Gaining Privileged Access on Windows Networks

Benjamin Rasper
Kevin Bong
About Sikich Security & Compliance

› A full-service information security and compliance consulting practice within Sikich
  › Audits and assessments
  › Penetration testing
  › Forensics
› Handle anything having to do with security or protecting data, including:
  › Credit card data (PCI DSS)
  › Patient data (HIPAA/HITECH)
  › Financial Information (FFIEC/GLBA)
  › Service provider reviews (SOC 1/2/3)
  › Federal information security standards (NIST/FISMA)
The Setup

› Assume we’ve gained a foothold into an internal network
  › Perhaps through a VPN, malware command-and-control (C&C) channels, a wireless connection or physical intrusion
› Assume patches are up to date and anti-virus is running
› We’ll demonstrate six common ways we gain or elevate domain access
› We’ll display a recap slide at the end of the presentation and give you time to snap a picture

Diagram:
- Domain Controller
- Domain Member Workstation
- Pentest Workstation
Time to put on your hoodie and start hacking...
Questions?

Benjamin Rasper
benjamin.rasper@sikich.com

Kevin Bong
kevin.bong@sikich.com

877.403.5227
Recap

- All demos used the Kali Linux distribution
- Used Responder to spoof Link-Local Multicast Name Resolution (LLMNR) responses, and then Hashcat to crack those hashes
- Used nmap to find systems running Server Message Block (SMB), and then enum4linux to find systems with null SMB sessions and extract accessible data
- Used Medusa to perform password spraying
- Used Metasploit’s:
  - smb_share_enum module to find accessible files on file shares
  - Kiwi module to extract cached passwords from Local Security Authority Subsystem Service (LSASS)
  - hashdump module to extract local password hashes