HamiD Rezaei

Mashhad • Iran • +98 9150670783
aha@4xmen.ir / hamid@offsec.ir • www.4xmen.ir / www.offsec.ir

Summary:

I became familiar with the concept of RCE in 2007. A few years later in 2010, I wrote a comprehensive e-book about the Olly Debugger in Persian. At the same time, I began to analyze malwares such as Ramnit.h, Alman.NAB, some Ransom ware, etc. and created Anti to clean infected systems. I wrote my BOF e-book in 2009 that started my activity in the software exploiting. Software exploiting interesting to me. Therefore, I did research on the security mechanisms like DEP, ASLR, SEHOP, etc , So I learned ways to bypass them and results presented at the SoftSec2014 conference in an essay called "*Propose a partial solution against ROP technique*". I obtained CCNA certification from Sharif University of Technology that started my activities in field of network attacks and routing protocols by python coding. RSA and AES/RIJNDAEL algorithms in cryptography science attracted my attention then I worked on the analysis and attacks on them.

I believe this sentence, *There are always things to learn.*

Work Experience:

Freelancer
Computer Security Specialist 2012 to 2015

Education:

2013	Jihad University of UAST *B.S. Degree - Computer Software Engineering*	Bojnourd, North kh.
2012	Training Department of Sharif University *CCNA (Cisco Certified Network Associate)*	Certification No. 91-07-2325
2010	Profs. Hesabi College Boys *Associate's Degree, Computer software*	Shirvan, North kh.
2008	Mahmoudieh *Technical Diploma(2nd and 3rd), Computer*	Quchan, Razavi Kh.

Skills:

Programming

Able to code custom tools and scripts related to databases, RCE and network using Delphi, Assembly and Python such as fuzzing, fuzzer and using SCAPY, Sulley, PyDBG and other modules.

Network

Capable of handling all layer 2 attacks/defense and other layers, router hardening, security at routing protocols such as OSPF,BGP,RIP. Familiar with TOR network, Onion Routing and user anonymity. Able to implement different attacks in network and develop new tools for different/new attacks when necessary.

Cryptography

Analyze cryptography methods like RSA and AES used in packet encryption in malwares. also able to analyze custom cryptography functions like custom XOR.

Forensics

Experience in handling different file formats like ZIP,DOC,DOCX,JPG, etc. and also able to analyze memory dumps for malwares and vulnerabilities.

Malware Analysis

Analyze different type of malwares and find out custom methods they are using on Windows, Android.

Vulnerability Analysis

Analyze vulnerabilities in binary files in both kernel and user mode.

Publications:

How to buffer overflow and exploiting - 2009
My e-Book is about buffer overflow vulnerability and how to exploit it, also this paper describes some problem and solution with techniques in exploiting.

A new attack on link-state database in open shortest path first routing protocol - 2014
Published in JEEE journal, Journal of Electrical and Electronic Engineering.

Comprehensive OllyDBG Learning 2nd Edition - 2010
Private Publication : 2010
Public Publication : 2013

Security in cloud computing - 2013
Published in national conference on creativity on computer engineering and information technology of Tonekabon.

New attack on LSDBs in OSPF Routing - 2013
Oral presentation in 8th SASTECH (CNMSecure), 8th symposium on Advance in science & Technology. Presented in Ferdowsi university of Mashhad.

Security in Link-State Protocol-Introducing specific vulnerability - 2013
Oral presentation in national conference on emerging trends in engineering and computer retrieval of information.

Experimental study and propose a partial solution against ROP technique - 2014
Published in System and Application Security conference A.K.A. SoftSec held by University of Shiraz.

Discovered a new hole in OSPF routing protocol OSPF ver 2,3 - 2013
Oral presentation in 16th national association of electrical engineering conference.

Security of link state routing protocol - 2013
Oral presentation in sixth e-business system conference held by Aamirkabir University of Technology. Accepted as a best paper at Network Security & Cyber Passive Defense panel.

Subvert windows, bypass Security measures - 2014
Oral presentation in seventh e-business system conference held by Aamirkabir University of Technology. It's about software exploiting in two modes on MS-Windows family OS (user-mode and kernel-mode).

Awards:

- Ranked 1st at HackIM Nullcon Ninjas 2014 Qualification Round (Couldn't participate at final round due to visa issue) and got VIP Pass for Nullcon2014 Conference.
- Accepted as a Best Paper at the sixth International conference on E-Business System held by Amirkabir University of Technology, Tehran Polytechnic in 2013
- Ranked 1st at NSEC CTF Qualification round (Isfahan Hacking Contest held by Isfahan University of technology) in 2013
- Ranked 4st at Forth national hacking contest held by Sharif University of Technology in 2013
- Ranked 2st and prized at NSEC CTF Final Round (Isfahan Hacking Contest held by Isfahan University of technology) in 2013
- Presenter at Malwares Analysis workshop, Jihad University of UAST North Kh. in 2015

References:

Publications and references available upon request.

contact information :