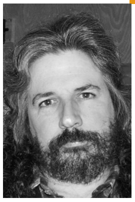
ROBERT G. FERRELL

/dev/random: a realist's glossary of terms widely employed in the information security arena



Robert G. Ferrell is an information security geek biding his time until that genius grant finally comes through.

rgferrell@gmail.com

Accountability: the principle that actions taken on a system can be traced to a specific user who is not under any circumstances you.

Accreditation: a decision taken by a senior management official to allow an information system to operate securely so long as it doesn't negatively impact the budget.

Advanced Encryption Standard: the protocol employed to produce most legislation and contractual documents.

Antivirus: a signature-based software product which sometimes prevents malicious code that the black hat community has long since stopped deploying from infecting an information system.

Botnet: a dynamically distributed sensor array for monitoring the aggregate online user IQ in real time.

Certification: the miraculous process of converting money into expertise by filling in scan sheets.

Compensating Controls: those wholly ineffective measures stipulated by management as a cost-saving substitute for the recommended security controls.

Compromise: the point at which most senior managers realize those memos they've been getting from the information security staff the past few weeks/months/years were not just instances of employee whining, after all.

Cross-Site Scripting (XSS): an undocumented feature of most Web browsers.

Cryptography: the process by which the real meaning of content is obfuscated. Examples include EULAs, legislation, and telephone bills.

Disaster Recovery Plan: a detailed strategy for dealing with the impact of poor executive decision-making.

Distributed Denial of Service: technical name for the Worldwide Web.

Hacking: the process of employing a computer system to some significant fraction of its full potential.

Honeypot: a site where your actions and habits are closely scrutinized; i.e., virtually any commercial site on the Web today.

Incident: something that happens to other people.

Incident Handling: the policies and procedures in place to deal with user behavior.

Information Security: a dangerous, wholly imaginary state achieved by "experts" through a mixture of placebos, false promises, and outright fabrication. Alternate meaning: the condition achieved when all sources of power for the system have been disabled.

Information System Security Officer: a hapless individual charged with maintaining a strong information assurance posture without sufficient resources or management support.

Insider Threat: the elephant in the computer room.

IT Security Investment: a negatively asymptotic value tending toward zero.

Kerberos: a system for secure authentication so long as no one else is listening.

Macro Virus: a feature of most word processing and spreadsheet applications.

Man-in-the-Middle Attack: a bucket brigade where one of the participants substitutes kerosene for water.

Memorandum of Understanding: a mostly incomprehensible document wherein both sides agree not to take responsibility for the security of a shared information system.

Mission Critical: any software or hardware that, if it fails to function properly, may jeopardize the bonus of an executive or senior manager.

Password: a means of identification and authentication that experiences a dramatic loss of efficacy once it passes a length of about eight characters.

Patching: the penultimate phase of the commercial software development lifecycle, immediately preceding cessation of vendor support to the end user.

Phishing: a means for collecting sensitive personal information over the Web. See also: *eCommerce*.

Plan of Action and Milestones: a document detailing the tasks that need to be accomplished and estimating a completion date for each, created to postpone as long as possible actually doing any work to achieve those goals.

Port Scan: a diversionary tactic designed to keep intrusion detection systems and security administrators occupied while the real damage is being done elsewhere.

Residual Risk: that which remains after the IT security budget is exhausted, usually approximately ten working days into the fiscal year.

Responsible Individual: the person whose fault it is when something bad happens. Also known as “that other guy.”

Risk Management: the process by which stakeholders and executive leadership are made to feel all warm and fuzzy about the organization’s security posture by the use of empty assertions, inane media-created buzzwords, and meaningless jargon.

Secure Socket Layer: a Web-based protocol employed to give users the illusion that their transactions are secure by displaying a little padlock in the status bar. The fact that padlocks can be broken with one swing of a sledgehammer is generally ignored.

Social Engineering: the precept that people will tell you anything you want to know if you ask nicely enough.

Spyware: any software that has been downloaded from the Internet, either with or without the user’s conscious participation.

SQL Injection: a clever programming trick employed primarily by obscure commercial sites to augment their media footprint.

System Administrator: see *Scapegoat*.

Threat Assessment: a careful perusal of the employee directory.

Training: the egregiously mistaken belief that “boot camps” are all it takes to prepare someone for the real world.

Trojan: malware that infects your computer surreptitiously if you’re not practicing safe surfing. See also: *Irony*.

User:

1) the principal threat to any information system.

2) the justification for existence of any information system.

Virus: a nasty piece of malicious code that wriggles its way into your machine and disrupts its functioning to the point of non-usability. See also: *Operating System*.