Case Study #1- Security Audit & Penetration Test of an EU City Hall prior to major EU Summit

Standard/Methodology

1. OSCP (Offensive Security Certified Professional) methodology
2. Open Web Application Security Project (OWASP)
3. Penetration Testing Execution Standard (PTES)
4. SANS: Advanced Penetration Testing, Exploit Writing, and Ethical Hacking
5. Information Systems Security Assessment Framework (ISSAF)

Done:

- penetration test of external (255 IPs), internal (>500 workstations) and wireless network (6 access points)
- penetration test and source code audit 13 external and 31 internal web applications
- social engineering (phishing messages to >500 employees)

The result:

- 320 vulnerabilities (11 of them critical) were detected
- staff training (phishing, social engineering) was conducted
- detailed report of 350 pages about the process of simulating an attack, a detailed description of vulnerabilities and recommendations for their removal was provided
- repeated audit was conducted after 30 days. It confirmed the higher level of protection of all the resources.

Case Study #2 - EU Energy Provider Penetration Test

Industry: Energy

Business Challenge:
The client is one of the leading companies from Central Europe providing fuel, energy, retail services and petrochemicals, best known to the public for its service stations and for exploring and producing oil and gas on land and at sea. Prominent in over 70 countries and territories and employing more than 97,000 people around the globe.

The European Union (EU) legislation makes senior managers personally accountable for ensuring that regulatory requirements pertaining to IT security are met in full. With this in mind, the CEO and board of directors decided to engage our team to test the effectiveness of the company's cyber security controls and its ability to both detect and respond to malicious behaviour.

The client required Infrastructure Penetration Testing, ICS/SCADA, Web Application, Web Service (API) and Mobile platform. The requirement was for a multi-part pentest which needed to be delivered in separate phases in order to archive compliance and EU regulation standards, protecting employee and customer data.

Solution:

For this engagement, we utilised techniques and procedures (TTPs) of real-world attackers to emulate advanced threat actor activities within the organisation's network environment. The project involved testing all facets of the company's IT defences.

To ensure the engagement was conducted as realistically as possible, we received no internal information or access to the client's business. All knowledge was obtained leveraging open source threat intelligence (OSINT) gathering techniques to identify valuable information that was available within the public domain.

The engagement was a replication of the Ukraine power grid cyberattack which took place on 23 December 2015 and is considered to be the first known successful cyberattack on a power grid. Hackers were able to successfully compromise information systems of three energy distribution companies in Ukraine and temporarily disrupt electricity supply to the end consumers. Most affected were consumers of «Prykarpattyaoblenergo» (Ukrainian: Прикарпаттяобленерго; servicing Ivano-Frankivsk Oblast): 30 substations were switched off, and about 230 thousand people were left without electricity for a period from 1 to 6 hours.

People, Processes, & Technology:
Penetration testing can be conducted in many ways and methodologies. Usually we follow this process:

Test Planning
·Meeting with customer
·Align tests goals and scope
·Intelligence gathering

Vulnerabilities Identification
·Potential vulnerabilities detection
·Threat modeling
·Business process analysis

Vulnerabilities Exploiting
·Vulnerabilities testing
·Vulnerabilities validation
·Vulnerability research

Post Exploitation
·Escalating privileges
·Infrastructure analysis
·Vulnerability research

Reporting and Recommendation
Create a report for system owners, including found vulnerabilities and recommendations how to eliminate them.

For our client's specific requirements and geographical locations, we agreed to pursue the following methods: black box tests, social engineering, email phishing, and onsite red teaming.

# Standard/Methodology
1. IEC 62443: Network and System Security for ICS
2. Open Web Application Security Project (OWASP)
3. Penetration Testing Execution Standard (PTES)
4. SANS: Advanced Penetration Testing, Exploit Writing, and Ethical Hacking
5. Information Systems Security Assessment Framework (ISSAF)

With a team of 2 engineers and a duration of 4 weeks we were able to fully compromise not only the organizations infrastructure but also, web applications as well as expose critical data related to key organizational stakeholders.

The Result:

Penetration testing is often done for varying reasons. Two of the key goals we and our client aimed for, were to increase upper management awareness of security issues and to test intrusion detection and response capabilities. After conducting the penetration test and compromising the organization engaged the client in a controlled offensive/defensive threat detection challenge, allowing the client several days to identify and remediate active threats within their systems. After this challenge was complete we provided clear guidance on how to mitigate the risk, recommending specific solutions, policies or training courses as appropriate. Consequently, the business is now putting in place new measures to better protect its data, employees and customers. In the end our client was able to meet the highest level of compliance and regulation standards, develop better security practices and reassure their customers, employees, and board of their continued dedication to best business practices and continued growth.

Key Benefits:

- **Increase Business Continuity**
- **Protect Clients, Partners and Third Parties**
- **Help to evaluate Security Investments**