
Mickey Lasky

GCFA RHCE CEH

4079 Britwell Place, Fairfax, VA 22033

(703) 942-9156 | mickey@ita.org

Senior Security Analyst | INFOSEC Engineer | Forensics Analyst

Technical Expertise

Operating Systems	Microsoft Windows (XP, Vista, 2003, 2000), Linux, Solaris
Hardware	Nokia Firewalls (IP330, IP1260, IP1280, IP2450), McAfee Network Security Platform (formerly Intrushield IPS), McAfee Data Loss Prevention Monitor (formerly Reconnex iGuard Monitor), Solera DS3150 Forensics Capture Appliance, Solera DS Storage Appliance, VOOM HardCopy II, Tableau USB Forensic Bridge, Network Critical Network Taps, Cisco switches/routers, Cisco PIX 515/ASA 5520
Software	Check Point Firewall-1/VPN-1 NG/NGX, Check Point SecureClient/SecuRemote, Nokia IPSO 4.2/6.0/6.1, Metasploit, nmap, Wireshark, Network Observer, Tenable Nessus, Snort, tcpdump, Netflow, iptables, Paros, Acunetix Web Vulnerability Scanner, honeypots
Forensics	AccessData Forensic Toolkit 1.x/2.x, X-Ways Forensics, Guidance EnCase 4.x, Autopsy Forensic Browser, The Sleuth Kit (TSK), Windows Forensic Toolkit, RegRipper, Volatility, SANS SIFT Workstation, Foremost, Scalpel, Sysinternals Suite

Professional Experience

Georgetown University, Washington, DC, May 2005 – Present

Senior Security Analyst

Re-create the University Information Security Office. Oversee day-to-day information security operations with junior analysts. Perform security architecture reviews, vulnerability analyses, penetration tests, and risk assessments for University organizations and IT projects. Perform incident response and forensics for security breaches and litigation support. Act as a tier 3 escalation contact for University help desk services.

Accomplishments:

- Project management, design, implementation, and management of main campus border HA VPN Nokia firewall cluster, main campus data center HA Nokia firewall cluster, School of Foreign Service in Qatar HA Nokia firewall cluster, and disaster recovery site Nokia firewall.
- Design, implementation, and management of campus-wide McAfee Data Loss Prevention Monitor (formerly Reconnex iGuard) system.
- Design, implementation, and management of campus-wide McAfee Intrushield Intrusion Prevention System.
- Design, implementation, and management of Solera DS Series Network Forensics Appliance.
- Assisted in the reviewing and securing of over 500 University servers in order to move the campus network to a default deny security stance.
- Performed forensics on a 2006 data breach that directly led to arrests and prosecution by Federal authorities.
- Managed the University Information Security Office student internship program.
- Guest lectured for computer science classes on the topic of Information Security.

Mickey Lasky

Computer Associates, Herndon, VA, May 2004 – May 2005

Security Specialist

Deployed and operated the Managed Vulnerability Service (MVS) and Vulnerability Operations Center (VOC). Worked with clients to integrate the CA Unicenter suite into their existing environments to mitigate security threats. Create and distribute impact analysis reports to clients on existing and emerging security vulnerabilities.

Accomplishments:

- Built the MVS Vulnerability Operations Center from scratch to support the newly launched MVS service.
- Configured, deployed, and managed Juniper Netscreen 204 and 5GT firewalls in a VPN configuration to support secure communications between the MVS VOC and client sites.
- Successfully deployed CA Unicenter to act as a patch management infrastructure for a large government agency supporting thousands of workstations simultaneously.

Counterpane Internet Security, Chantilly, VA, January 2003 – May 2004

SOC Engineer

Perform technical operations in a 24x7x365 Security Operations Center environment. Monitor third-party news sources to develop emerging security trends. Develop, write, and distribute Intelligence Objects (security reports and updates) to keep clients up to date on threats that may affect them. Perform incident response for clients. Manage client security monitoring devices.

Accomplishments:

- Part of the first team to detect the SQL Slammer outbreak before it became public and advised clients on how to remediate the threat.

Education/Certifications

Bachelor of Arts in Broadcast Journalism, The American University, 1994

SANS GIAC Certified Forensic Analyst (GCFA) #4598

Red Hat Certified Engineer (RHCE) #805009840838122

EC Council Certified Ethical Hacker

Registered Virginia Private Investigator DCJS #99143477

Check Point Certified Security Instructor

Check Point Certified Security Administrator vNG

Check Point Certified Security Engineer vNG plus Enterprise Integration and Troubleshooting

Merits/Achievements

Volunteer of the Year 2005, Fairfax County Animal Services Division, FCPD

Placed 4th in the 2006 DC3 Forensics Challenge

Passed Bureau of Alcohol, Tobacco, and Firearms SSBI investigation

Professional Memberships

Private Investigators Association of Virginia (PIAVA)

Mickey Lasky

- 2 -