SMB Weakness

The attackers take advantage of a number of different Server Message Block (SMB) issues that can be used for post-exploitation. From SMB Signing disabled to using SMBv1.

DETECTION

User and Entity Behavior Analytics
SIEM Log Analysis
Firewall Log Review

TOOLS

NTLMRelayX
CrackMapExec
Responder
Inveigh

https://github.com/Kevin-Robertson/Inveigh

https://www.blackhillsinfosec.com/an-smb-relay-race-how-to-exploit-llmnr-and-smb-message-signing-for-fun-and-profit

https://www.blackhillsinfosec.com/webcast-group-policies-that-kill-kill-chains

EXPV1_0421

Backdoors & Breaches™

PIVOT and ESCALATE

Created by: BLACK HILLS | Information Security