

Forum:[Hack Forums](#)

Thread: [In-Depth RAT creation tutorial + TCP/IP Stack Explanation + UDP Explanation](#)

blake.hale - June 20, 2014, 9:43 pm

Hello!

My name is blake and I am currently doing my CCNA.

I have come here and looked over topics for a while that have helped me understand crypters.

So I thought to give back, I would release a PDF tutorial on how to create a RAT in visual basic using the UDP protocol.

This tutorial contains the following information:How to create a RAT

Explanation of how UDP works

TCP/IP Stack explanation

9 Pages of information

Have fun reading! If you spot any errors, please feel free to let me know as I would like to make this information as accurate as possible!

Download Link (Cause where is the attach button?)

<https://www.mediafire.com/?j1e14ab1hol1ns9>

--Blake

SIM-1676753 - June 21, 2014, 12:24 am

(Jun 21, 2014 12:20 AM)Lord Pankake Wrote: [\[CITE\]](#) Opened the link, viewed the PDF and Malwarebytes shat itself. I looked at the "PDF" and it prompted me multiple times to install the latest flash player.

Reported.

Opened fine on the website for me. Download an update straight from Adobe.

Sam Winchester - June 21, 2014, 12:27 am

It's his 1st post. I ain't downloading that before someone can verify if it's clean or not.

SIM-1676753 - June 21, 2014, 12:28 am

(Jun 21, 2014 12:25 AM)Lord Pankake Wrote: [\[CITE\]](#) That's not my main concern. The problem is how much MBAM shat itself. PDF files don't do that. And since when have PDF files needed flash? Seriously?

What browser are you using? Chrome has a built in PDF plug-in from Adobe.

Goodies - June 21, 2014, 12:29 am

I'm curious, why on earth would you use UDP over TCP? I also have my CCNA and am doing CCNP. I would definitely use TCP or SCTP (use SCTP, it's rare enough to perhaps not be detected by some proto-based IDSes)

Zettabit - June 21, 2014, 12:30 am

I opened this, and it doesn't seem to be infected. @Pankake, it could be because of the content

explained in the PDF.

GenericSkid - June 21, 2014, 12:33 am

(Jun 21, 2014 12:24 AM)Mr. Trvp Wrote: [\[CITE\]](#) Opened fine on the website for me. Download an update straight from Adobe. (Jun 21, 2014 12:28 AM)Mr. Trvp Wrote: [\[CITE\]](#) What browser are you using? Chrome has a built in PDF plug-in from Adobe. (Jun 21, 2014 12:30 AM)Zettabit Wrote: [\[CITE\]](#) I opened this, and it doesn't seem to be infected. @Pankake, it could be because of the content explained in the PDF.

Nevermind. My computer's [\(I'm\)](#) just retarded. Excuse my tard-outburst.

(Jun 21, 2014 12:27 AM)Sam Winchester Wrote: [\[CITE\]](#) It's his 1st post. I ain't downloading that before someone can verify if it's clean or not.
I can vouch for the PDF's legitimacy.

SIM-1676753 - June 21, 2014, 12:37 am

(Jun 21, 2014 12:33 AM)Lord Pankake Wrote: [\[CITE\]](#) Nevermind. My computer's (I'm) just retarded. Excuse my tard-outburst, I can vouch for the PDF's legitimacy.
Just saw the prompt, it's an advertisement, lol.

(Jun 21, 2014 12:27 AM)Sam Winchester Wrote: [\[CITE\]](#) It's his 1st post. I ain't downloading that before someone can verify if it's clean or not.
I can also vouch for it's legitimacy.

MysticHacker - June 21, 2014, 12:38 am

(Jun 21, 2014 12:33 AM)Lord Pankake Wrote: [\[CITE\]](#) Nevermind. My computer's (I'm) just retarded. Excuse my tard-outburst, I can vouch for the PDF's legitimacy. I downloaded the pdf, nothing malicious there.

(Jun 21, 2014 12:29 AM)Goodies Wrote: [\[CITE\]](#) I'm curious, why on earth would you use UDP over TCP? I also have my CCNA and am doing CCNP. I would definitely use TCP or SCTP (use SCTP, it's rare enough to perhaps not be detected by some proto-based IDSes)
Correct. But at least he worked on this...

GenericSkid - June 21, 2014, 12:38 am

(Jun 21, 2014 12:37 AM)Mr. Trvp Wrote: [\[CITE\]](#) Just saw the prompt, it's an advertisement, lol. Chrome decided to turn off my adobe plugins... Never noticed since youtube's been using HTML recently. Again, pardon the tard-outburst. I overreacted due to a misconception.

blake.hale - June 21, 2014, 1:07 am

The reason I used UDP over TCP was simply to explain how to make a simple RAT.
I have made multiple RATs, and I would always use TCP.
But for teaching's sake, I used UDP because it's easy to write code for. I am going to write another PDF, which will be a continuation (built off this one) and will contain a TCP example.

EDIT: If you are worried about the PDF being infected

- 1) I can assure you it is not
- 2) I can post the ODT (Yes I use open office)

XeroNET - June 21, 2014, 5:26 am

This is a good start. Thanks for sharing!

h4kr! - June 21, 2014, 7:59 am

this is nice! thanks for sharing!

I've been looking into networking recently...

blake.hale - *June 21, 2014, 7:26 pm*

Thanks mate! This should be a good read for you to get started, then start to look into the OSI model and what each layer does.

?Opulence - *June 21, 2014, 7:38 pm*

great tut thanks OP! ill have to give it a try?

blake.hale - *June 21, 2014, 7:58 pm*

Sweet!

If you find any errors or recommendations drop a comment! :)

darkvas - *April 7, 2018, 3:45 pm*

thank you :) for the post,appreciated :)