1 Day 1

URL for this doc: https://goo.gl/jcmf9z

Info from APNIC:
haveibeenpwned.com
zone-h.org/archive
https://www.bennish.net/password-strength-checker/
http://www.informationisbeautiful.net/visualizations
netcraft.com
https://www.ssllabs.com/ssltest/

APNIC Wiki Page:
https://wiki.apnictraining.net/

Notes:

Questions:

1. How to recover the data if server is damage?
    a. Depends how bad the damage is. If it was a rootkit or a SYSTEM level compromise on Windows, then usually best to start up a new server fix the vulnerabilities, and restore files from a known good backup.

2. Does Macbook gets infected with malicious or virus ?
    a. Yep, although not as many as Windows. Google search will find Mac virus references, but as Macs get more popular and more devices, attackers will start targeting them more. Attackers are lazy, they go after easy targets.

3. I have win2012 server functioning as dhcp and ftp with active directory running on it. I have limited the user permission so that user can't delete the files or folders. But one of user accidentally uploaded a confidential file on the server and he wants to delete the file. I tried to give the permission back using the admin account but couldn't do it. It says you must be the user to give the permission. How do I go about it?
    a. We talk about this in 4-5 slides from now, but if the file was write only then that's a good thing and just a request to the system admin to delete the file rather than letting the user do it themselves.

4. What is bitcoin and how does it works
    a. Crypto currencies use hashes (like SHA1) that require the clients to perform a certain amount of work to generate a hash with the first few digits of a known state (usually zeros).   Beyond that, it's easiest to relate Bitcoin to the stock market, the more demand the higher the price goes up.
    b. The idea is to build a network of hashed transactions (each made up of hashed blocks). To unhash one block, one would need to have the compute power to unhash the whole hashed blocks before that particular block! Talk to us offline if you want to know more.
    c. Bitcoin (any many other similar crypto currencies) is one application that runs on the blockchain network. People mine bitcoins, which technically is people trying to secure that transaction with the right hash (the right "nonce")!

5. In network, router and firewall are the two devices which are considered to be very important in monitoring the network stability but having said that many don't exactly know the where firewall should be located. Should it be placed before router or after router in network?
    a. After the router, and if your router is powerful enough it can handle some basic ACLs to protect the firewall (yes, even firewalls need protection sometimes)
    b. FWs are generally suggested infront of services/applications while your router ACLs act as the first line of defense (your FWs could help test your router ACLs). This way your network is not slowed down by the FW. From network ops point of view, run a dirty but fast network (borrowed from Maz- IIJ) and have security measures where it is necessary (your services and applications).

6. Why 169.x.x.x is assigned to the router, since this address does not fall in the range of ip addresses?
    a. 169 is for unknown DHCP connections, check DHCP config
    b. To allow your devices (within a subnet/LAN) to talk to each other without a legitimate address from the DHCP server (similar to your link-locals in IPv6)

    How to stop router from assigning it..??

7. What is the best way to make secure wifi?
    a. WPA2 with a long passphrase, or use the corporate AAA version
    b. Use 802.1X (identity based auth requiring central AAA servers)
    c. Turn off WPS

8. How to use LDAP authentication for Mac user? what are the feature need to enable in window LDAP server to get all the mac and windows user can use window LDAP user authentication. (e,g windows LDAP server can work in windows OS user but not able to use in MAC OS user)

9. Securing IPV6 address publicly?
    a. ?
    b. All the stuffs that you do with v4, please do with v6, and a bit more specific to the protocol vulnerability itself (like extension header and ping-pong vulnerabilities).
    c.

10. How to configure/rename to reduce the information being broadcast about the apache server?
    a. ServerSignature Off
    b. ServerTokens Prod

11. How secure is the paid version google apps (currently using across all government agencies) to share any government confidential information?

12. Is it good to use nexgen firewall that has built-in firewall and IPS/IDS or is it good to use IPS separately?

13. How to detect admin of confession pages viz. Thimphu confession page created in SNS facebook?

14. It is good to use wifi controller captive portal to make user base authentication in the LAN?
    a. As mentioned in 7 above, please use 802.1x where possible instead of captive portal.

15. This regarding the SSL: in my organization, recently we purchased two SSL license and was installed in two load balancer not in web server. Some says that it should be in web server but the data center experts have installed it in load balancer. Is this the correct way if not, what would be the correct way?

16. Is there any other effective way to check if a laptop's CPU is used for cryptocurrency mining other than checking in through CPU usage manually? (Recently there were concerns over www.thepiratebay.se and few other websites using site visitors' CPU for mining as involuntary donations).
17. What are the advantages/disadvantages of using hardware vs s/w firewalls?

18. How to configure .htaccess file to protect the website?

19. Which one is good, to have dhcp server or assign dhcp from router..??

20. How reliable is an non repudiation technique?

21. What are the feature to enable in CheckPoint firewall to protect threats?

22. it good to stop SSH server?

23. Google Chrome eats up a lot of memory. Should that be a concern, any memory leakages?
    a. Chrome eats up a lot of memory because each tab is it's own protected process and memory, whiHow to patch a live server with multiple dependencies? For example, a small update on one services, brings down the server as its version is not compatible with the new update?
    b. Why do most hackings originate from Russia? Are they sponsored by the Govt.?
    c. Is ch allows for an individual tab to "crash" without taking down the whole browser. To help with memory consumption when keeping several tabs open, try out the Chrome extension "The Great Suspender" https://chrome.google.com/webstore/detail/the-great-suspender/klbibkeccnjlkjkiokjodocebajanak

24. Dark Web. What? Who? How?

General Feedback - Day 1:

Please add feedback below. If feedback is about a specific slide or module, please mention it.

- **Share workshop resources/ ppt slides**
- Good going
- excellent.

Specific Feedback - Day 1 (one block of feedback per person, copy/paste the question template)

What did you like best about today's training?

Security on all level and to defence from malicious activities

What would you like done differently/improved?

No comment.

What topics from today do you want more training on in the future?

Hands on practice on tools to defend our system

What did you like best about today's training?

Risk assessment

What would you like done differently/improved?

no

What topics from today do you want more training on in the future?

More on risk assessment

Day 2

References:

University of Texas - Redhat Hardening Guide (also has a Windows 2012 R2 ardening guide)
https://security.utexas.edu/os-hardening-checklist/linux-7

Center for Internet Security - Hardening Guides and Tools (some info requires paid subscription, so check out the cost and value you get)
https://www.cisecurity.org/

Redhat Hardening Guides
https://www.google.bt/search?q=redhat+hardening+guide&oq=redhat+hardening+guide

How to remove from the Google mail blacklist
https://www.rackaid.com/blog/gmail-blacklist-removal/

Feel free to use any of the content but do not repackage it and use it for commercial purpose!

Commands from today's session:

`nmap -sS -sV -O 127.0.0.1` (SYN scan to find open ports, services version, and OS fingerprinting)

`nmap -sU 127.0.0.1` (scan for open UDP ports)

`nmap –script smb-enum-users.nse –p 445 <target IP>` (run scripts)

`nbtscan-unixwiz -f <target IP>` (scan for open NETBIOS ports; address can be of the format 192.168.159.0/24 or 192.168.159.1-170)

`Enum4linux <target IP>` (try using wrapper scripts)

Questions ?

1. **Give us clear procedure on how to proceed with SSL**
    a. To deploy SSL/TLS, it is as simple as you generating a key pair (pub-pvt), sending a csr (cert signing request) which basically is a request to associate your public key to your domain, to your provider.
    b. Once you have your certificate, you would want to get your certificate(s) signed by trusted root CAs (certificate authorities- LetsEncrypt is an example), in order for browsers to trust your certificate (PKI is verified up the chain of trust).
    c. For BCPs (best practices), there are many free information out there to help you do it properly (SSL Labs is a good source)

2. **Has IPv6 been necessary from security point of view ?**
    a. If the question is whether the v6 protocol was conceived due to security reasons, NO! Rather, the way the protocol was designed, there are some serious security loopholes (which are being addressed through BCPs as opposed to modifying the protocol).
    b. Example: v6 introduced the idea of extended/chained headers, which effectively means that one could send packets with infinite packet headers without the actual payload, effectively DOSing the recipient

3. How do we remove our mail server domain from Google blacklist (we are using Zimbra with self-signed certificate)? We wrote several times to Google but haven't received any responses from them.

4. Any advice to be a White Hacker?
Look at training that leads towards the Certified Ethical Hacker (CEH) certification.
https://www.eccouncil.org/
Even if you don't sit the exam the training and exercises/labs will get you started in the right direction. There is a lot of information security training, one place is https://www.cybrary.it/ (stick to the free material)

5. Dark Web..??
Addressed already (read Q#26)
Having said that, there is something called Darknet, a tool used by Security folks: the idea is to advertise/announce your dark IP addresses (unlit or unused IP addresses) to the Internet, and log incoming packets to those dark addresses. Ideally, you should not be receiving any packets to your dark IPs. Ex: you could measure reflected traffic (somebody might have spoofed your addresses, and you could be receiving responses to those queries) using darknet.

6. Is it possible to do packet analysis using wireshark in simple LAN (meaning LAN without VLAN)
Yes, in fact it is much easier without network segments to capture and analyse.

7. How to crack windows 2003 server password…??

It depends what level of access you have already. It's usually hard to do it from over the network, but if you have even a user account on the server you can dump out the password hashes and then crack the passwords offline

8. How do we set up a honeypot in a network?

APNIC actually runs a small honeypot network that you can join. You need to create a Linux VM with a public IP address, and we give you some install scripts to run which configure the Honeypot. You have local root on the server so you can see all information collected, and a small subset of information is sent back to APNIC to be collected with other honeypots. You then get access to the web interface at APNIC to see the scans and attacks against all honeypots in the project, of course with some information anonymised.
Email Adli Wahid at APNIC for more information - adli@apnic.net

General Feedback - Day 2

- <feedback goes here>

Excellent course articles!!! Well packaged and delivered with high quality. I would like to thank the facilitators and the TEIN team
Topic cover are very much relevant for network administer
Resource person is knowledgeable
Handson practice
Nice and effective.
If there is more on practical hacking on real time, it would be better to understand..

Specific Feedback - Day 2 (one block of feedback per person, copy and paste question template before answering)

What did you like best about today's training?

- Hand on practice
- Practical session
- Using different tools to see the services running, OS being used and MAC address of clients in LAN or WAN
- Kali is Amazing

What would you like done differently/improved?

- More practicals on Wireshark and explanation

What topics from today do you want more training on in the future?

- more practical on white hacking
- Network monitoring tools for security reasons

What did you like best about today's training?

We got to learn penetrating tools to check vulnerabilities in a system or a network. I really got to know how powerful tool the Kali is and I believe more of such tools would help us know the risk of being hacked by intruders.

What would you like done differently/improved?

I would say, more of practical session would help us.

What topics from today do you want more training on in the future?

I would like to learn and explore more of Kali.
I would also love to know more on how Wireshark can be used to monitor the network traffic in the VLANed network.
Thank you.

What did you like best about today's training?

What would you like done differently/improved?

If the practical sessions are done bit slower as per our capacity all together

What topics from today do you want more training on in the future?

Kali and wireshark as those are very new to us

What did you like best about today's training?

I heard of kali linux but today got opportunity to lay my hands on it

What would you like done differently/improved?

If we were taught realtime hacking, practical

What topics from today do you want more training on in the future?

Ethical hacking

What did you like best about today's training?

Kali linux is a useful tools for network administrator

What would you like done differently/improved?

Using the tools to optimize the network and also help other organization for the new tools that we learn in today's lesson. I really want to learn more by using the new technology in the field of network.

What topics from today do you want more training on in the future?

Need more hands on practice to make ourselve confidence to use the tools in individual organization

----

What did you like best about today's training?

-Training was hands on

What would you like done differently/improved?

-More emphasis on the output for better understanding

What topics from today do you want more training on in the future?

-Methods of fixes to the vulnerabilities detected

What did you like best about today's training?

...answer here...

What would you like done differently/improved?

Linux System administration to have a better understanding of Linux which will then help us to understand the ethical hacking aspects!!!

What topics from today do you want more training on in the future?

...answer here…

What did you like best about today's training?

More practical

What would you like done differently/improved?

What topics from today do you want more training on in the future?

...answer here…

What did you like best about today's training?

-> The content of the training is very relevant

What would you like done differently/improved?

...answer here…

What topics from today do you want more training on in the future?

...answer here…

What did you like best about today's training?

...todays training was very much interesting and much relevant.

What would you like to do differently/improved?

..could give us more practical so that we can have more hands on.…

What topics from today do you want more training on in the future?

...wireshark and their finding and diagnostic. More on Kali applications …

What did you like best about today's training?

->todays training was very much interesting and much relevant.

What would you like done differently/improved?

-> no comments

What topics from today do you want more training on in the future

Windows security features and best practices.

What did you like best about today's training?

Got the opportunity learn how to use wireshark and nmap. Its effectiveness on identifying the vulnerabilty.

What would you like done differently/improved?

More commands and examples on nmap as it is proving to be quite useful

What topics from today do you want more training on in the future?

Effectiveness of such tools on the network and system vulnerablity as at the moment we are just touching the surface.

What did you like best about today’s training?
-The hands-on practical was interesting.
What would you like done differently/improved?
-More hands-on training
What topics from today do you want more training on in the future?
...answer here…

What did you like best about today’s training?
The hands on practical session, and also the topic on Wireshark which would be very helpful to analyse one’s network.

What would you like done differently/improved?
Today is only the first day of the practical session so nothing much to comment, but it would be great if the presentation slides are shared with us so that later whoever is interested can go through it again and also we will know what all will be covered the day after.

-

What topics from today do you want more training on in the future?
Perhaps, bit more in-depth on Wireshark and Kali application.

Day 3

References:

Download the slides from day 1-3 at
https://drive.google.com/file/d/0B7Pq5zKYazmVcUIOcHd1UzZIVjQ/view?usp=sharing

Day3 Commands:
Start SNMP service:

Look at SNMP (MIB info):

```
snmp-check -c public 127.0.0.1
snmpwalk -c public -v1 127.0.0.1 1
(this may not work)   snmpenum -t 127.0.0.1
```

SNMP Scanner (Onesixtyone):ta

```
cd /usr/share/metasploit-framework/data/wordlists/
ls -al /usr/share/metasploit-framework/data/wordlists/
less snmp_default_pass.txt

onesixtyone -c snmp_default_pass.txt 127.0.0.1
```

Open vulnerability assessment system (OpenVAS):

```
service apache2 stop
openvas-start
```

Browser: https://127.0.0.1:9392
OR

```
openvasmd --user=admin --new-p
```

```
assword=admin
openvas-check-setup
   openvas-stop
openvas-start
```

Questions?

1. **What is the danger if SNMP is exposed to attacker or if they can write to it.**
   a. Write access allows changing your device configuration

2. **Best wordlist recommendation please.**
   a. “Best” always changes, a Google search will find good ones. Most brute force scanning will involve randomly generating passwords rather than just using a word list

3. **If I hack into someone’s server/network using kali, will my IP be detected by the forensic experts or I am safe if I use Kali? Is there any other such free tools?**
   a. You are always detected unless you use proxies or similar jump hosts, but even then if those proxies log your connections you are still able to be traced

4. **Can we trace the anonymous(fake) user in facebook using Kali linux?**
   a. No, unfortunately you would need to be able to tie a Facebook login to an IP address to be able to trace them back. If you had a NextGen firewall or similar web proxy outbound you might be able to do corporate root/CA certificate man in the middle, which would let you observe all traffic outbound. Then it’s a matter for having tools that would allow you to see Facebook usernames and log them.

5. **How do we protect the console/auxiliary port on the router/switch?**
   a. As discussed in the presentation, have ACLs/login credentials even for console and AUX

6. **How do we disallow personal wireless router connecting to LAN?**
   a. Scanning for wifi networks, and if they are open (no password) then connecting to them and checking to see if you then have access into the corporate network/IP addresses. Some wifi controllers have this functionality built-in, and sometimes you may just want to install a wifi analyzer software on your mobile phone and walk around the office. (with a baseball/cricket bat)
   b. 802.1X can protect rogue APs from connecting to the LAN port

7. **Is there any way to overcome the hotspot issues? Once the host has logged in after using captive portal/802.1x, users connecting to the hosts hotspot is able to access the resources without any authentication.**
   a. Captive portal or 802.1x is just the network layer of authentication, for individual applications you still need to do an additional layer of authentication.

8. **Does Radius server and diameter AAA have user directory or it needs a separate one?**
   a. You can configure RADIUS or Diameter to back onto an LDAP or AD server for authentication, or you can configure a local user database.

9. **How to configure reverse mod_security server, if we have only one web server and router as gateway?**
   a. For one server it’s best if you can install ModSecurity on the web server, otherwise you will need another host between the web server and the internet. VMs or similar.

General Feedback - Day 3

- JG - fixed for slide 90 around nano command to save, copy from later slide. Nano doesn't display line numbers
- OpenVAS not running properly, needs openvas-check-setup then top then start maybe
- OpenVAS taking a long time to scan, maybe demo only, or run it at a different time not bounded on both sides by other hands on exercises
- Slide 98 - nano might not display line numbers, maybe use gedit or similar for non vi users
- Slide 100 - run help first to see msf commands, then get into search, use, info...
- JG - pre-run an OpenVAS scan in Kali against Meta2 and Meta3, then save the report to package Kali.OVA
- JG - setup a vulnerable PHP/MySQL app on Kali and create an exercise to show ModSecurity blocking SQL Injection attacks, example at https://www.digitalocean.com/community/tutorials/how-to-set-up-mod_security-with-apache-on-debian-ubuntu
- We would like to request you to Increase the font size of the linux terminal so that it would be visible from the distant seaters.
- ...

Specific Feedback - Day 3
(one block of feedback per person, copy and paste question template before answering)

- **How to hide apache information with ServerTokens and ServerSignature directives**
  https://www.virendrachandak.com/techtalk/how-to-hide-apache-information-with-servertokens-and-serversignature-directives/

What did you like best about today's training?

- Practical Demonstration along with presentation. Thumps up!

What would you like done differently/improved?

- Please provide us tagline along with the command code which will make us understand the codes better

What topics from today do you want more training on in the future?

- ...

What did you like best about today's training?

- Practical on Kali is the most interesting session
- The importance of maintaining a log
-
- What would you like done differently/improved?
- Thumbs up...

What topics from today do you want more training on in the future?

- More practical and hands on training
- ---

What did you like best about today's training?

- It is good session to learn practically for ethical hacking tool i really got new ideas

What would you like done differently/improved?

- It really improved my to make securing the network

What topics from today do you want more training on in the future?

- Need to have more practical session to make use of tools

What did you like best about today's training

- Practical was the best.

What would you like done differently/improved?

- It would have been better if we had 2 projector screens and bit better internet speed.

What topics from today do you want more training on in the future?

-

What did you like best about today's training?

- .

What would you like done differently/improved?

- ...

What topics from today do you want more training on in the future?

- ...

What did you like best about today's training?

- ...

What would you like done differently/improved?

- ...

What topics from today do you want more training on in the future?

- ...

What did you like best about today's training?

- ...

What would you like done differently/improved?

- ...

What topics from today do you want more training on in the future?

- ...

What did you like best about today's training?

- ...

What would you like done differently/improved?

- ...

What topics from today do you want more training on in the future?

- ...

Day 4

References:

https://developers.google.com/time/guides

Questions?

1. If we configure DNSSEC at our site, is it necessary to have DNSSEC at the ISP (the next DNS we point to from our network)?
    a. Like we discussed, DNSSEC works on a chain of trust. For your domain (name space) to be signed, your TLD needs to be signed first (eg: for **gov.bt** to be signed, .**bt** needs to be signed first in order for the validation to work up the chain of trust).
    b. However, you could have a dnssec validating resolver deployed in your network and point
    c. it to some public DNS servers

2. There is Internet access but some computers are not able to browse. When we manually assign dns, it does works sometimes and at times it is not working. What could be the reason behind this?
    a. Could be your DHCP server not assigning DNS info correctly, or
    b. It could be a NAT box issue (sessions might be running out), OR
    c. Could be path MTU issues (look at your interface MTUs, or TCP maximum segment size)

3. Can we access office internet to our home. If yes? What are the devices needed and great help if provide configuration too?

4. My router frequently goes down (once or twice in a week) and I was not able to identify the problem/issues. It usually gets into reload/reboot cycle and gets heated up. The router works when it is cooled down. I have the UPS, Air conditioning system running 24x7. What could be the possible reasons or solutions? It even goes down during weekend. No active users to use CPU or memory. Google did not help.
    a. we would need some more details - CPU usage, memory usage, etc

5. **Domain/Server Clustering**: how does domain cluster works in a network and how auto switching is done when one domain controller fails? The concept of having domain clustering is to have uninterrupted service in the network but how it's been setup? Does it require same hardware configuration suppose, I have three or more servers?
    a.

6. What VPN has got to do with security if it can be shared ?
    a. Any tunneling technique is basically you manipulating the encapsulation/decapsulation process on the TCP/IP stack (only the tunnel end-points know how to encapsulate and decapsulate)
    b. With VPNs (IPsec for example), the tunnel (or the secure channel) between A and B is a encrypted communication channel (uses symmetric encryption); meaning every message we exchange now is encrypted/secure (even if someone sniffs, they won't be able to decrypt - if they don't have access to the encryption key)

7. While installing OS, certain chunk of memory is reserved for system memory. Is this the functionality of DEP?/

8. IF we disable the password recovery option for router/switches & at the same time, if we forget the password our self...what is the possible way to recover the password?.
    a. This is a weird one ;-) because you disabled in the first place to not allow any password recovery.
    b. Anyways, the only option is to do a factory reset of the router/switch (break sequence during boot and reset to factory default).

General Feedback - Day 4

- Highlight on password strength/weakness was great.
- Network security slides was great
- Should have this type of workshop annually
- DITT should initiate to send any updates to all the ICT Personnel

Specific Feedback - Day 4

(one block of feedback per person, copy and paste question template before answering)

What did you like best about today's training?

- Device hardening was new concept and enjoy knowing to protect the system by shutting down the unused ports and services
-

What would you like done differently/improved?

- .Separate training for DNSSEC

What topics from today do you want more training on in the future?

- Practical hands on training using Kali to check vulnerability

----

What did you like best about today's training?

- DNSSEC require more practical session

What would you like done differently/improved?

- Need to add more details on individual topic that cover

What topics from today do you want more training on in the future?

- Required more real time session so that we can have grab the 95% of all the session cover today
-

What did you like best about today's training?

Packet inspection using Wireshark

What would you like done differently/improved?

- Detailed explanation on wireshark packet inspection.

What topics from today do you want more training on in the future?

- Want to learn more on DNS and DNSSEC
- Detail training on Wireshark

What did you like best about today's training?

-Different architectural models for firewalls.

What would you like done differently/improved?

- More on practical

What topics from today do you want more training on in the future?

- ...

What did you like best about today's training?

- ...

What would you like done differently/improved?

- ...

What topics from today do you want more training on in the future?

- ...

Note: Please share all the PPT for our reference please

Day 5

References:
https://www.bennish.net/password-strength-checker/
https://haveibeenpwned.com/Passwords

https://www.random.org/dice/?num=5
https://www.eff.org/files/2016/07/18/eff_large_wordlist.txt

Open Source OTP (2FA) Servers

- https://www.linotp.org/
- https://www.privacyidea.org/
-
- https://www.rcdevs.com/products/openotp/
- As well as the TOTP standard used by Google Authenticator

Questions?

1. What is SQL Injection? How can it be injected? How can it be prevented?
    a. Put simply, lets say a web page requires users to input a username and password. Now if you do not validate or sanitise user inputs on your web form, some one could insert special characters as username/password, which could make your database query logic valid, and access/read your database!
    b. Hence, you should never trust your users (always validate user inputs on any web forms!)
    c. Below is an example from the W3Schools (https://www.w3schools.com/) SQL injection:
    d. The SQL query statement is: `SELECT * FROM Users WHERE Name ="' + uName + '" AND Pass ="' + uPass + '"'` (This is a very bad code btw!)
    e. This allows you to access all the rows in the table “Users” in your database if the username and password is valid (ex: with the mysqli_query() function in php).
    f. If you do not validate or sanitise user inputs on your web form, some one could insert special characters as username/password: **`" or ""="`**
    g. Now the SQL query logic would be: `SELECT * FROM Users WHERE Name ="" or ""="" AND Pass ="" or ""="",` which is always true (similar to 1=1 logic)
    h. Now, the malicious user can access/read all rows from your “Users” table (every user and their passwords for example).

2. Can you share the concept of DMZ. How to design and implement?
    a. Some people also call it the “external server LAN”, meaning services hosted within this subnet is accessible from the internet, but is separate from your “NOC or internal server”

3. In VLAN setting, people use “dot1q” to encapsulate. What does dot1q means and what functionalities does it has? What does VLAN tunneling means?
    a. 802.1q is a VLAN tagging standard (a 4-byte tag added to the native Ethernet frame- hence from 18 bytes to 22 bytes headers for 1q tagged frames).
    b. The idea is to allow one physical switch to be logically divided into multiple LANs (multiple virtual switches if you like). With VLANs (802.1q tags), the inbound access port tags the frame with the assigned VLAN and is carried over a trunk (multiple VLANs can be carried over a trunk). This helps with traffic segmentation (you can only talk to devices in the same VLAN - without a router) and also localise broadcasts (each VLAN is now a separate broadcast domain).
    c. With regards to VLAN tunneling (also called QinQ), it is generally something used by operators to carry customer VLANs over their backbone, where the customer VLAN tags could already have been used in the operator’s backbone as well. But the problem with QinQ is you end up forwarding frames using customer’s destination MAC! Hence, now most operators use whats called PBB (provider backbone backhauling), which is a MAC-in-MAC technique (customer ethernet frame encapsulated in your ethernet frame!

4. robot.txt : Is this “robot.txt” use in securing the website pages? If so how to implement in website development.
    a. Robots.txt is used by a web server admin to tell web crawlers/spiders like GoogleBot and Yahoo crawler not to index certain parts of their web site. It’’s just a plain text file though, so its also fun to go looking for them to see what different web admins don’t want search engines looking at. Reference: https://support.google.com/webmasters/answer/6062596?hl=en
    b. Fun examples at https://searchengineland.com/fun-robots-txt-263796 (yes, robots.txt can be fun)

5. How to set up 2FA /Multi Factor Authentication in the centos server?
    a. See list of references above for open source OTP/2FA servers. Commercial OTP servers include RSA SecurID, SafeNet / Gemalto, and others
    b. Have a read through on our 2FA hands-on lab (https://wiki.apnictraining.net/netsec2017-png/agenda)

General Feedback - Day 5

- # Share the PPT for reference
-
- …
- ...

Specific Feedback - Day 5
(one block of feedback per person, copy and paste question template before answering)

What did you like best about today’s training?

- About how to make a strong password or any other user credentials.
-

What would you like done differently/improved?

- Internet speed is so pathetic. Cannot load anything.

What topics from today do you want more training on in the future?

- ...

What did you like best about today’s training?

- ...

What would you like done differently/improved?

- …..

What topics from today do you want more training on in the future?

- ...

What did you like best about today’s training?

- ...

What would you like done differently/improved?

- ...

What topics from today do you want more training on in the future?

- ...
