Search or type a command

Activity

Chat

Teams

Calendar

Shifts

Calls

Files

Apps

Help

DL **Ladouceur, David** Chat Files Organization Activity +

Ladouceur, David 6/10 8:32 AM
Hi James

6/10 8:33 AM
Hello, are you my security savior?

Ladouceur, David 6/10 8:34 AM
Haha, I am sort of. I just wanted to let you know that we are looking into a possible infection on your system

6/10 8:34 AM
nope, that was me, I did it

have a look around, i know what I did and can explain it to you

Ladouceur, David 6/10 8:35 AM
OK, can I ask why?

6/10 8:38 AM
I ran a penetration test because I was bored in the evening and wanted to see what the results would be, I didn't think it would trip any alarms, here''s the script I ran: https://github.com/carlospolop/privilege-escalation-awesome-scripts-suite/tree/master/winPEAS/winPEASbat (https://github.com/carlospolop/privilege-escalation-awesome-scripts-suite/tree/master/winPEAS/winPEASbat) I inspected before running and it's just a bunch of registry queires and a file search

carlospolop/privilege-escalati...
PEASS - Privilege Escalation Awesome

Ladouceur, David 6/10 8:39 AM
OK, let me look into a few things and get back to you.

thanks for explaining

Type a new message

Search or type a command

Activity

Chat

Teams

Calendar

Shifts

Calls

Files

Apps

Help

DL **Ladouceur, David** Chat Files Organization Activity +

REASS - Privilege Escalation Awesome

DL Ladouceur, David 6/10 8:39 AM
OK, let me look into a few things and get back to you.

thanks for explaining

6/10 8:40 AM
I ran a windows defender scan last night and no results were returned, my threat db was updated yesterday evening as well

6/10 8:49 AM
Hi David, one more thing that might help you track down what might have happened.
I crafted a Ntuser.man file with the goal of turning off UAS for a hot minute to remove some admin made shortcut icons from my desktop and to install visual studio 2019.
This method didn't work and I removed the file after words but

here's an article that goes over this method: https://medium.com/tenable-techblog/bypass-windows-10-user-group-policy-and-more-with-this-one-weird-trick-552d4bc5cc1b (https://medium.com/tenable-techblog/bypass-windows-10-user-group-policy-and-more-with-this-one-weird-trick-552d4bc5cc1b)

Bypass Windows 10 User Grou... ×
I'm going to share an (ab)use of a

I think adding a blank ntuser.man file to every users profile folder would mitigate this

6/10 9:56 AM
out of curiosity, and if you are allowed to tell me, what's the process for checking this out?

DL Ladouceur, David 6/10 9:57 AM 👍 1
We are basically just reviewing logs and waiting on bosses to tell us what to do. More waiting than anything.

June 11, 2020

Type a new message

Search or type a command

Activity

Chat

Teams

Calendar

Shifts

Calls

Files

Apps

Help

DL **Ladouceur, David** Chat Files Organization Activity +

6/10 9:56 AM
out of curiosity, and if you are allowed to tell me, what's the

DL Ladouceur, David 6/10 9:57 AM 👍 1
We are basically just reviewing logs and waiting on bosses to tell us what to do. More waiting than anything.

June 11, 2020

6/11 8:10 AM
Hi David, I stalked you on linked in and saw you worked at Data Innovations

DL Ladouceur, David 6/11 8:10 AM
Sure did

6/11 8:11 AM
I grew up with him

DL Ladouceur, David 6/11 8:11 AM 👍 1
nice, didn't know him long but he was one of the good devs

6/11 2:56 PM
Hi David, what are the chances that I'll be able to connect my

DL Ladouceur, David 6/11 2:57 PM
Hi, I'm not really sure I don't really have anything to do with

6/11 2:58 PM
who should I contact that would have more information?

DL Ladouceur, David 6/11 2:59 PM
The CISO Scott Carbee or Kevin Viani

Type a new message

Search or type a command

Activity

Chat

Teams

Calendar

Shifts

Calls

Files

Apps

Help

DL **Ladouceur, David** Chat Files Organization Activity +

DL Sure did

6/11 8:11 AM
I grew up with him

DL Ladouceur, David 6/11 8:11 AM 👍 1
nice, didn't know him long but he was one of the good devs

6/11 2:56 PM
Hi David, what are the chances that I'll be able to connect my

DL Ladouceur, David 6/11 2:57 PM
Hi, I'm not really sure I don't really have anything to do with

6/11 2:58 PM
who should I contact that would have more information?

DL Ladouceur, David 6/11 2:59 PM
The CISO Scott Carbee or Kevin Viani

6/11 2:59 PM
I'll start with Kevin, thank you

DL Ladouceur, David 6/11 2:59 PM 👍 1
Kevin is the AOE IT Director

Good luck sorry I can't be more help

6/11 2:59 PM Edited
no worries man, you've done all you can, thank you so much

DL Ladouceur, David 6/11 3:00 PM
Anytime

Type a new message