SecurityTeam, IST

João Francisco Vieira Gonçalves Pais Santos

Relatório de Aprendizagens

Resumo—A SecurityTeam é uma equipa composta principalmente por alunos de engenharia informática do Instituto Superior Técnico. Este relatório descreve as aprendizagens adquiridas com a realização desta actividade para a cadeira de portfolio IV. Estas aprendizagens são na sua maioria não técnicas embora que durante as competições apreendi a usar parcialmente duas novas ferramentas.

Palavras Chave—cibersegurança.

1 Introdução

Com a realização desta actividade, relacionada com cibersegurança, penso que aprendi muita coisa ao longo dos últimos meses. É uma área realmente bastante vasta e complexa e há muito para aprender. Como é praticamente impossível saber de tudo de tudo sobre segurança informática, ter uma boa equipa é essencial. Isto permite que nos possamos especializar num determinado tema, e assim conseguir resolver problemas bastante complexos de forma eficiente.
É preciso realmente uma grande dedicação e paixão para prosseguir nesta área informática.

2 Competências Transversais

De seguida, apresento um conjunto de competências que adquiri e outras que foram enriquecidas com a realização desta actividade.

2.1 Aprendizagem contínua

Inicialmente quando me inscrevi para esta actividade, sabia muito pouco ou mesmo quase nada de segurança informática. Para resolver estes problemas das competições, requer um grande conhecimento técnico. Embora nem todos tenham o mesmo grau de dificuldade, grande parte deles são bastante complexos.
O que começei por fazer, foi ir ao repositório oficial [1] disponibilizado pela organização no GitHub e começei por procurar por uma bibliografia base [2]–[5], usado pelos participantes. Embora não os tenha chegado a ler todos porque não só são bastantes extensos mas têm muitos pormenores, o livro do shellcoders [5] foi aquele onde investi mais tempo. Penso que explica bastante bem as vulnerabilidades em diferentes plataformas e os seus mecanismos de protecção.

2.1.1 Novas ferramentas

Aprendi a mexer em algumas pequenas ferramentas que nunca tinha utilizado como o objdump. Este serviu mais para desafios que envolvia a procura de vulnerabilidades dado um ficheiro binário. Também aprendi uns conhecimentos básicos com uso da ferramenta "pngcheck"e "GDB - Debugging Stripped Binaries"para tentativa de resolução dos problemas para a competição do Plaid CTF.

• *João Francisco Vieira Gonçalves Pais Santos, nr. 66373, Instituto Superior Técnico, Universidade de Lisboa.*

incompleto

Manuscrito recebido a Junho 6, 2015.

(1.0) Excellent	LEARNINGS						DOCUMENT						
(0.8) Very Good	Context×2	Skills×1	Reflect×4	Summ×.5	Concl×.5	SCORE	Struct ×.25	Ortog×.25	Exec×4	Form ×.25	Titles ×.5	File ×.5	SCORE
(0.6) Good	0.8	0.6	0.6	0.8	0.6		0.6	0.4	0.5	0.8	1.0	1.0	
(0.4) Fair													
(0.2) Weak													

2.2 Ética

Visto que estamos a tentar resolver problemas relacionados com segurança informática é preciso ter bastante cuidado em como vamos usar estes conhecimentos no futuro. Segundo o código penal português, artigo 221, relacionado com burla informática e nas comunicações, *Quem, com intenção de obter para si ou para terceiro enriquecimento ilegítimo, causar a outra pessoa prejuízo patrimonial, interferindo no resultado de tratamento de dados ou mediante estruturação incorrecta de programa informático, utilização incorrecta ou incompleta de dados, utilização de dados sem autorização ou intervenção por qualquer outro modo não autorizada no processamento, é punido com pena de prisão até 3 anos ou com pena de multa*. Este ponto é realmente importante porque até mesmo nós como estudantes, por curiosidade, começamos aplicar estes novos conhecimentos em aplicações reais do qual muita gente pode depender e facto de conseguirmos alterar sequer uma vírgula na bases de dados, pode comprometer o nosso futuro se não tivermos a devida autorização.
Outro caso que também pode surgir é quando identificamos uma vulnerabilidade e a reportamos a uma determinada entidade. Por muita boa que possa parecer esta acção, essa entidade não tem garantia que a pessoa não explorou o sistema maliciosamente. Essa entidade vai querer saber o que pode ter sido feito nos sistemas com esse conhecimento. Saber se houve alguma informação que foi comprometida.

2.3 Gestão de tempo

Muitos dos problemas que são propostos têm diferente grau de dificuldade. Uns que com conhecimentos bastante básicos conseguem-se resolver em poucas horas, depois á outros que requerem realmente uma grande dedicação e tempo da nossa parte. Pessoalmente, eu achei os exercícios relacionados com web mais acessíveis. Por exemplo, explorar vulnerabilidades relacionadas com injecção de código, nomeadamente Structured Query Language Injection (SQL) e Cross-Site Scripting (XSS). Onde tive bastante mais dificuldade, foi nos temas relacionados com criptografia e reversão engenharia. Embora tenha sido autor para resolução do problema do casino para a 31CTF, relacionado com reversão do algoritmo de número aleatórios, outros problemas de reversão perdi bastante tempo sem ter sucesso a encontrar a solução. Até mesmo após ver as publicações de certas soluções [1], vejo-me um pouco perdido com a sua complexidade.

2.4 Motivação

Como todos os problemas são únicos, individualmente a verdadeira motivação aqui é facto de querer adquirir novos conhecimentos. Em termos de grupo, espero um dia a equipa poder marcar na DEFCON que se realiza uma vez por ano. Esta é a verdadeira competição das competições, onde junta milhares pessoas fascinadas pela segurança informática.

2.5 Persistência

Como já foi mencionado anterior, estes problemas propostos têm grau de dificuldade que varia consoante a complexidade do problema. Por vezes, surge caso de estarmos tentar resolver um determinado problema e sentimos que estamos mesmo quase a chegar solução. Foi o que aconteçeu quando estava a fazer o exercício do "saw this" [6] para a competição do ASIS CTF. Passei bastantes horas a entrar descobrir o que fazer com informação que conseguia obter com impressão de variáveis. Infelizmente, acabei por não conseguir resolvê-lo.

2.6 Planeamento

Como esta actividade pode ocupar grande parte do nosso tempo, é preciso saber gerir bem os nossos recursos. É preciso tomar em conta o prazo de projectos e de outras actividades extra-curriculares. Podemos passar horas e horas sem chegar à solução final, enquanto se tivemos usado esse tempo noutra actividade poderia seria um pouco mais produtivo. Digo pouco, porque na verdade a pessoa está sempre a aprender ao tentar resolver um problema portanto nunca é na verdade uma perda de tempo completa. Retira-se sempre algo de positivo para o indivíduo.

2.7 Tomada de decisão

As competições normalmente têm uma duração 48 horas, e o número total de problemas que podem ser resolvidos, entre todas as diferentes categorias, situa-se na ordem dos 20 a 30 problemas. Como é esperar, talvez a melhor decisão a tomar seria por começar resolver os problemas mais fáceis. Até porque as equipas que forem as primeiras a apresentar a solução recebem pontos extra. Os problemas mais fáceis têm uma pontuação inferior ao mais complicados. Mas muitas das vezes estes problemas não são assim tão fáceis como parecem, principalmente quando não estamos confortáveis com determinada categoria. Nestes tem-se de tomar uma decisão rápida para ver se realmente vale a pena avançar profundamente. Não só porque há limite de conhecimento mas o tempo é limitado.

2.8 Trabalho em equipa

Este é um outro factor importante. A própria estrutura biológica do ser humano não permite que indivíduo retenha todo o conhecimento que vai adquirindo ao longo do anos. Assim, ter uma equipa especializada, onde todos os indivíduos são bastantes bons num determinado tema é fundamental para o sucesso. Para estas competições, eu focei-me principalmente nos desafios de web e de reversão de engenharia. São os problemas com os quais mais me identifico/gosto para tentar encontrar a solução.

3 Conclusão

Com a realização desta actividade permitiu-me obter diversas competências não técnicas. Acho que esta actividade é bastante produtiva se uma pessoa realmente gostar do que está fazer. Considero importante e bastante positiva a execução desta actividade, especialmente para quem está associado área da informática. Apreende-se mesmo bastante. Até porque a maioria destes conhecimentos não são muito aprofundados no curso de engenharia informática. Acho que seria importante para qual engenheiro informático ter alguns conhecimentos nesta área.

Referências

[1] "*GitHub - CTFs*," https://github.com/ctfs.
[2] J. Erickson, *Hacking: The Art of Exploitation*. Wiliam Pollock, 2008.
[3] C. Eagle, *The IDA Pro Book*. Wiliam Pollock, 2011.
[4] D. Stuttard and M. Pinto, *The Web Application Hacker's Handbook*. Wiley Publishing, Inc., 2011.
[5] C. Anley, J. Heasman, F. Linder, and G. Richarte, *The Shellcoder's Handbook*. Wiley Publishing, Inc., 2007.
[6] "*ASIS Quals CTF 2015: Saw this -1*," http://blog.tinduong.pw/asis-quals-2015-saw-this-writeup/.

Bio ?