Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

A "Bag of Tricks" Approach to Proactive Security

Security does not begin with the detection of a compromised server or other form of detected intrusion. Where then, does security begin? This paper explores this question. Simply stated this paper focuses on common sense. However, practically stated, the goal of this paper is to explore the tools, practices and procedures available to System Administrators prior to a security incident that will serve to negate the incident or significantly improve our recovery and forensic positions.

Copyright SANS Institute
Author Retains Full Rights

AD

Abstract

Security does not begin with the detection of a compromised server or other form of detected intrusion. Where then, does security begin? This paper explores this question. Simply stated this paper focuses on common sense. However, practically stated, the goal of this paper is to explore the tools, practices and procedures available to System Administrators prior to a security incident that will serve to negate the incident or significantly improve our recovery and forensic positions.

Introduction

There are numerous articles on the topic of computer and network security. These topics are presented to a growing audience, through increasingly diverse mediums, on almost a daily basis. Everyone is jumping on the security bandwagon, from 60 Minutes to the original 'Paul Reveres' of security (Security Focus, SANS, SlashDot, Eeye.com, etc)[1] . Yet, most of these sources deal with the report of security incidents. Only a few provide valid information on proactive measures as opposed to reactive. Typically, information pertaining to proactive measures comes from the 'Paul Revere' group. Unfortunately, this information is typically overlooked while looking for a 'quick-fix' to a detected problem. *If you think this sounds like a rather bleak statement, notice I did not say 'always overlooked'!* Sometimes the neglect to use this information is due to a lack of time, however, my experience seems to indicate the neglect stems more from lack of understanding of the need for proactive security. Regardless of the reason why proactive measures are ignored, proactive thought about security does not seem to kick in until a serious problem is encountered. This paper will ignore users lacking an understanding of the need for security. This paper will concentrate on users that have basic system administration skills and understand the need to go beyond reactive measures; however, it is written to benefit all.

The most significant challenge to conscientious system administrators is dealing with the daily overload of information. The source of this information overload includes but is not limited to dealing with daily tasks, reading daily security advisories, and reviewing logs and system performance. Just processing daily security advisories; determining if they pertain to any systems or services under your purview and taking the necessary actions, if any, can be a full-time job. This task is typically complicated by a lack of system documentation, central management tools and a lack of management support to facilitate accomplishing these tasks. An additional factor increasing the complexity of this task is the number of sources that provide security information. One could spend days reading and dealing with the reports from a single day! With so many sources of security information, how do we maintain a cohesive picture of the current (*and past*) **Threats** and **Vulnerabilities** that hackers use to build the tools, procedures and scripts that put our systems at **Risk**[2]? Organization and discipline is one possible answer. Organizing your system and service installations and configurations is one way to ease the time necessary to filter through advisories. We could also script the process however the time or knowledge may not be available to do this. Discipline goes a long way however, this does not assist in decreasing the amount of time needed. There is still one problem, time. We have not significantly reduced the time needed to perform our jobs

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

simply by being organized. Organization also has individual meaning; my organized is your insanity. We must also assume that as professionals we prescribe to the tenants of organization described above, therefore no significant gain is found.

There remains the question, how to manage the daily demands of our professional life (while maintaining a life) and still have the ability to thwart the threats to our systems and services. The issue is really one of time. Since we cannot create time (yet!), and we cannot clone ourselves (yuk!) we obviously need to be magicians. We know having a rabbit in our hat will not help, but perhaps a bag of tricks, the right tricks, might! The 'Bag of Tricks' term is typically associated with hackers as the tools they employ to compromise our systems[4,5,6]. As a 'Bag of Tricks' is associated with hacking, 'Best Practices' are associated with system administration. While best practices should be adhered to, is it enough? My opinion is no. Obviously, we want system administrators to follow best practices, keep patches current, monitor security information sites[1] for new exploits, and monitor our systems. Keeping these tasks up to date is a time consuming task as outlined above, and this is the chink in our armor. The hacker has all of the time in the world, we don't, or do we… We know that the hacker uses time to their advantage, to take advantage of the system administrator's excessive cognitive load. First, the hacker builds a picture of the network and systems gleaning crucial information for their craft. (*This picture may only include a firewall*) Then the hacker waits for a vulnerability to open so he/she can act. From a practical sense there is little that a system administrator can do to curtail the cataloging of accessible systems (*accessible remotely or via the Internet*), as most system administrators are not willing to disable ping, traceroute, the r-commands and other system and diagnostic tools. While disabling ping will protect us against mass scans, service based utilities (telnet, r-commands, ssh, etc) can still be detected with sys/ack scans. A possible solution here is to implement an ACL (Access Control List) however, this establishes a trust relationship with hosts we typically have no control over. Exploiting this vulnerability is the centerpiece of the infamous Mitnick vs. Shimomura confidentiality attack that exploited a trust relationship[7]. This example demonstrates the fact that there is no silver bullet. This does not mean we are defenseless, however, this could be viewed as disadvantaged. In reality, very few institutions (*NSA, DOD, some corporate*) that care if their accessible network is cataloged, it is the use of this knowledge concerns them. We as system administrators want to create an environment that can quickly recover when faced with adversity.

Thus far, we have established that the system administrator faces a shortage of time, information overload and the inability to total blind the Hacker to our network configuration. Given these facts and the reality of the workload most of us face, our ability to thwart the Hacker's onslaught seems almost pitiful. This is how I felt, until I remembered that a wise man once told me to always carry a 'Bag of Tricks' with me. He also told me to guard its contents from prying eyes. While this advice had nothing to do with computer security or anything remotely related to technology, I have found this advice to serve me well in every arena of my life. Computer security is no exception. Earlier we discussed the use of the 'Bag of Tricks' term, but what is a 'Bag of Tricks'? It is a 'bag' of resources, (*knowledge, tools, supplies, etc.*), that when faced with adversity we dip into to defend ourselves. The reason we keep these 'resources' in a 'bag' is to

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

make their use a surprise. We need surprise since the attacker/hacker has the upper hand in controlling the time of the adversarial actions. [*Note: Surprise is used figuratively. This paper is not dealing with the use of honeypots or honeynets*[8].] Adversity comes in many forms, for our purposes it will be in the form of a computer/network security threat[3]. The SANS definition of a threat model is " vulnerabilities are the gateway by which threats are manifested"[3]. By this definition, no vulnerability means, no risk. A paranoid system administrator (*me*) would extend this to say: "we should treat threatening actions as if a vulnerability exists, since *'vulnerabilities are the gateway by which threats are manifested'* [3]".

I must preface the remainder of this paper by stating that I consider myself new to the realm of Computer Security. The following is a presentation of what I believe to be a good 'Bag of Tricks'. In many ways writing on this topic violates the advice I was given, however, no knowledge can be gained that is not first shared.

Using a 'Bag of Tricks'

There are numerous tools available to the system administrator and hacker alike. All are easily accessible via the Internet and most are straightforward to use. Some of the reasons that these tools are not used have been outlined above. Let us now explore how some of these tools can serve to negate prospective incidents or in the event of an incident, significantly improve our recovery and forensic positions. The procedures and mindset we have discussed and the tools we are about to explore make up the bulk of the contents of our 'Bag of Tricks'. Once complete we will employ this 'Bag of Tricks' similar to a hacker except for defensive purposes. While forensic resources (see The Coroners Toolkit[1,2]) should be available and a part of the 'Bag of Tricks' extensive coverage is not provided here. The reason for this is this paper focuses on proactive system administration while forensic tools focus on 'recovery, collection, and analysis[2].

Proactive not Reactive

With the increasing number of computer security incidents reported daily, it is no longer sufficient to be reactive. Gone are the days of simply reviewing the Cert advisories and taking the appropriate actions. This alone is insufficient; this has become reactive in many ways. The primary reason is the speed with which vulnerabilities are exploited. The answer is in proactive behavior. Treat your systems as a hacker would. Catalog them so that you can move quickly to correct discovered vulnerabilities. Monitor them the way a hacker would so any small change to your systems is detected. Follow Best Practices but use tools to assist in following them. You do not need to be a Hacker to protect your systems from Hackers. No more then we need to be criminals to 'think' like one, and thereby catch one! System Administrator's and Hacker's have different viewpoints of the systems they 'work on'. This somewhat opposing view leads to a weakness for both. The System Administrator's weakness is time, resources and oversight or perhaps underestimation. While as the adversary, the Hacker, has the advantage he does have weaknesses. The Hackers weakness is in the unknown and knowledge. He is never sure of what systems he probes, assaults and if his knowledge is not sufficient he will fail, or what is worse be found out. Though proactive actions, the

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

System Administrator can exploit these weaknesses to his advantage. There is one caveat, there always exists someone better then ourselves we only hope we do not encounter him or her.

The Big Picture Connection

There is one issue related to system administration that should be considered before using a 'Bag of Tricks' or any type of security related tool, accountability. Since the actions we take can have a direct impact on the systems and networks we protect we are accountable. This is can be an awesome responsibility and burden at the same time. System administrators need the freedom to perform job correctly, however the performance of this job may conflict with company policies. Because of this fact, a personal policy statement[9] is an essential resource in your 'Bag of Tricks'. Even though it is not technically a 'trick', a personal policy statement will allow the use of tools (*war dialers, passwords crackers, etc.*) and performance of certain actions (*crack passwords, vulnerability scans, etc.*) typically in blatant violation of standard company policies. Even the most experienced user of any of these tools can have a momentary lapse in judgment or simple mess up! There is one aid in mitigating these mistakes or at the least recovering from them, standard operating procedures (SOP). Establish personal SOPs for all system administration tasks. In doing this, we can cut down significantly the time we spend attempting to remember how things were done. If all servers are configured in a certain way, it significantly reduces the complexity of troubleshooting compared to ad hoc operations. Performing tasks in this way also aids in reducing 'stupid' mistakes, as most tasks become second nature or well documented. The biggest benefit of SOPs is they can fortify your accountability. If there is ever a problem, there is never a question as to how something was done. When dealing with events that are significantly dated we cannot remember 'what we did' unless we prescribe to strict personal SOPs. This can save us considerable explanation!

A Bag of Tricks: The Contents

No magic combination of tools and practices exists (yet!) that comprise the perfect System Administrator's 'Bag of Tricks' (yet!). This is the strength of the **paradigm**. If there were such a list of tools and practices, Hackers would also have it, thereby decreasing its efficiency. Instead, the selection of actual tool sets is left to the individual system administrators who can base its contents on their needs. The following collection of security tools is a compilation of all the tools I have identified through research and networking (*the people kind*). Please review this compilation in an appropriate fashion, it is not meant to be the best ordering of tools or an all-inclusive list. I am sure there will be disagreement on my assessments of the described tools and on those included or excluded. This paper is meant to stimulate the creation of a 'Bag of Tricks' not be the end all guide to the perfect one. There is a great need for System Administrators that excel at their jobs. Adequate system administrators are insufficient to meet today's network and security challenges. That being said we are all suffering from information overload as previously explored. This being the case it is difficult to excel at anything given the constant barrage on our cognitive processing unit (CPU = Brain!). Hence, this collection of security tools, the purpose of this list is two-fold

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

- Stimulate ideas on using different security tools together.
- Offer a resource to help fellow professionals and myself.

A copy of this list will be maintained at http://sp.uconn.edu/~msaba/infosectools.html. Additional and modifications will be made as information presents itself.

The remainder of this section details specific software tools that can and should be included in a 'Bag of Tricks'. A brief description and where appropriate a link is given for each tool. The tools are broken into five categories auditing; monitoring; policing; repelling, and maintenance. While there is significant crossover for some tools for this presentation only one category assignment is made.

The Tools

Auditing tools are used to catalog a machine or network; including services available and can include vulnerability scans.

The first such tool is Nessus[10], a highly rated and respected vulnerability scanner. The Nessus tool has no pre-coded assumptions regarding services and the ports they run on. Nessus is a remote security auditor, using a client/server architecture, with free versions for most flavors of Unix and Microsoft.

Nmap is an Open Source utility for "network exploration and security auditing"[11]. Very fast like Nessus, Nmap produces a picture of a system or network using raw IP packets that includes available hosts and services, the operating system type and version and what filters/firewall if any are employed to name a few. Nmap is a powerful, extensible, well documented, popular, free tool that must be in every 'Bag of Tricks' if for no other reason, everyone else has it!

lsof[12], a simple and powerful command line tool that is not part of most Unix installations. This tool provides the ability to view the open files (ports) to processes. This application is especially helpful after a compromise. lsof is descended from ofile, fstat, and of course, lsof. It is freely available for most Unix platforms. There is an lsof clone available for Windows called fport[13].

Monitoring tools provide us with a benchmark to gauge the state of our systems and/or aid in detecting unauthorized actions on the system. There are standard monitoring utilities in most operating systems, syslog to name one; we must not forget these as our baseline.

Tripwire[14] is perhaps one of the best monitoring tools when employed correctly. This tool verifies the integrity of pre-designated files and directories to notify the administrator of any changes due to tampering or corruption. This is helpful in detecting Trojaned commands, modified log files and the like. Proper operation of Tripwire is essential to insuring its integrity. This tool should be used daily and should be run from a cdrom-

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

drive so that it cannot be Trojaned. Depending on usage Tripwire is anywhere from free to very expensive.

Logcheck[15] version 1.1.1 aids in processing the many log files generated under Unix similar to Tripwire. This open source tool reports any strange behavior via e-mailed upon detection. Another similar open source program is swatch[16] that monitors system log files with predetermined rules and notification scheme.

With auditing and monitoring in place, we must not forget to police our weakest link, the user. Regular scans of the user disk space should be performed for unauthorized applications, incorrect permissions and account misuse. Some of the previous tools can aid in this task, however, our best tool here is scripted system commands run as cron jobs. Our policing efforts should not be restricted to users alone, as the tools will demonstrate.

Password cracking software is an essential part of the system administrators 'Bag of Tricks'. These programs/scripts allow the system administrator to insure that users have selected passwords of sufficient complexity. Most of these programs have features that automatically notify the accountholder that their password has been compromised, and instructs them to change it. This feature is useful, since the system administrator does not need to see the compromised password thereby mitigating his accountability. Password cracking programs include Crack, L0phtCrack, etc.

PortSentry[17] is a port scanning detection utility with the ability to react to the scans. The utility can react to scans by blocking the offending host in various ways through additions to host.deny, adding firewall rules or dropping the route. This utility needs to be handled with care or the Hacker could use it to perform a Denial of Service attack by exploiting its reactive feature.

Prepare to repel boarders! We want to be proactive. We want to do more then just detect scans and possible intrusions. We want to trap or block unwanted activity before it is a problem. TCP Wrappers provide extensive protection for systems when used properly. TCP Wrappers could also take a paper (or 2) to cover so that is left as an exercise. The most prevalent proactive measure today is Anti-virus software, weather it is McAfee, Norton or others, properly configured enterprise wide this can block the majority e-mail borne viruses, worms and malicious scripts. The key to this success is the central administration and speedy reaction time to new e-mail borne security events.

ZoneAlarm is perhaps the best personal firewall software on the market. It is the best because it blocks both incoming and outgoing traffic by application-port pair unless the application-port pair is enabled. This application is included here because ZoneAlarm (like many others) supports Console driven or centralized administration. The end-points of the network tend to be an overlooked access point, similar to modems.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

> With properly configured, centrally administered end-point firewall software in place, our security model is greatly improved. Additionally, the logging features allow data collection to better understand the threats to our network.
>
> Snort[18] is a flexible packet sniffer that detects attacks in real-time, sending and alert to syslog and the system administrator if specified. While Snort falls more in the policing category, it can be combined with other tools or your own actions to proactively stop an attack. "*It is free, scalable and very good at detecting stealthy recon efforts and probes*"[19].

There are several new utilities emerging for most platforms that will ease the burden of maintaining system patches and upgrades. These utilities sound very appealing however there is always an inherent risk in applying an upgrade or patch to a production system especially when it is completely automated. These utilities will significantly decrease the time needed for these tasks when used correctly. In lieu of these utilities, most systems have a utility that facilitate upgrades and patches called tar.

Summary

In presenting this material, several questions come to mind. First, that's it?! The retort is, yes, this presentation is not meant to be exhaustive but to stimulate the creation of a 'Bag of Tricks'. Leaving the list of tools short but comprehensive provides for individual growth thereby enhancing the surprise factor. Another is why a 'Bag of Tricks', isn't a 'Bag of Tricks' really just an IDS? The response to this is no. While an IDS is intended to detect an intrusion and alert you to it, a 'Bag of Tricks' is supposed to aid in thwarting the intrusion. In the event of an intrusion, the 'Bag of Tricks' approach will provide information similar to the IDS. However the 'Bag of Tricks' will include many of the tools need to recover from the incident and IDS won't. This is not to say that we can forego the inclusion of an IDS system in our network when using of a 'Bag of Tricks'. What this means is, an IDS can and should be on of the tricks in the bag! There will inevitably be those who disagree with the 'Bag of Tricks' approach, however, when faced with adversity best practices and reactive measures simply are not enough.

References

1. http://sp.uconn.edu/~msaba/certgroups.html

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

2. SANS Security Essentials threat+vulnerability=risk quote. Pg 1-3
3. SANS Security Essentials pg 1-4
4. Web sites beware: Cyber-vandals armed with bag of tricks
http://sanjose.bcentral.com/sanjose/stories/1999/12/13/story7.html
5. The Back Door Into Cyber-Terrorism: Report Says Security Flaws Give Hackers Easy Access
http://www.punjabilok.com/infotech/backdoor_cyber_terrorism.htm
6. Trapping and Tracking Hackers: Collective Security for Survival in the Internet Age
http://www.recourse.com/download/white/isw2000-urls.pdf
7. SANS Security Essentials pg 1-7
8. What is a honeypot and how is it used?
http://www.sans.org/newlook/resources/IDFAQ/honeypot.htm
9. SANS Security Essentials Pg 6-21-2
10. http://www.nessus.org
11. http://www.insecure.org/nmap/
12. http://www.appwatch.com/Linux/App/47/data.html
13. http://www.foundstone.com/rdlabs/tools.php?category=Intrusion+Detection
14. http://www.tripwire.com
15. http://www.psionic.com/abacus/logcheck/
16. http://www.oit.ucsb.edu/~eta/swatch
17. http://www.psionic.com/abacus/portsentry/
18. http://www.snort.org
19. SANS Kick Start Intrusion Detection: The Big Picture pg 3-7

© SANS Institute 2001, Author retains full rights

Last Updated: May 22nd, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	**Cyberjaya, MY**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
SANS Pen Test Berlin 2013	**Berlin, DE**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
Industial Control Systems Security Training - Houston	**Houston, TXUS**	**Jun 10, 2013 - Jun 15, 2013**	**Live Event**
Security Impact of IPv6 Summit 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 16, 2013**	**Live Event**
SANSFIRE 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 22, 2013**	**Live Event**
SANS Canberra 2013	**Canberra, AU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
Mobile Device Security Summit 2013	**OnlineCAUS**	**May 30, 2013 - Jun 06, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**