Internal Network Reconnaissance

Internal Network Reconnaissance is where an attacker enumerates information about a target environment before completing their later objectives in the attack such as elevating their privileges or stealing sensitive information.

Do not underestimate the value of technical information describing your environment and the business information describing your organisation to your attacker.

Target information (examples)

- **Targeted environment information**
  - File shares
  - Domain controllers
  - Network diagrams
  - User directories
  - Proxy settings

- **Targeted user information**
  - Logged-in users
  - Admin account lists
  - Password hashes

- **Targeted system information**
  - Running applications and services
  - System configuration
  - Anti-virus vendors

Objectives

- Identify key environment information
- Download of additional tools to collect environment information
- Elevate privileges to collect environment information
- Lateral movement
- Stage environment for exfiltration

Priority controls

- Log analysis
  - Collection and analysis of system and network logs for security events
- Incident Response
  - People, process and technology to manage and respond to attacks
- Network monitoring
  - Collection of network and endpoint data to identify malicious activity
- Account monitoring
  - Detection of attempts to impersonate legitimate users through inactive user accounts

Ideal controls

- Software inventory
  - A list of known and approved software within the organisation
- Behavioural analysis
  - The identification of suspicious patterns of behaviour from network traffic and endpoint activity
- Network segregation
  - Segregating sensitive data and systems to make them more difficult to access
- Threat intelligence
  - Collection, analysis and sharing of attacker data to determine the threat to your environment
- Privileged user management
  - Control and lockdown on accounts with high privileges and administration rights
1. Have we identified information that an attacker would target, in order to improve their understanding of our infrastructure(s) and data we possess, to progress an attack post initial-compromise?

2. Do we have effective measures in place to protect this information from an attacker who has already breached our perimeter and is inside our network?

3. What measures do we have in place to impede the progress of an attacker and make them more visible to enable detection of their activities?

4. Do we have plans and capabilities to react and stop an attacker who has already breached our perimeter and is searching around inside our network – can we stop them before they complete objectives (e.g. disrupt operations or steal information)?

5. What are we doing to enhance our existing measures to detect, impede and stop an attacker inside our IT infrastructure?