



Mississippi State
UNIVERSITY

CySA+

Cybersecurity Analyst

CCI
Post Office Box 9627
Mississippi State, MS 39762



Mississippi State University Center for Cyber Innovation



CySA+

Part 3 Cyber Incident Response



Selecting the Best Course of Action

Chapter 10



Outline

- **Network-Related Symptoms**
- **Host-Related Symptoms**
- **Application-Related Symptoms**
- **Quiz**



Network-Related Symptoms

- **Network Sensors**
 - Usually will provide the first indicators that something is wrong
- **Bandwidth Utilization**
 - **Bandwidth**
 - The rate data can be transferred through a medium
 - Usually measured in bits per second
 - **Normal Bandwidth Utilization**
 - An organization's network will usually have a pattern of utilization with normal ebbs and flows
 - An adversary can hide data exfiltration if they are patient
 - Very difficult to detect by looking at the network traffic

[1]



Network-Related Symptoms

- **Bandwidth Utilization**

- **Abnormal Bandwidth Utilization**

- **Most often, an attacker will want to quickly exfiltrate data, and this can be seen by looking at network traffic**
 - **Another indicator can be seen by looking at endpoints and directionality of the connection**
 - **Below figure 10-1 shows a suspicious pattern of NetFlow activity. Though one host (10.0.0.6) is clearly consuming more bandwidth than the others, this fact alone can have a multitude of benign explanations.**

Src IP	Src Port	Dst IP	Dst Port	Protocol	Packets	Bytes/Pkt
10.0.0.3	54902	192.168.0.7	80	TCP	2491	740
10.0.0.6	55097	172.31.21.3	443	TCP	100227	1528
10.0.0.12	993	10.0.0.3	48450	TCP	2210	762
10.0.0.6	443	10.0.0.7	54122	TCP	2271	1040
10.0.0.6	443	10.0.0.3	53112	TCP	1022	810

Figure 10-1 NetFlow report showing suspicious bandwidth use

[1]



Network-Related Symptoms

- **Beacons**
 - **Beaconing**
 - A periodical outbound connection between a compromised computer and an external controller
 - **Some legitimate connections can look like beacons**
 - E.g. High-end software will periodically check licensing of the software
 - **Detecting beacons with endpoint analysis**
 - Analyze how regularly the host communicate with other hosts
 - First, sort traffic logs by internal source address
 - Second, sort traffic logs by the destination address
 - Third sort traffic logs by time
 - Typical beacons will be apparent using this method

[1]



Network-Related Symptoms

- **Irregular Peer-to-Peer Communication**
 - **Normal Peer-to-Peer Communication**
 - Usually, there is a small number of servers that provide services to several non-server computers
 - It is rare to find two peer workstations talking to one another and is an indication of a compromised host
 - **Abnormal Peer-to-Peer Communication**
 - Unprivileged accounts connecting to other hosts
 - Privileged accounts connecting from regular hosts
 - Repeated failed remote logins
 - **Lateral movement**
 - The process of an attacker compromising additional hosts within a network
 - Can be done by utilizing trusted tools such as
 - SMB and PsExec in Windows or SSH in Linux
 - All that is need to use these tools is a username and password

[1]



Interactive Exercise 1

Name 5 network-related symptoms of attack?

How to determine the Beacon behavior?

What are the three steps of endpoint analysis?



Interactive Exercise 1 Answers

Name 5 network-related symptoms of attack?

1. Bandwidth Utilization,
2. Beaconsing,
3. Irregular P2P communication,
4. Rogue devices on the network
5. Scan sweeps

How to determine the Beacon behavior?

Can be determined using endpoint analysis

What are the three steps of endpoint analysis?

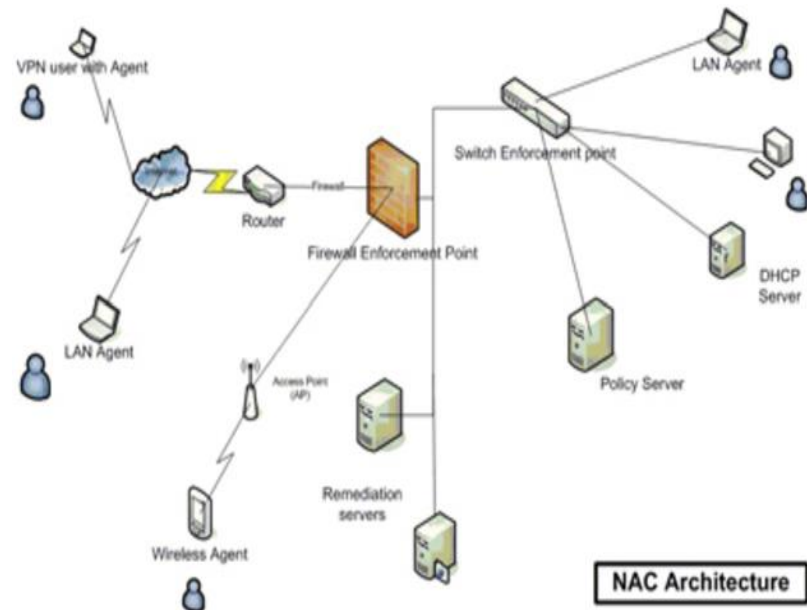
1. sort traffic logs by internal source address
2. sort traffic logs by the destination address
3. sort traffic logs by time

[1,2]



Network-Related Symptoms

- **Rogue Devices on the Network**
 - **Rogue devices**
 - **Are unauthorized devices on the network**
 - **Network Access Control (NAC)**
 - **Ensures that each device trying to connect to the network is**
 - **Authenticated, scanned, and connected to the appropriate network**
 - **Provides fine-grain controls to implement policies**
 - **Provides centralized logs that can be used to detect rogue devices attempting to connect**



[1,3]



Network-Related Symptoms

- **Rogue Devices on the Network**
 - **Access Points (APs)**
 - **If your environment does not have NAC, then**
 - Send all AP logs to a central store
 - Physically look for MAC addresses you have not seen before
 - **Issues with this method**
 - Can be tedious
 - It is easy for an attacker to change their MAC address to a legitimate user

[1]



Interactive Exercise 2

Why is P2P communication suspicious?

What does the term "lateral movement" mean?

Name 2 ways we can detect rogue devices connected to our network?



Interactive Exercise 2 Answers

Why is P2P communication suspicious?	It 's rare in a corporate network for two peer workstations to be communicating with each other.
What does the term "lateral movement" mean?	the process by which attackers compromise additional hosts within a network after having established a foothold in one.
Name 2 ways we can detect rogue devices connected to our network?	<ol style="list-style-type: none">1. deploy NAC to ensure each device is authenticated, potentially scanned, and then joined to the appropriate network2. all logs from your APs sent to a central store in which you can look for physical MAC addresses

[1,2]



Network-Related Symptoms

- **Scan Sweeps**
 - **Non-stealthy attackers**
 - Will use a tool like Nmap to scan sweep and map out an environment after compromising a host
 - The compromised host is easy to pick out given that it is generating a lot of connection attempts to a mass of endpoints
 - **Address Resolution Protocol (ARP)**
 - Is used by interfaces to determine the address of the next hop toward the final destination of a packet
 - **ARP Request**
 - A node that asks all other nodes on the LAN who handles this IP address
 - **Ensure your organization has a sensor in every subnet, monitoring ARP messages**

[1]



Network-Related Symptoms

- **Scan Sweeps**
 - **A Scan Sweep Attempt**
 - Will generate a lot of ARP queries
 - Unless authorized by a security staff member, any attempts should be investigated
 - Below figure 10-2 example, shows most of the request will go unanswered because there are only a handful of host on the network segment though the subnet mask is for 255 addresses signaling a scan sweep.

Time	Source	Destination	Protocol	Length	Info
1.88519600	Vmware_4a:58:30	Broadcast	ARP	42	who has 192.168.192.162? Tell 192.168.192.6
1.88528900	Vmware_4a:58:30	Broadcast	ARP	42	who has 192.168.192.163? Tell 192.168.192.6
1.88540000	Vmware_4a:58:30	Broadcast	ARP	42	who has 192.168.192.164? Tell 192.168.192.6
1.88555900	Vmware_4a:58:30	Broadcast	ARP	42	who has 192.168.192.165? Tell 192.168.192.6
1.88566200	Vmware_4a:58:30	Broadcast	ARP	42	who has 192.168.192.166? Tell 192.168.192.6
1.88574400	Vmware_4a:58:30	Broadcast	ARP	42	who has 192.168.192.167? Tell 192.168.192.6
1.88583400	Vmware_4a:58:30	Broadcast	ARP	42	who has 192.168.192.168? Tell 192.168.192.6
1.88591000	Vmware_4a:58:30	Broadcast	ARP	42	who has 192.168.192.169? Tell 192.168.192.6
1.88601800	Vmware_4a:58:30	Broadcast	ARP	42	who has 192.168.192.170? Tell 192.168.192.6
1.88610000	Vmware_4a:58:30	Broadcast	ARP	42	who has 192.168.192.171? Tell 192.168.192.6
1.88618800	Vmware_4a:58:30	Broadcast	ARP	42	who has 192.168.192.172? Tell 192.168.192.6
1.88626800	Vmware_4a:58:30	Broadcast	ARP	42	who has 192.168.192.173? Tell 192.168.192.6
1.88643300	Vmware_4a:58:30	Broadcast	ARP	42	who has 192.168.192.174? Tell 192.168.192.6
1.88654100	Vmware_4a:58:30	Broadcast	ARP	42	who has 192.168.192.175? Tell 192.168.192.6
1.88663100	Vmware_4a:58:30	Broadcast	ARP	42	who has 192.168.192.176? Tell 192.168.192.6
1.88671500	Vmware_4a:58:30	Broadcast	ARP	42	who has 192.168.192.177? Tell 192.168.192.6

Figure 10-2 ARP queries associated with a scan sweep

[1]



Host-Related Symptoms

- **Running Processes**

- **“Malware can hide, but it has to run.”**

- **Meaning when responding to an incident, first look at running processes**
 - **Tools are readily available on all major OSs to view running processes**
 - **Do not rely on these tools; too much more sophisticated malware will be able to conceal itself**
 - **By capturing volatile memory and performing memory forensic analysis, a trained eye should be able to find any attempts at malware concealment**

- **Normal running processes**

- **Normal Windows processes**

- **E.g., svchost.exe and lsass.exe**

- **Normal Linux processes**

- **E.g., kthreadd and watchdog**

- **Knowing what is normal**

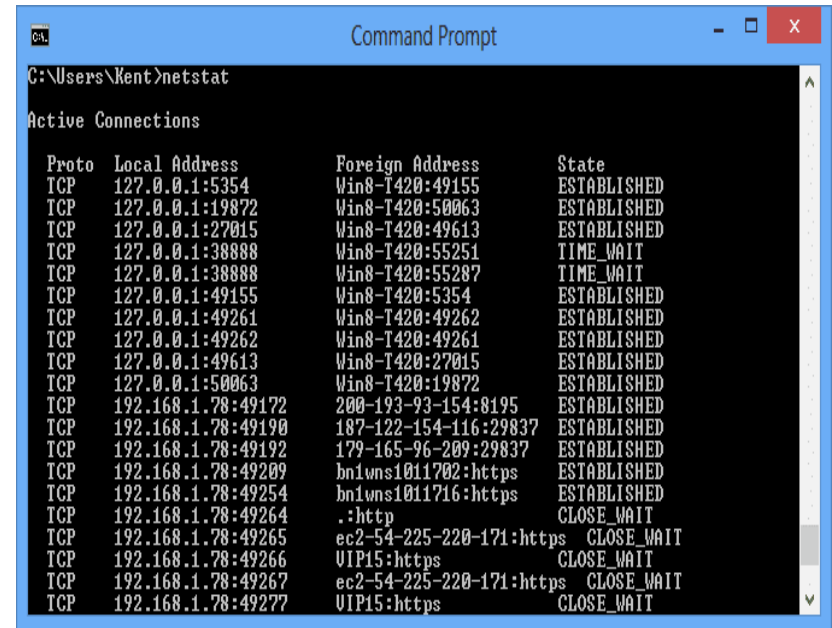
- **This is key to finding malware in running processes**
 - **Having a baseline and notes on what is normal will help weed out the known normal processes**
 - **Advisories will often name their processes similarly to benign processes**
 - » **E.g., svchost.exe will end in an “s”**
 - » **E.g., lsass.exe will start with a “l”**

[1]



Host-Related Symptoms

- **Running Processes**
 - **Abnormal Running Processes**
 - **Nefarious processes will utilize resources such as**
 - Network sockets, CPU cycles, and memory
 - **Netstat command will make it easy to see which sockets belong to which processes**
 - Windows Example
 - » `netstat -ano`
 - Mac OS
 - » `netstat -v`
 - Linux
 - » `netstat -nap`



```
C:\Users\Kent>netstat

Active Connections

Proto Local Address          Foreign Address        State
TCP    127.0.0.1:5354          Win8-T420:49155       ESTABLISHED
TCP    127.0.0.1:19872        Win8-T420:50063       ESTABLISHED
TCP    127.0.0.1:27015        Win8-T420:49613       ESTABLISHED
TCP    127.0.0.1:38888        Win8-T420:55251       TIME_WAIT
TCP    127.0.0.1:38888        Win8-T420:55287       TIME_WAIT
TCP    127.0.0.1:49155        Win8-T420:5354        ESTABLISHED
TCP    127.0.0.1:49261        Win8-T420:49262       ESTABLISHED
TCP    127.0.0.1:49262        Win8-T420:49261       ESTABLISHED
TCP    127.0.0.1:49613        Win8-T420:27015       ESTABLISHED
TCP    127.0.0.1:50063        Win8-T420:19872       ESTABLISHED
TCP    192.168.1.78:49172      200-193-93-154:8195   ESTABLISHED
TCP    192.168.1.78:49190      187-122-154-116:29837 ESTABLISHED
TCP    192.168.1.78:49192      179-165-96-209:29837 ESTABLISHED
TCP    192.168.1.78:49209      bn1wns1011702:https   ESTABLISHED
TCP    192.168.1.78:49254      bn1wns1011716:https   ESTABLISHED
TCP    192.168.1.78:49264      .:http                 CLOSE_WAIT
TCP    192.168.1.78:49265      ec2-54-225-220-171:https CLOSE_WAIT
TCP    192.168.1.78:49266      VIP15:https            CLOSE_WAIT
TCP    192.168.1.78:49267      ec2-54-225-220-171:https CLOSE_WAIT
TCP    192.168.1.78:49277      VIP15:https            CLOSE_WAIT
```

[1,4]



Interactive Exercise 3

What type of traffic/messages should you be on the lookout for if you want to detect unauthorized scan sweeps?

You see scvhosts.exe running on your windows system. Is this normal?

What would this netstat command be for a Windows, Mac OS, and Linux system?



Interactive Exercise 3 Answers

What type of traffic/messages should you be on the lookout for if you want to detect unauthorized scan sweeps?

When an attacker attempts a scan sweep of a network, the scanner will generate a large number of ARP queries

You see scvhosts.exe running on your windows system. Is this normal?

An attacker as added an extra "s" to fool you.

What would this netstat command be for a Windows, Mac OS, and Linux system?

1. Windows = netstat -b or netstat -ano
2. Mac OS = netstat -v
3. Linux = netstat -nap

[1,2]



Host-Related Symptoms

- **Running Processes**
 - **Abnormal Running Processes**
 - **A busy malicious process will use a large number of CPU cycles**
 - In Windows, use Task Manager to view CPU usage and running processes
 - In Linux, use “top” or “ps” utilities

[1]



Host-Related Symptoms

- **Memory Contents**
 - **Collecting volatile memory**
 - **FTK**
 - Captures memory and file systems from Windows machines
 - **Hal Pomeranz's Linux Memory Grabber**
 - Captures memory from Linux Machines
 - **Ensure to dump the memory to a clean external hard drive from your jump bag**
 - **Volatile memory analysis**
 - **Is a sure way to find any malware, even rootkits**
 - **The problem with this method is that it takes time to capture a full memory image and even longer to analyze**
 - **Advisory will use tools that only reside in memory**
 - Incident responders will have to rely on memory forensics to detect and understand them
 - **Volatility**
 - Is a tool used to analyze captured memory images

[1]



Interactive Exercise 4

What are the two tools used to dump the contents of memory to disk mentioned earlier?

What is the major problem when using volatile memory analysis method?

A trained eye should be able to find any attempts at malware concealment after completing what two steps?



Interactive Exercise 4 Answers

What are the two tools used to dump the contents of memory to disk mentioned earlier?

1. FTK Imager (Windows systems)
2. Hal Pomeranza's (Linux OS)

What is the major problem when using volatile memory analysis method?

it takes time to capture a full memory image and even longer to analyze

A trained eye should be able to find any attempts at malware concealment after completing what two steps?

1. capturing volatile memory
2. performing memory forensic analysis



Host-Related Symptoms

- **File System**
 - Is the set of processes and data structures that the OS uses to manage persistent storage devices
 - **Artifacts**
 - Generally means digital object of interests to a forensic investigation
 - Usually, in incident response, the file system is the focal point due to typically holding relevant artifacts
 - It is very difficult for adversaries to not leave evidence of their actions on the file system

[1]



Host-Related Symptoms

- **Unauthorized Software**
 - **Bypassing antimalware systems**
 - **Signature detection systems**
 - Are often deceived by adversaries obscuring the code
 - **Behavioral detection systems**
 - Are often deceived by the adversaries change what the code does
 - **Software Whitelisting**
 - **Process that ensures only known-good software can execute on a system**
 - **Very effective at reducing attack surfaces**
 - **Very unpopular by the user, given any new application must be first reviewed and approved by IT**
 - **Software Blacklisting**
 - **Process that ensures known-bad software is not executed on a system**
 - **Much more common**
 - **Best Practice**
 - **If whitelisting is not possible, at least have an inventory of all software that is installed on each system**

[1]



Host-Related Symptoms

- **Unauthorized Changes**

- **Example Unauthorized Changes**

- **Advisories will try to maintain access to compromised machines by replacing system libraries with malicious ones**
 - **The stand-in libraries will act as the original but also run malicious code**

- **Preventing Unauthorized Changes**

- **Object Access Auditing**

- **Windows built-in feature**
 - **Automatically logs any access or changes to files in the audit space**
 - **Should be selective of which files should be audited to not generate too many alerts**

- **Hash the files**

- **Store the hash value of a file in a secure place and periodically compare the hash to ensure the file has not changed**
 - **Can be easily automated**

- **There are commercial options available such as Tripwire**

[1]



Host-Related Symptoms

- **Data Exfiltration**

- **Detecting Exfiltration**

- Will usually be easy to detect if the adversary is exfiltrating a large amount of data
 - These attempts will try to mimic an acceptable transfer such as a web or email connection
 - Might look like a genuine connection, but the volume of data taken and the endpoint will not
 - Set automated alarms that trigger on large data transfers with unusual destinations

- **Data Loss Prevention (DLP)**

- Rely on tamper-resistant labels on files
 - Tracks those files as they move in and out of the network
 - Requires data inventories, data classification system, and technical controls

[1]



Interactive Exercise 5

How can you detect data exfiltration?

What 2 antimalware systems are commonly bypassed by unauthorized software?

What is a file system?



Interactive Exercise 5 Answers

How can you detect data exfiltration?

User has noticed connection will look legitimate, but its volume and endpoint will not. The pattern will also be broken.

What 2 antimalware systems are commonly bypassed by unauthorized software?

1. Signature detection systems
2. Behavioral detection systems

What is a file system?

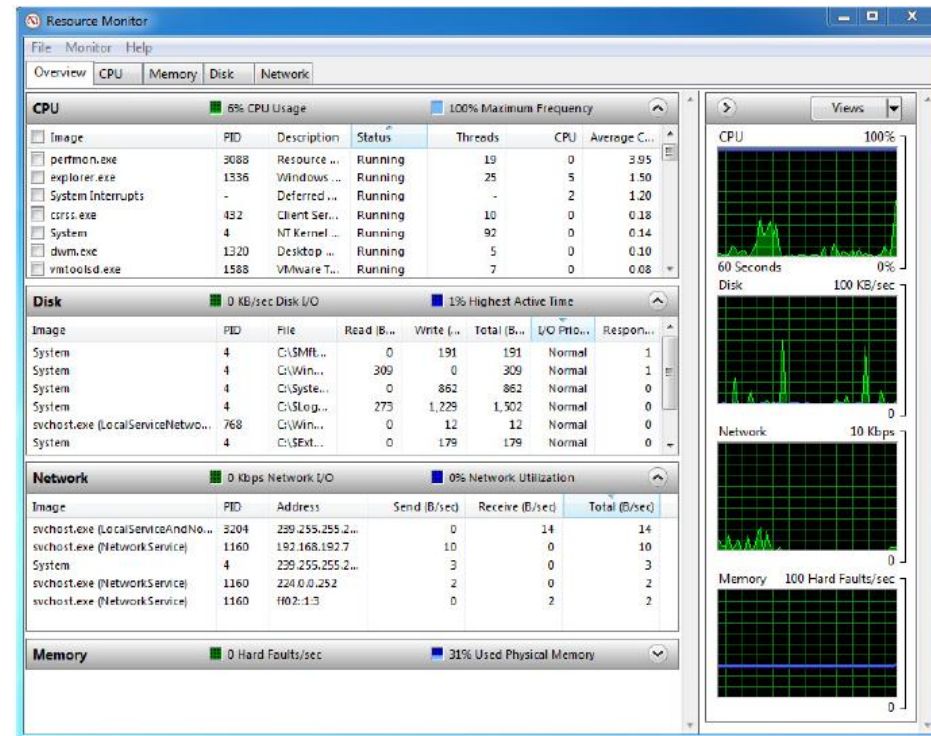
Is a set of processes and data structures that the OS uses to manage persistent storage devices



Host-Related Symptoms

- **Capacity Consumption**

- Most attacks will create spikes in either memory, CPU cycles, disk space, or network bandwidth
- In the CySA+ exam, you will be tested on identifying anomalies in a scenario
- In the figure to the right is a Windows 7 Resource Monitor
 - On the exam, you will have an image like this one and be asked questions on the resource usage



[1]



Host-Related Symptoms

- **Unauthorized Privileges**
 - **Privilege escalation**
 - Elevating limited access account to acquire unauthorized privileges
 - **Methods of gaining unauthorized privileges**
 - Acquiring privileged credentials
 - Exploiting software flaws
 - Exploiting misconfigurations
 - **Response to detected unauthorized privileges**
 - **Disable the suspected account globally and isolate the host**
 - Depending on the situation, this is the simplest approach
 - This is risky and could cause harm
 - » E.g. This could be a legitimate action taken by a teammate performing a vital function
 - **Monitor the activities on the account to determine if malicious or benign**
 - This approach reduces false positives
 - There is a risk of allowing the attacker to continue potentially harmful actions
 - Your response depends greatly on the situation

[1]



Interactive Exercise 6

What are 5 host-related symptoms indicative of an infected system?

Name 3 ways in which a privilege escalation can occur.

you want to check its memory, CPU cycles, disk What tool would be used to check a computer's memory, CPU cycles, disk space and network bandwidth?

[1,2]



Interactive Exercise 6 Answers

What are 5 host-related symptoms indicative of an infected system?

1. Running processes
2. Memory contents/Memory dumps
3. File system changes
4. Capacity consumption
5. Unauthorized privileges

Name 3 ways in which a privilege escalation can occur.

1. Acquiring privileged credentials
2. Exploiting software flaws
3. Exploiting misconfigurations

you want to check its memory, CPU cycles, disk What tool would be used to check a computer's memory, CPU cycles, disk space and network bandwidth?

The correct tool to utilize would be the resource monitor.



Application-Related Symptoms

- **Application-Related Symptoms**
 - “Application” in this section refers to user-level rather than system-level features and services
 - This section will review applications like Microsoft Office, or Google Chrome rather than web or email services
- **Anomalous Activity**
 - This is when an application displays unusual behavior
 - E.g., In a web browser, frozen pages, rapidly changing URLs in the address bar are both indicators of an exploited application
 - Challenge with detecting this type of activity
 - Anomalous behavior tends to mimic normal software flaws
 - Best practice
 - It is best to take caution and quickly isolate the host
 - See if the application tries to make any outbound connection attempts

[1]



Application-Related Symptoms

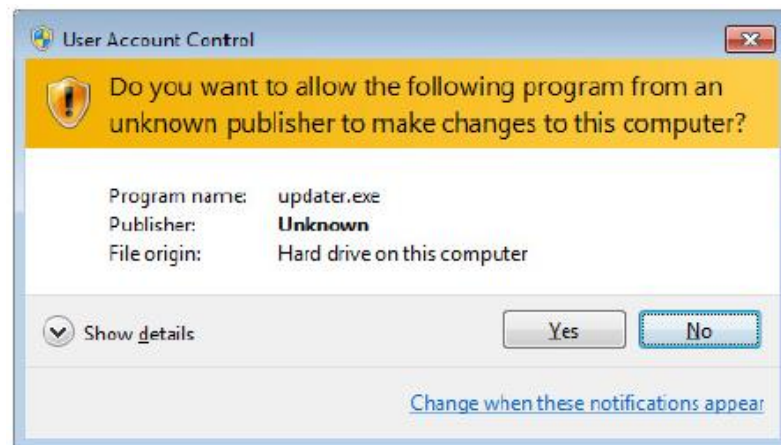
- **Introduction of New Accounts**
 - **Attackers will sometimes try to create a new account for two purposes**
 - **To install and run tools to maintain persistence on the host**
 - **To have an alternate more normal persistence in a domain account**
 - **If you detect an unexpected new account**
 - **Reset the password on the account and log off the user**
 - **Monitor the account for attempted logins to find the source of the attempt**

[1]



Application-Related Symptoms

- **Unexpected Output**
 - **Sign of compromised applications**
 - Unexpected output like various types of pop-up messages
 - **User Access Control (UAC) pop-ups**
 - The pop-up in the figure to the right is almost always malicious if the user is not trying to install any new software
 - **Navigation confirmation or Certification pop-ups**
 - Users tend to not read these pup-ups and select okay



[1]



Interactive Exercise 7

What is a common technique that attackers use to establish persistence in a network?

What were the 2 kinds of pop-ups mentioned in the slides that you should look for?

Name 2 signs of anomalous behavior for a Web browser.



Interactive Exercise 7 Answers

What is a common technique that attackers use to establish persistence in a network? Adding a new user account

What were the 2 kinds of pop-ups mentioned in the slides that you should look for?

1. Unexpected User Access Control (UAC)
2. Certificate warnings and navigation confirmation dialogs

Name 2 signs of anomalous behavior for a Web browser.

1. Frozen pages
2. Rapidly changing URLs in the address bar



Application-Related Symptoms

- **Unexpected Outbound Communication**
 - **This is the number one indicator of a compromised application**
 - It is rare for a compromise not to involve an outbound connection
 - **Detecting this is difficult**
 - A network sensors cannot easily tell if the outbound connection on port 443 was initiated by Google Chrome or by Notepad
 - We will need a host-based sensor or IDS to detect this kind of behavior
 - The connection could be valid and just mean that the application software is updating
 - **Best response when detected**
 - Automatically block the connection attempt if the application has not been whitelisted

[1]



Application-Related Symptoms

- **Service Interruption**
 - **Should investigate services that display unusual behavior such as**
 - Starting, stopping, restarting, or crashing
 - E.g., An antimalware icon in the status bar disappears could mean that an attacker disabled its protection
 - Look at the resource manager and log files to determine if the symptoms are malicious activities
- **Memory Overflows**
 - **Memory is a complex environment malware activity tends to disrupt this environment**
 - If an attacker is off by even a byte when writing to memory, this will cause an error notification to display to the user
 - Messages sometimes mean the attack has failed
 - **Best practice**
 - If you get a memory error message, it is best to analyze a memory dump to find the problem

[1]



Interactive Exercise Final

You notice that some of your services are crashing. What does this mean?

Why is unexpected outbound communication a sign of compromise?

Name 6 application-related symptoms of a compromised applications



Interactive Exercise Final Ans

You notice that some of your services are crashing. What does this mean?

User may be facing malicious activity. An examination of the resource manager and log files will help you determine issue.

Why is unexpected outbound communication a sign of compromise?

normally it's not possible for a network sensor to tell that an outbound connection was initiated by Internet Explorer or by Notepad

Name 6 application-related symptoms of a compromised applications

1. Anomalous activity,
2. Introduction of new accounts,
3. Unexpected outputs,
4. Unexpected outbound communication,
5. Service interruption, and
6. Memory Overflows



Quiz

Chapter 10



Question #1

- 1. the practice of permitting only known-benign software to run is referred to as what?
 - A. Blacklisting
 - B. Whitelisting
 - C. Blackhatting
 - D. Vulnerability scanning

[1]



Answer #1

- **B**
 - Whitelisting is the process of ensuring that only known-good software can execute on a system
 - Rather than preventing known-bad software from running, this technique only allows approved software to run in the first place

[1]



Question #2

- **2. Which of the following is not considered part of the lateral movement process?**
 - A. Internal reconnaissance**
 - B. Privilege escalation**
 - C. Exfiltration**
 - D. Pivoting attacks**

[1]



Answer #2

- **C**
 - Lateral movement is the process by which attackers compromise additional hosts within a network after having established a foothold in one
 - Often achieved by leveraging the trust between hosts to conduct internal reconnaissance, privilege escalation, and pivoting attacks

[1]



Question #3

- **3. What is a common technique that attackers use to establish persistence in a network?**
 - A. Buffer overflow
 - B. Adding new user accounts
 - C. Deleting all administrator accounts
 - D. Registry editing

[1]



Answer #3

- **B**
 - A clever way that attackers use for permanence is to add administrative accounts or groups and then work from those new accounts to conduct additional attacks

[1]



Question #4

- **4. Which one of the following storage devices is considered to be the most volatile?**
 - A. Random-access memory
 - B. Read-only memory
 - C. Cloud storage
 - D. Solid-state drive

[1]



Answer #4

- **A**
 - Random-access memory (RAM) is the most volatile type of storage listed
 - RAM requires power to keep its data, and once power is removed, it loses its content very quickly

[1]



Question #5

- **5. Which of the following is not an area to investigate when looking for indicators of threat activity?**
 - A. Network speed
 - B. Memory usage
 - C. CPU cycles
 - D. Disk space

[1]



Answer #5

- **A**
 - Spikes in memory CPU, disk, or network usage (not necessarily network speed) might be indicative of threat activity
 - It's important to understand what the normal levels of usage are to more easily identify abnormal activity

[1]



Question #6

- **6. What is a useful method to curb the use of rogue devices on a network?**
 - A. SSID**
 - B. FLAC**
 - C. WPA**
 - D. NAC**

[1]



Answer #6

- **D**
 - **Network Access Control (NAC) is a method to ensure that each device is authenticated, scanned, and joined to the right network**
 - **NAC solutions often give fine-grained controls for policy enforcement**

[1]



Scenario for Questions 7-10

- You receive a call from the head of the R&D division because one of her engineers recently discovered images and promotional information of a product that looks remarkably like on that your company has been working on for months. When reading more about the device, it becomes clear to the R&D head that this is in fact the same product that was supposed to have been kept under wraps. She suspects that the plans have been stolen. When inspecting the traffic from the R&D workstations, you notice a few patterns in the outbound traffic. The machines all regularly contact a domain registered to a design software company, exchanging a few byte of information at a time. However, all of the R&D machines regularly communicate to a print server on the same LAN belonging to Logistics, sending several hundred megabytes in regular intervals**



Question #7

- **7. What is the most likely explanation for the outbound communications from all the R&D workstations to the design company?**
 - A. Command-and-control instructions
 - B. Exfiltration of large design files
 - C. License verification
 - D. Streaming video

[1]



Answer #7

- **C**
 - Some types of software, particularly those for high-end design, will periodically check licensing using network connection

[1]



Question #8

- **8. What device does it make sense to check next to discover the source of the leak?**
 - A. The DNS server
 - B. The printer belonging to Logistics
 - C. The mail server
 - D. The local backup of the R&D systems

[1]



Answer #8

- **B**
 - A common approach to removing data from the network without being detected is to first consolidate it in a staging location within the target network
 - Noting the size of the transfers to the print server, it makes sense to check to see if it is serving as a staging location and communicating out of the network

[1]



Question #9

- **9. Why is this device an idea choice as a source of the leak?**
 - A. This device might not arouse suspicion due to its normal purpose on the network**
 - B. The device has regular communications outside of the corporate network**
 - C. This device can emulate many systems easily**
 - D. This device normally has massive amounts of storage**

[1]



Answer #9

- **A**
 - This device is a good choice because an administrator would not normally think to check it
 - However, because a print server normally has no reason to reach outside of the network, it should alert you to investigate further

[1]



Question #10

- **10. What is the term for the periodic communications observed by the R&D workstations?**
 - A. Fingerprinting
 - B. Chatter
 - C. Footprinting
 - D. Beaconing

[1]



Answer #10

- **D**
 - **Beaconing is a periodical outbound connection between a compromised computer and an external controller**
 - **This beaconing behavior can be detected by its two common characteristics: periodicity and destination**
 - **Beaconing is not always malicious, but it warrants further exploration**

[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. **friedaj friedaj, “CySA+ Chapter 10: Selecting the Best Course of Action,” quizlet, 15-Jul-2018. [Online]. Available: <https://quizlet.com/296891201/cysa-chapter-10-selecting-the-best-course-of-action-flash-cards/>. [Accessed: 22-Dec-2020].**
3. **N. Sharma and N. 26, “Network Access Control (NAC),” Help Net Security, 26-Nov-2007. [Online]. Available: <https://www.helpnetsecurity.com/2007/11/26/network-access-control-nac/>. [Accessed: 08-Jan-2021].**
4. **K. Chen, “Troubleshooting Network Connections with Command Line Netstat,” Next of Windows, 05-Aug-2014. [Online]. Available: <https://www.nextofwindows.com/netstat>. [Accessed: 08-Jan-2021].**

