Kerberoasting/ASREPRoasting

The attackers use a "feature" of service principal names (SPNs) to extract and crack service passwords.

DETECTION

SIEM Log Analysis
User and Entity Behavior Analytics
Cyber Deception

TOOLS

GhostPack:
- Rubeus

Impacket:
- GetNPUsers.py
- GetUserSPNs.py

Hashcat for Cracking

HASHCAT

https://github.com/GhostPack

https://github.com/SecureAuthCorp/impacket

https://github.com/hashcat/hashcat

https://www.blackhillsinfosec.com/running-hashcat-on-ubuntu-18-04-server-with-1080ti

Backdoors™ & Breaches

PIVOT and ESCALATE

Created by: BLACK HILLS | Information Security