

DISSECTING THE HACK

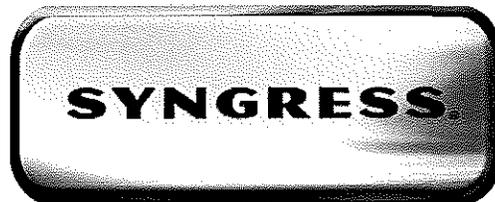
The Forbidden Network |

Jayson E. Street |
Kent Nabors |

If you like what you read here, get 30%
of the list price with the discount code
F0rb1dd3n at checkout.

Publishing September 2009.

Go to **www.syngress.com** to redeem.
WWW.SYNGRESS.COM



AUTHOR BIOGRAPHIES

Jayson E. Street

Jayson is well versed in the ten domains of Information Systems security defined by the International Information Systems Security Certification Consortium. He specializes in intrusion detection response, penetration testing, and auditing. He also has a working knowledge of the implementation and administration of major firewalls, vulnerability scanners, and intrusion detection systems.

He has created and conducted security awareness training for a major Internet bank and has created security policies and procedures currently used by several companies. He also created and taught a three day training course on Intrusion Detection Systems for an undisclosed government agency in Washington D.C.. He has also created and taught a workshop on ethical pen-testing with Backtrack 3 for ISSA. He also taught a two day class for BackTrack 4 for ISACA.

His consultation with the FBI and Secret Service on attempted network breaches resulted in the capture and successful prosecution of the criminals involved. In 2007 he consulted with the Secret Service on the WI-FI security posture at the White House.

He has also spoken from Belgium to Brazil and at several other colleges and organizations on a variety of Information Security subjects.

He has attended XCon 2008 in Beijing, the 25th CCC in Berlin, SYSCAN '09 in Shanghai as well as PH-Neutral 0x7d9 plus he is a regular attendee at Black Hat and DEFCON.

Forbes and Scientific American interviewed him regarding his research on the issue of cyber-warfare as it relates to China and their preparedness for an online war. He was an expert witness in two cases involving the RIAA. His declaration was on Slashdot and other websites and is currently being taught as source material at a University in Massachusetts.

He is on the SANS GIAC Advisory Board as well as a mentor for SANS. He is also a current member on the board of directors for the Oklahoma "INFRAGARD". He is also Vice President for ISSA OKC and a member of the "OSVDB". Jayson is also a longtime member of the "SNOsoft" research team.

On a humorous note he was chosen as one of Time's persons of the year for 2006. ;)

Kent Nabors

Kent Nabors serves as Vice President of Information Security for a multi-billion dollar financial institution. He has significant experience in both the banking and IT industries. He has worked in bank examinations with the Federal Deposit Insurance Corporation and the Federal Reserve Bank.

Kent's background includes security policy development, systems implementation, incident response, and training development.

Kent is a graduate of the University of Oklahoma and Southern Nazarene University.

When he isn't thinking about locking down bits and bytes, he is usually trying to keep up with his wife and two daughters. Quiet time usually involves power tools or an eclectic reading list.

ROUGH DRAFT

WWW.SYNGRESS.COM

Copyright 2009 Elsevier

How to Read

DISSECTING THE HACK

The Forbidden Network

Both sections of this book tell a single story. The adventures of Bob and Leon are more than just a fun read. They illustrate many very real threats to individuals, businesses, organizations, and even countries. The networked world is so interconnected; many don't realize how valuable a target they really are. The best and worst of humanity connected with the speed and power of modern technology comes together in a world of our own making that we do not yet understand.

DISSECTING THE HACK: The Forbidden Network tells the story of two kids caught up in an adventure they did not expect. Bob and Leon are most comfortable in a digital world, but soon find that digital actions have physical consequences. Throughout their fictional story are real-world lessons.

"The Security Threats Are Real" or STAR focuses on those real-world lessons. The hacks and tools in the fictional story are very real. STAR provides the details, sources, and references to learn more about the threats, defensive techniques, attacker techniques, and even cool toys of the fictional story.

The Forbidden Network can be read by itself as a story. It can also be read as an illustration of the issues described in STAR. Throughout The Forbidden Network you will find links that point to specific references in STAR where you can get more information about key concepts. Or if you read STAR, you will find links to The Forbidden Network where the story illustrates a scenario where very real tools and techniques are applied. Each section leans on the other. How you read them is entirely up to you.

For the more adventurous reader, The Forbidden Network contains "Easter Eggs" as well. Woven throughout are references, hints, phrases, and more that will lead you to significant or trivial insights into hacker culture. Again, STAR will help you find out more about the "Easter Eggs." But not all the answers are given away. There must be some unsolved mystery to make hacking worth the time.

So read The Forbidden Network as a story. Read STAR as a reference work. Dig for "Easter Eggs" in The Forbidden Network. Or put it all together to learn more about the very real threats of the digital world we all live in.

DISSECTING THE HACK: The Forbidden Network can happen IRL.

PROLOGUE

00000000

A New Assignment

Thursday, 9:24am

Stepan Senn looked up at the clear blue sky of a fall morning. He could hear the crunch of dry grass beneath him as he turned his head slightly. The cool air on his face felt sharp against the hot blood that trickled from the corner of his mouth that was quickly swelling. He tried to sit up, but his body wouldn't obey. There was a sharp sound of metal on metal. The sound was familiar, but his mind wasn't working fast enough to recognize his situation. He craned his neck as he struggled to look above him. He saw legs, a hard face looking down at him, and a gun. The shape of the gun seemed to grow large enough to fill all he could see.

Everything began to spin in his mind. He closed his eyes hard against the image.

“Sir? Excuse me, sir?” A hand touched Stepan on the shoulder and he jolted awake. “I’m sorry, I didn’t mean to startle you.”

“No problem.” Stepan replied automatically as he picked up the briefcase he had just kicked over. He hadn’t realized how tired he was after staying up late the last couple of nights.

“Sir, I believe your flight is boarding.”

Stepan looked blearily at the Aeroflot gate agent. As his brain came back into focus, he stood.

“Thank you,” he replied as he gathered his briefcase and carry-on bag. He made his way down the gangway and onto the plane in a mental fog. His clouded mind began to clear as it processed the surroundings he had awakened to find.

Stepan Senn’s job had taken him all over the world. He had flown in many types of aircraft. But the Russian Tupolov 154 was not his favorite. He had flown on Aeroflot a couple of years after the collapse of the U.S.S.R. He remembered back then all the staff put on a good show, but the aircraft itself had looked tired. The exterior paint was faded and chipped. The interior was worn. Seats were dirty. Even the crew’s uniforms looked threadbare. Stepan hadn’t been convinced then that the plane should have been in service.

Stepan also remembered when he was in Barcelona on business not that long ago and an Aeroflot pilot landed this same type of aircraft 250 meters to the right of the runway. Aeroflot just wasn’t good enough for Stepan.

As he took his seat, this aircraft didn’t improve his impression of the airline. The cabin was more cramped than similar-sized Boeing and Airbus planes Stepan had flown in. Its oval shape and low ceiling made sitting in a window seat particularly unpleasant. He was thankful that he wouldn’t be repeating this journey.

“But what should I expect when I’m flying to the second-poorest country in Europe?” he thought to himself.

After they reached cruising altitude, Stepan relaxed again and closed his eyes. He began to think back to how he had ended up on this flight. He had been in Moscow. October trips to the Russian capital weren’t a problem for a man from Switzerland. A Russian Autumn was a nice change of pace, and his employer made sure he traveled well. Or that’s what he had believed until now.

Stepan had been sent to hand-deliver a package to the office of one of his employer’s partners. He didn’t know the full story of what he had been carrying, but not-knowing was a major part of his job. He had handed the envelope to the receptionist. Once she had sent an email to his boss confirming delivery, Stepan left the office with his Moscow business complete. He knew better than to ask questions or, even worse, try to see what was on the disk he had guessed had been in the envelope.

It was a clear, cold day, so Stepan decided to walk back to the hotel. It only took about twenty-five minutes for the walk to the Rossiya Hotel. He even took the time to go past the east side of the Kremlin, turning at the Spasskaya Tower and on to the Rossiya. Once in his room, Stepan turned on his laptop and connected it to the hotel network. He typed in his overly long password, all the while wishing for some painful end for the skinny technician back at the office that insisted everyone had to memorize such nonsense just to gain access to their laptops.

(□Pg. #)

Stepan pulled out his access token and typed in the six-digit random number from the token and the four-digit PIN he had memorized. Soon he had established an encrypted

connection to the office back in Zurich, Switzerland. (□Pg. #) He opened his email software and found the message waiting for him:

Your contact is waiting in Chisinau, Moldova. Your flight arrangements have been made. You leave at 7:00am local time tomorrow on Aeroflot. You are booked in the Hotel Dedeman Grand Chisinau. There is a package for you at the front desk that you need to deliver.

You will meet Simon Torgova at the outdoor café across from the Central Garden on Columna Street the day you arrive at 3:00pm local time. Tell him his password is the same as your project name. Report back here when an agreement is obtained.

This was Stepan's first project where he had been "let in" on more of the story. He had grown tired of the desk time he spent as a researcher for an international oil-brokerage firm headquartered in his hometown. He had come up with an idea that could give his employer a huge advantage in the international trading game. In fact, he believed he had created a new product line for their brokerage activities: information. He had identified the target company and even found someone that might be easily influenced to assist them. When Stepan turned in all of his research, he was told to do some courier jobs while preparations were made. It had been two months before this email message from his boss told him it was time for action.

Stepan's boss had taken care of identifying an appropriate operative. Stepan didn't have any contacts that could help him with that part of the project. But this project started with his

idea. He would be able to move out of research and maybe have a chance to be in on some of his employer's deals. But why Moldova, and where was that, anyway?

Stepan opened Google and typed in "Moldova." He thought he had seen a lot of the world, especially in the last two months of fieldwork, but backwater former Soviet territories had not been on any previous itinerary. "*Land-locked, near the Black Sea, south of Ukraine and east of Romania. Why would anyone want to operate out of such a place?*" he thought to himself.

With a jolt Stepan opened his eyes. He had fallen asleep again. As the plane dissipated its speed over the bumpy runway in Chisinau, Stepan blinked his eyes and looked around. He made a promise to himself to either drink more coffee or sleep better on his next trip. It was time to begin his work in Moldova. He pulled his briefcase out from under the seat in front of him and waited for the plane to stop at the gate.

Stepan looked out the window of the aircraft. The side of the airport facing the tarmac was neglected and dingy. The plane finally stopped short of the terminal and stairs were rolled to the door. Stepan and his fellow travelers had to walk down the stairs, across the tarmac and into the airport. No covered automatic walkways with protection from the weather.

"*Why Moldova?*" Stepan mumbled to himself as he walked through the airport, his poor opinion of the little country now confirmed. The inside of the airport was a relic of past glory – although glory was hardly the word to describe it. The faces of the people sitting and waiting for flights seemed much happier than those of the arriving passengers. Stepan's countenance matched his fellow travelers as he waited for his one suitcase.

Once outside the airport, Stepan turned and looked at the front of the building. Its blue windows and bright red front entrance were a clean, modern-looking contrast to the run-down cold war relic he had seen from the other side. Stepan shook his head as he was suddenly even more grateful for living in Switzerland. He soon found a taxi to take him to the Dedeman. The weather was warmer than Moscow, but still brisk.

“Welcome to the Dedeman sir, how long will you be staying with us?”

“One night.”

“All right, if you will fill out this information, I’ll get a room for you.”

The clerk passed a form and pen to Stepan. As Stepan completed the form, he asked, “Do you have a concierge?”

“Yes sir. His name is Viktor. He is right over there” the clerk pointed to an average-sized young man standing at a counter on the other side of the lobby.

“Thank you.”

“And sir, I believe this is for you.” The clerk turned and pulled a small, bulging envelope from a desk behind the counter and handed it to Stepan. Stepan collected the envelope and the key card for his room and walked across the lobby to Viktor.

“Welcome sir, what can I do for you?”

“I will be checking out in the morning. I’m in room 330. Please make sure I have a taxi ready at 8:00am for the airport.”

“No problem sir. Anything else?”

“Yes. Is that the Central Garden across the street?” Stepan asked as he pointed to the front of the hotel.

“Yes sir. It’s not as pretty in the fall, but it is still a good place to start if you would like to take a walk around town.”

As Stepan walked away, Viktor typed a note in the hotel’s new guest information system so he would get a reminder in the morning to have the cab ready for Mr. Senn, room 330.

Stepan made his way to his room, set his bag and briefcase on the bed and checked his watch. He was hungry and he had several hours before his meeting. He checked his pockets.

“Envelope. Room key. Wallet. Phone. Okay, time for food,” he told himself as the door closed behind him. He left the elevator, made his way through the lobby to the hotel restaurant. He was soon seated by an attractive, if over-eager hostess with bright eyes and a quick smile.

“Okay, perhaps there are a few redeeming qualities to this country,” he thought as he took the menu and returned the smile from the hostess.

Stepan took his time making a selection and then settled into a decent meal. Sitting still and eating was a pleasure compared to his flight.

Viktor watched from across the lobby as Stepan began to eat. He had worked as a concierge for the hotel for almost a year. It gave him an opportunity to practice his language skills and make the Leus needed to pay for school. The phone call Viktor was about to make would get him the Euros he needed for pocket money.

“I think your guest has arrived.”

“Are you sure?”

“You said there would be a business man traveling alone; he would arrive this afternoon, and only stay for one night. We’ve only had one man check in by himself today and he’s scheduled to check out in the morning.”

“Good job. We will be there shortly. Pay attention and let me know if he leaves the hotel.”

Stepan finished his meal, charged it to his room account and then walked out onto the street. Moldova wasn’t much, but he would at least have a look while he had the time. He didn’t notice how carefully Viktor watched his movement and noted the time as he left.

Two men entered the lobby a few minutes later. Vlad was middle-aged and tall, with cold gray eyes and dark brown hair cut tight on the sides but just long enough on top to show a natural wave he brushed back as they came out of the breeze. He moved with the ease of an athlete, but was dressed like a well-traveled businessman with a black open collared shirt and silk sport coat. Pavel was younger and shorter. He had dirty-blond hair that was pulled into a short ponytail and a rather dingy backpack slung over one shoulder. He stooped under the weight of the load as they made their way across the lobby to the concierge.

Viktor was nervous as Vlad approached, but the presence of Pavel, Viktor’s older brother helped him stay in control.

“Hello, Viktor. Thanks for the call.”

“Sir, here is the room key you misplaced,” Viktor said a little too loudly.

“Thank you. I always liked the service at this hotel. Your brother here is doing good work for me. Keep up your studies at university and maybe I’ll have a job for you as well.”

“Yes, sir. Your associate left just five minutes ago.”

Vlad took the room key card and made their way to Stepan’s room along with his companion. Inside they found what they were looking for – a briefcase with a new IBM Thinkpad computer inside. It was one of those ultra-light computers that doubled as an executive toy.

“Pavel, start with the laptop while I have a look around,” Vlad ordered.

While Vlad walked around room, looking in drawers and sorting through Stepan’s suitcase, Pavel lifted the computer deftly as someone who was comfortable with any device connected to a keyboard. He turned on the power and hit the default key combination to modify the boot settings. No power-on password. Pavel could always count on business-types to not think of the basics. They always thought spying was only targeted at governments. (□Pg. #)

Pavel enabled the laptop for booting from a USB device. He pulled out his keychain and plugged the tiny storage device into the port on the right of the laptop case. Instead of the normal start-up screen that Stepan saw every day, Pavel was greeted with a black screen with a few simple command options. This was a handy tool Pavel had picked up from a security web site. It allowed him to reset any password on a Windows system as long as he could control how the system started. Pavel didn’t bother giving the Administrator account a new password. He set it to a blank password, disconnected his USB device and rebooted the machine. (□Pg. #) Soon the Windows XP “splash” screen appeared. He typed in “administrator” for the ID and no

password and pressed the “Enter” key. He was in. Pavel turned the computer on the small desk and stood to give Vlad room to sit down.

“This is too easy. I wish he had used another hotel,” Pavel said as Vlad sat in front of the now unlocked computer. “At least then it would have been a challenge.”

“What challenge would you want?” asked Vlad.

“Viktor getting us into the room means that we got the laptop information, but now I don’t need to do the Hotel Hack.”

“The what?”

“At DEFCON Major Malfunction presented a hack using a Linux box to break into hotel information systems through the TV set in a room. You can grab reservation information, TV movies they’ve watched, and sometimes even credit card information or read their emails.”

(□Pg. #)

Copyright 2009 Elsevier

“Who is Major Malfunction?”

“What? You don’t know? He’s the guy who wrote the hack!”

“Never heard of him,” Vlad responded.

“You should really keep up with what the über-leet guys are-”

Pavel saw a subtle firmness appear in Vlad’s expression and he stopped himself.

“That’s right, you were busy recruiting virus writers for one of your jobs. You missed out on some of the really skilled hackers.” Pavel was pushing his luck with the way he talked to

Vlad. But he knew he was right. If Vlad kept bringing in work like this, Pavel knew he needed to practice a variety of skills.

Vlad seemed to have had enough of the conversation. He removed a Swiss Army knife from his pocket. He opened a small connector from the knife, which fit neatly into the USB port on Stepan's laptop. Soon he was copying the "My Documents" folder from Stepan's laptop to his "pocket knife." (□Pg. #)

"Only 10 megabytes. He must have another computer at his office or he keeps everything in email," Pavel said as he looked over Vlad's shoulder.

A quick look from Vlad reminded Pavel that he was already getting on his employer's nerves. Pavel shut up and walked across the room and picked up the remote to the TV set.

ROUGH DRAFT

Vlad ignored Pavel and kept his attention on the laptop. He looked in the default folder and quickly found the file he wanted. He copied the "outlook.pst" file to the pocketknife. This would give him a copy of all the emails Stepan had stored locally. With the email secured, he looked up at Pavel. (□Pg. #)

"What are you doing?"

Pavel was looking at what appeared to be Stepan's room bill displayed on the TV.

"This guy hasn't had any time to pick out a movie and didn't use the Internet email system offered by the hotel. But, he's got a request for a taxi at 8:00am tomorrow, and he paid for everything with an American Express Card. Here's the number. I can't believe they didn't set this thing up to mask the digits on the display!"

“This could be useful,” Vlad replied with a slight smile. Pavel was a resourceful young man to keep around, Vlad reminded himself, even if he was annoying at times.

“Now that you’re done playing with the television, finish up on this laptop for me,” Vlad ordered.

Pavel took Stepan’s laptop from Vlad and blanked the three Windows event log files. Next he changed the “Last logged in user” registry key so that it would appear that Stepan’s account was the last one used. (□Pg. #)

“Do you want me to reset the Administrator password?” Pavel asked.

“No. You’ve done enough. This one won’t ever know what he lost,” Vlad answered as he walked towards the door.

Pavel powered down the computer, returned it to where he found it and followed his boss.

Vlad and Pavel strolled through the lobby without speaking. Vlad led the way as they walked across the street and into a small café. They took a table near the window where Vlad had a clear view of the hotel entrance in case Stepan returned.

“Set up your laptop. I want to see what we found,” Vlad ordered.

Pavel complied and pulled his own sticker-covered laptop from his backpack and set it on the table between them. He logged in and took the pocketknife Vlad offered and connected it to a USB port.

Vlad took Pavel's laptop and looked over the list of files they had just acquired from Stepan's laptop. He didn't have much time, so he sorted the files by "Last Modified Date" and scanned the list. One file caught his eye immediately. It was called "Odysseus.doc" and was last updated just one day before.

"That would be too obvious," he said mostly to himself as he double-clicked on the file name.

After a quick scan of the first page he said, "I've got what I need Pavel. You can take the rest of the day off. I'll call later if something comes up from the meeting. In the mean time, I'm going to be borrowing your laptop."

Pavel paused. He wasn't one to part with his laptop. He had too many tools there that he had spent months "acquiring." But he also knew that Vlad was not one to be disobeyed.

"Be careful with the laptop. I've been working on a potential new IE vulnerability and all my notes are stored there. Let me give you an account so you can get to the tools you need without messing with all of my short cuts."

Pavel took the laptop back from Vlad and created a new user account. He then did a "change user" command, typed "boss" for the user ID, and pushed the laptop back across the table.

"Your password is 'penguin'. Just call me and I'll come pick it up when you're done." Pavel stood from the table and walked away. At least Vlad was going to have to pay for his meal.

As Pavel left the hotel restaurant, Vlad began typing his password.

“That kid never stops,” he thought to himself as he finished typing the not-too-subtle reminder from Pavel that Vlad didn’t really know how to use Linux even though he insisted on using it as his main operating system. Vlad found the document he had been reviewing and continued reading. It looked like Stepan had been given a research project by his employer. Stepan had filled this document with notes and information pulled from web sites. He had started with a company called Data Mining, Inc. based in Raleigh-Durham, North Carolina. He had some information about a small firm called 3DNF, Inc. that had been acquired by Data Mining within the last six months. Vlad found some links from the United States’ Securities and Exchange Commission web site and the text from a press release about the acquisition (□Pg. #)

Then Stepan had listed some names and email addresses that belonged to the 3dnf.com domain. Vlad could only guess that Stepan had “Googled” the domain name to harvest the addresses. If so, Stepan was a fairly resourceful researcher. (□Pg. #)

One of the names was in a red font instead of black like all of the others. Michael Rosel was someone of interest to Stepan. There were links to what appeared to be blog pages by Michael. There were even links to gambling sites. Then there were some notes by Stepan:

Michael Resol is the best target. He is a network admin that has worked at 3DNF for five years. He has been passed over for promotions and he talks too much about his employer on his blog site. Both his blog and Facebook sits reference his favorite online gambling pages. I think he has some financial problems - see link below.

Michael's tech position, length of time with 3DNF and money problems make him a good candidate for deployment of our application.

"Interesting, but what is the 'application'?" Vlad muttered to himself. He had an idea based on the name of the file he was reading. Vlad looked at his watch. He needed to move along. He would have to fill in the gaps during his meeting with Stepan. And there were other files yet to read from Stepan's laptop.

Vlad shut down the laptop and stood to leave. He was in a good mood because of the progress so far. He left a large tip and paid for his and Pavel's meal. Outside, Vlad walked across Puskin Street and into the central garden at the middle of town. He made his way down the tree-lined walk, to the central fountain. On the far side of the fountain he turned to his right and made his way to Columna Street. A left turn and one more block and he could see the outdoor café.

As Vlad approached, he could see a small man in his thirties sitting alone at one of the four outdoor tables. He had blonde hair cut short, glasses, and sharp facial features. There was something about the way he moved that suggested to Vlad that whatever was around the next corner was sure to surprise this man. As Vlad approached, he saw that he was making a bad show of reading a newspaper.

"Impressive. You don't look like someone who can read Romanian," Vlad said in perfect English. In fact, every word Vlad said sounded as if it had been given individual consideration before it was spoken. He knew his baritone voice was a tool he could wield effectively.

“I can’t,” Stepan admitted nervously. “But I thought I should at least take a look and see if I could learn a little about the city.” Stepan’s Swiss accent was obvious to Vlad at once. He sat down in the empty chair across from Stepan. “Are you Simon?” Stepan asked.

“Yes,” Vlad lied. As sloppy as Stepan had been securing his laptop, Vlad knew he would have exposed too much about his activities. “*That’s why you never use your real name,*” he thought to himself.

“You must be Stepan.”

“My employer tells me you come highly recommended.”

“I finish my jobs efficiently if that is what you mean” Vlad responded.

“Uh, yes.”

Stepan was obviously new at this business.

“What consultation does your firm require?” Vlad asked.

“We need someone who can install a certain program on a computer inside a company located in Houston, Texas, USA.”

“What type of program, and what type of company?” Vlad responded.

“A rootkit to answer your first question, and a database consulting firm to answer your second.” Stepan responded.

“That hardly seems like a task worth the cost of my skills,” Vlad answered.

“We need to be certain that the program is installed on a particular system and we are willing to pay to ensure that it functions as designed. We need this to be done discretely and efficiently,” Stepan answered.

“I can get that done. Is that all?”

“There are a few other steps to help ensure the information we need is accessible. The details are documented for you.”

“Are you aware of my fees?” Vlad asked.

“Yes,” Stepan answered.

Vlad took a pen and small piece of paper from his coat pocket and wrote “Volksbank, 111-8-18-1-13-15-27-1” from memory (□Pg. #). “Have the first half of the payment deposited here. I’ll start as soon as I have confirmed the funds. And by the way, don’t complain if you see any extra charges on your American Express card. I’ll expect you to cover some of my travel costs.”

“Certainly. Do you have the necessary account information?”

Stepan’s confused look was a pleasure to Vlad.

“I took the liberty of acquiring some financial information about you. Just a demonstration of the skills you are retaining,” Vlad told him. “*You’re too inept to be doing this,*” he thought to himself as he met Stepan’s surprised gaze.

“Yes – well – of course, we will cover whatever expenses are required to complete the job.” Stepan took an envelope out of his coat and slid it across the table. “My employer has also provided some background information on the job that you will find useful.”

Vlad opened the sealed envelope. It contained a pen.

“What is the pen for?”

“It’s a data storage device. If you pull the top off, you will see a USB connector for your computer. Inside is an encrypted file that details the instructions for your team, as well as the application we need installed on the target system. To access the files, you’ll need the password – Odysseus.”

Vlad allowed himself a small smile at that last piece of information.

“As I said, I’ll begin when I have confirmed payment.”

Stepan obviously wasn’t sure what to do next. He began to gather up his newspaper and then paused.

“I have to ask – I understand you operate in many countries, so why Moldova? Are you from here?”

Vlad let out an honest laugh.

“No, I’m not from Moldova. But I do have some family ties here. I have found the legal environment of this country to be accommodating to my line of work. Local talent, although sometimes hard to find, is quite affordable. People from here are anxious to find work that gets them out of the country. And for the right skills, I can offer that.”

“Oh, well, that does make sense. I’ll make sure everything is in order.” Stepan stood and walked away.

Vlad ordered a cup of coffee and then turned on Pavel’s computer that he was still carrying. He logged in with the “boss” account Pavel had setup for him and connected the pen. He opened a window to review the files on the pen. Sure enough – two files. One was called “instructions.exe” and “files.exe”. Vlad double-clicked on the file called “instructions.exe” and was greeted with an error message.

“Everyone assumes the whole world runs Windows,” he muttered. Vlad looked through the program list on Pavel’s Linux laptop. Sure enough – VMWare. Vlad launched the program and found that Pavel had several different Windows operating system images available. He clicked on the one Pavel had named “Surfing Win2K” and waited for it to boot. Vlad smiled – Pavel had modified that splash screen to show a penguin instead of the normal “Windows” welcome. It didn’t require a password to open either. Vlad tried again to open the file. This time a window appeared asking for a password. He typed in “Odysseus”. The program built a directory called “Transfer” on the desktop. Vlad opened the directory and inside were the files he expected. Vlad opened the one called “instructions.doc” and began to read.

Thirty minutes later he was walking through town. It looked like he had to start his job a little sooner than expected. The last page of the file included instructions that he was to eliminate anyone who had complete knowledge of his activities – beginning with the individual who had delivered the instructions. At least there would be an extra payment for this service. He pulled out his cell phone and dialed a programmed number.

“Da?” The course voice sounded half-asleep.

Vlad sighed disapprovingly as he answered in Russian “Andrei, I need you to pick someone up tomorrow morning at 8:00am at the Dedemon hotel in a taxi.”

Stepan was feeling pretty good the next morning. He had completed his first real “field assignment” without any problems. He also had finally put in motion an idea he had been working on for months. If Simon succeeded in setting up a reliable back door to the American company, he would be able to show his bosses a new revenue stream. Arbitrage of commodities had been lucrative to his firm for years, but it was old school. Arbitrage of information was how Stepan would become partner.

Stepan knew a former partner of Mark Richardson started his firm. The American had fled his home country after some questionable business dealings and set up an international trading company in Switzerland. Their new practice had been successful because of a willingness to deal with anyone. Stepan’s plan would fit in just fine with such a firm.

Stepan finished packing and went down to the lobby. He walked over to Viktor at the concierge desk.

“Do you have that taxi ready for me?”

“Excuse me sir, what room?”

“330.”

“Oh yes. He is waiting for you just outside. Do you need help with your bags?”

“No.” Stepan was ready to start making progress home. He walked out the door and met his ride.

“Good morning. I need to go to the airport.”

“Yes, sir,” was the response from the cabbie with a thick Russian accent. The cabbie took Stepan’s bags and placed them in the trunk. Stepan got in the back seat and settled in for the brief ride back to the airport.

The day was clear and crisp. There was a slight breeze, but everyone on the street seemed to appreciate the sunshine. Stepan noticed more of the city as they drove than he had on the way in the day before. This time his attitude wasn’t as gray and he was able to enjoy what he saw. He saw mostly old, Russian-made cars on the streets. He noticed the small shops that were starting to open for the day. The park he had walked through the afternoon before was mostly empty. A few people were walking through, probably on their way to work.

The traffic wasn’t bad this morning. The drive down Bucuresti Street went quickly, and soon the city fell away and Stepan could see more of the landscape. Modest homes gradually yielded to countryside. The landscape seemed hard because of the coming winter, but the brightness of the day brought warmth in through the cab window. Suddenly Stepan’s senses sharpened and he leaned forward in his seat.

“Is this the way to the airport?”

“Yes, sir,” was the quick answer.

“This doesn’t look like the way I came yesterday.”

“Yes, sir.”

“Do you speak English?” Stepan asked with growing concern.

“Yes sir.”

That answer didn't convince Stepan. He leaned back in his seat and began to realize his problem. He was alone in a country he didn't know. His bags were in the trunk. He couldn't communicate with his driver. But the driver obviously had a destination planned. He thought about jumping out of the car. But that didn't make sense either. He would be abandoning his bags, and he wouldn't know how to get back to the city or the airport.

The cabbie turned off the road suddenly. They pulled down a gravel road, turned right past some trees and came to a stop beyond a little rise in the ground. Stepan looked around. He couldn't see the road. The cabbie turned off the car and got out. Stepan was too scared to even speak. His heart began to pound in his chest and his hands started shaking.

Andrei opened Stepan's door and caught him hard in the mouth with his fist. Stepan slumped. He wasn't unconscious – at least not quite. The shock of the act had the desired effect. Stepan stumbled as Andrei dragged him from the car and tossed him to the ground outside the car.

Stepan Senn looked up at the clear blue sky of a fall morning. He could hear the crunch of dry grass beneath him as he turned his head slightly. The cool air on his face felt sharp against the hot blood that trickled from the corner of his mouth that was quickly swelling. He tried to sit up, but his body wouldn't obey. There was a sharp sound of metal on metal. The sound was familiar, but his mind wasn't working fast enough to recognize his situation. He craned his neck as he struggled to look above him. He saw legs, a hard face looking down at him, and a gun. The shape of the gun seemed to grow large enough to fill all he could see.

Andrei pulled the trigger and walked back to his car. He would collect his payment from Vlad that afternoon for another completed job. Vlad had been keeping Andrei busy lately.

ROUGH DRAFT
WWW.SYNGRESS.COM
Copyright 2009 Elsevier

THE PROLOGUE D1\$\$ECTED

THE TECHNICAL CHAPTERS

Since we are giving this one away for free we can't tell you what and how the technical side of the book constructed, in fact we will just give you the information and let you figure out which FICTIONAL STORY DISSECTED falls into what technical chapter | Recon | Scanning | Explore | Exploit | Expunge | IT Policy | IT Infrastructure | Software, Hardware, and Wetware | Bleeding Edge Technology | Hacker Culture | Easter Eggs | or | Misc. If you know you might just be on to something...here we go!

FICTIONAL STORY DISSECTED – Password Management.

Page XX

He typed in his overly long password, all the while wishing for some painful end for the skinny technician back at the office that insisted everyone had to memorize such nonsense just to gain access to their laptops.

Stepan pulled out his access token and typed in the six-digit random number from the token and the four-digit PIN he had memorized. Soon he had established an encrypted connection to the office back in Zurich, Switzerland.

Password management is a critical part of IT policy. Without a strong password management solution, an organization will surely be caught surprised when a simple lucky guess of an employee's computer account password opens the door to the most confidential and proprietary information.

Stepan needs to understand that the skinny network technician is his company's saving grace because the last thing his company needs is someone to guess his password and get into his

laptop. The overly long password helps to deter hackers from brute forcing their way in. Sometimes hackers will take a long list of common words found in the English dictionary and run that against the login prompt until there is a match. Many password brute force programs will incorporate not only English dictionary words but also other languages too. Depending on information the hacker collected in the recon stage, he/she might realize if you are a US based company all they need is an English dictionary but if you are a worldwide American company with offices in Japan they might also consider including a Japanese dictionary listing.

Stepan also uses an access token that has a randomly generated number on it to access his company's network. Stepan has just used two factor authentication to access his office back in Zurich. This is very important to understand because to defeat this two factor authentication, a hacker must be able to obtain the token itself and then record the random number that is generated or they must be able to guess what the random number generated will be. Not only does the hacker need the random number from the token but they need the four digit pin that coincides with the randomly generated number. This is called a two factor authentication because Stepan must have the token and know the four digit pin. If he also had to swipe his finger on the laptop to gain access to his office's network that would be a third factor, and the use of biometrics to physically recognize Stepan. This is something he is. All three together are considered a three factor authentication method. This is the hardest to break into for hackers.

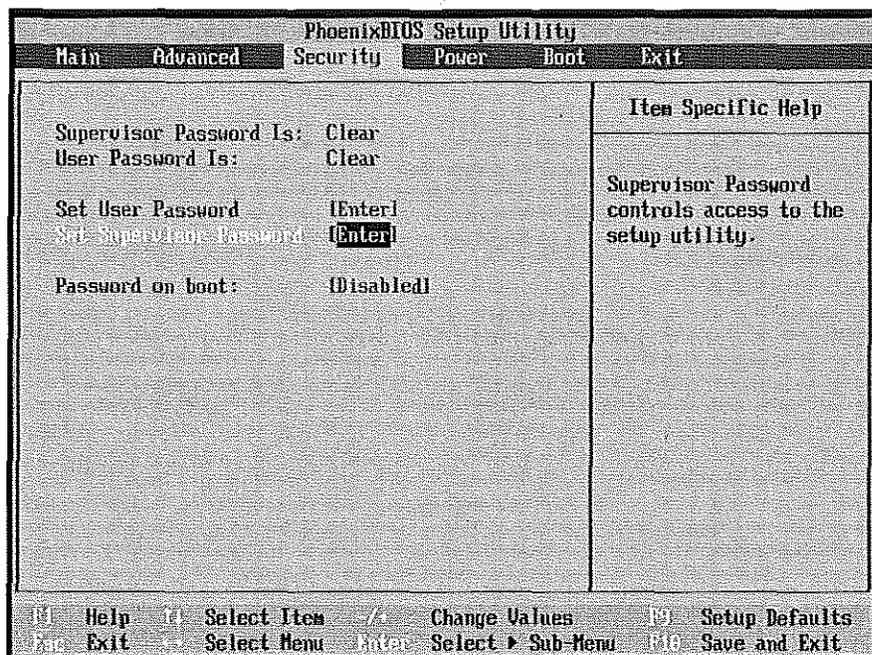
FICTIONAL STORY DISSECTED - BIOS Password

Page XX

He turned on the power and hit the default key combination to modify the boot settings. No power-on password. Pavel could always count on business-types to not think of the basics. They always thought spying was only targeted at governments.

Pavel is using one of the oldest tricks in hacking. He is accessing the computer's Basic Input Out System (BIOS). The BIOS is software that controls all of the hardware components of a computer. The BIOS also allows the user or administrator to set a password to protect the computer from being turned on. Once this power-on password is applied the user must enter it every time the computer is turned on. If the user does not supply the computer with the correct power-on password they cannot access BIOS, the operating system or even the logon screen for their account. As Figure P.1 shows there is a spot for a supervisor and user to apply a BIOS password that will protect the computer from being turned on without proper authorization. Pavel makes a remark about business-types not thinking of the basics, well I wouldn't blame them in particular, I would point the finger at their IT people responsible for the company's password policy.

Figure P.1 – BIOS Password.



Stepan pulled out his access token and typed in the six-digit random number from the token and the four-digit PIN he had memorized. Soon he had established an encrypted connection to the office back in Zurich, Switzerland.

In this situation Stepan is accessing his work's computer network remotely from his hotel room by setting up a virtual private network (VPN) between his computer and his office. A VPN is a computer network in which some of the links between nodes are carried by open connections or virtual circuits in some larger networks (such as the Internet), as opposed to running across a single private network. Stepan is using a secure VPN to gain access to his email server in his office. Secure VPNs use cryptographic tunneling protocols to provide the intended confidentiality (blocking snooping and thus Packet sniffing), sender authentication (blocking identity spoofing), and message integrity (blocking message alteration) to achieve privacy. When properly chosen, implemented, and operated, such techniques can provide secure communications over unsecured networks.

Mobile VPNs are VPNs for mobile and wireless users. They apply standards-based authentication and encryption technologies to secure communications with mobile devices and to protect networks from unauthorized users. Designed for wireless environments, Mobile VPNs provide an access solution for mobile users who require secure access to information and applications over a variety of wired and wireless networks. Mobile VPNs allow users to roam seamlessly across IP-based networks and in and out of wireless-coverage areas without losing application sessions or dropping the secure VPN session. For instance, highway patrol officers require access to mission-critical applications as they travel between different subnets of a

mobile network, much as a cellular radio has to hand off its link to repeaters at different cell towers.

Before Stepan establishes his VPN he uses an access token to obtain a one-time password to begin the authentication process for set up of a VPN. Figure 7.2 shows a picture of the token Stepan might have used to attain this one-time password. Other types of access tokens can look like Figure 7.1 and Figure 7.3. The purpose of a one-time password (OTP) is to make it more difficult to gain unauthorized access to restricted resources, like a computer account. Traditionally static passwords can more easily be accessed by an unauthorized intruder given enough attempts and time. By constantly altering the password, as is done with a one-time password, this risk can be greatly reduced. There are basically five types of one-time passwords:

1. Using a mathematical algorithm to generate a new password based on the previous password.
2. Based on time-synchronization between the authentication server and the client providing the password.
3. Using a mathematical algorithm, but the new password is based on a challenge (e.g., a random number chosen by the authentication server or transaction details) and a counter instead of being based on the previous password.
4. Using a list of passwords printed on paper.

5. Using portable electronic devices (e.g., mobile phones) as an out-of-band method for transmitting one-time passwords.

Stepan uses the time-synchronized one-time password token method. There are many different kinds of tokens, some open up doors and others are used to simply generate random numbers. For instance, figure P.2 and figure P.3 are both tokens. But figure P.2 is a token for accessing a door and figure P.3 is a token used to access information from a network by using the randomly generated numbers displayed in the screen. Figure P.3 is the type of token Stepan used to access his corporate network. Inside this token is an accurate clock that has been synchronized with the clock on the authentication server. On these OTP systems, time is an important part of the password algorithm since the generation of new passwords is based on the current time rather than the previous password or a secret key. Mobile phones and PDAs can also be used to generate a time-synchronized one-time password. This approach could be a more cost effective alternative since most Internet users already have mobile phones. Additionally, this approach could be more convenient since the user would not need to carry around a separate hardware token for each security domain to which he or she requires access.

Figure P.2 – Access token for door.



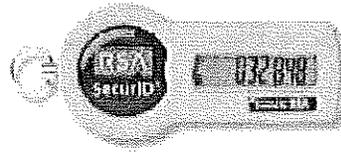
Figure P.3 – RSA One-time-password token. (Time-synchronized)



Figure P.4 – Other types of One-time Password tokens. (Time-synchronized)



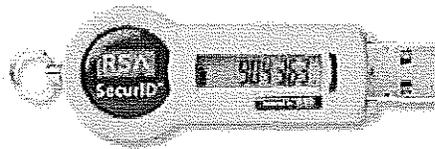
RSA SecurID SD600



RSA SecurID SID700



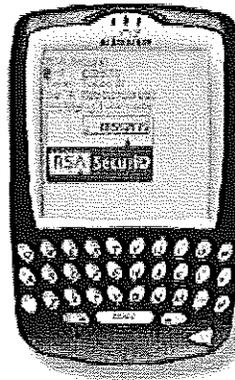
RSA SecurID SD200



RSA SecurID SID800



RSA SecurID SD520



BlackBerry with
RSA SecurID software token

FICTIONAL STORY DISSECTED – Clear event logs.

Page XX

Pavel took Stepan's laptop from Vlad and blanked the three Windows event log files. Next he changed the "Last logged in user" registry key so that it would appear that Stepan's account was the last one used.

Expunging the three Windows event log files and changing the "last logged in user" is critical to covering your tracks for a hacker. Pavel is a very skilled computer hacker and does not mind covering his tracks even though many normal computer users would not even notice things

such as Windows event logs or who the last user logged in was. In fact you have to drill down a few Windows' menus before you can bring up the Windows Event Viewer and skim over the Application, Security, and System logs. But Pavel feels that he better be safe than sorry, because hacking is easily traced if you do not cover your tracks. Little things like this need to be tightened up when malicious hackers do not want anyone to trace their activities.

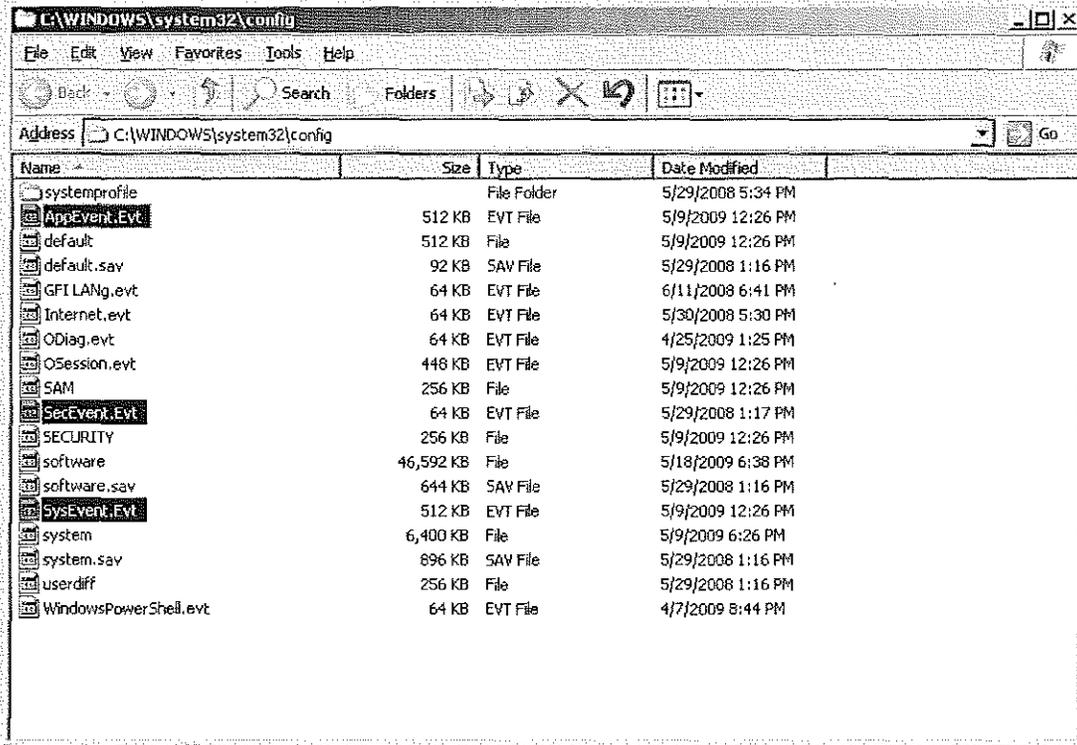
So who can you prevent people like Pavel from expunging your logs? Well in the "STOP HACKING ME PLEASE!" section we will discuss how to secure log files so that only authorized users with proper permissions can access critical log files.

STOP HACKING ME PLEASE! – Securing your logs.

Everyone wants to keep their system's logs from being tampered with, right? Windows has some powerful logging features. Unfortunately, if you're still running an older Windows system, such as a variety of Windows 2000, by default the event logs are not protected against unauthorized access or modification. You might not realize that even though you have to view the logs through the Event Viewer, they are simply regular files just like any others. To secure them, all you need to do is locate them and apply the proper Access Control Lists (ACL).

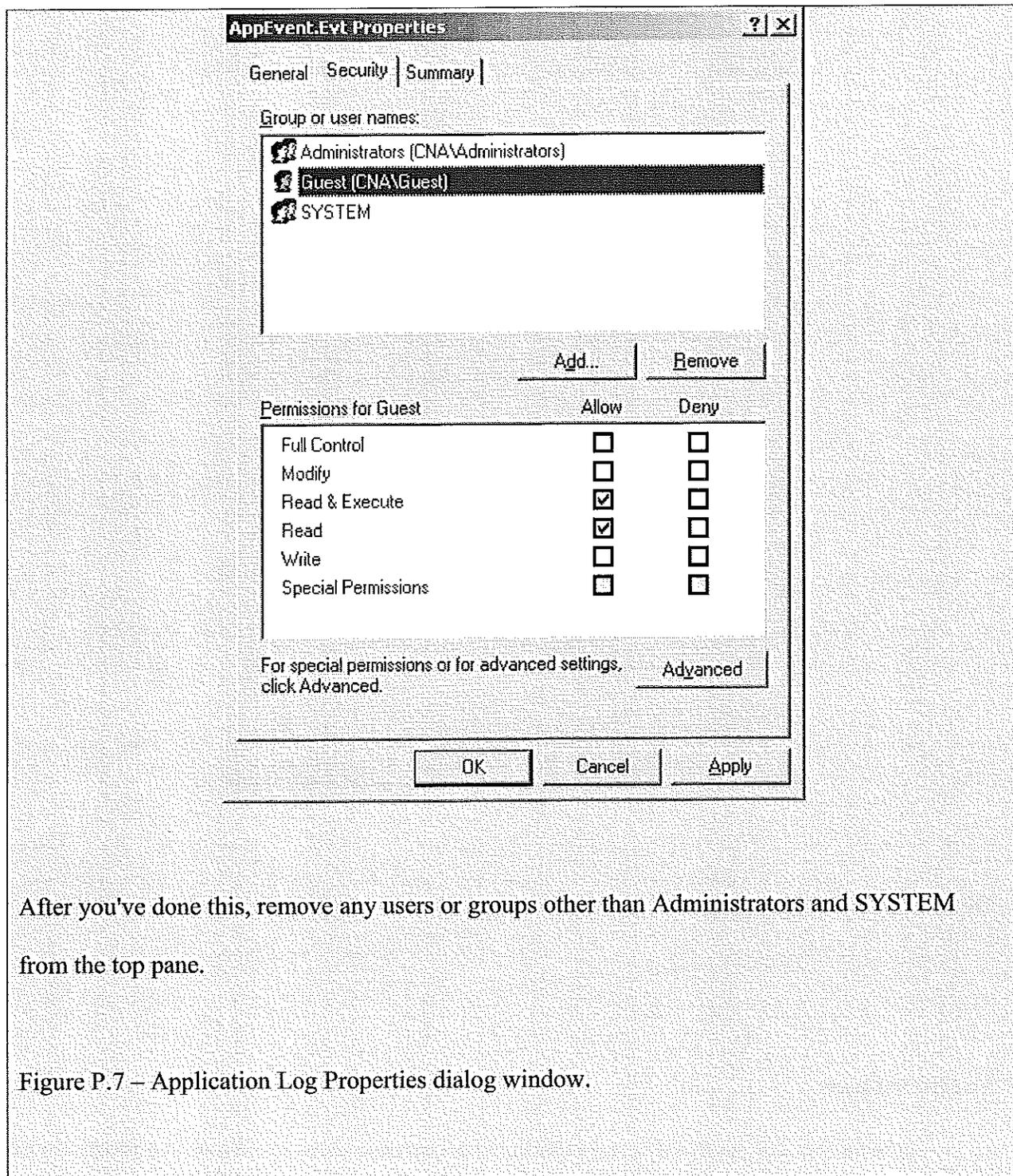
Unless their locations have been changed through the Registry, you should be able to find the logs in the %SystemRoot%\system32\config directory, see figure P.5. The three files that correspond to the Application Log, Security Log, and System Log are AppEvent.Evt, SecEvent.Evt, and SysEvent.Evt, respectively.

Figure P.5 - %SystemRoot%\system32\config directory.



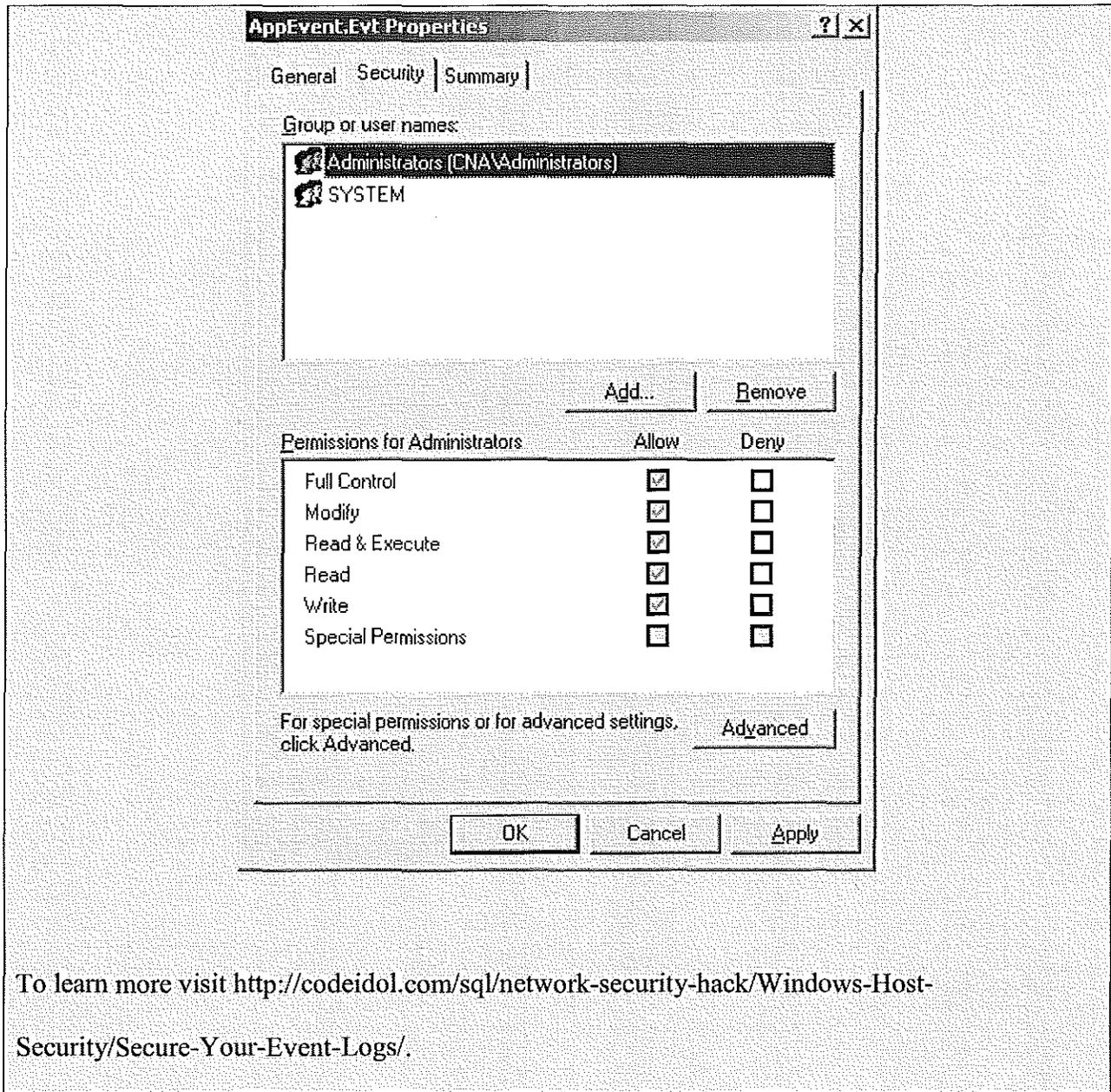
Now, apply ACLs to limit access to only Administrator accounts. You can do this by bringing up the Properties dialog for the files and clicking the Security tab. An example is shown in figure P.6 with unauthorized user permissions for the guest account. In figure P.7 the account for guest has been removed.

Figure P.6 – Application log Properties dialog window.



After you've done this, remove any users or groups other than Administrators and SYSTEM from the top pane.

Figure P.7 – Application Log Properties dialog window.



To learn more visit <http://codeidol.com/sql/network-security-hack/Windows-Host-Security/Secure-Your-Event-Logs/>.

Event Viewer

In Windows XP, an event is any significant occurrence in the system or in a program that requires users to be notified, or an entry added to a log. The Event Log Service records application, security, and system events in Event Viewer. With the event logs in Event Viewer, you can obtain information about your hardware, software, and system components, and monitor

security events on a local or remote computer. Event logs can help you identify and diagnose the source of current system problems, or help you predict potential system problems.

HOW TO - Event log types.

A Windows XP-based computer records events in the following three logs:

Application log: The application log contains events logged by programs. For example, a database program may record a file error in the application log. Events that are written to the application log are determined by the developers of the software program.

Security log: The security log records events such as valid and invalid logon attempts, as well as events related to resource use, such as the creating, opening, or deleting of files. For example, when logon auditing is enabled, an event is recorded in the security log each time a user attempts to log on to the computer. You must be logged on as Administrator or as a member of the Administrators group in order to turn on, use, and specify which events are recorded in the security log.

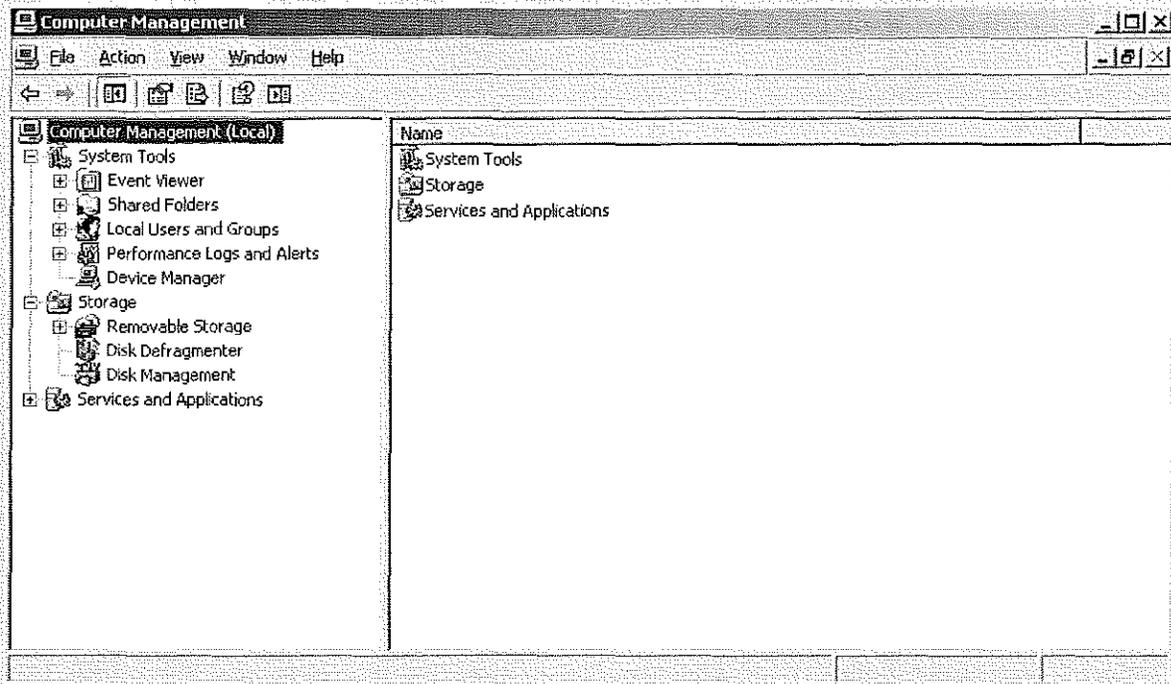
System log: The system log contains events logged by Windows XP system components. For example, if a driver fails to load during startup, an event is recorded in the system log. Windows XP predetermines the events that are logged by system components. To read more visit <http://support.microsoft.com/kb/308427>.

To open Event Viewer, follow these steps:

1. Click **Start**, and then click **Control Panel**. Click **Performance and Maintenance**, then

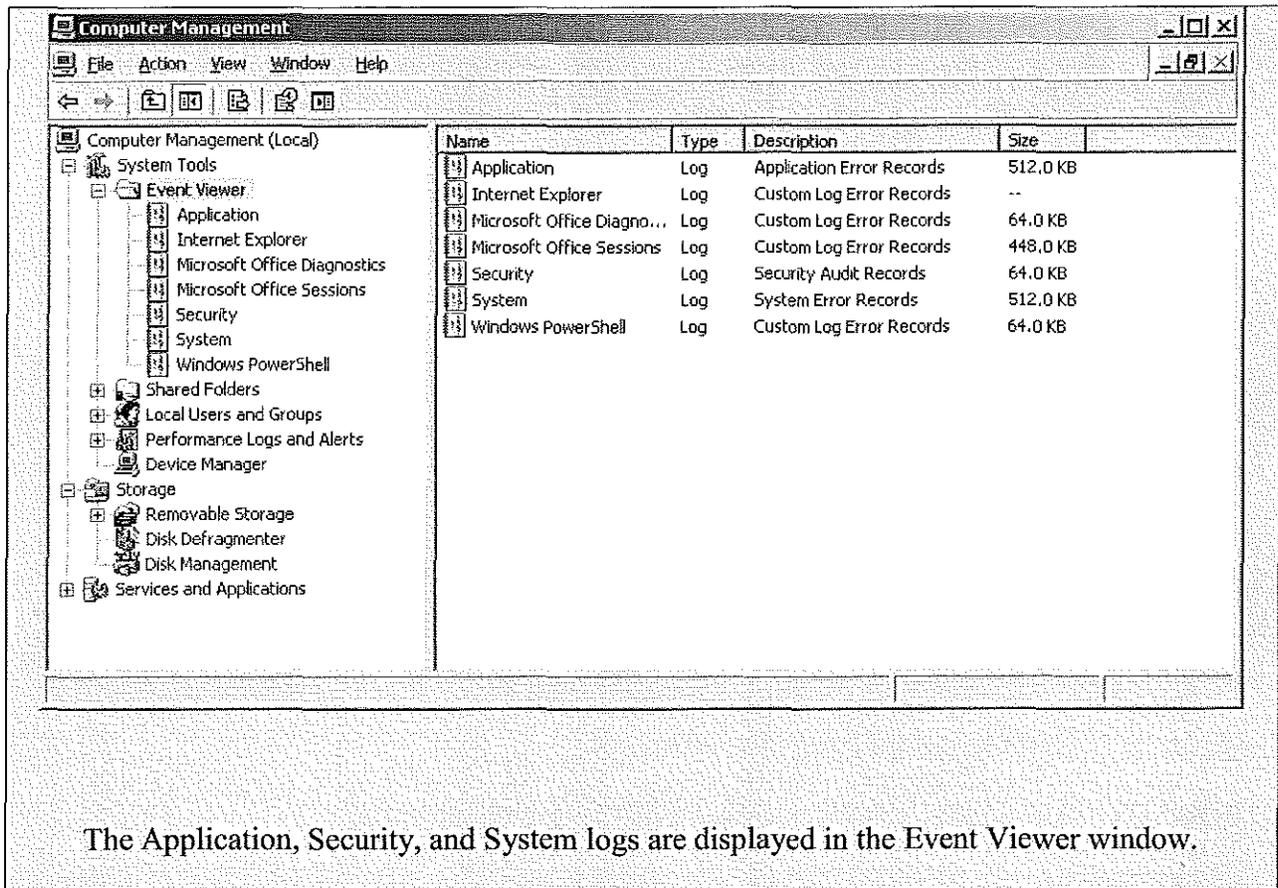
click **Administrative Tools**, and then double-click **Computer Management** as seen in figure P.8. Or, open the MMC containing the Event Viewer snap-in.

Figure P.8 – Computer Management.



2. In the console tree, click **Event Viewer** as seen in figure P.9.

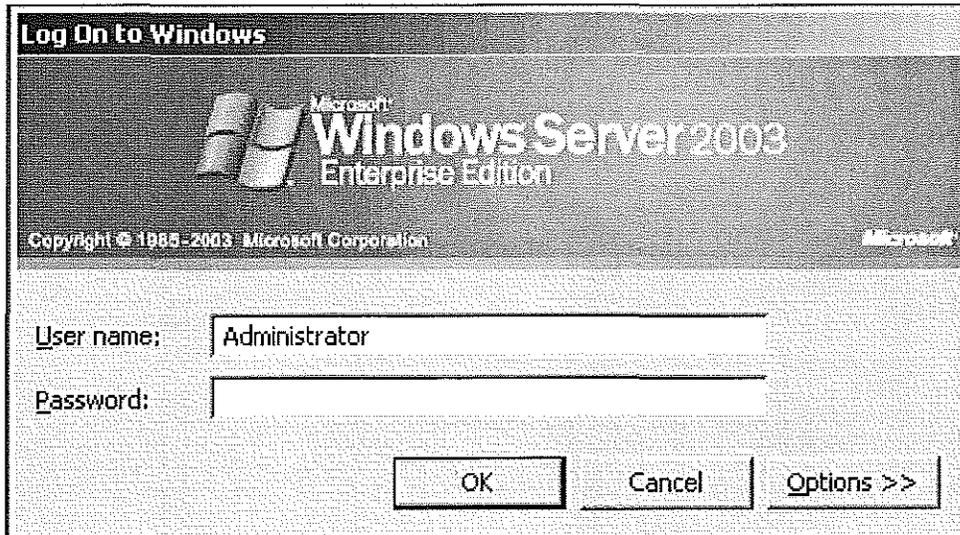
Figure P.9 – Event Viewer selected inside of Computer Management.



Copyright 2009 Elsevier

Pavel changes the last user logged in on Stepan's laptop so when the computer boots up again the dialog box does not display a username other than Stepan's username he used to log into this computer last. Pavel is smart because if he had not changed the last user logged in from appearing in the logon prompt window Stepan would have definitely noticed it because Stepan would have to retype his username to login. In figure P.10 the username "Administrator" was the last user to login the computer.

Figure P.10 – Logon prompt



In order to stop windows from showing up the username of the last user logged in successfully you would need to apply a minor registry hack which would prevent windows from displaying the last username logged in windows.

HOW TO - Stop Windows from showing the last username logged in.

1. Open Start Menu, click Run, type regedit and press Enter as seen in figure P.11. Then Registry Editor program will appear as seen in figure P.12.

Figure P.11 – Run window.

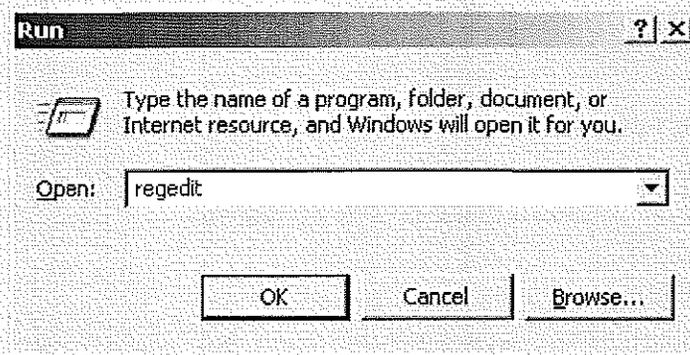
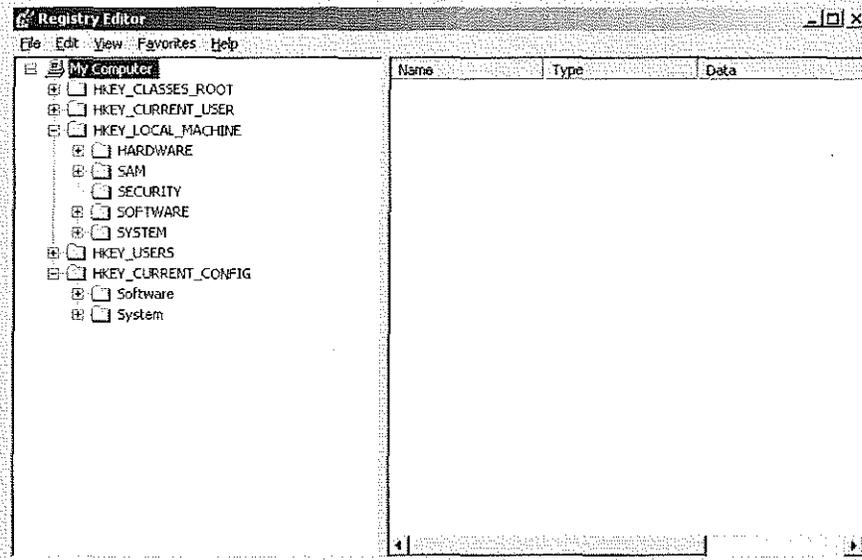


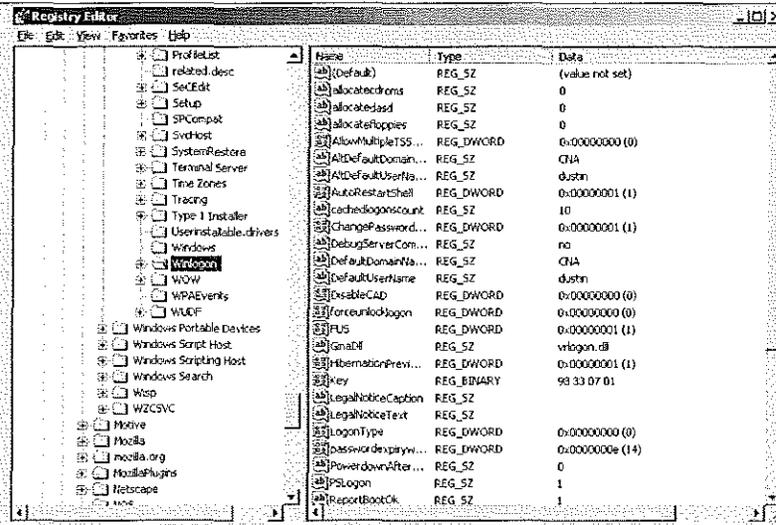
Figure P.12 – Registry Editor.



2. Navigate to the following path as seen in figure. P.13.

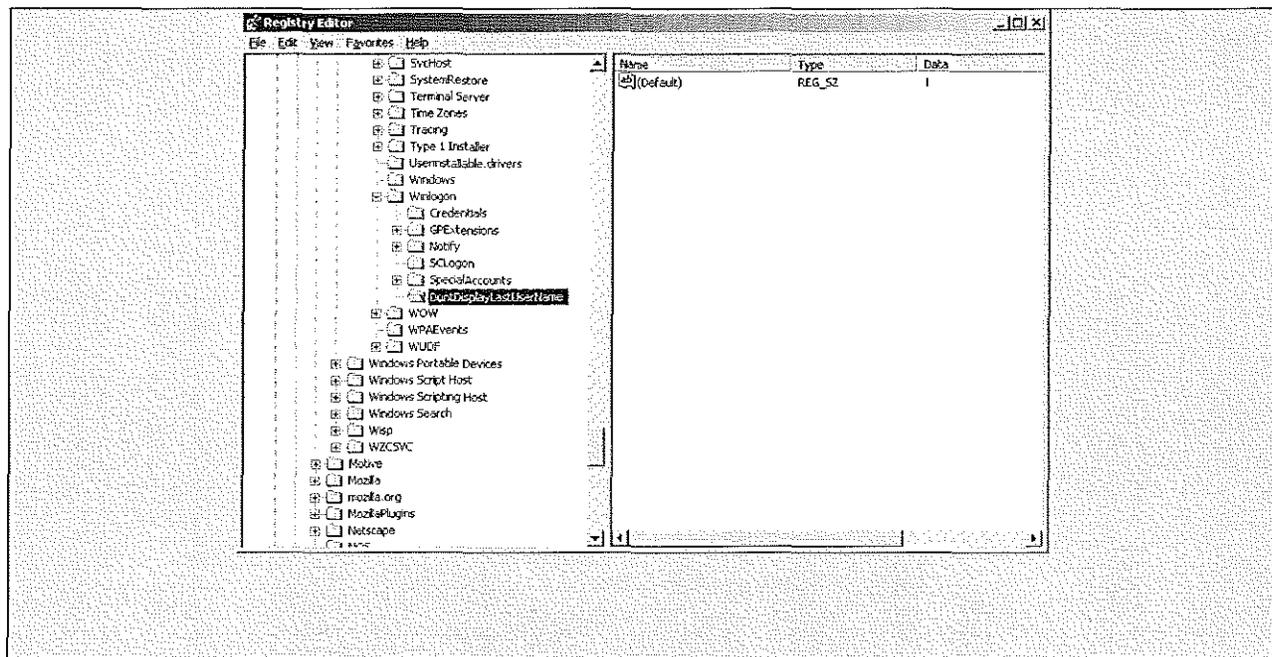
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon

Figure P.13 – Registry Editor navigation.



3. Right click in the empty area in the right pane and create a new registry key of type REG_SZ with value named DontDisplayLastUserName and set the value to 1 to enable the key as seen in figure P.14, on the other hand value 0 will disable this key and windows will display the username of the last user logged in windows.

Figure P.14 – Registry Editor new registry key called DontDisplayLastUserName.



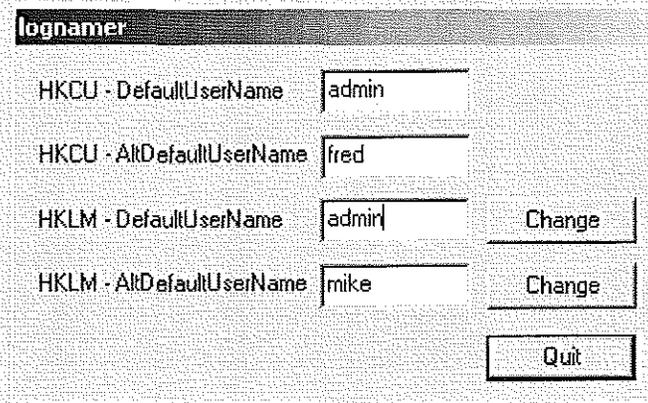
There are a few freeware and shareware tools that can be used to change and record user logins. There is also a great tool used to expunge Internet Explorer logs. Some that we will discuss below are Lognamer, IEClean, Last True Login, lastLogoff.vbs, and Winzapper. The first two tools (Lognamer and IEClean) are used to manipulate and/or expunge the trace of malicious activity by someone who does not want to be caught missing around with a computers file system.

HOW TO - Manipulate last user logged on using Lognamer tool.

Lognamer is a small tool which lets you change the username of the last user logged in, this way you can enter any other valid username on the computer to hide your own username from appearing the login dialog box. See figure P.15 for a screen shot of this tool. This tool is a dialog-tool for XP and allows you to set the winlogon default user names, so they show instead of the name you used for your current logon. Neat if you do not want people to know who logged

on the last time!

Figure P.15 – Lognamer tool.



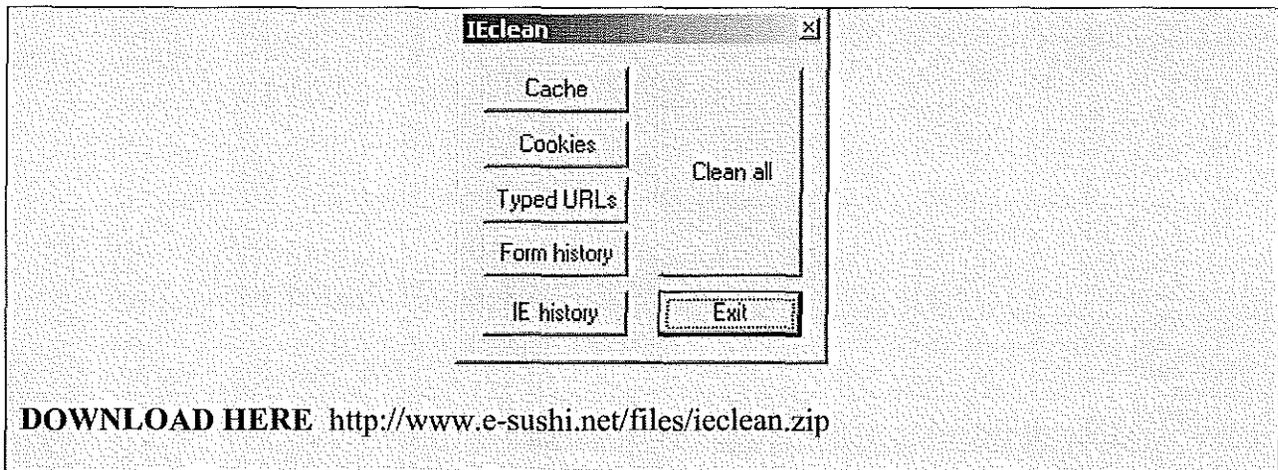
DOWNLOAD HERE <http://www.e-sushi.net/files/lognamer.zip>

Copyright 2009 Elsevier

HOW TO – Cleaning out the Internet Explorer cache, cookies, and history using IEClean tool.

IEClean is a simple, yet effective cleaning utility by e-sushi. A screen shot of this tool is in figure P.16. It is the fastest way to clean up after yourself when you have used Internet Explorer on a computer, but do not want people to know where you surfed to. Or you can use this software to quickly reclaim some disk space. Whatever your reasons for using it may be: it cleans what it says, whipping the data found from your hard disk by overwriting the disk-sectors with 0-bytes, making undeletion near to impossible.

Figure P.16 – IEClean tool.



STOP HACKING ME PLEASE! – Last True Login tool.

What if you could find the true last logon time for every user and computer account. That would be great! No more malicious activity will get in my way...well you can clean up your Active Directory by easily identifying unused or obsolete user and computer accounts by identifying their true last logon time and account status. The true last logon time can be a problem for system administrators as different times are stored on each domain controller. The True Last Logon tool queries all Active Directory Domain Controllers to gain the true last logon time. The easy to use interface also shows the account expiry date and time, whether or not the account is locked out and whether or not the account is currently enabled or disabled. Old or redundant accounts can be disabled or deleted from within the program, or you can choose to print or save the results to a CSV or tab delimited text file. In figure P.17 the option to use True Lat Logon via the command line is shown. Figure P.18 is the front end graphical user interface (GUI).

Figure P.17 – Last True Login Command Line Options.

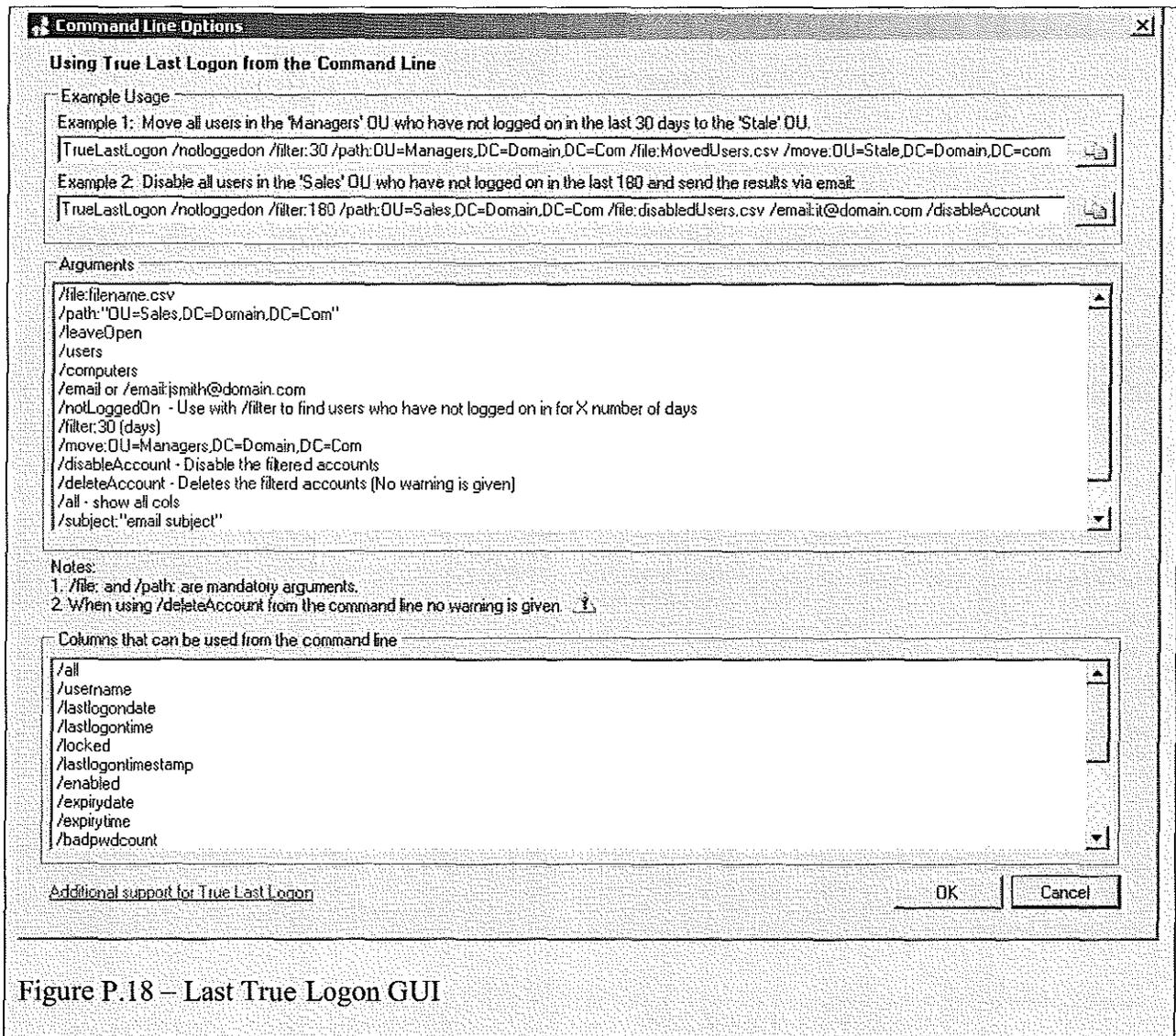


Figure P.18 – Last True Logon GUI

True Last Logon 2.8

File Action Help

Query: Users Computers Both

OU: DC=domain,DC=com Browse

Domain: DC=domain,DC=com Query all DCs

Results Filter

Show accounts: 30 days

Note: Columns can be sorted by clicking the column header. Columns can also be placed in a different order by dragging and dropping.

| Name | Username | Last Logon Date | Last Logon Time | Last Logon Timestamp | Enabled | Locked | Pwd Never Expires | Expiry Date | |
|-------------------------------------|--------------------|-----------------|-----------------|----------------------|------------------|--------|-------------------|-------------|------------|
| <input type="checkbox"/> | Abdul Mutalib | AbdulM | 15/01/2007 | 14:24 | 21/05/2007 09:11 | True | False | False | No Data |
| <input type="checkbox"/> | Adam Kehoe | AdamK | 09/01/2007 | 14:13 | 18/05/2007 10:29 | True | False | False | No Data |
| <input type="checkbox"/> | Adams Thomas | Adams | 15/01/2007 | 14:25 | 21/05/2007 09:28 | True | False | False | No Data |
| <input type="checkbox"/> | Alger Horatio | Alger | 15/01/2007 | 13:15 | 18/05/2007 09:39 | True | False | False | No Data |
| <input checked="" type="checkbox"/> | Ammons Virgie | Ammons | 12/01/2007 | 13:25 | 18/05/2007 11:57 | True | False | False | No Data |
| <input checked="" type="checkbox"/> | Angelou Maya | Angelou | 15/01/2007 | 14:55 | 18/05/2007 15:35 | True | False | False | No Data |
| <input checked="" type="checkbox"/> | Asimov Issac | Asimov | 15/01/2007 | 15:46 | 14/05/2007 08:33 | False | False | False | No Data |
| <input checked="" type="checkbox"/> | Aspdin Joseph | Aspdin | 07/01/2007 | 23:38 | 17/05/2007 16:28 | True | False | False | No Data |
| <input type="checkbox"/> | Asselbergs Edward | Asselbergs | 12/01/2007 | 10:02 | 18/05/2007 09:40 | True | False | False | No Data |
| <input type="checkbox"/> | Baekeland Leo | Baekelanc | 15/01/2007 | 11:48 | 14/05/2007 09:49 | True | False | False | No Data |
| <input type="checkbox"/> | Baer Ralph | BaerR | 12/01/2007 | 13:05 | 13/05/2007 20:01 | True | False | False | No Data |
| <input type="checkbox"/> | Beacher Harriet | Beacher | 13/01/2007 | 17:33 | 17/05/2007 07:32 | True | False | True | No Data |
| <input type="checkbox"/> | Bellow Saul | Bellow | 15/01/2007 | 13:58 | 16/05/2007 09:14 | True | False | False | No Data |
| <input type="checkbox"/> | Berliner Emile | Berliner | 15/01/2007 | 10:50 | 18/05/2007 11:57 | True | False | False | No Data |
| <input type="checkbox"/> | Berners-Lee Tim | BernersL | 15/01/2007 | 15:03 | 18/05/2007 10:08 | True | False | False | No Data |
| <input type="checkbox"/> | Blodgett Katherine | BlodgettK | 12/01/2007 | 15:21 | 18/05/2007 08:43 | False | False | False | No Data |
| <input type="checkbox"/> | Bronte Charlotte | BronteC | 15/01/2007 | 14:40 | 18/05/2007 10:49 | True | False | False | No Data |
| <input type="checkbox"/> | Canfield Dorothy | Canfield | 15/01/2007 | 14:29 | 18/05/2007 12:28 | True | False | False | 21/05/2007 |
| <input type="checkbox"/> | Capote Truman | Capote | 15/01/2007 | 14:44 | 14/05/2007 09:42 | True | False | False | No Data |

Done. Displaying 16 objects

DOWNLOAD HERE <http://www.dovestones.com/Downloads/Demos/TrueLastLogonTrial.msi>

STOP HACKING ME PLEASE! – Recording users last logoff time.

Active Directory contains an attribute named lastLogoff alongside the lastLogon attribute. However unlike lastLogon the lastLogoff attribute is not written too and doesn't appear to be used by Active Directory running on Windows 2000 or Windows Server 2003 Server. Microsoft has plans to use this attribute at a future date in the mean time we can use the solution described below.

Recording users last logoff time

One solution is to store a user's last log off time in another attribute which you can easily read using Active Directory Users and Computers and True Last Logon. When a user logs off a domain connected computer we can store the date and time in an unused Active Directory attribute. We can do this by running a script when the user logs off. When the script runs it uses the credentials of the user that is logged on (well logging off), by default a user has permission to update certain attributes within their Active Directory user object, some of these attributes are listed below. Active Directory does have an attribute named 'lastLogoff' unfortunately this attribute is read-only so we cannot use this so we need to store the last logoff date and time in an attribute we can use.

How it works

1. Use the lastLogoff.vbs script to populate a chosen attribute with the date and time the user logged off.
2. Edit the script so that date is being stored in an attribute you aren't currently using (see list below).
3. Assign the script to run at logoff using Group Policy.
4. Add the attribute to True Last Logon by clicking on the 'Add/Remove Columns' button.
5. When True Last Logon queries user accounts the last logoff date and time will be retrieved.

The last logoff date can be stored in one of the following attributes.

General Tab

telephoneNumber

wWWHomePage

url

Address Tab

streetAddress

postOfficeBox

l (City)

st (State)

postalCode

Telephone Tab

info (Notes, found on the Address tab)

homePhone

otherHomePhone

pager

otherPager

mobile

otherMobile

facsimileTelephoneNumber

otherFacsimileTelephoneNumber

ipPhone

otherIpPhone

DOWNLOAD HERE <http://www.dovestones.com/active-directory/true-last-logon/last-logoff.html#script>

'<Script Starts>

'Saves users logoff date and time

'Use Group Policy to run the script when users logs off.

```
ON ERROR RESUME NEXT
```

```
Set objSysInfo = CreateObject("ADSystemInfo")
```

```
strUser = objSysInfo.UserName
```

```
Set objUser = GetObject("LDAP://" & strUser)
```

```
strlogoffTime = Cstr(Now)
```

```
'The logoff time needs to be stored in an unused attribute
```

```
'Select one attribute from the list below and uncomment that line.
```

```
'objUser.info = strlogoffTime
```

```
'objUser.telephoneNumber = strlogoffTime
```

```
'objUser.url = strlogoffTime
```

```
'objUser.wwwHomePage = strlogoffTime
```

```
'objUser.streetAddress = strlogoffTime
```

```
'objUser.postOfficeBox = strlogoffTime
```

```
'objUser.l = strlogoffTime
```

```
'objUser.st = strlogoffTime
```

```
'objUser.postalCode = strlogoffTime
```

```
'objUser.homePhone = strlogoffTime
```

```
'objUser.otherHomePhone = strlogoffTime
```

```
'objUser.pager = strlogoffTime
```

```
'objUser.otherPager = strlogoffTime
```

```
'objUser.mobile = strlogoffTime
```

```
'objUser.otherMobile = strlogoffTime
```

```
'objUser.facsimileTelephoneNumber = strlogoffTime
```

```
'objUser.otherFacsimileTelephoneNumber = strlogoffTime  
'objUser.ipPhone = strlogoffTime  
'objUser.otherIpPhone = strlogoffTime  
objUser.SetInfo  
'<Script Ends>
```

PUBLIC RECORD ON TAP – Windows Security Log

The Security Log

In Microsoft Windows, there is a log that contains records of login/logout activity and/or other security-related events specified by the system's audit policy. Auditing allows administrators to configure Windows to record operating system activity in the Security Log.

The Security Log is one of three logs viewable under Event Viewer. Local Security Authority Subsystem Service writes events to the log. The Security Log is one of the primary tools used by Administrators to detect and investigate attempted and successful unauthorized activity and to troubleshoot problems; Microsoft describes it as “Your Best and Last Defense.”¹ The log and the audit policies that govern it are also favorite targets of hackers and rogue system administrators seeking to cover their tracks before and after committing unauthorized activity.²

Types of data logged

¹ *The NT Security Log - Your Best and Last Defense*, R. Franklin Smith
<http://www.microsoft.com/technet/archive/winntas/maintain/security/ntsecuri.mspx?mfr=true>

² *Protecting the NT Security Log*, Randy Franklin Smith, Windows IT Pro, July 2000.
<http://www.windowsitpro.com/Windows/Article/ArticleID/8785/8785.html>

If the audit policy is set to record logins, a successful login results in the user's user name and computer name being logged as well as the user name they are logging into.³ Depending on the version of Windows and the method of login, the IP address may or may not be recorded.

Windows 2000 Web Server, for instance, does not log IP addresses for successful logins, but Windows Server 2003 includes this capability.⁴ The categories of events that can be logged are:⁵

- ✓ Account logon events
- ✓ Account management
- ✓ Directory service access
- ✓ Logon events
- ✓ Object access
- ✓ Policy change
- ✓ Privilege use
- ✓ Process tracking
- ✓ System events

³ *Tracking Logon and Logoff Activity in Windows 2000*, Microsoft. <http://technet.microsoft.com/en-us/library/Bb742436.aspx>

⁴ *Capturing IP Addresses for Web Server Logon Events*, Randy Franklin Smith, *Windows IT Pro*, October 2003. <http://www.windowsitpro.com/Windows/Article/ArticleID/40022/40022.html>

⁵ *Auditing Policy*, Microsoft. <http://technet2.microsoft.com/windowsserver/en/library/962f5863-15df-4271-9ae0-4b0412e297491033.msp?mfr=true>

The sheer number of loggable events means that security log analysis can be a time-consuming task.⁶ Third-party utilities have been developed to help identify suspicious trends. It is also possible to filter the log using customized criteria.

Attacks and countermeasures

Administrators are allowed to view and clear the log (there is no way to separate the rights to view and clear the log).⁷ In addition, an Administrator can use Winzapper⁸ (see figure P.19) to delete specific events from the log.

Figure P.19 - Winzapper

ROUGH DRAFT
WWW.SYNGRESS.COM
Copyright 2009 Elsevier

⁶ *Five Mistakes of Security Log Analysis*, Anton Chuvakin, Ph.D., GCIA, GCIH.
http://www.infosecwriters.com/text_resources/pdf/top5-log-analysis-mistakes.pdf

⁷ *Access Denied: Letting Users View Security Logs*, Randy Franklin Smith, July 2004 -- intermittently broken link as of 2007-9-27. <http://www.windowsitpro.com/WindowsSecurity/Article/ArticleID/42811/42811.html>

⁸ Winzapper is a freeware utility and hacking tool used to delete events from the Microsoft Windows NT 4.0 and Windows 2000 Security Log. It was developed by Peter Nordahl as a proof-of-concept tool, demonstrating that once the Administrator account has been compromised, event logs are no longer reliable. According to *Hacking Exposed: Windows Server 2003*, Winzapper works with Windows NT/2000/2003.

| Type | Date and Time | Category | User | More Info |
|---------------|--------------------------|-------------------|---------------------|------------|
| Success Audit | Thu Feb 15 19:18:35 2007 | Object Access | NT AUTHORITY\SYSTEM | SecurityA |
| Success Audit | Thu Feb 15 19:18:35 2007 | Object Access | NT AUTHORITY\SYSTEM | SecurityA |
| Success Audit | Thu Feb 15 19:18:35 2007 | Object Access | NT AUTHORITY\SYSTEM | SecurityA |
| Success Audit | Thu Feb 15 19:18:35 2007 | Object Access | NT AUTHORITY\SYSTEM | SecurityA |
| Success Audit | Thu Feb 15 19:18:35 2007 | Policy Change | NT AUTHORITY\SYSTEM | + + + + - |
| Success Audit | Thu Feb 15 19:18:40 2007 | Object Access | NT AUTHORITY\SYSTEM | SecurityA |
| Success Audit | Thu Feb 15 19:18:40 2007 | Object Access | NT AUTHORITY\SYSTEM | SecurityA |
| Success Audit | Thu Feb 15 19:18:40 2007 | Object Access | NT AUTHORITY\SYSTEM | SecurityA |
| Success Audit | Thu Feb 15 19:18:40 2007 | Policy Change | NT AUTHORITY\SYSTEM | + + + + - |
| Success Audit | Thu Feb 15 19:18:40 2007 | Object Access | NT AUTHORITY\SYSTEM | SecurityA |
| Success Audit | Thu Feb 15 19:19:07 2007 | Detailed Tracking | TEST\Administrator | 856 Admir |
| Success Audit | Thu Feb 15 19:19:09 2007 | Privilege Use | TEST\Administrator | Security - |
| Success Audit | Thu Feb 15 19:19:09 2007 | Detailed Tracking | TEST\Administrator | 796 {WINI |
| Success Audit | Thu Feb 15 19:19:09 2007 | Privilege Use | TEST\Administrator | Security - |
| Success Audit | Thu Feb 15 19:19:11 2007 | Privilege Use | TEST\Administrator | EventLog |
| Success Audit | Thu Feb 15 19:19:15 2007 | Detailed Tracking | TEST\Administrator | 796 Admir |
| Success Audit | Thu Feb 15 19:19:27 2007 | Privilege Use | TEST\Administrator | Security - |
| Success Audit | Thu Feb 15 19:19:50 2007 | Privilege Use | TEST\Administrator | Security - |
| Success Audit | Thu Feb 15 19:19:50 2007 | Detailed Tracking | TEST\Administrator | 332 {Prog |
| Success Audit | Thu Feb 15 19:19:50 2007 | Privilege Use | TEST\Administrator | Security - |
| Success Audit | Thu Feb 15 19:20:23 2007 | Detailed Tracking | NT AUTHORITY\SYSTEM | 784 TEST: |
| Success Audit | Thu Feb 15 19:24:14 2007 | Detailed Tracking | TEST\Administrator | 332 Admir |
| Success Audit | Thu Feb 15 19:24:22 2007 | Privilege Use | TEST\Administrator | Security - |
| Success Audit | Thu Feb 15 19:24:22 2007 | Detailed Tracking | TEST\Administrator | 848 {WINI |

WinZapper 1.0 - (c) 2000, Arne Vidstrom, arne.vidstrom@ntsecurity.nu - <http://ntsecurity.nu/toolbox/winzapper/>

For this reason, once the Administrator account has been compromised, the event history as contained in the Security Log is unreliable.⁹ A defense against this is to set up a remote log server with all services shut off, allowing only console access.¹⁰

As the log approaches its maximum size, it can either overwrite old events or stop logging new events. This makes it susceptible to attacks in which an intruder can flood the log by generating a large number of new events. A partial defense against this is to increase the maximum log size so that a greater number of events will be required to flood the log. It is possible to set the log to not

⁹ Winzapper FAQ, NTSecurity. <http://www.ntsecurity.nu/toolbox/winzapper/>

¹⁰ Know Your Enemy: II, HoneyNet Project. <http://honeynet.org/papers/enemy2/index.html>

overwrite old events, but as Chris Brenton notes, “the only problem is that NT has a really bad habit of crashing when its logs become full.”¹¹

Randy Franklin Smith’s *Ultimate Windows Security* points out that given the ability of administrators to manipulate the Security Log to cover unauthorized activity, separation of duty between operations and security-monitoring IT staff, combined with frequent backups of the log to a server accessible only to the latter, can improve security.¹²

Another way to defeat the Security Log would be for a user to login as Administrator and change the auditing policies to stop logging the unauthorized activity he intends to carry out. The policy change itself could be logged, depending on the “audit policy change” setting, but this event could be deleted from the log using Winzapper; and from that point onward, the activity would not generate a trail in the Security Log.⁵

Microsoft notes, “It is possible to detect attempts to elude a security monitoring solution with such techniques, but it is challenging to do so because many of the same events that can occur during an attempt to cover the tracks of intrusive activity are events that occur regularly on any typical business network.”¹³

As Brenton points out, one way of preventing successful attacks is security through obscurity.

Keeping the IT department's security systems and practices confidential helps prevent users from

¹¹ *Auditing Windows NT*, Chris Brenton. <http://www.arcert.gov.ar/webs/textos/ntaudit.pdf>

¹² *Ultimate Windows Security*, Randy Franklin Smith. <http://www.ultimatewindowssecurity.com/>

¹³ *Security Monitoring and Attack Detection*, Microsoft, Aug. 29, 2006.

<http://www.microsoft.com/technet/security/midsizedbusiness/topics/serversecurity/attackdetection.mspx>

formulating ways to cover their tracks. If users are aware that the log is copied over to the remote log server at :00 of every hour, for instance, they may take measures to defeat that system by attacking at :10 and then deleting the relevant log events before the top of the next hour.¹¹

Of course, log manipulation is not needed for all attacks. Simply being aware of how the Security Log works can be enough to take precautions against detection. For instance, a user wanting to log into a fellow employee's account on a corporate network might wait until after hours to gain unobserved physical access to the computer in their cubicle; surreptitiously use a hardware keylogger¹⁴ to obtain their password; and later login to that user's account through Terminal Services from a Wi-Fi hotspot whose IP address cannot be traced back to the intruder. After the log is cleared through Event Viewer, one log entry is immediately created in the freshly-cleared log noting the time it was cleared and the admin who cleared it. This information can be a starting point in the investigation of the suspicious activity.

In addition to the Windows Security Log, admins can check the Internet Connection Firewall security log for clues.

Writing false events to the log

It is theoretically possible to write false events to the log. Microsoft notes, "To be able to write to

¹⁴ Hardware keyloggers are used for keystroke logging, a method of capturing and recording computer users' keystrokes, including sensitive passwords. They can be implemented via BIOS-level firmware, or alternatively, via a device plugged in line between a computer keyboard and a computer. They log all keyboard activity to their internal memory.

the Security log, SeAuditPrivilege is required. By default, only Local System and Network Service accounts have such privilege.”¹⁵ *Microsoft Windows Internals* states, “Processes that call audit system services . . . must have the SeAuditPrivilege privilege to successfully generate an audit record.”¹⁶ The Winzapper FAQ notes that it is “possible to add your own ‘made up’ event records to the log” but this feature was not added because it was considered “too nasty,” a reference to the fact that someone with Administrator access could use such functionality to shift the blame for unauthorized activity to an innocent party.⁹ Server 2003 added some API calls so that applications could register with the security event logs and write security audit entries. Specifically, the AuthzInstallSecurityEventSource function installs the specified source as a security event source.¹⁷

Admissibility in court

The EventTracker newsletter states that “The possibility of tampering is not enough to cause the logs to be inadmissible; there must be specific evidence of tampering in order for the logs to be considered inadmissible.”¹⁸

FICTIONAL STORY DISSECTED – Infrared hotel attack

Page XX

“At DEFCON Major Malfunction presented a hack using a Linux box to break into hotel information systems through the TV set in a room. You can grab reservation

¹⁵ Auditing Security Events, Microsoft. <http://msdn2.microsoft.com/en-us/library/ms731669.aspx>

¹⁶ *Microsoft Windows Internals*, Microsoft. <http://technet.microsoft.com/en-us/sysinternals/bb963901.aspx>

¹⁷ AuthzInstallSecurityEventSource Function, Microsoft. <http://msdn.microsoft.com/en-us/library/aa376314.aspx>

¹⁸ EventTracker Newsletter, April 2006, Will your log files stand up in court? Authentication vs. logon events? <http://web.archive.org/web/20061030180841/www.eventlogmanager.com/subpass/newsletter/april06.htm>

information, TV movies they've watched, and sometimes even credit card information or read their emails."

Adam Laurie, technical director of The Bunker, a managed network data services firm, is known as Major Malfunction in the hacker community. In 2005 at the Riviera Hotel & Casino in Las Vegas, Nevada, Major Malfunction stood up and walked to the podium at a well known conference called DEFCON. He was about to give a presentation describing how he was able to view hotel guests information using the in-room TV. Using a laptop, an infrared transmitter and a USB TV tuner Major Malfunction was able to pick up information through the hotel TV from the backend databases. These backend databases contained such things as billing for the minibar, remote-minibar locking system, room-cleaning status, and billing systems used to check account balances. ¹⁹ This bleeding edge technique allowed him to view the channels he wanted without the hotel knowing anything. It also gave him the ability to view other hotel guest's private channels where they would normally check their hotel bill from the TV. The whole thing started when he was bored in his Miami hotel one day and decided to see if he could watch some adult movies for free. To read more about Major Malfunction, visit <http://www.defcon.org/html/defcon-13/dc13-speakers.html#major>.

FICTIONAL STORY DISSECTED – USB Knife, Swiss Army knife with USB storage

Page XX

He removed a Swiss Army knife from his pocket. He opened a small connector from the knife, which fit neatly into the USB port on Stepan's laptop. Soon he was copying the "My Documents" folder from Stepan's laptop to his "pocket knife."

¹⁹ A Hacker Games the Hotel by Kim Zetter, Wired.com, <http://www.wired.com/politics/security/news/2005/07/68370>

Vlad has all the cool hacking hardware including what you see in Figure P.20. A Swiss army knife with a USB thumb drive attached is a very convenient item to have on your person at all times for someone like Vlad. Vlad uses this device to conceal its true purpose as an external storage device. Vlad quickly snatches all of Stepan’s personal documents from the “My Computer” folder, the default Windows folder for a user’s documents, pictures, and music.

Figure P.20 – Swiss Army knife with USB storage.



FICTIONAL STORY DISSECTED – USB storage built into a pen

Page XX

“What is the pen for?”

“It’s a data storage device. If you pull the top off, you will see a USB connector for your computer. Inside is an encrypted file that details the instructions for your team, as well as the application we need installed on the target system.”

There are many kinds of common office supplies that are also used as a USB device for external storage. Figure P.21 is a picture of what Stepan might have given to Vlad. Also in figure P.22 is another common item everybody uses, a key. This key is special because it is a USB device. It looks and smells like a key but look closely and you will notice the rectangle shaped body of a USB device.

Figure P.21 – USB pen.

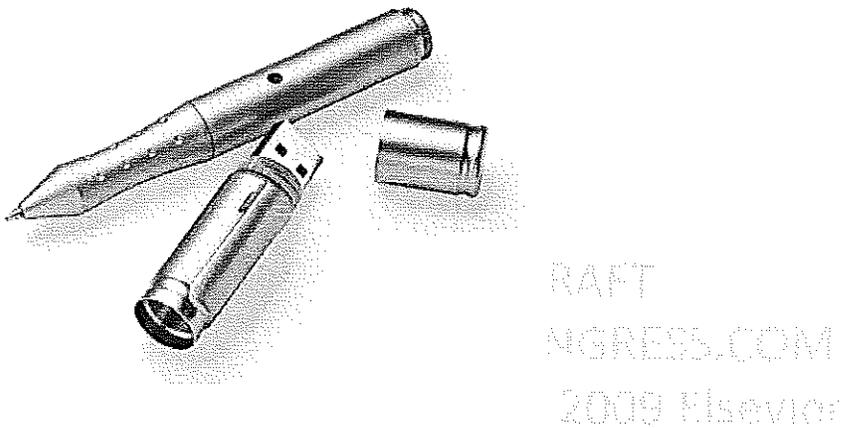
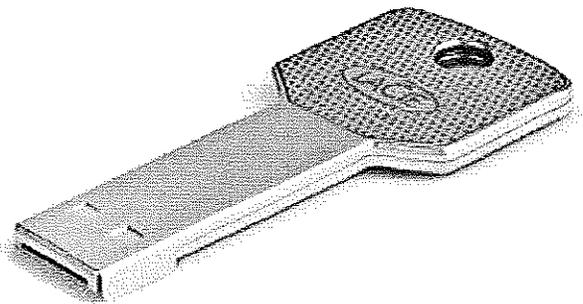


Figure P.22 – USB key.



He looked in the default folder and quickly found the file he wanted. He copied the “outlook.pst” file to the pocketknife. This would give him a copy of all the emails Stepan had stored locally. With the email secured, he looked up at Pavel.

Microsoft Outlook stores all of your email in a single file per email account you have set up. This single file is called a Personal Storage Table (.pst) and is a file used to store local copies of messages, calendar events, and other items within Microsoft software such as Microsoft Exchange Client, Windows Messaging, and Microsoft Outlook. In Microsoft Exchange Server, the messages, calendar and other data items are delivered to and stored on the server not the local computer. Figure P.23 is a screen shot of where the default location is for all .pst files. In standalone applications on local machines like Stepan’s IBM laptop, the messages, calendar and other data items are delivered to and stored locally in a Personal Storage Table (.pst) file that is located on the computer. Now the .pst files themselves have the capability to be password protected. But even Microsoft admits that the password adds no protection, since anyone with access to your .pst file can simply remove the password using commonly available tools. For instance, PstPassword is a small utility that recovers a lost password for Outlook .pst files. Figure P.24 has a screen shot of this tool.

Figure P.23 – Default folder for .pst files.

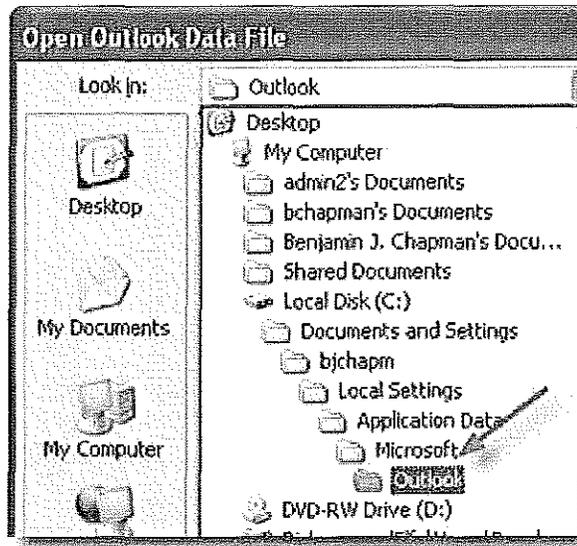


Figure P.24 – PstPassword tool.

| Filename | Encryption | Version | CRC Value | Password 1 | Password 2 | Password 3 | Full Path |
|-------------------|--------------|---------|------------|------------|------------|------------|-----------|
| Copy of 1.pst | Best | 14 | 0x2dfd2d88 | bt7FL4 | Pvjs27 | VNrIJI | F:\Do |
| Copy (2) of 1.pst | Best | 14 | 0x8b1b92b8 | SU48Y6 | Q85GI7 | WMfeYA | F:\Do |
| 2.pst | Best | 14 | 0xa1a5248e | gr5q9 | 0EeBW3 | LVA5c4 | F:\Do |
| 3.pst | Best | 14 | 0x586a0425 | 2222 | YUTqJB | hkMkvE | F:\Do |
| 0000.pst | None | 14 | 0xa52a526a | EfsT04 | TWYw76 | yk1Qr9 | F:\Do |
| abcd.pst | Best | 23 | 0xcc6120d | abcd | sph9t0 | mRSGU1 | F:\Do |
| Copy of abcd.pst | Best | 23 | 0xcc6120d | abcd | sph9t0 | mRSGU1 | F:\Do |
| Outlook.pst | Compressible | 23 | 0x00000000 | | | | F:\Do |
| 6.pst | Compressible | 14 | 0xcfa9599 | 6 | yZUzCC | YUFCxF | F:\Do |
| nir1.pst | Compressible | 14 | 0xd0286bd1 | nir1 | lsCm61 | SBEG68 | F:\Do |
| 1.pst | Best | 14 | 0xd7e37b41 | 4YCyv | bi5gh4 | 1f3tA5 | F:\Do |
| 1234.pst | Compressible | 14 | 0xbaa73fbf | 1234 | yZdHpA | hkNkwC | F:\Do |
| 5.pst | Compressible | 14 | 0x00000000 | | | | F:\Do |

16 pst file(s), 1 Selected

PUBLIC RECORD ON TAP – Microsoft said .pst files are vulnerable with passwords applied.

The password protection for Microsoft personal information store (PST) files provides only limited security. Adopting certain practices can increase this security. Utilities that can remove

or bypass the password on a PST have been posted on the Internet. None of these utilities are endorsed or supported by Microsoft.

Limiting physical access to a PST file increases the security of the data. Anyone who has physical access to a PST file and has one of these utilities can remove or bypass the PST password. These utilities will remove or bypass the PST password even for PSTs created with the Compressible Encryption and Best Encryption options.

In order to protect sensitive e-mail against unauthorized access, consider the following practices: Do not use a PST file. Store all sensitive e-mail in the Exchange Server Information Store. This is the default configuration for all clients that are used with Exchange Server.

If you need to use a PST file that is located on a file server or is in a shared directory, use file-level permissions to control which users can access the PST file.

If you use a PST file that is located on your local computer, limit access to the computer by using password-protected screen savers, locking the computer, or locking the office where the computer resides. If you are running Microsoft Windows NT, you can use the Windows NT File System (NTFS) to limit access to the owner of the PST.

To read more visit <http://support.microsoft.com/kb/143241>.

He had some information about a small firm called 3DNF, Inc. that had been acquired by Data Mining within the last six months. Vlad found some links from the United States' Securities and Exchange Commission web site and the text from a press release about the acquisition.

Stepan uses www.sec.gov to find out more information about 3DNF Inc. by searching through the EDGAR system provided by the US Securities and Exchange Commission's website. This site is a very powerful tool in researching public and private businesses who file their financials each quarter and each year. To demonstrate how easy it is to find certain information that can help collect information during the recon stage, Figure P.25 shows Google Inc.'s information. In Figure P.26 Google's Inc.'s physical address and phone number are listed along with their mailing address. This information is very useful to someone like Vlad who can now fly to California and look for potential employees that work at Google to target one of them for more information. Vlad also has an upper hand through obtaining Google's phone number. He can start conducting social engineering probes by paying some college student from the local area to call Google's number and asking some more probing questions like, "What are the working hours for Google employees?" What if you had Google's CIK number? Well with a CIK number you can find out many things, for example who the stockholders and owners are of that company. In Figure 1.3 sec.gov provides the CIK number for Google and also other helpful facts. For instance, the kind of company Google is (SIC: 7370 - Services-Computer Programming, Data Processing, Etc.), the location (CA), where Google was incorporated (DE) and their fiscal year end (12 month calendar ending December 31st each year). With such

information you can arrive at what Figure P.28 is showing, ownership data. Vlad did not do anything illegal when he found information on 3DNF's acquisition with Data Mining from sec.gov, but what he used the information for was illegal. The US Securities and Exchange Commission website is a very powerful tool in the art of recon.

Figure P.25 – Google Inc. on SEC.gov.

Search Results

SEC Items • Search the Next-Generation EDGAR System • Company Search • Current Page

Google Inc. CIK#: 0001288776 (see all company filings)

SIC: 7379 - SERVICES, COMPUTER PROGRAMING, DATA PROCESSING, ETC
 State location: CA | State of Inc.: DE | Fiscal Year End: 1231
 (Assistant Director Office HQ)
 Get insider transactions for this Issuer.
 Get insider transactions for this reporting owner.

Business Address
 1600 AMPHITHEATRE PARKWAY
 MOUNTAIN VIEW CA 94043
 650 625 4000

Mailing Address
 1600 AMPHITHEATRE PARKWAY
 MOUNTAIN VIEW CA 94043

Filter Results: Filing Type: Prior to: (YYYYMMDD): Ownership? include exclude only Limit Results Per Page: 40 Entries Search Show All

Items 1 - 40 [PDF Feed] [Next 40]

| Filing | Format | Description | Filing Date | File Firm Number |
|----------|--------------------------|---|-------------|-----------------------|
| 8-K | Document | Current report Items 5 02 and 9 01 Acc-no: 0001193125-09-107396 (34 Act) | 2009-05-11 | 000-10728 09816368 |
| 10-Q | Document | Quarterly report (Sections 13 or 15(a)) Acc-no: 0001193125-09-101727 (34 Act) | 2009-09-06 | 000-10728 09502485 |
| POSASR | Document | Post-effective Amendment to an automatic shelf registration statement Acc-no: 0001193125-09-080556 (33 Act) | 2009-04-16 | 33-142243 09753950 |
| 8-K | Document | Current report Items 2 02, 6 02, 8 01, and 9 01 Acc-no: 0001193125-09-060581 (34 Act) | 2009-04-16 | 000-10728 09753949 |
| DEFA14A | Document | Additional definitive proxy soliciting materials and Rule 14(a)(12) material Acc-no: 0001193125-09-062003 (34 Act) | 2009-03-24 | 000-10728 03701951 |
| DEF 14A | Document | Other definitive proxy statements Acc-no: 0001193125-09-061999 (34 Act) | 2009-03-24 | 000-10728 03701940 |
| SC TO-BA | Document | [Amend]Tender offer statement by Issuer Acc-no: 0001193125-09-049937 (34 Act) | 2009-03-10 | 000-10728 09670195 |
| SC TO-FA | Document | [Amend]Tender offer statement by Issuer Acc-no: 0001193125-09-046426 (34 Act) | 2009-03-06 | 000-10728 09560295 |

Figure P.26 – Google Inc.'s address and phone number.

| | |
|--|---|
| Business Address 1600 AMPHITHEATRE PARKWAY MOUNTAIN VIEW CA 94043 650 623 4000 | Mailing Address 1600 AMPHITHEATRE PARKWAY MOUNTAIN VIEW CA 94043 |
|--|---|

Figure P.27 – Google Inc.'s financial details.

Google Inc. CIK#: 0001288776 (see all company filings)

SIC: 7370 - SERVICES-COMPUTER PROGRAMMING, DATA PROCESSING, ETC.
State location: CA | State of Inc.: DE | Fiscal Year End: 1231

Figure P.28 – Google Inc.’s owners.

Ownership Reports from: (Click on owner name to see other issuer holdings for the owner, or CIK for owner filings.)

| Ownership Data | Filings | Type of Owner |
|---------------------------------------|----------------------------|---|
| AMERICA ONLINE INC | 0000883780 | 10 percent owner |
| YAHOO INC | 0001011006 | other: See remarks |
| DOERR L JOHN | 0001032455 | director |
| TIME WARNER INC | 0001105705 | 10 percent owner |
| REYES GEORGE | 0001184217 | officer: Chief Financial Officer |
| OTELLINI PAUL S | 0001188930 | director |
| HENNESSY JOHN L | 0001198046 | director |
| MORITZ MICHAEL J | 0001201045 | director |
| LEVINSON ARTHUR D | 0001214128 | director |
| SCHMIDT ERIC E | 0001242463 | director, officer: CEO, Chairman |
| MATHER ANN | 0001244892 | director |
| PICHETTE PATRICK | 0001275968 | officer: SVP & Chief Financial Officer |
| Kordestani Omid | 0001294397 | officer: SVP, World Wide Sales/Oper. |
| Rosenberg Jonathan J | 0001295029 | officer: VP Prod. Mgmt. |
| Drummond David C | 0001295030 | officer: VP, Gen. Counsel, Secty |
| Brown Shona L | 0001295031 | officer: VP Business Oper. |
| Brin Sergey | 0001295032 | director, 10 percent owner, officer: President, Tech, Asst. Secty |
| Shriram Kavitarik Ram | 0001295084 | director |
| Rosing Wayne | 0001295085 | officer: VP Engineering |
| Page Lawrence | 0001295231 | director, 10 percent owner, officer: Pres, Products, Asst. Secty |
| Eustace Robert Alan | 0001323010 | officer: Vice President of Engineering |
| Tilghman Shirley M | 0001340514 | director |

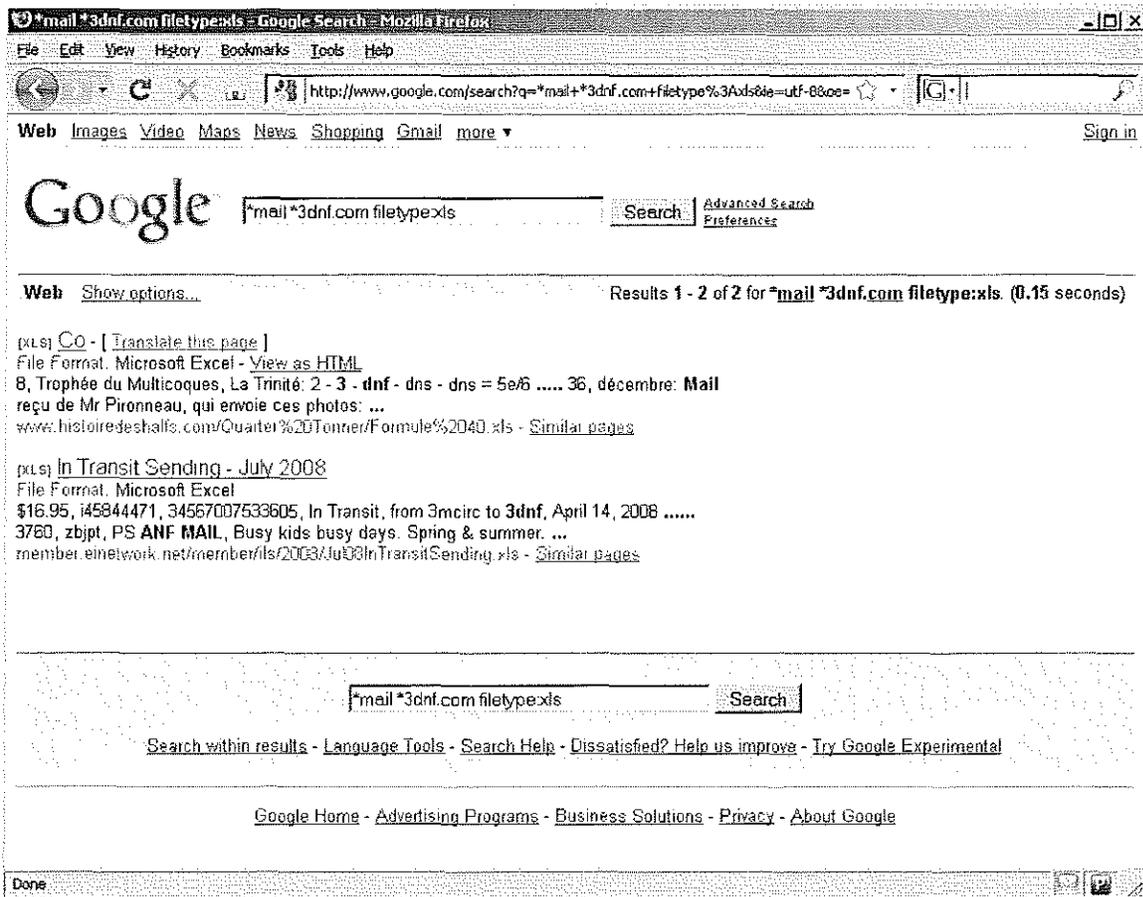
FICTIONAL STORY DISSECTED – Harvesting addresses.

Page XX

Then Stepan had listed some names and email addresses that belonged to the 3dnf.com domain. Vlad could only guess that Stepan had “Googled” the domain name to harvest the addresses. If so, Stepan was a fairly resourceful researcher.

Stepan is smart because he realizes that using a free service like Google can allow him to harvest millions of email addresses and then if he wants he can drill down even more specifically to certain email addresses he might want to pay more attention to. How did he do it? Well Stepan used a string of text in the Google search bar that might have looked like this: ***mail *3dnf.com filetype:xls**, as Figure P.29 shows.

Figure P.29 – Stepan using Google to find 3DNF email addresses.



The first word “*mail” specifies that you are looking for mail with an asterisk (*) allowing that word to be preceded by anything. The next word “*3dnf.com” tells Google what domain you want to find email addresses in. And lastly the “filetype:xls” only searches for files with an .xls extension which means Microsoft Excel spreadsheet files. In Figure P.30 Google has

searched for email addresses within the U.S. Department of Veterans Affairs (va.gov) domain. Figure P.30 also shows that there are 15,700 results for spreadsheets within the va.gov domain. Figure P.31 shows the contents of just one of the 15,700 spreadsheets. Over 80 email addresses have been found by just one click of the mouse using Google. This is recon and this is how people like Stepan find their targets.

Figure P.30 – Google email harvesting using “*mail *va.gov filetype:xls”

ROUGH DRAFT
WWW.SYNGRESS.COM
Copyright 2009 Elsevier

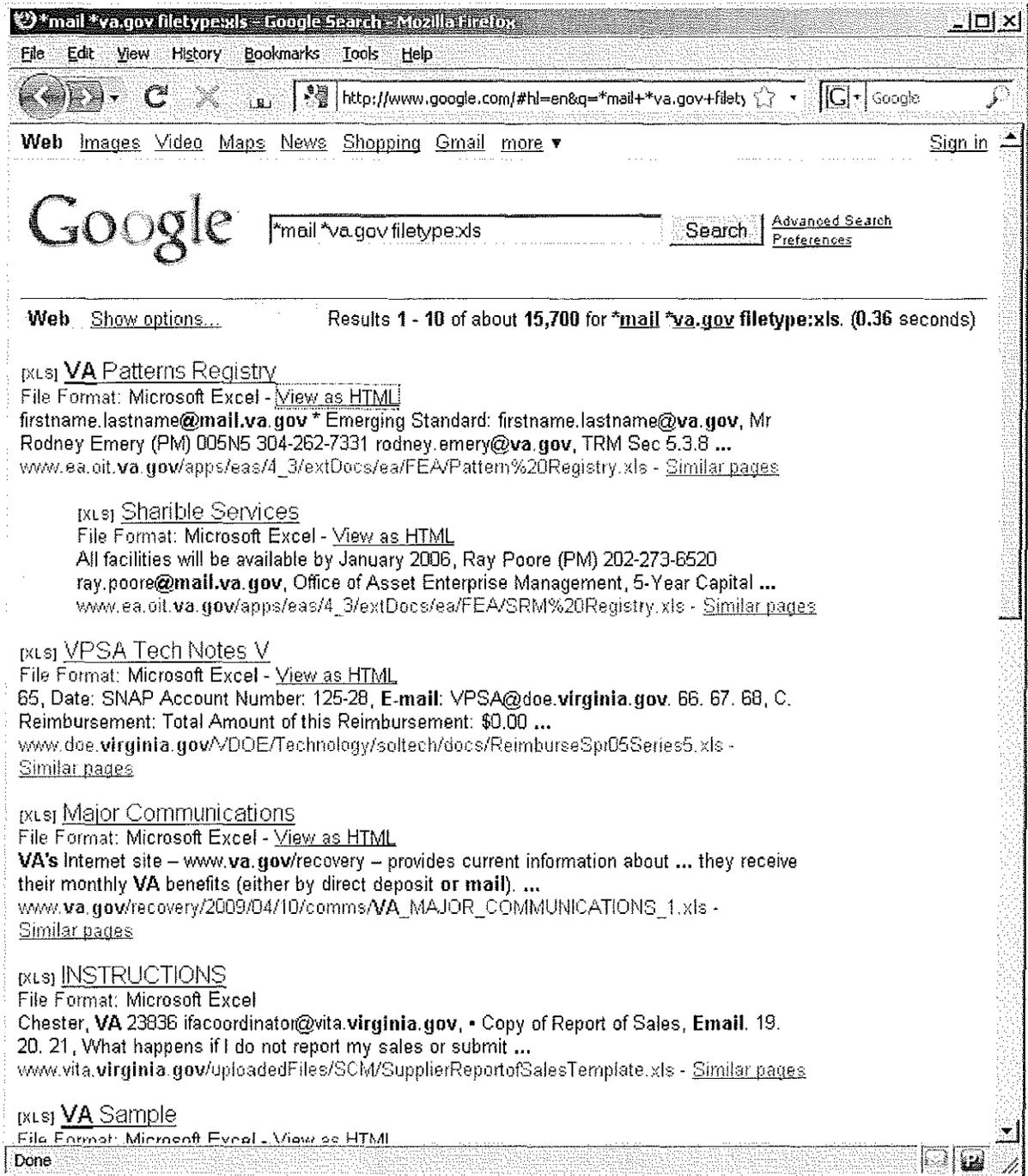


Figure P.31 – Spreadsheet with va.gov email addresses and much more.

VHA Program Office Admin POCs of Contact, Department of Veterans Affairs, Medical Facility

http://74.125.113.132/search?cache=039444CgJwww.residms.va.gov/tracks/MSpages/admin/contacts/LMS_VHA_PgmOffe

Google automatically generates this HTML view of the file http://www.residms.va.gov/tracks/MSpages/admin/contacts/LMS_VHA_PgmOffe_admin_contacts_FC_0103.xls as we crawl the web.

These search terms are highlighted: mail va.gov

Google is neither affiliated with the authors of this page nor responsible for its content.

VHA PgmOff

| | E | F | I | J | L | M | N | O | P |
|----|---|----------------|------------|---------|----------------------|---------------------------|---------------------------|--------------|----|
| 1 | VHA Program Office LMS Administrator/POC contacts | | | | | | | | |
| 2 | Sorted by Description | | | | | | | | |
| 3 | 6/20/09 | | | | | | | | |
| 4 | | | | | | | | | |
| 5 | Description | Station Number | Last | First | Phone | Email | Address | City | ST |
| 6 | VHA Chief Business Office | 101 | Ntschke | Vickie | 202-254-0323 | Vickie.Ntschke@va.gov | 1722 Eye St NW | Washington | DC |
| 7 | VHA Chief Business Office | 101 | Staples | Brian | 202-254-0349 | Brian.Staples@va.gov | 1722 Eye St NW | Washington | DC |
| 8 | Consolidated Mail Outpatient Pharmacy-Bedford | 761 | Hines | Daniel | 878-244-1300 ext2006 | daniel.hines@va.gov | 10 Industrial Ave | Chelmsford | MA |
| 9 | Consolidated Mail Outpatient Pharmacy-Charleston | 766 | Winslow | Troy | 843-745-6649 | troy.winslow@va.gov | 3725 Rivers Ave Suite 2 | Washington | DC |
| 10 | Consolidated Mail Outpatient Pharmacy-Dallas | 763 | Laurant | Wanda | 972-228-6240 | wanda.laurant@va.gov | 2962 S Longhorn Dr | Lancaster | TX |
| 11 | Consolidated Mail Outpatient Pharmacy-Dallas | 763 | Cleveland | Hillary | 972-228-6246 | hillary.cleveland@va.gov | 2962 S Longhorn Dr | Lancaster | TX |
| 12 | Consolidated Mail Outpatient Pharmacy-Hines | 766 | McIntosh | Ntando | 708-766-7816 | ntando.mcintosh@va.gov | 5th & Roosevelt Road | Hines | IL |
| 13 | Consolidated Mail Outpatient Pharmacy-Hines (alternate) | 766 | Mayhew | Mary | (708) 766-7667 | mary.mayhew@va.gov | 5th & Roosevelt Road | Hines | IL |
| 14 | Consolidated Mail Outpatient Pharmacy-Leavenworth | | Caraway | Linda | 813-727-4064 | linda.caraway2@va.gov | 5000 S 13th St | Leavenworth | KS |
| 15 | Consolidated Mail Outpatient Pharmacy-Tucson | 762 | Gordon | Phil | (520) 209-3032 | phil.gordon@va.gov | 3675 East Briarsara Drive | Tucson | AZ |
| 16 | Consolidated Mail Outpatient Pharmacy-Murfreesboro | 764 | Smith | Sharon | not provided | sharon.smith7@va.gov | 5171 Sam Jared Drive | Murfreesboro | TN |
| 17 | Consolidated Mail Outpatient Pharmacy-Murfreesboro | 764 | Sketton | Terry | 615-867-6187 | terry.sketton@va.gov | 5171 Sam Jared Drive | Murfreesboro | TN |
| 18 | Consolidated Patient Accounting Center | 730 | Roberts | Djuna | 828-298-7911 x1-5830 | Djuna.Roberts@va.gov | 1100 Tunnel Rd | Ashville | NC |
| 19 | Consolidated Patient Accounting Center | 730 | Priestwood | Barbara | 828-298-7911 x1-5678 | barbara.priestwood@va.gov | 1100 Tunnel Rd | Ashville | NC |
| 20 | Consolidated Patient Accounting Center | 730 | Elington | Lacey | 828-298-7911 x13659 | lacey.elington@va.gov | 1100 Tunnel Rd | Ashville | NC |
| 21 | Consolidated Patient Accounting Center | 730 | Garrett | Dana | 828-298-7911 x1-3483 | Dana.Garrett@va.gov | 1100 Tunnel Rd | Ashville | NC |
| 22 | Corporate Franchise Data Center (Point of Contact) | | DeJoy | Gabriel | 612-326-6541 | gabriel.dejoy@va.gov | 1615 Woodward St | Austin | TX |
| 23 | Corporate Franchise Data Center | 800 | Carragher | Lisa | 612-326-6713 | lisa.carragher@va.gov | 1615 Woodward St | Austin | TX |
| 24 | Emergency Management Strategic Healthcare Group (PHEH) | 613 | McVey | Terry | 304-264-4829 | terry.mcvay@va.gov | 510 Butler Avenue | Martinsburg | WV |

PUBLIC RECORD ON TAP – Real-Time E-mail Harvesting.

Real-Time E-mail Harvesting on Twitter: Careless users unwillingly maintain an up-to-date list of e-mail addresses

By Lucian Constantin, Web News Editor, 14th of May 2009, 10:21 GMT

Just one day after a method of harvesting e-mails from Twitter was exposed on WebProNews, a proof-of-concept Twitter e-mail grabber was released. The technique relies on using the service's real-time search function to exploit the carelessness of users

who post their addresses in status updates.

There is nothing new about the fact that spammers and e-mail marketers are using automated tools to locate e-mail addresses through Google, Yahoo! and other search engines. Some are also employing their own custom-coded robots that crawl the web specifically for this purpose. Such programs are called e-mail harvesters or grabbers and the action e-mail harvesting.

So, why would Twitter be any different in this respect? As it turns out, it is and it isn't. It is, because someone posting their e-mail address within their messages automatically makes it searchable, just like people posting it on their websites make it available on Google. This might seem obvious to many of you, but, judging by the feedback received on the issue, even knowledgeable users have overlooked this simple fact.

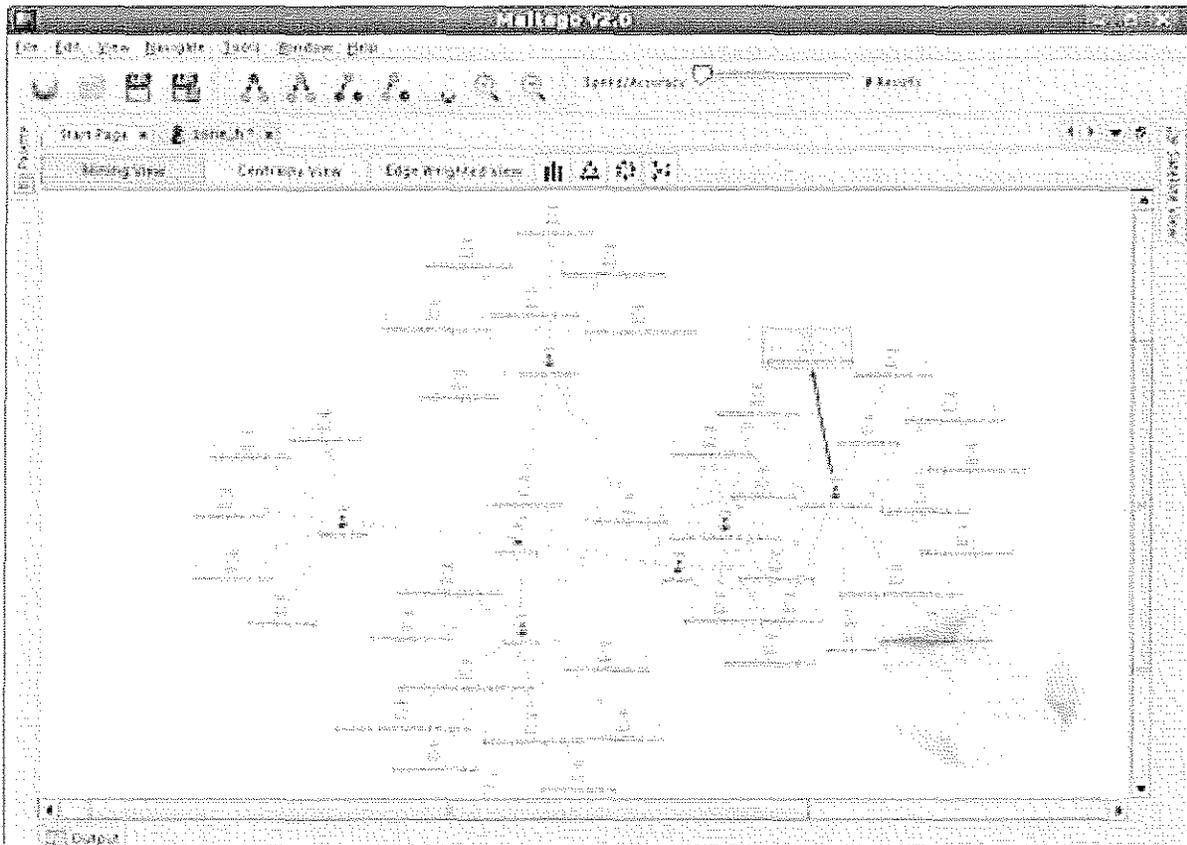
To read more visit: <http://news.softpedia.com/news/Real-time-E-mail-Harvesting-on-Twitter-111609.shtml>

Maltego

Maltego is an open source intelligence and forensics application. It allows for the mining and gathering of information as well as the representation of this information in a meaningful way. Maltego is also featured in Backtrack 4.²⁰ Figure P.32 is a screen shot of this tool and the website is <http://www.paterva.com/maltego/>.

²⁰ <http://www.remote-exploit.org/news.html>

Figure P.32 – Maltego.



FICTIONAL STORY DISSECTED - The account number.

Page XX

Vlad took a pen and small piece of paper from his coat pocket and wrote “Volksbank, 111-8-18-1-13-15-27-1” from memory

Vlad’s Volksbank account number is a derivative of the number used in the Bourne Identity. “A wounded man is found by a village doctor on beach in France. Taking care of the found, the doctor finds a microfilm under the man's skin. Under the microscope the microfilm shows a Swiss bank account number as seen in figure P.33. Since the man has lost all memory of

his life and identity, he decides to go to Switzerland and find out what he can about himself from the account number. We later learn that this man is an American spy called Jason Bourne.”²¹

Figure P.33 – Microfilm Swiss bank account number



THE PROLOGUE DISSECTED ALL OVER...but wait the real book is on sale at amazon.com!

SYNGRESS.COM
WWW.SYNGRESS.COM
Copyright 2009 Elsevier

²¹ <http://swiss-bank-accounts.com/e/fiction/bourne-identity-1988/index.html>

