Please note this event may be photographed

Network Forensics

Utilising Wireshark

The Legal Bit

- The skills taught in these sessions allow identification and exploitation of security vulnerabilities in systems. We strive to give you a place to practice legally, and can point you to other places to practice. These skills should not be used on systems where you do not have explicit permission from the owner of the system. It is **VERY** easy to end up in breach of relevant laws, and we can accept no responsibility for anything you do with the skills learnt here.
- If we have reason to believe that you are utilising these skills against systems where you are not authorised you will be banned from our events, and if necessary the relevant authorities will be alerted.
- Remember, if you have any doubts as to if something is legal or authorised, just don't do it until you are able to confirm you are allowed to.

Code of Conduct

- Before proceeding past this point you must read and agree our Code of Conduct, this is a requirement from the University for us to operate as a society.
- If you have any doubts or need anything clarified, please ask a member of the committee.
- Breaching the Code of Conduct = immediate ejection and further consequences.

- Code of Conduct can be found at https://wiki.shefesh.com/doku.php?id=code_conduct

A bit of background – Hubs

- Historically, hubs were used to connect devices together on a LAN
- Connects networked devices together, such as clients and servers
- Can be interconnected to provide more ports -> leads to more errors
- Receives information in one port and rebroadcasts to all the other ports

A bit of background – switches

- Much like a hub, it connects networked devices together
- Switches learn what devices are on which switch ports
- Switches only forward traffic received from a port to the destination port, based on the device's hardware (MAC) address
- Provides more security and more bandwidth efficient than a hub

Address Resolution Protocol (ARP)

- ARP ‘translates’ between IP addresses and MAC (hardware) addresses on a LAN
- ARP cache is a table of devices associated with IPs and MACs so packets can be routed accordingly
- If a device doesn’t exist on the ARP cache, an ARP packet is sent to every device on the network asking which device is associated with the IP
- Device with associated IP should be the only one to respond
- “Who has xxx.xxx.xxx.xxx? Tell xxx.xxx.xxx.xxx”

What is packet sniffing?

- Sitting on a LAN, you can intercept traffic and analyse communications.
- Two types
  - Passive sniffing
  - Active sniffing
- Passive sniffing doesn't really happen anymore – tends to happens on trunk ports/hubs
- Active sniffing
  - More difficult – occurs on switches
  - Few methods to enable this

Switch table flooding

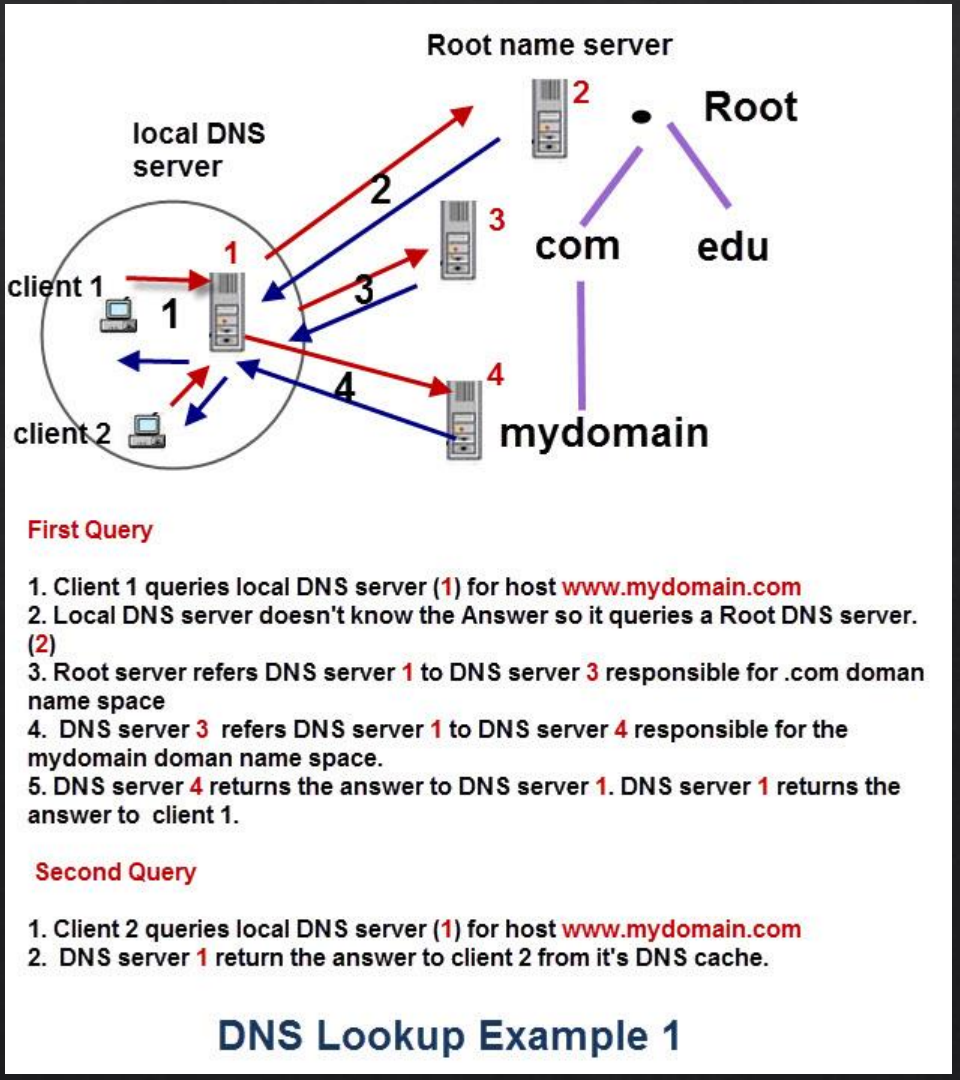
- On older/less powerful switches, you can flood the CAM table on the switch so that it goes into failover mode. Switches failover into hubs, so all traffic is broadcast to all ports.
- This doesn't tend to happen so much with newer switches – purposefully designed to prevent this occurring.

ARP Spoofing/Poisoning

- ARP Spoofing enables a poisoning attack
  - Spoofing involves crafting bogus ARP packets with false destination/source in an attempt to associate the attacker's MAC with another device's IP
- When this is successful, the ARP cache is 'poisoned' with false information, packets destined for the target will instead go to the attacker's machine
- This is a Man-In-The-Middle (MITM) when the attacker then passes on these packets to the target machine
- Intercepted packets can then be analysed
- Can also enable us to DHCP spoof, so that we can MITM devices that are looking to lease IPs

A bit of background - DNS

- DNS behaves much like ARP, it 'translates' human-friendly domain names into IP addresses
- This is achieved by contacting a DNS server which will have a lookup table of known IPs/hosts, or will contact other DNS servers until it gets answers (up to root name servers and then down)
- DNS lookups are an inverted tree-like structure
- e.g. ibm.com
  - Local DNS server doesn't know, referred to root server
  - Root server refers to DNS server responsible for .com
  - Then finally the DNS server associated with ibm.com returns an IP



DNS Spoofing

- Attacking the DNS cache of the DNS server allows attacker to modify entries, so attacker could redirect traffic destined to a domain to a server they control instead
- It is difficult to verify the IP returned is legitimate, usually assumed correct
- 1/3 of internet-facing DNS servers are spoofable!

Analysis tools

- Most common – you guessed it – Wireshark!
- Other alternatives exist
  - Command-line, more powerful if you know how to use it: t-shark
  - Cloud-based: CloudShark
  - Cain & Abel – Older, Windows based but lots of good features ie ARP spoofing, VoIP recording, SSL breaking etc.
  - tcpdump – Also command-line based
  - Ettercap – older, much like Cain but UNIX based

Looking at unencrypted packets

- Unencrypted data is great for us, we can view the contents very easily!
- Wireshark handily distinguishes between different protocols for us so we can quickly identify which are in use
- Selecting a packet will bring all the information associated with it in a readable format as well as hex

Following data streams

- Single packets aren't necessarily useful, it can be better to look at whole streams to understand a bigger picture.
- Analyze -> Follow -> xxx stream
- Can quickly browse through different streams, communication direction denoted by different highlighting colour
- Wireshark applies the filter for you

The power of filtering

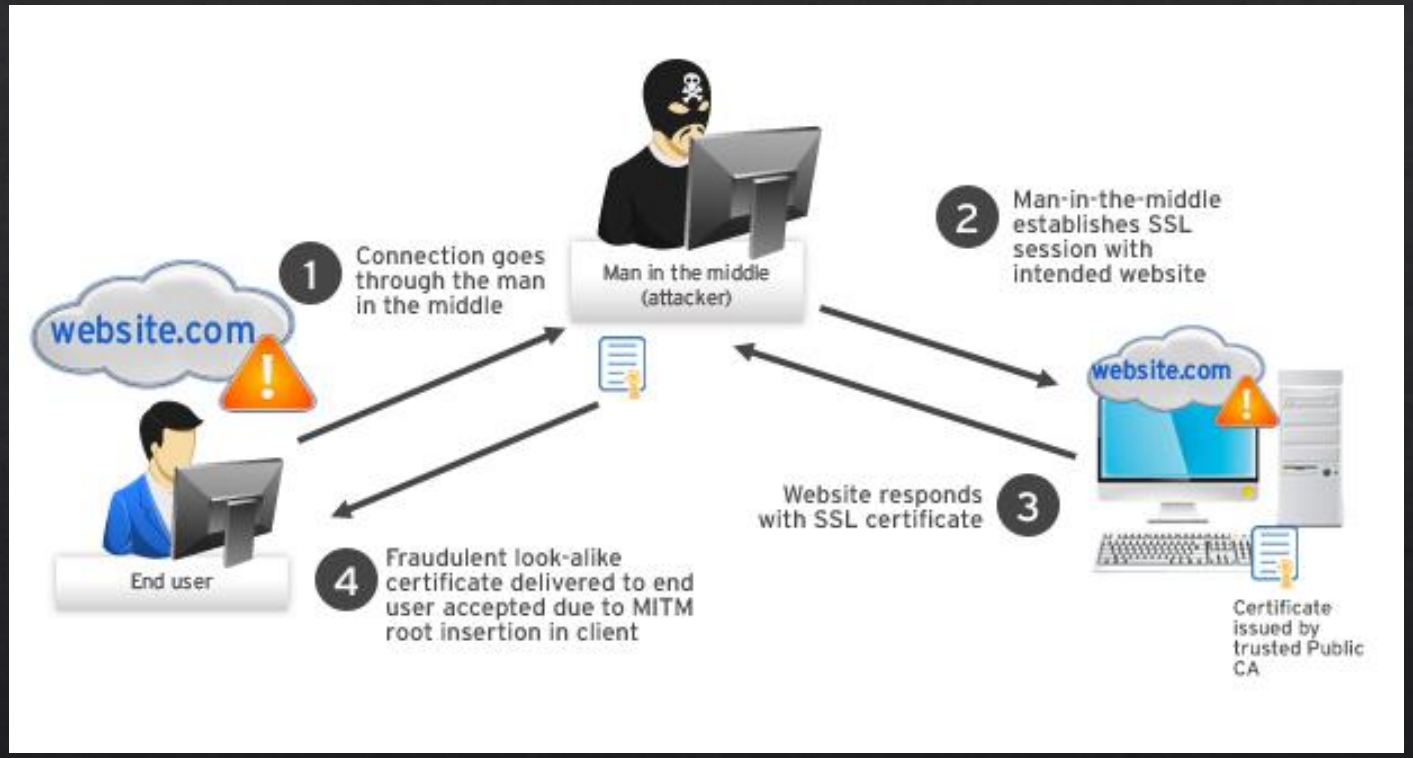
- You can apply a lot of filters through the GUI or by entering them into the command bar
- Can filter by protocol, IP addresses, strings etc. A lot of possibilities!
- Logical operators can be used, daisy-chain commands together to get a better filter on the traffic you want
- E.g. if I wanted to narrow my view down to HTTP traffic with a specific IP
  - http && ip.addr == xxx.xxx.xxx.xxx

Advanced analysis tools

- Wireshark can also be used to pull and recreate images/binaries/files from packet captures. Very easy to export through File -> Export Objects
- Other protocols such as RTP used for VoIP/media streaming can also be recreated. Can extract audio data
- Wireshark provides a lot of different statistical views of packet captures, can be useful to look at these first to see where potentially more interesting communications are occurring

MITM & Breaking SSL

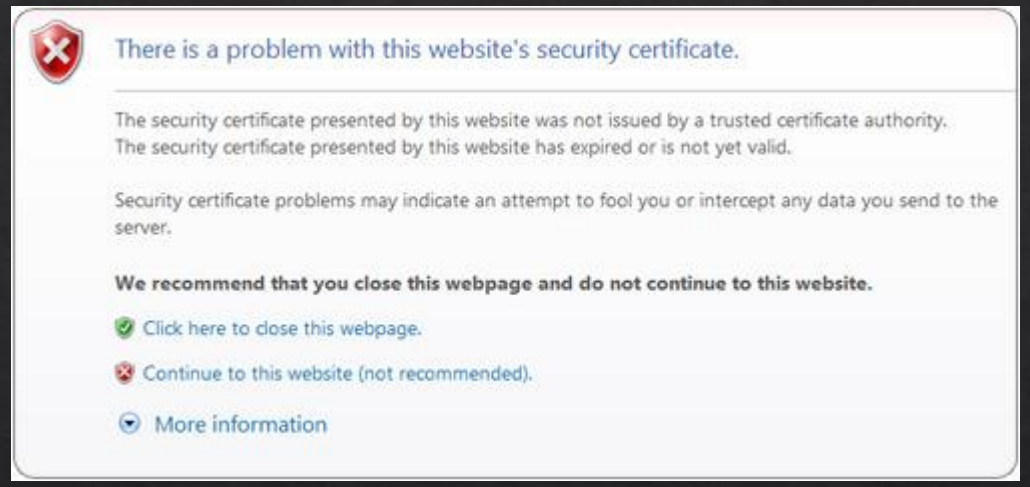
- Encrypted traffic makes it much more difficult for us to see what's going on
- If we have the SSL keys, we can decrypt this and see what's going on – but it's not too often you get your hands on these
- Sitting as a Man-In-The-Middle, we can intercept SSL requests.
- Tools include Cain, mitmproxy and sslsplit

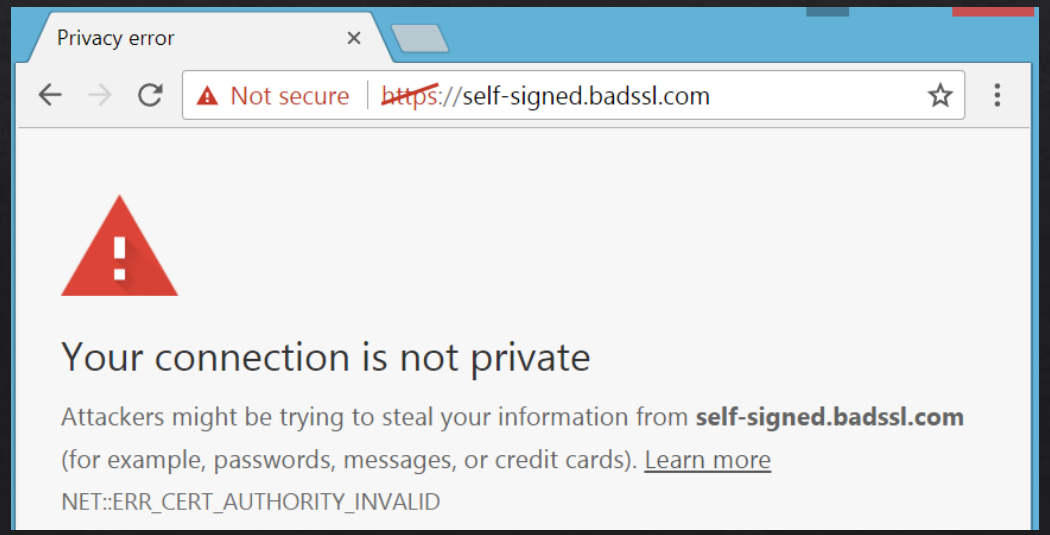


MITM & Breaking SSL Cont'd

- User makes request, we detect this and instead make an SSL request to the intended server
- Intended server then replies with a certificate
- We then pull the details from this certificate and create a 'realistic' looking certificate with the same details, to be used between us and the victim
- The victim will get a certificate warning, so we're relying on them to not investigate further than the details we implanted in the certificate
- We can then decrypt the traffic between us and the victim using our certificate, as well as passing this on to the actual intended server – victim is none the wiser as all works as normal

Seen this before?





In the real world

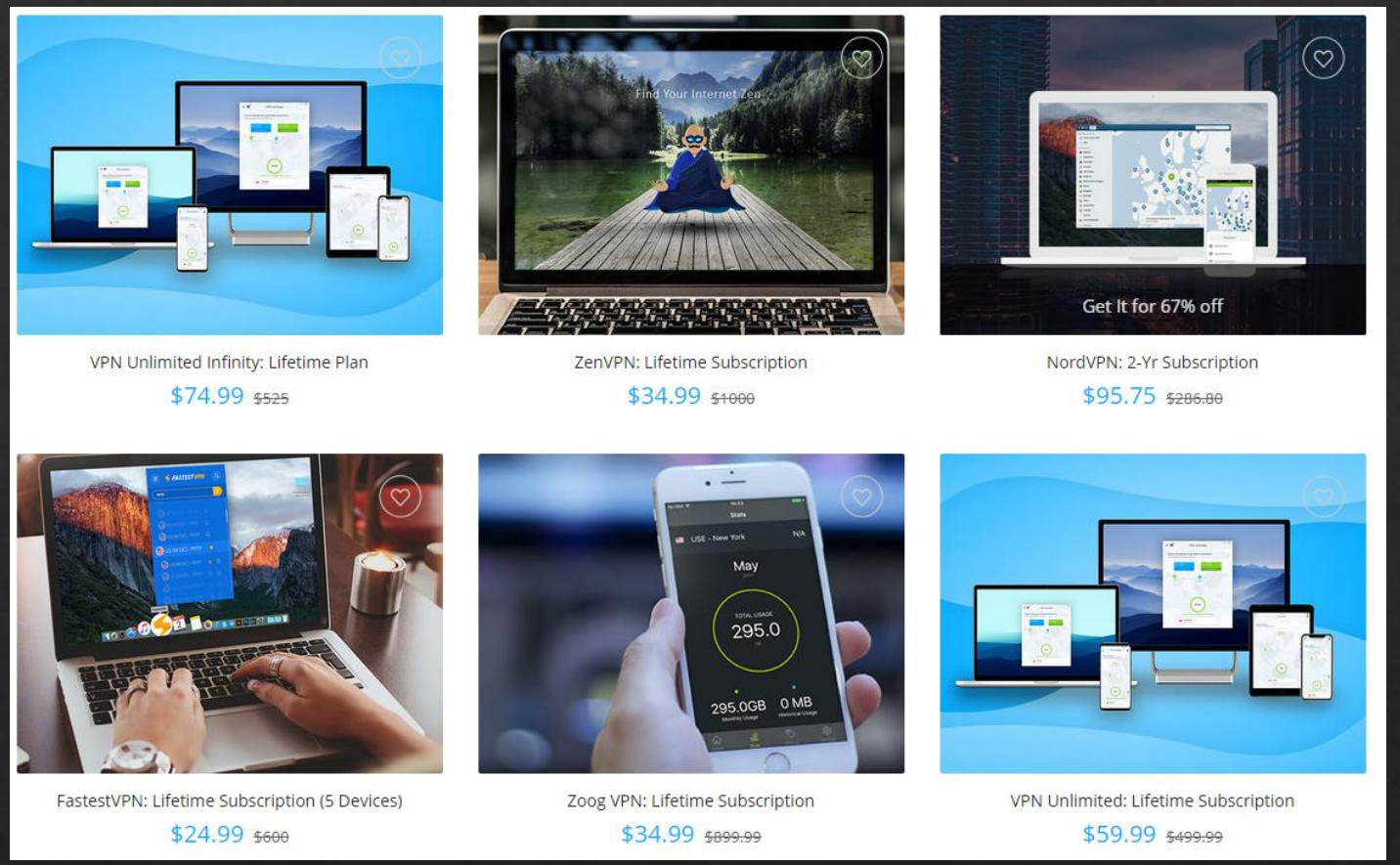
- Users have been systematically trained to click “Okay” to errors and warnings
  - Especially SSL certificate warnings – intranets, outdated systems etc.
- This means that the users are likely to ignore when they’re being intercepted!
- Some major online services have protections against this

Network sniffing countermeasures

- Solid networking gear – port security, shuts down ports in case of violation
- Monitor for ARP cache poisoning – IDS product, ARPwatch, Snort etc.
- Use encrypted protocols – use a VPN if you're on an untrusted network
- Train train train! Users are the #1 weakness in any system, don't indoctrinate them into ignoring warnings!
- DNSsec for your DNS servers – digitally signing replies from zones

A word on VPNs

- All you're doing is shifting your trust from the administrator of the local network to the administrator of your VPN service
- Is your data worth more or less than $25?
- Think about the running costs of a large-scale VPN service, bandwidth costs, server costs, legal fees etc.
- A lot of these services run on the business-model that a majority of users will never actually utilise them a lot in the long run
- Unsustainable?



VPN Unlimited Infinity: Lifetime Plan
$74.99 ~~$525~~

ZenVPN: Lifetime Subscription
$34.99 ~~$1000~~

NordVPN: 2-Yr Subscription
$95.75 ~~$286.80~~

FastestVPN: Lifetime Subscription (5 Devices)
$24.99 ~~$600~~

Zoog VPN: Lifetime Subscription
$34.99 ~~$899.99~~

VPN Unlimited: Lifetime Subscription
$59.99 ~~$499.99~~

- In no way am I saying that these specific services are illegitimate, but you must consider the implications of offering a lifetime service for $25

AGM – Elections!

- Do you think you could do a better job than us?
- Get voting on the 1st April at our usual session!
- Our AGM will be coming up in a few weeks time. So if you want to run for a committee position, start thinking about it now and nominate yourself if you're up for it. Preferably do this via e-mail or telling us in a session ASAP.
- A secret ballot will be held, and we will have the committee handover ready for the new academic year!

- We've only just really started and there's so much more we want to achieve! We want your input and ideas to make ShefESH a success for you and the future.

Now over to you!

- PCAP challenge can be found on the wiki under misc resources.
- 5 flags to find, ask us for help/hints, you might need to dig deeper for clues!
- First hint: it's Halloween themed

- If you've completed this challenge, try giving the FartKnocker box a go, this is a VulnHub machine that involves analysis PCAP files to find the correct ports to knock. Eventually you'll own the box, pending a few unexpected surprises! OVA file (~600MB) also on misc resources, or you can deploy it for free on TryHackMe (as KnockKnock). Also available locally.