Module 3
(Ground Rules and Rules of Engagement)

• At the end of this module, you should have a good idea of how to lay out the ground rules for a penetration test and what issues must be addressed by your rules of engagement.
Verifying IP Address Ranges

• It is absolutely critical that when carrying out a penetration test, you test the correct machines.

• Companies may try to give you a single domain name and ask you to hack in *just like the bad guys do.* (Kevin Johnson: “Does that mean I get to sell all the information I find, just like the bad guys do?”)

• Third Parties abound. You need their permission as well:
  - Cloud services
  - ISP
  - Web Hosting
  - Managed Security Services Providers (MSSPs)
  - Know what countries these machines are in and know their laws.
Social Engineering Pretexts

- Companies may be sensitive about what ways of fooling their employees are appropriate.
- Explain current popular phishing exploits.
- Some pretexts may use sensitive content (e.g. sexual performance enhancement, pornographic services, etc.) that companies do not want to impose on their employees.
- Make sure that any pretexts to be used in phishing are approved. In particular, get specific approval of every phishing message to be sent.
Communication and Contact Information

- Identify how and how often information will be conveyed concerning the state of the penetration test.
- Provide contact information about everyone involved in the penetration test including emergency contact information.
  - Name
  - Title
  - Emergency contact information (24/7)
  - Secure bulk data transfer method (sftp or encrypted email)
- Agree to an incident reporting process
- Share encryption keys. (Not an option.)
Rules of Engagement

- Timeline for the test.
- Locations (if on-site)
- Method of disclosure of sensitive information. Data may be protected by HIPAA. Avoid copying personal health information (PHI) and other personally identifiable information (PII).
- Evidence handling (use encryption)
- Regular status meetings
- Time of day to test
- Dealing with shunning
- Permission to test (including scope and possible negative outcomes of testing such as system instability, crashes, etc.)
- Legal considerations (wiretapping laws, etc.)
Testing the Customers Detection Capabilities

- Ability to detect and respond to information gathering
- Ability to detect and respond to foot printing
- Ability to detect and respond to scanning and vulnerability analysis
- Ability to detect and respond to infiltration (attacks)
- Ability to detect and respond to data aggregation
- Ability to detect and respond to data ex-filtration