SecurityTeam@IST

Tiago Miguel Rodrigues Simões

Relatório de Actividades

Resumo—Este relatório tem como finalidade descrever o trabalho e reflexões desenvolvidas, ao longo do semestre, durante a actividade SecurityTeam@IST no âmbito da cadeira de Portfolio Pessoal III. Serão discutidas as aprendizagens e conhecimentos adquiridos relativos ao tema cibersegurança. Os factos aqui referidos derivam directamente dos factos relatados no relatório de actividades.

Palavras Chave—STT IST segurança informática ataques defesa

O Documento muito POBRE em Termos de aprendizagens Transversais

Este documento confunde a descrição das APRENDIZAGENS mas está a usar o MODELO ERRADO!

1 Introdução

Este documento tem como objectivo narrar a experiência, em termos de aprendizagem, adquiridas durante a actividade SecurityTeam@IST (STT). Aqui, apresento os aspectos ligados às aprendizagens e conhecimentos adquiridos tanto a nível informático, que é o principal objectivo, bem como a nível social. Enunciarei também alguns conceitos e outros tópicos essenciais para o bom entendimento do tema.

NÃO DEVIA!

2 Informática

Informática é um termo que se refere ao processamento automático de informação através de dispositivos electrónicos e sistemas computacionais, tal como a palavra indica, "informação automática".

A informática reúne muitas técnicas que o ser humano desenvolveu com o objectivo de potenciar a sua capacidade de pensamento, memória e comunicação. É considerada uma área da ciência sem limites, sendo utilizada nos mais variados meios: gestão, armazenamento de dados/informação, comunicação, transportes, medicina entre muitos outros. Dentro desta ciência existem diversas áreas que podemos explorar - Sistemas Inteligentes, Sistemas Embebidos, Sistemas Distribuídos, Sistema de Rede, Multimédia, Engenharia de Software, entre outras.

2.1 Segurança Informática

O conceito de segurança da informação está relacionado com a proteção de um conjunto de dados e/ou informações, no sentido de preservar o valor que possuem para um dado índividuo ou organização. Um serviço seguro deve garantir privacidade, integridade e disponibilidade.

Existem, no entanto, um conjunto de ameaças que devemos ter em conta cada vez que utilizamos um serviço informático. Acessos não autorizados, admissão de informação falsa, interrupção do correcto funcionamento de uma operação e usurpação são ameaças mais comuns no mundo virtual.

3 Mecanismos de Segurança

Dentro dos mecanismos de segurança podemos listar dois tipos: os controlos físicos, que são barreiras que limitam o contacto ou acesso directo à informação ou a estrutura que a suporta - portas, paredes, guardas; e os controlos lógicos, que são barreiras que impedem ou limitam o acesso à informação através de mecanismos automatizados - protocolos, encriptação e certificados.

• *Tiago Miguel Rodrigues Simões, nr. 73100, E-mail: tiagosimoes@ist.utl.pt, Instituto Superior Técnico, Universidade de Lisboa.*

Manuscrito entregue a 16 de Janeiro de 2015.

(1.0) Excelent	ACTIVITY					DOCUMENT						
(0.8) Very Good	~~Objectives~~ x2	~~Options~~ x1	~~Execution~~ x4	~~STC~~ x1	SCORE	Structure x0.25	Ortogr. x0.25	Gramm. x0,.25	Format x0.25	Title x0.5	Filename x0.5	SCORE
(0.6) Good												
(0.4) Fair	0.4	0.2	0.8	0.4	1.8	0.25	0.25	0.25	0	0.3	0.5	1.55
(0.2) Weak												

Como seria de esperar, os mecanismos de controlos lógicos foram os únicos a serem explorados durante a actividade.

4 Exploração de Vulnerabilidades

Conseguir descobrir vulnerabilidades e falhas nos sistemas informáticos/electrónicos, é o principal objectivo desta actividade.
Das diversas fontes de ataques, podemos classificar os riscos da seguinte forma: intercepção de comunicações, recusas de serviço, intrusões e alçapões.

4.1 Intercepção de comunicações

Ao interceptar comunicações entre computadores ou entre computadores e *routers* é possível roubar sessões (nome do utilizador e palavra-chave), usurpar identidades, e ainda desviar ou alterar mensagens.

4.2 Recusas de serviço

São ataques destinados a perturbar o bom funcionamento de um serviço, tornando os serviços indisponíveis por tempo indeterminado.

4.3 Intrusões

Normalmente o atacante recorre a uma técnica chamada "Elevação de Privilégios"que tem como objectivo ganhar o controlo da máquina atacada. Este tipo de ataque consiste em explorar uma vulnerabilidade de uma aplicação enviando um pedido específico tendo como efeito um comportamento anormal que pode conduzir a um acesso ao sistema.

4.4 Alçapões

Aproveitar uma porta escondida dissimulada num programa, permitindo um acesso não autorizado pelo criador. Também conhecido por *backdoor*.

5 Aprendizagem

Enquanto membro activo da STT, foi possível aprender a utilzar quase todos os métodos referidos. Todos eles tem maneiras e formas de actuação únicas, o que torna díficil a aprenidizagem de todos. Além dos métodos aqui relatados, existem muitos mais tipos de ataques. Mas os mais comuns e os mais debatidos na STT foram estes quatro.
Nos primórdios da STT, inclinei-me sobretudo nos ataques de Intrusões. Era o que me chamava mais à atenção. Consegui desenvolver e ser bem sucedido em alguns ataques. Mais tarde, surgiu o interesse por Alçapões. Era um domínio da segurança informática que pouco me chamava à atenção, e pouco ou nada percebia. Com a ajuda dos meus colegas de equipa e tutoriais, consegui evoluir bastante nesta área.
Entrar em competições na área da informática também foi uma novidade para mim. Nunca tinha participado em semelhante actividade. Foi, de facto, uma agradável surpresa. Penso que para grande parte dos meus colegas a presença em competições internacionais de segurança informática também tenha sido uma novidade.
O ser humano é um ser social desde que nasce, portanto é essencial desenvolver essa qualidade, e este tipo de actividade suscita a comunicação e a partilha de ideias. O que considero, excelentente!

6 Conclusão

Após vivenciar três meses na STT, apenas conto com experiências positivas. Recomendo a todos os alunos de Mestrado em Engenharia Informática (MEIC) e a outros possíveis interessados em informática. Todos os elementos da equipa são prestáveis e sempre dispostos a ajudar no que souberem. Ao mesmo tempo que aprendemos a fazer algo de útil também nos divertimos a faze-lo.

Agradecimentos

Quero agradecer ao professor Pedro Adão, sem ele a STT não tinha começado; aos meus colegas de equipa; e sem nunca esquecer ao IST, que forneceu meios para a realização de reuniões e competições.

Tiago Miguel Rodrigues Simões , aluno de 4º ano no IST a estudar Engenharia Informática na área de Sistemas Distribuídos e Engenharia de Software.