Global Information Assurance Certification Paper

The Commonality of Authenticators Vulnerability Relative to NT Local Administrator Accounts

By Daniel Marvin

The Local Administrator account exists by default on every NT machine in any enterprise. Do all your NT machines have this account renamed uniquely and a unique password applied? I didn't think so. This paper addresses the vulnerability of these shared authenticators and the mitigations of that risk.

The Vulnerability:

I can't say it any better than this, *"It is a common practice for many workstations in a domain to share the same Local Administrator password. This is sometimes a result of workstation build procedures (disk cloning software or unattended software installs) or sometimes it is simply left that way for the ease of support personnel who must access those workstations and don't want to carry around a huge list of Local Administrator passwords."* [1]
This commonality of authenticators means that a compromise of one machine translates into the exposure of multiple machines.

This vulnerability is quite widespread due to the dearth of education in this matter. Microsoft says only that, "This password should be guarded carefully.."[2] (no mention of unique passwords per machine). It is not addressed in the Windows NT Security, Step by Step guide distributed by the SANS Institute. No mention can be found of "uniqueness" with respect to Local Administrator accounts – at least in version 2.15. *(Hopefully this oversight will be rectified in the next release of the SANS NT security guide).*

The good folks at SANS shouldn't feel badly however, they are in excellent company with the likes of the Naval Surface Warfare Center.[3]
The only reference I could find relative to Local Administrator accounts is a blurb on "Prevent users from setting up an automatic login as the administrator."[4] A consultation of the Windows NT Security Handbook by Tom Sheldon also produced no mention of unique passwords.

I thought NT passwords were secure?

"There are two factors which in combination create the vulnerability. First, local NT accounts are easy to crack [5]. Even with a "locked down" box (profiles, syskey, etc.), a determined local user can crack other local account names and passwords. And, of course, one of those other "local" accounts is the Administrator account. Which brings us to the second contributing factor.

---

[1] Marvin, Daniel and Parker, Steven Local Account Password Manager, http://www.foghornsecurity.com/lapm/lapm.
[2] http://www.microsoft.com/technet/winnt/winntas/manuals/concept/xcp02.asp
[3] Naval Surface Warfare Center, Dahlgren Division IS Security Security Office, "Windows NT Computer Risk Assessment" specifically referencing sub document titled "Best Password Practices for Windows NT", http://www.nswc.navy.mil/ISSEC/Form/acc_part2_nt.html .
[4] http://www.nswc.navy.mil/ISSEC/Form/nt40_help.html#passwords
[5] http://www.l0pht.com

The second factor is the commonality of authenticators in most large NT installations for reasons stated above. Once the account name and password are obtained for a single machine, that information extends ones access to all machines which share the common authenticators. In other words, the information needed to access all the machines in a domain, exists on every machine. That's bad!" [6]

Note that with physical access the attacker can use simple tools like "NTFS for DOS" [7] or "LockSmith" [8] and L0phtcrack (password cracker)[9]. The attacker could also simply remove the hard drive and mount it in another NT machine.
Here's what an attack might look like in an enterprise suffering from the commonality of authenticators:

1. From a workstation
   a) A new contractor is provided with an NT workstation.
   b) Using a DOS boot disk and an NTFS utility he copies the local SAM to the floppy disk.
   c) Using L0phtCrack software he cracks the local administrator account on his workstation.
   d) Now he can access any workstation as "local administrator" because all the workstations have the same local administrator password.
   e) He installs a keyboard sniffer on any target workstation and waits for the target to authenticate to the domain.
   f) With a little patience, he will soon know all the victim's passwords for any platform remotely logged into by the victim – mail systems, file systems, mainframes, etc…

Don't underestimate the importance of securing the NT workstation. All to often the focus is on the NT servers without sufficient regard to the workstation.

"Since NT environments are almost universally networked, securing individual workstations is as important as securing the servers."[10]

2. From a server
   a) A support person has access to a single NT server
   b) He cracks the local admin account on that single server
   c) Now he can access multiple servers
   d) This support person has now bypassed our attempts to restrict his access to a single server.

Mitigations

Securing your enterprise is a constant battle with management and other business units whose

---

[6] Marvin, http://www.foghornsecurity.com/lapm/lapm .
[7] http://www.sysinternals.com/ntfs30.htm
[8] http://www.winternals.com/products/repairandrecovery/0locksmith.shtml
[9] http://www.l0pht.com
[10] The SANS Institute, Windows NT Security Step by Step, version 2.15, 7/30/1999, introduction page 2.

sole desire is the greatest functionality at the lowest cost. If you cannot remove the commonality of authenticators for whatever reason, then consider implementing the following mitigation steps.

Living with commonality (if you must)

1) Restrict local administrator from network login.
If an attacker gains Local Administrator on one machine, this will limit the exposure to those machines to which the attacker has physical access. Use UserManager to remove the user right of "access this computer from the network" from the Local Administrators Group and add this right to the Domain Administrators group

2) Change local administrator accounts throughout the enterprise frequently.
The strength of the passwords you choose relative to the length of time needed to crack them will determine how often you change the passwords.

3) Change the accounts without giving away any domain accounts.

Mudge, an expert on cracking NT passwords states, "..even if you have installed Service Pack 3 and enabled SAM encryption your passwords are still vulnerable if they go over the network."[11]

We cannot simply use a domain admin account and an automation script (ex. use PERL and the NetAdmin module) to access every machine and change the Local Administrator account. This would give away the domain admin account information to any compromised workstation we might touch in the process of changing the Local Administrator password. The domain account being used to apply new local account passwords should have its own password changed frequently during the application process and absolutely must have its password changed when finished applying new passwords.

The above security measures will improve your security stance but don't overlook the remaining gaps.

Weaknesses of the above mitigations:

Mitigation number 1:

- Leaves the attacker capable of accessing any NT machine to which they have physical access.
- All they have to do is install a keyboard sniffer on their neighbor's workstation.
- Depends on mitigation #2 to prevent the attacker from gaining support personnel access when support personnel logon to the attacker's PC.

Mitigation number 2:

- Unless we change the password faster than it can be cracked, we have gained

[11] http://www.insecure.org/sploits/l0phtcrack.lanman.problems.html, mudge, 7/12/97

nothing.

Mitigation number 3:

- This is difficult to accomplish without specialized tools such as ZenWorks from Novell.
- If we use a script and a domain account to change the Local Administrator passwords remotely, we must remember to change the password of the domain account we are using faster than it can be cracked.
- While we could use the Local Administrator account to change the local password, we would then have to maintain a mapping of workstations to passwords.

Given the remaining weaknesses of the above mitigation steps, it is clearly preferable to remove the commonality entirely.

Removing Commonality (preferred!)

There are several issues to consider in the removal of common passwords. First, the issue of **uniqueness**.
"If the problem is sameness, then uniqueness is obviously a good start at a solution." However, uniqueness alone is not enough. We are really concerned with predictability - How easy is it to determine one password from knowledge of another. Common passwords are 100% predictable, while random passwords are, by definition, 0%predictable. The closer to 0% predictability, the better." [12]

The second issue is **strength**, which is an extension of uniqueness. Essentially, strong passwords will incorporate the "0% predictable" aspect of uniqueness and also be brute force attack resistant. The latter is achieved by utilizing a large character set and a long password length.

The third issue is **recoverability**. The pragmatic realities of corporate life usually dictates that Local Administrator passwords be recoverable. When the CEO's PC needs its IP stack reinstalled the support personnel will crucify whoever mandates that they cannot recover the Local Administrator password! Recoverability is key to administrative functionality. If we didn't care about recoverability, then we should use randomly generated passwords – and if we do then the password management issues disappear. Unfortunately, recoverability is a necessary evil of administrative functionality. I haven't seen a business yet that didn't have a strong case for recoverability, which brings us to the issue of password manageability.

The fourth issue is **manageability**. The administrative needs of an enterprise require access to the Local Administrator accounts. How will we manage the generation of unique and strong passwords? How will we manage the application of those passwords? How will we manage the storage of those passwords? How will we manage the dissemination of those passwords when needed?

[12] Marvin, http://www.foghornsecurity.com/lapm/solution .

If you design your own solution you should carefully think through the above four issues. **If you don't have uniqueness, you've gained nothing**. If you don't have strength you've gained very little. If you don't have recoverability you might be looking for a new job. If you don't have a cogent plan for manageability then you must be concerned with storage considerations, manual recovery procedures, generation algorithms, and a dissemination process to support staff.

If you want an inexpensive commercial tool that addresses the above four issues, then you might consider the Local Account Password Manager from Foghorn Security (www.foghornsecurity.com).

Additional Considerations When Removing Commonality:

1) When support personnel logon to a user's workstation, your policy should require that they use only the local administrator account.

Assuming the workstation to be potentially compromised, you don't want to give away your domain account information to any hardware [13], software [14] keyboard sniffing agents, or SMB gathering software [15] installed on the local machine.

Cautions:

- Support personnel find this to be restrictive; in particular if there are resources on the network that require domain account authentication.
- This relies on personnel compliance with policy.

2) Do not extend the above policy to servers, rather you will want to require domain accounts or local user accounts for the purposes of auditing.

It is essential to know who did what when on your servers. We cannot allow local logins using the Local Administrator account or we forfeit any meaningful auditing due to the anonymity of the Local Administrator account.

Cautions:

- An attacker can easily gain the domain access of other support personnel by grabbing their SMB packets or installing a keyboard sniffer on a compromised server. This cannot be avoided without sacrificing the native audit capabilities of NT.

[13] http://www.keyghost.com
[14] http://www.tucows.com
[15] http://www.l0pht.com

Bibliography

The SANS Institute, Windows NT Security, Step by Step, version 2.15. Copyright 1999

Risk Assessment/Countermeasure Analysis/Security Test and Evaluation (ST&E) for Microsoft Windows NT Computer Systems NAVAL SURFACE WARFARE CENTER, DAHLGREN DIVISION IS SECURITY OFFICE, AUGUST 25, 1999 PART II (V3.1.1) http://www.nswc.navy.mil/ISSEC/Form/acc_part2_nt.html (2/12/2001)

Best Practices for NT Passwords, (sub document of above), NAVAL SURFACE WARFARE CENTER, DAHLGREN DIVISION IS SECURITY OFFICE, AUGUST 25, 1999 PART II (V3.1.1) http://www.nswc.navy.mil/ISSEC/Form/nt40_help.html#passwords (2/12/2001)

Windows NT 4.0 Risk Assessment Helpfile (sub document of above) http://www.nswc.navy.mil/ISSEC/Form/nt40_help.html#passwords (2/12/2001)

Marvin, Daniel and Parker, Steven. Local Account Password Manager. Foghorn Security, http://www.foghornsecurity.com/lapm/lapm, (2/12/2001)

Sheldon, Tom. Windows NT Security Handbook. Osborne McGraw-Hill, © 1997

Mudge, http://www.insecure.org/sploits/l0phtcrack.lanman.problems.html, 7/12/97

Microsoft Online Technet, http://www.microsoft.com/technet/winnt/winntas/manuals/concept/xcp02.asp (2/12/2001)