Introdução: Hashes em Windows

~~~~~~

Arquivos

~~~~~~

SAM -Security Account Manager (Windows)

- Armazena as contas dos usuários
- %SystemRoot%/system32/config/sam ← BLOQUEADO EM EXECUÇÃO

NTDS.DIT (Windows Server / Active Directory)

- Armazena dados do AD incluindo as contas de usuários
- %SystemRoot%/ntds/ntds.dit ← BLOQUEADO EM EXECUÇÃO

SYSTEM ← BLOQUEADO EM EXECUÇÃO

- Arquivo do sistema necessário para decriptar o SAM/NTDS.DIT
- %SystemRoot%/system32/config/system

~~~~~~

Soluções

~~~~~~

LOCALMENTE

- Acesso físico ao computador? Realizar boot com live cd e capturar os arquivos

REMOTAMENTE

- C:\Windows\repair (apenas sistemas antigos como XP/2003)
- Salvar direto do registro do windows (Desde versões antigas a versões recentes) ←

Ex: reg save hklm |sam

- Cópia sombra do volume (Versões mais recentes) ←

Ex: vssadmin

~~~~~~

Ataques

~~~~~~

- Obter os arquivos e usá-los para obter os hashes
- Tentar descobrir os hashes obtidos

OUTRAS TÉCNICAS

- Senhas em memória/cache - Utilizar técnicas para obter senhas em cache
ou na memória do Sistema.
- Pass The Hash - Técnica para utilizar um hash sem precisar quebrá-lo
- Captura de hashes na rede

Exemplo de Hashes no Windows

Usuário – ID – LM (LAN MANAGER) - NTLM (NT LAN MANAGER)

Administrador:500:aad3b435b51404eeaad3b435b51404ee:ae4b9891ebd7e330df8bbfe37d5e5e08:::

Convidado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

HelpAssistant:1000:53400e6be3b44a71ae7c89da5d20c6e3:389b28049ba082c4a57c336976f3f520:::

rafaela:1005:aad3b435b51404eeaad3b435b51404ee:ee8ba375ac2b804683ab960dad19581e:::

aad3b435b51404eeaad3b435b51404ee == vazio (significa que não está usando LM)