Investigaciones & Espionaje Profesional

By: ExorciseThat
C.C. Misael Sandoval X.

1. Phishing Avanzado
1.1. Clasificación del Phishing
1.2. Vectores de Ataque
1.3. Diseño de Ataques
1.4. Análisis de Phishing
1.5. Detección de Phishing

2. OSINT Avanzado
2.1. Creación de Dorks Avanzados
2.2. DorkMe
2.3. GitRob
2.4. Registros DNS (A, MX, CNAME & TXT)
2.5. DMARC, SPF & DKIM
2.6. Firma Digital DKIM
2.7. E-Mail Headers Análisis
2.8. OSINT con Python

3. Reverse Privacy (Recopilación desde fuentes privadas)
3.1. Fuentes Privadas de Investigación
3.2. Intelx.io
3.3. Bases de Datos
3.4. Deep Web

4. OpSec
4.1. Whonix Gateway
4.2. Tunelización del Tráfico de Kali
4.3. Configuración para Redes sociales Anónimas (parcialmente)
4.4. Zero Knowledge Services
4.5. Proveedores de E-mail: Proton, Tutanota y Mailfence
4.6. Números Virtuales

5. Detracing 2.0
5.1. OpSec vs Detracing
5.2. Identidad Falsa
5.3. Redes Sociales
5.4. Doxxes Falsos
5.5. Eliminado de Información Real

6. Evasión Profesional de Mecanismos de Seguridad
6.1. Proxies
6.2. Red Tor
6.3. Virtual Private Network (VPN)

6.4. Comparación de Intrusividad con Wireshark
6.5. Blockchain

7. Auditoría de Seguridad Informática
7.1. ISO 27001
7.2. Proceso de Auditoría
7.3. Gestión de Vulnerabilidades: Nessus & Qualys
7.4. SIEM: IBM QRadar
7.5. Encriptación: VeraCrypt
7.6. Elaboración de Políticas de Seguridad Zero Trust
7.7. Capacitaciones al Personal Empresarial