Cybersecurity Risk Assessment

Descubrir posibles brechas de seguridad que pudieran ser explotados desde el punto de vista de **un atacante** y utilizados para efectuar un ataque sobre la infraestructura tecnológica y a los sistemas de su organización.

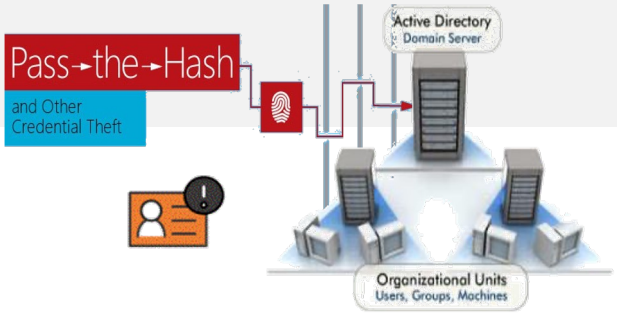
Esto nos permitirá **medir el actual nivel de Riesgo** y plantear un Plan Efectivo de mejora.

Seguridad de Infraestructura Externa

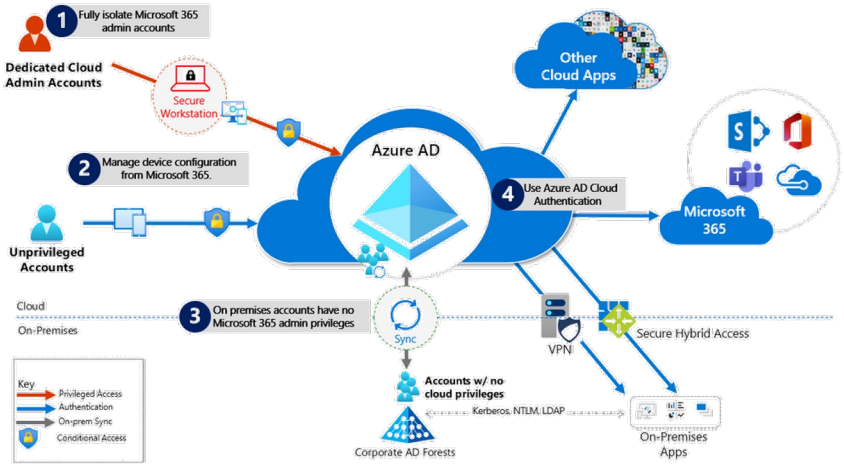
- ✓ Reconocimiento de la Superficie de Ataque
- ✓ Ataques de Password Spray
- ✓ Enumeración de Office365 & Azure por medio de APIs
- ✓ Enumeración OnPremise
- ✓ Identificación de Trayectorias mas Cortas a Domain Admin
- ✓ Movimiento Lateral
- ✓ Escalación Privilegios
- ✓ Riesgo de fuga masiva de Credenciales
- ✓ Acceso a Activos Valiosos

Pruebas de Seguridad al Directorio Activo

Dada la importancia de mantener la seguridad en los servidores de Dominio y en el Directorio Activo en general, se realizarán pruebas avanzadas de penetración al Directorio Activo y de robo de Credenciales de sistemas Windows, considerando las técnicas recientemente reportadas como amenazas por Microsoft.



Escalación del ataque



Seguridad de Infraestructura Interna

- ✓ Powershell attacks
- ✓ Password spray
- ✓ Pass-the-Hash attacks (NTLMv2)
- ✓ Pass-The-Ticket , Golden & Silver Tickets (Kerberos)
- ✓ Kerberos Delegation abuse
- ✓ Kerberoasting attacks
- ✓ DCShadow and DCSync attacks to DCs
- ✓ Unconstrained Delegation attacks
- • **Active Directory Full Compromise**