SecurityTeam@IST

Filipe Teixeira

Relatório de Aprendizagens

Resumo—A SecurityTeam@IST é uma equipa com o objectivo de participação em competições nacionais e internacionais na área da Segurança de Redes e Sistemas Informáticos. Estas competições, comummente designadas por Capture The Flag juntam digitalmente centenas de equipas e milhares de entusiastas à volta do mundo. Através da participação na SecurityTeam@IST foram desenvolvidos várias actividades que serviram para melhorar algumas capacidades transversais e não só. Através da participação da equipa no evento RuCTFE foram várias as conclusões a tirar, não só no âmbito da segurança mas também de competências transversais como o trabalho em equipa ou a ética profissional.

Palavras Chave—securityteam@ist, securityteam, ist, cibersegurança, RuCTFE, HAX.TOR, Filipe Teixeira, , LaTeX, paper.

1 Introdução

Trabalhar na área da segurança informática não é uma tarefa fácil, muitas vezes, se não praticamente todas, os erros explorados por atacantes são o resultado de falta de atenção, de conhecimento ou mesmo de experiência. O trabalho desenvolvido por uma equipa como a SecurityTeam não se compara ao dia-a-dia de um Engenheiro de Segurança, mas o objectivo é semelhante. A SecurityTeam, fruto do empenho e dedicação do Professor Pedro Adão, não envolve o trabalho de professor-aluno mas sim de aprendizagem entre grupo através da passagem de experiências entre os participantes. Isto pode ser um entrave ao desenvolvimento de algumas capacidades necessárias ao bom desempenho em competições CTF ou semelhante.

2 Competências Transversais

As competências transversais são um conjunto de atributos necessários para melhorar um indivíduo como trabalhador, sendo transversais ao tipo de actividade que este tem não depende da carreira escolhida e são esperadas em todos os trabalhadores.

2.1 Trabalho de Equipa

A capacidade de trabalho em equipa é muito importante e neste caso mais ainda. Estando as competições agrupadas em vários tipo de exercícios é fundamental saber interagir com os restantes elementos do grupo para não colocar o esforço de todos em causa. Quer como líder de equipa quer como membro desta é importante cada um saber o seu lugar assim como é importante quem dirige a equipa saber coordená-la. Através da participação é fácil perceber que se houver alguma quebra na comunicação da equipa isso leva a uma descoordenação que irá trazer mais falta de comunicação tornando-se uma bola de neve. Foi importante dividir os diferentes exercícios por partes da equipas e tornar assim a comunicação entre pequenos grupos menos frequente aumentando a comunicação dentro daquele grupo. Essa diminuição nos participantes de cada grupo levou a uma melhor organização conseguindo assim tornar a equipa mais eficiente.

• *Filipe Teixeira, nr. 73045, E-mail: filipelteixeira@gmail.com, Instituto Superior Técnico, Universidade de Lisboa.*

Manuscripto recebido Janeiro 17, 2015.

(1.0) Excelent	LEARNING					DOCUMENT						
(0.8) Very Good	CONTEXT x2	SKILLS x1	REFLECT x4	S+C 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	2	1	4	0.8	7.8	0.25	0.25	0.25	0.25	0.5	0.5	2
(0.2) Weak												

2.2 Ética

A ética é uma questão muito importante e onde existem diferentes divergências não havendo assim um modelo a seguir. No caso da experiência da SecurityTeam a ética é extremamente importante. Devido ao âmbito do trabalho desenvolvido é fácil muitas vezes haver um limite muito ténuo entre o que é correcto ou não. Quando se exploram vulnerabilidades está se a fazer um trabalho destrutivo mas dependendo do resultado final pode ser avaliado como correcto ou não. A exploração de vulnerabilidades pode ser usada para descobrir falhas em sistemas considerados seguros e que devem ser resolvidas o mais rapidamente possível. Ao explorar estas falhas em ambientes não controlados podem haver danos colaterais em empresas, sistemas, serviços, etc. Este facto é extremamente importante para o trabalho que pretende ser desenvolvido pela SecurityTeam. Alguns dos maiores vírus informáticos que já existiram originaram de práticas em ambientes inseguros com capacidade de os espalhar para outras redes, serviços e máquinas. Um exemplo da importância desta ética foi um dos problemas que apareceram na participação na RuCTFE. Quando foi ligada a máquina servidora para o concurso foi detectada uma falha de segurança que permitia atacantes experientes de aceder à sub-rede onde estávamos ligados o que poderia por em causa todos os equipamentos ligados naquela sub-rede. Podíamos ter ignorado este facto e continuado com a participação esperando que ninguém nos fosse atacar dessa forma, mas foi claramente deliberado que se punha em causa outros equipamentos esse risco não seria corrido.

2.3 Atitude

Ter uma boa postura e uma atitude correcta não só é saudável mas também é muito importante em exercícios cansativos e desgastantes como pode ser a detecção de vulnerabilidades. Muitas vezes são precisas horas intensas de procura sem nenhum resultado para no fim conseguir descobrir aquela pequena falha que compromete todo o sistema, ou aquela simples resolução de entre um milhão que resolve um problema grave de segurança.

2.4 Controlo do Tempo e Organização

A organização é importante para qualquer tipo de actividade e muito mais em informática. Quando um programa se expande aos milhares de milhões de linhas de código é extremamente importante haver uma estrutura bem organizada que evita perder muito tempo quando existem alterações a serem feitas. No caso das competições CTF também esta organização e capacidade de controlar o tempo que se gasta num certo exercício é muito importante. Como todas as competições têm um tempo limite e a velocidade com que se chega a uma solução é imperativo. Também se pode transferir esta ideia para o mercado laboral, quando é descoberta uma vulnerabilidade, nomeadamente chamada de vulnerabilidade de dia zero, é muito importante a velocidade com que os Engenheiros de Segurança conseguem arranjar um solução para o problema.

2.5 Crítica

Para crescer não só como trabalhador mas também como pessoa é muito importante saber aceitar e aprender através de críticas construtivas, assim como saber criticar os outros de forma a que eles possam aprender com os seus erros e melhorar as suas performances. Assim como cada um tem os seus defeitos também cada um tem áreas de conhecimento que domina melhor do que outras e o pior que pode acontecer é alguma vez alguém deixar de ser aluno porque todos temos algo a aprender ainda. Como o método de aprendizagem na SecurityTeam não seguia o método convencional de professor-alunos como já foi referido anteriormente é extremamente necessário cada participante estar disposto a ouvir o seu colega e conseguir melhorar os seus pontos menos fortes através da partilha dos outros membros.

3 Ferramentas

Apesar de o objectivo principal não incidir sobre as competências específicas é de salientar a aprendizagem e experiência que foram desenvolvidas em algumas ferramentas importantes para o objectivo da SecurityTeam.

- Wireshark [1] - é uma ferramenta utilizada para a análise de pacotes. Muitas vezes utilizada para perceber interacções entre clientes e servidores, serviços, ou mesmo informações sobre ou dentro de uma rede.
- tcpdump [2] - Muito similar ao Wireshark, o seu propósito também é a análise de pacotes de dados numa determinada rede. Esta ferramenta, apesar de ter menos funcionalidades que o Wireshark, continua a ser usada porque permite uma interacção simples através da linha de comandos.
- OpenSSH [3] - Utilizado para criar sessões seguras entre computadores utilizando o protocolo SSH.
- MD5 Decrypter [4] - uma base de dados que tenta encontrar colisões para uma determinada chave MD5.
- Charles [5] - uma aplicação de proxy que consegue alterar datagramas de forma a tentar explorar vulnerabilidades através de personificação da autenticação efectuada. Exemplo: Personificação de IP.

4 Conclusão

Através dos obstáculos que se apresentaram pelo caminho foram várias as lições a tirar. Em suma penso que toda a aprendizagem e experiência que foram colhidos deste desafio vão ter uma grande importância no meu crescimento não só no exercício da minha futura profissão mas também como pessoa. Foi muito importante a colaboração de todos os membros da SecurityTeam assim como todas as linhas directivas dadas pelo Professor Pedro Adão. Concluindo, está actividade foi bastante interessante e motivadora, espero então poder continuar inserido neste grupo e melhorar assim continuamente tanto as minhas capacidades como o meu conhecimento e experiência.

Neste tipo de documento (Técnico) a Conclusão deve começar com um Resumo do assunto abordado e depois deve realçar os resultados

Agradecimentos

Gostaria de agradecer ao Professor Pedro Adão quer pela grande iniciativa que teve em fundar a SecurityTeam@IST quer em aceitar a minha inscrição e proporcionar não só a mim mas a todos os participantes uma grande fonte de aprendizagem e por a cima de tudo nos ajudar e incentivar apesar das dificuldades e mostrar que nunca se desiste. Também gostaria de agradecer ao Professor Ricardo Chaves pela ajuda que prestou na competição onde participámos. A estes e a todos os participantes da SecurityTeam@IST obrigado.

REFERÊNCIAS

[1] https://www.wireshark.org/
[2] http://www.tcpdump.org/
[3] http://www.openssh.com/
[4] http://www.hashkiller.co.uk/md5-decrypter.aspx
[5] http://www.charlesproxy.com/

Filipe Alexandre Lourenço Teixeira Masters Student at Instituto Superior Técnico (IST).