Priviledge Escalation

Nic Maurel

Escalation

- -- are generally less protections inside a server
- -- can use local resources to crack passwords and brute force
- -- certain exploits are local only (packetstorm)
- -- better chance of finding "lazy" errors - bad permissions, etc
- -- traffic sniffing
- -- session sniffing
- -- code injection into running processes

Backdoor

- -- phone home
- -- shell shovelling
- -- php shells
- -- non-standard port
- -- trojaned binaries
- -- setting up certificates
- -- rootkit

Clean up

- -- wiping logs
- -- watching for checksum checks
- -- watch resource use
- -- no give away process names
- -- hidden files/folders/processes

bouncing

- -- can I get to other systems on the box?
- -- can I get to other machines on the same network?
- -- can I get to any other machines the company has?
- -- how can I exploit trust relationships

Prize Gathering

- --what was I tasked to get?
- -- certain data
- -- certain file
- -- certain password
- -- certain email

Corporate vs Criminal

- -- understand difference between something which is against corporate policy and something against criminal law
- -- understand responsibilties

Reporting

- -- present facts
- -- do not lay blame
- -- use business speak
- -- give solutions
- -- work with not against

Rinse and Repeat

- -- setup timetable for redoing tests
- -- new tech means new risk
- -- more usage means more risk
- -- increased data value means increased risk
- -- when baseline of tested system changes test is null and void

Thank you for listening