PWNDEFEND

Internal Network Attack Flow

We are inside a network, we have a foothold in a network adjacent position with a device we control. We might not have credentials. Here is a flowchart to help think about enumeration and attack paths. It's not means to be a step by step guide. Use at own risk. Ensure you have permission before conducting offensive security operations.

This is NOT an ABC guide or flow, the process is iterative and not all steps are required subject to context and objective.

Attacker Resources

Management	Operators	Researchers
Guides	Tools	Document Management
Payloads	C2	Exfil Services

Flow nodes

START → Situation Awareness → Find DNS

Situation Awareness branch:
- What are the goals?
- What are the objectives?
- What are the ROEs?
- What are the constraints?
- What are the timescales?

OSINT/RECON/HUMINT → START

Egress / network discovery (bottom-up):
- Understand Egress
- Look for web content filtering
- Look for protective DNS
- Check egress DNS
- Find proxies
- Find Routes to the internet

IP configuration chain:
- Get Ip configuration
- Look on the wire (wireshark/tcpdump)
- Look for DHCP
- Look for routing paths
- Look for Public DNS Resolvers etc.
- Look for domain name (assigned via DHCP)

Find DNS:
- Find domain controllers
- Find Computers

Find Active Directory → Gain Access → Enumerate → Post Access → Maintain Access

Enumerate Security:
- AV
- EDR
- Logging
- Canaries
- IPS/IDS
- DLP

Gain Access:
- Null BIND
- Stolen Creds
- PTH
- SMB RELAY
- Compromised Computer/User
- MITM/MITMv6
- Brute Force Auth

Enumerate:
- Find Computers
- Find Users
- Find Groups
- Find Shares
- Find Contacts/Email Addresses
- Find Printers
- Find Forest/Trusts
- Find GPOS
- Find scripts in SYSVOL
- Find Backup Services
- Find RAS/VPN Services
- Find supply chain info
- Find LAPS
- Find the MSPs
- Find the security team
- Find the SOC
- Find database servers
- Find web services

Middle column:
- File Servers/DFS Roots
- Print Servers
- Document Management
- LOB Systems
- Management Systems
- Security Systems
- Exchange Servers
- PKI (ADCS) Servers
- Identity Systems e.g. AD Connect
- Network Management
- Cloud Services
- Find other networks e.g. Operational Technology Networks
- Physical Security Systems → CCTV → Door Access Control → Alarms
- HVAC Systems
- Find SharePoint (don't be Snowden!)

Post Access:
- Dump Info
- Run Audit Tools
- Assess Security Defences
- Dump Creds
- Dump Configurations
- Replicate Domain
- Enumerate Access Privs
- Are we high priv? (decision)
- Do we need to be? (decision)
  - Yes
  - Privesc or Move Laterally

Maintain Access:
- Implant
- Backdoor Auth
- Golden Ticket
- Sneaky User Access
- Sneaky Admin Access

Lower left workgroup branch:
Find workgroup servers, PCs and network equipment → Gain Access → Post Access

- ARP
- ICMP
- DNS
- Port Scans
- Fingerprinting
- Ethernet Analysis
- SNMP
- Find Management Interfaces
- Find User Interfaces

Gain Access (lower):
- NULL BIND
- Attack Auth
- Phish and Steal SMB hashes
- Brute Force
- Find Open Shares
- Find Creds Elsewhere
- Known Exploit (RCE/Information Disclosure etc.)
- Supply Chain Compromise

Post Access (lower):
- Enumerate Security Defences
- Dump Info
- Dump Configurations
- Enumerate Access Privs

Exfiltrate Data → Affect Target → Cover Tracks → Disapear → END

Exfiltrate Data:
- Direct Service Connect
- DNS Exfil
- Cloud Service
- Abuse Target DMZ/Web Hosting
- ICMP Exfil
- Abuse legitimate service
- Email Exfil
- SMTP
- FTP Push
- FTP Pull
- SMB Push
- SMB Pull

Affect Target:
- Do nothing but steal data/spy
- Damage Integrity
- Destroy Backups
- Destroy Data
- Deny availability
- Weaken Defences
- Subvert Operator View
- Business Logic Tampering

Cover Tracks:
- Remove footprints
- Frame someone
- Disappear in the noise
- Disable logging capabilities