CND Final Exam

Rajat Vij

1. Can stack overflows be mitigated by having arrays grow upward instead of down into the return address / stack frame?

Ans 1. No, I don't think stack buffer overflow can be mitigated by having arrays grow upwards instead of down into the return address / stack frame as even if we are able to make a data structure with properties of dynamic array growing upwards to avoid overflow by doubling the size of array whenever the array is filled to the last element or goes out of bound because in case of infinite recursive functions the size will kept on increasing and there will be no memory left to allocate and it would be unjustified to have a dynamic array to mitigate overflows as we allocate appropriate amount of memory to stack keeping in mind about the priority and requirement of the program using the stack. So using dynamic array might allocate memory to a low priority process which in turn might block a high priority process.

[NOTE: I am assuming to use dynamic array instead of normal array as I feel a normal array will just give out of bound exceptions instead of stack overflows which is not that different from using stack]

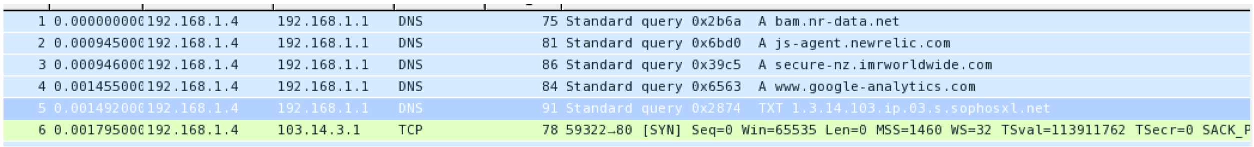
2. Explain in as much detail and demonstrate what happens when you navigate to www.radionz.co.nz in a web browser. Be verbose - this should take a page or more.

- You must include all tools and technologies that you used and determine at minimum:
- How does your machine communicate with other hosts on the local network? What protocols does it use and how do they work?
- How does your machine communicate outside of the local network?
- How does your local network (LAN) access the Internet?
- What IP is hosting the domain? How do you find this out? Who owns the domain and IP?
- What Autonomous Systems does your traffic pass through?
- Include all steps from your local network to the remote network.
- If you have local issues, you may use a Looking Glass server.

Ans 2. When we navigate to www.radionz.co.nz in a web browser following steps happen:

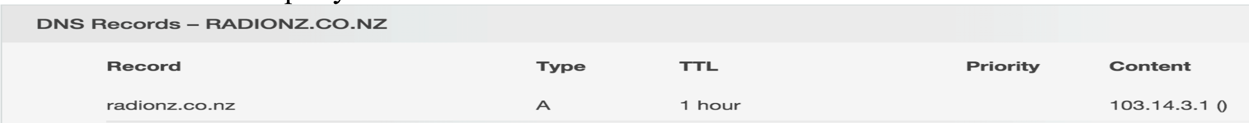
1. Multiple DNS Requests are made to resolve the site and the content on the web page. Ideally we should see a DNS request to www.radionz.co.nz but we can see multiple DNS request(to 198.168.1.1) on Wireshark which is probably because the content on

the page is coming from multiple sources and the DNS request is made for those multiple sources.



```
1 0.000000000 192.168.1.4    192.168.1.1    DNS        75 Standard query 0x2b6a  A bam.nr-data.net
2 0.000945000 192.168.1.4    192.168.1.1    DNS        81 Standard query 0x6bd0  A js-agent.newrelic.com
3 0.000946000 192.168.1.4    192.168.1.1    DNS        86 Standard query 0x39c5  A secure-nz.imrworldwide.com
4 0.001455000 192.168.1.4    192.168.1.1    DNS        84 Standard query 0x6563  A www.google-analytics.com
5 0.001492000 192.168.1.4    192.168.1.1    DNS        91 Standard query 0x2874  TXT 1.3.14.103.ip.03.s.sophosxl.net
6 0.001795000 192.168.1.4    103.14.3.1     TCP        78 59322→80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=113911762 TSecr=0 SACK_P
```

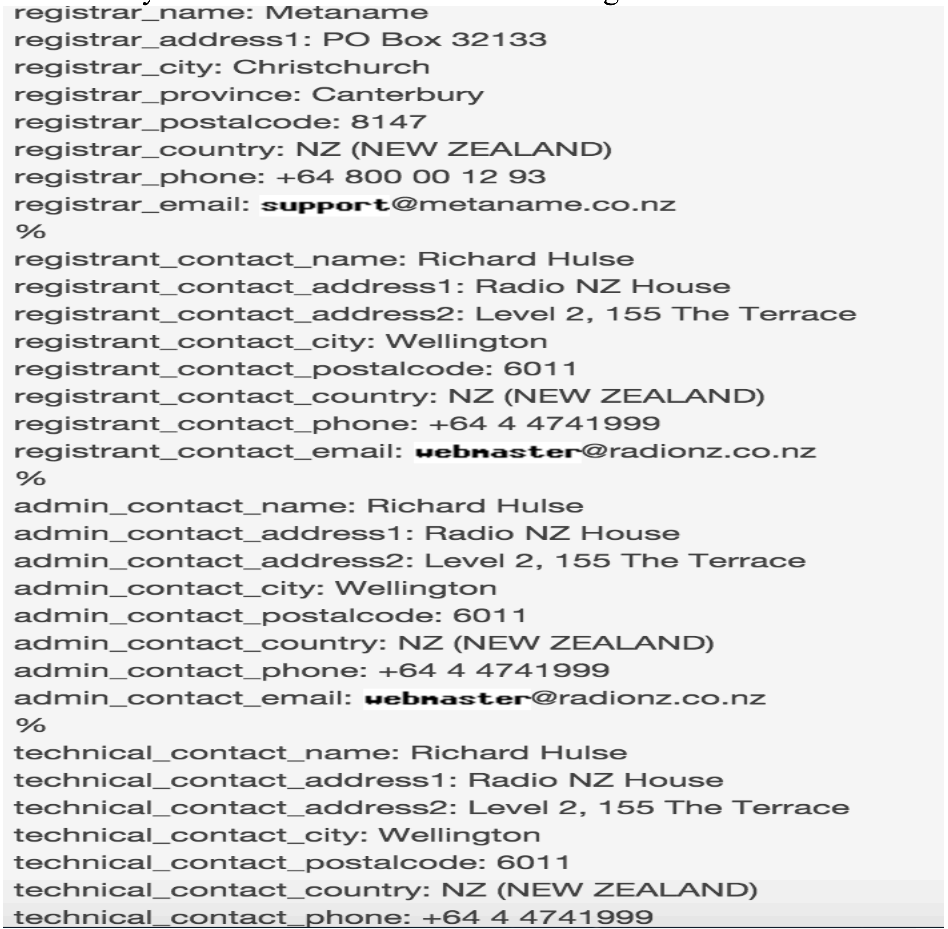
If we do a DNS resolution of the www.radionz.co.nz we can see that its ip address is 103.14.3.1, which is the 5th DNS query in above screenshot.



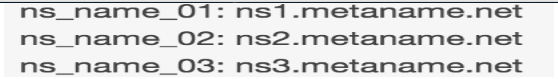
DNS Records – RADIONZ.CO.NZ

Record	Type	TTL	Priority	Content
radionz.co.nz	A	1 hour		103.14.3.1 ()

I found the IP address using https://who.is. From the registrar information we can see that the site is owned by Radio New Zealand with following contact information:

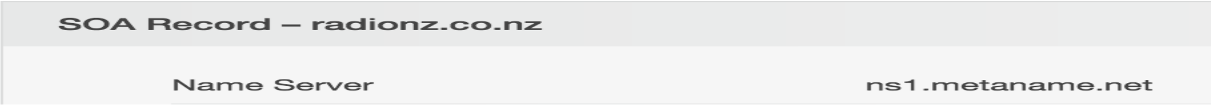


```
registrar_name: Metaname
registrar_address1: PO Box 32133
registrar_city: Christchurch
registrar_province: Canterbury
registrar_postalcode: 8147
registrar_country: NZ (NEW ZEALAND)
registrar_phone: +64 800 00 12 93
registrar_email: support@metaname.co.nz
%
registrant_contact_name: Richard Hulse
registrant_contact_address1: Radio NZ House
registrant_contact_address2: Level 2, 155 The Terrace
registrant_contact_city: Wellington
registrant_contact_postalcode: 6011
registrant_contact_country: NZ (NEW ZEALAND)
registrant_contact_phone: +64 4 4741999
registrant_contact_email: webmaster@radionz.co.nz
%
admin_contact_name: Richard Hulse
admin_contact_address1: Radio NZ House
admin_contact_address2: Level 2, 155 The Terrace
admin_contact_city: Wellington
admin_contact_postalcode: 6011
admin_contact_country: NZ (NEW ZEALAND)
admin_contact_phone: +64 4 4741999
admin_contact_email: webmaster@radionz.co.nz
%
technical_contact_name: Richard Hulse
technical_contact_address1: Radio NZ House
technical_contact_address2: Level 2, 155 The Terrace
technical_contact_city: Wellington
technical_contact_postalcode: 6011
technical_contact_country: NZ (NEW ZEALAND)
technical_contact_phone: +64 4 4741999
```



```
ns_name_01: ns1.metaname.net
ns_name_02: ns2.metaname.net
ns_name_03: ns3.metaname.net
```

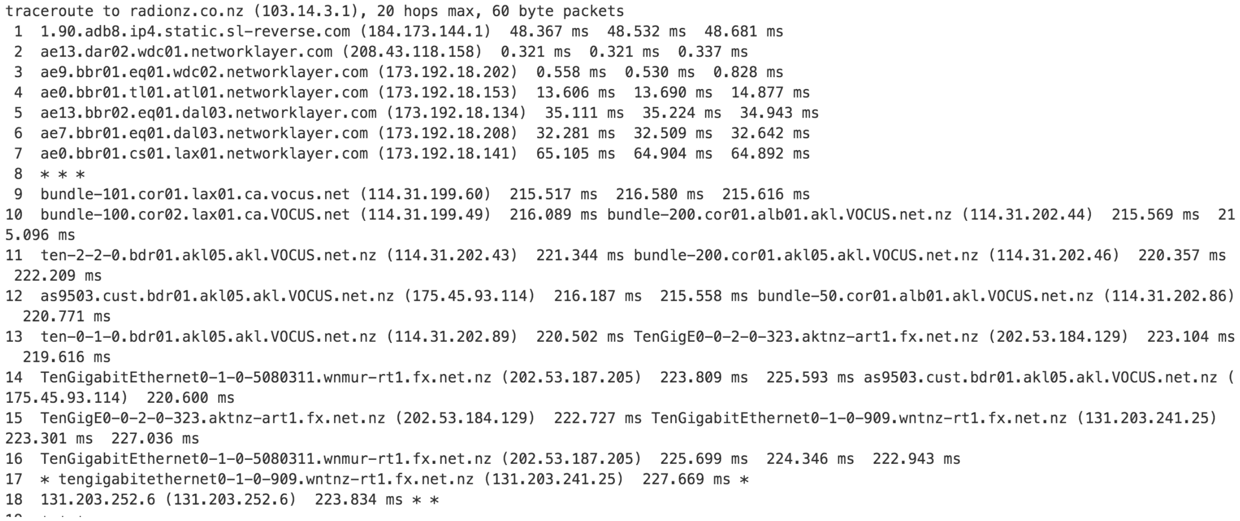
With following ns Records: of which my traffic passed through ns1.metaname.net



SOA Record – radionz.co.nz

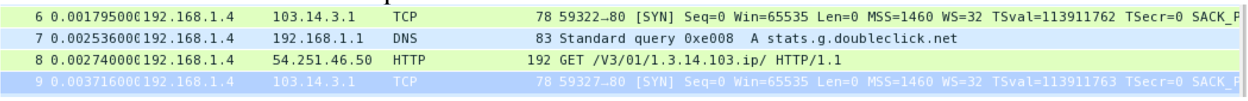
Name Server	ns1.metaname.net

2. Ideally an ARP request to gateway should be made to gateway as this is not in my subnet. I got the ARP request the first time when I connected to the site in Wireshark but after that I couldn't see arp request again, maybe because it is save in my cache?
3. [My Understanding] After getting the ip address of the site my system checks if the site is in same subnet or not. In this case it is not in same subnet so it sends and ARP request to gateway to communicate to router which then tries to find shortest path with minimum hops to the site. Doing a trace route here it took 18 hops to reach the site:



```
traceroute to radionz.co.nz (103.14.3.1), 20 hops max, 60 byte packets
 1  1.90.adb8.ip4.static.sl-reverse.com (184.173.144.1)  48.367 ms  48.532 ms  48.681 ms
 2  ae13.dar02.wdc01.networklayer.com (208.43.118.158)  0.321 ms  0.321 ms  0.337 ms
 3  ae9.bbr01.eq01.wdc02.networklayer.com (173.192.18.202)  0.558 ms  0.530 ms  0.828 ms
 4  ae0.bbr01.tl01.atl01.networklayer.com (173.192.18.153)  13.606 ms  13.690 ms  14.877 ms
 5  ae13.bbr02.eq01.dal03.networklayer.com (173.192.18.134)  35.111 ms  35.224 ms  34.943 ms
 6  ae7.bbr01.eq01.dal03.networklayer.com (173.192.18.208)  32.281 ms  32.509 ms  32.642 ms
 7  ae0.bbr01.cs01.lax01.networklayer.com (173.192.18.141)  65.105 ms  64.904 ms  64.892 ms
 8  * * *
 9  bundle-101.cor01.lax01.ca.vocus.net (114.31.199.60)  215.517 ms  216.580 ms  215.616 ms
10  bundle-100.cor02.lax01.ca.VOCUS.net (114.31.199.49)  216.089 ms bundle-200.cor01.alb01.akl.VOCUS.net.nz (114.31.202.44)  215.569 ms  21
5.096 ms
11  ten-2-2-0.bdr01.akl05.akl.VOCUS.net.nz (114.31.202.43)  221.344 ms bundle-200.cor01.akl05.akl.VOCUS.net.nz (114.31.202.46)  220.357 ms
 222.209 ms
12  as9503.cust.bdr01.akl05.akl.VOCUS.net.nz (175.45.93.114)  216.187 ms  215.558 ms bundle-50.cor01.alb01.akl.VOCUS.net.nz (114.31.202.86)
  220.771 ms
13  ten-0-1-0.bdr01.akl05.akl.VOCUS.net.nz (114.31.202.89)  220.502 ms TenGigE0-0-2-0-323.aktnz-art1.fx.net.nz (202.53.184.129)  223.104 ms
  219.616 ms
14  TenGigabitEthernet0-1-0-5080311.wnmur-rt1.fx.net.nz (202.53.187.205)  223.809 ms  225.593 ms as9503.cust.bdr01.akl05.akl.VOCUS.net.nz (
175.45.93.114)  220.600 ms
15  TenGigE0-0-2-0-323.aktnz-art1.fx.net.nz (202.53.184.129)  222.727 ms TenGigabitEthernet0-1-0-909.wntnz-rt1.fx.net.nz (131.203.241.25)
223.301 ms  227.036 ms
16  TenGigabitEthernet0-1-0-5080311.wnmur-rt1.fx.net.nz (202.53.187.205)  225.699 ms  224.346 ms  222.943 ms
17  * tengigabitethernet0-1-0-909.wntnz-rt1.fx.net.nz (131.203.241.25)  227.669 ms *
18  131.203.252.6 (131.203.252.6)  223.834 ms * *
```

4. Then a TCP Connection is established to the www.radionz.co.nz as displayed in above screenshot.
5. An HTTP GET request is made as shown in screenshot:



```
    6 0.00179500192.168.1.4     103.14.3.1     TCP              78 59322→80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=113911762 TSecr=0 SACK_P
    7 0.00253600192.168.1.4     192.168.1.1    DNS              83 Standard query 0xe008  A stats.g.doubleclick.net
    8 0.00274000192.168.1.4     54.251.46.50   HTTP            192 GET /V3/01/1.3.14.103.ip/ HTTP/1.1
    9 0.00371600192.168.1.4     103.14.3.1     TCP              78 59327→80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=113911763 TSecr=0 SACK_P
```

5. Finally Browser collects the response and renders it to display.

3. Describe in detail how you would obtain password hashes from a system and how you would then crack them to obtain the raw plaintext passwords. Describe specific tools and technologies that you would use. Also, do you need to crack all of the passwords to be able to exploit them?
•Extra credit: Describe in detail how you can defend your network against this kind of attack.

Ans 3. For windows I can get password hashes from SAM file in Windows/System32/Config folder and on linux we can get shadow file from /etc/passwd or /etc/shadow (I have seen it in /etc/shadow)

We can use bkhive and samdump2 to get the hashes from windows system if we are mounting a windows system in a linux system to obtain password hashes, where:

- **bkhive** - dumps the syskey bootkey from a Windows system hive.
- **samdump2** - dumps Windows 2k/NT/XP/Vista password hashes.

And we can use shadow-util package (which is already installed by default in most of linux os) to access /etc/shadow file to obtain password hashes

We can crack the passwords using tools like John the ripper, Cain and Abel etc. To speed up the cracking password we can specify the algorithm used to hash the passwords. Usually is LM or NTLM for windows and in linux based systems we can easily get the algorithm used by using following command:

```
Authconfig –test|grep hashing
```

We can probably reset all other passwords once we crack admin or root password so I don't think we need to crack all passwords. But I think even without cracking we can just bypass the whole login process altogether and reset the passwords if we want using utilities like BootRoot, SysRQ2 and Kon-Boot.[Referred from http://bernardodamele.blogspot.in/2011/12/dump-windows-password-hashes.html]

I would do following to defend against these attacks [NOTE: Its not just for the above attacks but for a general security]:

- Enable security monitoring to monitor and track password attacks and generate alerts on any such attack.
- Make sure the network is safe and secure so as attacker wont have system access on our domain controller. We can make sure that our firewall secures well known and concealed ports.
- We can implement account lockout functionality against failed login attempts.[Although this wont help against above methods but this surely will help against password guessing]
- We can use auto resetting of password after certain period of time.
- Password protect system BIOS, and protect boot order.
- We can use stronger authentication methods such as challenge/response, smart cards, tokens, biometrics or digital signatures.
- Make sure that hashing algorithm uses salt.
- For windows we should disable LM hashing and use NTLMv2 and for linux we can specify stronger hashing algorithm.
- For windows Disable LAN Manager and NTLM authentication
- We can enable logon screen warning messages on login attempts.

4. Assume that you know that spear phishing email from a particular source are on the rise in your corporate sector. You do not have any specialized tools or existing capability to identify these attacks.
Note: State all assumptions and use your own words, no quotations for this response.

   1. What existing steps, tools, and capabilities could you use to detect the traffic.

      Ans. Wireshark, NetWitness Investigator and snort to detect the traffic.

   2. Where in your network could you best implement additional tools and capabilities? You may specify multiple places.

Ans. We can implement it at our gateway or router because all the traffic is coming and and going through these so we would be able to monitor the whole network's traffic and act upon it. We can also implement ACL's for our DNS.

3. What are some simple and cheap tools or capabilities could you implement to provide an immediate improvement in detection?

Ans. We can identify the sources of the spear phishing mails and the network traffic pattern to generate snort rules for such traffic to avoid them. We can configure our mail client to detect such phishing mails and send them to spam and alert us about it. We can implement IDS too to enhance detection from the source.

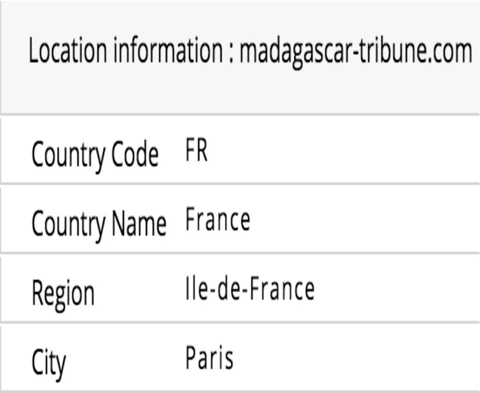
4. What more advanced tools or capabilities would you implement with more time or money?
Ans. We can implement IDS and block/drop traffic from the source.

5. In the x86 instruction set architecture a stack buffer overflow overwrites what register(s)? What do these register(s) do?

Ans 5. EIP will be overwritten. EIP is the Extended Instruction Pointer it is a read-only register and it contains the address of the next instruction to read on the program, point always to the "Program Code" memory segment. To mock a buffer overflow attack we write JMP to ESP instruction to EIP usually.

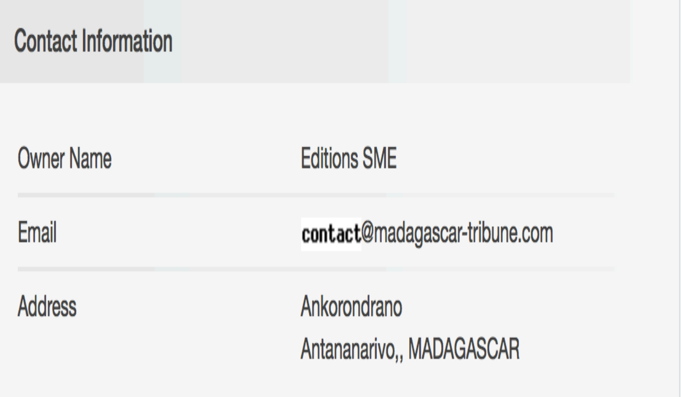
6. In what country/providence/city is madagascar-tribune.com registered? Where is it hosted? Anything interesting about the registry contacts? Describe how you identified this information.

Ans 6. It is registered/owned in Ankorondrano Antananarivo, MADAGASCAR and located/hosted in Paris, France. It is inactive at the moment. It seems it is registered at a different place and located/host at a different place. It is hosted at ip 213.186.33.16. I found following information about its registry contact from https://who.is :



Location information : madagascar-tribune.com

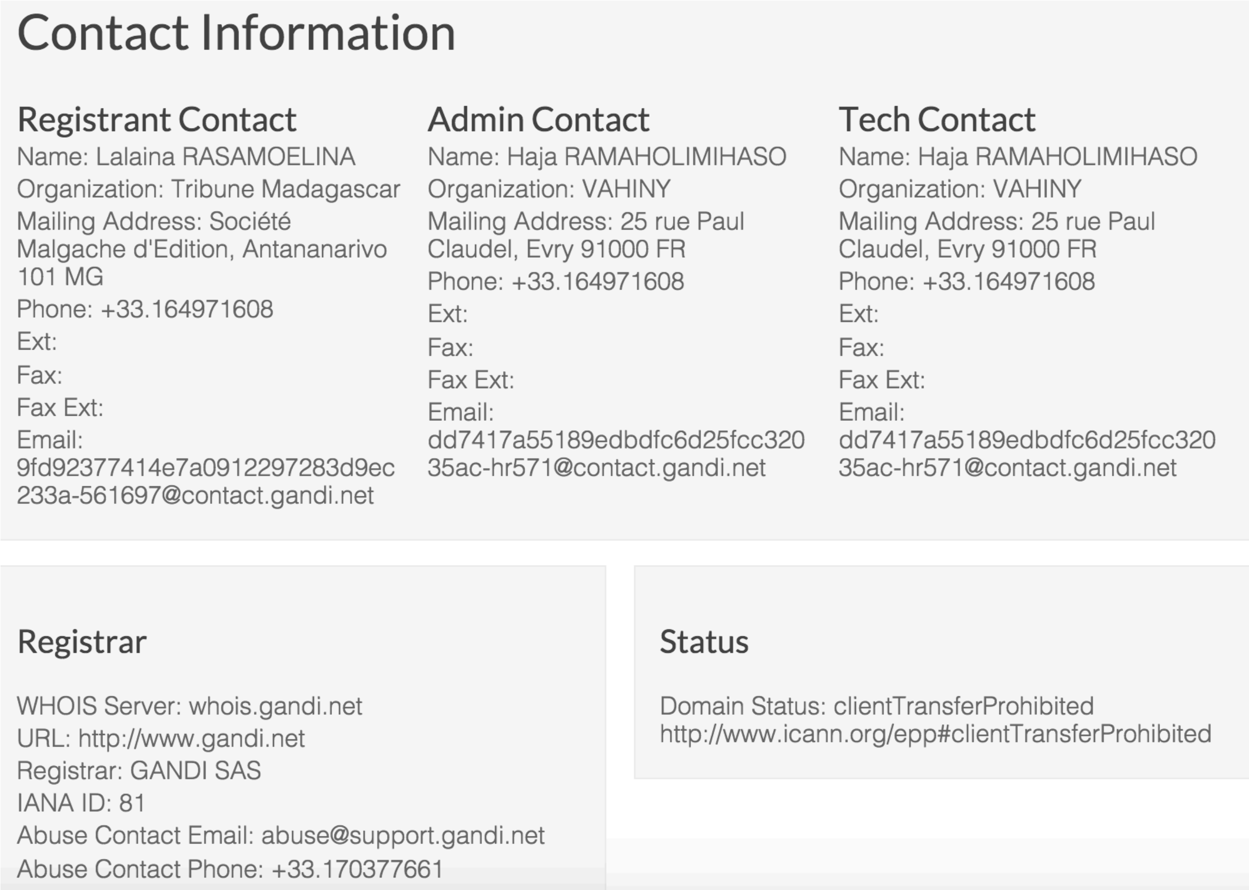
Country Code	FR
Country Name	France
Region	Ile-de-France
City	Paris



Contact Information

Owner Name	Editions SME
Email	contact@madagascar-tribune.com
Address	Ankorondrano Antananarivo,, MADAGASCAR

We can see the contact information below:



Contact Information

Registrant Contact

Name: Lalaina RASAMOELINA
Organization: Tribune Madagascar
Mailing Address: Société Malgache d'Edition, Antananarivo 101 MG
Phone: +33.164971608
Ext:
Fax:
Fax Ext:
Email: 9fd92377414e7a0912297283d9ec233a-561697@contact.gandi.net

Admin Contact

Name: Haja RAMAHOLIMIHASO
Organization: VAHINY
Mailing Address: 25 rue Paul Claudel, Evry 91000 FR
Phone: +33.164971608
Ext:
Fax:
Fax Ext:
Email: dd7417a55189edbdfc6d25fcc32035ac-hr571@contact.gandi.net

Tech Contact

Name: Haja RAMAHOLIMIHASO
Organization: VAHINY
Mailing Address: 25 rue Paul Claudel, Evry 91000 FR
Phone: +33.164971608
Ext:
Fax:
Fax Ext:
Email: dd7417a55189edbdfc6d25fcc32035ac-hr571@contact.gandi.net

Registrar

WHOIS Server: whois.gandi.net
URL: http://www.gandi.net
Registrar: GANDI SAS
IANA ID: 81
Abuse Contact Email: abuse@support.gandi.net
Abuse Contact Phone: +33.170377661

Status

Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited

I found that **GANDI.net** was one of the first and largest domain name registrars approved by ICANN for **.COM, .NET,.ORG, .BIZ, .INFO, .NAME, .BE, .FR, .EU** domains in France.

7. In the network 10.78.224.0/27, how many possible hosts are there?

Ans. Host range for the network is 10.78.224.0-31 with 32 Hosts in total and possible usable host are 30 i.e. from 10.78.224.1-31 with 10.78.224.0 as Network address and 10.78.224.31 as Broadcast address.

8. Describe what the following two commands return on a UNIX system:
• sudo ls -R -lha /var/log | egrep ".\.log$”
• netstat -an | grep '^tcp' | grep 'LISTEN' | sed 's/:/ /g' | awk '{print $4;}'
Note: You must describe what each of the commands listed above do and how they interact with each other.

Ans. sudo ls -R -lha /var/log | egrep ".\.log$” gives list of log files present in any folder under /var/log i.e. /var/log/anyfolder/anyfilename.log [I used ‘sudo ls -R -lha /var/log | grep .\.log$’ in mac] This basically lists the files ending with .log.

Here

–l is to list files
-a is to Include directory entries whose names begin with a dot(.). Lists hidden files too.
-h is used with –l to use suffixes for Byte KiloBytes
- R is used to Recursively list subdirectories encountered.

netstat -an | grep '^tcp' | grep 'LISTEN' | sed 's/:/ /g' | awk '{print $4;}' is used to get the list local addresses listening to tcp connection.

Here netstat –an is used to display:
-a : With the default display, show the state of all sockets; normally sockets used by server processes are not shown. With the routing table display (option -r, as described below), show protocol-cloned routes (routes generated by a RTF_PRCLONING parent route); normally these routes are not shown.
-n: Show network addresses as numbers.

grep tcp is used to display only tcp connections
grep 'LISTEN' is used to filter LISTEN
awk '{print $4;}' is used to filter out and display 4th column.
sed 's/:/ /g' is used to remove ':' from the output.

To check how they interact with each other I tried to open all files in a single cat and filter result with the ip address we found that are listening tcp connection.

To do that we need to get absolute path of the log files, we can get that using find

```
sudo find . -type f | xargs sudo ls -alh | awk -v pwd="$PWD" '{ print $(NF-2), $(NF-1) , pwd substr($(NF), 2)}' | grep log$ | awk '{print $3}'
```

I stored output of cat and netstat in two different files and then did 'grep –f pattern output' to get the output related to the ip address.
Apologies, but I couldn't understand any relation between the commands using all this. Or maybe there is something wrong with my grep command as I thought I would see entries of all the lines in all the logs having those ip addresses, but I couldn't see anything related to that, the only thing I could see was the partially matching lines usually due to various time in seconds.
If I do grep –wFf pattern output I cant see anything which is used to match whole words only.
[patters is the file with list of ip addresses, the output of netstat and output is the consolidated log file.

For the next two questions, please provide a detailed response. Concentrate on type of technologies instead of specific tools or products. Think back to the Systematic Security lecture and your Attack Defense planning. Diagrams are appreciated.

9. Given the network services you were required to maintain during the attack/ defense exercise (HTTP/SMTP/SMB/Custom App), if you had time (and budget), what are some specific technologies that you would implement to

improve the security of the network?

- Are there specific network topologies/designs that you would implement to augment the security? How would you architect the network? What sort of access control would you enact and where you you implement it?

Ans. I would like to modify my router to act as Hardware Firewall, I would try to set up port forwarding and set one of my machine in a DMZ and make it as a honeypot for attackers and monitor the intrusion network traffic. I would like to make a proxy server and would make all genuine traffic go through the proxy server and filter it by implementing firewall on proxy server. I would install various network monitoring and analysis tool and data collecting tool at both honeypot and proxy server.

- What technologies would you use to provide thorough visibility into network traffic? How would you identify known attacks? How could you identify previously unknown attacks? Ensure that you name technologies that monitor as many layers of the stack as possible - from layer 3 to layer 7. Multiple tools can be implemented in combination to provide detailed visibility.

Ans. We can monitor traffic at switches and routers to gain thorough visibility into the network.[Referring my answer from https://www.invea.com/data/flowmon/invea_cisco_wp_en.pdf] I can say that we can use a solution like Application Visibility and Control to get application level visibility, monitoring and traffic control. Apart from this we can always use Wireshark and snort in conjunction with this. We can identify previously known attacks using process and application monitoring system with intrusion detection system to gain knowledge about any out of the order behavior and identify its source in the network flow. Once identified we can deal with such network flow using snort and firewall. We can use Deep packet inspection, monitoring and analysis tools to inspect, analyse and monitor traffic from OSI layer 2-7, some techniques available are PACE, OpenDPI, nDPI, L7-filter, Libprotoident and NBAR with pcapbuilder or wireshark.

- Would you enact active defense in addition to passive monitoring?

Ans. Yes I would like to use port forwarding and filter the network traffic to allow traffic only from the defensive network that are having services of other teams to interact to my network and block all other traffic.

- What other technologies/products/policies would you implement to defend the network?

Ans. We can implement security at IPSec and implement group policies to use windows firewall effectively. We should also use SSL for our mail services.

Note: In this question concentrate on protecting the network architecture

10. You have been assigned to secure a small workgroup. You will inherit all enterprise technologies from the previous question. You can deploy any additional technologies to secure your enclave/workgroup. What would you

deploy to ensure that the individual systems and their local data are secure?
How can you monitor the settings?

Ans. I would just implement firewall and filter data using appropriate ports and allow data from the identified subnets of other teams only. If that doesn't work, then I would like to identify the incoming traffic and use and IDS to identify any out of the order behavior, once identified I would deal with is in appropriate manner depending on its nature by either using firewall to drop packets from its source or filter malicious traffic.

Note: In this question concentrate on endpoints.

11. Why do malware authors typically remove the NULL '0x00' character from shell code?
Ans. Malware Authors typically remove NULL '0x00' character from shell code because working shell code doesn't have null characters.

12. Explain why the LANMAN password algorithm is insecure. Provide at least three weaknesses/reasons.

Ans 12. LANMAN password algorithm is insecure because:

- More Vulnerable to brute force(Max password length 7) than its counterparts. (even more than historic Unix crypt() hashes)
- Stores Unsalted hash
- Stores hash of UPPER CASE form of password
- Pad password with '00' up to 14 characters in length.
- The password is split into two 7 byte chunk.
- Generate parity of each group of 7 bits.. This increases the length to 64 bit value.
- The two values are combined to for 16 byte hash

13. Of the security activities listed, pick two that you think will provide the most security to an Internet facing web server.
1. patching
2. local firewall configuration
3. stopping unnecessary services
4. removing unnecessary accounts and resetting passwords
5. installing antivirus
6. process and application monitoring
Explain your reasoning in detail.

Ans. I think local firewall configuration and process and application monitoring would provide most security to an internet facing web server as we will be able to identify any malicious activity by monitoring our processes and applications and would then be able to configure our firewall accordingly to avoid that malicious activity.