Comp 4108 - Assignment 3

Student Name: Ben Cendana
Student #:100811212

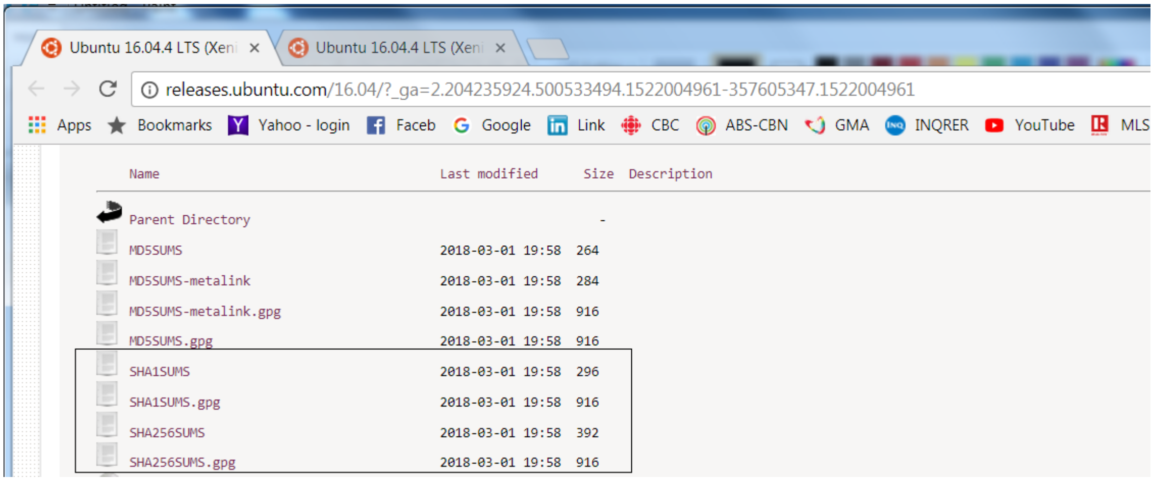
Contents

1.0: Attack Detection – Integrity and Authenticity Of Linux Installation

1.1: Checking For Authenticity and Integrity

In order to check the authenticity and integrity of the ISO image of our Linux distribution we must first check the authenticity of the file. To do this we need to find the vendor/owner of the ISO file and get the ISO hash of the original file.

As an example lets assume we intend to install Ubuntu Linux, after downloading the ISO file we can retrieve the SHA1 or SHA256 hash then compare it against our download.

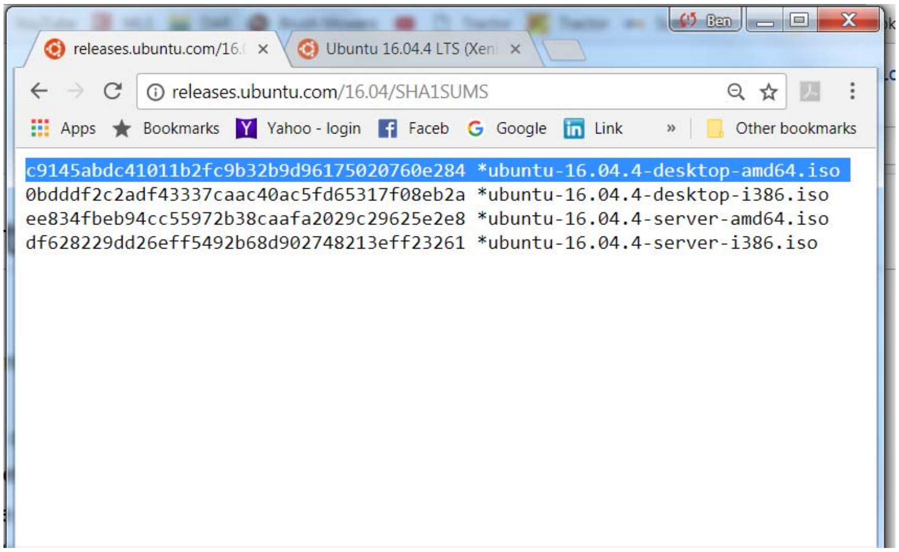


```
Name                          Last modified      Size  Description

Parent Directory                                    -
MD5SUMS                       2018-03-01 19:58   264
MD5SUMS-metalink              2018-03-01 19:58   284
MD5SUMS-metalink.gpg          2018-03-01 19:58   916
MD5SUMS.gpg                   2018-03-01 19:58   916
SHA1SUMS                      2018-03-01 19:58   296
SHA1SUMS.gpg                  2018-03-01 19:58   916
SHA256SUMS                    2018-03-01 19:58   392
SHA256SUMS.gpg                2018-03-01 19:58   916
```

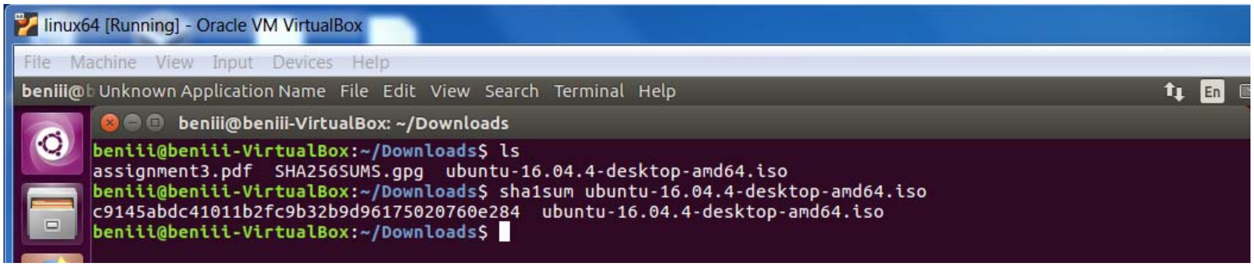
Figure 1: Downloading The ISO Hash From The Vendor

Next we open the file and find out what the SHA1 hash sum is (Figure 2).



```
c9145abdc41011b2fc9b32b9d96175020760e284 *ubuntu-16.04.4-desktop-amd64.iso
0bdddf2c2adf43337caac40ac5fd65317f08eb2a *ubuntu-16.04.4-desktop-i386.iso
ee834fbeb94cc55972b38caafa2029c29625e2e8 *ubuntu-16.04.4-server-amd64.iso
df628229dd26eff5492b68d902748213eff23261 *ubuntu-16.04.4-server-i386.iso
```

Figure 2: The SHA1 Hash


linux64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
beniii@b Unknown Application Name File Edit View Search Terminal Help
En
beniii@beniii-VirtualBox: ~/Downloads

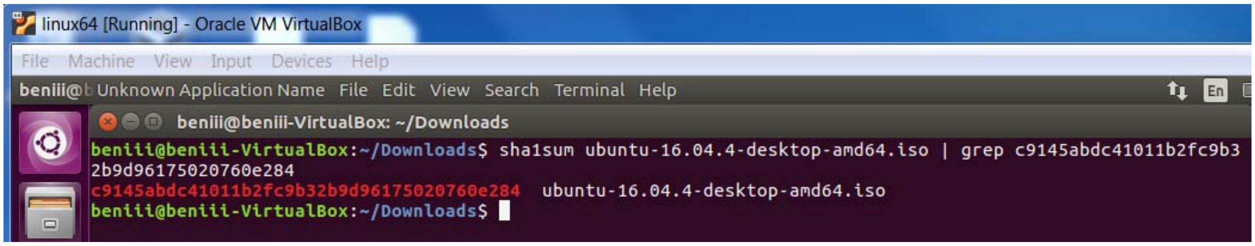
```
beniii@beniii-VirtualBox:~/Downloads$ ls
assignment3.pdf  SHA256SUMS.gpg  ubuntu-16.04.4-desktop-amd64.iso
beniii@beniii-VirtualBox:~/Downloads$ sha1sum ubuntu-16.04.4-desktop-amd64.iso
c9145abdc41011b2fc9b32b9d96175020760e284  ubuntu-16.04.4-desktop-amd64.iso
beniii@beniii-VirtualBox:~/Downloads$
```

Figure 3: Verifying The Checksum

In Ubuntu we use the command *sha1 filename* to verify the ISO file, in this case we type in *sha1 ubuntu-16.04.4-desktop-amd64.iso.*

As can be seen in Figure 3 we generated a sha1 hash with the digits: c914 5abd c410 11b2 fc9b 32b9 d961 7502 076 0e28 which matches the hash provided by the vendor (Figure 2).

We further check to make sure that it is the exact file by typing in *sha1 ubuntu-16.04.4-desktop-amd64.iso | grep* c914 5abd c410 11b2 fc9b 32b9 d961 7502 076 0e28. This will compare the file with the hash from the vendor.


linux64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
beniii@b Unknown Application Name File Edit View Search Terminal Help
En
beniii@beniii-VirtualBox: ~/Downloads

```
beniii@beniii-VirtualBox:~/Downloads$ sha1sum ubuntu-16.04.4-desktop-amd64.iso | grep c9145abdc41011b2fc9b3
2b9d96175020760e284
c9145abdc41011b2fc9b32b9d96175020760e284  ubuntu-16.04.4-desktop-amd64.iso
beniii@beniii-VirtualBox:~/Downloads$
```

Figure 4: Comparing The Checksum

As we can see in figure 4 the checksum is an exact match as it was outputted in red, thus the file has preserved integrity and authenticity.

2.1: Assumptions Of The Integrity and Authenticity

Several assumptions were made with the ISO file, the first assumption is the authenticity of the vendor. Even if the checksum of the ISO file was proven a match if the file wasn't coming from a trusted and authenticated source the file could still be malicious.

If the file was already tampered with before we received it we would have no way of knowing since a checksum will only make us aware of any file tampering that occurred between the moment we download the ISO and received it.

2.0: Attack Detection – Anomaly Intrusion Detection Systems (IDS)

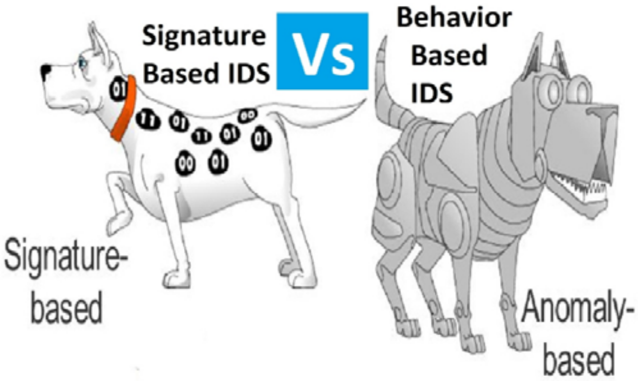


Figure 5: Signature Based Vs Anomaly Based IDS

Its entirely possible that an attack which involves a Trojan, backdoor or malware to go completely undetected by a signature or specification based IDS. However the attack may be detected by an anomaly based intrusion detection system.

The reason why a signature based IDS will fail is because a signature based intrusion detection system works by looking for particular code signatures. Since a Trojan is malicious code with a disguised code signature it would bypass the signature that the intrusion detection system is checking for.

A specification intrusion detection system would also fail because it works by setting traffic rules, the Trojan may have evolved and new traffic rules maybe required to prevent it from entering the system but since these new rules haven't been added the Trojan will bypass the IDS.

In contrast to the other two intrusion detection systems an anomaly based system operates by looking for irregular user or traffic patterns within the system. The Trojan horse may suddenly open a backdoor and suddenly the IDS will be alerted by traffic entering the system without the users permission.

The anomaly based IDS will suspect this behavior is unusually and detect it as some form of attack. Thus in this case scenario an anomaly based IDS is best since it is the most effective at detecting unusually network traffic.

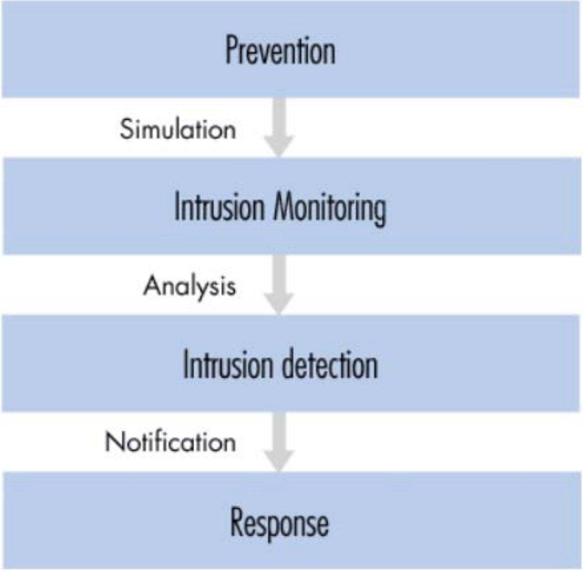


Figure 6: Intrusion Detection System Steps

3.0: IDS and Anti Malware Systems Similarities and Differences

One of the major differences between intrusion detection systems and anti-malware systems is the fact that anti malware systems block bad content from entering the system while Intrusion detection systems simple monitor the system and send an alert to the user of suspicious activity (Figure 6).

We can consider intrusion detection systems and Anti malware systems similar as they both implement signature, heuristics and behavior checks. However we can also consider them different since there methods/checks are implemented differently.

3.1: Similarities - Anti Malware Signatures Vs. Signatures Based IDS

Signature methods used by both anti malware and signature intrusion detection systems both operate by targeting a specific code signature which is based on the four different signature types, these are:

1. Full File
2. Partial File
3. Fuzzy Signature
4. String Signature

With a full file or partial file technique a file or packet will be put into its cryptographic hash and will be analyzed against the hash of a known malicious file or packet. If the hashes are a match the IDS will send an alert while the anti malware will remove and block the packet.

Fuzzy and string signatures look for specific structures and properties of the file these include symbols and/or headers.

In either case we can conclude that antimalware and signature based intrusion detection systems check the code signatures the same way, the only difference is an alert will be sent by the IDS were as with an anti malware system it will block the content.

3.2: Similarities - Anti Malware Heuristics and Behaviors Vs. Anomaly IDS

IDS anomaly systems work by checking for unusually behaviors detected within the system and then use some form of heuristic to determine if an intrusion has occurred.

Anti malware also implements heuristics and behavior check techniques, however they are implemented differently and perform differently. Nevertheless we can consider anti malware and anomaly based IDS check methods similar from a conceptual basis.

3.3: Differences - Anti Malware Heuristics and Behaviors Vs. Anomaly IDS

Although we made mention that anti malware and IDS anomaly systems can be similar as both implement heuristic and behavior checks they can also be considered different in the way they perform.

An anomaly intrusion detection system will try to figure out the systems behavior by profiling the user or the systems activity. Then it will use this information to produce a statistical analysis based heuristic to determine what is/what is not normal.

In contrast an anti malware system will try to find out the systems behavior by looking at the code and determining what it does. For example if we look at a car class we can determine what the code does by analyzing its behavior functions these include: run(), drive(), slow(), stop().

Anti malware also performs a heuristic check but it involves either active or passive heuristics. A passive heuristic would isolate the suspicions code and attempt to run it while a passive heuristic will try to see how it runs by looking at its code.

3.4: Conclusion

In conclusion IDS systems and Antimalware systems can be considered similar as they both involve using signature, behavior and heuristics methods. However they may differ in terms of how the techniques are implemented.

Furthermore an intrusion detection system will only alert the user of suspicious of activity were as an anti malware system will operate closer to an anti virus system and try to either isolate or remove the file packets from entering the system.

4.0: Why Signatures IDS is Popular

In contrast to the other intrusion detection systems signature IDS are the most stable and reliable therefore it is chosen over the other intrusion detection systems.

With a specification based IDS the users may not like the policy restrictions, with an anomaly based intrusion detection system the heuristics may be incorrect resulting in to many false positive alerts.

Thus signature based IDS is chosen because the benefits of implementing such a system are equal to the negatives.

For example with an anomaly based intrusion detection system you first need to have sufficient data on the user(s) or the system. Then once the data is available you need to be able to come up with some kind of heuristic.

Your heuristic may have calculated that if the user clicks on a login screen 3 times it might be an intrusion, but in reality this might be normal behavior for a particular user that keeps forgetting there password.

As a result by the 3rd time they try to log in to the system your heuristic will assume an intrusion has taken place and an alert will be sent which ends up being a false positive.

With specification based intrusion detection users may not like having certain policy limitations on what they may or may not be able to do with the system. User A might not like the policy of not being able to browse web content from a particular source, as a result user A may bypass the restrictions or the policy restrictions become relaxed. In either case the rules/polices implemented in a specification based intrusion detection become invalid

For all the reasons listed above signature based intrusion detection systems are the most reliable of all the intrusion detection systems.

5.0: Insider Attacks

5.1: Insider vs. Outsider Attacks.

When it comes to attacks Insider attacks are considered more dangerous then outsider attacks simply because the perpetrator has already been given access to the system. In contrast to outsider attacks were the outsider will first have to find a way to penetrate into the system and then gain access.

The insider also has the advantage of already being familiar with the systems protection policies and knows how to circumvent them. Even If the insider hasn’t been given access privileges the insider will know how to gain higher privileges simply by knowing the systems architecture and system policies.

Furthermore most system security mechanisms are built on the assumption that all threats will be coming from outside of the system and little emphasis is made on protecting the system from internal threats.

5.2: Insider Attacks Example

Rarely if ever do insider attacks involve malware or virus, in most cases Insider attacks normally involve data leaks or data being stolen. Some of the most recent famous insider attacks involve cases such as Edward Snowden and wiki leaks. These cases demonstrate how easy it is for an insider with access privileges to leak confidential data.

A simple example on how a data leak could occur is lets assume there exists a disgruntled teaching assistant they may or may not have complete access privileges as a professor but they have the ability to gain higher access privileges to access confidential data and potentially leak data.

6.0: Least Understood Concept

As previously mentioned by Dr. Somayaji intrusion detection systems are the least understood subject in computer security especially anomaly detection.

Since anomaly detection can lead to false positives if implemented incorrectly it would be interesting to clarify what are the algorithms that do work and why do the ones that don't fail.

7.0: Bibliography

Section 2.0 – 4.0

Malware Protection Techniques. Sourcefire. N.p., 4 Sept. 2012. Web. 20 Mar. 2018. <https://www.youtube.com/watch?v=7fgJvXwxFrs>.

"IDS Signatures." IDS Signatures :: Chapter 16. Intrusion-Detection System :: Part VII: Detecting and Preventing Attacks :: Router Firewall Security :: Networking :: ETutorials.org. N.p., 2008. Web. 25 Mar. 2018. <http://etutorials.org/Networking/Router+firewall+security/Part+VII+Detecting+and+Preventing+Attacks/Chapter+16.+Intrusion-Detection+System/IDS+Signatures/>.

Section 5.0

"What Is an Insider Attack? - Definition from Techopedia." Techopedia.com. N.p., n.d. Web. 25 Mar. 2018. <https://www.techopedia.com/definition/26217/insider-attack>.

Gregg, Michael. "Insider vs. Outsider Threats." Global Knowledge Blog. N.p., 23 Jan. 2012. Web. 25 Mar. 2018. <https://www.globalknowledge.com/blog/2012/01/23/insider-vs-outsider-threats/>.