

15 FEB

FIRST PHASE OF HACKING

Footprinting

→ Intel gathering

Phases

P1 Reconnaissance (Footprinting)

P2 Scanning

P3 Gaining access

P4 Maintaining access

P5 Covering tracks

Information gathering

- Domain Name
- Network service
- Contact Info
- Access control

Common Tools For Footprinting

- Domain Name Lookup
- Whois
- Social Engineering
- Info Leak
- Social media Invest

DNS Info

- A
- SOA (STATE OF AUTHORITY)
- CNAME (CANONICAL NAME)
- MX Mail EXCHANGE
- SRV (Service)
- PTR (Pointer)
- NS (Name Server)