Network Security 1: Introduction

i.g.batten@bham.ac.uk

Timetable Weirdness

Tues 1400 G33, Wed 0900 (sorry!) **Arts 125**. **But…**

19th January	Extra Lecture, 0900 Arts 223
23rd January	No Lecture
24th January	No Lecture
29th January	Extra Lecture, 0900 Arts 223
6th March	Lecture is in Aston Webb WG5
20th March	Lecture is in Aston Webb WG5

What this course is

- Enough network security that you could make a reasonable job of securing an enterprise network…
- …except you might need someone to help with the technical details of the precise hardware you are using.
- Emphasis on the **what** and the **why**, rather than the **how**. This is not a CCIE class.
- But we will get practical in some exercises.
- Caveat: 10 credits, right?

Requirements

- We are going to get our hands dirty with some Unix (Linux, although you can use MacOS or Solaris if you want, because pf and ipf are cool)
- It would be very, very helpful if you have a laptop which can run medium-size virtual machines, ideally two at a time.
- No programming requirements, although being able to script in bash/perl/python would be useful.
- I am assuming you've done my Networking course or similar, to the point you're familiar with TCP at a packet level.
- I'm also assuming you've taken either Secure System Management or Tom's second-year course, but I'll attempt to fill in the gaps for those of you that haven't. Hands up…?

What you will learn

- How to assess what needs securing (to a point)
- How to secure it
- How to test and evaluate the security
- Some realism in what does and does not work

Week 1

- All of this is slightly tentative as I want to make space for a much more in-depth look at webserver security than I have done in previous years.
- This introduction
- Assets, Threats, Risks: recap and focus on networks and network connected equipment

Week 2

- Host security: logging, patching, service minimisation
- Host security: least privilege, isolation, jails, zones, virtualisation, containers, etc

Week 3

- Defence in depth vs. multiple shallow defences. Attack trees. Side-channel and subsidiary protocols (some of you have seen some of this content before in SSM).
- Make a start on firewalling to introduce the exercise.
- **NB: actually Friday of Week 2, and Monday of Week 4**.

Week 4

- Firewalling: host, network. Design issues. Testing. IPv6 issues. Statefullness.
- Firewall implementation. Linux v everything else (IP stack v interfaces)

Week 5

- Network IPS/IDS, concepts and limitations. Host IDSes, Tripwire, etc.
- Admission control, Wireless authentication, Radius for 802.1x, WPA2/PSK, WPA2 Enterprise.

Week 6

- Data diodes, proxies, other firewall alternatives.
  - Some of this is necessarily speculative as data diodes are mostly custom for specialist customers.
- Web Server Security (HSTS, Content-Security-Policy).

Week 7

- Application security: application design, firewall friendliness, NAT friendliness
- Application security: TLS and authentication via certificates. OTP tokens. Oauth (maybe).

Week 8

- Denial of service, amplification attacks, mitigations, egress filtering for “good network citizens”
- Attacks on DNS
- Certification issues (HPKP and its problems, CAA, etc).

Week 9

- VPNs: concepts and components
- Probably start on IPsec

Week 10

- IPsec: concepts and components
- IPsec: Key exchange

Week 11

- VPNs: protocols (OpenVPN/SSL-VPN, IPsec, extensions to IPsec, IPv6 issues)
- Recap, exercise tutorial, spare

Books

- More resources on the net than in print
- Still recommend the Nutshell book “Practical Unix and Internet Security” by Garfinkel and Spafford, even though the technology is largely out of date.
- Also “Stalking the Wily Hacker” by Cheswick and Bellovin, with the same caveat.
- Ross Anderson’s “Security Engineering” (2nd Edition) is always worth reading

Assessment

- Due 12th February: building a firewall and testing it
- Due 12th March: IPsec configuration (probably, but possibly Content-Security-Policy depending on practicality)
- In each case, two week deadline, and a lecture of feedback and discussion.

Office Hours

- 1000–1200 Tuesdays and Wednesdays, CS room 132
- Or mail me and make an appointment
- Or just bang on my door (I now have a less scary photograph, apparently)

Lab Session

- 1100–1200 Mondays, UG04, when there is an exercise live and/or something useful to do.
- This clashes with Advanced Crypto: hands up? Proposals?

Timetable Weirdness

Tues 1400 G33, Wed 0900 (sorry!) **Arts 125**. **But…**

19th January	Extra Lecture, 0900 Arts 223
23rd January	No Lecture
24th January	No Lecture
29th January	Extra Lecture, 0900 Arts 223
6th March	Lecture is in Aston Webb WG5
20th March	Lecture is in Aston Webb WG5