NETWORK ENGINEER

Career Overview

Seeking network security or operation position. My goal is to continue working in the computer security field, by improving a company's security infrastructure posture. i enjoy working with teams with a strong sense of ethics and commitment on quality and delivery. I have hands-on expertise on Sourcefire/Snort and other IDS/IPS products like, tuning, deployment, technical support on all aspects at data centers, and/or it security centers. Since 2000 I have had the opportunity to work with multiple security products, commercial and open source. i.e.: Sourcefire, Snort, McFee NSP + ePO, Peakflow, Arcsight, Splunk, Netscout, Tripwire, Dragon, NFR, network taps (dump and intelligent), Cisco, Nagios, MRGT, Apcon (matrix aggregator switches), Proxies, Load Balancers (Citrix, F5), Checkpoint, Blue Coat, Fortinet, Guardian, Nmap, Nitko, Metaexploits, backtrack, cain and abel, saint, and satan. and other Department of Defense classified security products. Qualifications Summary Type Description Equivalent Years

Qualifications

Familiar with Linux/Unix command line tools/environment. Basic Unix system administration skills Knowledge of TCP/IP networking Several years customer service experience

Technical Skills

Skills	Experience	Total Years	Last Used
Linux/Unix OS	Medium	15 years	current
McAfee Intrusion Detection System	Medium	1	Feb-2015
Sourcefire IDS	Expert	8	current
McAfee ePO DLP	Medium	1	Feb-2015
Splunk	Medium	2	Feb 2015
Packet Analysis WireShark	Medium	10	Feb 2015
Incident Analysis	Medium	10	Feb 2015

Accomplishments

* Discovery of Compromised servers with malicious activity.

* Discovery of Policy violations activity.

* Mentor junior Security Analysts

* Provide management and network engineer a better understanding of security postures.

Work Experience

Network Engineer Star2star Communications Huntsville , AL

- Deployed Network Operations Center (Small business), by installing and configuring a Windows 2000, and 2003 servers, with Exchange server 2003, IIS 6.0 web server, and CRM.
- Install a Linux box for Blog Wiki experiment.
- Configure a Cisco PIX 506e firewall, and Fortigate firewall.
- Install and configure a wireless enterprise 3Com access point with antenna.
- Oversee and maintain the small business network operations.

Computer Analyst Louisiana State University Baton Rouge , LA

- Location: DoD, TRANSCOM, SDDC.
- Alexandria, VA.
- Tested patches of the Worldwide Port System (WPS-Oracle based) application running under various HP-UX (Unix 10.5 and 11.0) releases and Windows 2000 server platforms.
- Configured and tested peripherals attached to these operating systems (printers, bar code scanners, etc).
- Responsible for providing 2nd Tier UNIX Engineering Technical support for the WPS 24x7 for their UNIX systems, which required strong knowledge of UNIX systems and Windows 2000 and 2003 servers.
- Review system logs of each UNIX and Windows servers, and prepare twice a day a report for management to report any reportable issue and its resolution.

Security Analyst L2 08/2010 to 02/2015 Jacobs Engineering Group Inc. Jacksonville , FL

- Maintain uptime, performance, reliability, and updates across al data centers IPS/IDS appliances (Sourcefire, etc.
- McAfee NSP) infrastructure and network Taps (NetOptics) and ApCon (switch-port aggregators) appliances.
- Work with ArcSight, Splunk, ePO & DLP, NetScout engineers integration with the IPS/IDS platform.

Intrusion Detection Analyst 01/2007 to 04/2007 Arch Capital Group Ltd. Los Angeles , CA

- Experience in network protocols & packet analysis.
- Familiar with shell & perl, scripts Performed intrusion detection analysis for different Federal agencies like DHS-TSA, and Census Bureau.
- Prepared daily intrusion detection reports for team leads.

- Monitor real-time using Arcsight, network traffic anomalies for any indication of malicious activity.

Senior Network Engineer 01/2005 to 01/2007 Leidos Holdings Inc. Frisco , TX

- Aberdeen Proving Ground, CIMP Supports the Center for Intrusion Monitoring and Protection (CIMP), which include both the Army Material Command's Computer Security Incident Response Team (CSIRT) and the High Performance Computing (HPC) Computer Emergency Response Team (CERT).
- Operates the Army Research Laboratory tool suite including the NIDS system, Snort and Courtney.
- Monitors in real-time several networks for intrusion attempts and attacks using the current ARL CIMP software tool set.
- Responsible for a large array of administrative duties such as daily task management, responding to reported incidents (which often requires coordination of activities through multiple agencies and sites), and preparing and conducting meetings detailing current incident status to customers and team members.
- Called upon to initiate and monitor router blocks across the DREN network to counteract hostile activity.
- Creates the "shell" for and conducts initial reviews of several of the Standard Operating Procedures (SOPs) and documentation including daily and weekly reports.
- Prepares and distributes reports on current vulnerabilities and/or any situational information to customers.
- Provides retrospective analysis for the CIMP using the current database to track trends for intelligence purposes.
- This information is used to determine new exploits and an increase in hostile activity along with being used to create a list of hostile IP's for tracking purposes.
- Once compiled this information can be given to the analyst to ensure a more thorough examination of all network traffic for new exploits and hostile computer users.
- Provides support for criminal investigations by providing After Action Reports and coordinating information with relevant organizations including CID, DoDCERT, ACERT, NAVCIRT and AFCERT.

Information Assurance Engineer 01/2004 to 01/2005 Asrc Federal Holding Company North Charleston , SC

- Compile a Security Test & Evaluation (ST&E) document, a Penetration Testing Plan, a Risk Assessment plan for the US Department of Labor-Office of the Chief Financial Officer for their HR and Payroll system.
- In addition, was responsible to execute the Penetration Testing plan as well as the ST&E.
- Deployed a 2003 Windows servers, with the following requirements: Share point server, ISA 2004 server and SQL server.

IDS Network Engineer 01/2003 to 01/2004 Apex Systems Conshohocken , PA

- Perform real-time IDS analysis and technical engineering support to the Army DOD IDS team.
- Prepare daily incident report using the following security tools: NetForensics, Bro (IDS), Argus (IDS), Snort (IDS), Stealth Watch (Advanced Threat Management), Peakflow X (Network Management Threat tool), ISS Real Secure (IDS), and Remedy (Reporting).
- Provide forensic technical support during the course of the incident.
- As an IDS analyst, frequently you call to assist others in the resolution of incidents, such as assisting forensics staff, firewall staff, and other security personnel.
- Provide documentation for training of new staff and/or senior management about the status of IDS project.
- This was done on a weekly basis.
- Recommend blocks of addresses that represent a threat to firewall/route group.
- Site requires 24/7 real-time monitoring and working diverse shifts and be on-call.
- Set-up and maintain IDS sensors and tuning, and push new signatures.
- Compile trends, forensic, reporting analysis of intrusion activities.
- IDS product was DRAGON, which is a UNIX/LINUX based product; this mandated a complete command of UNIX/LINUX knowledge.
- Develop (LINUX/UNIX) scripts for IDS log data manipulation, i.e.
- reduce False/Positives, look for potential threats, illegal company policies activities.
- Maintain a CVS of emerging threats (or events) with other government CERT groups.
- Recommend IDS and network security changes.
- Execute Vulnerability assessment with Nessus and ISS scanners.

Network Security Engineer Consultant 01/2002 to 01/2003 M&T Bank City , STATE

- Work at AllFirst bank as a consultant at their Information Security Division, deploying IDS (Dragon 6.0), in its enterprise network.
- Perform 24/7 real-time IDS monitoring on the client site.
- Prepare a daily incident report to management, and made recommendation of how to mitigate these incidents or threats.
- Once months compiled and prepare a monthly report for the Audit Department of the bank.
- Installing and configuring IDS sensors, and analyzing signatures.
- Provide trends, forensic, reporting analysis of intrusion activities.
- Developing scripts for IDS log data manipulation, i.e.
- reduce False/Positives, trace potential threats, illegal company policies activities.
- Recommend IDS and network security changes.

Network Security Analyst 01/2000 to 01/2002 CACI International City , STATE

- CACI Network Security Lab.

- Analyze real-time and archived intrusion, vulnerability and audit data.
- Analyze and develop responses to never seen before security incidents in real time to prevent or limit compromise of systems and data.
- Investigate and document security incidents.
- Prepare and documented security daily reports for clients, based on data collected and criteria from the IDS (Dragon & Snort) and Firewall (Checkpoint) log.
- Immediately alert clients and management of compromise computers or intrusion.
- CACI-Network Security Group.
- Train new staff on the IDS monitoring and incident handling.
- Installation of MS and Linux networks, including wireless networks.

Network Security Engineer 03/2001 to 11/2001 Aligned Development Strategies International City , STATE

- Lockheed Martin Greenbelt Office, Greenbelt, MD.
- Work as an IT Risk Assessment/Information Assurance Specialist in partnership with Lockheed Martin assessing a major state government IT security and assurance infrastructure.
- My responsibilities are: identify, map and analyze network topology.
- Assess security IT weaknesses, conduct Network Scanning and Discovery using commonly known IT scanning and discovery tools.
- Analyze, prepare, and write document results of network scanning and discovery.
- Prepare and support contractor's Network Security Engineer on how to secure network infrastructure, in case-by-case basis, and complexity.
- Support IT Risk Assessment Teams help desk needs, due to its mobility from site to site.

Technical Support Manager/System Administrator 01/1999 to 01/2000 Cintronix, Inc City , STATE

- Deployed and implemented LAN Windows NT for clients; troubleshoot, repair, and assemble PCs, setup Win NT clients and servers (hardware & software), administer Cintronix/ISI LAN, performed migration from Novell 3.12 to Win NT, backups, up dated pricing catalog.
- Install and troubleshoot PC applications.
- Designed/deployed networking solutions (Web Servers, Mail Servers, Backups, Firewalls, ISP) to meet client needs.
- Define requirements for such solutions.
- Perform critical evaluation and selection of architecture, technology, and network components and services, including solution development, installation, and operation that best meets the requirements.
- Analyze local and wide area network systems, including planning, designing, evaluating, and selecting operating systems and protocol suites.
- Configure communication media with concentrators, bridges, and other devices.
- Resolve interoperability problems to obtain operations across all platforms, including e-mail, files transfer, multimedia, and teleconferencing.
- Manage internetworking of various operating systems, including Windows NT/95 and one or more versions of UNIX across both LAN/WAN.
- Monitor performance and stability of networks.
- Configure systems to user environments.
- Support acquisition of hardware and software as well as subcontractor services as needed.

MIS 01/1988 to 01/1989 US Coast Guard City , STATE

- Cert MCSE and MCP 1 Cert Certified Ethical Hacker 5 Total Equivalent Years Experience: 46.5 Accomplishments and Strengths Experienced in diverse network security tools, either commercial, Open Source, and government tools: Snort, Dragon, ISS, Netforensic, PeakFlow, StealthWatch, Nessus, and Real Secure.
- Successfully created several network operations centers for small business, containing web servers, mail servers, DNS, DHCP, and customized financial operations: Cook Electric, Baltimore Contractors, Seton Church, Improsive Technologies, and Smithsonian Institution.
- Participate as team member and then team lead with ADSI/Lockheed and the DC Government in the performance of Risk Assessment, in order to comply with GAO findings.
- Developed customized scripts for major bank (M&T Bank) to order to capture statistical data regarding network intrusion activities, while performing intrusion analysis.
- Recognized for many years as a proven team member and team leader, and trainer.
- Successfully deployed new technologies and trained Smithsonian Institution Grants staff in the use of these new technologies, software usage (excel, financial/accounting program).
- Was instrumental in the automation of tasks for the Exxon Valdez oil spill, in order to assess damaged costs, and agencies participating in the disaster recovery, by using spreadsheets and developing macros.
- For this accomplishment, I was awarded a cash award.
- Managed to successfully deploy Microsoft SharePoint server for the US Department of Labor, Chief Financial Office.
- This deployment was crucial for managing several major contractors working in the new DOL financial system.

Education and Training
Bachelor : Science- Management 1985 New Hampshire College University of Southern Hampshire Science- Management
Bachelor InterAmerican University City
Certified Ethical Hacker Training-Infosec Institute, Technical Training: Certified Cisco Network Engineer, Technical Training: Microsoft Train-the-Trainer, Technical Training: CheckPoint FW rel 71.0

MCSE and MCP Certification: Certified Ethical Hacker (CEH) Certification: Certified Security Professional Course Work New Hampshire College City , State

MBA University of Puerto Rico City , Puerto Rico

Skills

3D, administrative, analyst, Army, automation, Basic, bridges, catalog, Cisco, Com, hardware, network systems, consultant, CRM, client, clients, customer service experience, CVS, database, DC, designing, DHCP, disaster recovery, DNS, documentation, e-mail, email, Engineer, senior management, fast, Financial, financial/accounting, Firewalls, Firewall, Government, Grants, help desk, HP-UX, HR, IDS, IIS 6.0, Information Security, IP, ISA, ISP, LAN, team lead, team leader, LINUX, Lockheed Martin, macros, managing, McAfee, meetings, access, MCP, MCSE, excel, Exchange server, Mail, Office, Windows, Windows 2000, Windows NT, Win NT, migration, Monitors, multimedia, enterprise 3, enterprise, Network Management, Network Engineer, Network Security, Network, networking, networks, Novell 3.12, oil, operating systems, Oracle, Organizational skills, Payroll, People skills, peripherals, perl, personnel, policies, pricing, printers, problem solving skills, protocols, real-time, real time, reporting, Research, Risk Assessment, router, scanners, Scanning, Servers, shell, scripts, spreadsheets, SQL server, switch, TCP/IP networking, team player, Technical support, Technical Training, telephone, Trainer, troubleshoot, UNIX, Unix system administration, UNIX) scripts, upgrades, verbal communication skills, WAN, Web Servers, web server, Windows 2000 server, Written