Examining NTP and NFS Enumeration

Dale Meredith
MCT | CEI | CEH | MCSA | MCSE
Cyber Security Expert

dalemeredith.com | Twitter: @dalemeredith | Linkedin: dalemeredith

Network Time Protocol

(NTP)

If you're lost, you can look and find me. Time after time.

Cyndi Lauper

Network Time Protocol (NTP)

Protocol that synchronizes time on all networked systems

Extremely important to directory services

Universal Time Coordinated (UTC)

Default NTP server in Windows will be the DC flagged as the PDC Emulator

Behind NTP

Ports

UDP 123

Extremely accurate

Private Networks / 200µs

Public Networks / 10ms

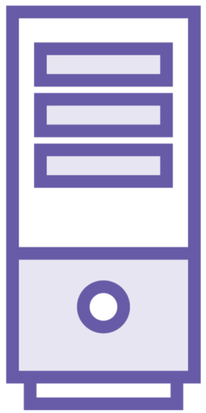
What Can We Learn from NTP?

Compile a list of hosts

Gather IP addresses

Identify system names

Collect displayed operating systems



NFS Enumeration

Network File System (NFS)

A networking protocol for distributed file sharing that is used to serve and share files on a network.

Network Attached Storage (NAS)

A device that allows users to access files through a network by using NFS protocols

Advantages

Disadvantages

NFS Enumeration

- Nmap
- Showmount -3 <ip address>
- SuperEnum
- PRCScan

- /etc/exports
- NFS servers allow or deny access based on credentials
- Port 2049
- Directories, clients and IP addresses

Network-based intrusion detection system (NIDS)

Detects malicious traffic on a network

Learning Check

Learning Check

- Port 123
- Port 2049
- showmount
- NAS

Up Next: Exploring SMTP Enumeration