Playbook Intra-Network Execution Process

Initial setup and passive listening

Passive network sniffing

```
clw dumpcap -i eth0 -a duration:300
```

Wait for switch port to enter forwarding state

```
clw dumpcap -i eth0 -a duration:90
```

Target Files (ROE excluded)

```
psql -d site -A -t -c
  "SELECT DISTINCT ip_net FROM playbook_roe_ip_nets
    WHERE (NOT in_scope) AND (4 = family(ip_net))
    ORDER BY ip_net" >> ~/.clw/ROE-Excluded-IPV4-${UUID}
```

Phase 1

Initial Host Discovery

```
clw ping -4 -n -I eth0 -L -c 4 -b 1.2.3.255
clw ping -4 -n -I eth0 -L -c 4 -b 255.255.255.255
```

Host Discovery and IP Protocol Scans

```
clw nmap   -n -e eth0 -sn -PR -T4 --script '(ip-forwarding)'
  --excludefile ~/.netmeld/playbook/ROE-Excluded-IPv4-${UUID}
  1.2.3.0/24

clw nmap   -n -e eth0 -sO -PR -T4
  --excludefile ~/.netmeld/playbook/ROE-Excluded-IPv4-${UUID}
  1.2.3.0/24
```

Phase 2

Target Files (Responding Hosts)

```
psql -d site -A -t -c
  "SELECT DISTINCT ia.ip_addr FROM raw_ip_addrs AS ia
   JOIN tool_runs AS tr
     ON (ia.tool_run_id = tr.id)
   JOIN playbook_roe_ip_nets AS roe
     ON (ia.ip_addr <<= roe.ip_net)
   WHERE (ia.is_responding)
     AND (4 = family(ia.ip_addr))
     AND (roe.in_scope)
     AND (ia.ip_addr <<= '1.2.3.0/24')
   ORDER BY ia.ip_addr"
  >> ~/.netmeld/playbook/Responding-Hosts-IPv4-${UUID}
```

Port Scans (plus basic info gathering)

```
clw nmap   -n -e eth0 -sS -PR -T4 -O
  --script '(banner or dns-nsid or ntp-info or rpcinfo or ssh-hostkey
     or ssh2-enum-algos or ssl-cert or smtp-commands
     or smb-os-discovery or smbv2-enabled or vnc-info)'
  -p `nmdb-export-port-list --tcp-all`
  -iL ~/.netmeld/playbook/Responding-Hosts-IPv4-${UUID}
  --excludefile ~/.netmeld/playbook/ROE-Excluded-IPv4-${UUID}

clw nmap   -n -e eth0 -sU -PR -T4 -O
  --script '(banner or dns-nsid or ntp-info or rpcinfo or ssh-hostkey
     or ssh2-enum-algos or ssl-cert or smtp-commands
     or smb-os-discovery or smbv2-enabled or vnc-info)'
  -p `nmdb-export-port-list --udp`
  -iL ~/.netmeld/playbook/Responding-Hosts-IPv4-${UUID}
  --excludefile ~/.netmeld/playbook/ROE-Excluded-IPv4-${UUID}
```

Service Scans (most scripts enabled)

```
clw nmap   -n -e eth0 -sS -PR -T4 -A
  --script '((default or discovery) and not (external or brute or dos))'
  -p `nmdb-export-port-list --tcp-all`
  -iL ~/.netmeld/playbook/Responding-Hosts-IPv4-${UUID}
  --excludefile ~/.netmeld/playbook/ROE-Excluded-IPv4-${UUID}
```

Phase 3

Manual testing or script

Tear down

Deconfigure interface

```
Assume:
  psql site -c "insert into playbook_roe_ip_nets values ('1.2.3.0/24', true)"
  nmdb-playbook-insert-source --intra-network --interface eth0 --ip-addr 1.2.3.4/24 --stage 1
Execution:
  nmdb-playbook --intra-network --execute
```