**1. Describe in detail possible attacks against LM, NTLM and Kerberos.**

NTLM refers to the networking authentication protocols designed for devices operating on windows platform, and windows based standalone systems. It is mainly used for login sessions and its credentials are dependent on data acquired on the login process; username, domain name, and one-way password hash. (Satran, 2018)

The first attack on this is the “mimikatz” malware which is basically designed to extract plain text from the hashed passwords, passphrases, security codes, and Kerberos tickets from computer memories. in windows operating system security, (Metcalf, 2018). It is designed in C and can trigger tickets; golden and silver tickets, (GitHub, 2018).

The second most common type of attack is the Trojan Horse malware, (Malware-traffic-analysis.net, 2018). Trojan horse malware is capable of taking advantage of both the LM, NTLM; infect computers networks and spreads itself. We can trace this malware using Wireshark. This method can be implemented together with a program like “MimiKatz” to breach AD, LM, NTLM and Kerberos security. According to the training exercise, (Malware-traffic-analysis.net, 2018), this method can be used in multiple scenarios to infect the mentioned windows security technologies. In the linked posted above, there is a training exercise where you download a packet log and analyze the data provided.

**2. Explain the difference between cooperative multitasking and preemptive multitasking. What are security implications of each? Which method is more secure?**

Cooperative multitasking, also referred to as non-preemptive multitasking, is a computer process multitasking criteria where the operating system does not interfere with the running process on the CPU; no context-switching from running process to the next on the queue, a task switch can only be done only when the current task calls the kernel (En.wikipedia.org, 2018). It operated cooperatively and one process voluntarily gives the kernel a chance to perform the task switch. On the other hand, preemptive multitasking allows task switches to be initiated directly from the interrupt handler, (On-time.com, 2018).

The main advantage of preemptive scheduling is the fast/real-time response on the task level, it has a short response time to new tasks. A task waiting for an interrupt is activated depending on the interrupt latency or the delay during which no other process interrupt can be accepted. With cooperative, substantially less re-entrance problems can occur than preemptive as tasks cannot arbitrarily be interrupted by other processes, but only when and where the programmer allows; like upon kernel calls, though this does not apply to multiprocessor kernel. (On-time.com, 2018). Cooperative is not widely used since all the programs needs to cooperate for the scheme to work, hence preemptive is the best and secure.

The application of cooperate multitasking is widely used in memory-constrained embedded systems and specific applications like JES2 and CICS subsystems. It was primarily designed for 16-bits windows application.

**3. Expand on what a memory leak is, how it is caused**

Memory leaks refer to the kind of a bug in which the application fails to release the memory when it’s no longer needed. With time these bugs cause failure to the application as well as the operating system which is caused by eventual memory leaks that affect the performance of both specific application and the operating system causing a large leak that might hence result in unacceptable response time because of the excess paging.

Secondly, a memory leak can occur in the essence where all available RAM get used causing degrade in its performance. This is caused when the software fails to manage the present ram correctly. Without any alert as the computer functions normally the ram gets used by software in a dynamic fashion, and memory resources are allocated as needed. In a situation with a memory leak, RAM gets allocated to the software but is not freed up when no longer needed hence dysfunctional.

Lastly memory leak is an unintentional form of memory consumption in which the developer fails to free an allocated block of memory when it is no longer needed. Therefore, the consequences of such an issue rely on the application itself.”

Memory Leaks have two common and sometimes overlapping causes which include error conditions and other exceptional circumstances and the confusion over which part of the program is responsible for freeing the memory

consequently, most memory leaks result in a general software reliability problem, so if an attacker intentionally triggers a memory leak, it might be able to launch crashing to the program or cause other unexpected program behavior resulting from a low memory condition.

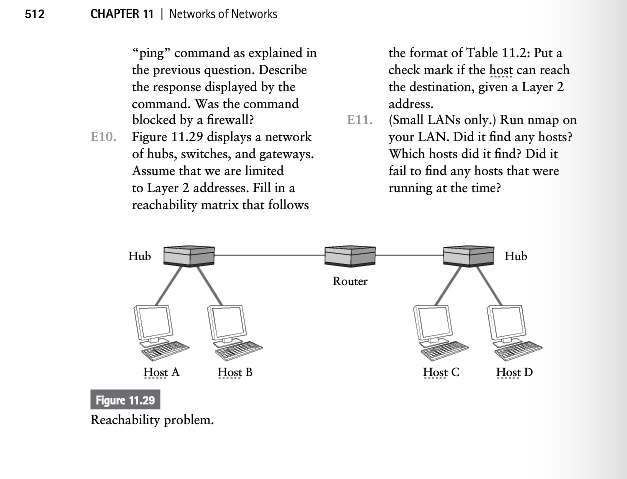
**4. What types of challenges does a zero-day exploit present to an organization? How are APT attacks different then Zues attacks?**

Zero-day exploit is the code used by attackers to exploit zero-day vulnerability (security flaw in software applications that the owner or antivirus vendors has no idea about its existence). Hackers use this flaw to gain access, install malwares to devices, carry out attacks, and compromise sensitive data. ("What is a Zero-day? A definition of Zero-day Exploits & Vulnerabilities", 2018)

Zeus refers to a malware which infects computer systems, changing them into Zombies that remain unusable. The infected computer becomes a Zombie with ZeuS or ZBOT Trojan and are part of the botnet. They come from spam which comes as a program from legitimate sources tricking targets to click links, ad their main purpose is to steal account information or data. Apparently, the Botnet itself has grown in size and subsequently the target range. ("The ZeuS, ZBOT, and Kneber Connection - Threat Encyclopedia - Trend Micro USA", 2018).

ARP refers to an advanced persistent threat made up of highly skilled individuals who can use their skills, and from access points, bypass the set security or defense measures, then breach the network in a short time. Additionally, these individuals can stay stealthy for a long period of time. They have knowledge of malwares, servers, and they can use different procedures and tools to apply their schemes to manipulate the network. (Threats, 2018). It can also be defined as a prolonged and aimed attack on a target with the intent to breach the security system and gain access to target infrastructure and information. (Arntz & Arntz, 2018). Basically, in my own words, APT would be a threat actor targeting a system for an extended period of time and trying to search for weaknesses that can circumvent defenses. This is very different than Zeus which is a type of Malware which can be used for the purpose of APT. According to Symantec, Zeus is a piece of malware dating back to Windows XP/Me and tries to send HTTP activity via the use of the ZLob Trojan. ("System Infected: Trojan Zeus Activity: Attack Signature - Symantec Corp.", 2018)

**5. Refer to Figure 11.29 (Pg 512) in your book, this figure displays a network of hubs, switches and gateways’s. Assume that we are limited to Layer 2 addresses. Fill in a reachability matrix that follows the format of Table 11.2 (pg 500). Put a check mark if the host can reach the destination, given a Layer 2 address.**

****

1. Do Exercise 6 from Chapter 8 (pg 371) of the book.
2. Do Exercise 8 from Chapter 9 (pg 423) of the book.
3. Pick a public spot (mall, store, park etc…) and note it’s location (name). Use a laptop or other device to identify wireless LAN’s in that area. For each LAN you find, try to determine:
   1. Its effectiveness in coverage and availability
   2. Describe security measures, if any like the type of encryption used
4. Company ACME, wants to protect the data link when employee’s visit the company website to work from home. Alice argues for using SSL and Tina argues for using IPSec.
   1. List arguments Alice might use in favor of SSL
   2. List arguments Tina might use in favor of IPSec
5. Decode the below ciphertext which is encoded using XOR with a key of 0x21.

**Ciphertext =** 0x68 0x03 0x4C 0x7E 0x46 0x4E 0x48 0x4F 0x46 0x7E 0x55 0x4E 0x7E 0x4C 0x40 0x4A 0x44 0x7E 0x49 0x48 0x4C 0x7E 0x40 0x4F 0x7E 0x4E 0x47 0x47 0x44 0x53 0x7E 0x49 0x44 0x7E 0x42 0x40 0x4F 0x03 0x55 0x7E 0x53 0x44 0x47 0x54 0x52 0x44

**Additional Questions**

1. Explain the difference between /etc/passwd and /etc/shadow. How /etc/shadow is implemented?
2. Describe in detail the boot process for Windows XP operating system. What security implications are here? (Think rootkits)
3. Explain superblock with respect to Linux filesystem.
4. Research about IPv6 and describe the key reasons behind its design and implementation. How is it more secure then IPv4?
5. What are the features and differences of the following routing protocols RIP, IGRP and OSPF.
6. What is malware reverse engineering? Explain to me the different types of analysis and the goals?
7. How can digital forensics be used to investigate intrusions? How does it differ from criminal digital forensics?

Bonus/Challenge Question:

Write a script Program to solve Mandatory Question #11.

**Reference:**

Satran, M. (2018). Microsoft NTLM. [online] Docs.microsoft.com. Available at: https://docs.microsoft.com/en-us/windows/desktop/SecAuthN/microsoft-ntlm [Accessed 11 Jul. 2018].

GitHub. (2018). gentilkiwi/mimikatz. [online] Available at: https://github.com/gentilkiwi/mimikatz [Accessed 11 Jul. 2018].

Metcalf, S. (2018). Mimikatz and Active Directory Kerberos Attacks – Active Directory Security. [online] Adsecurity.org. Available at: https://adsecurity.org/?p=556 [Accessed 11 Jul. 2018].

Malware-traffic-analysis.net. (2018). Malware-Traffic-Analysis.net - Traffic Analysis Exercises. [online] Available at: https://www.malware-traffic-analysis.net/training-exercises.html [Accessed 11 Jul. 2018].

Malware-traffic-analysis.net. (2018). Malware-Traffic-Analysis.net - 2018-01-18 - Traffic analysis exercise - "Mars Smart". [online] Available at: https://www.malware-traffic-analysis.net/2018/01/16/index2.html [Accessed 11 Jul. 2018].

En.wikipedia.org. (2018). Cooperative multitasking. [online] Available at: https://en.wikipedia.org/wiki/Cooperative\_multitasking [Accessed 11 Jul. 2018].

On-time.com. (2018). Preemptive or Cooperative Multitasking? [online] Available at: http://www.on-time.com/rtos-32-docs/rtkernel-32/programming-manual/advanced-topics/preemptive-or-cooperative-multitasking.htm [Accessed 11 Jul. 2018].

On-time.com. (2018). Preemptive or Cooperative Multitasking?. [online] Available at: http://www.on-time.com/rtos-32-docs/rtkernel-32/programming-manual/advanced-topics/preemptive-or-cooperative-multitasking.htm [Accessed 11 Jul. 2018].

Threats, A. (2018). Anatomy of an APT (Advanced Persistent Threat) Attack | FireEye. Retrieved from https://www.fireeye.com/current-threats/anatomy-of-a-cyber-attack.html

Arntz, P., & Arntz, P. (2018). Explained: Advanced Persistent Threat (APT) - Malwarebytes Labs. Retrieved from https://blog.malwarebytes.com/cybercrime/malware/2016/07/explained-advanced-persistent-threat-apt/

System Infected: Trojan Zeus Activity: Attack Signature - Symantec Corp. (2018). Retrieved from https://www.symantec.com/security\_response/attacksignatures/detail.jsp?asid=24265

The ZeuS, ZBOT, and Kneber Connection - Threat Encyclopedia - Trend Micro USA. (2018). Retrieved from https://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/16/the-zeus-zbot-and-kneber-connection

What is a Zero-day? A definition of Zero-day Exploits & Vulnerabilities. (2018). Retrieved from https://digitalguardian.com/blog/what-zero-day-definition-zero-day-exploits-vulnerabilities