Firewall Enumeration, Data Component DC0044

Archived: 2026-04-05 16:58:14 UTC

Querying and extracting a list of available firewalls or their associated configurations and rules. This activity can occur across host systems and cloud control planes, providing insight into the state and configuration of firewalls that protect the environment. Examples:

- Querying Host-Based Firewalls: Using Windows PowerShell commands like `Get-NetFirewallRule` or Linux commands such as `iptables -L` or `firewalld --list-all`.
- Cloud Firewall Rule Listing: Running commands like `az network firewall list` for Azure or `aws ec2 describe-security-groups` for AWS.
- Using Management APIs: Leveraging APIs like Google Cloud Firewall's `list` API method or AWS's DescribeSecurityGroups API.
  Identifying Misconfigurations: Extracting firewall rules to identify "allow all" policies or rules that lack logging.
- Enumerating with CLI Tools: Using CLI commands like `gcloud compute firewall-rules list` to extract firewall settings in Google Cloud.

Source: https://attack.mitre.org/datacomponents/DC0044