

# Forum:[Hack Forums](#)

Thread: [Another windows 7 authentication bypass Exploit](#)

**mudasir007** - November 18, 2013, 8:50 am

The credit for this awesome Exploit goes to Mubix. The prerequisites for this exploit are intel 64 bit CPU and fully patched installation 64 bit windows 7 including a guest account on the machine.

## How to Exploit

The Exploit comes with a proof of the concept POC.Exe. Simply you have to attach the sysret.exe to some process like cmd.exe or Explorer.exe and once sysret is attached to the process you have full system rights.

1. Create a Guest account in windows 7
2. Open Cmd and type whoami You will get response user/guest
3. Place the Exploit ie sysret.exe in your C:\ Drive or in any folder like Public folder
4. Open up cmd and type task list notice the PID of explorer.exe process eg PID=4572
5. Now attach Sysret to Explorer.exe by command Sysret -PID 4572
6. Now you have full Administrative rights on system
7. Enjoy

## How It Works

I am a Noob don't know how it works .Sysret exploit escalates your user permissions (essentially bypassing UAC) on a 64bit Windows 7 (fully patched) machine. This exploit works on 64bit Intel Chips, including Windows and Linux.

## Conclusion

All Praise goes to Exploit coder The Exploit helped me esclate from guest to admin The Exploit can be downloaded at <http://packetstormsecurity.org/files/115908/sysret.rar>  
<http://www.exploit-db.com/sploits/20861.rar> and <https://github.com/shjalayeri/sysret??>

**ghostkilla112** - November 18, 2013, 8:51 am

Thanks i was looking for this, I want to use on school !

**mudasir007** - November 18, 2013, 8:53 am

(Nov 18, 2013 09:51 AM)ghostkilla112 Wrote: [CITE](#) Thanks i was looking for this, I want to use on school !the previous exploit that i posted is even more easy

**kift11** - November 18, 2013, 9:35 am

Cool man ....screams high quality. Nice share.

**mudasir007** - November 18, 2013, 9:39 am

(Nov 18, 2013 10:36 AM)- Sam - Wrote: [\[CITE\]](#) Sorry, this isn't allowed on HF. It's strictly forbidden.i don't know it brother are you suggesting that i shouldn't post about exploits

**mudasir007** - November 18, 2013, 9:46 am

(Nov 18, 2013 10:41 AM)- Sam - Wrote: [\[CITE\]](#) Serials and software cracks are not allowed.this is just a publically available and known Exploit i think it is fine to post about these if Hackforum permits

**XRAFFY** - November 14, 2014, 10:35 am

I'm interested to exploit for windows 7

**anil\_ak** - November 22, 2014, 8:26 pm

Thnxx for such nice tutorial, lukiing for such another threads by u,