PRACTICAL 7

* RECONNAISSANCE
* VULNERABILITY
* WHY WE REQUIRE RECONNAISSANCE TOOL?
* RECONNISSANCE TOOLS

RECONNAISSANCE

Reconnaissance is the information-gathering stage of ethical hacking, where you collect data about the target system. This data can include anything from network infrastructure to employee contact details. The goal of reconnaissance is to identify as many potential attack vectors as possible.

VULNERABILITY

**Vulnerabilities** are weaknesses in a system that gives threats the opportunity to compromise assets. All systems have vulnerabilities. Even though the technologies are improving but the number of vulnerabilities are increasing such as tens of millions of lines of code, many developers, human weaknesses, etc. Vulnerabilities mostly happened because of Hardware, Software, Network and Procedural vulnerabilities.

**There are 2 types of vulnerability**:-

**1**.Hardware vulnerability

**2**.Software vulnerability

WHY WE REQUIRE RECONNAISSANCE TOOL?

Reconnaissance is a critical phase in the adversary cycle. It's not uncommon for hackers to spend much more time on the pre-attack than on the actual attack. And wrong or incomplete reconnaissance can result in a massive failure for the attackers. The goal of reconnaissance is to identify as many potential attack vectors as possible. Data collected from reconnaissance may include: Security policies. Knowing an organization's security policies can help you find weaknesses in their system.

RECONNISSANCE TOOLS

FireCompass

Firecompass uses elaborate reconnaissance techniques same like the nation-state actors and the platform automatically discovers an organization’s dynamic digital attack surface, including unknown exposed databases, cloud buckets, code leaks, exposed credentials, risky cloud assets, and open ports & more.

Recon- NG

Recon-Ng is a web-based web reconnaissance tool written in Python. This tool is mainly applied by pen testers seeking web-based information. Recon-NG is preferred due to its intuitive functionalities making it fast and effective to gather a lot of data quickly.

Censys

Censys provides an avenue to gather data regarding all your assets to help you prevent target attacks. This tool provides actionable insights and helps you track changes in all your assets and identify potential vulnerabilities.

Shodan

Shodan is among the first search engines for internet-connected devices. With servers located all over the world, it provides real-time intelligence regarding attest technological trends. It also has APIs that other recon tools like Nmap, Metasploit, Maltego, and FOCA use for analysis.