STOP SPAM.
SAVE TIME.

SPAM TITAN

THE ULTIMATE SYSADMIN TOOLBOX

Security Incident Cheat Sheets

For any small- to medium-sized business, funding and maintaining an IT infrastructure is always a daunting proposition. Just procuring the appropriate hardware and software is time-consuming and expensive, and then there's the ongoing expense (and time expenditure) of day-to-day maintenance.

Maintenance involves more than keeping hardware and software updated. It's critical that security is always up to speed. Small- and medium-sized businesses are vulnerable to attacks of all kinds, including distributed denial-of-service attacks, system compromise, and even total IT intrusion.

The first line of defense is the system administrator, the tireless hero who works 24 X 7 X 365 to ensure that the IT infrastructure is always secure. The sys admin's work often goes unnoticed, though it's the work that lets employees and business owners enjoy a problem-free seamless working environment. When things go wrong, though, everyone notices and appreciates what the sys admin contributes, as he or she brings a sense of calm to a world in chaos. There's even a special appreciation day dedicated to all you hard-working sys admins, 'System Administrator Day'.

SpamTitan would like to make life just a bit easier for the overworked system administrator by providing a convenient cheat sheet for diagnosing common problems. The following resources will come in handy if you are ever hit with a security incident or breach. These tools guide you through preparing for a disaster and recovering from one. They're designed to help you overcome distributed denial-of-service attacks and malicious software intrusions by hackers. They'll also assist in checking for system integrity.

The following three tools help you diagnose any general security breaches you may encounter:

- **Security Incident Questionaire**
- **Security Incident Survey Cheat Sheet**
- **Critical Log Review Checklist for Security Incidents**

The biggest fears faced by system administrators? A total meltdown of servers brought on by a DDOS attack or a widespread intrusion into the IT infrastructure by a malicious third party probably top the list. These tools help to avoid these situations:

If your servers ever come under attack by malformed data packets, use this tool to get back on track:

- **DDOS Incident Cheat Sheet**

If you are using Linux-based servers and they become a victim of an intrusion attack, use the following:

- **Linux Intrusion Detection Discovery Cheat Sheet**
- **Checking UNIX/Linux - Systems for Signs of Compromise**

The Windows Server environment is as prone to attacks and hacks as the Linux environment. For Windows Server attacks, the following resources will be handy:

- **Windows Intrusion Detection Checklist**
- **Windows Intrusion Detection Discovery Cheat Sheet**
- **Checking Windows - Systems for Signs of Compromise**

Security Online Resources

At SpamTitan, we're in a good position to observe just how unrelentingly small- to medium-sized businesses are jeopardized by security threats, and how the dangers continue to worsen every day. It is a constant uphill battle not just for the security and network administrators, but for security vendors as well. Trying to keep up with hacks and threats is a like being at war, as system administrators know all to well.

To be battle ready, a systems administrator needs to have security tools at his or her disposal at a minute's notice. When it comes to finding security resources or contacting security vendors for their solutions, there's no time to waste. What resources can a network administrator use immediately?

To begin with, here are resources that give you immediate access to various security centers worldwide. You can contact any of these centers at any time for more information and data.

resource is useful for verifying if the website you're visiting is safe. It also gives you insights on how to conduct safer web surfing practices:

To see the current security vulnerabilities in the United States, use this resource:

- **US-CERT Current Events**

To see the current security threats in Europe, use this tool:

- **List of European CERTs**

To get an idea of current worldwide attack vectors, these are some of the sites we at SpamTitan find especially useful:

- **Internet Storm Center @ SANS.org**
- **Digital Attack Map: worldwide DDoS in (nearly) realtime and historic data**
- **HPI-VDB - searchable Vuln-Database**
- **Security Information Center @ mare-system.de**

If you are using a network intrusion device, such as a Snort Sensor (a device to help 'sniff out' bad data packets which could be used to launch an attack), use the following plugin. It correlates your information and data among other Snort Sensors worldwide, giving you a pretty good indication of how vulnerable your business is to an attack:

- **autoshun.org -> live threats and stats from snort-sensors**

Websites can be easily spoofed and look convincingly like the real thing. The following resource is useful for verifying if the website you're visiting is safe. At SpamTitan, we also recommend it for the insights it gives you on how to conduct safer web surfing practices:

- **Google Safebrowsing Transparencyreport about Malware-infected Sites**

The following tools are very useful for verifying the legitimacy of IP addresses and domain names. You can also use them to determine which domain name an IP address belongs to, or to find out who owns a domain name:

- **BGP-Toolkit - AS+Domain-Information from HE**
- **Who.Is - Extended WHOIS+DNS-Information**

If you do not know the domain name but just have the IP address, you can do what is known as a 'reverse' lookup and obtain the domain name that way:

- **Reverse IP Lookup @ ip-address.org**
- **Reverse IP Domain Check @ yougetsignal.com**

Email headers do not appear when you receive an email, but you can fully analyze them using this resource:

- **Mail-Header Analysis**

Creating secure passwords is often very difficult because passwords are the first thing hackers and Identity thieves go after. In order to make sure that you are creating the safest passwords possible for you and your employees, use this website:

- **https://makepw.com/32/**

Online Website Checks

One of the best ways to know if you are on a secure website is through the use of the network protocol known as Secure Sockets Layer, or SSL for short. SSL allows important confidential information to be scrambled or encrypted over the network medium.

Whenever a new server is installed, most of the system administrator's time is devoted to just getting the server up and running and making sure that it works within the entire IT infrastructure. There's not much time left to check for other things, such as verifying whether SSL is installed on the server. These tools will give the system administrator the ability to check for SSL installations:

These three tools conduct an in-depth analysis of the SSL certificate on the server side:

- **SNI-Client-Test @ velox.ch**
- **SSLLabs Server-Test**
- **Thawte SSL-Check**

These two tools help you to diagnose any problems you may be experiencing with an SSL certificate:

- **DigiCert - Check**
- **SSL-Check @ sslshopper.com**

To see if your web browser is SSL compliant, the following resources are useful. This is important to verify, because if your computer is covertly hijacked the SSL on your web browser will be rendered useless:

- **Symantec SSL-Cert-Check**
- **SSL-TrustSSLLabs Client-Test**
- **How's My SSL?**
- **SSL-Trust**

Malware can be defined specifically as 'malicious software.' This is software that's installed on your computer without your prior knowledge or consent. Examples of malware include worms, Trojan horses, and viruses. These types of malware can be picked up anywhere, but infected websites are among the most common sources of contagion.

Use the following resources to make sure that the websites you are visiting are free from malware. All of these tools conduct a deep penetrating analysis of the website in question, letting you know if it's infected with malware before you even visit it:

- **urlvoid.com**
- **sitecheck.sucuri.net**
- **unmaskparasites.com**
- **WebOfTrust mywot.com**
- **Google-Safebrowsing**
- **URL-Scan @ VirusTotal**
- **MARE Sitescan**
- **WatchScript.p**

Here's another tool for verifying website security. This tool analyzes header security and lets you know immediately if the security is adequate according to criteria established by security professionals:

- **SecurityHeaders.com**

Phishing can be defined as creating a fake website that looks authentic enough to lure users into giving up their personal and confidential information. We at SpamTitan enjoy using this handy web page that helps distinguish fake sites from real ones. Just type in the website address, and within seconds you get a message indicating if the website you want to visit is fake or not:

- **PhishTank.com**

System Administrator References

At SpamTitan, we've gotten enthusiastic recommendations for all of these resources from our Linux-loving friends. If your small business is operating in a Linux environment, the following resources are invaluable. They run the gamut from how to properly administer a Linux server, to securing it, to managing IP tables. You can even learn how to program a Linux server via the command line structure:

- **Linux Admin Quick Reference**
- **Linux Security Quick Reference**
- **Excellent IPTables-Tutorial**
- **Linux Command Line Tools Summary**
- **NFTables - Intro**

If your business uses Debian Linux, here are some very convenient references. The first is a handy card you can carry in your pocket. The second and third tools are text-based and HTML-based references, respectively.

- **Debian Reference PocketCard**
- **Debian Reference (Full, txt)**
- **Debian Reference (Full, html)**

If you use Zypper Version 1.0.9 as your primary Operating System (OS), then use this resource:

- **Zypper CheatSheet**

The following Windows-based resources are great tools for command line programming:

- **Windows Shell Commands**
- **Windows PowerShell 3.0 and Server Manager Quick Reference Guides**
- **Windows PowerShell Quick Reference**
- **Command Line References @ SS64.com**

If you find that your Windows registry is corrupt and in need of repair, use this tool:

- **Windows Offline Password & Registry Editor**

This tool is great for programming in an Apple OSX environment:

- **OSX-Reference**

This resource is perfect for programming command line structures in Windows XP:

- **WindowsXP**

Every dynamic website needs a database in order to capture the information and data in real time. Two of the most popular databases to use are SQL Server (from Microsoft) and Oracle. Here are two online references for these databases:

- **SQL-Server**
- **Oracle**

Bash stands for 'Bourne Again Shell,' which is a scripting language. The first reference is a complete manual for Bash; the second resource provides an at-a-glance view of the command line structures; the third resource provides the system administrator with an easy-to-carry pocket guide of the command line codes needed for quick programming (in three different file versions); and, finally, the last reference tool gives the resources needed to program in Linux:

- **Bash Reference Manual from gnu.org**
- **Bash Quick Reference**
- **Bash Programming Pocket Reference (pdf)**
- **Bash Programming Pocket Reference (txt)**
- **Bash Programming Pocket Reference (html)**
- **Bash**

Stream Editor (SED) is another scripting language. This reference provides an in-depth tutorial in using SED:

- **Sed-Tutorial**

If you are scripting in the Tripwire language, the following resource will be useful:

- **TRIPWIRE Reference Card**

The following two online tools provide quick references for composing commands in general purpose scripting:

- **SCREEN Cheat Sheet**
- **VI Quick Reference**

EMACS is another scripting language that has been around for quite some time--since the dawn of the mainframe. If you're programming in EMACS, you'll appreciate this reference:

- **EMACS Quick Reference**

NMAP stands for 'Network Mapper.' This tool is used to map servers on a specified network. It does this by triggering specialized data packets and analyzing the **servers'** responses in order to create a network map. The following is a quick reference guide for doing this:

- **Nmap CheatSheet**

KVM stands for 'Kernel-based Virtual Machine,' and the following tools allow you to create a Linux-based virtualization infrastructure:

- **KVM CheatSheet (uncomplete)**
- **RedHat KVM Cheat sheet**
- **Linux Virtualisation Cheat Sheet**

At SpamTitan, we love 'GIT.' GIT is a software version control tool that emphasizes software speed and integrity. The following resource provides the command-line structures needed to use this tool:

- **GIT Quick Reference (also nice artwork) (large version)**

SVN stands for 'Subversion,' and it too is a software configuration management tool. Use this resource if you are using SVN for your version control needs:

- **SVN Quick Reference**

Mercurial is yet another software version control tool, but one with the advantage of cross-platform compatibility. It can operate across Windows, UNIX, Mac OSX, and Linux. It's available in both command line and graphical user interface (GUI) formats. The following resource is a reference for the command line language:

- **Mercurial Usage Reference**
- **more versions, 300dpi**

GNU is hacker slang meaning 'GNU is not UNIX.' It is an entirely free, open-source operating system (OS). The following reference provides a listing of all of the software tools that are associated with GNU, such as archiving, database, and editor tools:

- **GNU Manuals Online**

The following two tools allow you to convert a domain name from the International Domain Name (IDN) standard to either the Unicode or ASCII formats:

- **PunyCode-Converter**
- **PunyCode-Converter @ VeriSign**

XML stands for the 'eXtensible Markup Language,' which is a programming language for developing either static or dynamic web pages. The following tools will double check the validity of the XML code you have created:

- **XML-Validator @ w3schools**
- **URL Encode/Decode**

PHP stands for 'Hypertext Preprocessor,' and it's another programming language used to create and design web pages. The following reference will double check the validity of the PHP code you have written:

- **Base64/PHP-Decoder**

UTF-8 stands for 'Unicode Transformation Format-8.' Essentially, UTF-8 defines the character formatting on a web page, allowing the web browser to automatically define how the web content will be displayed. To help decode the formatting codes in UTF-8, use the following tool:

- **UTF8-Decoder**

Use the following tool to double check for URL validity before launching your website:

- **REDBot - HTTP-Resources-Check and analysis**

The UNIX geeks here at SpamTitan love these three resources that provide you with an in-depth look at the UNIX command line codes, a must-know if you're a UNIX enthusiast too:

- **UNIX Rosetta Stone bhami.com/rosetta.html**
- **Treebeard's Unix Cheat Sheet**
- **Unix Reference Card**

New to UNIX? Here's a complete eBook about using it:

- **Guide to Unix - Book :: compiled from wikibooks.org**

If you're programming in BSDA, this is a much-needed reference:

- **BSDA-Command_Reference from bsdcertification.org**

The following will be useful if you're programming in Sun Solaris UNIX:

- **BigAdmin Solaris - Shell - Commands @ sun.com**

Finally, if your IT infrastructure goes down, everybody at your company needs to be talking the same language in order to communicate quickly and effectively. SpamTitan has recommended the following cheat sheet to its customers. We find it can be really helpful in furthering the flow of communications between all of the departments in your business:

- **Human Communications Cheat-Sheet**

Real Time Attacks & Outages

At SpamTitan, we find the following online tools fascinating. They give you the information you need to see what kind of Internet attacks are occurring around the world. All you have to do is either look up or enter the country of interest:

- **Digital Attack Map: worldwide DDoS in (nearly) realtime and historic data**
- **Realtime-Attack-Map by Norse**
- **Akamai Global Statistics**
- **Team Cymru Internet Critical Infrastructure Monitoring**
- **Internet Traffic Report**
- **autoshun.org -> live threats and stats from snort-sensors**
- **Internet Storm Center Infocon-Status**

Viruses and spam can also cause Internet outages. To get the latest on these two threats on a global basis, click here:

- **Curent Anti-Virus Alerts and Stats**
- **Realtime (nearly) Spam-Statistics**

Rescue CD's

In the case of total server failure, the system administrator does not have time to fumble through the desk drawers trying to find the rescue CDs. What's required are tools that can be quickly accessed and that will have the servers back up again in just a matter of seconds.

It should be noted here that these rescue downloads serve both the Linux- and Windows-based environments, therefore we have provided the appropriate operating system breakdowns as follows:

At SpamTitan, we've heard from our Linux customers that the following tools are invaluable for helping you to restore your Linux system:

- **SystemRescueCd**
- **GRML**
- **Knoppix**
- **Bitdefender RescueCD**
- **Kaspersky RescueCDs**

If you are running both Linux and Windows, you need the following resource:

- **F-Secure Rescue-CD 3.11**

If your servers are running in a pure Windows environment, the following rescue software will be of interest:

- **FREE Bootable AntiVirus Rescue CDs Download List (blog)**

If you'd like to compare the various rescue software packages before making a final decision, the following resource will be helpful:

- **13 Antivirus Rescue CDs Software Compared in Search For the Best Rescue Disk (blog)**

WHOIS/TRACE ROUTE INFORMATION

Given today's extremely sophisticated hijacks and attacks, anything online can be stolen and pop up later under purportedly different ownership. At SpamTitan, we hear about shocking cyber thefts every day. Even brand fraud can occur, including illegal knockoffs, copyright infringements, and email scams. The first person to get the blame for this is typically the system administrator. How should a business protect its online intellectual property, making the life of the system administrator as painless as possible?

These two online resources will give you all of the DNS information you need about a domain names and IP addresses:

- **mxtoolbox.com**
- **whois.domaintools.com**

If you need to confirm the DNS information on your own computer, use these two tools:

- **robtex.com**
- **dshield.org**

NETWORK CALCULATIONS & CHEATSHEETS

Keeping a corporate website up and running 24 X 7 x 365 takes enormous network capability, especially if the website incorporates an online store. Network usage and bandwidth can be a costly proposition for a business, especially if it is leased directly from a network supplier. It's very important for a business to use network availability optimally. Figuring this out can be very tedious work for the system administrator.

SpamTitan has made a list of resources, and the good news is that there are lots of online network websites that help calculate many of the variables quickly. Some of the variables are:

Subnet Calculations: The term 'subnetting' means dividing an entire network infrastructure into smaller ones in order to improve efficiency. In other words, a 'subnet' is merely a network segment. To calculate the appropriate subnet structures, use these online resources:

- **Subnet-Calculator**
- **IPv4 - Subnetting Cheat Sheet @ packetlife.net**
- **Subnet - Cheatsheet**
- **ICMP Cheat Sheet**

Data Packets: It is the data packet that allows communication on the Internet to take place, such as the sending and receiving of email, instant messaging, etc. The data from the sending computer gets broken into smaller bits of information, which are stored in a data packet. The data packet gets transmitted over the Internet to the receiving computer, where all of those bits of information are then reassembled into the original message. For the exact details on what comprises a data packet and how it can be used efficiently, check out this resource:

- **ISC TCP/IP + tcpdump - Cheatsheet**

HTTP Status Codes: These codes tell you what the status of a particular website page is. Probably one of the most common codes is 'Code 303'. In order to see all of the web-based status codes, use this online resource:

- **HTTP - Status - Codes**

SMTP Status Codes: These codes serve the same purpose as HTTP Status Codes, but they are used specifically for email applications and communications. For an overview of SMTP Codes, use this:

- **SMTP - Status - Codes**

Port Numbers: These are simply the physical communication endpoints between computers in a network. Specific port numbers serve specific software applications. To get an overview of which port is associated with which type of software application, use these resources:

- **Common Ports Cheat Sheet @ packetlife.net**
- **TCP Ports List**

Network Protocols: These are the standards used to define how the data packets will be exchanged over a network infrastructure such as the Internet. Each network protocol has its own unique method for formatting and sending the data packets. The most common network protocol is the 'Hyper Text Transfer Protocol' (HTTP), which is used to retrieve and browse through various websites and web pages. To get a description of all of the various network protocols and the applications they are used for, use this resource:

- **Common Ports Cheat Sheet @ packetlife.net**

ONLINE-ANTIVIRUS, SYSTEM, and BROWSER CHECK

The main purpose of malware is to covertly track your movements on the Internet. Adware is software that automatically displays popup ads and other unwanted ads on your computer. How can you combat each of these two threats?

Using the traditional tools of detection, it takes a systems administrator a long time to find the root cause of viruses like this. Luckily, there are various online tools we at SpamTitan have found useful that can assist in diagnosing viruses quickly and easily.

To check against infected files on your hard drive, the following resources are helpful. Damaged files can be repaired within minutes:

- **Virustotal**
- **Jotti**
- **Kaspersky**
- **McAfee**
- **Dr. Web**

Keep in mind that malicious software packages do not just manifest themselves within your computer files. You can also get them by simply visiting a spoofed website, a website that may look authentic, but is full of adware and malware. Once you log into it, your computer could be completely infected within seconds. Here are six online resources to help you combat this:

- **NOD32/Eset**
- **BitDefender**
- **Kaspersky**
- **TrendMicro**
- **a-squared**
- **Conficker Online Test @ uni-bonn.de**

To get the latest research papers and reports on malware, spyware, and adware, use this resource:

- **F-Secure**

SpamTitan loves this online tool that helps you to stay ahead of the game by examining specific application types, DNS servers, intrusion attacks, spoofed IP addresses and domain names, infected websites, and known viruses:

- **Barracuda Central**

These two resources provide detailed information about virus threats that are occurring in the United States and worldwide:

- **McAfee Threat Center**
- **Virus Bulletin**

This resource provides all of the information and data you need about high level security threats and risks that have been reported to United States authorities:

- **US-CERT Current Events**

Given the sophistication of today's data-driven websites (which contain JavaScripting, embedded photos and videos, and other pieces of active content), your web browser can also easily become infected with viruses. The following tools allow you to quickly test to see if your browser is indeed infected and take the appropriate actions to repair any security holes or gaps.

This tool will check to see how unique your web browser is. The more unique it is, the less chances of it being hacked:

- **Panopticlick@EFF**

To make sure that your Mozilla web browser is up to snuff on security standards, use this tool:

- **Mozilla-Plugincheck**

The following three sources will do a general check on the security of your web browser:

- **Browser - SSL Cipher Suite Details**
- **The H Browsercheck**
- **Windows-System-Check (.de)**

This online resource helps to determine if your web browser has any insecure plugins that need to be deleted:

- **Qualys - Browsercheck for insecure Plugins or Browserversions**

This free tool explains in detail what cookies are and how they can be maliciously used on your web browser:

- **Browser-Fingerprinting - Article @ The H**

DNSRBL Lookups

DNSRBL stands for 'DNS Real-time Blackhole List.' This is a listing of all of the IP addresses of computers and networks that are associated with spamming. The DNSRBL is not actually a listing per se, but rather it is a software package that uses various criteria to determine if an IP address is actually a source of spam.

If it is, it then gets 'blacklisted.' If a business' domain gets blacklisted, the person who has to fix this is the network administrator. It can be a real pain to get 'un-blacklisted' again.

The following online tools will check to see if your domain is indeed blacklisted, and if it is, it details the corrective actions that you can take. These free resources include the following:

- **Spam-List-Check @ heise.de**
- **RBL-Toolbox @ webhotel.net**
- **mxtoolbox.com**

Apart from seeing if your domain is blacklisted, you need to be proactive about keeping it from being blacklisted at any point in the future. These online resources will help:

- **UCE-Protect Network**
- **Google spam and Security trends**

SpamTitan offers all of these free resources as a way of saying 'thank you' to the thousands of system administrators who work countless hours--day in and day out--in order to ensure that their IT infrastructures are up and running. This article is intended to serve as an easy-to-use, one-stop reference, enabling you to find all of the information you need at a quick glance and download it within seconds. Please consider this as our gift to you, in honor of 'System Administrator Appreciation Day!!!'