



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials Bootcamp Style (Security 401)"
at <http://www.giac.org/registration/gsec>

Intel v. Randal L. Schwartz

Anthony Hakim

October 10, 2004

Who is Randal Schwartz?

Randal Schwartz is a recognized expert in the Practical Extraction Report Language (PERL)^[1]. He is also a consultant who has been actively working in the fields of systems administration, training and computer security for many years. Randal spent a number of years (1988 – 1993) consulting at Intel Corporation^[2] mainly in a systems administration capacity, which arguably included security. In July of 1995, Randal was convicted in an Oregon Court of Law on three felony counts:

1. Mr. Schwartz unlawfully, knowingly and without authorization altered a computer and computer network consisting of Intel computers Mink and Brillig.
2. Mr. Schwartz unlawfully, and knowingly access and use a computer and computer network for the purpose of committing theft of the Intel SSD's password file.
3. Mr. Schwartz unlawfully, knowingly access and use a computer and computer system for the purpose of committing theft of the Intel SSD individual user's passwords.

Count 1 – Randal installed a backdoor program 'gate' on two of Intel's firewalls (on separate occasions), which essentially enabled him to access Intel's internal network (to check email) from the Internet.

Counts 2 and 3 – Randal who was an advocate of good security measures ran the program crack^[3] on a password file from a system which was within a division that he at one time provided systems administration (and still had an active account on, although it should have been disabled), to determine the level of compliance based on Intel's password policy. Upon running this, a password was cracked quite effortlessly. To verify his results (from running crack), Randal logged in to the system using the cracked userid/password. Randal then logged in to a cluster within SSD (which was a division that Randal also no longer administered, nor had access to) with the cracked userid/password. Upon logging in to the cluster, Randal copied its password file to run crack at a later date to determine the level of compliance within this division.

What steps can we take to stop this from happening to us?

There are a number of principles that can be employed to eliminate or minimize the issues that surfaced in the Randal Schwartz case. The flushing out of unauthorized applications (as was 'gate') can be greatly improved by using such practices as Separation of Duties and Configuration Management.

Separation of Duties

People within the organization are the largest category of risk to the LAN and WAN. Separation of duties is a key to internal control and should be, designed to make fraud or abuse difficult without collusion. For example, setting up the LAN security controls, auditing the controls, and management review of the results should be performed by different persons.^[4]

Configuration Management

Configuration Management identifies in detail the total configuration (i.e. hardware, firmware, software, services and supplies) current at any time in the life cycle of each system to which it is applied, together with any changes or enhancements that are proposed or are in course of being implemented. It provides traceability of changes through the lifecycle of each system and across associated systems or groups of systems. It therefore permits the retrospective reconstruction of a system whenever necessary.^[5]

Also, we must ensure that we employ sound user account management policies and procedures. This includes the auditing and subsequent disabling of user accounts for personnel that have been assigned new responsibilities (as was the case with Randal, who transferred from one division within Intel to another).

User Administration

Effective administration of users' computer access is essential to maintaining system security. *User account management* focuses on identification, authentication, and access authorizations. This is augmented by the process of *auditing* and otherwise periodically verifying the legitimacy of current accounts and access authorizations. Finally, there are considerations involved in the *timely modification or removal of access* and associated issues for employees who are reassigned, promoted, or terminated, or who retire.^[4]

An Issue-Specific Security Policy, in this example referring to password auditing/assessment, is strongly recommended as is creating a personal security policy, which should identify and clarify our roles and responsibilities that are beyond the scope of our organization's security policy.

Systems administrators are responsible for taking proactive steps to assure the security of the server. Examples include regularly checking for weak user passwords and checking the system for common security vulnerabilities.^[6]

Summary

I don't think that Randal acted with any malicious intent, in fact he didn't seem to make any attempts to stealth his 'illegal' activities such as running his backdoor

program and crack under his userid merlyn. The backdoor that Randal placed on Intel's firewalls appeared to have been installed and used merely out of convenience. Randal knew that he was violating Intel policy, as he was warned of these breaches on several occasions, but he chose to continue despite the warnings.

Performing password assessments should be a part of every security professional's regimen. We need to regularly audit our passwords to identify and rectify our potential weaknesses. How else are we to know if our user community is using 'hard to guess' passwords or not. The path of least resistance seems to be the one that is most frequently traveled by attackers, so we need to ensure that our organizations have strong password policies and that they enforced. It is essential that we effectively communicate with the user community why it is important that they comply with such policies.

I think one of the most important points is that we, as security professionals need to ensure that we have an insurance policy in the form of a written personal security policy that covers all facets of the tasks that we perform, and that this document is authorized and signed by upper-level management. It certainly would have greatly impacted the Randal Schwartz case.

References

- [1] PERL
URL: <http://www.perl.com> (October 10, 2004)
- [2] Intel Corporation
URL: <http://www.intel.com> (October 10, 2004)
- [3] Crack and its author Alec Muffett
URL: <ftp://ftp.cerias.purdue.edu/pub/tools/unix/pwdutils/crack> (October 10, 2004)
URL: <http://www.users.dircon.co.uk/~crypto> (October 10, 2004)
- [4] Tipton, Hal and Krause, Micki (Consulting Editors) "Handbook of Information Security Management" January 1, 1998
- [5] BS 6488 the British Standard Code of Practice for Configuration Management of computer based systems. [BS 6488 - Ref 4]
URL: <http://www.bsi-global.com> (October 10, 2004)
URL: <http://www.dis.port.ac.uk/~allangw/papers/pub97a.htm> (October 10, 2004)
- [6] Administrative Computing Security Policy – University of Pennsylvania
URL: <http://www.upenn.edu/computing/policy/acsp.html> (October 10, 2004)

Upcoming Training

Click Here to
{Get CERTIFIED!}



SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor