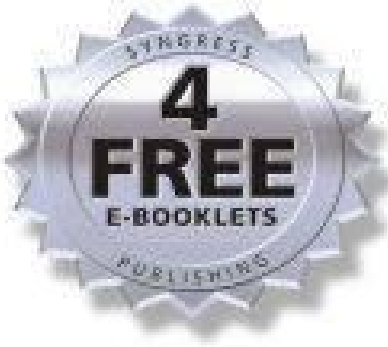
SYNGRESS®

4 FREE BOOKLETS
YOUR SOLUTIONS MEMBERSHIP



Perfect Passwords

SELECTION, PROTECTION, AUTHENTICATION

Create Password Policies That Baffle the Bad Guys, Not Your Users

- Master the 20 Pointers for Perfect Passwords
- Build Password Policies That Won't Be Ignored
- Check Out the 500 Worst Passwords of All Time

Mark Burnett
Dave Kleiman Technical Editor

"DUDE, THIS IS PRETTY COOL STUFF."
—JESPER M. JOHANSSON
MICROSOFT CORPORATION

Table of Contents

Register for Free Membership to

solutions@syngress.com

Over the last few years, Syngress has published many best-selling and critically acclaimed book including Tom Shinder's *Configuring ISA Server 2004*, Brian Caswell and Jay Beale's *Snort 2 Intrusion Detection*, and Angela Orebaugh and Gilbert Ramirez's *Ethereal Packet Sniffing*. One of th reasons for the success of these books has been our unique **solutions@syngress.com** program Through this site, we've been able to provide readers a real time extension to the printed book.

As a registered owner of this book, you will qualify for free access to our members-on solutions@syngress.com program. Once you have registered, you will enjoy several benefit including:

- Four downloadable e-booklets on topics related to the book. Each booklet is approximately 2 30 pages in Adobe PDF format. They have been selected by our editors from other best-sellin Syngress books as providing topic coverage that is directly related to the coverage in this boo
- A comprehensive FAQ page that consolidates all of the key points of this book into an easy-to search web page, providing you with the concise, easy-to-access data you need to perform yo job.
- A "From the Author" Forum that allows the authors of this book to post timely updates links t related sites, or additional topic coverage that may have been requested by readers.

Just visit us at **www.syngress.com/solutions** and follow the simple registration process. You will nee to have this book with you when you register.

Thank you for giving us the opportunity to serve your needs. And be sure to let us know if there anything else we can do to make your job easier.

SYNGRESS®

Perfect Passwords

SELECTION, PROTECTION, AUTHENTICATION

Mark Burnett
Dave Kleiman Technical Editor

KEY	SERIAL NUMBER
001	HJIRTCV764
002	PO9873D5FG
003	829KM8NJH2
004	83TMSW28HT
005	CVPLQ6WQ23
006	VBP965T5T5
007	HJJJ863WD3E
008	2987GVTWMK
009	629MP5SDJT
010	IMWQ295T6T

PUBLISHED BY
Syngress Publishing, Inc.
800 Hingham Street
Rockland, MA 02370

Perfect Passwords: Selection, Protection, Authentication

Printed in Canada
1 2 3 4 5 6 7 8 9 0
ISBN: 1-59749-041-5

Publisher: Andrew Williams
Acquisitions Editor: Gary Byrne
Technical Editor: Dave Kleiman
Cover Designer: Michael Kavish
Page Layout and Art: Patricia Lupien
Copy Editors: Michael McGee, Judy Eby
Indexer:Julie Kawabata

Distributed by O'Reilly Media, Inc. in the United States and Canada.

For information on rights, translations, and bulk purchases contact Matt Pedersen, Director of Sales and Rights, at Syngress Publishing; email matt@syngress.com or fax to 781-681-3585.

Acknowledgments

Syngress would like to acknowledge the following people for their kindness and support in maki
this book possible.
Syngress books are now distributed in the United States and Canada by O'Reilly Media, Inc. Th
enthusiasm and work ethic at O'Reilly are incredible, and we would like to thank everyone there f
their time and efforts to bring Syngress books to market: Tim O'Reilly, Laura Baldwin, Mar
Brokering, Mike Leonard, Donna Selenko, Bonnie Sheehan, Cindy Davis, Grant Kikkert, Op
Matsutaro, Steve Hazelwood, Mark Wilson, Rick Brown, Tim Hinton, Kyle Hart, Sara Winge, Pete
Pardo, Leslie Crandell, Regina Aggio Wilkinson, Pascal Honscher, Preston Paull, Susan Thompson
Bruce Stewart, Laura Schmier, Sue Willing, Mark Jacobsen, Betsy Waliszewski, Kathryn Barrett, Joh
Chodacki, Rob Bullington, Kerry Beck, Karen Montgomery, and Patrick Dirden.
The incredibly hardworking team at Elsevier Science, including Jonathan Bunkell, Ian Seager, Dunca
Enright, David Burton, Rosanna Ramacciotti, Robert Fairbrother, Miguel Sanchez, Klaus Bera
Emma Wyatt, Krista Leppiko, Marcel Koppes, Judy Chappell, Radek Janousek, Rosie Moss, Davi
Lockley, Nicola Haden, Bill Kennedy, Martina Morris, Kai Wuerfl-Davidek, Christian
Leipersberger,Yvonne Grueneklee, Nadia Balavoine, and Chris Reinders for making certain that ou
vision remains worldwide in scope.
David Buckland, Marie Chieng, Lucy Chong, Leslie Lim, Audrey Gan, Pang Ai Hua, Joseph Cha
June Lim, and Siti Zuraidah Ahmad of Pansing Distributors for the enthusiasm with which the
receive our books.
David Scott, Tricia Wilden, Marilla Burgess, Annette Scott, Andrew Swaffer, Stephen O'Donoghue
Bec Lowe, Mark Langley, and Anyo Geddes of Woodslane for distributing our books throughou
Australia, New Zealand, Papua New Guinea, Fiji, Tonga, Solomon Islands, and the Cook Islands.

Author

Mark Burnett is a recognized security consultant, author, and researcher who specializes i hardening Microsoft Windows-based servers and networks. He has spent nearly a decade developir unique strategies and techniques for locking down Windows servers and maintaining his specialize expertise of Windows security. Mark is coauthor and technical editor of *Microsoft Log Parser Toolk* (Syngress Publishing, ISBN: 1-932266-52-6), author of *Hacking the Code: ASP.NET Web Applicatio Security* (Syngress Publishing, ISBN: 1-932266-65-8), coauthor of *Maximum Windows 2000 Securi* (SAMS Publishing, ISBN: 0-672319-65-9), and coauthor of *Stealing the Network: How to Own t Box* (Syngress Publishing, ISBN: 1-931836-87-6). He also contributed to *Dr.Tom Shinder's ISA Serve and Beyond: Real World Security Solutions for Microsoft Enterprise Networks* (Syngress Publishin ISBN: 1-931836-66-3) and was a contributor and technical editor for *Special Ops: Host and Netwo Security for Microsoft, UNIX, and Oracle* (Syngress Publishing, ISBN: 1-931836-69-8). Mark speal at security conferences and has published dozens of security articles that have appeared publications such as *Windows IT Pro Magazine* (formerly *Windows &.NET Magazine*) , *Redmor Magazine*, *Windows Web Solutions* , *Security Administrator*, *SecurityFocus. com*, *TheRegister.co.u* and *WindowsSecrets.com*, among others. Microsoft has twice recognized Mark's contribution to th Windows community with the Windows Server Most Valued Professional (MVP) award.

Technical Editor

Dave Kleiman (CAS, CCE, CIFI, CISM, CISSP, ISSAP, ISSMP, MCSE) has worked in th Information Technology Security sector since 1990. Currently, he is the owner SecurityBreachResponse.com and is the Chief Information Security Officer for Securit-e-Doc, In Before starting this position, he was Vice President of Technical Operations at Intelliswitch, Inc where he supervised an international telecommunications and Internet service provider network. Dav is a recognized security expert; a former Florida Certified Law Enforcement Officer, he specializes computer forensic investigations, incident response, intrusion analysis, security audits, and secu network infrastructures. He has written several secure installation and configuration guides abo Microsoft technologies that are used by network professionals. He has developed a Windov Operating System lockdown tool, S-Lok (www.s-doc.com/products/slok.asp), which surpasses NS NIST, and Microsoft Common Criteria Guidelines. Dave was a contributing author to *Microsoft Lo Parser Toolkit* (Syngress Publishing, ISBN: 1-932266-52-6). He is frequently a speaker at mar national security conferences and is a regular contributor to many security-related newsletters, We sites, and Internet forums. Dave is a member of several organizations, including the Internation Association of Counter Terrorism and Security Professionals (IACSP), International Society Forensic Computer Examiners® (ISFCE), Information Systems Audit and Control Association (ISACA), High Technology Crime Investigation Association (HTCIA), Network and System Professionals Association (NaSPA), Association of Certified Fraud Examiners (ACFE), An Terrorism Accreditation
Board (ATAB), and ASIS International®. He is also a Secure Member and Sector Chief fo Information Technology at The FBI's InfraGard® and a Member and Director of Education at th International Information Systems Forensics Association (IISFA).

Techical Reviewer

Ryan Russell (Blue Boar) has worked in the IT field for more than 13 years, focusing on informatio security for the last seven. He was the lead author of *Hack Proofing Your Network, Second Editio* (Syngress, ISBN: 1-928994- 70-9), contributing author and technical editor of *Stealing the Networ How to Own the Box* (Syngress, ISBN: 1- 931836-87-6) and other books in the Stealing the Netwo series, and a frequent technical editor for the Hack Proofing series of books from Syngress. He als was a technical adviser on *Snort 2.0 Intrusion Detection* (Syngress, ISBN: 1-931836-74-4). Rya founded the vuln-dev mailing list and moderated it for three years under the alias "Blue Boar."

Chapter 1

Passwords: The Basics and Beyond

…alighting from his beast, he tied it up to a tree, and going to the entrance, pronounced the wor
which he had not forgotten, "*Open, Sesame!*? Hereat, as was its wont, the door flew open, a
entering thereby he saw the goods and hoard of gold and silver untouched and lying as he had le
them.

—Arabian Nights, The Forty Thiev

The Beginning

My fascination with security began perhaps a decade ago when I took my first job with the offici title of software developer. I had written code casually for years, but this was the first time someo paid me to do it. I was a corporate employee. I wrote code all day. I had a network account that logged in to every morning. Like almost everyone else at the company, I had a weak password that swapped every three months with another weak password.

I had been interested in various aspects of security for a long time, but information at that time w scarce. Back then, you couldn't just search on Google for something; you found the good informatio by navigating an endless pathway of hyperlinks from one Web site to the next. The information that did find was often obsolete, unreliable, or limited in context; thus, I was left unsatisfied.

Nevertheless, I studied everything I could find during any spare minute I had. After I read an reread stacks of printouts, they slowly started to make sense to me. Although I was merely a beginne I learned a few tricks that enabled me to gain already some rank as the office hacker.

Then one morning I got my calling. A friend of mine who was one of the company executive pulled me into his office, explained a predicament the company faced, and told me that the compan needed my help. The senior network administrator had been in a heated argument with the compan vice president earlier that morning. In the middle of the argument, the network administrator slamme his keys on the table, cleared out his desk, and left the company. Now, the company manageme wanted me to break in to all the systems and recover all the administrator's passwords because the V was too scorned to call the admin asking for the passwords. I knew that I didn't have the experience take on such a task, but still I couldn't help being seduced by the challenge. I told him I would do it.

But once I sat down at my desk, reality set in; I was enormously intimidated by this undertakin Sure, I knew a few tricks, but presuming that I could actually accomplish this task was absurd. thought that perhaps I should have admitted to my friend that I wasn't as skilled as he thought. Had gone too far? Had my own hubris clouded my judgment? As inconsequential as this incident migh sound, it was my defining moment.

I could have failed. I would have failed that day if I had not discovered this remarkable truth abo hackers: their superhuman skills don't make them successful; rather, everyone else fails so much security that hackers just make it look easy. I discovered that people don't have strong password Moreover, we use the same passwords repeatedly, never straying far from a few core passwords. Whe it comes to passwords, we just aren't that clever.

I obtained the administrator's Microsoft Access password and then his e-mail password. Next, I g his Windows NT administrator password. One password at a time his security fell—*superman1 superman23*, *superman95*, *Wonderwoman*.

I didn't do anything special that day except discover this decisive weakness of human security- that is, that humans are horribly predictable. Late that night I e-mailed the list of passwords to m friend. I went home, buzzing from the thrill of what I had just accomplished.

The next morning I just happened to approach the office building at the same time as the compan president and vice president. They both turned, and as if they had rehearsed it beforehand, opened th front door and bowed before me. I was confused at first, but then realized that they had already hea about the passwords I had collected. I walked through the doorway feeling happy for the recognitio from the top of the company. I loved the attention, but from that point on, I was infatuated—almo obsessed—with security, passwords, and the character of human behavior.

Passwords, in some form or another, have long been associated with security. We see it in literatur all the time: to unlock a door, to pass a guard, or to distinguish friend from enemy. These ambiguou words or phrases are the keys to magical spells or the secret codes to identify one spy to another.

Secret codes are an indispensable part of our modern lives. We use them to check our e-mail ar voice mailboxes. We need them to withdraw money from an ATM or to connect to our online bankin account. We use them to authorize financial transactions and to buy and sell items on the Internet. W use them to limit access to wireless Internet connections and to encrypt our most sensitive priva data.You may even find yourself needing a password to order pizza, purchase flowers, rent a DVD, get a car wash. We are a world of secrets.

Whether they are referred to as passwords, PINs, passcodes, or some other name, they are all secr keys that we hold to gain access to the protected portions of our lives.

Passwords are more than just a key. They serve several purposes. They *authenticate* us to a machi to prove our identity—a secret that only we should know. They ensure our *privacy*, keeping o sensitive information secure. They also enforce *nonrepudiation*, preventing us from later rejecting th validity of transactions authenticated with our passwords. Our username identifies us; the passwo validates us.

But passwords have some weaknesses: more than one person can possess knowledge of the secret any one time. Unlike a physical key that only one person can hold at a time, you have no guarant that someone else hasn’t somehow obtained your password, with or without your knowledg Moreover, there is a constant threat of losing your password to someone else with malicious inter Password thefts can and do happen on a daily basis—by the thousands.Your only defense is to build strong password, protect it carefully, and change it regularly.

The other weakness with passwords is human behavior. Human nature is such that we do not fe threats that we do not perceive. We cannot imagine why someone would want to gain access to our mail or network accounts. We feel reasonably safe with the passwords that we select.

That one day at work, I walked past the company president and vice president, passed through th entrance, walked down the hall, and sat down at my desk. I logged in to my network account with m own weak password and was suddenly struck with the knowledge of my own weakness. I realized th my own security was just as fragile as the security system that I had broken the day before. Just seei my last two passwords, someone could easily guess my current password and probably the next or after that. At least one other coworker already knew my password because I shared it with him one da when I was out sick so that he could access my files. I decided that day to change my attitude abo passwords.

A number of years ago, I sat in an audience and watched a performance of the amazing Kreskin, a sel proclaimed mentalist. I watched as he consistently predicted and manipulated the human behavior the audience. During his tricks, he explained that he didn't have any special powers, just a extraordinary understanding of human behavior.

He consistently guessed secrets selected by the audience and related facts about the personal liv of many audience members, facts such as their social security numbers or dates of birth. He is n alone. Psychics, fortune-tellers, mediums, magicians, and others often depend on human predictabili for the success of their crafts. Undoubtedly, people just behave the same.

If you ask someone to name a vegetable, 98 percent of the time, that person will tell you a carro Tell someone to pick an even number between 50 and 100, where both digits are different, mo commonly people will pick the number 68. Think of a card. The most common choices predictably a nine of diamonds, ace of spades, queen of hearts, or the six of clubs.

You might even find yourself with exceptional skills at predicting human nature, anticipating th behavior of others, for example, or guessing the ends of movies. Remarkably, as poor as we are avoiding predictability, we are exceptionally capable of detecting predictability in others.

Consider the list of random passwords shown in Table 1.1. If you study the list for a few minute you will start to see simple and predictable patterns emerge.

bmw66	fuzzy1	trisha
Jessica1	Steven	123456
sa1856	Alexis	gregory2
843520	xmen94	brutus1
0214866	link11	lakers7
m9153p	1nani1	lamacod1
cyril87	Bubba1	pariz2
7082382	856899	letmein
100265	grady6	tiger69
jimmyd2	mpick1	cats999
wes333	mjordan2	supra1
053092	sti2000	bearcub
4Obelix	usa123	wargame6
6Bueler	Lieve27	dan1028
Franc1	3089172	13crow
Nicole3	Roswell	ncc1701
elin97	67bird	jun0214
toyota4	rat22	password

Table 1.1 Random Passwords

The amazing thing is that this small list accurately represents the nature of human passwords. could give you a list of a thousand or even a million passwords, and you would learn little more abo passwords than you could from this small list.

I know because I have actually done it. Over the years I have collected real passwords from eve source I could find. I have collected almost 4 million passwords, and my list continues to gro through an automated set of tools that scour the Internet for passwords, often using nothing more tha ordinary search engines such as Google. I collected these passwords to gain a better understanding how people select passwords. For five years I collected, researched, and stared at passwords- thousands of *QWERTY*s, thousands of *12345*s.

The most amazing discovery I made was absolutely nothing. Having more passwords did not chang any of my password statistics; the choices of characters remained the same. The top 500 passwor were mostly the same. Password length, complexity, and lack of creativity—all unchanged.

In fact, my numbers were pretty close to other password studies conducted decades ago. Passwor were—and still are—predictably the same over and over: a number or two at the end, a couple numbers at the beginning, all numbers, names of loved ones, dates, vehicles, sports teams, pop cultu references, and the ever-present *letmein* and *password*. I could collect another four million passwor and would probably get the same results.

If anything frustrates me about passwords, it is that so many people think they are being clever unique, but they just aren't. If you could see a million passwords, you would probably be surprised find that your password looks a lot like everyone else's. If you have ever gone on a long flight acro the continental United States, you might have noticed that there is not a lot to see but thousands square miles of empty space. Occasionally, you pass over a cluster of civilization, but then it's rig back to empty land.

That is very much what I see when I look at passwords. So many possibilities remain untouche while thousands cluster around the same few passwords.

Over the years, I began to categorize passwords by their patterns. Here are some of the mo common categories of password-writing patterns. These are examples of what you should *not* d never follow these patterns.

Weak Wordlist Words

This category includes dictionary words, your first or last name, a common password, or a simp phrase that you are likely to find on some wordlist somewhere. These passwords are the worst becau they are so vulnerable to dictionary attacks as explained in the next chapter.

- cupcake
- auto
- badger
- letmein
- Jonathon
- Red Sox
- dirty dog

Weak Wordlist Words with Numbers

Only trivially stronger than a simple wordlist word, these passwords include numbers that people ad to the front or end of a password in attempt at security or to meet specific policy requirements. He are some examples:

- deer2000
- atlanta33
- dana55
- fred1234
- 99skip

Weak Wordlist Words with Simple Obfuscation

Again, these passwords are only slightly stronger than a simple wordlist word. These passwor usually have some simple character replacements or deliberate misspellings. Here are a few example

- B0ngh
- g0ldf1sh
- j@ke

License Plate Passwords

These passwords include some short phrase that makes use of abbreviations, numbers, or oth techniques. These passwords certainly are stronger than a wordlist word, but they are by no mea unique. They often read like license plates. Here are some examples:

- sk8ordie
- just4fun
- dabomb
- kissme
- laterpeeps

Weak Wordlist Words Doubled

Most password-cracking tools will check for this simple pattern. Here are some examples:

- crabcrab
- patpat
- joejoe

Garbled Randomness

These passwords are technically more secure because they are random and less predictable, but as yo will read in this book, having a password that is easy to remember and easy to type is also essential f security. Here are some examples:

- 9uxg$t5C
- Bn2#sz63j
- &fM3tc8b

Patterns or Sequences

These passwords could fall into the category of wordlist words because they are so common. The passwords include some pattern or sequence that is based on the appearance or shape of letters or the location of the keys on the keyboard.

- QWERTY
- 123456
- xcvb
- abc123
- typewriter (all letters on the same keyboard row)

Summary

The single most important aspect of information security is strong passwords. Likewise, the sing greatest security failure is weak passwords. Network administrators blame users for selecting su poor passwords, and users blame network administrators for the inconvenience of their draconi password policies.

Further complicating the problem are hundreds of thousands of software and hardware products th have been and continue to be sold with default passwords that users never get around to changing (s defaultpassword.com to understand how big this problem really is).

People select poor passwords and do little to protect them. They share their passwords with othe and use the same passwords repeatedly on multiple systems. At the same time, computing power h increased along with the number and quality of tools available to hackers.

Consequently, many have predicted that passwords, at least by themselves, will someday becom obsolete. I hear people talk about retina or fingerprint scanners, but at some point, security will st involve some secret, some password.

The good news is that passwords don’t have to be obsolete. In this book, I describe techniques f how you can build very strong passwords and explain how to protect your password from attack. A we need to do is follow some simple rules, use some basic common sense, and treat our passwor like real secrets. By implementing these practices, we can extend the life of this simple method authentication.

The age of the password is not over yet.

Chapter 2

Meet Your Opponent

The Cracker

Password cracking is the method of employing various techniques and tools to guess, methodical determine, or otherwise obtain a password to gain unauthorized access to a protected resourc Password cracking is sometimes used to legitimately recover a lost password, and sometimes a administrator will use password cracking to test user passwords. But, for the most part, passwo cracking is used to steal passwords.

Some call it a game; others, a crime. But whatever it is called, both the most talented comput professionals and the novice use it. As one hacker told me, "[Password cracking] is power… the pow to compel a system to yield its knowledge."

I met that hacker in an IRC room. Well known in the hacking underground for his specialize password-cracking software, this hacker agreed to speak with me on conditions of anonymity—n even a reference to his pseudonym. "I'm not a hacker or an exploiter. I just crack passwords," he to me, "but still everyone calls me a hacker. Hacker, cracker; it's all the same."

Why does he do it? "For trading, selling, sharing," he told me. "It gets me respect, and, hey, it's fu and addicting," he explained, "and I'm not the only one doing this; it goes on all the time."

This is the reality. There are people who steal passwords for some form of gain, and it happens a the time.

Perhaps the most common question I hear when it comes to security is, why would one individu have anything tantalizing enough for a hacker to steal his or her passwords? One reason for hacker attacks might be to disguise their identities for purposes such as sending spam, or the attack might b just one jump in the process of leapfrogging toward bigger targets. The attack might be to perfor financial transactions to defraud others, or it might be to gain access to one of your subscribe services. The fact is that you cannot even comprehend the ways in which your password would b useful to another.

Password theft is a huge problem. Some Web sites are obviously more attractive targets, but n target, no matter how small, is exempt from this problem.

Password Cracking

Password cracking, once a specialized skill, is now available to just about anyone using wide available tools with names like L0phtcrack, John the Ripper, and Cain & Abel. However, befor learning about password-cracking techniques, it is important to understand how a system stores yo password.