

Discovering Enumeration Countermeasures



Dale Meredith

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

dalemeredith.com | Twitter: @dalemeredith | LinkedIn: dalemeredith





Launch countermeasures.

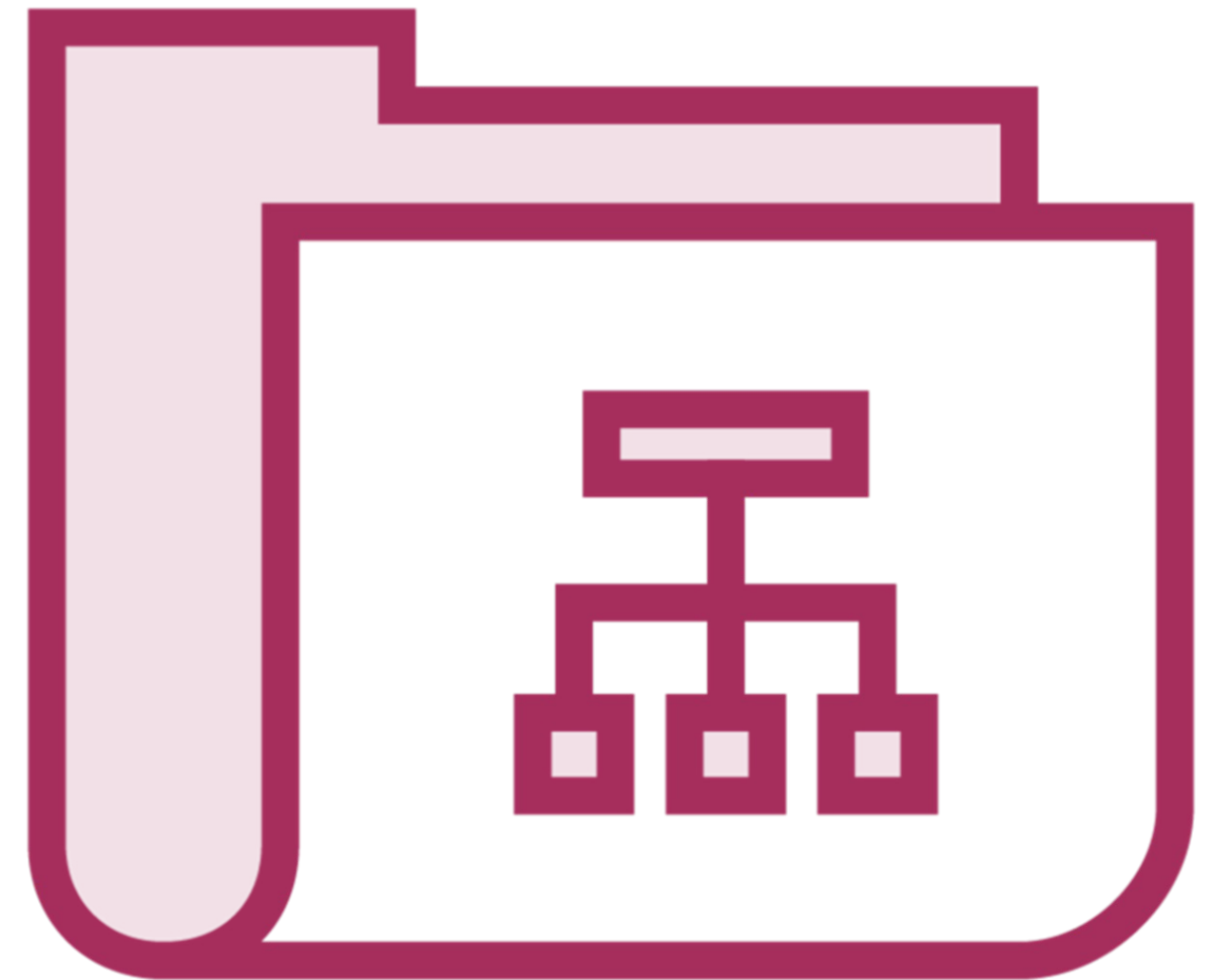
Capt. Marko Ramius





Defaults & NetBIOS

Change it
Be aware of your ports
Turn off SMB



Countermeasures for SNMP



Turn it off

Upgrade to v3

Group policy: “additional restrictions for anonymous connections”



Countermeasures for SNMP



Turn it off

Upgrade to v3

Group policy: “additional restrictions for anonymous connections”

Block ports 161 on TCP/UDP

IPSec filtering

Limit access to null sessions

Countermeasures for LDAP

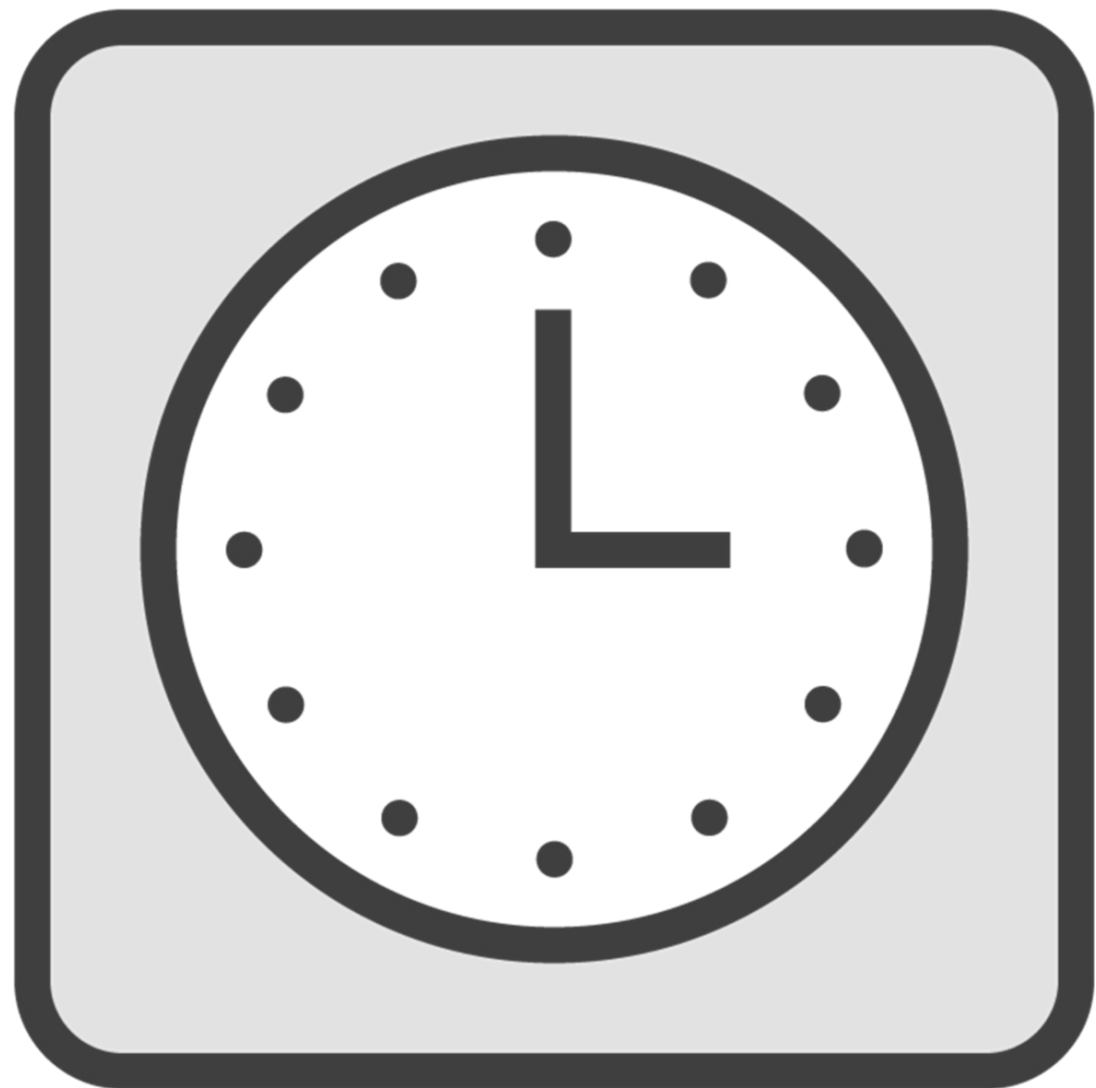
Separate email address and logon names

Use SSL to encrypt LDAP

Encrypt drives that store LDAP databases



Countermeasures for NTP



Watch your ports

Understand what software is installed

Check your master NTP

Countermeasures for SMTP



Disable open relays

Drop unknown recipients

Never include email server info in your email or posts

Countermeasures for DNS

Configure DNS Zone Transfer to explicit servers

Ensure that nonpublic hostnames are not referenced to IP within the DNS zone files or publicly accessible DNS servers

Check both internal and external DNS servers

Ensure that HINFO and other records do not appear in DNS zone files



Learning Check

Learning Check



Port 161



Change it!



HINFO



Use SSL



Ethical Hacking Series

