

How to get the owner of a process?

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.platformsdk.security/2005-06/0160.html>

From: Sudhakar Govindavajhala (sudhakarg79_re_move_me_at_hotmail.com)

Date: 06/15/05

Date: Wed, 15 Jun 2005 01:44:02 -0700

Hi there,

I am having trouble in finding out who the owner of a process is, orogrammatically. Can someone help? I am admin of the machine and I am running with debug privilege enabled. I am not able to open the process token for me to query it.

This is my code:

```
int main(int argc, char **argv )
{
    if( argc != 2 ) {
        cerr << " usage: " << argv[0] << " <pid> " << endl;
        exit(1);
    }

    DWORD pid = atoi(argv[1]);

    HANDLE currentProcessToken = NULL ;

    if (!OpenProcessToken(GetCurrentProcess(),
        TOKEN_ADJUST_PRIVILEGES,
        &currentProcessToken ))
    {
        fprintf(stderr,"Failed OpenProcessToken\n");
        return FALSE;
    }

    BOOL ret = _SetPrivilege(currentProcessToken, "SeDebugPrivilege",
        TRUE);

    if ( ret != TRUE ) {
        cerr << "setpriv failure in getting DebugPrivilege \n";
        CloseHandle(currentProcessToken);
    }
}
```

microsoft.public.platformsdk.security: How to get the owner of a process?

```
    return FALSE;
}

HANDLE process = OpenProcess(PROCESS_ALL_ACCESS|PROCESS_QUERY_INFORMATION,
    FALSE, // Do not inheric handle
    pid);

if ( process == NULL ) {
    cerr << "OpemProcess failed\n";
    exit(1);
}

cout << "Open Process works.. \n";

HANDLE processToken = NULL;

if ( OpenProcessToken(process, TOKEN_QUERY,
    &processToken) == 0 ) {

    cerr << "OpenProcessToken failed";
    exit(1);

}

cout << "openprocesstoken works \n" ;

}
```

It works for lsass.exe. But it fails for alg.exe owned by NT Auth\Local service. I get access denied error for alg.exe

thanks,
Sudhakar.

Can anyone guide me as to whats going on?

thanks,
Sudhakar.