



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 San Francisco Fall 2018	San Francisco, CA	Nov 26, 2018 - Dec 01, 2018	Live Event
Austin 2018 - SEC401: Security Essentials Bootcamp Style	Austin, TX	Nov 26, 2018 - Dec 01, 2018	vLive
SANS Austin 2018	Austin, TX	Nov 26, 2018 - Dec 01, 2018	Live Event
SANS Santa Monica 2018	Santa Monica, CA	Dec 03, 2018 - Dec 08, 2018	Live Event
SANS Nashville 2018	Nashville, TN	Dec 03, 2018 - Dec 08, 2018	Live Event
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201812,	Dec 11, 2018 - Jan 29, 2019	vLive
SANS Cyber Defense Initiative 2018	Washington, DC	Dec 11, 2018 - Dec 18, 2018	Live Event
Community SANS Burbank SEC401	Burbank, CA	Jan 07, 2019 - Jan 12, 2019	Community SANS
SANS Amsterdam January 2019	Amsterdam, Netherlands	Jan 14, 2019 - Jan 19, 2019	Live Event
Community SANS Toronto SEC401	Toronto, ON	Jan 14, 2019 - Jan 19, 2019	Community SANS
Sonoma 2019 - SEC401: Security Essentials Bootcamp Style	Santa Rosa, CA	Jan 14, 2019 - Jan 19, 2019	vLive
SANS Sonoma 2019	Santa Rosa, CA	Jan 14, 2019 - Jan 19, 2019	Live Event
Mentor Session - SEC401	Columbia, SC	Jan 15, 2019 - Feb 26, 2019	Mentor
Mentor Session - SEC401	Jacksonville, FL	Jan 19, 2019 - Feb 23, 2019	Mentor
SANS Miami 2019	Miami, FL	Jan 21, 2019 - Jan 26, 2019	Live Event
Community SANS Omaha SEC401	Omaha, NE	Jan 21, 2019 - Jan 26, 2019	Community SANS
Mentor Session - SEC401	Cleveland, OH	Jan 23, 2019 - Mar 06, 2019	Mentor
Mentor Session - SEC401	Des Moines, IA	Jan 28, 2019 - Feb 27, 2019	Mentor
SANS Las Vegas 2019	Las Vegas, NV	Jan 28, 2019 - Feb 02, 2019	Live Event
Mentor Session - SEC401	Richmond, VA	Jan 31, 2019 - Apr 04, 2019	Mentor
SANS Security East 2019	New Orleans, LA	Feb 02, 2019 - Feb 09, 2019	Live Event
Security East 2019 - SEC401: Security Essentials Bootcamp Style	New Orleans, LA	Feb 04, 2019 - Feb 09, 2019	vLive
Community SANS Raleigh SEC401	Raleigh, NC	Feb 04, 2019 - Feb 09, 2019	Community SANS
SANS London February 2019	London, United Kingdom	Feb 11, 2019 - Feb 16, 2019	Live Event
SANS Northern VA Spring- Tysons 2019	Vienna, VA	Feb 11, 2019 - Feb 16, 2019	Live Event
SANS Anaheim 2019	Anaheim, CA	Feb 11, 2019 - Feb 16, 2019	Live Event
SANS Dallas 2019	Dallas, TX	Feb 18, 2019 - Feb 23, 2019	Live Event
SANS Secure Japan 2019	Tokyo, Japan	Feb 18, 2019 - Mar 02, 2019	Live Event
SANS Scottsdale 2019	Scottsdale, AZ	Feb 18, 2019 - Feb 23, 2019	Live Event
SANS New York Metro Winter 2019	Jersey City, NJ	Feb 18, 2019 - Feb 23, 2019	Live Event
SANS Reno Tahoe 2019	Reno, NV	Feb 25, 2019 - Mar 02, 2019	Live Event