Scanning (OSINT)

Georgios Bakirtzis

2024-09-18

Link Analysis Exercise:

1. Understand link analysis
   (a) Define link analysis and its purpose in information gathering
   (b) Discuss examples of first-degree and second-degree connections
2. Explore the WHOIS database
   (a) Open a terminal in Kali Linux
   (b) Use the command: `whois zoom.us`
   (c) Analyze the information returned, focusing on contact details
3. Investigate domain privacy
   (a) Research why some domains have private WHOIS information
   (b) Find out why .us domains are required to publish contact information
4. Compare WHOIS results
   (a) Look up WHOIS information for 3 different domains (.com, .org, .us)
   (b) Note differences in available information
5. Discuss ethical considerations
   (a) Consider the implications of publicly available contact information
   (b) Debate the balance between transparency and privacy
6. Create a simple link analysis diagram
   (a) Use the information gathered from WHOIS lookups
   (b) Map out potential connections between domain owners

Maltego Link Analysis Exercise:

1. Set up Maltego
   (a) Start your Kali Linux virtual machine
   (b) Search for Maltego in the Applications menu
   (c) Select Maltego CE (free version)
   (d) Follow the setup wizard, selecting defaults
2. Create an anonymous email (for Maltego registration)

   (a) Go to Protonmail.com and create an account
   (b) If Protonmail is blocked, use Opera browser with built-in VPN
   (c) Use this email to register for Maltego
3. Familiarize yourself with Maltego interface
   (a) Observe the empty canvas
   (b) Explore the various entity types available
4. Add a domain entity
   (a) Click "New Entity Type"
   (b) Search for and select "Domain"
   (c) Add the Domain entity to the canvas
5. Investigate maltego.com
   (a) Change the URL of the domain entity to maltego.com
   (b) Right-click the entity to explore available transforms
6. Apply transforms
   (a) Use transforms to discover related information (e.g., DNS servers, web servers)
   (b) Apply transforms that search public forums for usernames or email addresses
7. Analyze the results
   (a) Observe the connections Maltego discovers
   (b) Identify different types of information revealed (infrastructure, contact info, etc.)
8. Check for leaked credentials
   (a) Install the haveibeenpwned transform in Maltego
   (b) Run the transform on any email addresses discovered
   (c) Alternatively, manually check https://haveibeenpwned.com/
9. Discuss findings and implications
   (a) What kind of information was easily discoverable?
   (b) How might this information be used by hackers or security researchers?
   (c) Consider the ethical implications of using such tools and databases
   (d) Discuss the importance of unique passwords and regular password changes

Password Security Exercise:

1. Understand the risks of password leaks
   (a) Discuss the scale of major password leaks (e.g., 1.4 billion credentials)
   (b) Explore the potential consequences of leaked passwords
2. Check for compromised accounts (ethically)
   (a) Visit https://haveibeenpwned.com/
   (b) Check your own email addresses for potential breaches
   (c) Discuss the importance of this knowledge for personal security

3. Analyze password strength
    (a) Use an online password strength checker (e.g., https://howsecureismypassword.net/)
    (b) Test the strength of sample passwords (not real ones)
    (c) Discuss what makes a password strong or weak
4. Explore password managers
    (a) Research popular password manager options
    (b) Discuss the benefits and potential risks of using password managers
5. Implement multi-factor authentication (MFA)
    (a) Set up MFA on a test account or discuss the process
    (b) Explore different types of MFA (SMS, app-based, hardware keys)
6. Create a personal action plan
    (a) List steps to improve personal password security
    (b) Develop a strategy for managing passwords across multiple accounts
7. Discuss ethical implications
    (a) Explore the ethics of password cracking and using leaked databases
    (b) Debate the balance between security research and privacy

Google Dorking Awareness Exercise:

1. Understand Google Dorking
    (a) Define Google Dorking and its potential uses in cybersecurity
    (b) Discuss the ethical and legal implications (e.g., CFAA)
2. Explore Google search operators
    (a) Learn about operators like inurl:, filetype:, intext:, after:
    (b) Discuss how these can be used to refine searches
3. Analyze example queries (without executing them)
    (a) Examine the structure of queries like:
        - inurl:"live/cam.html"
        - "Pop-up" + "Live Image" inurl:index.html
        - filetype:log intext:password after:2019 intext:@gmail.com | @yahoo.com
    (b) Discuss what each part of the query is attempting to find
4. Discuss protective measures
    (a) Explore the use and limitations of robots.txt
    (b) Discuss the importance of proper authentication for sensitive pages
5. Create a security checklist
    (a) Develop a list of best practices to protect against Google Dorking
    (b) Include items like regular security audits, proper access controls, etc.

6. Role-play scenario
    (a) In pairs, have one student play a system administrator and another an ethical hacker
    (b) The "hacker" explains potential vulnerabilities, the "admin" proposes solutions
7. Discuss responsible disclosure
    (a) Learn about ethical ways to report vulnerabilities if discovered
    (b) Explore bug bounty programs and their role in cybersecurity

Internet Scanning Exercise:

1. Set up the environment
    (a) Ensure you're using a Kali Linux virtual machine
    (b) Open a terminal window
2. Download the exclusion list
    (a) Visit https://github.com/robertdavidgraham/masscan/blob/master/data/exclude.conf
    (b) Save the content to a file named 'exclude.txt' on your VM
3. Review the exclusion list
    (a) Open 'exclude.txt' in a text editor
    (b) Identify and note down some key excluded IP ranges (e.g., NASA, US Navy)
    (c) Observe the FBI honeypot IP ranges listed
4. Install Masscan (if not already installed)
    (a) Run: `sudo apt-get install masscan`
5. Prepare a limited scan command
    (a) Construct a Masscan command to scan a single port at 100,000 packets per second
    (b) Example: `sudo masscan 0.0.0.0/0 -p80 -rate=100000 -excludefile exclude.txt`
    (c) Note: Do NOT execute this command
6. Analyze the command
    (a) Explain what each part of the command does
    (b) Discuss why we use the exclusion list
    (c) Calculate how long this scan would take to complete
7. Discuss ethical implications
    (a) List potential legal issues with scanning the entire internet
    (b) Explain why certain IP ranges are excluded
    (c) Discuss the purpose of FBI honeypots
8. Create a report
    (a) Summarize what you've learned about internet-scale scanning
    (b) Explain the ethical considerations and best practices
    (c) Discuss alternatives to large-scale scanning for security research

Performing a Masscan Scan:

1. Prepare the configuration file
   (a) Open your preferred text editor
   (b) Add the following content:

```
rate = 100000.00
output-format = xml
output-status = all
output-filename = scan.xml
ports = 0-65535
range = 192.168.1.0-192.168.1.255
excludefile = exclude.txt
```

   (c) Save the file as 'scan.conf'
2. Understand the configuration
   (a) rate: number of packets to transmit per second
   (b) ports: range of ports to scan (0 to 65,535)
   (c) range: IP addresses to scan in your virtual environment
   (d) excludefile: specifies the exclusion list (important for public internet scans)
3. Run the scan
   (a) Open a terminal on your Kali Linux virtual machine
   (b) Execute the command: `sudo masscan -c scan.conf`
4. Observe the scan progress
   (a) Watch for the status screen, which should display:

```
Starting masscan (http://bit.ly/14GZzcT)
--forced options: -sS -Pn -n --randomize-hosts -v --send-eth
Initiating SYN Stealth Scan
Scanning 256 hosts [65536 ports/host]
rate: 13.39-kpps, 4.28% done, 0:20:56 remaining, found=0
```

5. View the results
   (a) After the scan completes, open 'scan.xml' in Mousepad or your preferred text editor
   (b) The file will contain a list of machines and open ports in XML format
   (c) Example of the output:

```
<?xml version="1.0"?>
<!-- masscan v1.0 scan -->
<?xml-stylesheet href="" type="text/xsl"?>
<nmaprun scanner="masscan" start="1606781854" version="1.0-BETA"
```

Reading Banner Information with Masscan:

1. Understand the purpose
   (a) Banner information can reveal application details, including versions
   (b) This can help identify vulnerable machines quickly
2. Prepare for banner scanning
   (a) Use the –source-ip option to avoid conflicts with the OS's TCP/IP stack
   (b) Choose a unique IP address on your network for this purpose
3. Run the banner scan
   (a) Open a terminal in your Kali Linux VM
   (b) Execute the following command: `sudo masscan 192.168.1.0/24 -p443 -banners -heartbleed -source-ip 192.168.1.200`
   (c) Understand the command components:
   - 192.168.1.0/24: IP range to scan (in CIDR notation)
   - -p443: Check port 443 (HTTPS)
   - –banners: Inspect the banner
   - –heartbleed: Check for Heartbleed vulnerability
   - –source-ip 192.168.1.200: Assign a unique network ID
4. Analyze the output
   (a) Look for open ports and banner information
   (b) Example output:

```
Discovered open port 443/tcp on 192.168.1.1
Banner on port 443/tcp on 192.168.1.1: [ssl] TLS/1.1 cipher:0xc014,
pfSense-5 f57a7f8465ea, pfSense-5f57a7f8465ea
Banner on port 443/tcp on 192.168.1.1: [vuln] SSL[heartbeat]
```

   (c) Identify potentially vulnerable machines (e.g., [vuln] SSL[heartbeat])
5. Additional steps for non-VM environments
   (a) If scanning over WiFi or outside the VM, block Masscan's port with a firewall
   (b) On Linux, use iptables: `iptables -A INPUT -p tcp -dport 3000 -j DROP`
   (c) This drops incoming TCP packets on port 3000
6. Further reading
   (a) Consult the Masscan documentation for more details: https://github.com/robertdavidgraham/masscan/

Setting Up Nessus Vulnerability Scanner:

1. Download Nessus
   (a) Open a browser on your Kali Linux virtual machine
   (b) Go to https://www.tenable.com/downloads/nessus/
   (c) Download the Nessus scanner for Debian
2. Install Nessus

(a) Open a terminal

(b) Navigate to the Downloads folder: `cd /Downloads`

(c) Install using dpkg: `sudo dpkg -i Nessus-<version number>-debian6_amd64.deb`

(d) Replace <version number> with the actual version you downloaded

3. Start Nessus service

(a) Enable Nessus: `sudo systemctl enable nessusd`

(b) Start Nessus: `sudo systemctl start nessusd`

4. Access Nessus web interface

(a) Open Firefox on Kali Linux

(b) Go to https://127.0.0.1:8834/

5. Handle security warning

(a) You will see a security warning due to self-signed certificate

(b) Click on "Advanced"

(c) Select "Accept the Risk and Continue"

6. Complete Nessus setup

(a) Follow on-screen instructions to create an account and set up Nessus

(b) Note: Nessus Home is free but limited to scanning 16 IP addresses

7. Prepare for scanning

(a) Ensure you have permission to scan the target systems

(b) Limit scans to your virtual lab environment

8. (Optional) Explore alternatives

(a) Consider open-source alternatives like OpenVAS

(b) Look into Metasploit's Nexpose scanning module

nmap Scanning Techniques:

1. HTTP Enumeration Scan

(a) Open a terminal in Kali Linux

(b) Execute: `sudo nmap -sV -p 80 -script http-enum <IP address of victim machine>`

(c) This scan enumerates files and folders on a website

2. Stealthy OS and Service Detection Scan

(a) Run: `sudo nmap -A -sV -D <decoy-IP-1,decoy-IP-2,MY-IP,decoy-IP-3...> <IP address of victim machine>`

(b) -A: Enables OS detection, version scanning, script scanning, and traceroute

(c) -D: Uses decoys to avoid firewall detection

3. Vulnerability Scanning

(a) Execute: `sudo nmap -sV -script vulners <IP address of victim machine>`

(b) This scan uses the vulners script to detect CVE vulnerabilities

4. View Available nmap Scripts
    (a) List all installed nmap scripts: `ls /usr/share/nmap/scripts/`
5. Comprehensive Port Scan with Default Scripts
    (a) Run: `nmap -sV -sC -p- -oN scanResults.nmap <IP address of victim machine>`
    (b) -sV: Probe open ports to determine service/version info
    (c) -sC: Use default nmap scripts
    (d) -p-: Scan all ports
    (e) -oN: Output results in normal format to scanResults.nmap file
6. Important Notes
    (a) Always ensure you have permission to scan the target system
    (b) Be aware that some scans may be detected by firewalls or intrusion detection systems
    (c) Interpret results carefully and verify findings to avoid false positives

Setting Up and Using Discover for OSINT and Vulnerability Scanning:

1. Install Discover
    (a) Open a terminal in Kali Linux
    (b) Clone the repository: `sudo git clone https://github.com/leebaird/discover /opt/discover/`
    (c) Navigate to the directory: `cd /opt/discover/`
    (d) Run the update script: `sudo ./update.sh`
    (e) Follow prompts to create a certificate (use dummy information)
2. Understand Discover's Capabilities
    (a) Passive scanning tools:
        - ARIN and Whois: Identifies IP addresses
        - dnsrecon: Collects OSINT from DNS servers
        - goofile: Searches domains for specific file types
        - theHarvester: Searches public sources for email addresses
        - Metasploit scanning tool: Performs Metasploit framework scans
        - URLCrazy: Checks for URL variations
        - Recon-ng: Web-based reconnaissance tools
    (b) Active scanning tools:
        - traceroute: Discovers routers along the path to a server
        - Whatweb: Probes websites to uncover technologies used
3. Run Discover
    (a) Navigate to the Discover directory: `cd /opt/discover/`
    (b) Execute Discover: `sudo ./discover.sh`
    (c) Follow the on-screen prompts to select scanning options
4. Analyze Results
    (a) After the scan completes, review the generated report

(b) The report will contain comprehensive information gathered from various tools

5. Important Considerations

   (a) Ensure you have permission to scan target systems/domains
   (b) Be aware that active scans may be detected by the target
   (c) Use the information gathered ethically and responsibly