CySA+

Cybersecurity Analyst

CCI
Post Office Box 9627
Mississippi State, MS 39762

CySA+

Part 1

Threat Management

Securing a Corporate Network

Chapter 4

Outline

- Penetration Testing
- Reverse Engineering
- Training and Exercises
- Risk Evaluations

Securing a Corporate Network

- **An analyst’s job is a part of securing a corporate network, which includes**
  - **Penetration testing**
  - **Reverse engineering malware**
  - **Training and exercises**
  - **Risks evaluations**

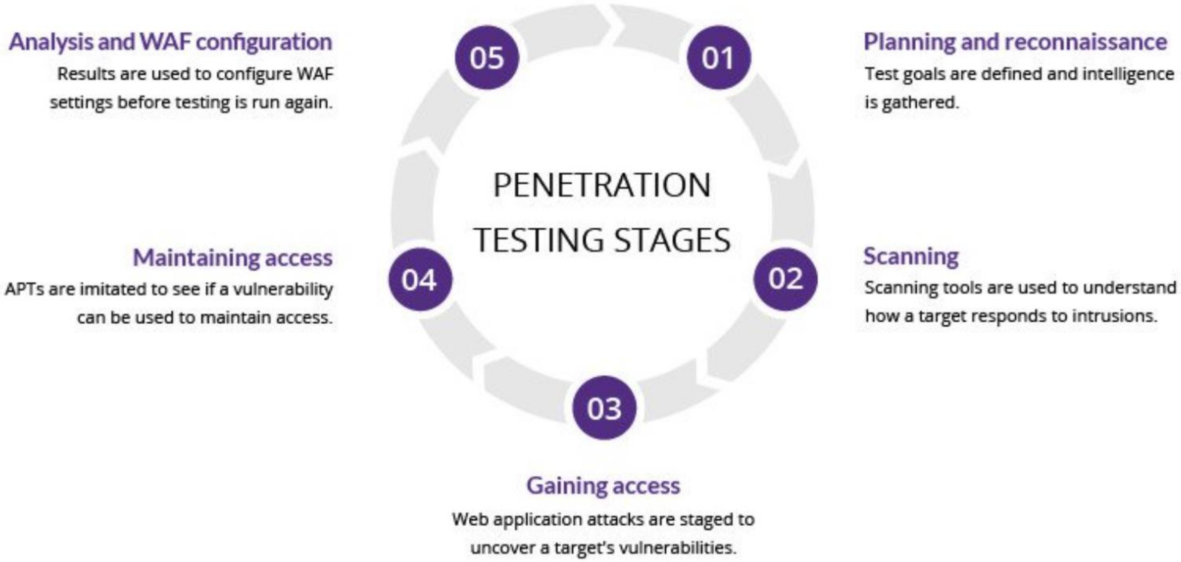
[1]

Penetration Testing

- **Pen testing**
  - **Testing the security of the organization through realistic attacks using hacking tactics, techniques, and procedures (TTPs)**
    - **Third party organizations are often hired to perform vulnerability and penetration testing**
    - **Can be intrusive and disruptive to the organization**
  - **Used to evaluate the security of**
    - **Web servers, DNS servers, Router configurations, Workstation vulnerability, Access to sensitive information, Remote dial-in access, Open ports, Properties of available services**
  - **At the end of the test, a report is given to management with**
    - **Details on all identified vulnerabilities**
    - **The severity of those vulnerabilities**
    - **Suggestion for remediation**

[1]

Penetration Testing Methodology ex.



PENETRATION TESTING STAGES

01 Planning and reconnaissance
Test goals are defined and intelligence is gathered.

02 Scanning
Scanning tools are used to understand how a target responds to intrusions.

03 Gaining access
Web application attacks are staged to uncover a target's vulnerabilities.

04 Maintaining access
APTs are imitated to see if a vulnerability can be used to maintain access.

05 Analysis and WAF configuration
Results are used to configure WAF settings before testing is run again.

[2]

Penetration Testing

- **The kill chain**
  1. **Reconnaissance**
     - **Footprinting and gathering information about the target**
  2. **Exploitation**
     - **Compromising a security control or otherwise gaining illicit access**
  3. **Lateral Movement**
     - **Compromising additional systems from the exploited system**
  4. **Report to Management**
     - **Delivering to management documentation**

[1]

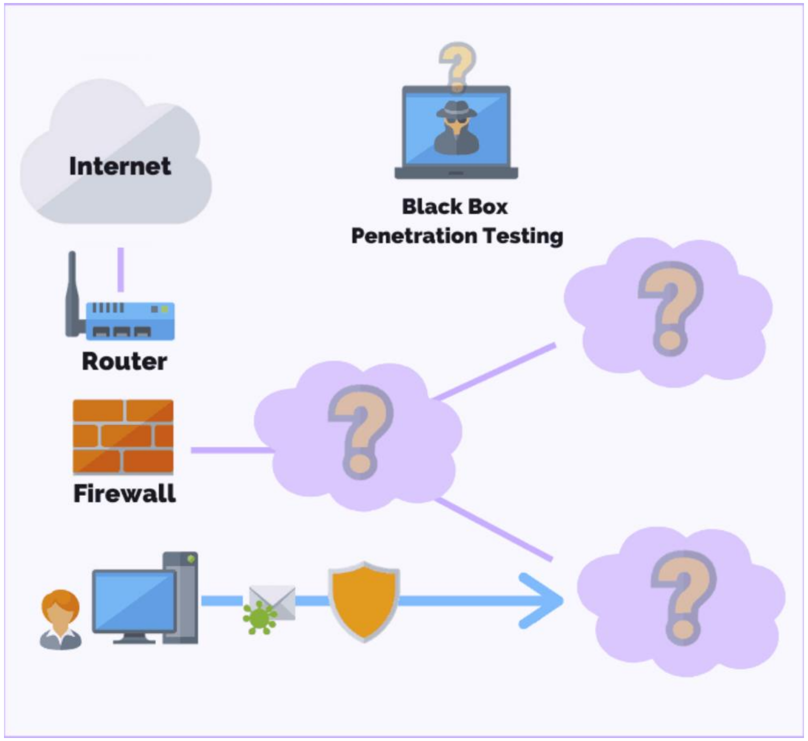
Penetration Testing

- The different degrees of knowledge of the target before performing a pen test
  - Zero-Knowledge
    - Also known as black-box pen testing
  - Partial Knowledge
    - Also known as gray-box pen testing
  - Full Knowledge
    - Also known as white-box pen testing

[1]

Black-Box Pen Testing Visualization

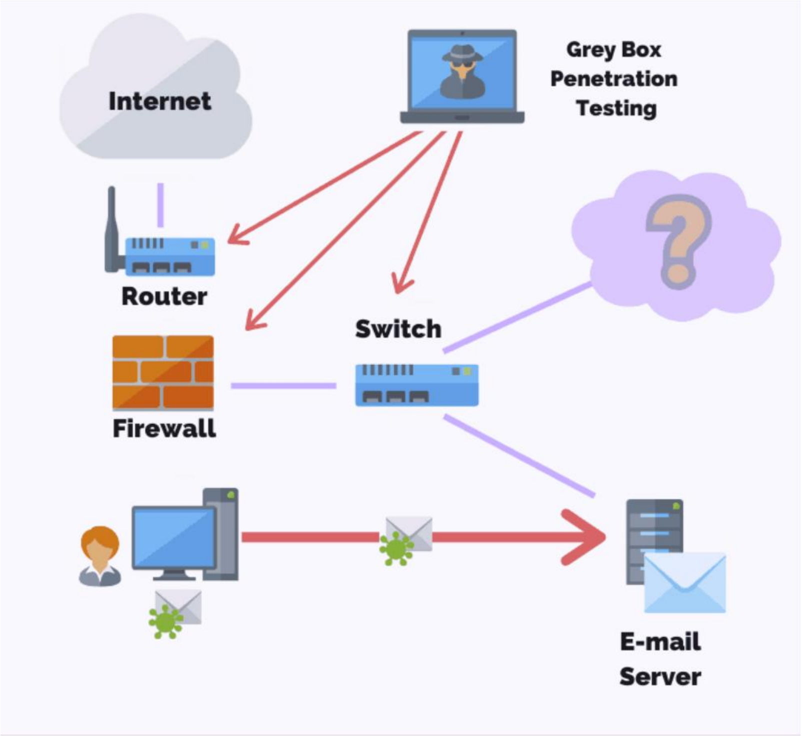
- **The pen testers do not have any knowledge of the target**



[3]

Gray-Box Pen Testing Visualization

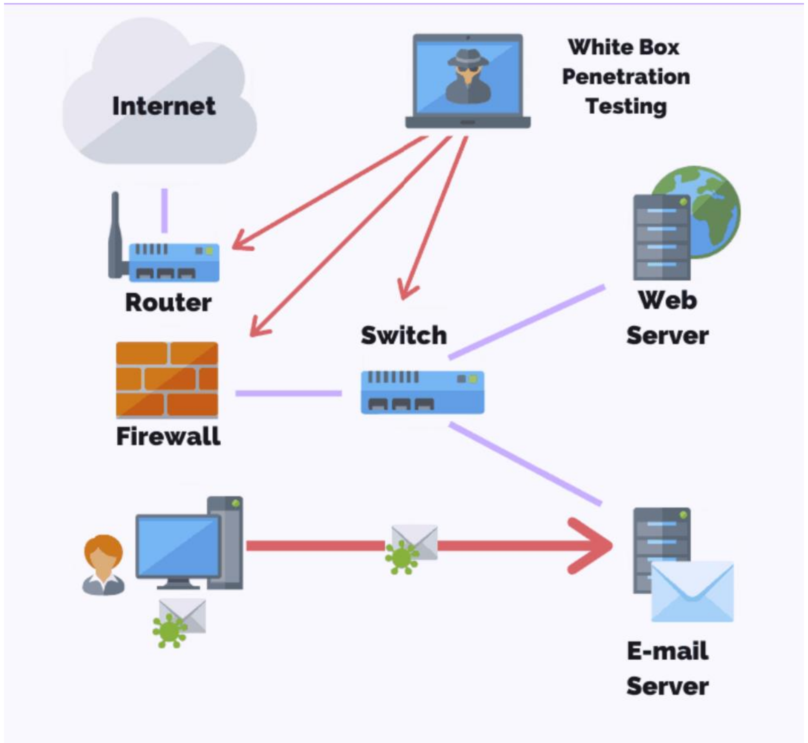
- **The pen testers have some knowledge of the target**



[3]

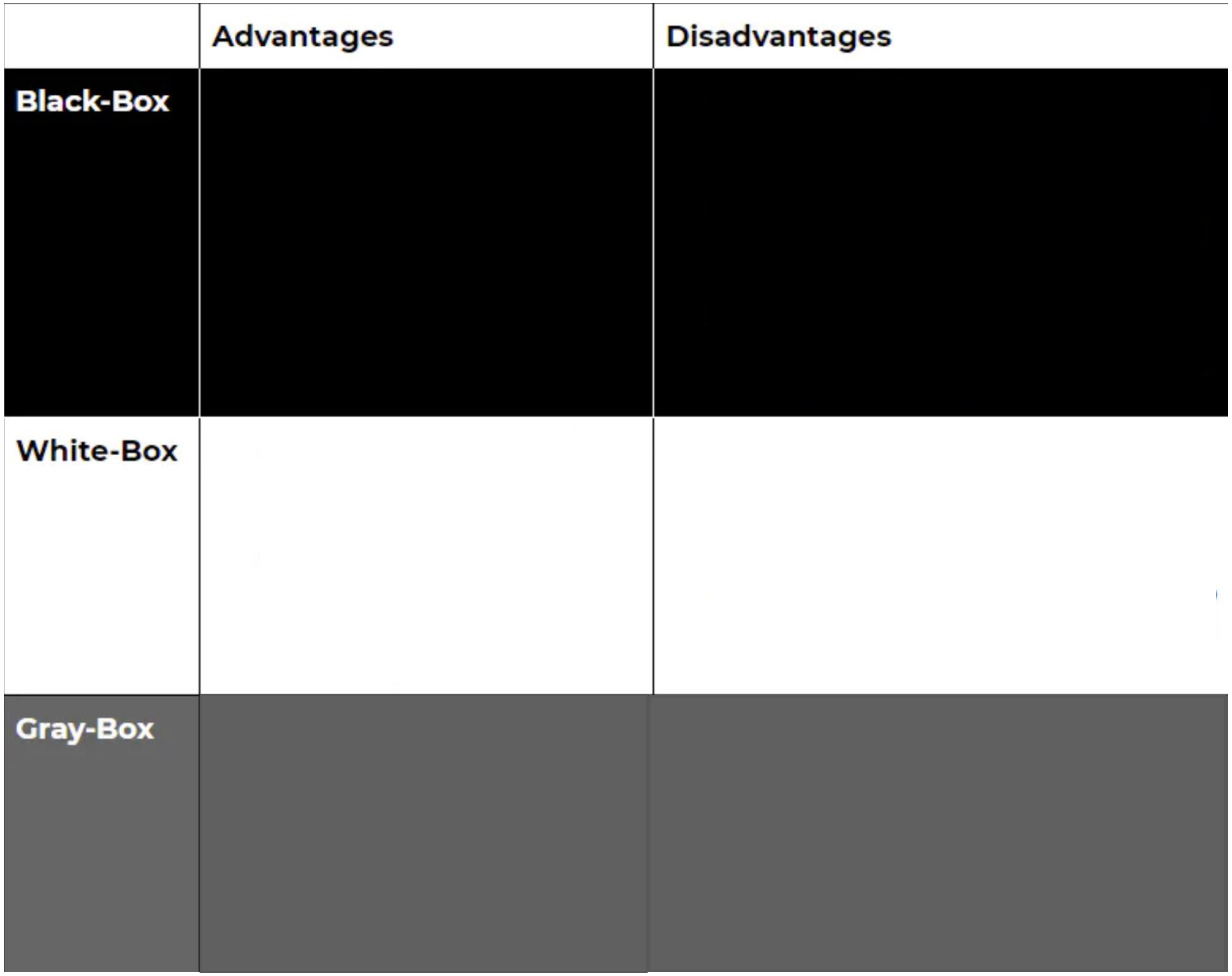
White-Box Pen Testing Visualization

- **The pen testers have intimate knowledge of the target**



[3]

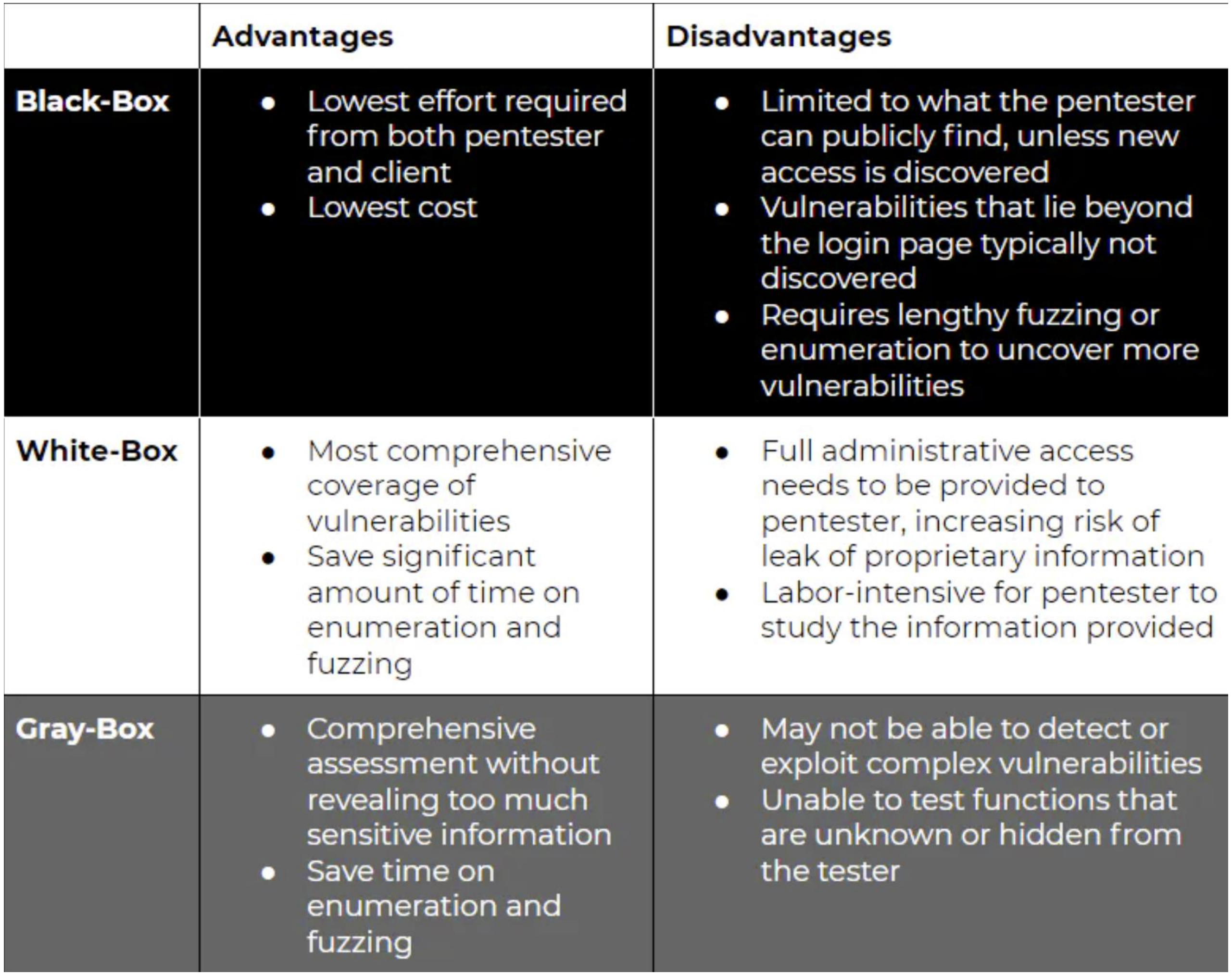
Box Pen Testing Brainstorming EX



	Advantages	Disadvantages
Black-Box		
White-Box		
Gray-Box		

[4]

Box Pen Testing Brainstorming ANS



	Advantages	Disadvantages
Black-Box	• Lowest effort required from both pentester and client • Lowest cost	• Limited to what the pentester can publicly find, unless new access is discovered • Vulnerabilities that lie beyond the login page typically not discovered • Requires lengthy fuzzing or enumeration to uncover more vulnerabilities
White-Box	• Most comprehensive coverage of vulnerabilities • Save significant amount of time on enumeration and fuzzing	• Full administrative access needs to be provided to pentester, increasing risk of leak of proprietary information • Labor-intensive for pentester to study the information provided
Gray-Box	• Comprehensive assessment without revealing too much sensitive information • Save time on enumeration and fuzzing	• May not be able to detect or exploit complex vulnerabilities • Unable to test functions that are unknown or hidden from the tester

[4]

Penetration Testing

- Rules of Engagement
  - Before pen-testing an organization clearly define
    - Timing
    - Scope
    - Authorizations
    - Exploitation techniques
    - Communication mechanisms
  - Pen testing the wrong target in the organization at the wrong time, would hurt the organization rather than helping it
  - Example
    - Bring down service at an inopportune time the company could lose money

[1]

Penetration Testing

- **Timing**
  - **Timing Considerations**
    - **Scope dictates the minimum downtime duration**
      - **Example: Pen testing on a regional bank can be performed more quickly than on a large multinational corporation**
    - **Balancing the number of risks being tested against the number of days**
    - **Must take extra care if pen-testing during business hours**
    - **Conducting test after working hours will lessen the value of the training for the organization's defenders**
    - **Pen testing during times that the organization has seen the most attacks**

[1]

Penetration Testing

- Scope
  - Ensure that the target is not part of the organization’s outsourced information infrastructure
  - Two questions to ask
    - What is in scope?
      - An organization may provide pen testers with a list of IP subnets that can be targeted
    - What is out of scope?
      - It is important to know what cannot be targeted such as, personal healthcare information (PHI)
  - Whitelist systems
    - Only the systems on the whitelist can be targeted
  - Blacklist systems
    - None of the systems on the blacklist can be targeted

[1]

Penetration Testing

- Authorization
  - Pen testing can be hazardous to the organization
    - Systems or services may be inadvertently taken down
  - Ensure senior management is aware of the penetration test
  - Obtain an authorization letter or memo from the organization
    - This type of letter is called a "Get Out of Jail Free Card."
    - The pen testing team should all have a copy of this letter
    - Should include
      - Contact information for key personnel
      - A call tree in the case something does go wrong

[1]

Penetration Testing

- **Exploitation**
  - Utilizing a vulnerability found in the target machine to cause unintended, unanticipated, or unauthorized behavior
  - Involves a compromise to the confidentiality, integrity, or availability of the target
  - Exploits
    - Specifically, crafted software, data, or commands that trigger the vulnerability
    - Can be innocuous or cause damage to the target

[1]

Penetration Testing

- Communication
  - Communication process should be carefully planned
    - Ensure the team has contact information of key personnel in the case something goes wrong
    - Ensure the team knows who should and should not know about the pen tests
  - Double-Blind Test
    - Pen testers are not aware of the defenders of the organization
    - Defenders of the organization are not aware of the penetration tests
- Reporting
  - Detailed report on
    - How the organization can be successfully attacked
    - Step-by-step methodology recommended to mitigate the risks

[1]

Reverse Engineering

- Reverse Engineering
  - Deconstructing something to discover what it does and how it does it
  - Is required if there is no documentation at hand
- Hardware
  - No longer immutable due to software-defined "things"
  - Generalized hardware platforms running custom software is trending
    - Easier, faster, and cheaper to update software than to replace hardware

[1]

Reverse Engineering

- Source Authenticity
  - Assurance that a product is from the source it claims to be manufactured from
  - Security Issues
    - Counterfeit products can
      - Have malicious features
      - Be made with low-quality material
      - Fail at a higher rate
      - Lack of manufacturer support
    - Malicious Organizations or Governments will try to insert modified popular products such as routers
      - These type of modified products can be used to
        - Steal information or data from the target
        - Blackmail an organization with a “kill” switch

[1]

Reverse Engineering

- **Avoid counterfeit products**
  - – **You get what you pay for**
    - **The appeal for most counterfeits is the lower price**
  - – **Buy from authorized retailers**
    - **Most vital manufactures will have a network of authorized retailers**
  - – **Check the serial number**
    - **Most manufactures will have a system to verify that their product's serial number maps to a legitimate product**
    - **A duplicate serial number could indicate a counterfeit product**

[1]

Reverse Engineering

- **Trusted Foundry**
  - **Trusted Foundry Program**
    - **Instituted by the DoD**
    - **Ensures mission-critical military and government systems are developed using a supply chain that is hardened against external threats**
  - **Through a special review process the trust is ensured by the NSA**
- **OEM Documentation**
  - **Original equipment manufacturers(OEMs)**
    - **Provides detailed documentation on**
      - **The features of their products**
      - **Detailed performance parameters and characteristics to verify that the product it performing as intended**
    - **Can be used to ensure the products in question are genuine**

[1]

Reverse Engineering

- Reversing Hardware
  - – Techniques discussed will likely void the products warranty and might violate laws in some jurisdictions
    - Read the products end-user license and any legal warnings
  - – General Approaches
    - Open enclosure and observe the layout of the chips on the boards
    - Research online for photos taken of the product and compare those to your version of the product
      - – Look for any suspicious components
    - Inventory component chips
    - Read chip manufacturers publish technical datasheets
      - – Will provide information on every input and output pin on the chip

[1]

Reverse Engineering

- **Reversing Hardware**
  - **Firmware**
    - **Software that is permanently programmed into the read-only memory(ROM) on a hardware component**
  - **Extract the firmware and analyze it to fully understand the device**
    - **A general-purpose ROM programmer will be needed to read the software**
    - **The code will be in binary**
  - **Analyze captured the signals at the interface**
    - **Can get a high-level view of the communications patterns using a pocket analyzer**
    - **Can view the raw voltage level fluctuations using an oscilloscope or logic analyzer**
    - **These tools will allow an analyst to monitor individual chip components behavior and inject inputs to find hidden features**

[1]

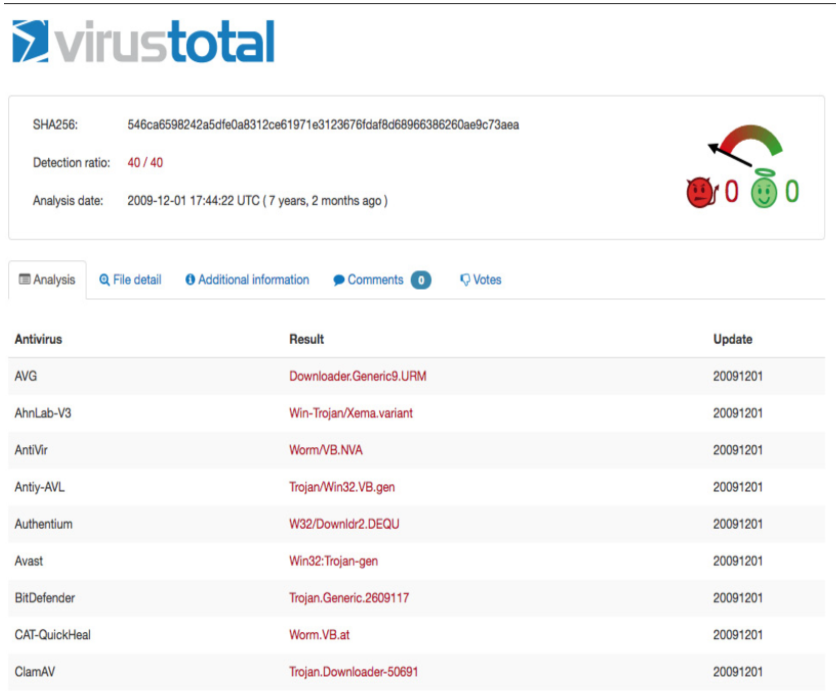
Reverse Engineering

- Software/Malware
  - Requires in-depth understanding of the processors
  - Reversing binaries for one processor is significantly different than for another processor
- Fingerprinting/Hashing
  - Hashing function
    - The one-way function that takes variable-length input and produces a fixed-length result called a hash-value
    - Can be used to check the integrity of data
      - Example: A file is copied if the hashes from the two files are the same it, can be reasonably assumed, they are the same file
    - The same can be done for known malware packets
      - Example: Take a hash of a suspicious file and compare its hash against a knowledge base of known-bad hashes

[1]

VirusTotal Utilization

- **VirusTotal.com is a website owned by Google that allows for hashes or entire files to be compared against its database of known bad hashes**



virustotal

SHA256: 546ca6598242a5dfe0a8312ce61971e3123676fdaf8d68966386260ae9c73aea

Detection ratio: 40 / 40

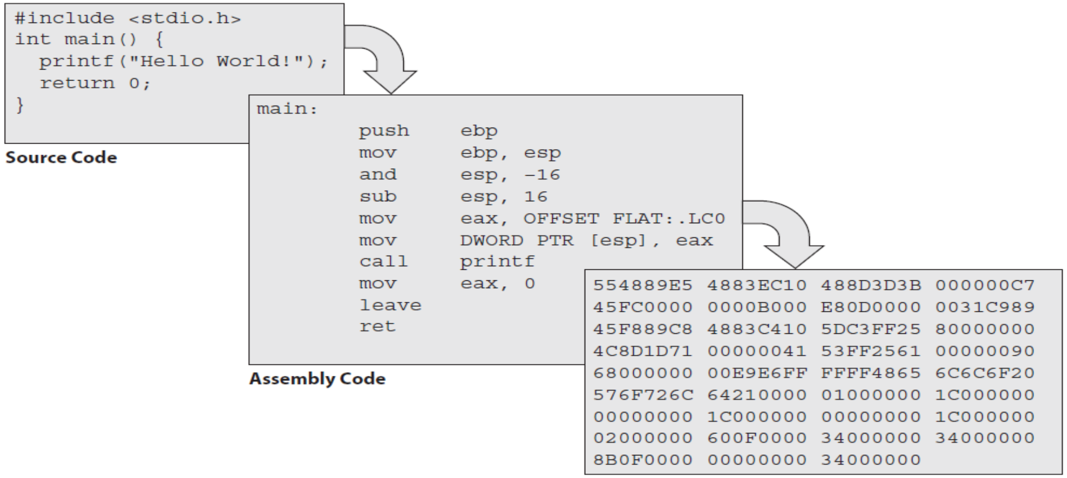
Analysis date: 2009-12-01 17:44:22 UTC (7 years, 2 months ago)

Antivirus	Result	Update
AVG	Downloader.Generic9.URM	20091201
AhnLab-V3	Win-Trojan/Xema.variant	20091201
AntiVir	Worm/VB.NVA	20091201
Antiy-AVL	Trojan/Win32.VB.gen	20091201
Authentium	W32/Downldr2.DEQU	20091201
Avast	Win32:Trojan-gen	20091201
BitDefender	Trojan.Generic.2609117	20091201
CAT-QuickHeal	Worm.VB.at	20091201
ClamAV	Trojan.Downloader-50691	20091201

[1]

Reverse Engineering

- **Decomposition**
  - **Three decomposition steps**
    - **Programming languages**
      - **Human-readable language, which is compiled into assembly**
    - **Assembly**
      - **Hardware code, which is assembled into binary**
    - **Binary**
      - **Computer-readable language, which is a binary executable**



```
#include <stdio.h>
int main() {
  printf("Hello World!");
  return 0;
}
```

Source Code

```
main:
        push    ebp
        mov     ebp, esp
        and     esp, -16
        sub     esp, 16
        mov     eax, OFFSET FLAT:.LC0
        mov     DWORD PTR [esp], eax
        call    printf
        mov     eax, 0
        leave
        ret
```

Assembly Code

```
554889E5 4883EC10 488D3D3B 000000C7
45FC0000 0000B000 E80D0000 0031C989
45F889C8 4883C410 5DC3FF25 80000000
4C8D1D71 00000041 53FF2561 00000090
68000000 00E9E6FF FFFF4865 6C6C6F20
576F726C 64210000 01000000 1C000000
00000000 1C000000 00000000 1C000000
02000000 600F0000 34000000 34000000
8B0F0000 00000000 34000000
```

Machine Code

[1]

Decomposition Cont’d

- Portable Executable (PE) format
  - Windows programs are packaged in PE format
  - Every file starts with the 2-byte sequence 5A 4D
    - Depending on the operating system, it could start with 4D 5A
- Executable and Linkable Format (ELE)
  - Linux executables are packaged in ELE format
  - Every file starts with the 4-byte sequence 7F 45 4C 46

Reverse Engineering

- **Generations of Computer Languages**
  - **First-generation**
    - **Machine language**
      - **A sequence of operators and arguments represented as ones and zeros or hexadecimal**
    - **Example: Intel x85**
  - **Second-generation**
    - **Assembly Language**
      - **Represents machine language operators**
      - **The assembler turns assembly language into machine code**
  - **Third-generation**
    - **Human-like language**
      - **BASIC, Pascal, C/C++, Java, and Python**
      - **A compiler is used to translate third generation language into second-generation assembly language**

[1]

Reverse Engineering

- **Analyzing Malware**
  - **Rarely will an analyst have access to malware source code**
  - **Malware found is usually a machine language binary file**
  - **IDA Pro**
    - **A disassembler that converts the machine code back into assembly language**
  - **Decompilers**
    - **Usually not worth the effort and easier to just reverse engineer assembly**
    - **There are too many possible compilers that could have been used, and finding the right one is difficult**

[1]

Reverse Engineering

- **Isolation/Sandboxing**
  - Usually used by an analyst to understand what a running executable is doing in isolation
  - cuckoo
    - Cuckoo Sandbox
    - Popular opensource isolation environment
    - Safely runs suspicious binaries on a virtual computer using either VirtualBox or VMware Workstation
    - Capable with Windows, Linux, Mac OS, or Android virtual devices
    - Used to analyze malware
  - REMnux
    - REMnux
    - Linux distribution
    - Comes with malware reverse engineering tools

[1,5,6]

Training and Exercises

- Training
  - Give individuals or help them maintain a set of skills, knowledge, or attributes to effectively do their job
    - Example: Giving security training to employees to ensure they are aware of possible fishing attacks
- Exercises
  - An event where individuals apply their skills, knowledge, or attributes to a given scenario
    - Example: Creating a simulated scenario that tests the defensive team's ability to overcome an incident
- All training events and exercises should start with goals and outcomes
  - At an operational level, this will examine how successful the training/exercise was
  - At a managerial level, this will examine the usefulness of the training/exercise

[1]

Types of Exercises

- Tabletop Exercises (TTXs)
  - Test procedures and ensure they do what they were intended to do
  - These tests individuals on their roles in responding to an event
  - A planning team develops scenarios that test the response plan
    - Also considers branches and sequels at each point of the scenario
  - Branch
    - A point in the scenario where the participants may choose one of the multiple approaches to respond to
  - Sequels
    - A follow-on to action in the response

[1]

Types of Exercises

- **Live-Fire Exercises (LFXs)**
  - **Participants are defending real or simulated information systems against friendly attackers**
  - **Challenges in organizing an LFXs**
    - **Developing an infrastructure that is like the real systems**
    - **Obtaining a good adversary team (Red Team)**
    - **Getting the right defending team (Blue Team) for the duration of the exercise**
    - **Is costly**
  - **Pattern-of-life (POL)**
    - **The day-to-day network traffic, such as users exchanging emails and visiting websites**
    - **Needed for a realistic LFX**
    - **Can hire a group of individuals that can simulate real-world network traffic during the event**
    - **Traffic generators automatically inject packets but not very realistic**

[1]

Types of Exercises

- Red Team
  - Are the adversaries during an exercise
  - Requires a skilled group of people to be effective
- Blue Team
  - A group of people that are the focus of the exercise
  - They are the defenders of the organization
- White Team
  - The group of people that plan and organize the exercise
  - In charge of
    - Developing the scenario
    - Develop the schedule so that the goals of the exercise are met
    - Conduct after-action review by documenting and sharing their observations

[1]

Risk Evaluation

- Risk
  - The possibility of damage to or loss of any information system assets and its ramifications
  - Is the product of impact on the organization and the likelihood of the risk
- Risk Evaluation
  - The process of ranking risks, categorizing them and determining the best controls to mitigate them
  - Cannot be 100 percent secure
    - Risk evaluation helps balance the value of risk with the cost of control to mitigate it

[1]

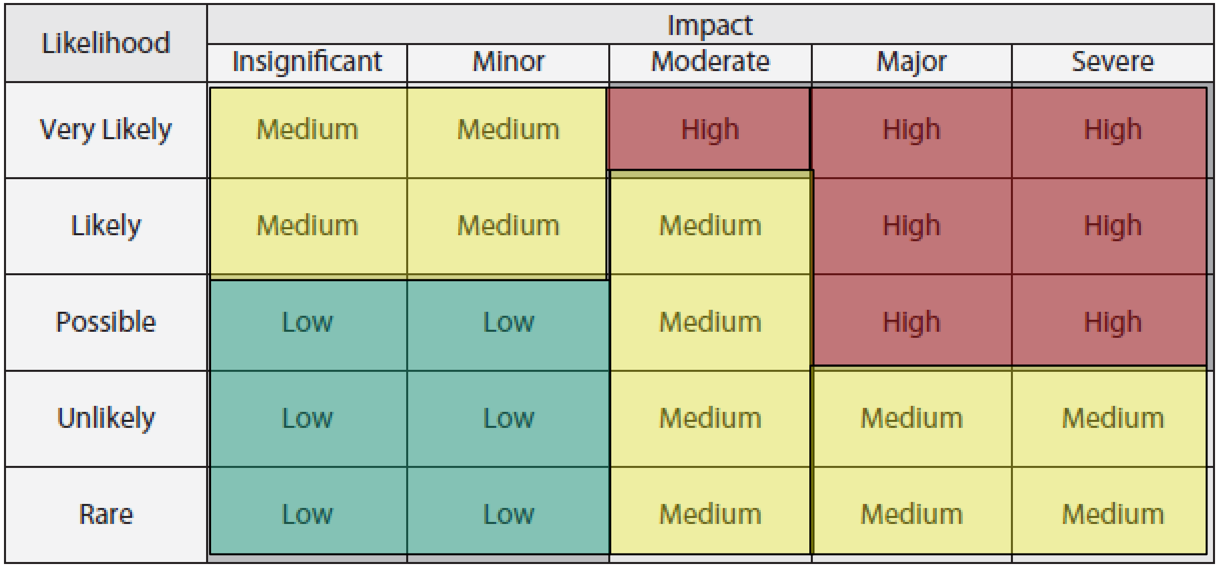
Impact and Likelihood

- Quantitative Analysis
  - The mathematical approach to risk evaluation
  - Assigns a numeric value to all assets that could be impacted by risk
  - These numeric values are used in an equation to determine total and residual risk
- Qualitative Analysis
  - Assigns ratings to the risk such as high medium and low
  - Example
    - A result of qualitative analysis could be if an organization’s web server was exploited, they would risk losing 100,000 dollars
  - Can yield numeric values by assigning a value to each rating
    - Example
      - High = 3
      - Medium = 2
      - Low = 1

[1]

Impact and Likelihood

- A few qualitative techniques for gathering data
  - Focus groups, surveys, questionnaires, checklists, etc.
- A common risk matrix
  - Can be used to evaluate the fitness of technical and operational controls



Likelihood	Impact				
	Insignificant	Minor	Moderate	Major	Severe
Very Likely	Medium	Medium	High	High	High
Likely	Medium	Medium	Medium	High	High
Possible	Low	Low	Medium	High	High
Unlikely	Low	Low	Medium	Medium	Medium
Rare	Low	Low	Medium	Medium	Medium

[1]

Impact and Likelihood

- **Avoid group biases (aka groupthink)**
  - **It is best to perform risk evaluation as a group, but groups can come to similar results**
  - **Keep groups sizes small (no more than 12)**
  - **Ask participants to write down their answers before speaking aloud**
  - **Encourage respectful disagreement**
  - **Leave time for discussion with a time limit**

[1]

Technical Control Review

- Technical Controls
  - Implemented security controls through software or hardware components such as
    - Firewalls, IDS, encryption, identification and authentication mechanisms
- Technical control review
  - An assessment of technical control choices and how each technical control is implemented and managed
  - Technical controls should be reviewed periodically
  - Example
    - A firewall might be the best control once in place, but it must be assessed to ensure it is still working as expected

[1]

Operational Control Review

- Operational controls
  - Security controls implemented through
    - business processes
    - codified in documents such as
      - Policy letters
      - Standing operation procedures (SOPs)
  - Administrative control examples
    - Security documentation
    - Risk management
    - Personnel security
- Operational control review
  - An assessment of operational control choices and how each control is implemented and managed
  - Policies can become outdated over time and must be maintained to remain effective

[1]

Quiz

Chapter 4

Question #1

- **The practice of moving, or pivoting, from a compromised machine to another machine on the network is referred to as what?**
  A. Exploitation
  B. Trusted foundry
  C. Decomposition
  D. Lateral movement

[1]

Answer #1

- D
  - Lateral movement is the act of compromising additional systems from the initially breached one.

[1]

Question #2

- **Which is not a consideration to take during a penetration test?**
  A. None, the goal is to be as realistic as possible
  B. Personal healthcare information
  C. Time limitations
  D. Effects on production services

[1]

Answer #2

- A
  - A successful penetration requires lots of preparation, which includes defining the scope, objectives, off-limit areas, timing, and duration of the test.

[1]

Question #3

- **Who is the ultimate giver of consent for a penetration test?**
  A. The penetration tester or analyst
  B. The security company
  C. The system owner
  D. The FBI

[1]

Answer #3

- C
  - Consent of the system owner is critical for a penetration test because many of the tasks involved in this activity are illegal in most countries

[1]

Question #4

- In an exercise, which type of team is the focus of the exercise, performing their duties as they would normally in a day-to-day operation?
  A. Blue Team
  B. Red Team
  C. Gray Team
  D. White Team

[1]

Answer #4

- **A**
  - **The blue team is the group of participants who are the focus of an exercise and will be tested the most while performing the same tasks in a notional event as they would perform in their real jobs.**

[1]

Question #5

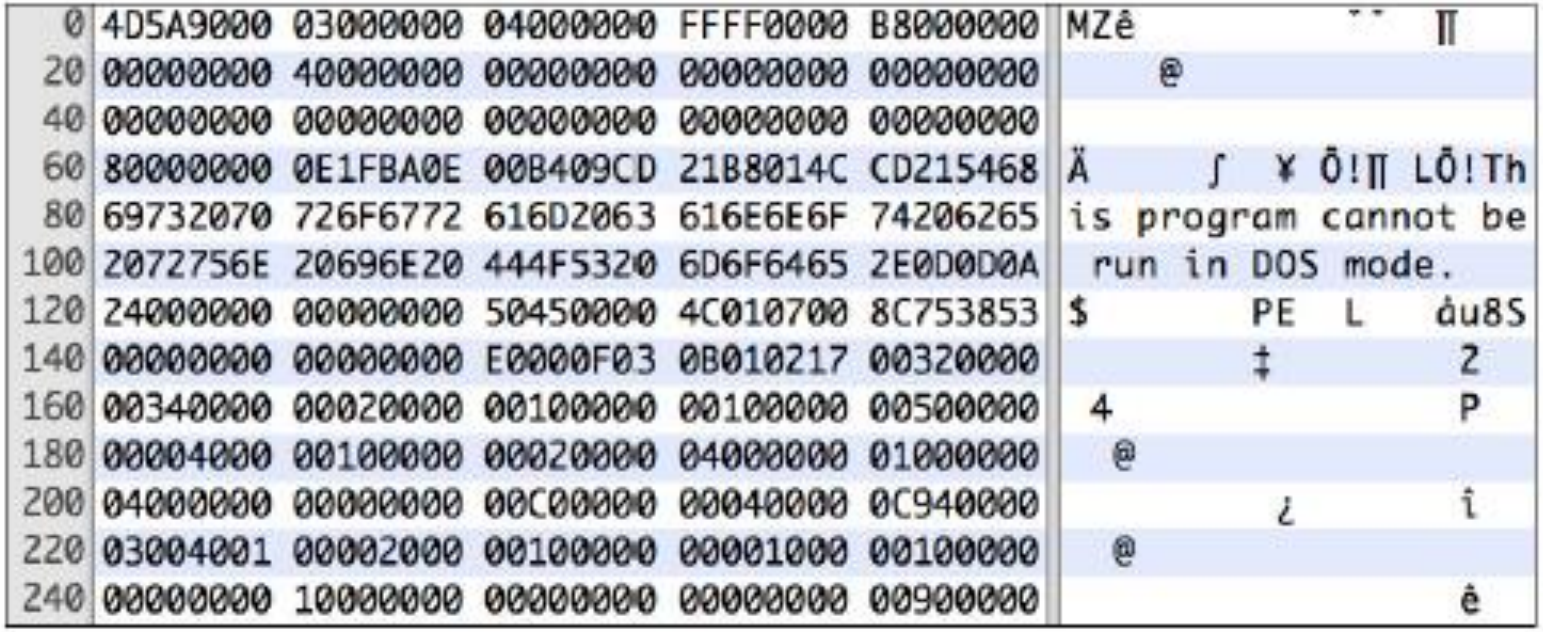
- **Which of the following addresses the vulnerabilities associated with component supply chains**
  A. **Exploitation bank**
  B. **Partial knowledge**
  C. **Reporting chain**
  D. **Trusted foundry**

[1]

Answer #5

- D
  - A trusted foundry is an organization capable of developing prototype or production-grade microelectronics in a manner that ensures the integrity of their products.

[1]



```
  0 4D5A9000 03000000 04000000 FFFF0000 B8000000 MZê         ˇˇ  ∏
 20 00000000 40000000 00000000 00000000 00000000     @
 40 00000000 00000000 00000000 00000000 00000000
 60 80000000 0E1FBA0E 00B409CD 21B8014C CD215468 Ä     ∫  ¥ Õ!∏ LÕ!Th
 80 69732070 726F6772 616D2063 616E6E6F 74206265 is program cannot be
100 2072756E 20696E20 444F5320 6D6F6465 2E0D0D0A  run in DOS mode.
120 24000000 00000000 50450000 4C010700 8C753853 $       PE  L   åu8S
140 00000000 00000000 E0000F03 0B010217 00320000         ‡        2
160 00340000 00020000 00100000 00100000 00500000  4               P
180 00004000 00100000 00020000 04000000 01000000   @
200 04000000 00000000 00C00000 00040000 0C940000          ¿       î
220 03004001 00002000 00100000 00001000 00100000   @
240 00000000 10000000 00000000 00000000 00900000                  ê
```

Question #6

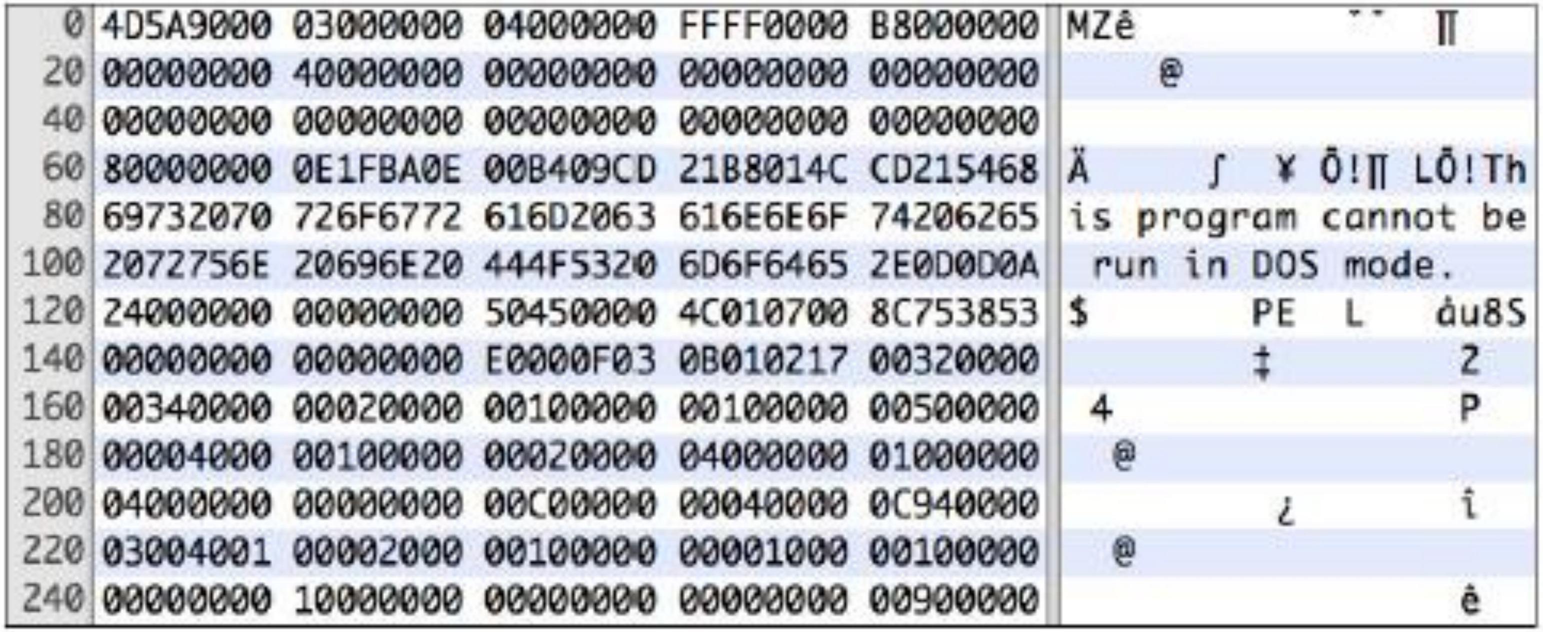
- **You are analyzing a suspicious executable you suspect to be malware. In what language is this file being viewed?**
  - **A. Natural language**
  - **B. High-level language**
  - **C. Assembly language**
  - **D. Machine language**

[1]

Answer #6

- D
  - Machine language is represented as a series of ones and zeros, or sometimes in hexadecimal

[1]



```
  0 4D5A9000 03000000 04000000 FFFF0000 B8000000 MZê         ˇˇ  ∏
 20 00000000 40000000 00000000 00000000 00000000     @
 40 00000000 00000000 00000000 00000000 00000000
 60 80000000 0E1FBA0E 00B409CD 21B8014C CD215468 Ä     ∫  ¥ Õ!∏ LÕ!Th
 80 69732070 726F6772 616D2063 616E6E6F 74206265 is program cannot be
100 2072756E 20696E20 444F5320 6D6F6465 2E0D0D0A  run in DOS mode.
120 24000000 00000000 50450000 4C010700 8C753853 $       PE  L   åu8S
140 00000000 00000000 E0000F03 0B010217 00320000         ‡        2
160 00340000 00020000 00100000 00100000 00500000  4               P
180 00004000 00100000 00020000 04000000 01000000   @
200 04000000 00000000 00C00000 00040000 0C940000          ¿       î
220 03004001 00002000 00100000 00001000 00100000   @
240 00000000 10000000 00000000 00000000 00900000                  ê
```

Question #7

- **Which operating system is this program designed for?**
  - **A. Linux**
  - **B. Windows**
  - **C. Mac OS**
  - **D. iOS**

[1]

Answer #7

- B
  - Windows executable always start with the byte sequence 5A4D or 4D5A, depending on which OS you are using to inspect the file.
  - They also typically include the string “This program cannot be run in DOS mode” for backward compatibility.

[1]

Question #8

- What two factors are considered in making a quantitative assessment on risk?
  A. Expected value and probability of occurrence
  B. Expected value and probability of vulnerability
  C. Potential loss and probability of occurrence
  D. Potential loss and expected value

[1]

Answer #8

- C
  - Quantitative risk assessment is calculated using the amount of the potential loss and the probability that the loss will occur.

[1]

Scenario for Questions 9 - 12

- Your company was hired to perform a penetration test on a small financial services company. The company has no in-house expertise in security assessment and is relying on your team to help them address their challenges. The Chief Information Officer invites you to review the network with his network engineer. Since they are a small company, the engineer tells you that they haven’t been targeted for many attacks. Additionally, most of the production systems see the most traffic during local business hours of 9 a.m. to 5 p.m., and they cannot, under any circumstances, be disrupted.

[1]

Question #9

- **Based on the meeting with the CIO, what kind of penetration test will you be conducting?**
  A. **Partial knowledge**
  B. **Red box**
  C. **Total recall**
  D. **Zero knowledge**

[1]

Answer #9

- **A**
  - **Because the CIO and network engineer provided you with upfront information about the target, you have partial knowledge about this system.**

[1]

Question #10

- **Before leaving the office, you ask the CIO to provide which formal document authorizing you to perform certain activities on the network?**
  A. **Syslogs**
  B. **Network flows**
  C. **Certificate Authority**
  D. **Authorization memo**

[1]

Answer #10

- D
  - An authorization memo includes the extent of the testing authorization and should be made available to team members during the testing period.

[1]

Question #11

- **Considering the scope of this test, what is your recommendation for the best times to conduct the test?**
  - A. Any time during normal business hours
  - B. Beginning at 7 p.m.
  - C. Over lunchtime
  - D. Exactly at 9 a.m.

[1]

Answer #11

- B
  - Because the CIO prioritizes uptime of critical production systems, it’s best to avoid performing the pen test during those hours.

[1]

Question #12

- **You complete the pen test and are preparing the final report. Which areas should you normally not include in the deliverables?**
  A. Information that could be gleaned about the company from open sources
  B. Specific exploitable technical features of the network
  C. Audit of the existing physical infrastructure
  D. Full packet captures

[1]

Answer #12

- D
  - Penetration testing isn’t restricted to technology only. The report should cover all discovered vulnerabilities in physical and information security, including the successful use of social engineering.
  - You would normally not want to include full packet captures because, absent specific authorizations, this could lead to privacy or regulatory problems.

[1]

References

1. Maymí Fernando, and Brent Chapman. CompTIA CSA+ Cybersecurity Analyst Certification All-in-One Exam Guide (Exam CS0-001). McGraw-Hill Education, 2018.
2. "What is Penetration Testing: Step-By-Step Process & Methods: Imperva," *Learning Center*, 29-Dec-2019. [Online]. Available: https://www.imperva.com/learn/application-security/penetration-testing/. [Accessed: 17-Nov-2020].
3. J. Firch and J. Firch, "What Are The Different Types Of Penetration Testing?," *PurpleSec*, 07-Dec-2020. [Online]. Available: https://purplesec.us/types-penetration-testing/. [Accessed: 17-Nov-2020].
4. "Between The Shades: Black, White & Gray-Box Penetration Testing," *Horangi Cyber Security*. [Online]. Available: https://www.horangi.com/blog/black-white-gray-box-penetration. [Accessed: 17-Nov-2020].
5. "Automated Malware Analysis," *Cuckoo Sandbox - Automated Malware Analysis*. [Online]. Available: https://cuckoosandbox.org/. [Accessed: 17-Nov-2020].
6. "A Linux Toolkit for Malware Analysis," *REMnux*. [Online]. Available: https://remnux.org/. [Accessed: 17-Nov-2020].