google Dorking**

Horizontal Phase

In Horizontal phase, there is a different definition and we will focus on a larger scale of the target, in fact Horizontal phase includes all the assets of the target! For example if we are working on `Google.com`, our Horizontal phase will include All Google assets like `YouTube` & `Android` and etc.

> So the difference between the Vertical and Horizontal phases was that the Vertical phase include target subdomains and the Horizontal phase include the target assets, most of the targets that we spend time on and have experience working on are placed in the Vertical phase!

Horizontal Phase Workflow

- **Organizational Information Gathering**
- **Check the IPs and IP ranges associated with the domain**
- **Social Media Analysis**
- **Follow Company News & Check The New Assets**

- **Social Engineering**
- **Google Dorking**

INTERNAL RECON

This step is done after initial access to the target, this type of detection involves direct interaction with the target and may be more visible and increase detection by defense systems(**WAF**). The goal of this phase is to gather more detailed and complete information from the internal infrastructure to plan more advanced attacks. This section only have one phase: **Application Recon**(**Narrow Recon**).

Application Recon

In this phase, we will examine the internal target and try to discover the vulnerable services and technologies of the target, also in this phase we will examine **logical** and **technical** vulnerabilities.

Application Recon Phase Workflow

- **Port Scan** → `Nmap` , `RustScan`
- **Service & Technology Discovery**
- **Hidden Content Discovery** → `X8` , `Ffuf` , `FallParams`…
- **Check Web Archive** → `Waybackurls`
- **Directory & file Discovery** → `Katana` , `Gospider` , `Hakrawler` , `Gau` …
- **Find Vulnerable & Unpatched Service,Plugin,Library…**
- **Vulnerability Scanner** → `Acunetix` , `Nuclei` , `Nessus` …
- **Google & GitHub Dorking**
- **Manual Testing** → `BurpSuite`

> Be sure to take Recon seriously and set aside time to learn Recon topics, after learning the topics properly and deeply, try to automate each route and create a personal tool, because automating the steps and routes will increase your speed and accuracy.

In the next articles, I will post more specialized and detailed information about each of the categories and phases of RECON, in this article I was just trying to familiarize you with the concept of RECON and its categories.

GitHub: https://github.com/abolfazlvaziri
Instagram: https://instagram.com/abolfazlvaziriofficial
Telegram Channel: https://t.me/AVN_COMMUNITY
YouTube: https://www.youtube.com/@abolfazlvaziri