[Spiegazione attacchi]

Null session

1)il Null session è un attacco che serve per recuperare dati su target macchine, tipo password,utenti di sis
tema,gruppi,processi,e programmi aperti.
2) i sistemi vulnerabili sono tutti quelli senza credenziali e legacy
3)sono quasi estinti questi sistmei essendo storica la vulnerabilità
4)per risolverlo basta disabilitare smbv1 con powershell,abilitare: l'accesso anonimo ristrtto non aabilitare
enumerazione di anonimi e share
disabilitare: tutti possono diventare anonimi,dare anonymous sid NAME accesso ristretto a null session re
gistry
5)la smbv1 e il file all'interno che permette di controllare tutto e gli accessi anonimi sono quello che da lib
ertà all'hacker di entrare e fare quello che vole ovvero chinque

Arp Poisoning

1)Arp Poisoning è un attacco che usa Lan e manda pacchetti sulla lan sul getway in modo da cambiare IP
al Mac address table
2)Tutte le reti e gli utenti che hanno IP e sono su switch
3)per torvarlo si puo usare wireshark o semplicemente il prompt comandi
4) trovandolo e togliendo Arp il beneficio è che non si rubano file e non si confondono ip adress di altri ute
nti quindi un grnade vantaggio per l'azienda