Metadata Clues

1. ExifTool: A powerful tool for reading, writing, and editing metadata in image and document files.

Command Examples:

exiftool filename.jpg: Extracts all metadata from the specified image.

exiftool -Author -CreateDate document.pdf: Retrieves specific metadata fields (author and creation date) from a PDF.

2. pdfinfo: A utility to extract information from PDF files, including metadata.

Command Example:

pdfinfo file.pdf: Displays detailed metadata such as title, author, and number of pages.

Network Mapping

1. Nmap: A network scanning tool used to discover hosts and services on a network.

Command Examples:

nmap -A targetIP: Performs an aggressive scan, detecting OS, versions, and running services.

nmap --script vuln targetIP: Runs vulnerability scripts against the target to identify known vulnerabilities.

2. Maltego: A data mining tool for gathering information and visualizing relationships.

Usage: Create graphical representations of relationships between people, organizations, and online data, facilitating deeper insights into connections.

Global Surveillance and Device Mapping

1. Shodan: A search engine for internet-connected devices, providing visibility into vulnerabilities and exposures.

Command Examples:

shodan search "port:23 country:US": Searches for devices with open Telnet ports in the U.S.

shodan download query-name "vuln:CVE-2019-0708": Downloads data related to specific vulnerabilities.

2. Google Dorks: Advanced search queries that uncover hidden data on websites.

Command Examples:

site:gov filetype:xls: Searches for Excel files on government websites.

intitle:"index of" password: Looks for exposed directories containing password files.

3. Wireshark: A network protocol analyzer for capturing and inspecting packet data.

Command Examples:

wireshark -i eth0: Launches Wireshark to capture traffic on the specified network interface.

Filter Example: Use http.request to filter and display only HTTP requests in captured data.

Geotag Tracing and Physical Indicators

1. ExifTool: Also useful for extracting geolocation data from images.

Command Example:

exiftool -gpslatitude -gpslongitude filename.jpg: Extracts GPS coordinates from the image metadata.

2. Google Earth: A geospatial tool that allows users to view and analyze satellite imagery and maps.

Usage: Correlate images with geographic data to identify locations and features.

3. OpenStreetMap: A collaborative mapping project offering free geographic data.

Usage: Query for information related to infrastructure, utilities, and public assets.

Cross-Continent Operations & VM Management

1. SSH: A protocol for securely accessing remote servers and devices.

Command Examples:

ssh user@remote-IP: Connects to a remote server via SSH.

ssh -L local-port:remote-IP:remote-port user@remote-IP: Sets up a tunnel for forwarding ports securely.

2. Telnet: A network protocol for connecting to remote servers, useful for troubleshooting.

Command Example:

telnet remote-IP port: Connects to a specified remote IP and port.

3. Ansible: An automation tool for managing and configuring servers.

Command Example:

ansible-playbook -i hosts deploy.yml: Executes a playbook to configure multiple hosts defined in the inventory.

Advanced Reconnaissance

1. theHarvester: A tool for gathering email addresses, subdomains, and hostnames.

Command Example:

theharvester -d domain.com -b google: Searches Google for data related to a specific domain.

2. Sublist3r: A tool for enumerating subdomains of a target domain.

Command Example:

sublist3r -d example.com: Identifies and lists subdomains associated with the target domain.

3. Recon-ng: A web reconnaissance framework with various modules for data gathering.

Command Examples:

recon-ng: Starts the Recon-ng console.

modules load recon/domains-hosts/hackertarget: Loads a specific module for domain reconnaissance.

Social Engineering Techniques

1. Phishing: Techniques for creating deceptive emails to gather sensitive information.

Tools: Use Gophish or PhishMe for designing and launching phishing campaigns.

2. LinkedIn OSINT: Techniques for gathering professional data from LinkedIn.

Command Example:

theharvester -d linkedin.com -b bing: Scrapes LinkedIn for relevant profiles and information.

3. Facebook Intelligence: Utilize Facebook's search capabilities to gather data on individuals.

Usage: Analyze relationships and interactions to build profiles of targets.

4. Phone Pretexting: Techniques for impersonating trusted contacts via phone.

Tools: Use SpoofCard or Google Voice for creating fake caller IDs.

5. Social Media Cross-referencing: Identify and gather data across multiple social platforms.

Command Example:

python3 social-analyzer.py -username exampleuser -platforms all: Analyzes social media presence across various platforms.

6. Email Spoofing: Techniques to send deceptive emails that appear to come from a trusted source.

Command Example:

sendmail -t -f "trusted@sender.com" -u "Subject: Urgent": Sends an email with a spoofed sender address.

7. Creepy: A geolocation tool that analyzes social media and geolocation data.

Command Example:

creepy -i useraccount -o outputfile: Collects geolocation data from the specified user account.

8. OSINT Combine: A collection of tools for gathering and analyzing data from social media.

Usage: Leverage various tools offered in the OSINT Combine suite for comprehensive investigations.

---

This expanded list provides a more detailed overview of each tool and command, including their applications and contexts for use in OSINT and social engineering tasks.