Ankur Tyagi

InfoSec Enthusiast

[Cell: +91 819 777 2634 | Mail: 7h3rAm]

[GitHub: 7h3rAm]
[Twitter: @7h3rAm]
[Linkedin: ankurstyagi]
[Blog: 7h3ram.github.io]

SUMMARY

I'm an enthusiastic and dedicated professional with a strong technical background in the field of information security. I've a solid combination of skills and knowledge that includes Advanced Persistent Threat analysis, exploitation, reverse engineering, protocol/file-format decoding/analysis and vulnerability assessment.

I've excellent presentation, interpersonal, analytical and problem-solving skills. I'm skilled in applying analytical and technical knowledge to produce practical solutions. I can deliver results and can manage multiple projects simultaneously, unsupervised, in a fast-paced and rapidly evolving environment. I've a strong interest in research and solving complex technical issues.

PROFESSIONAL EXPERIENCE

Software Engineer, Juniper Networks, Bangalore *April 2012 – Present*

- Ensuring coverage against latest vulnerabilities and exploits through signature development for Juniper's security portfolio devices.
- Regular updates of active signatures to ensure coverage against evolving IDS/IPS evasion techniques as well as for quality assurance.
- Testing and updates of in-house automation tools that help with coverage analysis against various exploitation frameworks.
- Vulnerability analysis, assessment, exploit testing and threat prevention.
- Contributing towards research activities that help with product enhancements.

Information Security Engineer, SecurView Systems, Pune *December 2010 – April 2012*

- Security Analyst for the Cisco Security IntelliShield Alert Manager Service.
- Involved in vulnerability research, exploit development, testing and verification.
- Active member of the Secur-I research group with activities involving monthly publication of critical vulnerability assessments (available here) and concentrated vulnerability research.

Member of Technical Staff, AirTight Networks, Pune *August 2010 – November 2010*

- Responsible for handling technical issues with AirTight Network's wireless IDS/IPS offering, SpectraGuard.
- Modeling and planning of RF installations for customer sites with Intrusion Detection, Intrusion Prevention and Device Location Tracking support.

SPECIALITIES

- Malware Analysis (Static/Dynamic, (un)?pack - manual/automated, {web, file}-based)
- File-Format Decoding and Analysis (PDF/Flash/OLE/JAR/PE)
- Protocol Decoding and Reversing (nc, tcpdump, wireshark, scapy)
- Memory/Network Forensics (Volatility, libnids)
- Generic Reverse Engineering (GDB, objdump, ImmDbg - immlib, IDA Free)
- Exploitation (Stack, Heap, SEH, DEP/ASLR Bypass, ROP, UAF, InfoLeaks)
- Automation Scripting (Python, JavaScript, Shell, Batch, PowerShell)
- Programming/Development (C, C++, Java, VB, Python, ASM - x86(_64)?, Win32, Linux – IPC/Socket/Kernel)

TECHNICAL SKILLS

Platforms

- Windows: 2003, XP, Vista, 2008, and 7 .... 0 1 2 3 4 5 6 7 [✓ 8] 9
- *nix: Fedora, Arch Linux, Ubuntu, FreeBSD and Solaris .... 0 1 2 3 4 5 6 7 [✓ 8] 9
- Routing/Switching: Cisco IOS, Juniper Junos and Vyatta .... 0 1 2 3 4 5 6 7 [✓ 8] 9

Programming/Scripting

- x86 Assembly, C/C++, Java, Python .... 0 1 2 3 4 5 6 7 [✓ 8] 9
- PCRE/DFA and Bash (PERL, SED, AWK, GREP, Expect/TCL) .... 0 1 2 3 4 5 6 7 [✓ 8] 9
- Basic understanding and reasoning with VB/JavaScript/Ruby .... 0 1 2 3 4 5 [✓ 6] 7 8 9

Networks and Security

- Packet Sniffing/Crafting/Injection .... 0 1 2 3 4 5 6 7 [✓ 8] 9
- IDS/IPS Signature Development and Testing .... 0 1 2 3 4 5 6 [✓ 7] 8 9
- Protocol Decoding and RFC Compliance Testing .... 0 1 2 3 4 5 6 [✓ 7] 8 9
- Vulnerability Research, Analysis and Assessment .... 0 1 2 3 4 5 6 7 [✓ 8] 9
- Patch Analysis, Binary Diffing and Reverse Engineering .... 0 1 2 3 4 5 6 [✓ 7] 8 9

Attack Vectors

- File Format Exploits .... 0 1 2 3 4 5 6 7 [✓ 8] 9
- TCP/IP Attacks – Spoofing, MitM and DoS .... 0 1 2 3 4 5 6 7 [✓ 8] 9
- Stack/SEH Overflows, Return-to-Libc, Format Strings .... 0 1 2 3 4 5 6 7 [✓ 8] 9
- Bypassing /GS, /SafeSEH, /NXCOMPAT and /DYNAMICBASE .... 0 1 2 3 4 5 6 [✓ 7] 8 9
- Web Applications – XSS/CSRF/ActiveX/SQL Injection .... 0 1 2 3 4 5 [✓ 6] 7 8 9

CERTIFICATIONS

GIAC Penetration Tester – GPEN (SEC 560), SANS

License ID: 7545 *March 2012 – March 2016*

Certified Ethical Hacker – C|EH v7 (312-50), EC-Council

License ID: ECC949105 *May 2011 – May 2013*

Cisco Certified Network Associate – CCNA (640-802), Cisco Networks

License ID: CSCO11172762 *January 2010 – January 2013*

OCW/MOOC CERTIFICATIONS

Malicious Software and its Underground Economy: Two Sides to Every Story **Coursera - University of London International Programmes**

Score: 100%, Distinction *July 2013*

An Introduction to Interactive Programming in Python **Coursera - Rice University**

Score: 90.8%, Distinction *December 2013*

Internet History, Technology, and Security **Coursera - University of Michigan**

Score: 94.6%, Distinction *December 2013*

ACADEMICS

Birla Institute of Science and Technology, Pilani

Master of Science, Software Systems *January 2013 – December 2014 (Expected)*

D. Y. Patil College of Engineering, University of Pune, Maharashtra

Bachelor of Engineering, IT (First Class – 65.8%) *August 2007 – June 2010*

B. S. D. Polytechnic, MSBTE - Mumbai, Maharashtra

Diploma, IT (First Class – 71.4%) *July 2005 – June 2007*

Awarded for securing First position in Final Year – June 2007