Tools POC

🛠 Tool Name: wget

History

Developed by the GNU Project, wget has been a staple command-line utility for retrieving files using HTTP, HTTPS, and FTP protocols.

📄 Description:

A non-interactive network downloader for downloading files from the web via terminal.

📌 What Is This Tool About?

wget is primarily used to fetch files and mirror websites through command-line-based operations.

⭐ Key Characteristics / Features:

- Supports HTTP, HTTPS, and FTP
- Recursive downloading
- Download resumption
- Timestamping
- Proxy support
- IPv6 support
- Portable and scriptable

🔧 Types / Modules Available:

- Recursive fetcher
- Timestamp handler
- FTP/HTTP/HTTPS modules
- Logging and reporting module

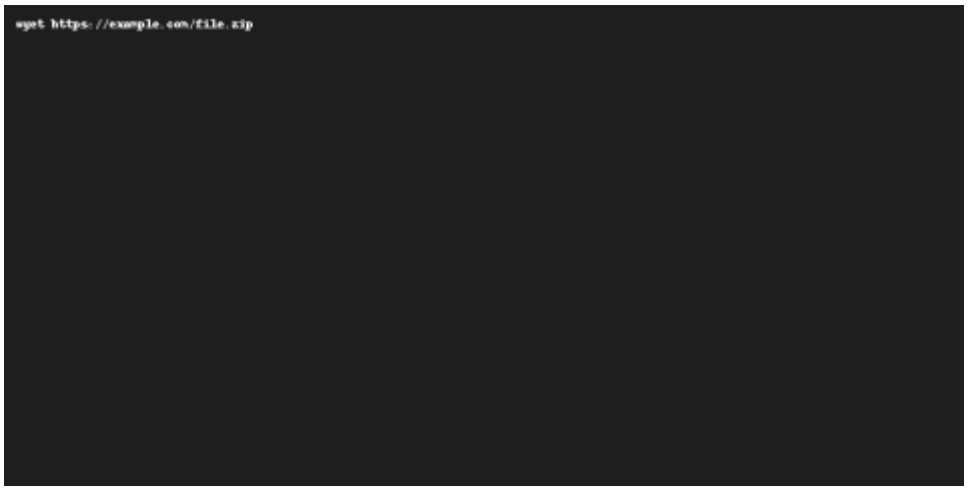
🎯 How Will This Tool Help?

- Download entire websites for offline use
- Retrieve single or multiple files remotely

• Scripted downloading in automation

• Good for data acquisition from URLs

🖼 Proof of Concept (PoC) Images:



15-Liner Summary:

• Cross-platform tool

• Supports recursion and mirroring

• Ideal for automation

• Lightweight utility

• Supports both CLI and scripting

• Handles file resumption

• Includes logging support

• Compatible with cron jobs

• Fast and efficient

• Minimal dependencies

• Supports proxies

• Download rate control

• Free and open-source

• Easy integration in scripts

• Regularly updated

⏱️ Time to Use / Best Case Scenarios:

• Automated downloading in investigation

• Collecting data from malicious URLs

• Mirroring threat actor websites

🛥️ When to Use During Investigation:

• During data acquisition

• Initial stage of incident response

• During OSINT investigation

🕵️ Best Person to Use This Tool & Required Skills:

Best User: Cybersecurity Analyst / Threat Hunter

Required Skills:

• Command-line proficiency

• Understanding of protocols

• Bash/Python scripting knowledge

🩹 Flaws / Suggestions to Improve:

• No GUI available

• Limited support for JavaScript-heavy pages

• Complex syntax for deep recursion

☑ Good About the Tool:

• Highly scriptable

• Reliable for batch downloading

• Widely documented

🛠 Tool Name: ssh

History

Introduced as a secure replacement to Telnet in the 1990s, SSH (Secure Shell) enables encrypted remote access over insecure networks.

📄 Description:

SSH is a cryptographic protocol and tool that allows secure remote login and command execution over a network.

📌 What Is This Tool About?

It provides encrypted communication, secure file transfer, and port forwarding features widely used in system administration and digital forensics.

★ Key Characteristics / Features:

• End-to-end encryption

• Remote terminal access

• Supports SCP, SFTP

• Key-based authentication

• Port forwarding/tunneling

• Command execution logging

🔧 Types / Modules Available:

• SCP module

• SFTP module

• Remote shell module

• Key authentication handler

🎯 How Will This Tool Help?

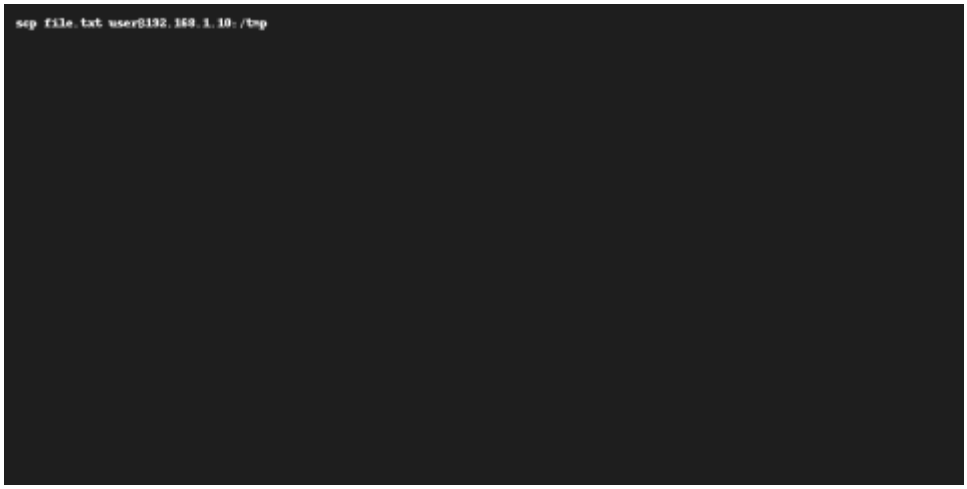
• Securely connect to remote machines

• Transfer forensic evidence securely

• Tunneling traffic during analysis

• Remote live forensics

🖼 Proof of Concept (PoC) Images:



📄 15-Liner Summary:

• Secure access to systems

• Supports port forwarding

• Used in network pivoting

• Integrates with forensic suites

• Automates secure transfers

• CLI based lightweight utility

- Multiplatform tool
- Auditing capabilities
- Logging enabled
- Supports certificate auth
- Open source and robust
- Integration with bash/python
- Used in SOC environments
- Helpful in remote triage
- Flexible authentication methods

⏱️ Time to Use / Best Case Scenarios:

- Remote triage of compromised system
- Live forensics from remote systems
- Transferring memory dumps securely

🧍 When to Use During Investigation:

- During incident response
- Initial system access
- Remote artifact collection

👨‍💻 Best Person to Use This Tool & Required Skills:

Best User: Incident Responder / Forensic Examiner

Required Skills:

- Knowledge of SSH protocol
- Linux command-line skills
- Basic network security awareness

🔗 Flaws / Suggestions to Improve:

- Brute-force attacks on weak credentials
- No native GUI
- Can be blocked by firewalls

☑ Good About the Tool:

- Highly secure connection
- Widely supported and documented
- Used in nearly all IR scenarios