MODULE 03 // TECHNICAL EXPLOITS

ENUMERATION & EXPLOITATION

Deep-dive technical methodology for information extraction and system penetration.

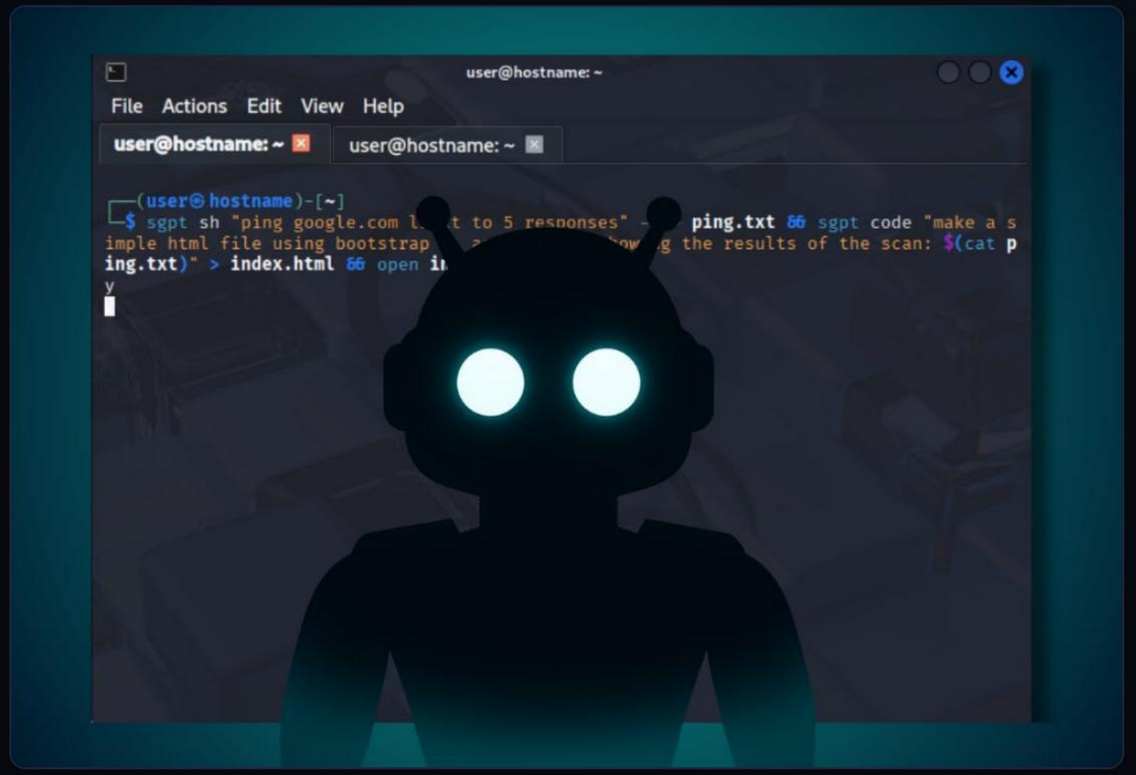
1. ENUMERATION
2. TOOLS & TECHS
3. EXPLOITATION
4. EVASION
5. PW CRACKERS
6. ROOTKITS
7. NET WORKS
8. SERVICES

Introduction to Enumeration

What is Enumeration?

Enumeration is the vital process of **extracting detailed information** from a target machine, establishing the bridge between silent reconnaissance and target attack.

- Converted strictly after initial reconnaissance stage.
- Unveils user accounts, privileges, services, and share paths.
- Directly supplies precise entry vectors for the exploitation stage.



Common Enumeration Techniques

Identity Map

User & Group: Mapping valid user profiles and permission tiers across directories.

```
$ enum4linux -U [IP]
```

Share & DNS

Network Shares: Disclosing exposed shared folders and query-able zone files.

```
$ host -t axfr [Domain]
```

Protocols

SNMP & LDAP: Parsing management tables, directory schemas, and system metadata.

```
$ snmpwalk -v1 -c public
```

Soft Objective vs. Attack Phase

Soft Objective

Perform precise data collection operations designed specifically to minimize active operational footprints.

- No system disruption
- No payload execution
- Minimize modifications

PASSIVE SCAN

Looking Around

Continuous observation of structural host behaviors to index exposed network nodes and ports.

- Inspect public headers
- Evaluate open gates
- Document stack versions

LOW VISIBILITY

Attack Phase

Deploy active exploits targeted at vetted vulnerabilities to establish localized control on systems.

- Exploit configuration bugs
- Gain host shell access
- Escalate user rights

ACTIVE INTRUSION

Elements of Enumeration

Crucial Target Elements

- **User Profiles:** Valid local names and domain identifiers.
- **Groups & Privileges:** Mapping admin and standard users.
- **Shared Resources:** Unsecured directory exports and shares.
- **Security Rules:** Configuration details of firewall gates.

Mapping the Attack Surface

By cataloging these core infrastructural items, testers construct a comprehensive network profile. Understanding security configurations helps prevent dead-end attack paths during penetration testing.

> *"Proper enumeration is the master blueprint that transforms random brute-forcing into precise ethical hacking."*

Transition to Exploitation

Target Mapping to Validation

Once enumeration delivers raw target files, the attack profile transitions to high-priority active exploits.

- Prioritize critical service configuration gaps.
- Select specific vulnerability exploit paths.
- Verify testing boundaries for target networks.

Exploitation & Intuitive Testing

Exploitation

Controlled attempts to execute verified system exploits, proving structural vulnerabilities exist while demonstrating the actual business threat level of target infrastructure weaknesses.

Intuitive Testing

Leveraging expertise over strict scripts. Testers adapt dynamically, finding complex, logical configuration gaps and unexpected application pathways automated scanners regularly miss.

Evasion & Group Analysis

Evasion Methodologies

Testing a system's resilience by bypassing standard defensive monitors (IDS/IPS/SIEM). These exercises assess whether local administrators can detect deep system alterations.

```
[Evasion Objective] Verify intrusion alerting triggers and event logging pipelines.
```

Mapping Rights & Groups

By examining membership databases, security analysts search for weak permission links that facilitate horizontal moves and administrative privilege escalation.

- Exploit weak service accounts.
- Pivot through multi-domain links.

Operating Systems & Post-Exploit

Operating Systems

Custom exploit strategies targeted directly for distinct target kernels:

- Windows (AD/GPO)
- Linux (SUDO/Kernel)
- macOS & Unix platforms

Password Crackers

Testing authentication configurations by reviewing hash safety against dictionary, brute force, and hybrid methods.

- Hashcat / John the Ripper

Rootkits

Testing host integrity by assessing how software can maintain unauthorized admin persistence while hiding active system processes.

- User-space vs. Kernel

Vulnerable Surface Areas

Attack Domain	Critical Infrastructure Elements	Primary Areas of Concern
Applications	Web applications, enterprise software, custom database backends	Injection vulnerabilities, flawed authorization, legacy endpoints
Networks	Routing protocols, firewalls, switches, network architecture	Unencrypted management paths, open gateways, flat structures
Services	DNS zones, DHCP scopes, FTP servers, default email gateways	Default authentication, unpatched vulnerabilities, misconfigurations

Image Sources

http://googleusercontent.com/image_collection/image_retrieval/4989934763584170823_0

Primary Source: Cybersecurity Server Scanning Illustration / Command Line Concept

---

http://googleusercontent.com/image_collection/image_retrieval/8442597539625283401_0

Secondary Source: Glitch Security Lock Concept / Cyber Attack Vector

Image Sources

https://substackcdn.com/image/fetch/$s_!hbTF!,f_auto,q_auto:good,fl_progressive:steep/https%3A%2F%2Fsubstack-post-media.s3.amazonaws.com%2Fpublic%2Fimages%2Feeec1517-aa18-451f-bfab-5e23d95956e5_1000x700.png

Source: darkmarc.substack.com

https://elements-resized.envatousercontent.com/elements-video-cover-images/d400448b-51c8-4c59-b0df-ab6b63c9f431/video_preview/video_preview_0000.jpg?w=500&cf_fit=cover&q=85&format=auto&s=41340c559a3d46e8051ab0ea78b10cfd255edd0471d2eeaa31ee71426bf8952e

Source: elements.envato.com