SecurityTeam@IST

Filipe Apolinário

Relatório de Aprendizagens

Resumo—No presente relatório apresento todas as capacidades que adquiri ao exercer actividades na SecurityTeam@IST, divididas em dois tipos hardskills e softskills.
As hardskills adquiridas nas actividades desempenhadas na SecurityTeam@IST estão relacionadas com a área de cibersegurança e divididas em três categorias, Reconnaissance, Spoofing e Variable Manipulation. Por outro lado, as softskills adquiridas nas actividades desempenhadas incluem capacidades de coordenação, comunicação, relacionamento interpessoal, resolução de problemas, pensamento crítico, escuta activa, vontade de aprender, boa gestão de tempo, trabalho de equipa e flexiblidade.
Estou certo que após a leitura deste relatório, é perceptivel a razão pela qual foi minha intenção juntar-me à SecurityTeam@IST, mas também o porquê de achar que as competências adquiridas me serão útil num futuro próximo.

Palavras Chave—Capacidades Adquiridas, hardskills,cibersegurança, SecurityTeam@IST,sistemas de informação,técnicas de análise de sistemas de informação,ataques a sistemas de informação,Reconnaissance, exame de cabeçalhos HTTP, exame de cookies HTTP,Spoofing, Spoofing de useragent do browser de HTML, Spoofing através de referer, Variable Manipulation,SQL injection,Buffer overflow, Server Side Include, softskills, coordenação, comunicação, relacionamento interpessoal, resolução de problemas e pensamento crítico, escuta activa, vontade de aprender, boa gestão de tempo, trabalho de equipa, Flexibilidade.

EXCESSIVO E INADEQUADO!
Grande parte do documento descreve a actividade delegando a descrição das competências transversais para algumas frases telegráficas.

1 Introdução

Desde o inicio dos meus estudos académicos que expresso um grande fascínio académico pela área de cibersegurança e por à prova os diversos mecanismos de segurança, procurando a descoberta de falhas e possíveis melhoramentos dos mecanismos analisados. Foi pelo interesse nesta área e pela esperança de expandir o meu conhecimento em análise de sistemas de informação que me decidi inscrever na SecurityTeam@IST.
Desde o momento em que tomei a decisão de me inscrever no grupo até hoje só vejo aspectos positivos na experiência que adquiri ao desempenhar as actividades que me foram delegadas.

2 Capacidades Adquiridas

Nos meses em que desempenhei actividades na SecurityTeam@IST, adquiri várias capacidades técnicas (hardskills) bem como várias capacidades profissionais (softskills). Estas técnicas serão descritas nas próximas subsecções.

• *Filipe Apolinário, nr. 70571,*
E-mail: f.apolinario30@gmail.com

Janeiro 17, 2015.

2.1 Hardskills aprendidas

2.1.1 Reconnaissance

Reconnaissance é um termo usado por militares e serve para obter informação sobre o inimigo ou sobre recursos que este possui. Esta observação pode ser feita a partir de observação visual ou outros métodos de detecção de informação. No caso da cibersegurança, as técnicas de Reconnaissance são muito usadas quer por atacantes quer pela defesa do sistema, permitindo assim descobrir informação sobre o sistema alvo e consequentemente detectar vulnerabilidades ou possíveis ameaças, desempenhando assim um papel essencial no planeamento de um possível ataque ou na defesa de determinado sistema.
Durante as actividades que desempenhei no grupo aprendi várias técnicas de Reconnaissance, nomeadamente:

(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	1.4	0.7	2.8	0.6	5.5	0.25	0.15	0.2	0.2	0.5	0.5	1.8
(0.2) Weak												

1) exame de cabeçalhos ou cookies HTTP, de forma a identificar vulnerabilidades na informação comunicação entre cliente/servidor
2) exploração de erros verbosos no sistema apresentado ao cliente de forma a identificar o efeito do erro no sistema, a linguagem foi usada para programar o sistema e que bugs existem no código do sistema.

2.1.2 *Spoofing*

Spoofing, ou Spoofing Attack, é designado em cibersegurança como uma situação em que uma pessoa ou programa 'A' se mascara como outra pessoa ou programa 'B' levando eficazmente o sistema alvo a achar que se trata de 'B' em vez de 'A'. Este ataque é usado para contornar as defesas do sistema alvo e aceder a dados ou executar operações privilegiadas.
Durante as actividades no grupo aprendi várias técnicas de Spoofing através de falhas de HTTP, nomeadamente:

1) Spoofing de useragent do browser de HTML, acontece quando um site dá permissões especiais a alguns tipos de utilizadores ou browsers de HTML. Este ataque apesar de ser raramente eficaz, é facilmente executado, bastando apenas modificar os campos correspondentes no cabeçalho HTTP.
2) Spoofing usando cookie HTTP, acontece quando um site dá permissões especiais a alguns tipos de utilizadores usando campos do cookie para garantir essa permissão. Tal como o spoofing de useragent do browser para realizar este ataque basta alterar o campo do cookie para o valor pretendido.
3) Spoofing através de referer, acontece quando um site dá permissões especiais a utilizadores que acedem ao sistema a partir de outro site. Neste caso o ataque é um pouco mais complexo, mas igualmente fácil de realizar.

2.1.3 *Variable Manipulation*

Variable Manipulation é designado em cibersegurança por uma situação em que o atacante se aproveita do mau tratamento dos dados fornecidos pelo utilizador de forma a provocar situações de falha, ou realizar operações a ficheiros que não deviam ser permitidas a um utilizador normal do sistema, nomeadamente:

1) SQL injection, onde um atacante executa pedidos à base de Dados SQL de um servidor de forma a revelar erros, descobrir dados previligiados e consequentemente manipula-los conforme a sua necessidade.
2) Buffer overflow, onde um atacante fornece dados a um determinado vector de input de forma a escrever em variáveis de acesso restrito e consequentemente executar operações privilegiadas, que não seriam possível executar normalmente.Este ataque é possível realizar em várias linguagens de programação, como é o caso da linguagem C.
3) Server Side Include, onde atacante se aproveita da função do PHP include() e faz com que o servidor inclua no seu código php a página inserida na função include(). Este ataque permite ao utilizador modificar dados do servidor e inclusivo infectar o servidor com ficheiros maliciosos capazes de atacar o servidor de forma autónoma.

2.2 Softskills Aprendidas

Para alem das hardskills aprendidas, as actividades na SecurityTeam@IST permitiram-me adquirir várias softskills, nomeadamente:

2.2.1 *Coordenação de pessoas*

No início do grupo e durante o semestre voluntariei-me para coordenar a actividade do grupo na plataforma do Trello. A gestão da plataforma como explicado no Activity Report envolveu o registo da organização na plataforma e gestão de todas as actividades envolvendo esta plataforma.

2.2.2 *Comunicação*

Durante as reuniões da SecurityTeam@IST tive a oportunidade de participar activamente em várias discussões e de apresentar um ataque

de segurança informática. Estas actividades durante as reuniões, permitiram-me melhorar o meu discurso e batalhar a minha timidez de discursar em publico.

2.2.3 Relacionamento interpessoal

Durante as "coffee breaks"das reuniões e competições que o grupo realizou, tive a oportunidade de conversar abertamente com vários membros do grupo; melhorando assim as minhas capacidades de relacionamento interpessoal.
Para além das coffee breaks, houveram várias situações durante a competição em que houve partilha de conhecimentos e de entreajuda. Estas situações também representam um factor decisivo no melhoramento das relações interpessoais.

2.2.4 Resolução de problemas e pensamento crítico

As competições da SecurityTeam@IST permitiram desenvolver bastante a resolução de problemas e o pensamento crítico. Estas capacidades foram estimuladas várias vezes pelos desafios apresentados pela competição em sí, mas também por causa de falhas de equipamento, exigindo a tomada de decisões de forma rápida e eficaz.

2.2.5 Escuta activa

Nas reuniões da SecurityTeam@IST as minhas competências de escuta activa foram estimuladas através das apresentações dos diversos membros. De forma a não perturbar o raciocínio do interlocutor, tive de gerir as questões que colocava durante a apresentação, fazendo-o apenas quando necessário.

2.2.6 Vontade de aprender

Toda a actividade da SecurityTeam@IST obrigou-me a investigar sobre temas desconhecidos relativos a cibersegurança exigindo assim grande vontade de aprendizagem.

2.2.7 Boa gestão de tempo

Sendo uma actividade extra-curricular com duração semestral, exigiu uma ginástica entre o trabalho curricular e a SecurityTeam@IST.

2.2.8 Trabalho de equipa

Nas competições da SecurityTeam@IST a resolução de desafios foi feita em equipa, aumentando assim as minhas capacidades de trabalho em equipa.

2.2.9 Flexibilidade

A versatilidade dos desafios das competições, exigiram-me flexibilidade na maneira como encarava os desafios, obrigando assim a usar diferentes abordagens.

3 Conclusão

Considerando todas as capacidades de hardskills e softskills e a experiência que adquiri, os desafios propostos nesta área de competências extra-curricular revelaram-se uma grande mais valia para mim quer em termos de curriculum quer em termos de intelecto. No meu ponto de vista as actividades na SecurityTeam@IST foram de extrema importância por se tratar de uma área complementar à matéria leccionada no meu mestrado em Sistemas Distribuídos permitindo-me assim, vestir a pele de um atacante e pôr os sistemas que desenvolvi à prova. É por esta razão que estou confiante que esta experiência me abre a mente para uma nova perspectiva de análise de problemas.
Para alem das actividades desempenhadas e dos desafios que fui confrontado, as softskills que adquiri são extremamente úteis e estou confiante que serão factor decisivo na minha performance em entrevistas de emprego e no resto do meu futuro profissional.
Foi com estes conhecimentos adquiridos que suspendi a actividade no dia 29 de Dezembro de 2014 e é a com esperança de aumentar o conhecimento nesta área de competências que espero retomar com a mesma força de vontade e aprendizagem em Fevereiro de 2015 quando a SecurityTeam@IST voltar a actividade.

Agradecimentos

Gostaria de aproveitar esta secção para deixar um cumprimento a todos os meus colegas da SecurityTeam@IST e em especial ao professor Pedro Adão que promoveu, criou e participou no grupo.

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

Gostaria também de aproveitar esta secção para agradecer e deixar um voto de solidariedade ao website http://www.enigmagroup.org/, ao qual devo grande parte do conhecimento necessário para as competições e que apesar de várias dificuldades monetárias, tem conseguido manter-se online graças às doações dos membros do site.