Wrong Template!

SecurityTeam@IST

Mbuku Ditutala

Relatório de Actividades

Abstract—A aquisição de competências extra-escolares é um dos principais objectivos da cadeira de Portfólio IV. Quando se fala de segurança informática a questão é ainda mais abrangente.
O SecurityTeam@IST é um grupo que visa ganhar expertise na área de defesa-ataque, no que a segurança de informática diz respeito.
Este grupo participou de uma competição realizada anualmente - DefCon2015.
Apresentamos neste documento as várias fases pelas quais o grupo passou para competir positivamente no DefCon2015. Os resultados obtidos espelham o quanto esperançosos o team está em poder superar-se cada vez mais. E para mim, foi um ganho total ter participado do grupo.

Index Terms—PortFolio IV, Security, Capture the Flag, CTF, DefCon, Hacking, Exploit, Hopper, IDA Pro, Reverse Engineering, String Format Attack, Attack

extensivo! bastam 5 ou 6!

1 Introdução

Este artigo visa apresentar as actividades realizadas no âmbito da cadeira de Portfólio IV, no presente ano lectivo de 2014/2015.
O SecurityTeam@IST é um grupo constituído por estudantes de informática, espalhados desde estudantes de licenciatura até doutorandos.
A actividade visou a participação do grupo na competição deste ano, 2015, denominada DefCon2015 [1] Nas secções seguintes, deste documento, apresento detatlhes de como foram realizadas cada uma das actividades, sendo que Secção 2 apresentamos as actividades que estive a realizar, na secção 3 consta alguns principais ataques no mundo da web, na Secção 4 contém os detalhes da participação no ASIS CTF QUALS 2015 [2], na secção 5 a participação no DefCon2015, seguida por apresentação dos próximos passos e conclusões, na secção 7.

• *Mbuku Ditutala, nr. 77245,*
E-mail: mbuku.ditutala@tecnico.ulisboa.pt,
Instituto Superior Técnico, Universidade de Lisboa.

Manuscrito recebido em 06 de Junho de 2015.

2 Actividades Realizadas

Dentre as várias actividades propostas pelo corpo docente da cadeira de Portfólio IV, no presente ano lectivo de 2014/2015, decidi fazer parte do Security Team do IST.
Inicialmente as actividades disponíveis foram divididas nas seguintes categorias:

- Actividades Individuais
- Actividades de Grupo

No meu caso, decidi escolher uma actividade individual, neste caso, a SecurityTeam@IST.
A escolha desta actividade deveu-se em parte ao facto de estar a realizar a minha dissertação para o mestrado em Ciber-Segurança. Por outro lado, também contribuiu a minha sempre curiosidade nos temas relacionados ao Hacking.
O coordenador do grupo, o Prof. Pedro Adão, organizou as actividades em duas classes principais:

- Reuniões Semanais de Grupo
- Participação das Competições

2.1 Reuniões Semanais de Grupo

As reuniões semanais decorreram nas instalações do IST-Alameda, na sala 14 do Pavilhão de Informática I; sempre que foram marcadas iniciaram-se por volta das 17H30 e tiveram uma duração de cerca de 60

STAMPED TABLE STAMPED TABLE STAMPED TABLE STAMPED TABLE STAMPED TABLE

	ACTIVITY						DOCUMENT						
(1.0) Excellent													
(0.8) Very Good	Object×2	Opt×1	Exec×4	Summ×.5	Concl×.5	SCORE	Struct ×.25	Ortog×.25	Exec×4	Form ×.25	Titles ×.5	File ×.5	SCORE
(0.6) Good	0.6	0.6	0.6	0.6	0.4		0.4	0.4	0.4	0.1	1.0	0.8	
(0.4) Fair													
(0.2) Weak													

minutos.
Na primeira reunião em que participei o objectivo principal da mesma era a partilha de conhecimentos sobre as principais técnicas e ataques relacionados com Web sites.
Dentre os ataques apresentados, por um dos colegas, foram considerados como mais comuns, os seguintes:

- SQL Injection
- PHP Injection
- XSS - Cross-Site Scripting
- CSRF - Cross-Site Request Forgery
- File Inclusion
- Overflows

2.2 Participação em Competições

O objectivo primário do grupo era participar em mais uma DefCon, isto é, participar da DefCon2015.
A DefCon é essencialmente uma competição entre diversas equipas, das mais diversas naturezas, que vão desde jornalistas, advogados, juristas, informáticos, pesquisadores, estudantes de informática ou de áreas afins, até aos especialistas de segurança e hackers; o objectivo primário é atacar ou resolver problemas propostos pelos organizadores.
A organização da DefCon é anual e decorre em Las Vegas - USA.
Entre as várias provas realizadas numa DefCon, destaca-se a Capture The Flag ou vulgarmente conhecida por CTF.

3 Principais Ataques Informáticos

Nesta secção apresentaremos alguns detalhes, minimalistas, visto não pretender-se fazer deste relatório um descritivo de cada um daqueles ataques.

3.1 SQL Injection

SQL Injection é uma técnica de ataque que visa inserir (injectar) comandos SQL maliciosos através dos campos de preenchimento em formulários Web ou através de URLs.
Como a maior parte dos principais fabricantes de base de dados relacionais usam o padrão SQL-92 ANSI, que é antigo e apresenta muitas falhas de segurança, qualquer pessoa mal intencionada pode tirar proveito dessas falhas e injectar código malicioso ao preencher um formulário em uma aplicação web. Em casos de sucessos esses ataques podem ir desde um simples acesso a informação não autorizada, como senhas até ao derrube ou apagar a própria base de dados.
Para prevenir este tipo de ataques a OWASP [3] recomenda que:

- Parametrizar as Consultas
- Usar Stored Procedures
- Escapar todas entradas fornecidas pelo utilizador
- Limitar privilégios de acesso por utilizador

3.2 PHP Injection

Esta técnica de ataque é em quase tudo semelhante ao SQL Injection, diferindo apenas no facto de que para PHP Injection o código injectado nos campos dos formulários web é um script PHP.
É um ataque muito poderoso naquilo que pode fazer, podendo mesmo o atacante tomar controlo da máquina atacada. Em geral aproveita-se do uso directamente de texto inserido pelo utilizador em comandos PHP sem os sanitizar. Neste caso, o código injectado, código PHP, vai executar-se sobre o servidor web, podendo este ser sucedido, dependendo de outras proteções que o servidor possa ter ou não.

3.3 XSS - Cross-Site Scripting

É outro ataque baseado na exploração da falta de sanitização dos textos passados quer através de campos de formulários bem como através de URLs [4].
O atacante injecta scripts na página infectada, que ao ser executada pelo utilizador o encaminhará para outro sítio, em geral controlado pelo atacante.

Decidi não detalhar os outros ataques, não por serem menos importantes, mas sim apenas por uma questão de gestão de espaço do relatório bem como do tempo.

4 ASIS CTF Quals 2015

Esta actividade teve lugar entre os dias 09/05/2015 e 11/05/2015.
Como esta era efectivamente a primeira competição para mim, minha participação foi essencialemte passiva. Outra coisa que dificultou a minha participação foi o facto da mesma ter sido online.
Entretanto, a nossa equipa conseguiu resolver alguns problemas entre os propostos tendo mesmo obtido uma classificação aceitável, cerca de 101 pontos. O melhor team teve 1801 pontos.

5 DefCon 2015

A competição mereceu um encontro de preparação, onde o coordenador apresentou a estratégia que deveria ser seguida, que passava pela leitura dos resultados dos últimos DefCon (write-ups), instalar e estudar as ferramentas necessárias, IDA Pro, Debbug, Dump de Memória, Assembly Code, Reverse Engineering e Cryptography.
Organizou-se ainda uma spreadsheet no google drive, para partilhar as soluções encontradas para cada um dos problemas apresentados na preparação.
A competição começou no dia 16/05/2015 às 01H00 a.m Hora de Lisboa e terminou no dia 18/05/2015 às 01H00 a.m de Lisboa.
Como sempre foram propostas várias tarefas, sendo que um novo desafio era introduzido assim que algum grupo conseguisse resolver o anterior.
As principais categorias dos desafios ou tarefas apresentadas foram:

- Baby's First
- Coding Challange
- Pwnable utilizador
- Reverse Engineering
- Web
- Miscellaneous Conseguimos ultrapassar cinco desafios que resultaram em 8 pontos. De salientar que um último desafio, da área de Web, não foi apresentada solução atempadamente, o que poderia elevar a pontuação para os 10 valores caso o grupo tivesse apresentado aquele resultado a tempo.

Entretanto nossa classificação final foi o 142º lugar. Nada mal se tivermos em conta que concorreram mais de mil grupos de todas as partes do mundo. Salienta-se ainda que a pontuação dos grupos, excepto o primeiro classificado, é resultante de um rácio entre o total de pontos conquistados pelo grupo e o total de pontos do melhor grupo (grupo com mais pontos).

6 Próximos Passos

No final da minha participação, o professor apresentou os desafios para o próximo semestre, a começar em Setembro próximo e apresentou encourajamento ao grupo no sentido de melhorar-se aperformance do grupo para as futuras participações.
Foram identificados os pontos fracos e os pontos fortes do grupo. Tendo coordenador apresentado um estudo comparativo entre a nossa participação e de outros grupos, acima do nosso, do qual se pôde claramente ver que temos vantagens em algums tipos de problemas em comparação com grupos que ficaram melhor classificados nesta competição. Apontou por isso, como meta para a próxima competição a melhoria das valências do grupo naqueles campos que não foram bem sucedidos e melhorar ainda a performance (sobre tudo timing) na resolução dos problemas das áreas de nosso domínio.

7 Conclusão

Participar de DefCon foi um prémio para a minha formação, por tudo o que aprendi no pouco tempo que durou a minha participação. Quer a DefCon quer o ASIS Quals foram actividades que permitiram-me aumentar os meus conhecimentos na área de segurança informática, mas particularmente nesta área de Ataque-Defesa.

Agradecimentos

Agradecer primeiramente à Deus (Todo-Poderoso) por ter-nos dado vida e a oportunidade de participar deste cadeira.
Agradecemos ainda a iniciativa do Prof. Rui Cruz em incluir esta classe de actividades

no leque daquelas que foram as actividades propostas neste semestre.
Gostaria também de agradecer e encorajar o Prof. Pedro Adão, na criação do grupo de Segurança do IST; por fim agradecer à todos os colegas que comigo partilharam aqueles momentos de magia, no que a segurança informática diz respeito.
E um bem haja à todos nós.

REFERENCES

[1] G. DEFCON. (2015, May) Defcom@hacking conference. [Online]. Available: https://www.defcon.org/html/links/dc-ctf.html
[2] ASIS. (2015, May) Asis cyber security context. [Online]. Available: http://asis-ctf.ir/scoreboard/
[3] F. OWASP. (2015, May) Owasp. [Online]. Available: https://www.owasp.org/index.php/SQL_Injection_Prevention_Cheat_Sheet
[4] ——. (2015, May) Owasp. [Online]. Available: https://www.owasp.org/index.php/XSS