Hay Mizrachi

MAMRAM graduate, Cyber and information security expert, specialist in Penetration Testing, Red Teaming projects (a strong Active Directory and OSINT background knowledge), Code Review and Security Research. Graduate Computer Science at The College of Management Academic Studies (B.Sc), and Practical Engineering at Computer Software.

Rishon LeZion,
Israel
(050) 8841480
haymizrachi@gmail.com
LinkedIn:
https://linkedin.com/in/hay-mizrachi/

EXPERIENCE

Security Researcher — Noname Security, Start Up

Jan 2022– PRESENT

Offensive Security Researcher & Penetration Tester, Technical Leader — OTORIO, Start Up

May 2019 – Jan 2022

Taking part of the Offensive Security Team at OTORIO, which responsible for conducting Web PT engagements, Vulnerabilities Research and Red Team (External & Internal) simulations and attacks for various of OT customers: Cruises, Pulp & Paper, Electricity, and grids powers industries and more:

- Internal Active Directory and External Applications and Infrastructure engagements – Performing internal AD reconnaissance in the network, gaining Domain Admin privileges, Privilege Escalation and Lateral Movement, Cross-Trusting abusing, Kerberos attacks (Kerberos User Enumeration, Kerberoasting, AS-REPs Roasting, GPP) and NTLM authentication (NTLM Relay, Offline Cracking), Using built-in tools and public tools (BloodHound, Powerview, Pingcastle, Impacket, ACL Abuse and Public Exploits – ZeroLogon, MS14-068, BlueKeep and MS17-010) and more.

- On Site of silently Red Team projects on physical cruises worldwide abroad including physical security attacks – WiFi scenarios, tunneling and captive portal bypasses, MiTM, and more.

- Interview of new candidates for the PT team –including phone calls, physical and internet-online technical interviews with my personal manager including performing exams of infrastructure and application attack scenarios.

- Conduct vulnerability research of new vulnerabilities in the SCADA industry and perform CVE's submission of them of various SCADA and OT products and solutions such as: Siemens, MBConnect, B&R Automation, and more.

SKILLS

Cyber Security Red Team, Penetration Testing, Code Review, Malware Analysis, Web Application Security, Network Architecture, System Architecture, C, Assembly, Win32API, Web Application Development, Active Directory.

AWARDS

3st Place, Mafat Hackathon - HacknProtect (2017):
https://www.globes.co.il/news/article.aspx?did=1001196885

Courses - John Bryce

- C Attack and Defense
- Introduction to Cyber Warfare
- Ream Team Expert
- אנטומיה של תקיפה
- Partly CCNA (During practical engineering)

LANGUAGES

Hebrew
English

- Research and Development of attacker's methodology for the team (junior and senior candidates as well) of new internal and public attacking tools, OSINT reconnaissance, Quiet Red Team methodology, Web-Application methodology, tunneling techniques, and more.

- Writing final PT reports in English including all the scenarios, mitigation attacks, and executive summary for the clients and supporting them all along the way.

- Training new employees in the team for our internal attacking methodologies as a baseline for their daily basis working.

- Presenting webinars of technical vulnerabilities for conferences in the SCADA industry.

- Conducting public OSINT / WEBINT reconnaissance for Threat Intelligence reports in order to expose the external surface and internet leaks of customer companies on the Internet.

- Performing Code Review projects in order to find vulnerabilities directly in the source code and mitigate against them for a several of project categories.

Pentester Member at Red Team — Mamram Unit, IDF

June 2015 – May 2019

Taking part of the Red Team at Mamram, which conduct penetration testing engagements for internal IDF systems and solutions in web application and infrastructure projects:

- Performing Penetration Testing jobs for projects, in Whitebox and Blackbox methods with OWASP methodology and PTES:
    - Using information gathering techniques, set attack vectors on systems, writing final architecture.
    - Using Kali distribution and public tools such as Burp Suite, Nmap, Metasploit, tcpdump, wireshark, public exploits, and more.
    - Using methods of Post Exploitation such as Privilege Escalation and Lateral Movement, and persistence techniques backdoors.
- Write private tools and automations for internal using in the team
- Write a PT methodology learning for new beginners soldiers to get into the team.
- Writing final PT Reports which show the potential impacts to the system, and suggest solutions to reduce the risk.
- Writing application and network security architectures documents for application and infrastructures systems before entering into the Data Center:
    - Experience with Data Filter networks solutions between different types of networks such IBM DataPower, WAF, Firewall - Rules, Black and White Lists, ports and types of secure protocols.
    - Writing High Level Visio Architectures for projects and systems.

- Performing Basic Reverse Engineering for Malware executables and writing Win32API malwares POC's to training the SOC and the Blue teams:
    - Using tools such as IDA Pro, Ollydbg, Hex Editors, play With Memory Forensics, Hard Disk, Obfuscations encoders and signatures, Registry components, and Anti Virus Evasion.
      Using Anti Debugging and Anti Virtualizations techniques.
- Performing Security Research on SCADA systems, starting from information gathering until conducting research on dedicated network protocols and sensors to get remote code execution.

Lecturer for Computer Science — Ort Singalovski

Jan 2015 - June 2016

Lecturer for Computer Science for Practical Engineering students at courses of:

1. Low Level Programming in C and Assembly languages.

2. Web development projects - Javascript, HTML, CSS, and more

Pentester Member, CyberHat

Jul 2013 - Oct 2013

Penetration Tester in Web Application projects.

Starting before Army service, through my studies at Practical Engineering as a student.

Frontend Web Developer, Tel Aviv University

June 2011 - Sep 2011

Responsible for managing and inserting contents to the Summer Camp site for Tel Aviv University campus.

Working in Front End languages - such as HTML, CSS, Javascript, and Wordpress CMS platform.

EDUCATION

The College of Management, Rishon LeZion - B.Sc. in Computer Science

Cyber Security Specialization, GPA 86

2016-2019

Ort Singalovski, Tel-Aviv - Software Practical Engineer

2013-2015

95, Excellent

PROJECTS

B&R MBConnect Remote Access Solutions Vulnerabilities Disclosure— *2021*

Multiple vulnerabilities found in MBConnect Remote Access Solution:

ICS Advisory link: https://cert.vde.com/de-de/advisories/vde-2021-003

https://www.otorio.com/blog/otorio-s-pen-testers-discovered-more-than-20-vulnerabilities-in-a-popular-industrial-remote-access-solution/

https://www.industrialcyber.co/article/security-gaps-found-in-mbconnects-industrial-remote-access-offering/

CVE-2020-35557 - Improper Privilege Management

CVE-2020-12527 - Improper Privilege Management

CVE-2020-12528 - Improper Privilege Management

CVE-2020-35570 - Files or Directories Accessible to External Parties

CVE-2020-35558 - Server-Side Request Forgery (SSRF)

CVE-2020-12529 - Server-Side Request Forgery (SSRF)

CVE-2020-35560 - Open Redirect

CVE-2020-12530 - Cross Site Scripting (XSS)

CVE-2020-35563 - Cross Site Scripting (XSS)

CVE-2020-35564 - Cross Site Scripting (XSS)

CVE-2020-35569 - Cross Site Scripting (XSS)

CVE-2020-35566 - Local File Inclusion (LFI)

CVE-2020-35559 - Denial Of Service (DOS)

CVE-2020-35568 - Sensitive Information Disclosure

CVE-2020-35567 - Shared Password

CVE-2020-35565 - Insecure Default Initialization of Resource

CVE-2020-35561 - Server-Side Request Forgery (SSRF)

CVE-2020-10384 - Improper Privilege Management

B&R GateManager and SiteManager Vulnerabilities Publication — *2020*

Multiple vulnerabilities found in B&R GateManager and SiteManager remote access solutions.

ICS Advisory link: https://us-cert.cisa.gov/ics/advisories/icsa-20-273-03

CVE-2020-11641 - SiteManager Local File Inclusion Vulnerability

CVE-2020-11642 - SiteManager Denial of Service via Local File Inclusion Vulnerability

CVE-2020-11643 - GateManager Information Disclosure Vulnerability

CVE-2020-11644 - GateManager Audit Message Spoofing Vulnerability

CVE-2020-11645 - GateManager Denial of Service Vulnerability

CVE-2020-11646 - GateManager Log Information Disclosure Vulnerability

Published officially by B&R Automation:

https://www.br-automation.com/downloads_br_productcatalogue/assets/1600003183751-de-original-1.0.pdf

Published by the press :

1. https://thehackernews.com/2020/10/industrial-remote-access.html
2. https://securityaffairs.co/wordpress/108991/hacking/industrial-remote-access-systems-flaws.html
3. https://www.infosecurity-magazine.com/news/flaws-found-in-remote-access/
4. https://thecybersecurity.news/general-cyber-security-news/critical-vulnerabilities-found-in-remote-access-software-2199/

Project Researchers:

Nikolay Sokolik and Hay Mizrachi of OTORIO reported these vulnerabilities to CISA.

MBConnect Vulnerabilities Publication — *2020*

Multiple vulnerabilities found in MBConnect remote access solutions.

ICS Advisory link: https://us-cert.cisa.gov/ics/advisories/icsa-20-273-01

CVE-2020-24568 - Blind SQL injection on mbConnect service

CVE-2020-24569 - Blind SQL injection on mbConnect service

CVE-2020-24570 - SSRF/CSRF on mbConnect service

Project Researchers:

Alik Koldobsky, Ofir Manzur, Hay Mizrachi, Nikolay Sokolik, and Haviv Vaizman from OTORIO reported these vulnerabilities to CISA.

Offical publication by VDE CERT:
https://cert.vde.com/de-de/advisories/vde-2020-035

https://thehackernews.com/2020/10/industrial-remote-access.html

https://www.otorio.com/news-events/press-release/otorio-discovers-critical-vulnerabilities-in-leading-industrial-remote-access-software-solutions

SIEMENS vulnerability research — *2019*

Exposed new SCALANCE X-200 OT switch family model versions that also affected to the current vulnerability for CVE-2013-3633.

Vulnerability Details:

The user privileges for the web interface are only enforced on client side and not properly verified on server side. Therefore, an attacker is able to execute privileged commands using an unprivileged account.

Siemens thanks the following parties for their efforts:

• Hay Mizrachi from OTORIO for reporting CVE-2013-3633 also for Scalance X-200 switch family

https://cert-portal.siemens.com/productcert/pdf/ssa-170686.pdf

https://www.us-cert.gov/ics/advisories/ICSA-13-149-01

Vulnerability research on a WIFI Repeater — *2017*

A vulnerability research on a common consumer WIFI Repeater.

CVE submissions:

1. CVE-2017-13713 (Remote Code Execution) -

https://nvd.nist.gov/vuln/detail/CVE-2017-13713

2. CVE-2017-8770 (Local File Inclusion Vulnerability) -

https://nvd.nist.gov/vuln/detail/CVE-2017-8770

3. CVE-2017-8771 - https://nvd.nist.gov/vuln/detail/CVE-2017-8771

4. CVE-2017-8772 - https://nvd.nist.gov/vuln/detail/CVE-2017-8772

Exploit-DB Publications:

https://www.exploit-db.com/exploits/42547/ - Wireless Repeater BE126 - Local File Inclusion

https://www.exploit-db.com/exploits/42608/ - CVE-2017-13713 - Command Injection through HTTP

Publications

Digital Whisper Magazine —

Anti Virtualization - טכניקות לזיהוי וירטואליזציה בפוגענים

2016

https://www.digitalwhisper.co.il/files/Zines/0x45/DW69-1-AntiVirtualization.pdf

Don’t Repeater Me - חלק א', איך הבסנו רכיב תקשורת מסוג מגדיל טווח

2017

https://www.digitalwhisper.co.il/files/Zines/0x56/DW86-1-RepeaterHack.pdf

Volunteer Experience

Adult Medic at Magen David Adom

2010-2015

I volunteered from age 16 in high school until the start of my IDF military service.