Erik Buschardt

Final Exam & Presentation

CSSS 5990 §08

Adv Topics / Malware

Fall II 2016

Webster University

12/12/16 7:30pm & REVISED & Questions

Final Presentation

Not allowed to do (6) Action Obj... whoops!

---

① Choose 2 phases: Recon, Delivery.

② a) Describe Recon & Deliv from ATK view pt

b) Explain link between phases & Malware used by cyber criminals

Delivery is performed via methodologies learned via recon phase (correct environment, ~~correct~~ effective format, etc.)

c) Define defenders goals for both phases:

Recon	Observe excessive logins for example abnormal behaviors
Deliv	edu users not to click emails! ~~Or install~~ etc.

d) Describe how one would achieve goals using P/P/Tech

Please see next page. (Matrix)

12/12/16 4 PM

Final Presentation

Inst/C2 is 1 phase.

1) Choose 2 diff phases of KC except last phase: Recon & Action.

2) Deliver a presentation regarding the following:

a) Describe Recon and Action from attackers view

→ b) Explain link between phases & Malware used by Cyber Criminals

Actionable objectives on Advanced Persistent Targets are carried out via weaponized payloads. These payloads are designed using specifications against a target infrastructure gathered during the Reconnaissance phase.

c) Define defenders goals for both of your phases

	How to defend against threats both known and unknown?	Chosen.
Recon	Education of users on abnormal activities such as multiple login attempts	
Action	Attempt to migitate breach(es), implement Detection & response action plans, IR/DR/BC, etc.	

d) Describe how one would achieve the goals using people, processes & technology.

Please see next page.

12/5 ✓ = Confident of mastery (self)

Examples of Potential Questions

1. What is a botnet and what are botnets typically used for? ✓

171.161.160.10
sproxy1.bankofamerica.com

2. Your company's CEO can't access his bank's website because your DNS server is down. You have the IP Address of the website stored. Explain a temporary workaround for the CEO. ✓

Use numeric addresses or 8.8.8.8 Google Public DNS ~~Proxy gateway~~ also 8.8.4.4 also IPv6 are online.

3. Describe your understanding of a client-server architecture. ✓

4. Is it possible to embed a payload in another payload? Provide supporting reasons for your answer - yes or no. ✓

5. Summarize the difference between a reverse shell and shellcode. Which one is the function and which is the format? ✓

6. What are the three solution components for defending in each of the Kill Chain phases? What are the goals of the attacker or defender in each phase? PPT/... ✓

7. Maltego is used for what? ✓ Maltego Carbon CE traces relationships between online entities such as GPS, Social media, network infrastructure, etc.

8. TOR is used for what? Explain. ✓ The Onion Router
Used to ~~make~~ enable anonymous communication.

9. Explain the role of people, process, and technology in the defending against malware. ✓

10. Provide one example of an IOC in one phase of the Kill Chain. ✓ (clicking on link from email)
(Delivery) installation of a malicious package by a user

11. Give two common tell tale signs that an email is a phishing email. ✓
~~Quite~~ Common misspellings, lots of images, unusual sender address

12. Provide one example of the difference between wireshark capture and display filters. ✓

13. Name one use for the Social Engineering Toolkit, (SET). ZK things.

14. Describe how LinkedIn can be used as a honey pot. Human honey pot ✓

15. In your opinion, what is the most important phase of the Kill Chain? Defend your answer. ✓
Using passive recon to learn what technologies are used in the ~~co~~company.

16. Define what is meant by post-exploitation activities. ✓

Attacker point of view

Recon ~~Ch~~ Lincoln: 6 hrs chop tree, 4 hrs sharpen ax. to carry out intended objectives of the payload.

12/12 | Finals Questions (Polishing Up!)

(6) What are the three solution components for defending in each of the LM KC phases? What are the (overall/high level) goals of the attacker vs. defender in each phase?

	People (education)	Process (policies)	Technology (tools)
GOALS (Atk)	• Social engineering • recognize (auth) attempts/abnormalities	• Taking adv of possible lackluster training • Recon: Enforcement? Taking adv of	• Based on Recon, build Weaponization tools
GOALS (Def)	• Train on common cybersec best practices	• ~~Patch~~ Ensure 100% mandatory compliance • IR/DR/BC Processes	• Based on red-team Pen testing etc, refine ~~not~~ defenses in network architecture.

(9) Explain the role of people, processes & technology in defending against malware?

People: Educate users (in particular cyber pros) to recognize attempts & abnormalities.

Processes: Design & implement policies to counter anticipated threats towards known vulnerabilities.

Technology: Build & deploy tools that will mitigate these threats.

(13) Name one (1) use for the Social Engineering Toolkit (SET).

SET is specifically designed to perform advanced attacks against the human element. SET was designed to be released with the launch of Social-engineer.org website, and is a standard tool of the penetration-testing toolkit.

Self Grade 23/25 Objectives 4.5/5

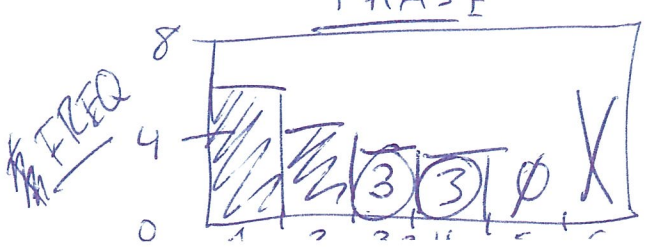
12/12 # LMKC Matrix for Final exam subset (2 phases) Compare & contrast:

Finals presentations evening: Recap

Presenter	Phases introduced
1) Durgesh	1, 4
2) Jasmin	1, 2
3) Com	1, 2
4) Amber	3, 4
→ 5) Erik	1, ~~4~~ 3 (Action/Obj not allowed. Too obvious)
6) Saulo	~~3~~, 3, 4
7) Ahmed	1, 2
8) Robyn	1, 2

Limit
1 recon ✓
2 weap ✓
3 deliv ✓
4 exploit
5 install/C2
6 Action obj

Objectives
- Explain 2 phases each given phase describe 1 from attackers & defenders POV
- Compare & contrast
- Q & A



← Histogram

3) Delivery

Analogy

Trojan horse delivered inside Castle gates

Goals	People	Process	Technology
Attack			email
Defend			

Erik Buschardt	Comments
Presentation	Good opening with objectives. Multiple uses of notes.
Application of Principles	Very Good. Impressive.
Use of Analogies and Stories	Server in a restaurant analogy. Fake news.
Responses to Questions	Botnet. Client - Server IoE Kali Linux. File Carving. False true.
Confidence of Delivery	Very Good.

-1