Global Information Assurance Certification Paper

Offline NT Password & Registry Editor
An Administrator Tool that Compromises Security

By: John J. Orsini

The "cleaning person" looks around carefully. Noticing that everyone is gone for the day, he slips a disk out of his pocket and into your machine. He reboots the machine and a few moments later is staring at the screen that says: "Please enter new password or nothing to leave unchanged:". The attacker enters a password of his choosing, removes the diskette, and reboots. Then, he accesses the local administrator account using the password he just entered. He takes another disk from his pocket and installs stealth key logging software. After rebooting one final time, he continues with his vacuuming. Later that week he returns to find your passwords to the routers, domain, Novell shares, and your personal bank and online brokerage account neatly saved on a file. Your organization's security as well as your personal information has been compromised – all because of one little disk. The following paper will discuss that "little disk" – formally known as Offline NT Password & Registry Editor – an administrator tool written by Petter Nordahl-Hagen. This tool was originally designed for system administrators who needed to reset the administrator's or user's passwords on a local machine. In the wrong hands, it can be used to attack the same network administrator's it was created to serve. The pages that follow outline where to get this tool, a step-by-step list of instructions on how to use it, the implications of its application, and counter-measures you can employ against Offline NT Password & Registry Editor to secure a network from this type of threat. Recognizing and preparing for this type of disk based local attack is essential. There has been an increase in the number of powerful Linux based tools that allow attackers to gain local administrator privileges on Windows NT machines.

I. Downloading and Using the Offline NT Password & Registry Editor

The tool, called Offline NT Password & Registry Editor, is available for download from http://home.eunet.no/~pnordahl/ntpasswd/bootdisk.html. The user will need to download, at a minimum, the following files: bd010114.zip and rawwrite2.zip. If the user requires additional support for SCSI cards or RAID arrays, he must also download sc010114.zip. First, unzip the files to a folder on the hard drive. Using rawrite2, create a bootable floppy that contains the Offline NT Password & Registry Editor. This can be accomplished using the following command at a DOS command prompt: *rawrite2 –f: bd010114.bin –d: A*. If a Linux or Unix machine is available, the command *dd if=bootdisk.bin of=/dev/fd0 bs=1024* will also produce the boot disk. Once the boot disk has been successfully created, the next step involves booting the machine from the floppy drive. **CAUTION**: Please make an Emergency Repair Disk before using this utility to avoid having to rebuild the machine in case of registry corruption. Upon booting, the utility loads a custom mini Linux distribution and displays the following statement:

> This utility will enable you to change the password of almost any user (including administrator) on an Windows NT installation WITHOUT knowing the old password.
> The program is now able to actually parse/follow the internal registry structure completely. (this version contains partial registry-editor with 'only-write-same-size' write support).
> Tested on: NT3.51 & NT4 Workstation, Standalone server, PDC.
> Win2k Prof & Server RC2 (not with Active Directory server)
> Now also handles (disables) syskey, read warnings if applicable.
> You may either let the scripts try to figure out your configuration, or you may do it manually from the shell prompts.
> Good Luck!

From this point, the user is prompted to press enter. The utility then asks the user if they want to probe for, specify, or skip loading SCSI drivers. After the user selects the proper response for his environment, the program then displays a list of partitions and asks which partition contains the Windows NT installation. The partition that contains the NT installation is selected by default. When the user selects the partition on which the NT installation resides, the utility mounts that partition as read/write and prompts the user for the type of action to be performed. The choices are set passwords (the default) or edit the registry. After choosing to set passwords, the utility then asks for the full path to the registry directory. After entering the correct path and pressing enter, the user is asked to select what hive they want to edit. Once again pressing enter will accept the default hives necessary to successfully change the desired passwords. When the enter key is pressed, the SAM, system, and security hives are copied to the /tmp directory and all local users of the machine are listed on the screen. Any user that has a blank password will have a comma after their name and the words "***BLANK Password***". The utility then displays a warning message about disabling the syskey function in Windows 2000, the utility will ask the user if they really want to disable the syskey. This is not suggested in Windows 2000 (doing so may corrupt the sam file). After making that selection, the user will be prompted with the username that they would like to change. The username of the local system administrator (no matter what the name actual name is) will appear as the default. After entering the name of the account whose password the user wants to change, the user will be prompted to enter the new password. Finally, after entering the password, the user will be prompted to make sure he wants to make the change. When the user selects "yes", he will have the option to change another password or quit the program. The process is repeated until all of the desired passwords have been changed. When the user selects "quit" by pressing the "!", a summary screen will appear noting what registry hives have been changed and asking if the user wants to write to the hive files. After selecting yes, the user will be prompted again asking if they want to perform the write. Finally, the write back to the appropriate hives is made. The user can now remove the disk from the floppy and reboot. In summary, the only changes that have to be made are the selection of the proper SCSI card drivers (if necessary), entry of a user name if they if they want to change someone other than the local administrator's password, and typing "y" for the last three questions.

II. Implication of the Utilities' Use

"Your security is only as strong as the weakest link." Every security professional has heard this euphemism. In this case, the weakest link is the local administrator account of a Windows NT machine on your network. The reason that this tool deserves special attention is that it brings to a relatively unskilled person the capability to gain control of the local administrator's account in a relatively short period of time. In addition, the direct forensic evidence of its use is minimal.

In this section, we will examine the Offline NT Password and Registry Editor in the context of the "Three Bedrock Principles" and the three elements of "The LevelOne Threat Model" that were presented in the first section of the Security Essentials Course. The use of this tool attacks all three "Bedrock Principles" – confidentiality, integrity, and availability. Confidentiality is attacked by the attacker gaining access to the local machine and editing the Security Access Manager (SAM) database file. Integrity of the local workstation is compromised when the attacker logs on to the local workstation with the local administrator's. The final principle, availability, is attacked because the changing of the local administrator's password prevents the legitimate administrator from logging on to that machine.

The three elements of the "LevelOne Threat Model" are threat, vulnerability, and compromise. The Offline NT Password and Registry Editor fits this model very well. The threat is an attacker armed with this utility who wishes to subvert a machine on the network for a variety of reasons – reconnaissance, password theft, or denial of service. The vulnerability exists because Windows NT has no method of protecting or logging changes to the SAM file or registry before the operating system is booted. Also, preventing physical access to the machine at all times may be impossible in many situations. The final element of this model, compromise, occurs when the attacker (the threat) exploits the vulnerability.

III. Countermeasures

The countermeasures that may be employed against this utility fall into two broad categories. The two categories are the physical security of the machine and detecting the symptoms of the utilities' use through anti-virus or asset management software and intrusion detection systems. The reason that there are very few other categories of countermeasures that may be utilized by a security administrator is that the tool is very intelligent. For example, because this utility reads from the registry, moving the default location of the NT install from C:\WINNT to C:\FOO or renaming the local administrator account to RealAdmin have no effect.

The first category, physically securing the machine, should allow the system administrator to limit the methods by which the intruder can employ this utility. As a most basic precaution, the company should monitor access to the building, and if it is warranted, have contractors and employees that work in secured areas complete a background check. The computer case should be locked to prevent unauthorized access to the jumpers on the motherboard and the BIOS should be password protected. In addition, the computer should be set to boot from the hard drive only. Since these precautions can be easily defeated, however, a system administrator may choose to

remove all bootable devices besides the hard disk drive (floppy, CD-Rom, and ZIP-type drives). If the need for these drives is greater than the perceived benefit from permanently removing them, there are various floppy and CD-Rom locks that would allow the administrator to retain positive control of those resources, but still allow him to unlock and use them when necessary. Due to the proliferation of USB and FireWire bootable drives, the administrator may also choose to disable those interfaces, as well as any unused COM or LPT ports, in the BIOS. In cases where extreme security is a necessity, the use of thin clients or removable hard drives that would be locked in a secure area when not in use are possibilities, albeit very expensive ones if a different architecture is already in place. While these steps may slow an attacker's attempt to gain the use of the local administrator account on a machine, they can be subverted.

An attacker is not likely to cease his penetration after having gained administrative rights to a single machine. He would probably attempt to steal information from the host machine outright or install various utilities that would allow him to map the network, attack and subvert other machines, or monitor users' activities to gain additional passwords or other personal information. This is where a company who has implemented a defense-in-depth based strategy will reap the benefits. The attacker's attempt to steal sensitive data from the local machine can be thwarted by the absence of removable media drives, the data being encrypted using PGP or some other strong encryption, or a company policy that does not allow for the saving of any information to the local drives. This policy can be enforced systemically using a variety of registry keys and ACLs that effectively lock the users out of My Computer, Network Neighborhood, Control Panel, DOS command windows, the Run command, and many other local system resources.

If the attacker chooses to install secondary utilities, such as network scanning or trojan software, the presence and activity of these programs on the affected host machine or across the network will be the administrator's most valuable clues that one of their hosts was subverted. If any common backdoor or trojan software package (Sub-seven or Back Orifice) installations are attempted, the anti-virus software installed on the local host should detect this and should quarantine the "virus" and notify the system administrator. If the administrator has deployed asset management software, such as Unicenter TNG, the administrator would be alerted to an unauthorized program being installed on the machine. Host-based software firewalls and Intrusion Detection Systems (IDS), such as Zone Alarm or Tiny Firewall would also prevent trojan executables from "phoning home". Some of the more advanced centrally managed host-based IDSs would also alert the system administrator to these attempts. Similarly, a network based IDS configured to monitor the internal network may detect the scanning from the subverted host machine. The IDS may also notice that the network card has been turned on in promiscuous mode or that additional ports may be open on the host machine. IDSs in place on the border router may detect traffic on known trojan ports or destined for domains that the administrator's may deem unusual or unsafe.

System auditing would be the one of the last methods of detecting this utility's use and the subsequent installation of scanning or backdoor software. As mentioned above, there is scant forensic evidence left from the Offline NT Password and Registry Editor. The only forensic evidence left in the logs on the computer will be an illegal shutdown and a successful login of the local administrator account. If the logging

utilities are set up to record this type of information AND the logs are reviewed in a timely manner, they will provide the system administrator with his first clues that the machine has been compromised. The use of sysdiff to compare a baseline machine to its current configuration would expose the presence of additional programs that had been installed. As a final line of defense, users should have their concurrent logins set to an appropriate (low) number and the times that they have network access limited to their official work hours. This would limit an undetected attacker's opportunity to utilize any passwords that he has captured.

IV. Conclusion

A system administrator or security professional that has read the preceding sections now has a clear understanding of the capabilities and threats posed by the Offline NT Password & Registry Editor. He realizes that there are many additional attacks that are facilitated once an attacker gains the foothold of administrator privileges on a local workstation. In addition, he is now aware of the many individual countermeasures that can be employed against this type of threat. While implementing some of these defenses separately will serve him well, he will be certain that a defense in depth strategy will protect his network more thoroughly than any subset of the individual defenses mentioned. With these defenses in place, your environment will provide a much greater challenge to the "cleaning person" using the Offline NT Password & Registry Editor for more than its original purpose. While the local administrator account on a workstation may not be considered the crown jewels of your company, it certainly provides a key to getting into the safe.

References

1. Bowen, Ted. "Lockdown." Network World Magazine. (April 30, 2001): 42 – 43, 46.
2. Introduction to Information Systems Security (INFOSEC) Guidebook. URL: http://www.fma.hq.navy.mil/FMA/Publications/NAVSO%20Publications/P5239-01.pdf. (March 24, 2001)
3. Nordahl-Hagan, Petter. "Offline NT Password & Registry Editor." URL: http://home.eunet.no/~pnordahl/ntpasswd/ (March 23, 2001).
4. Nordahl-Hagan, Petter. "Offline NT Password & Registry Editor, Bootdisk." URL: http://home.eunet.no/~pnordahl/ntpasswd/bootdisk.html (March 23, 2001).
5. Sutton, Steven. "Windows NT Security Guidelines." June 3, 1999. URL: http://www.trustedsystems.com/download/NSAGuideV2.PDF (March 27,2001).

Last Updated: July 25th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event