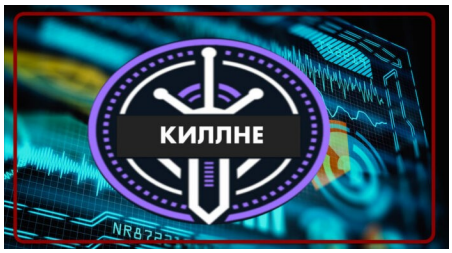
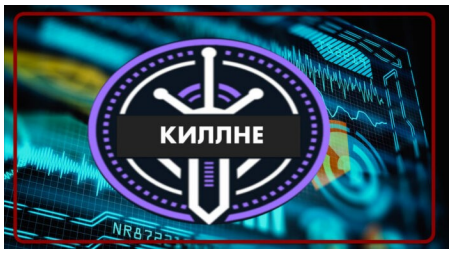


PROTOCOLO PARA LA PENETRACIÓN EN SISTEMAS INFORMÁTICOS.

1. **Reconocimiento**: Recopilación de información. Info pública (whois, DNS, alojamiento, servidores, …) Ingeniería social con el objetivo de accesos secundarios para la escalada de



privilegios. https://whois.icann.org/es/c%C3%B3mo-usar-whois

https://www.nic.es/sgnd/dominio/publicInformacionDominios.action

2. **Escaneo**: Ocultar info (https://vpnoverview.com/es/mejores-proveedores-vpn/servicios-vpn-gratis/). Wireshark si tenemos un punto de acceso. Recopilación de info en la LAN. Pasivo sin contramedidas. Uso de TOR https://www.torproject.org/es/download/ Buscadores https://www.webhostingsecretrevealed.net/es/blog/security/dark-web-websites-onion-links/ La DarkWeb … el sentido de la contra indexación.
3. **Obtener Acceso**: Uso de metasploit (https://www.metasploit.com/) Arsenal (https://github.com/topics/arsenal)
4. **Mantenerlo**: Uso de contramedidas. Creación del Caos … el caos confunde y genera errores. El error forzado es su debilidad si se ha preparado el escenario para recuperar passwords, reventar updates, controlar los servicios es capacitar el secuestro del host. La libertad vigilada permite localizar en la deep web los zero times que faciliten el acceso antes que a los administradores juniors. Los seniors han sido despedidos por el “coste excesivo”. El Sistema hace que los juniors crean que controlan la Red y … cuando se encuentran reventados no saben operar. Centros de datos completos funcionando en Botnets.
5. **Borrar el rastro**: entrar y salir sin que quede una huella. Lo máximo que se han borrado las huellas en el visor de sucesos en windows. Es más sencillo en GNU/Linux. Veni, vidi, vinci … es el último mensaje que debe quedar en el log.