Managing Risks in Enterprise VPNs: A Framework

MSc Research Project

MSc Top-Up Cybersecurity

Darragh Gavin

Student ID: 22157468

School of Computing

National College of Ireland

Supervisor: Ross Spelman

Link for VIVA

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name: Darragh Gavin……………………………………………………………………………………

Student ID: 22157468………………………………………………………………………………………..…

Programme: MSc Top-up CyberSecurity………………… **Year:** 2024………………..

Module: MSc Research Project……………………………………………………………………….……

Supervisor: Ross Spellman…………………………………………………………………………….………

Submission Due Date: August 12th …………………………………………………………………………….……

Project Title: Managing Risk in Enterprise VPNs: A Framework……………………….……

Word Count: ……………………… **Page Count**……10………………………………………….

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: Darragh Gavin……………………………………………………………………………………

Date: 11/08/24………………………………………………………………………………

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

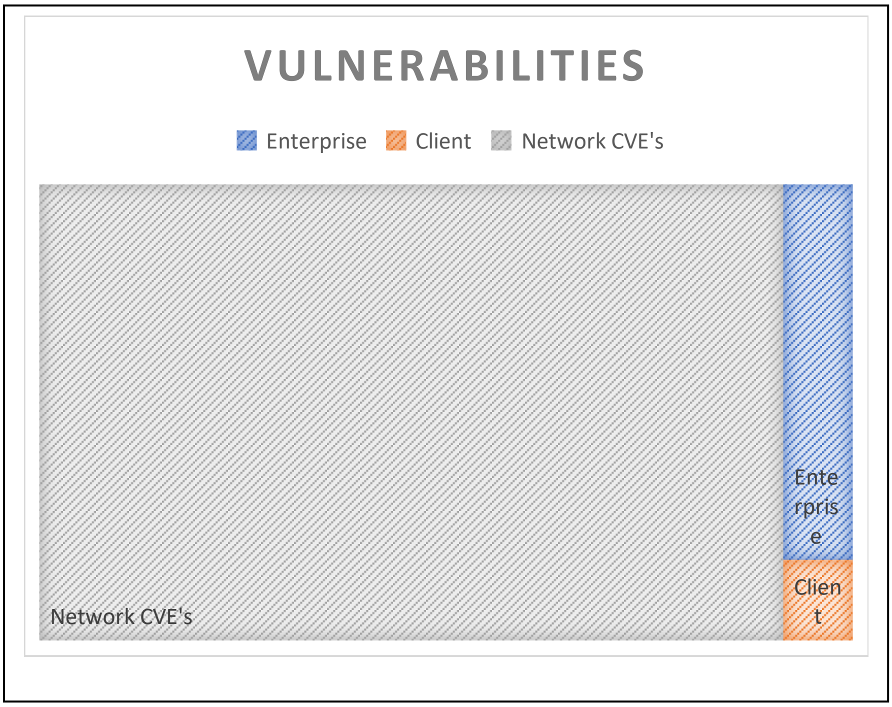
Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

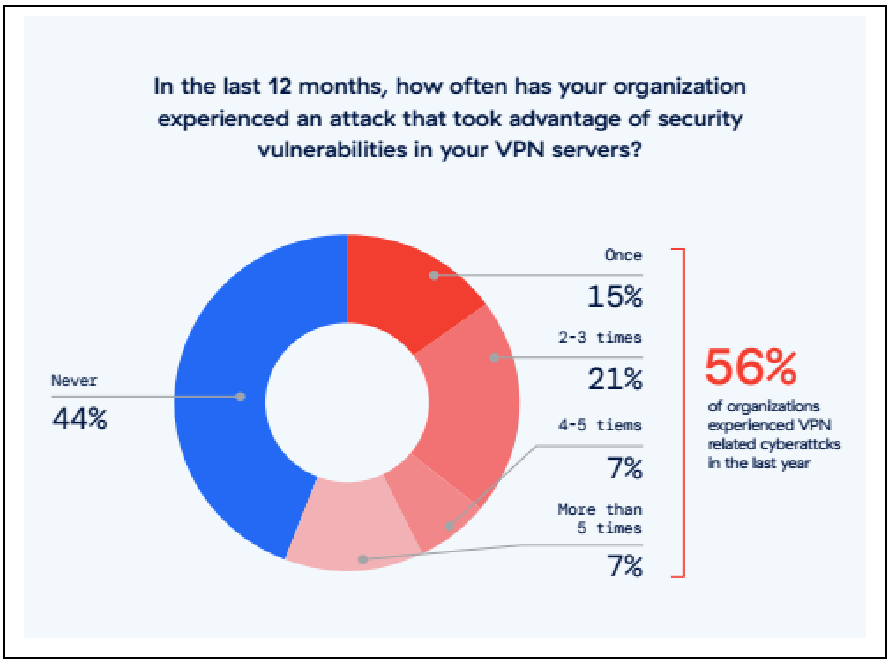
Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

VPN Security Framework

While accounting for only just over half a percent of total CVEs since 2020, VPN attacks have been some of the most damaging and are on the rise.



- 458 Enterprise CVE's, 98 Client-side CVE's, Total CVEs since 2020 – over 100,000
- Total network related CVEs since 2020 – over 6,000
- 93% of Organisations currently use a VPN (2023 stat) [1][2]
- 1/3 of global internet users (1.6 million) users with VPN
- 56% with 1 attack. 35% with 2+ attacks

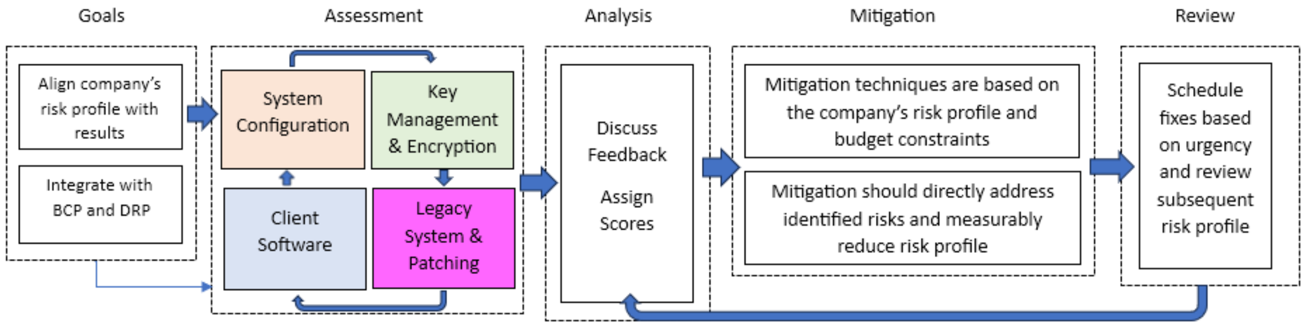


CVE's Year on Year

Below charts the increase in vulnerabilities found in VPN software (via CVEs). We can see that client-side vulnerabilities found have been increasing (with 20 already in 2024). While this doesn't necessarily correlate to an increase in attacks, it does show that there is an appetite there for attacking VPN client software. This coupled with industry reports and ongoing high-profile attacks (Ivanti, AnyConnect, etc), shows that this is definitely an area worth consideration.

	Total	2024	2023	2022	2021	2020
Client-side CVE's	98	20	26	8	23	21
Total CVE's	458	39	127	98	89	105

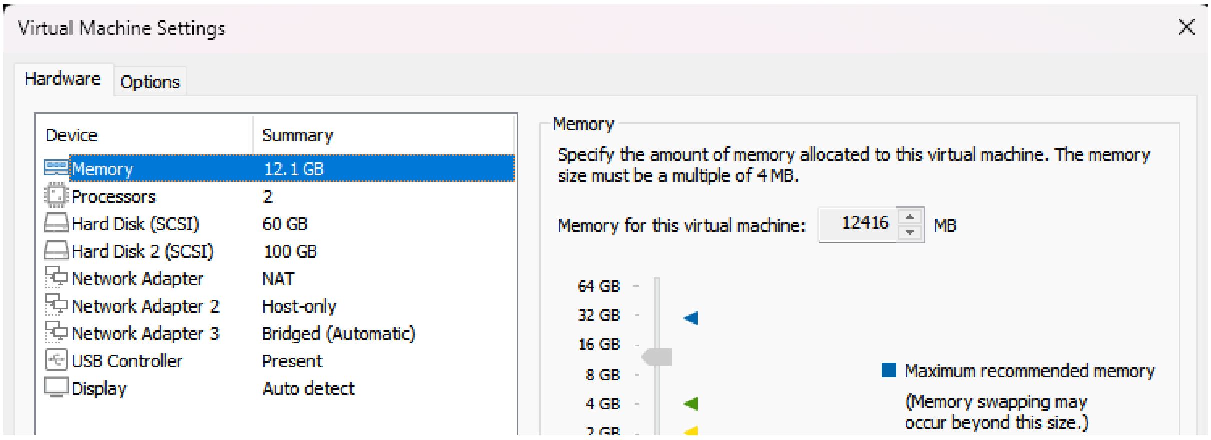
Framework Stages


Goals
Assessment
Analysis
Mitigation
Review
Align company's risk profile with results
Integrate with BCP and DRP
System Configuration
Key Management & Encryption
Client Software
Legacy System & Patching
Discuss Feedback
Assign Scores
Mitigation techniques are based on the company's risk profile and budget constraints
Mitigation should directly address identified risks and measurably reduce risk profile
Schedule fixes based on urgency and review subsequent risk profile

Lab Environment

VM-WARE

- 8Gb RAM allocation and 60Gb HD recommended. Only 2 cores needed. NAT was available but not used.



Device	Summary
Memory	12.1 GB
Processors	2
Hard Disk (SCSI)	60 GB
Hard Disk 2 (SCSI)	100 GB
Network Adapter	NAT
Network Adapter 2	Host-only
Network Adapter 3	Bridged (Automatic)
USB Controller	Present
Display	Auto detect

Memory

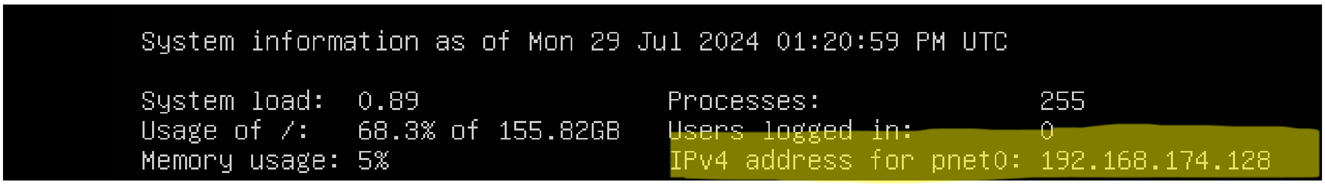
Specify the amount of memory allocated to this virtual machine. The memory size must be a multiple of 4 MB.

Memory for this virtual machine: 12416 MB

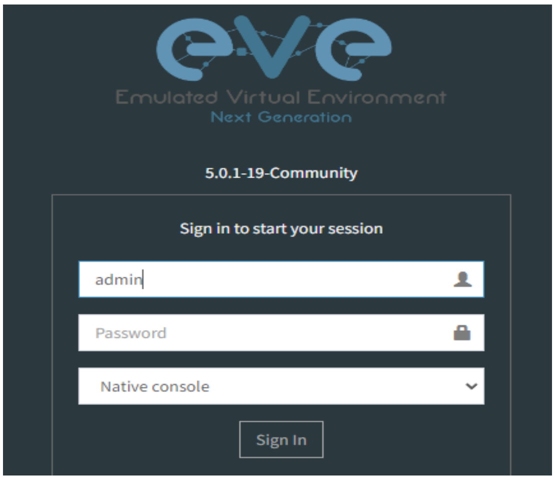
■ Maximum recommended memory
(Memory swapping may occur beyond this size.)

Eve-NG

- Eve-NG is a simple install, and for this lab doesn't require a NAT'ed network adaptor.
- Analysis software should be included in the Eve-NG install, such as WireShark etc.
- Once started in you Virtual Machine, it will give the local address for logging in



```
  System information as of Mon 29 Jul 2024 01:20:59 PM UTC

  System load:  0.89               Processes:             255
  Usage of /:   68.3% of 155.82GB  Users logged in:       0
  Memory usage: 5%                 IPv4 address for pnet0: 192.168.174.128
```



5.0.1-19-Community

Sign in to start your session

admin

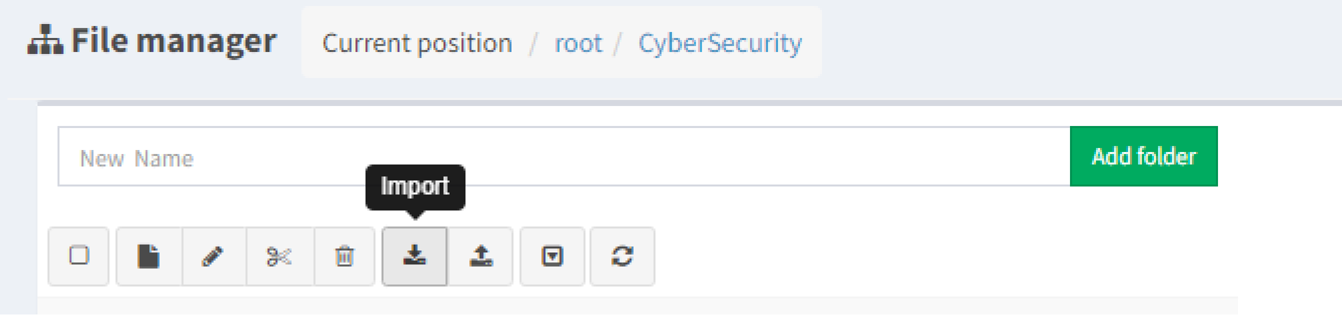
This is the login screen after you navigate to the localhost address provided. The generic credentials are:

- admin
- eve
- native console

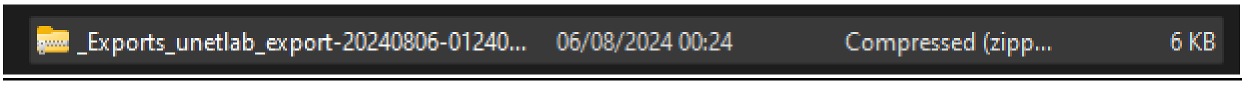
This should open to the main page to allow for the import

How to Import the Lab & OS (discussed in VIVA)

- Once logged in, you can click the import button and choose the labs provided
- The shell of the lab will open as shown in the diagrams but without the Operating Systems
- The OS for each device will be listed and needs to be available in Eve-NG for the devices to boot.
- All config files for devices are provided as part of the uploaded files.

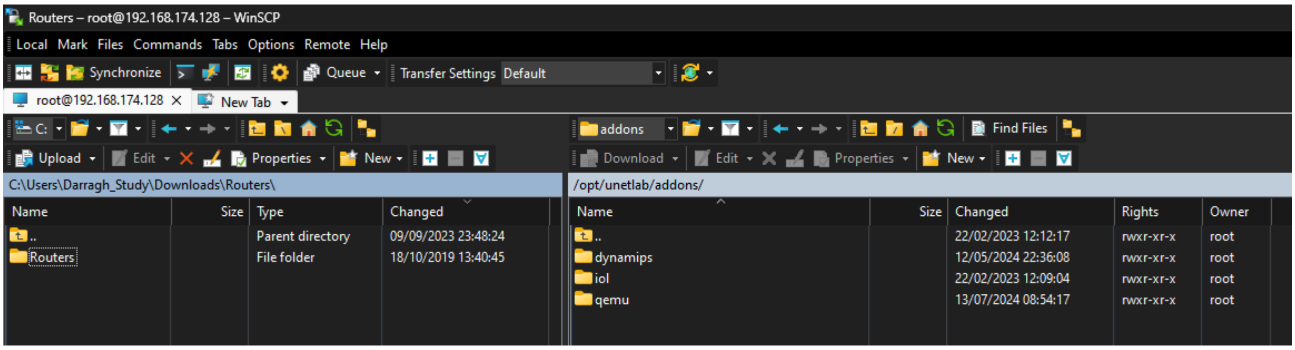


- The files should not be un-zipped before importing



_Exports_unetlab_export-20240806-01240... 06/08/2024 00:24 Compressed (zipp... 6 KB

WINSCP (Uploading OS files)


Routers – root@192.168.174.128 – WinSCP
Local Mark Files Commands Tabs Options Remote Help
Synchronize
Queue
Transfer Settings Default
root@192.168.174.128
New Tab
C:
addons
Find Files
Upload
Edit
Properties
New
Download
Edit
Properties
New

C:\Users\Darragh_Study\Downloads\Routers\

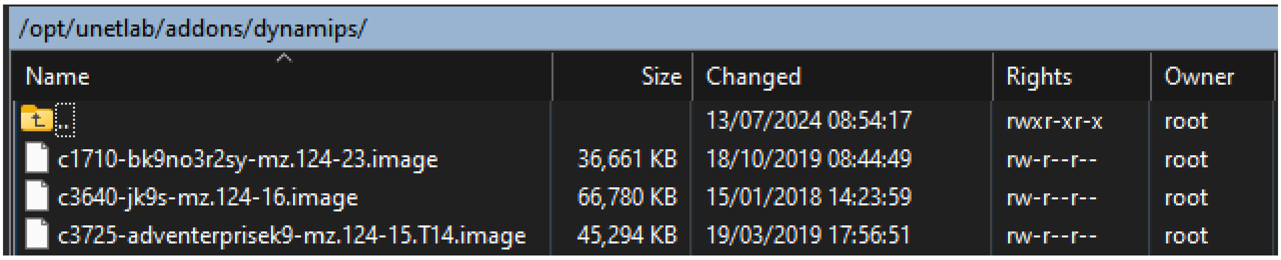
Name	Size	Type	Changed
..		Parent directory	09/09/2023 23:48:24
Routers		File folder	18/10/2019 13:40:45

/opt/unetlab/addons/

Name	Size	Changed	Rights	Owner
..		22/02/2023 12:12:17	rwxr-xr-x	root
dynamips		12/05/2024 22:36:08	rwxr-xr-x	root
iol		22/02/2023 12:09:04	rwxr-xr-x	root
qemu		13/07/2024 08:54:17	rwxr-xr-x	root

- The majority of files used by Eve-NG are in the .qcow2 format, and saved in the “qemu” folder

Naming Convention



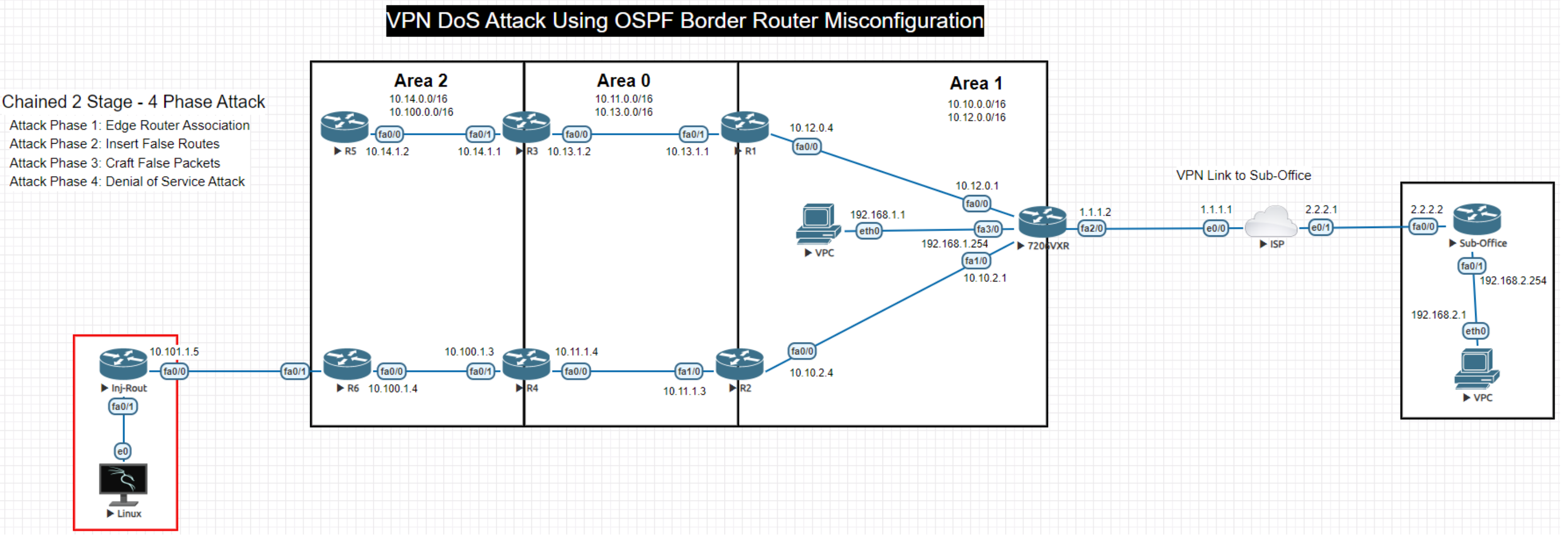
/opt/unetlab/addons/dynamips/

Name	Size	Changed	Rights	Owner
..		13/07/2024 08:54:17	rwxr-xr-x	root
c1710-bk9no3r2sy-mz.124-23.image	36,661 KB	18/10/2019 08:44:49	rw-r--r--	root
c3640-jk9s-mz.124-16.image	66,780 KB	15/01/2018 14:23:59	rw-r--r--	root
c3725-adventerprisek9-mz.124-15.T14.image	45,294 KB	19/03/2019 17:56:51	rw-r--r--	root

- The folder structure (as above) and file names must be correct for Eve-NG to recognise the OS
- There must be an initial descriptor and then a hyphen (“-“). The format is outlined in an attachment.

Lab 1 Diagram

- Lab 1 is the environment for the attack that essentially ended IKEv1's viability, the DoS attack.
- This attack had 4 phases - shown below with mitigation steps. All configuration files are included with the submission



VPN Config

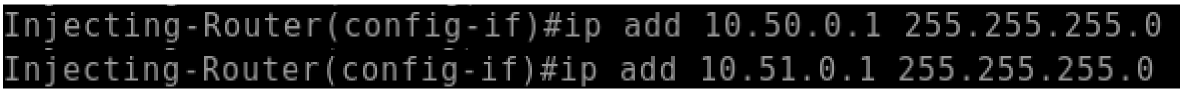
The config below outlines another issue with IKEv1 – it's lack of compatibility with stronger encryptions

- crypto isakmp policy 5 [encr 3des | authentication pre-share | group 2]
- crypto isakmp key choice15 address 2.2.2.2
- crypto ipsec transform-set TRANset1 esp-aes esp-md5-hmac
- crypto map MAP 10 ipsec-isakmp [set peer 2.2.2.2 | set transform-set TRANset1 | match address GWVPN]

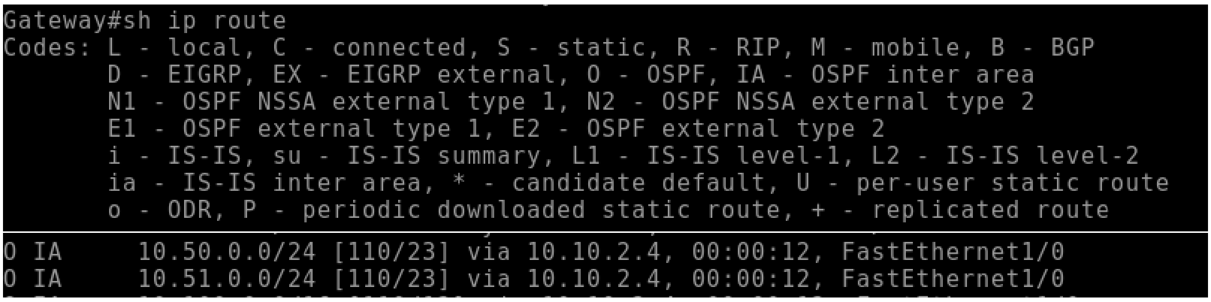
Attacking Machine Tools

- Kali Linux was used. Though any linux OS would work, Kali comes with many tools pre-installed
- Wireshark was used to both monitor the attack and provide data for Scapy
- Scapy is a Python based networking tool that was used to capture, understand, and create packets for the attack

Route Poisoning



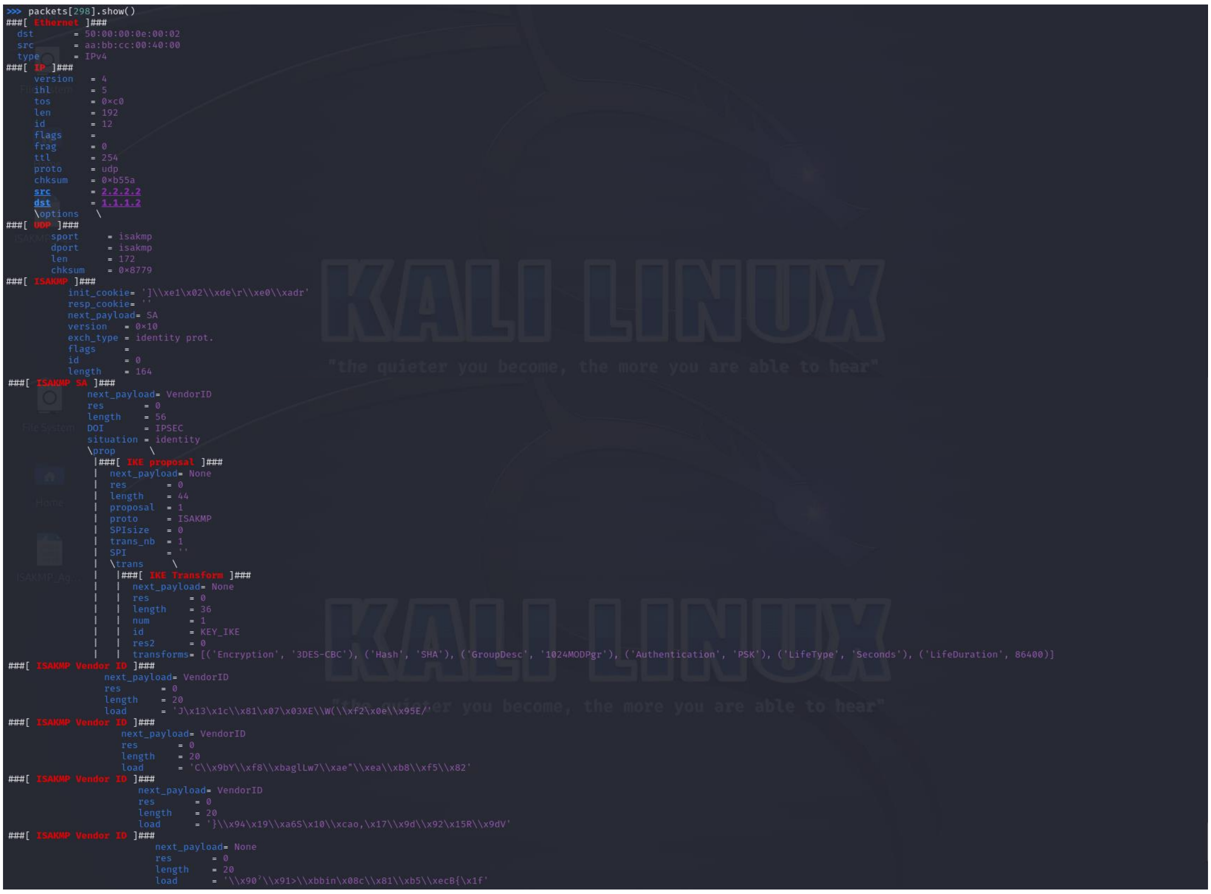
```
Injecting-Router(config-if)#ip add 10.50.0.1 255.255.255.0
Injecting-Router(config-if)#ip add 10.51.0.1 255.255.255.0
```



```
Gateway#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route

O IA     10.50.0.0/24 [110/23] via 10.10.2.4, 00:00:12, FastEthernet1/0
O IA     10.51.0.0/24 [110/23] via 10.10.2.4, 00:00:12, FastEthernet1/0
```

Packet Creation (Scapy)

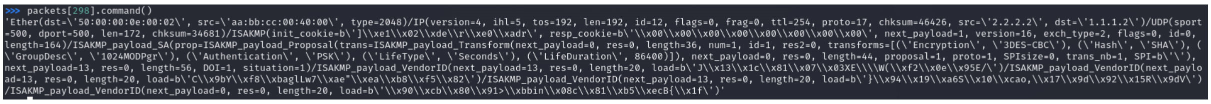
- Scapy allows for both packet capture as well as analysis. ISAKMP packets are quite complex.



```
>>> packets[298].show()
###[ Ethernet ]###
  dst       = 50:00:00:0e:00:02
  src       = aa:bb:cc:00:40:00
  type      = IPv4
###[ IP ]###
     version   = 4
     ihl       = 5
     tos       = 0×c0
     len       = 192
     id        = 12
     flags     = 
     frag      = 0
     ttl       = 254
     proto     = udp
     chksum    = 0×b55a
     src       = 2.2.2.2
     dst       = 1.1.1.2
     \options   \
###[ UDP ]###
        sport     = isakmp
        dport     = isakmp
        len       = 172
        chksum    = 0×8779
###[ ISAKMP ]###
           init_cookie= ']\\xe1\x02\\xde\r\\xe0\\xadr'
           resp_cookie= ''
           next_payload= SA
           version   = 0×10
           exch_type = identity prot.
           flags     = 
           id        = 0
           length    = 164
###[ ISAKMP SA ]###
              next_payload= VendorID
              res       = 0
              length    = 56
              DOI       = IPSEC
              situation = identity
              \prop      \
               |###[ IKE proposal ]###
               |  next_payload= None
               |  res       = 0
               |  length    = 44
               |  proposal  = 1
               |  proto     = ISAKMP
               |  SPIsize   = 0
               |  trans_nb  = 1
               |  SPI       = ''
               |  \trans     \
               |   |###[ IKE Transform ]###
               |   |  next_payload= None
               |   |  res       = 0
               |   |  length    = 36
               |   |  num       = 1
               |   |  id        = KEY_IKE
               |   |  res2      = 0
               |   |  transforms= [('Encryption', '3DES-CBC'), ('Hash', 'SHA'), ('GroupDesc', '1024MODPgr'), ('Authentication', 'PSK'), ('LifeType', 'Seconds'), ('LifeDuration', 86400)]
###[ ISAKMP Vendor ID ]###
                 next_payload= VendorID
                 res       = 0
                 length    = 20
                 load      = 'J\x13\x1c\\x81\x07\x03XE\\W(\\xf2\x0e\\x95E/'
###[ ISAKMP Vendor ID ]###
                    next_payload= VendorID
                    res       = 0
                    length    = 20
                    load      = 'C\\x9bY\\xf8\\xbaglLw7\\xae"\\xea\\xb8\\xf5\\x82'
###[ ISAKMP Vendor ID ]###
                       next_payload= VendorID
                       res       = 0
                       length    = 20
                       load      = '}\\x94\x19\\xa6S\x10\\xcao,\x17\\x9d\\x92\x15R\\x9dV'
###[ ISAKMP Vendor ID ]###
                          next_payload= None
                          res       = 0
                          length    = 20
                          load      = '\\x90'\\x91>\\xbbin\x08c\\x81\\xb5\\xecB{\x1f'
```

Packet Injection (Scapy)

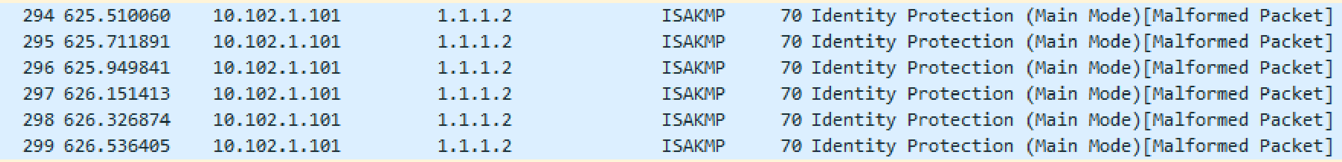
- Using the *command()* built-in, Scapy will allow us to recreate a given packet. The python build() function will also work.
- Packet[xx].command() *OR* Packet[xx].build()



```
>>> packets[298].command()
'Ether(dst=\'50:00:00:0e:00:02\', src=\'aa:bb:cc:00:40:00\', type=2048)/IP(version=4, ihl=5, tos=192, len=192, id=12, flags=0, frag=0, ttl=254, proto=17, chksum=46426, src=\'2.2.2.2\', dst=\'1.1.1.2\')/UDP(sport
=500, dport=500, len=172, chksum=34681)/ISAKMP(init_cookie=b\']\\xe1\\x02\\xde\\r\\xe0\\xadr\', resp_cookie=b\'\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\', next_payload=1, version=16, exch_type=2, flags=0, id=0,
length=164)/ISAKMP_payload_SA(prop=ISAKMP_payload_Proposal(trans=ISAKMP_payload_Transform(next_payload=0, res=0, length=36, num=1, id=1, res2=0, transforms=[(\'Encryption\', \'3DES-CBC\'), (\'Hash\', \'SHA\'), (
\'GroupDesc\', \'1024MODPgr\'), (\'Authentication\', \'PSK\'), (\'LifeType\', \'Seconds\'), (\'LifeDuration\', 86400)]), next_payload=0, res=0, length=44, proposal=1, proto=1, SPIsize=0, trans_nb=1, SPI=b\'\'),
next_payload=13, res=0, length=56, DOI=1, situation=1)/ISAKMP_payload_VendorID(next_payload=13, res=0, length=20, load=b\'J\\x13\\x1c\\x81\\x07\\x03XE\\\\W(\\xf2\\x0e\\x95E/\')/ISAKMP_payload_VendorID(next_paylo
ad=13, res=0, length=20, load=b\'C\\x9bY\\xf8\\xbaglLw7\\xae"\\xea\\xb8\\xf5\\x82\')/ISAKMP_payload_VendorID(next_payload=13, res=0, length=20, load=b\'}\\x94\\x19\\xa6S\\x10\\xcao,\\x17\\x9d\\x92\\x15R\\x9dV\')
/ISAKMP_payload_VendorID(next_payload=0, res=0, length=20, load=b\'\\x90\\xcb\\x80\\x91>\\xbbin\\x08c\\x81\\xb5\\xecB{\\x1f\')'
```

Packet Capture (WireShark)

- Flooding packets to the gateway router's VPN
- Given issues with the protocol layering, they showed as "malformed packets"

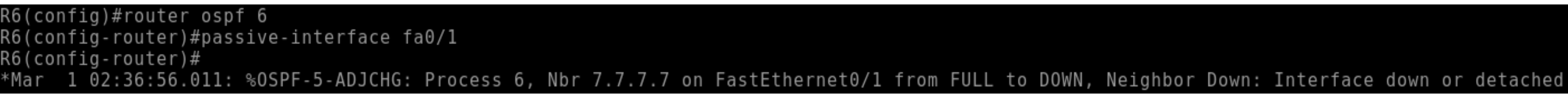


```
294 625.510060    10.102.1.101       1.1.1.2            ISAKMP     70 Identity Protection (Main Mode)[Malformed Packet]
295 625.711891    10.102.1.101       1.1.1.2            ISAKMP     70 Identity Protection (Main Mode)[Malformed Packet]
296 625.949841    10.102.1.101       1.1.1.2            ISAKMP     70 Identity Protection (Main Mode)[Malformed Packet]
297 626.151413    10.102.1.101       1.1.1.2            ISAKMP     70 Identity Protection (Main Mode)[Malformed Packet]
298 626.326874    10.102.1.101       1.1.1.2            ISAKMP     70 Identity Protection (Main Mode)[Malformed Packet]
299 626.536405    10.102.1.101       1.1.1.2            ISAKMP     70 Identity Protection (Main Mode)[Malformed Packet]
```

Mitigation

- The first step to securing against this issue is protecting the physical interface by making it passive.

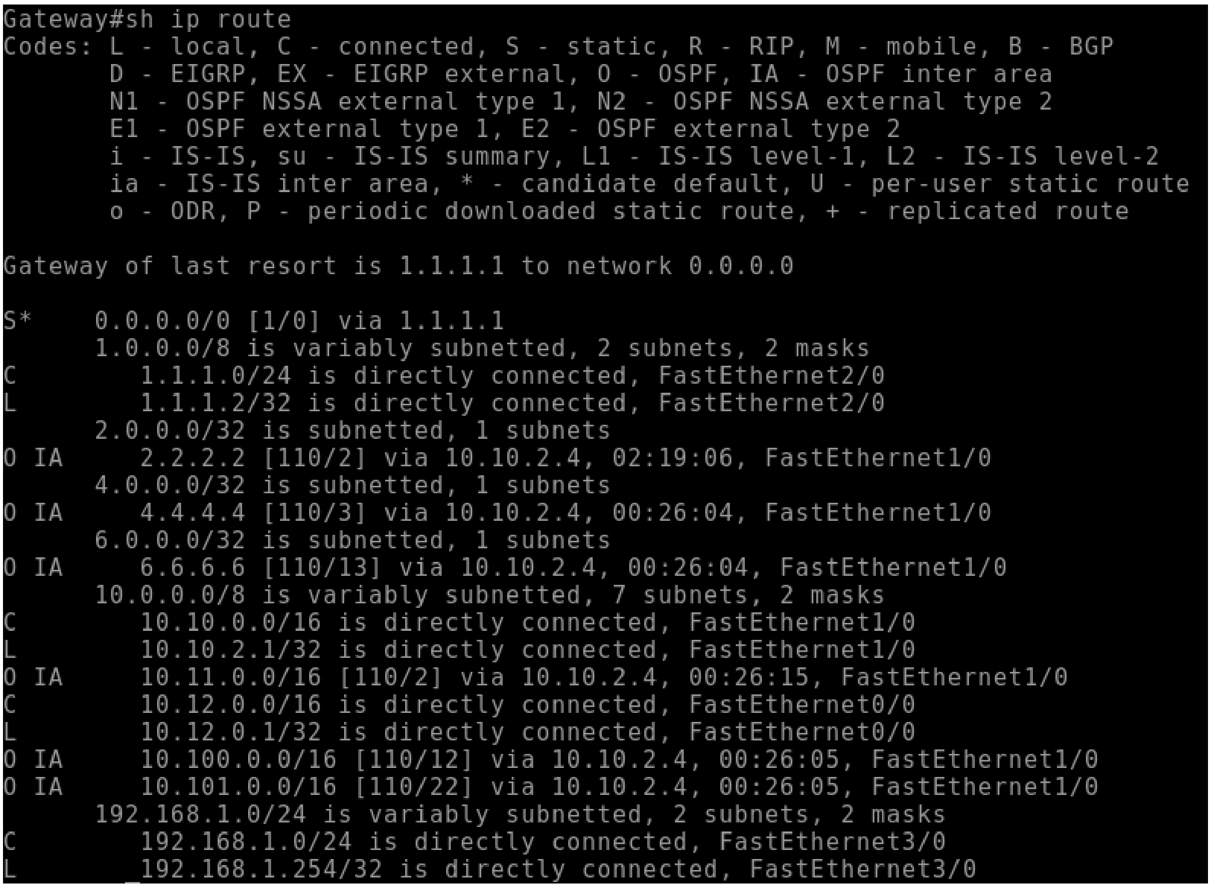
Edge Router (R6) - Passive



```
R6(config)#router ospf 6
R6(config-router)#passive-interface fa0/1
R6(config-router)#
*Mar  1 02:36:56.011: %OSPF-5-ADJCHG: Process 6, Nbr 7.7.7.7 on FastEthernet0/1 from FULL to DOWN, Neighbor Down: Interface down or detached
```

Route Table Updated

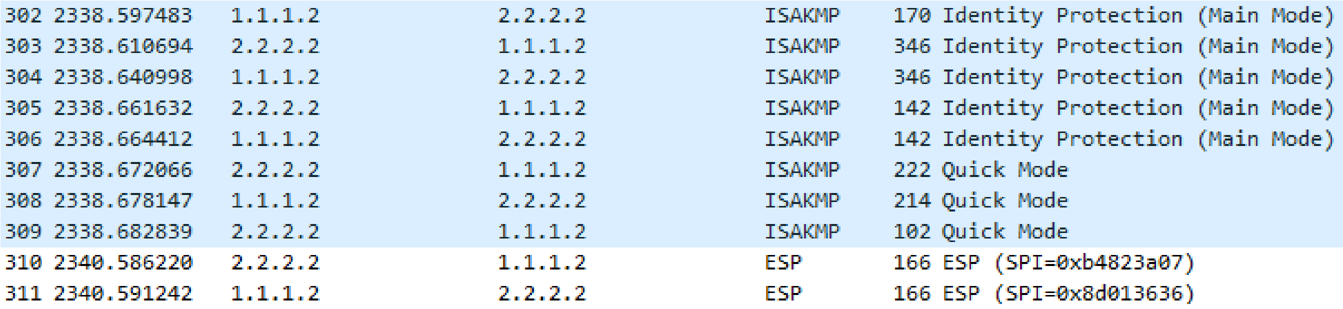
- Once this has been done, the route table will update quite quickly to remove the malicious routes.



```
Gateway#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route

Gateway of last resort is 1.1.1.1 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 1.1.1.1
      1.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        1.1.1.0/24 is directly connected, FastEthernet2/0
L        1.1.1.2/32 is directly connected, FastEthernet2/0
      2.0.0.0/32 is subnetted, 1 subnets
O IA     2.2.2.2 [110/2] via 10.10.2.4, 02:19:06, FastEthernet1/0
      4.0.0.0/32 is subnetted, 1 subnets
O IA     4.4.4.4 [110/3] via 10.10.2.4, 00:26:04, FastEthernet1/0
      6.0.0.0/32 is subnetted, 1 subnets
O IA     6.6.6.6 [110/13] via 10.10.2.4, 00:26:04, FastEthernet1/0
      10.0.0.0/8 is variably subnetted, 7 subnets, 2 masks
C        10.10.0.0/16 is directly connected, FastEthernet1/0
L        10.10.2.1/32 is directly connected, FastEthernet1/0
O IA     10.11.0.0/16 [110/2] via 10.10.2.4, 00:26:15, FastEthernet1/0
C        10.12.0.0/16 is directly connected, FastEthernet0/0
L        10.12.0.1/32 is directly connected, FastEthernet0/0
O IA     10.100.0.0/16 [110/12] via 10.10.2.4, 00:26:05, FastEthernet1/0
O IA     10.101.0.0/16 [110/22] via 10.10.2.4, 00:26:05, FastEthernet1/0
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, FastEthernet3/0
L        192.168.1.254/32 is directly connected, FastEthernet3/0
```

Results (Wireshark)

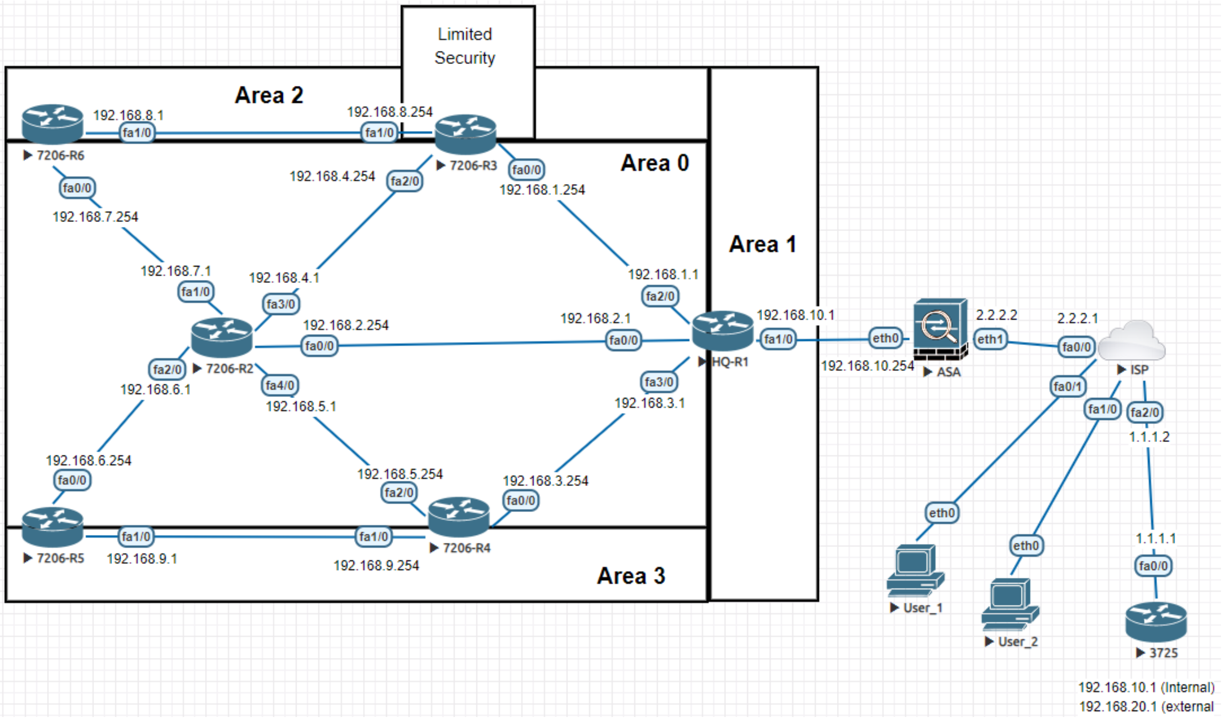
- We can see the tunnel has now formed and the last two packets are encrypted pings between the User_1/2 endpoints



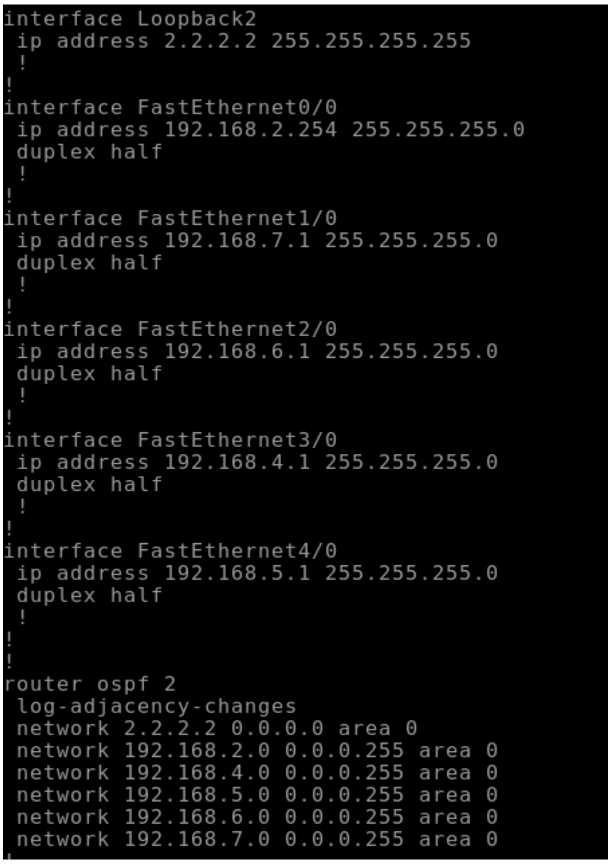
```
302 2338.597483   1.1.1.2            2.2.2.2            ISAKMP    170 Identity Protection (Main Mode)
303 2338.610694   2.2.2.2            1.1.1.2            ISAKMP    346 Identity Protection (Main Mode)
304 2338.640998   1.1.1.2            2.2.2.2            ISAKMP    346 Identity Protection (Main Mode)
305 2338.661632   2.2.2.2            1.1.1.2            ISAKMP    142 Identity Protection (Main Mode)
306 2338.664412   1.1.1.2            2.2.2.2            ISAKMP    142 Identity Protection (Main Mode)
307 2338.672066   2.2.2.2            1.1.1.2            ISAKMP    222 Quick Mode
308 2338.678147   1.1.1.2            2.2.2.2            ISAKMP    214 Quick Mode
309 2338.682839   2.2.2.2            1.1.1.2            ISAKMP    102 Quick Mode
310 2340.586220   2.2.2.2            1.1.1.2            ESP       166 ESP (SPI=0xb4823a07)
311 2340.591242   1.1.1.2            2.2.2.2            ESP       166 ESP (SPI=0x8d013636)
```

Lab 2 – Overview

This lab represents an enterprise environment with a site – site VPN, as well as VPN clients. There is redundancy in the network, but we can see one of the internal sites is potentially vulnerable. Also, the lack of proper segregation, with all points being able to freely communicate, means that User_1 can access everything.



Configuration



```
interface Loopback2
 ip address 2.2.2.2 255.255.255.255
 !
!
interface FastEthernet0/0
 ip address 192.168.2.254 255.255.255.0
 duplex half
 !
!
interface FastEthernet1/0
 ip address 192.168.7.1 255.255.255.0
 duplex half
 !
!
interface FastEthernet2/0
 ip address 192.168.6.1 255.255.255.0
 duplex half
 !
!
interface FastEthernet3/0
 ip address 192.168.4.1 255.255.255.0
 duplex half
 !
!
interface FastEthernet4/0
 ip address 192.168.5.1 255.255.255.0
 duplex half
 !
!
!
router ospf 2
 log-adjacency-changes
 network 2.2.2.2 0.0.0.0 area 0
 network 192.168.2.0 0.0.0.255 area 0
 network 192.168.4.0 0.0.0.255 area 0
 network 192.168.5.0 0.0.0.255 area 0
 network 192.168.6.0 0.0.0.255 area 0
 network 192.168.7.0 0.0.0.255 area 0
```

This is an excerpt of the config from R2 above, a central router. The config is minimal, covering the port configuration, OSPF configuration, and the loopback. All internal routers have a variation on this config.

The firewall has additional configuration to allow for the VPN to an external site. This was initially IKEv1, but upgraded to IKEv2 (shown below).

The config files are included with the uploaded documents.

Assessment Table

Assessment

A clear overview of each system with key security features outlined.

Risk Score (1-10)

- risk scores 1-3 means no obvious risk and no known CVE's
- risk scores 4-6 indicate known issues that aren't critical, i.e. an attack vector that can cause disruption but not a breach (DoS attacks etc)
- risk scores 7-9 indicates known issues that could result in a breach, or allow network access
- A risk score of 0 indicates a secure system that either cannot be accessed or has a multi-aspect MFA secured single point of access
- A risk score of 10 indicates a known, serious, vulnerability that requires immediate action

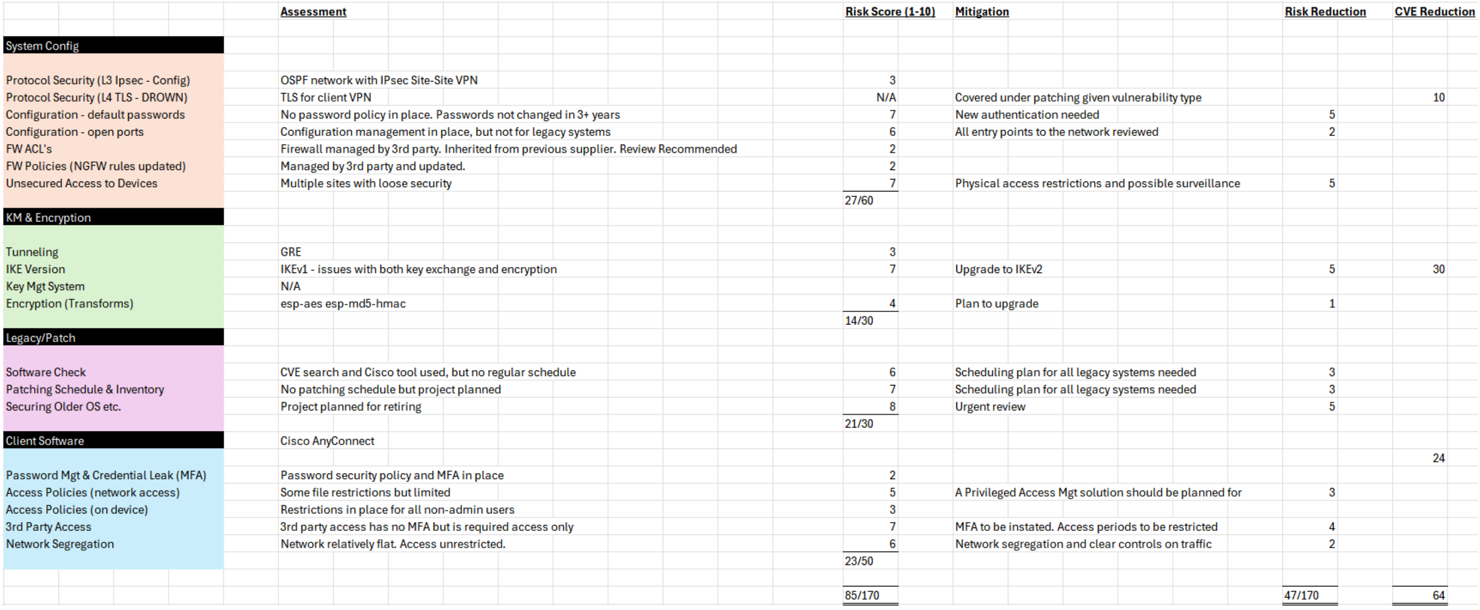
Mitigation

This should cover all steps necessary to bring issues in line with the organisation's risk policy.

CVE Reduction

- These can be found with a quick search on the CVE database site.
- Scores are given as a means of quantifying the threat reduction but, if anything, under-represent the benefits.
- Many attacks covered in this framework do not have a CVE and are not easily quantifiable, but are invaluable in securing systems

Framework Sample



	Assessment	**Risk Score (1-10)**	**Mitigation**	**Risk Reduction**	**CVE Reduction**
System Config					
Protocol Security (L3 Ipsec - Config)	OSPF network with IPsec Site-Site VPN	3			
Protocol Security (L4 TLS - DROWN)	TLS for client VPN	N/A	Covered under patching given vulnerability type		10
Configuration - default passwords	No password policy in place. Passwords not changed in 3+ years	7	New authentication needed	5	
Configuration - open ports	Configuration management in place, but not for legacy systems	6	All entry points to the network reviewed	2	
FW ACL's	Firewall managed by 3rd party. Inherited from previous supplier. Review Recommended	2			
FW Policies (NGFW rules updated)	Managed by 3rd party and updated.	2			
Unsecured Access to Devices	Multiple sites with loose security	7	Physical access restrictions and possible surveillance	5	
		27/60			
KM & Encryption					
Tunneling	GRE	3			
IKE Version	IKEv1 - issues with both key exchange and encryption	7	Upgrade to IKEv2	5	30
Key Mgt System	N/A				
Encryption (Transforms)	esp-aes esp-md5-hmac	4	Plan to upgrade	1	
		14/30			
Legacy/Patch					
Software Check	CVE search and Cisco tool used, but no regular schedule	6	Scheduling plan for all legacy systems needed	3	
Patching Schedule & Inventory	No patching schedule but project planned	7	Scheduling plan for all legacy systems needed	3	
Securing Older OS etc.	Project planned for retiring	8	Urgent review	5	
		21/30			
Client Software	Cisco AnyConnect				
					24
Password Mgt & Credential Leak (MFA)	Password security policy and MFA in place	2			
Access Policies (network access)	Some file restrictions but limited	5	A Privileged Access Mgt solution should be planned for	3	
Access Policies (on device)	Restrictions in place for all non-admin users	3			
3rd Party Access	3rd party access has no MFA but is required access only	7	MFA to be instated. Access periods to be restricted	4	
Network Segregation	Network relatively flat. Access unrestricted.	6	Network segregation and clear controls on traffic	2	
		23/50			
		85/170		47/170	64

Assessment

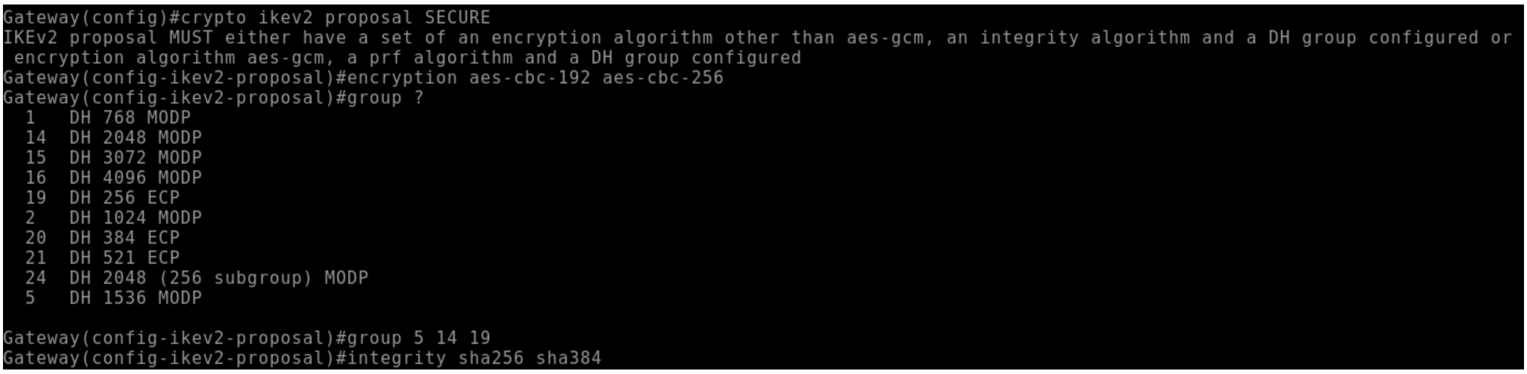
- The assessment process allows for three main risk brackets
- It outlines 4 categories, each will specific areas to be reviewed
- A risk score is assigned and then mitigation steps are presented for review with a risk reduction score to provide metrics for the current and subsequent

Mitigation Steps

- Passive Interface configuration for vulnerable routers
- Patching and updates – absolutely essential in vulnerability management
- IKE Upgrade – while attacks on IKEv1 are still limited, this significantly improves security
- Limiting Client Devices to Necessary Access – this is a push towards Zero Trust

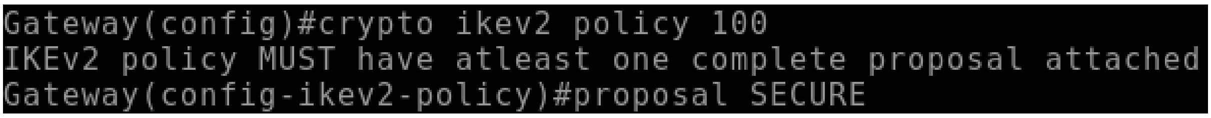
IKEv2

- Upgrading to IKEv2 allows for more secure DH groups to be used. As per Cisco's own guidelines [4], groups 1, 2, and 5 should not be used, though stronger encryption is not available with IKEv1.



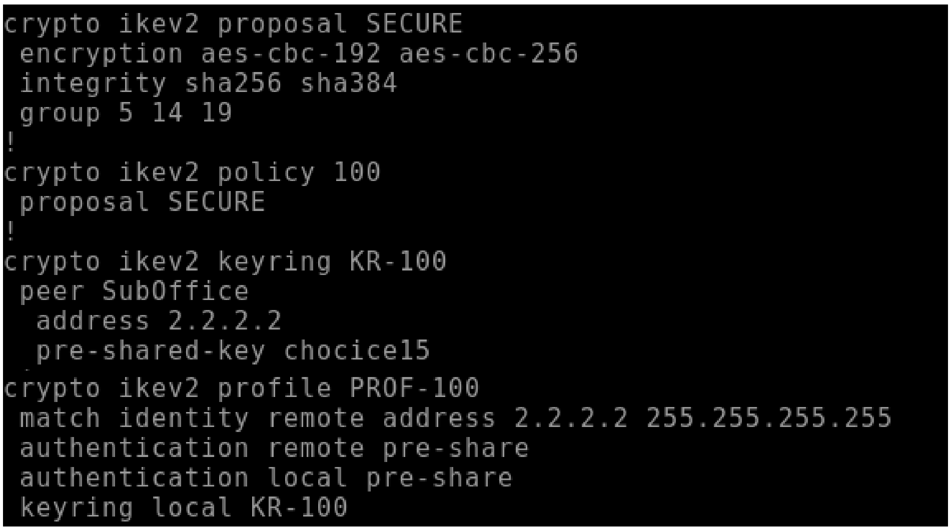
```
Gateway(config)#crypto ikev2 proposal SECURE
IKEv2 proposal MUST either have a set of an encryption algorithm other than aes-gcm, an integrity algorithm and a DH group configured or
 encryption algorithm aes-gcm, a prf algorithm and a DH group configured
Gateway(config-ikev2-proposal)#encryption aes-cbc-192 aes-cbc-256
Gateway(config-ikev2-proposal)#group ?
  1   DH 768 MODP
  14  DH 2048 MODP
  15  DH 3072 MODP
  16  DH 4096 MODP
  19  DH 256 ECP
  2   DH 1024 MODP
  20  DH 384 ECP
  21  DH 521 ECP
  24  DH 2048 (256 subgroup) MODP
  5   DH 1536 MODP

Gateway(config-ikev2-proposal)#group 5 14 19
Gateway(config-ikev2-proposal)#integrity sha256 sha384
```

- Encryption Upgrade – both Modulus and Elliptic Curve encryption is now available



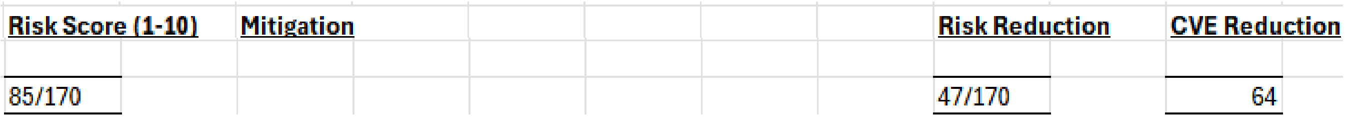
```
Gateway(config)#crypto ikev2 policy 100
IKEv2 policy MUST have atleast one complete proposal attached
Gateway(config-ikev2-policy)#proposal SECURE
```

- Negotiation of best security – IKEv2 allows multiple standards to be used and negotiates the most secure



```
crypto ikev2 proposal SECURE
 encryption aes-cbc-192 aes-cbc-256
 integrity sha256 sha384
 group 5 14 19
!
crypto ikev2 policy 100
 proposal SECURE
!
crypto ikev2 keyring KR-100
 peer SubOffice
  address 2.2.2.2
  pre-shared-key chocice15
crypto ikev2 profile PROF-100
 match identity remote address 2.2.2.2 255.255.255.255
 authentication remote pre-share
 authentication local pre-share
 keyring local KR-100
```

Scoring



Risk Score (1-10)	Mitigation	Risk Reduction	CVE Reduction
85/170		47/170	64

As shown above, the scoring is based on self-assessment, which is one area of this framework that would need reviewing. A more meticulous system for scoring would provide greater clarity, but may also prove overwhelming.

The initial assessment resulted in a score 85 (50%) which, while high, this doesn't provide any details of specific issues. In the example given, there are a number of higher scoring areas that would warrant attention. Most of these areas offer immediately implementable fixes, that would house any major financial burdens for the organisation save the Privileged Access Management system or network.

Results

- The assessment highlighted many basic issues with security policies and inventory which should force the organisation to institute procedures with a clearly defined schedule
- There were numerous mitigation steps proposed which resulted in a total 38 point (22%) reduction in risk. Many of these steps don't require a huge outlay of cash but would not have been found without a structured approach
- Areas secured include:
  -

CVE & Reduction (Table)

- The CVE values are pulled directly from the database to give an indication of how many vulnerabilities currently exist

Footnotes

*Added to the end of the document to avoid clutter

[1] https://dataprot.net/statistics/vpn-statistics/
[2] https://www.statista.com/statistics/1343692/worldwide-virtual-private-network-reasons-usage
[3] Zscaler ThreatLabz 2024 VPN Risk Report
[4] https://community.cisco.com/t5/security-knowledge-base/diffie-hellman-groups/ta-p/3147010