

RE: Threat vector of running a service using a domain account

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2007-09/msg00192.html>

- *From:* "Roger A. Grimes" <roger@xxxxxxxxxxxxxxx>
 - *Date:* Sat, 15 Sep 2007 15:22:30 -0400
-

Yes, I'm confusing my dumps. Service account passwords, which I think the original poster was inquiring about, dumps from memory using lsadump. Cachedumps are for local logon password dumps.

Lsadumps retrieve the passwords in plaintext (each char. separated by a . character).

Cachedump, which again, doesn't work so well against the latest versions of the Windows OS does dump the locally stored logon cached passwords. However, they are far from plaintext. The retrieved hashes are even stronger than the normally "hard to crack" NT hashes. I can retrieve the hashes fairly easily (logged in as local admin on an older version of Windows), but converting them from their hashed form is difficult. If the password is longer than 8 characters, a brute force method most likely won't work anytime soon. And there aren't any Rainbow tables for password hash cache dumps as far as I know.

So, unless your admin logon passwords are weak, extracting the logon hashes alone isn't that helpful, whereas, using lsadump has helped me privilege escalate from local admin to Enterprise Admin in a few minutes many times.

Of course the far bigger threat to any environment is nearly any other sort of client-side attack you can randomly think of.

Roger

```
*****
*Roger A. Grimes, InfoWorld, Security Columnist
*CPA, CISSP, CISA, MCSE: Security (2000/2003), CEH, yada...yada...
*email: roger_grimes@xxxxxxxxxxxxxxx or roger@xxxxxxxxxxxxxxx
*Author of Windows Vista Security: Securing Vista Against Malicious
Attacks (Wiley)
*http://www.amazon.com/Windows-Vista-Security-Securing-Malicious/dp/0470101555
*****
```

RE: Threat vector of running a service using a domain account

-----Original Message-----

From: listbounce@xxxxxxxxxxxxxxxxxxxxx [<mailto:listbounce@xxxxxxxxxxxxxxxxxxxxx>]
On Behalf Of Ramsdell, Scott
Sent: Friday, September 14, 2007 3:35 PM
To: Roger A. Grimes; Ali, Saqib; Jay
Cc: smanaois3@xxxxxxxxxxx; security-basics@xxxxxxxxxxxxxxxxxxxxx
Subject: RE: Threat vector of running a service using a domain account

From recollection, cachedump grabs the hashes that have been stored in the registry.

It is persistent across reboots therefore, and effected by the "Number of logons to cache" setting in AD.

I've used cachedump to demonstrate why the Helpdesk shouldn't login to user's workstations with domain admin creds, when the users themselves are local admins.

Kind Regards,
Scott Ramsdell

-----Original Message-----

From: Roger A. Grimes [<mailto:roger@xxxxxxxxxxxxxxxxxxxxx>]
Sent: Friday, September 14, 2007 2:25 PM
To: Ramsdell, Scott; Ali, Saqib; Jay
Cc: smanaois3@xxxxxxxxxxx; security-basics@xxxxxxxxxxxxxxxxxxxxx
Subject: RE: Threat vector of running a service using a domain account

I'm not sure...so I'm just speculating...but

All service account passwords are stored locally in the LSA secrets store.

Cachedump only works locally against the cached passwords, left in MEMORY to facilitate service authentications. You can't get to the truly stored hashes on the disk because they are protected by a secure mechanism, so you have to get them in the memory cache area. I'm guessing that the real hash is stored securely. When the service starts up and uses a Kerberos account, the pre-auth hash is sent, and in memory briefly. But after the pre-auth handshake, what is kept in memory is the Kerberos token, which is now used for all future auth. needs for the next 10 hours or more.

I could, and may be wrong.

Roger

RE: Threat vector of running a service using a domain account

RE: Threat vector of running a service using a domain account

*Roger A. Grimes, InfoWorld, Security Columnist *CPA, CISSP, CISA, MCSE:
Security (2000/2003), CEH, yada...yada...

*email: roger_grimes@xxxxxxxxxxxxxx or roger@xxxxxxxxxxxxxx *Author of
Windows Vista Security: Securing Vista Against Malicious Attacks (Wiley)

*<http://www.amazon.com/Windows-Vista-Security-Securing-Malicious/dp/0470101555>

-----Original Message-----

From: listbounce@xxxxxxxxxxxxxx [<mailto:listbounce@xxxxxxxxxxxxxx>]

On Behalf Of Ramsdell, Scott

Sent: Friday, September 14, 2007 9:01 AM

To: Ali, Saqib; Jay

Cc: smanaois3@xxxxxxxxxx; security-basics@xxxxxxxxxxxxxx

Subject: RE: Threat vector of running a service using a domain account

Saqib,

I believe you're right. Each time I've run cachedump for demonstration I do not receive hashes for services logging in over the network, I only receive hashes for interactive users.

Kind Regards,
Scott Ramsdell

-----Original Message-----

From: listbounce@xxxxxxxxxxxxxx [<mailto:listbounce@xxxxxxxxxxxxxx>]

On Behalf Of Ali, Saqib

Sent: Thursday, September 13, 2007 12:42 PM

To: Jay

Cc: smanaois3@xxxxxxxxxx; security-basics@xxxxxxxxxxxxxx

Subject: Re: Threat vector of running a service using a domain account

If a server does cache these credtonals then these can be attacked

independant of the AD and its underlying security controls.

If a service uses domain credential, do those credentials get cached?
I thought only interactive logon credentials are cached.

saqib

<http://security-basics.blogspot.com/>