Resources: Whitepapers

White Papers are an excellent source for information gathering, problem-solving and learning. Below is a list of White Papers written by penetration testing practitioners seeking certification. SANS attempts to ensure the accuracy of information, but papers are published "as is".

Errors or inconsistencies may exist or may be introduced over time. If you suspect a serious error, please contact webmaster@sans.org.

Featured Papers

This featured paper includes some really useful techniques that penetration testers should master. Read it, learn it, and live it, as you extend your skills.

- Using Windows Script Host and COM to Hack Windows

Penetration Testing Whitepapers

Most Recent | Title | Author | Cert

Paper	Author	Certification
Security Monitoring of Windows Containers	Di Giorgio, Peter	GCIH

Cyber Threats to the Bioengineering Supply Chain	Nawrocki, Scott	GCIH
PDF Metadata Extraction with Python	Plaisance, Christopher	GPYC
Template Injection Attacks - Bypassing Security Controls by Living off the Land	Wiltse, Brian	GCIH
Don't Knock Bro	Nafziger, Brian	GCIH
A Swipe and a Tap: Does Marketing Easier 2FA Increase Adoption?	Ackerman, Preston	GCIH
Hardening OpenShift Containers to complement Incident Handling	Holland, Kurtis	GCIH
All-Seeing Eye or Blind Man? Understanding the Linux Kernel Auditing System	Kennel, David	GCIH
Times Change and Your Training Data Should Too: The Effect of Training Data Recency on Twitter Classifiers	O'Grady, Ryan	GCIH
Content Security Policy in Practice	Palathuruthil,	GCIH

	Varghese	
Extracting Timely Sign-in Data from Office 365 Logs	Lucas, Mark	GCIH
Agile Security Patching	Hoehl, Michael	GCIH
Learning CBC Bit-flipping Through Gamification	Druin, Jeremy	GXPN
NOC/SOC Integration: Opportunities for Increased Efficiency in Incident Response within Cyber-Security	Hernandez, Nelson	GCIH
Learning Cryptography by Doing It Wrong: Cryptanalysis of the Vigenere Cipher	Druin, Jeremy	GCIH
High Assurance File Filtering, It's Not Magic	Gould, Adam	GCIH
BYOD Security Implementation for Small Organizations	Simmons, Raphael	GCIH
Hacking Humans: The Evolving Paradigm with Virtual Reality	Andrasik, Andrew	GPEN
Cyber Threat Intelligence Support to Incident Handling	Kime, Brian	GCIH

Creating a Logging Infrastructure	Todd, Brian	GCIH
Tackling DoD Cyber Red Team Deficiencies Through Systems Engineering	Schab, John	GPEN
Cracking Active Directory Passwords or "How to Cook AD Crack"	Boller, Martin	GPEN
The Conductor Role in Security Automation and Orchestration	Cakir, Murat	GCIH
A Practical Example of Incident Response to a Network Based Attack	Fraser, Gordon	GCIH
Offensive Intrusion Analysis: Uncovering Insiders with Threat Hunting and Active Defense	Hosburgh, Matthew	GCIH
Using Docker to Create Multi-Container Environments for Research and Sharing Lateral Movement	McCullough, Shaun	GXPN
Hunting through Log Data with Excel	Lalla, Greg	GCIH

Identifying Vulnerable Network Protocols with PowerShell	Fletcher, David	GCIH
Auto-Nuke It from Orbit: A Framework for Critical Security Control Automation	Hainly, Jeremiah	GCIH
Anomaly Detection, Alerting, and Incident Response for Containers	Borhani, Roozbeh	GCIH
From Security Perspective, the Quickest Way to Assess Your Web Application	Alduhaymi, Mohammed	GWAPT
Attack and Defend: Linux Privilege Escalation Techniques of 2016	Long II, Michael	GCIH
Node Router Sensors: What just happened?	Cary, Kim	GCIH
BGP Hijinks and Hijacks - Incident Response When Your Backbone Is Your Enemy	Collyer, Tim	GCIH
The Information We Seek	Ramos, Jose	GCIH
Detecting Incidents Using McAfee Products	Andrei, Lucian	GCIH

Demystifying Malware Traffic	Saxena, Sourabh	GCIH
Incident Handling Preparation: Learning Normal with the Kansa PowerShell Incident Response Framework	Simsay, Jason	GCIH
Polymorphic, multi-lingual websites: A theoretical approach for improved website security	Risto, Jonathan	GWAPT
Success Rates for Client Side Vulnerabilities	Risto, Jonathan	GCIH
Enterprise Survival Guide for Ransomware Attacks	Mehmood, Shafqat	GCIH
Using Sulley to Protocol Fuzz for Linux Software Vulnerabilities	Warren, Aron	GXPN
Boiling the Ocean: Security Operations and Log Analysis	Chisholm, Colin	GCIH
Testing stateful web application workflows	Veres-Szentkiralyi, Andras	GWAPT
Burp Suite(up) with fancy scanning mechanisms	Panczel, Zoltan	GWAPT

Applying Data Analytics on Vulnerability Data	Dhinwa, Yogesh	GCIH
Web Application File Upload Vulnerabilities	Koch, Matthew	GWAPT
Preparing to withstand a DDoS Attack	Pandya, Gaurang	GCIH
Analysis and Reporting improvements with Notebooks	Knowles, Ben	GCIH
Forensic Analysis On Android: A Practical Case	Alonso-Parrizas, Angel	GMOB
Deployment of a Flexible Malware Sandbox Environment Using Open Source Software	Ortiz, Jose	GCIH
Tunneling, Pivoting, and Web Application Penetration Testing	Fraser, Gordon	GWAPT
Incident Tracking In The Enterprise	Hall, Justin	GCIH
Psychology and the hacker - Psychological Incident Handling	Atkinson, Sean	GCIH

Accessing the inaccessible: Incident investigation in a world of embedded devices	Jodoin, Eric	GCIH
Using windows crash dumps for remote incident identification	Chua, Zong Fu	GCIH
Knitting SOCs	Imbert, Courtney	GCIH
Automated Security Testing of Oracle Forms Applications	Varga-Perke, Balint	GWAPT
Using Software Defined Radio to attack "Smart Home" systems	Eichelberger, Florian	GCIH
Practical El Jefe	Vedaa, Charles	GCIH
Correctly Implementing Forward Secrecy	Schum, Chris	GCIH
The Integration of Information Security to FDA and GAMP 5 Validation Processes	Young, Jason	GCIH
Detecting Crypto Currency Mining in Corporate Environments	D'Herdt, Jan	GCIH

Penetration Testing: Alternative to Password Cracking	Catanoi, Maxim	GPEN
Automated Defense - Using Threat Intelligence to Augment	Poputa-Clean, Paul	GCIH
Cyber Breach Coaching	Hoehl, Michael	GCIH
AIX for penetration testers	Panczel, Zoltan	GPEN
Let's face it, you are probably compromised. What next?	Thyer, Jonathan	GPEN
Secure Design with Exploit Infusion	Yew, Wen Chinn	GCIH
An Analysis of Meterpreter during Post-Exploitation	Wadner, Kiel	GCIH
A Qradar Log Source Extension Walkthrough	Stanton, Michael	GCIH
Differences between HTML5 or AJAX web applications	Thomassin, Sven	GWAPT
H.O.T. | Security	Rocha, Luis	GCIH

Small devices needs a large Firewall	Mastad, Paul	GCIH
Are there novel ways to mitigate credential theft attacks in Windows?	Foster, James	GCIH
Digital Certificate Revocation	Vandeven, Sally	GCIH
Web Application Penetration Testing for PCI	Hoehl, Michael	GWAPT
Securing Aviation Avionics	Panet-Raymond, Marc	GCIH
iPwn Apps: Pentesting iOS Applications	Kliarsky, Adam	GPEN
Incident Handling Annual Testing and Training	Holland, Kurtis	GCIH
Using Open Source Reconnaissance Tools for Business Partner Vulnerability Assessment	Young, Sue	GCIH
War Pi	Christie, Scott	GCIH
Getting Started with the Internet Storm Center Webhoneypot	Pokladnik, Mason	GWAPT

Getting Started with the Internet Storm Center Webhoneypot	Pokladnik, Mason	GWAPT
Home Field Advantage: Employing Active Detection Techniques	Jackson, Benjamin	GCIH
Introduction to the OWASP Mutillidae II Web Pen-Test Training Environment	Druin, Jeremy	GWAPT
Talking Out Both Sides of Your Mouth: Streamlining Communication via Metaphor	More, Josh	GCIH
SMS, iMessage and FaceTime security	Khalil, George	GCIH
Using DomainKeys Identified Mail (DKIM) to Protect your Email Reputation	Murphy, Christopher	GCIH
Detecting Security Incidents Using Windows Workstation Event Logs	Anthony, Russell	GCIH
Web Application Injection Vulnerabilities: A Web App's Security Nemesis?	Couture, Erik	GWAPT

Event Monitoring and Incident Response	Boyle, Ryan	GCIH
Website Security for Mobile	Ho, Alan	GWAPT
Web Log Analysis and Defense with Mod_Rewrite	Wanner, Rick	GCIH
How to identify malicious HTTP Requests	Sarokaari, Niklas	GWAPT
InfiniBand Fabric and Userland Attacks	Warren, Aron	GCIH
Incident Handling in the Healthcare Cloud: Liquid Data and the Need for Adaptive Patient Consent Management	Filkins, Barbara	GCIH
PDF Obfuscation - A Primer	Robertson, Chad	GPEN
Attributes of Malicious Files	Yonts, Joel	GCIH
Covert Channels Over Social Networks	Selvi, Jose	GCIH
Robots.txt	Lehman, Jim	GWAPT
Penetration Testing Of A Web Application Using Dangerous	Kim, Issac	GWAPT

HTTP Methods		
Shedding Light on Security Incidents Using Network Flows	Gennuso, Kevin	GCIH
Remote Access Point/IDS	Kee, Jared	GCIH
Post Exploitation using Metasploit pivot & port forward	Dodd, David	GPEN
Quick and Effective Windows System Baselining and Comparative Analysis for Troubleshooting and Incident Response	Fuller, Kevin	GCIH
iPhone Backup Files. A Penetration Tester's Treasure	Manners, Darren	GPEN
Securely deploying Android devices	Alonso-Parrizas, Angel	GCIH
Responding to Zero Day Threats	Kliarsky, Adam	GCIH
Practical OSSEC	Robertson, Chad	GCIH
Creating Your Own SIEM and Incident Response Toolkit Using Open Source Tools	Sweeny, Jonny	GCIH

An Overview Of The Casper RFI Bot	O'Connor, Dan	GCIH
Wireless Networks and the Windows Registry - Just where has your computer been?	Risto, Jonathan	GAWN
Pass-the-hash attacks: Tools and Mitigation	Ewaida, Bashar	GCIH
Solution Architecture for Cyber Deterrence	Mowbray, Thomas	GPEN
Malicious Android Applications: Risks and Exploitation	Boutet, Joany	GPEN
Security Incident Handling in High Availability Environments	Kibirkstis, Algis	GCIH
Penetration Testing in the Financial Services Industry	Olson, Christopher	GPEN
Which Disney© Princess are YOU?	Brower, Joshua	GCIH
One Admin's Documentation is their Hacker's Pentest	Vandenbrink, Robert	GPEN

IOSTrojan: Who really owns your router?	Santander Pelaez, Manuel Humberto	GCIH
Visualizing the Hosting Patterns of Modern Cybercriminals	Hunt, Drew	GCIH
PCI DSS and Incident Handling: What is required before, during and after an incident	Moldes, Christian	GCIH
IOScat - a Port of Netcat's TCP functions to Cisco IOS	Vandenbrink, Robert	GCIH
Bypassing Malware Defenses	Christiansen, Morton	GPEN
Investigative Tree Models	Caudle, Rodney	GCIH
A Guide to Encrypted Storage Incident Handling	Shanks, Wylie	GCIH
The SirEG Toolkit	Begin, Francois	GCIH
Using GUPI to Create A Null Box	Comella, Robert	GCIH

Using OSSEC with NETinVM	Allen, Jon Mark	GCIH
Document Metadata, the Silent Killer...	Pesce, Larry	GCIH
Espionage - Utilizing Web 2.0, SSH Tunneling and a Trusted Insider	Abdel-Aziz, Ahmed	GCIH
Following Incidents into the Cloud	Reed, Jeffrey	GCIH
Covering the Tracks on Mac OS X Leopard	Scott, Charles	GCIH
Winquisitor: Windows Information Gathering Tool	Cardosa, Michael	GCIH
An approach to the ultimate in-depth security event management framework	Pachis, Nicolas	GCIH
Scareware Traversing the World via a Web App Exploit	Hillick, Mark	GCIH
Virtual Rapid Response Systems	Mohan, Chris	GCIH
Computer Security Education The Tool for Today	Burke, Ian	GCIH

Preventing Incidents with a Hardened Web Browser	Crowley, Chris	GCIH
Baselines and Incident Handling	Christianson, Chris	GCIH
An Incident Handling Process for Small and Medium Businesses	Pokladnik, Mason	GCIH
Stack Based Overflows: Detect & Exploit	Christiansen, Morton	GCIH
Multi-Tool DVD Sets: An important addition to the Incident Handler/ Pen Tester's toolkit	Bandukwala, Jamal	GCIH
Expanding Response: Deeper Analysis for Incident Handlers	McRee, Russ	GCIH
Pros and Cons of using Linux and Windows Live CDs in Incident Handling and Forensics	Smith, Ricky	GCIH
Discovering Rogue Wireless Access Points Using Kismet and Disposable Hardware	Pesce, Larry	GAWN
Inside-Out Vulnerabilities, Reverse Shells	Hammer, Richard	GCIH

DNS Sinkhole	Bruneau, Guy	GCIH
The December Storm of WMF: Preparation, Identification, and Containment of Exploits	Voorhees, James	GCIH
Cisco Security Agent and Incident Handling	Farnham, Greg	GCIH
Effectiveness of Antivirus in Detecting Metasploit Payloads	Baggett, Mark	GCIH
Network Covert Channels: Subversive Secrecy	Sbrusch, Raymond	GCIH
Utilizing "AutoRuns" To Catch Malware	McMillan, Jim	GCIH
Exploiting BlackICE When a Security Product has a Security Flaw	Gara-Tarnoczi, Peter	GCIH
Valentine's Surprise Firedragging in Action	de Nie, Paula	GCIH
IBM AIX invscout Local Command Execution Vulnerability - **HONORS**	Horwath, Jim	GCIH

An Analysis of the Remote Code Execution Vulnerability as Described in Microsoft's MS05-002 Security Bulletin	Rose, Jerome	GCIH
Identity Theft Made Easy	Huber, Eric	GCIH
0day targeted malware attack	Villatte, Nicolas	GCIH
Windows Internet Naming Service - An Exploit Waiting to Happen	Berger, Jeremy	GCIH
Incident Handler Case File: A New Twist to Social Engineering	Hawkins, Ray	GCIH
Local Privilege Escalation in Solaris 8 and Solaris 9 via Buffer Overflow in passwd(1)	McAdams, Shaun	GCIH
What is Santy bringing you this year? **HONORS**	Danhieux, Pieter	GCIH
rLogin Buffer Overflow Vulnerability - Solaris	Corredor, Juan	GCIH
Fun with Batch Files: The Muma Worm	Mackey, David	GCIH
Remote Exploitation of Icecast 2.0.1 Server	Pittner, Jakub	GCIH

Freezing Icecast in its Tracks	McLaren, Jared	GCIH
A Picture is Worth 500 Malicious Dwords	Hall, Timothy	GCIH
Exploiting Internet Explorer via IFRAME	Becher, Jim	GCIH
Exploiting the Microsoft Internet Explorer Malformed IFRAME Vulnerability	Tu, Alan	GCIH
The Cisco IPv4 Blocked Interface Exploit	Johnson, Cortez	GCIH
DreamFTP - The Nightmare Begins!	Sorensen, Robert Peter	GCIH
phpMyAdmin 2.5.7 - Input Validation Vulnerability	Thurston, Tracy	GCIH
Exploiting the LSASS Buffer Overflow	Wohlberg, Jon	GCIH
PHP-Nuke: From SQL Injection to System Compromise	Paynter, Eric	GCIH
BruteSSH2 - 21st Century War Dialer	Thompson, Bill	GCIH

Incident Report for a Rootkit attack on a Fedora workstation	Norman, Bonita	GCIH
A Heap o' Trouble: Heap-based flag insertion buffer overflow in CVS	Conrad, Eric	GCIH
Phising Attack in Organizations: Incident Handlers Perspective	Ong, Leonard	GCIH
Cisco.s LEAP vulnerability and the .asleap.exploit	Goudie, Mark	GCIH
A Two Stage Attack Using One-Way Shellcode	Mathezer, Stephen	GCIH
Eradicating the Masses & Round 1 with Phatbot?	Fulton, Lora	GCIH
Discovering a Local SUID Exploit	Pike, Jeff	GCIH
Robbing the Bank with ITS/MHTML Protocol Handler	Balcik, James	GCIH
Real Network's Remote Server Remote Root Exploit	Lastor, Michael	GCIH

A Buffer Overflow Exploit Against the DameWare Remote Control Software	Strubinger, Ray	GCIH
Bad ESMTP Verb Usage Equals Bad Times for Exchange	Smith, Aaron	GCIH
Stay Alert While Browsing the Internet	LaValley, Jim	GCIH
Author Intruder Alert: Why Internal Security must not take a back seat.	Hendrick, Jim	GCIH
Microsoft RPC-DCOM Buffer Overflow Attack using Dcom.c	Farrington, Dean	GCIH
All Your Base Are Belong To Someone Else: An Analysis Of The Windows Messenger Service Buffer Overflow Vulnerability	Hewitt, Peter	GCIH
The enemy within: Handling the Insider Threat posed by Shatter Attacks	Layton, Meg	GCIH
Catch the culprit!	Perez, David	GCIH
An Attacker On RPC Compromised Remote VPN Host Runs Arbitrary Code on Microsoft Exchange Server 2000	Ho, Wai-Kit	GCIH

Combating the Nachia Worm in Enterprise Environments	Johnson, Brad	GCIH
GIAC Certified Incident Handling Practical	Yachera, Stanley	GCIH
A Study of the o_wks.c Exploit for MS03-049	Arnoth, Eric	GCIH
Nachi to the Rescue?	Griffith, Russ	GCIH
Windows Media Services NSIISLOG.DLL Remote Buffer Overflow	Smith, Steve	GCIH
Session stealing with WebMin	Murdoch, Don	GCIH
Hacker Techniques, Exploits, and Incident Handling	Brooker, Denis	GCIH
The Tactical Use of Rainbow Crack to Exploit Windows Authentication in a Hybrid Physical-Electronic Attack	Mahurin, Mike	GCIH
My First Incident Handling Experience	Kohli, Karmendra	GCIH
Breaking Windows 2000 Passwords via LDAP Password Crackers	Hamby, Charles	GCIH

Penetration Testing of a Secure Network	Pakala, Sangita	GCIH
A J0k3r Takes Over	Larrieu, Heather	GCIH
Real World ARP Spoofing	Siles, Raul	GCIH
A Weak Password And A Windows Rootkit: A Recipe For Trouble	Ives, John	GCIH
Back-Door'ed by the Slammer	Hally, John	GCIH
SMTP - Always a victim of a good time	Lock, James	GCIH
SQL Slammer and Other UDP Port 1434 Threats In support of the Cyber Defense Initiative	Ray, Edward	GCIH
0x333hate.c: Samba Remote Root Exploit	Embrich, Mark	GCIH
A Management Guide to Penetration Testing	Shinberg, David	GCIH
Hijacked Server Serves Up Foreign Bootlegged Pornography	Meyer, Russell	GCIH

Incident Analysis in a Mid-Sized Company	Garvin, Pete	GCIH
SQL Slammer Worm	Hayden, Chris	GCIH
The Microsoft IIS 5.0 Internet Printing ISAPI Extension Buffer Overflow	Clemenson, Christopher	GCIH
Traveling Through the OpenSSL Door	Murphy, Keven	GCIH
SQL Server Resolution Service Exploit in Action	Hoover, James	GCIH
Network Printers: Whose friend are they?	Hutcheson, Lorna	GCIH
Buffer overflow in BIND 8.2 via NXT records	Talianek, Chris	GCIH
Attack of Slammer worm - A practical case study	Huang, Dongmei	GCIH
Nimda - Surviving the Hydra	Schmelzel, Paul	GCIH
SMBdie'em All - Kill That Server	Kirby, Craig	GCIH

SMTP Loop Moderate Denial of Service: InterScan VirusWall NT & Lotus Domino Environment	Roberts, Brian	GCIH
Port 1433 Vulnerability: Unchecked Buffer in Password Encryption Procedure	Bryner, Jeff	GCIH
Solaris in.lpd Remote Command Execution Vulnerability	Seah, Meng Kuang	GCIH
System infiltration through Mercur Mail Server 4.2	Ben Alluch Ben Amar, Jamil	GCIH
Port 443 and Openssl-too-open	Lee, Chia-Ling	GCIH
SQL Snake and Other Port 1433 Threats In Support of the Cyber Defense Initiative	Short, Christopher	GCIH
First Response: An incident handling team learns a few lessons the hard way	Cragg, David	GCIH
Apache Web Server Chunk Handling Apache-nosejob.c	Sarrazyn, Dieter	GCIH

Windows Shell Document Viewer shdocvw.dll Feature or Trojan Horse?	Fenwick, Wynn	GCIH
Support for the Cyber Defense Initiative	Fresen, Lars	GCIH
Linux NTPD Buffer Overflow	Stadler, Philipp	GCIH
Identifying and Handling a PHP Exploit	Edelson, Eve	GCIH
KaZaA Media Desktop Virus: W32/kwbot	Will, Rita	GCIH
Dsniff and Switched Network Switching	Bowers, Brad	GCIH
Donald Dick 1.55 with Last Updated GUI Component from Version 1.53	Maglich, Ryan	GCIH
Widespread SNMP Vulnerabilities	Brooks, Greg	GCIH
Relative Shell Path Vulnerability	Evans, Earl	GCIH
Netscape Enterprise Server Denial of Service Exploit	Smith, Tony	GCIH

The t0rn Rootkit	Craveiro, Paulo	GCIH
FTP Port 21 "Friend or Foe" Support for the Cyber Defense Initiative	Karrick, Stephen	GCIH
False Alarm...Or Was It? Lessons Learned from a Badly Handled Incident	Graesser Williams, Dana	GCIH
Pass - Questions	Schultz, Tim	GCIH
Sun snmpXdmi Overflow	Miller, Kevin	GCIH
BackGate Kit: The Joy of "Experts"	DePriest, Paul	GCIH
Tracking the Back Orifice Trojan on a University Network	Knudsen, Kent	GCIH
IIS 5 In-Process Table Privilege Escalation Vulnerability	Fatnani, Kishin	GCIH
How to Gain Control of a Windows 2000 Server Using the In-Process Table Privilege Escalation Exploit	Stidham, Jonathan	GCIH
Simple Network Management Protocol: Now More than a "Default" Vulnerability	Fluharty, Daniel	GCIH

Exploiting the SSH CRC32 Compensation Attack Detector Vulnerability	Williams, R. Michael	GCIH
Sub Seven: A Risk to Your Internet Security	Ostrowski, Paul	GCIH
Importance of a Minor Incident: W32/Goner@MM	Legary, Michael	GCIH
Incident Handling Without Guidelines	McKellar, Neil	GCIH
What to do when you break WEP Wireless Security and the LAN	Poer, Geoffrey	GCIH
Phone Phreaking and Social Engineering	Tuey, Richard	GCIH
FTP Security and the WU-FTP File Globbing Heap Corruption Vulnerability	Webb, Warwick	GCIH
WU-FTPD Heap Corruption Vulnerability - HONORS	Allen, Jennifer	GCIH
Lotus Notes Penetration	Rademacher, Karl	GCIH

Employees Are Crackers Too	Stapleton, Curt	GCIH
GIAC GCIH Assignment - Pass	Harrison, Daniel	GCIH
Exploiting Vulnerabilities in Squirrelmail	Bong, Kevin	GCIH
Neptune.c the Birth of SYN Flood Attacks	Cardinal, Steven	GCIH
M@STER@GENTS: Masters of "SPAM"	Ashland, Joanne	GCIH
Mutated Code	Kopczynski, Tyson	GCIH
Revisiting the Code Red Worm	White, Ravila	GCIH
Once Bitten Twice Sly - Common Exploits Fueled by Common Mishap	Melvin, John	GCIH
FreeBSD 4.x local root vulnerability -- exec() of shared signal handler	Durkee, Ralph	GCIH
Reverse Engineering Srvcp.exe	Zeltser, Lenny	GCIH

Automated Execution of Arbitrary Code Using Forged MIME Headers in Microsoft Internet Explorer	Winters, Scott	GCIH
MS IIS CGI Filename Decode Error Vulnerability	Shenk, Jerry	GCIH
Exploit Analysis	Jenkinson, John	GCIH
Wireless LAN Honeypots to Catch IEEE 802.11 Intrusions	Mitchell, Gordon	GCIH
The fascinating tale of a lame hacker, a Linux Box, and how I received permission to deploy my IDS	Markham, George	GCIH
IP Masquerading Vulnerability for Linux 2.2.x - CVE-2000-0289	Baccam, Tanya	GCIH
Illustration of VS.SST@mm Virus Incident	Smith, Kevin	GCIH
The Search for "Kozirog"	Weaver, Greg	GCIH
Open Shares Vulnerability	Hill, Siegfried	GCIH
Anna Kournikova Worm	Ashworth, Robert	GCIH

Incident Illustration - HTTP Services Vulnerabilities	Modelo Howard, Gaspar	GCIH
Ramen Worm	Ives, Millie	GCIH
Incident Illustration - Firewall Attack	Reed, Bill	GCIH
Incident Illustration - Mstream	Gallo, Kenneth	GCIH
The Not-So Vicious Attacker	Mossholder, Matt	GCIH
Jolt2 or "IP Fragment Re-assembly	Beciragic, Jasmir	GCIH
Testing Web Applications for Malicious Input Attack Vulnerabilities	Grill, Robert	GCIH
Incident Illustration - Missing Files	White, Scott	GCIH
Cisco IOS Type 7 Password Vulnerability	Massey, Lee	GCIH
Incident Illustration - Corporate Compromise	Hall, Russell	GCIH

ICQ URL Remote Exploitable Buffer Overflow	de Beaupre, Adrien	GCIH
Local Exploit: dtprintinfo for Solaris 2.6 and 7	Sipes, Steven	GCIH
BIND 8.2 NXT Remote Buffer Overflow Exploit	Mcmahon, Robert	GCIH

Top ↑

Latest Blog Posts

Tips for Creating a Strong Cybersecurity Assessment Report
January 23, 2019 - 11:57 AM

Web Application Scanning Automation
January 23, 2019 - 4:03 AM

Latest Tweets @SANSPenTest

Demonstrate how your organization maximizes the value of its [...]
April 19, 2019 - 6:40 PM

SANS #PenTest Pivots & Payloads Poster/Board game is ava [...]
April 16, 2019 - 1:35 PM

Latest Papers

Security Monitoring of Windows Containers
By Peter Di Giorgio

Cyber Threats to the Bioengineering Supply Chain
By Scott Nawrocki

Secrets to Successful Cybersecurity Writing: Hack the Reader
January 11, 2019 - 2:00 PM

Join @lennyzeltser in NYC starting 6/1 to learn how to break [...]
April 14, 2019 - 6:55 PM

PDF Metadata Extraction with Python
By Christopher Plaisance

"This is the best hands-on course available anywhere."
- Whitney Janes, FedEx

"Ed Skoudis is the best teacher I've ever had. He is 100% competent and professional."
- Petra Klein, FRA

"This was by far the best course I have ever taken."
- Peter Lombars, Intrucom Inc.