A Iniciativa

A proposta deste conteúdo é fornecer um roteiro de estudo estruturado sobre segurança, com foco em aplicações web (embora não se restrinja somente a isso), visando incentivar que novos profissionais se interessem pela área. O intuído desse conteúdo é criar uma rota de aprendizagem colaborativa.

Contexto

Em 2001, dado as sucessivas detecções, análises e alertas generalizados referente a um *worm* conhecido como Li0n, criou-se o Internet Storm Center (ISC), uma central que provê análises e alertas para milhares de usuários e organizações na internet, contribuindo ativamente com os provedores de internet, no intuito de combater ataques maliciosos. Através de ferramentas como o DShield Sensor, o ISC coleta diariamente milhões de detecções, cobrindo mais de 500.000 endereços IP em mais de 50 países, com o apoio e suporte do instituto SANS, além de voluntários do setor denominados Handlers.

Handlers

Handlers[1] são profissionais que doam seu valioso tempo na detecção e investigação de incidentes e anomalias, provenientes de ataques cibernéticos. Atualmente formado por 19 pessoas, os Handlrers contribuem regularmente sobre o tema, seja elaborando ideias, pontuando observações ou apresentando casos reais de forma educativa.

A jornada para se tornar um Handler é longa, envolta de desafios e descobertas. O roadmap oficial contém detalhes minuciosos sobre o processo, bem como os requisitos a serem atendidos. Dentre eles, destacaremos aqui a:

1. Certificação GIAC ou uma significante contribuição na área.

Primeiros passos

Se você não faz ideia do que trata o certificado GIAC e tem zero contribuição na comunidade, não desanime, pois todo objetivo precisa iniciar de algum lugar, e é esse o propósito dessa iniciativa.

Explicado, vamos começar!

> ***Nota[1]**: o nome Handlers (Manipuladores, em tradução livre) é usado nesse contexto, pois no protocolo web, "Handlers" são pontos de passagem onde eventos ocorrem, podendo ser observados, capturados ou anulados.*

Primeiros passos

> **ATENÇÃO**: as técnicas demonstradas nesse conteúdo são as mesmas usadas por cibercriminosos, na tentativa de obter vantagem sobre um serviço ou empresa. Contudo, o intuito desse material é orientar novos especialistas no assunto, para que juntos possamos, cada vez mais, proteger nossos sistemas. Seja ético. Seja responsável.

Requisitos Técnicos

É de suma importância que alguns requisitos sejam atendidos, a título de tornar o caminho mais leve e compreensível. Embora não seja mandatório, é altamente recomendável que você possua a seguinte combinação de habilidades e conhecimento:

- Familiaridade com programação (qualquer linguagem);
- Vivência no uso do sistema operacional Linux (qualquer distribuição);
- Compreensão básica de protocolos e redes (tcp, udp, etc...);
- Autonomia para aprender.

> **ATENÇÃO**: o roteiro não visa detalhar minuciosamente cada aspecto ou ferramenta utilizada, portanto, sempre que se deparar com o ícone da lupa (🔍), interprete-o como um indicativo de que o entendimento sobre este item é crucial, portanto, é altamente recomendável que você dedique, sem pressa, um tempo considerável entendendo-o, antes de prosseguir. Caso você esteja aqui apenas pela curiosidade, siga em frente sem receio.

Jornada

- Prólogo - Por onde começar?;
- Ato I - Observando por trás da cortina;
- Ato II - Porta para todos os lugares.