TJENESTER

Intern penetrasjonstest av nettverk og infrastruktur

I en intern penetrasjonstest vil vi simulere en målrettet trusselaktør som har fått tilgang til det interne datanettverket i din bedrift, et såkalt «Assumed breach»-scenario.

Målet med penetrasjonstesten vil være å få tilgang til bedriftssensitive data og høy privilegerte brukere, som oftest domeneadministrator-konto. Vi tester også om det er mulig å ta over nettverksinfrastruktur.

En intern penetrasjonstest vil kunne simulere verst tenkelige tilfelle av en kompromittering, som ved for eksempel et avansert Ransomware-angrep

En intern penetrasjonstest utføres som oftest etter tre scenarioer:

Vi kobler til en uautorisert PC til nettverket uten tilgang til påloggingsinformasjon.

En uautorisert PC kobles til nettverket deres, og vi har tilgang til en gyldig bruker som reflekterer standard rettigheter som en bruker har

En standard PC tilhørende din bedrift blir satt opp og vi blir gitt tilgang til en standard bruker

Under en intern penetrasjonstest vil følgende være del av testingen:

- Segmentering mellom lokasjoner
- Sikkerhetsovervåking av nettverk og endepunkt
- Muligheten for å eksfiltrere data uten at dette blir detektert
- Koblinger mot leverandører
- Active Directory-oppsett
- Bedrift- og gjeste-WiFi
- Svake passord og passordgjenbruk
- Kommunikasjon med skyløsinger og eventuelt Azure AD-oppsett
- Nettverksinfrastruktur

RING OSS
95 55 15 15

MAIL OSS
post@netsecurity.no

LES MER
www.netsecurity.no