Tiered Logon Protocol / Role Based Access Control

A hacker / cybercriminal, having gained access to a system network, will begin to explore that network, looking to identify resources and acquire privileges to gain access. A good place to start is the machine on which the hacker is connected – looking for account credentials in the credential manager, registry, active memory, windows vault, caches of browsers, and so on. It is not necessary for a hacker to have remote control over a target PC – well designed software carried in through a phishing web page will suffice.

This white paper is focused an administrative model designed to prevent caching of credentials of privileged accounts, such that management information gleaned by the hacker is not useful. Four management roles will be defined, with enforcement of use restrictions such that it becomes very difficult for a hacker to gain access to an account with useful administrative rights. There are three topics to discuss, then: i) the particulars of the four management roles; ii) restrictions around the underlying NT security groups for the four management roles; and iii) enforcement, through policies and networking, of the use of the resulting four management accounts.

Cybersecurity is complex, and there are many aspects to securing a network. Detection of an intrusion is a different discipline – as a hacker begins to explore a network, there will be a distinctive pattern of events that can be detected, leading to an alert. This is the focus of an integrated SIEM (System Information and Event Management) and IDS (Intrusion Detection System) – another important aspect within the network security toolbox. This paper is focused not on detection, but on hindering the effectiveness of a hacker who has gained access to a network.

Four management roles are defined:

1. Domain management, with rights to manage user accounts, Group Policy Objects, DNS, and DHCP. This role can create, modify and delete user accounts and assign non-management security groups – for instance assign rights to access a particular file share. The domain management account should not be used to log into any computer – server, domain controller, or other.
2. Server management – a member of the local administrators group of servers and computers located on the server network. Accounts with this role are used to log onto any computer on the server network, and have full rights to perform any server work. Server work includes installation, configuration and removal of applications, services, and Windows roles and features to the server, creation and management of file shares, management of NTFS security.
3. Workstation management – a member of the local administrators group of computers located on the user network – primarily PCs and workstations. Accounts with this role should never be used to log onto any computer. These accounts can be used with the runas or similar mechanism when needed to install, configure or remove software or other local machine management tasks.
4. Workstation user account – used to log onto any computer on the user network. This account has only domain user rights – no access to any other system resources. It is preferable that a system administrator use this account, rather than their personal account, to log into computers other than their own. Reasons include i) folder redirection with local caching, if in use, should not replicate the personal folders and files of the system manager to the local drive; ii) unauthorized use of the account should not have access to file shares and other resources that may

have been assigned to the system manager's personal account; iii) credentials for the system manager's account typically provide access to the personal e-mail system, even if hosted and off-premises.

A fifth, restricted, management role is defined – the super-administrator, with domain admin rights, possibly also enterprise and schema admin rights. This is the only role that has rights to assign management rights to user accounts, and would be used to i) create and manage network administrator accounts; ii) modify Active Directory schema – for instance by installing services such as Exchange; iii) use in the event of system recovery and system procedures.

These management roles are implemented through use of NT security groups and Group Policy Objects (GPO). One NT security group is established for each role and location. Four are relatively easy:

- Workstation user account – this is simply a domain user account that is a member of the Domain Users group and no other. The account is allowed console logon to any computer – and so is able to log on to any PC. The account must be blocked from console logon to any server via GPO, by adding to the respective security group to the local security setting "Deny log on locally".
- Workstation management account – a GPO can add this account to the local administrators group of PCs and workstations. Assuming MFA, this account will not be able to log on directly, but can be used in a runas mechanism.
- Server management account – a GPO can add this account to the local remote desktop users group.
- Super-administrator – this is simply a standard account with full domain admin rights. The account will be blocked from logon to computers on the user LAN by MFA, as it will not have an assigned token.

This leaves the domain management account. Management rights for this account will require delegation of Active Directory rights for each of the administrative areas – users and computers, sites and services, group policy, and so on.

Not to overlook those NT groups that are used to grant management rights – these directory objects should all be located in an Organizational Unit (OU) that has been explicitly -not- been delegated to any of the management roles, such that a domain management account does not have rights to grant these roles to any user account. It follows that the standard built-in groups such as domain admins, enterprise admins, schema admins, as well as groups similar to vSphere admins, SQL admins should also be added to this restricted security groups OU. With this construct, these groups and the OU that contains them are not even visible or searchable from the management accounts.

Network segmentation, while not required to implement the Tiered Logon Protocol described here, is an important tool in restricting access and establishing a hierarchy of security shells, from public (Internet), Internet facing, user network, servers, and on to more highly secure networks. Access between networks can be restricted to authenticated and authorized connections, managed by a firewall. The TLP fits right into this network segmentation, starting with directing all network connections initially to the user segment, including all VPN connections as well as direct connections from all user areas. Only

user accounts are permitted to log into any computer on the user network, workstation management accounts are permitted only within a runas shell (with passwords not cached on the local machine), server management, domain management and super-administrator accounts are not allowed to log in to any computer on the user network. Now an intruder has access only to the user LAN, with no direct access to any server, and no access to a management account or cached management account credentials.

System administrators must first log into the user network, and then connect remotely to a computer (virtual PC, perhaps) on the server network. Caching of credentials to the remote desktop client can be prohibited by network policy. Once on the server network, only the server management account can be used for log onto any computer. All accounts permitted on the user network are blocked on the server network, and *vice versa*. Domain management and super-administrator accounts can only be run via runas or similar mechanism, and so passwords are not cached on the computer. And none of the management roles have the ability to grant management rights to any other account.

These measures are focused on management rights, and do not address secure concerns related to authorized access to company information from the user network. End-user accounts may have access to the most sensitive corporate information, in the form of file shares or database applications, and will necessarily be available on the user network. These concerns will require other technologies, likely including Data Loss Prevention (DLP), Internet Web Security (IWS), Intrusion Detection System (IDS), and e-mail inspection.

Access to Active Directory Domain Controllers pose special risk. An intruder who gains an active user session on a Domain Controller can quickly compromise overall network security at the highest level through creation of a special structure, stored within a file and usable over time from any computer. This structure is referred to as a "Golden Ticket", and use of this to access network resources over time is all but undetectable, as it is not logged in system security logs. For this reason it is recommended that logon to domain controllers is not allowed for system administrators, at any time. All domain management functions can be handled without directly logging onto these computers. Further, DCs should be running the Windows core operating system, without the standard windows GUI.