What are SOCKS proxies and proxychains?

A SOCKS proxy is a general-purpose proxy that forwards any TCP (and with SOCKS5, UDP) connection to a destination, commonly set up through a compromised pivot so the attacker's tools can reach the internal network. proxychains is a utility that forces a program's connections through that proxy, even tools with no built-in proxy support. Together they turn a single pivot (for example an `ssh -D` dynamic forward) into access to the whole internal subnet for any tool.

HOW IT WORKS

01 How they work and payload

The attacker opens a SOCKS proxy via the pivot, then runs tools through proxychains:

- Open a SOCKS proxy (dynamic SSH forward): `ssh -D 1080 user@PIVOT`
- Point proxychains at it (in `/etc/proxychains.conf`): `socks5 127.0.0.1 1080`
- Run any tool through it: `proxychains nmap -sT -Pn 10.10.0.0/24` or `proxychains smbclient //10.10.0.20/share`

Now the attacker's whole toolkit reaches the internal network through one foothold. Documented techniques shown for defenders.

> ONE PROXY, EVERY TOOL
>
> *A SOCKS proxy plus proxychains means the attacker does not forward ports one at a time, they route their entire toolkit through the pivot. That is why a single foothold can be so powerful.*

HOW TO DEFEND

- Segment the internal network so the pivot can reach little, which limits what any proxy exposes.
- Restrict egress so a compromised host cannot establish the outbound proxy connection.
- Monitor for SOCKS proxy patterns and for one internal host suddenly scanning or connecting to many others.
- Limit tooling and SSH on exposed servers.
- Detect the noisy scanning that often follows a new SOCKS pivot.

SOURCES

[1] MITRE ATT&CK: Lateral Movement (TA0008)

[2] NIST SP 800-115 Technical Guide to Security Testing

[3] Linux man-pages: ssh(1)

Find the lateral-movement paths before an attacker does.

securelayer7.net/learn/lateral-movement/what-is-socks-proxies-proxychains

Open online