

Assignment #5, COMP 5370/6270
Instructor: A. Skjellum; TA: A. Ravipati
Assigned: October 9, 2015
Due: October 23, 2015

Problems 1-4: 25 points each for Ugrads, 20 points each for Grads.

1. Learn & describe what is information foot printing. How does it help crackers vs hackers.

*Note: Definition of cracker and hacker in this context: Cracker – (Black Hat hacker)
The intention of cracker is to breach or bypass internet security for malicious gains.*

*Hacker – (White Hat Hacker) The intentions of hacker is to explore vulnerabilities
and take measures to patch the vulnerabilities.*

2. Learn about Whois, Nslookup, traceroute? Explain functions of each term.
3. What is Nmap?
4. <http://mxtoolbox.com/SuperTool.aspx> - Use this tool and write a report.

Steps to make a report using Super tool -

- Consider 3 or more domains (ex: Google, AUBURN.EDU, UA.EDU, Wikipedia.org, one you choose)
- Use Blacklists - Learn about any two blacklists and what they black list, and what it means to black list. What is grey listing?
- Analyze an email header - see DKIM signature. Using online resources to learn what DKIM is and how a DKIM signature helps.
- Goto more> Network > what is my ip . Learn about what information can be extracted if you know an IP address.
- The conclusion of your report should explain what the tool is about. How can it be used in securing any individual domain..

5. Problem Required for Graduate students (extra credit for Ugrad) – 20 points.

Study: <https://dmarc.org/>

See: <http://www.mcafee.com/us/resources/solution-briefs/sb-spf-dkim-dmarc-demystified.pdf>

Compare and contrast to DMARC, DKIM, SFP.

6. Extra Credit Problem (Ugrad and Grad) -10 points max.

Study DNS and what it does, and find some attacks against it. Why are attacks on DNS a big danger?

See: https://en.wikipedia.org/wiki/Domain_Name_System

See: https://en.wikipedia.org/wiki/DNS_spoofing

Try the Super Tool (see above) to discover properties of DNS (e.g., errors).