FG: Was hat dir denn am besten gefallen in der Vorlesung, wo sollte ich dich viel fragen?
BS: Die Sachen mit Angrifftechniken, TCP/IP-Angriffe und so fand ich eigentlich am besten.
FG: Gut. Wenn man eine security policy hat, dann macht man sich ja z.B. darüber Gedanken, gegen wen man sich schützen will. Wir als Lufg i4, was für eine Angreiferklasse betrachten wir hier wohl hauptsächlich?
BS: Das wäre dann wohl der "grad student", also der Typ Hacker, der im Allgemeinen keinen großen Schaden anrichten will, sondern Systeme komprimittiert, um sein Können zu beweisen, und aus Spaß.
FG: Mal angenommen, du würdest gerne meine Emails mitlesen, wie könntest du da vorgehen?
BS: Ich könnte versuchen, mir entweder physischen Zugang zum Rechner zu verschaffen oder auch von remote, und dann durch Privilegieneskalation, Knacken von schwachen Passwörtern oder Ausnutzen von Schwachstellen genug Rechte zu erlangen, um Ihre Emails lesen zu können.
FG: Da wir hier ja alle Profis sind, haben wir im Allgemeinen gute Passwörter, die Systeme werden gut administriert und gepatcht, also so wirst du da vielleicht keinen Erfolg haben. Was könntest du anderes versuchen?
BS: Ich könnte versuchen, der Netzwerkverkehr irgendwo abzuhören, also Mit-Sniffen, und hoffen, dass ich Mails mitlesen kann oder sogar Passwörter für Ihren Mail-Account mitbekomme.
FG: Stimmt, da müsstest du also hier zum Lehrstuhl kommen, und dich umgucken, vielleicht hier und da mal fragen: "Wie habt ihr das denn hier mit dem Netzwerk gemacht, ich interessiere mich dafür.." usw.
BS: Ein bißchen social engineering betreiben.
FG: Genau, um genug Insiderkenntnisse zu erlangen, damit du das Netzwerk abhorchen kannst. Okay, mal angenommen, du wolltest verhindern, dass morgen eine Klausur von uns stattfindet, und du weißt, dass wir im Moment noch daran arbeiten. Wie müsstest du da vorgehen?
BS: Also die brutale Variante wäre, hier reinzukommen und die Rechner zu zerschlagen, Kabel herauszureißen und einfach alles unbrauchbar zu machen. Eine andere Möglichkeit wäre eine geeignete DoS Attacke.
FG: Was gibt es da so an DoS?
BS: Einige zielen auf die Überlastung des Netzes, andere auf die Überlastung von Kerneldatenstrukturen, und es gibt noch Mail- und Kompressionsbomben.
FG: Wie kannst du verhindern, dass du bei einer DoS Attacke auf das Netz nicht erwischt wirst?
BS: Durch IP Spoofing beispielsweise.
FG: Ist das schwer?
BS: Nein, die Konstruktion eines IP-Paketes mit gefälschter Absenderadresse ist trivial.
FG: Aber ist das nicht illegal?
BS: Wenn ich die Klausur verhindern will, dann werde ich auch davor nicht zurückschrecken.
FG: Stimmt. Erkläre doch mal die smurf-Attacke.
BS: Man schickt mit gespoofter Absenderadresse des Opfers einen Echo

Request an eine Broadcast-Adresse im Netz, woraufhin alle Rechner im Netz das Opfer mit Echo Reply's überlasten.
FG: Ok, sagen wir mal, das Rechenzentrum will Pakete mit gespooften Absenderadressen filtern, wie könnten sie das machen?
BS: Reverse DNS Lookup, ob die IP-Adresse überhaupt existiert vielleicht...
FG: Ich dachte eher daran, dass z.B. Pakete, die von außen kommen, aber IP-Adressen von Netz–internen Rechnern haben, gefiltert werden, da sie offensichtlich gespooft sind. Das geht über die Netzmaske des RWTH-Netzes. Geht das denn schnell?
BS: Ja, da müssen dann nur die Bits in der Netzmaske verglichen werden, geht also sehr schnell. Umgekehrt würde es auch funktionieren, also Traffic von intern nach extern mit externer Absenderadresse.
FG: Ja. Was ist ein anderer Ansatz, um IP-Spoofing von vornherein zu verhindern?
BS: Authentifikation, z.B. wie in IPv6. Da stellt man also fest, dass auch wirklich derjenige auf der anderen Seite der Verbindung ist, für den er sich ausgibt.
FG: Wie geht das z.B. in ssh?
BS: Zunächst erfolgt Hostauthentifikation, da generieren Host und Client mit asymmetrischer PK-Verschlüsselung (Diffie-Hellmann-Schlüsseltausch) mit ihren Public Keys einen gemeinsamen Session-Key, ohne dass der wirklich über die Verbindung geschickt wird. Dieser wird dann für die symmetrische Verschlüsselung der Verbindung benutzt.
FG: Und bin ich denn dann schon eingeloggt auf meinen Rechner, wenn das vorbei ist?
BS: Nein, dann muss man sich als Client beim Host auch authentifizieren, mittels Passwort oder auch mit Public Key Kryptographie.
FG: Hier am Lufg ist Pflicht, dass man dafür auch PK-Kryptographie nimmt, wie funktioniert das dann?
BS: Der Client weist nach, dass er den privaten Schlüssel zu einem öffentlichen Schlüssel, den der Host kennt, kennt.
FG: Wie? Was leistet PK-Kryptographie noch?
BS: Signierung.
FG: Ok. Wir waren vorhin beim Spoofing. Es gibt ja auch Arp-Spoofing, in welchem Kontext ist das vielleicht erwünscht.?
BS: Gratuitous ARP bei IP-Failover (erklärt).
FG: Okay, wenn man einen Angriff plant, was macht man dann meistens zuerst?
BS: Port scanning.
FG: Okay, damit das Opfer keinen Verdacht schöpft, gibt es ja z.B. das Decoy Scanning.
BS: Ja, da scannt man mit vielen gespooften Adressen gleichzeitig das Opfer, in der Hoffnung, dass dabei der Angriff nicht erkannt wird.
FG: Was kann man dagegen machen?
BS: Richtig konfigurierte IDS, z.B. snort mit entsprechenden Regeln, sollten auch ein Decoy-Scanning erkennen können.
FG: Es gibt ja dann auch noch das Idle Scanning, wie geht das?

BS: *erklärt mit Skizzen*
FG: Was muss für den Zombie gelten?
BS: Es sollte ein schlecht oder gar nicht administrierter Rechner sein, die IPID muss vorhersagbar sein, und es sollte kein anderer Traffic stattfinden, da sonst das Idle Scanning nicht funktioniert.
FG: Okay, es gibt ja bei nmap diese Funktion, dass das Betriebssystem des Opfers bestimmt wird, wie geht denn das?
BS: Also zunächst mal z.B. durch die Art, wie sich die IPID verhält, das ist bei unterschiedlichen OS mitunter unterschiedlich. Außerdem verhalten sich vielleicht nicht alle OS RFC-konform, oder reagieren jedenfalls unterschiedlich auf verschiedene Pakete und Situationen, so dass man da mit einer Heuristik das OS ziemlich gut erraten kann.
FG: Okay, bitte mal kurz rausgehen.*30 Sekunden später:* Okay, bitte wieder herein: Bestanden.
Ich habe dich ja vor allem aus deinem "Spezial-Gebiet" gefragt, und da wusstest du auch so ziemlich alles. In einer Diplomprüfung würde ich sicher auch in den Fehlertoleranzteil noch reingehen, z.B. wie berechnet man die MTTF von RAID 5, oder wie bestimt man die availability aus der Zuverlässigkeitsfunktion berechnet, so was in der Art.

Prof. Freiling (Gärtner) war ein sehr angenehmer Prüfer, mit den Anwendungszenarien fällt einem der Einstieg in die Thematik leicht und man kommt gut die Prüfung rein. Die Fragen lassen genug Spielraum, so dass man ruhig schonmal länger reden kann, ohne unterbrochen zu werden, weil man abschweift. Auch das Feedback am Ende war gut, so dass ich jedem nur empfehlen kann, die Scheinprüfung zu machen, sollte er Prof. Freiling auch als Diplomprüfer in Betracht ziehen. Hilft sicher bei der echten Prüfung und mit einer Woche intensivem Lernen kann man den Stoff von VVS 1 gut durcharbeiten, um die Scheinprüfung ohne größere Probleme zu bestehen.