Ruturaj Patil

LetsUpgrade, (Cyber security for beginners)

Day 2

Information gathering & Scanning

To collect as much information as possible. Collecting information and knowing deeply about the target system is known as “Reconnaissance”. This data is the main street for the hackers to hack the target system. It involves Footprinting, Enumeration, and Scanning.

Passive vs. Active reconnaissance

Passive reconnaissance	Active reconnaissance
1. Gathering information without actually connecting to the target.	1. Gathering information about the target while initiating connections.
2. Passive reconnaissance generally involves Open Source Intelligence (OSINT) investigation.	2. Active reconnaissance typically involves using of varity of tools like port and vulnerability scanners.
3. This allow not being detected while gathering information.	3. This allow you to gather more information but allow you to be detected.

Google Dorking – It is a hacking technique that uses Google Search and other Google applications to find security holes in the configuration and computer code that websites are using. Google dorking could also be used for OSINT.

Cheatsheet –

Filter	Description	Example
allintext	Searches for occurrences of all the keywords given.	`allintext:"keyword"`

Filter	Description	Example
intext	Searches for the occurrences of keywords all at once or one at a time.	`intext:"keyword"`
inurl	Searches for a URL matching one of the keywords.	`inurl:"keyword"`
allinurl	Searches for a URL matching all the keywords in the query.	`allinurl:"keyword"`
intitle	Searches for occurrences of keywords in title all or one.	`intitle:"keyword"`
allintitle	Searches for occurrences of keywords all at a time.	`allintitle:"keyword"`
site	Specifically searches that particular site and lists all the results for that site.	`site:"www.google.com"`
filetype	Searches for a particular filetype mentioned in the query.	`filetype:"pdf"`
link	Searches for external links to pages.	`link:"keyword"`
numrange	Used to locate specific numbers in your searches.	`numrange:321-325`
before/after	Used to search within a particular date range.	`filetype:pdf & (before:2000-01-01 after:2001-01-01)`
allinanchor (and also inanchor)	This shows sites which have the keyterms in links pointing to them, in order of the most links.	`inanchor:rat`

Filter	Description	Example
allinpostauthor (and also inpostauthor)	Exclusive to blog search, this one picks out blog posts that are written by specific individuals.	`allinpostauthor:"keyword"`
related	List web pages that are “similar” to a specified web page.	`related:www.google.com`
cache	Shows the version of the web page that Google has in its cache.	`cache:www.google.com`

Recon Techniques

ARP-SCAN

WHATWEB

SubLister

NMAP

- Nmap is probably one of the most important tools in the pentesting tool kit.
- It is a versatile port scanner that can be used to scan entire networks to discover what ports are open.
- Information that nmap can gather includes:
    - Operating system
    - Services running on device
    - Open/closed ports
    - Vulnerabilities on that device

Usage of Nmap –

TCP syn-awk scan

> nmap -sS [Network]

All port scan

> nmap -p- [IP_Adderss]

Enumerate versions

> nmap -sV [IP_Adderss]

Aggressive OS enumeration

> nmap -A -O [IP_Adderss]

Recommended

> nmap -sC -sV [IP_Adderss]

Nmap Scripting Engine (NSE)

> nmap --script=vuln [IP_Adderss]

Vulnerability Scanners:

1. Nikto
2. NessusNetsparker
3. Acunetix