Please restrain yourself to **about 15 pages of text**. This assignment is **individual only**.

Items such as appendices, reference lists, cover sheet and screen shots are not included in the 15 page count (although you can embed images in the text). A table of contents is not required for such a short report.

Note: **You are given multiple areas to choose from, you choose one topic from one area only. Not one topic from each area.**

Attack & Security Tools

Select one of the following topics and choose 1 attack and 1 security tool:

~~• Trojans and Backdoor---currently planning on using darkcomet rat in vm in order to infect a HOSTS file of a windowsxp machine or smth and ensure it always forces user to go to bank webpage suggested by hacker instead of the actual banking webpage~~

~~++look for all common Trojan and backdoor attack types---like what they usually do and how darkcomet and accomplish that!+++try to see how its hide from firewall tool works and how to use defense tool orr technique to overcome it~~

~~---protection tool? Maybe firewall?---try looking up if you can find any other onesthat can directly mitigate such Trojan attack….or prevent any writing to HOSTS file….or detect HOST file code injection and thus send out an alert to user regarding it?~~

• Viruses and Worms

**//////ask Jamie whether this approaches are adequate or not for the scenario:**

*Currently, scenarioes that you want to check for the theme “Self made Virus attack that evades antivirus”:*

*----her advice don’t use dark comet as its an old tool which can be detected. Instead make your own malware using MSF payload and use the options there to evade antivirus detection*

*“MSF payload –malware on kali—remote shell== ways to evade antivirus using MSF tools”—the malware can be a form of Trojan or just smth that sends an alert saying that “hey you got hacked” or “creates a new user” or “creates a certain file”*

*Victim case: XP Pro Control PC (the one where we tested other malwares)*

*Hacker case: Using Kali to build and send it*

1. *Turn on the “hide from firewall” or smiliar feature when creating feature of malware and see how it attacks the pc*
2. *Do (1) except, keep firewall running*
3. *Do (1) except, use specialized detection tool running*

*For all 1,2,3 cases:*

1. *find the malware files or traces left by it---detection*
   1. *In rest/ inactive phase of rat*
   2. *In active phase (like using commands from hacker pc to send alerts to victim pc)*

*b) remove the malware files or traces left by it---mitigation*

* 1. *In rest/ inactive phase of rat*
  2. *In active phase (like using commands from hacker pc to send alerts to victim pc)*

*Matric to measure:*

*Time taken to detect*

*Locations where it was detected*

*Time taken to remove*

*Locations from where it has been removed (and any place where it still remained or got quarantined)*

**////////Ask the above part to Jamie**

• Sniffers

• Phishing

• Denial of Service

• Buffer Overflows

You will need to research 1 tool attacker’s use, and 1 security tool used to counter attackers in the area chosen. Your assignment involves running both tools, evaluating and analysing their use in means to evade or detect threats/detection. That is, how are you going to use these tools? To show how attackers can bypass detection, or how tools can be used to detect this threat type? Or show how both operate? From this perspective, you should justify your choice (over others), install, run and demonstrate the use of tools, producing some output or results. You should analyse and evaluate the usage and results from both attacker and defender perspectives, and potential impact. Be sure to discuss threats and countermeasures of these risks.

---no specific format---maybe check online?

Topic: “Trojans and Backdoor: How MSF enables code to evade the firewall and antivirus detection”

Need to have:

1. Cover page
2. Coverpage2 (with student details and stuff)
3. Introduction-----page number will start from here following the double page printing technique and pg numbering

--say what the document will cover and focus on and what topic had been chosen + what tools have been used and general importace of topic (make it brief, at max just one para on it)

Then list the machines + tools used (and their OS and other stuff in table like format)

(Put as a note saying that rationale will be provided in the justification and planning part)

1. Justification and planning

Scenario, choice of tools, threat/topic choice

[High level of justification has been provided with relevant examples. Landscape challenges have been highly consulted through reference, needs outlined and choice of tools,]

Describing background of the attack and defence in depth:

**(Background of topic):**

Say how things are in modern times regarding user and softwares and internet stuff… then jump into attack vectors and malwares (give examples, references and possible stats like any recent attack that took lots of data or smth…)

Then say smth like luckily there are various ways to protect our computers from these types of attack (give examples of some protective measures). But basically they can be divided into two types: a) preventing harmful software from getting into our system (by using softwares like……firewalls and stuff…) and b) quarantining and removing any that are already in the system (like antivirus and other malware detection tools…..)

But even so these are not fool proof leading to various level of impact (link to level of impact on individual customers, small companies and big companies)

So , in order to investigate how malware (focus on malicious code aspect) both gain entry and avoid detection, I have decided to setup the following scenario:

(((<https://www.google.com/search?q=when+was+Metasploit+Framework+created%3F&client=firefox-b-d&sxsrf=ALiCzsZbc6eL_H_JYfdytC6g12thwudqbA%3A1665786181581&ei=ReFJY9GEI7-x4-EP_fuguAk&ved=0ahUKEwiRu_-M4eD6AhW_2DgGHf09CJcQ4dUDCA0&uact=5&oq=when+was+Metasploit+Framework+created%3F&gs_lcp=Cgdnd3Mtd2l6EAMyCAghEMMEEKABOgoIABBHENYEELADOg0IABDkAhDWBBCwAxgBOgUIABCiBEoECE0YAUoECEEYAEoECEYYAVDrBViaCWDxDWgBcAF4AIABsAKIAeMDkgEHMC4xLjAuMZgBAKABAqABAcgBDcABAdoBBggBEAEYCQ&sclient=gws-wiz>

---link on when meterpreter had been created---may be useful for later)))

((Malwarebytes—antivirus released in 2006))

((XP released iin 2001))

((meterpreter released in 2003))

Describe scenario

**(Scenario:)**

[add a note here saying that here the literature part of scenario has been given, whilst the technical parts (regarding attack and defence tool setup and function) have been documented in the…….paragraph]

“….explain the scenario---like imagine a student is studying in 2006. He is using Windows XP in order to do his work and is suffering from storage issues. When he discusses about it with his friend, his friend take a moment before suggesting him to download a new secret tool called “CleanItUp.exe” from a certain website following the link:”……” which can clean up unnecessary files in the background and free up space. But since it’s a free software, windows doesn’t like it and thus tries to scare people off by saying that it’s a suspicious file or smth, so don’t listen to it. So the naïve student follows his friends’ advice and downloads the tool.

But since the website and file looks suspicious he runs the file across his antivirus (malwarebytes ) just in case. But antivirus didn’t detect anything and instead said everything was alright.

In the meanwhile, his friend had gotten access of the entire system and now could do anything on it. He tests it by putting a folder called “Cleaner” in the desktop of the student.

Seeing the new folder empty pop up, the student had been surprised and ran the antivirus software again. But again the software didn’t detect anything, causing student to believe it was just a normal occurrence”

Summary of scenario:--show in table format

OS used by naïve student (victim): Windows XP

Firewall used by victim:

IP address of victim:

AntiVirus used by victim:

OS used by his friend (culprit):

Tools used by culprit:

IP address of culprit:

Rationale behind scenario and the tools used

Why is this scenario used?

--retionalise the use of XP and Kali (like already available in VM, had necessary tools to simulate how attack would have been using this tool in that time) [Here add note that although Kali was most probably not available at that time, other Linux based OS were already there since 1991 (reference google…..) and they would have worked in similar manner]

--rationalise the use of the tool and payload or code……using it as proof of concenpt, so diddint want to damage the machine, instead just see that it was possible

+ say that here you are only passing built in payloads in MSF that only lets the user access the information present in victim’s computer …..not wanting to damage the VM in any irreversible manner…gaining access provides more flexibility then directly attacking…..can be used as test of concept as we can also craft custom payloads (using tools like….. [reference]) which can be used to used to pass actual malware through the system without detection

--rationalise use of firewall and antimalwarebyes (used )

Say that you used firewall as default one as most users tend to use the firewall that are inbuilt and instead rely on their antivirus for majority of the protections (try to give ref statistics chart or diagram for this)

Then say that since malware evading firewall has big impact or smth, you decided to investigate how it exactly does this, using tools such as……. For attack (~~say all the tools + languages used in order to craft the packet~~……Just Say MSF tool) and for defence you are using basic windows firewall

+ say that here you are testing it on windows XP pro control and attacking using Kali as…..VMware currently being used in course so well versed +…. Want to see how malware used to evade detection of firewall in past and try to use it to see if modern malware also used similar methods

Purpose of scenario:

--say in bullets (like checking whether it can bypass firewall and antivirus in both active and inactive stages in attacker POV)

Criteria of Success

--Say in bullet points (attacker able to get access to terminal + attacker able to puc in file ++ in both active and inactive cases (ie inactive vs active firewall, passive vs scanning antivirus))

Matric: just observing whether detected and stopped by fireall and antivirus?

1. Application and documentation ~~(change this title to “how the scenario had actually played out”)~~

Running of tools or solution, analysis software, etc., and the knowledge, security aspects. Assignment documentation as a whole

[In-depth documentation and high functionality configured. Leading tools have been chosen, and working. Security  
functionality (Goodware/Malware) is discussed in-depth. Report of is excellent quality.]

Show attacker side pre-setup: **(no need screenshot for steps, just define them in brief)**

How to use MSF works and how to pass simple payload through it

+perfrom obfusication(reference definition and also journal that explains what this concept is) technique to bypass firewall

Show defender side-setup:

How to setup firewall for general purpose

+ running antimalwarebytes

Show attack details

What happens during attack

Success or failure?

Message triggered? Or firewall detected and stpped or both? Or smth unexpected or new?

Was antivirus able to detect it or not?

Was the new file created?

Was the antivirus able to detect it again after new file had been created?

Put screenshots of attack outcome for all 4 cases

(fireall on and off, anti virus passive and active scanning mode)

1. Analysis (results + discussion)

Understanding the results achieved, analysing the impact/use/practicality/etc.

[Excellent analysis is presented. Connections are made across the topic and security landscape, along with future challenges. The analysis has been linked to aims. Both attacker and defender concepts, impact, challenges and considerations are compared and  
contrasted. These have been given considerate depth. The student has demonstrated excellent level of knowledge to analyse Criteria 3]

Elaborate and rationalize the findings:

Ie detected or not by both firewall and antivirus? Why or why not?

(explain in depth for both firwarewall and antivirus case and explain how the msp payload had been hiding from both)

Why was Creation of new file not detected?

(explain how reverse shell works and why creation of new file had not caused any alarm by the antivirus)

Judge on whether attacker success or defender successful—one line or smth

1. Evaluation (conlusion)

Effectively judge/critique/summarise the result, challenge, usage and/or threat/need within the security landscape

[Thorough and high evaluation of tools, threats, challenges, usage, results is given. Depth is shown, and contrasting and  
consideration is provided across previous, current and future factors. Relevant and evaluated support through reference is  
given]

What does this mean? Can we use it to pass malware into firewall and antivirus? How? (for current and mordern) + consider feasibility of scenario for single user, small business and large business. Are all of them vulnerable to this attack? What about attack of an upgraded version or similar type? Can their protection still be bypassed (hypothetically?)

Potential solution to this problem? ---(say it briefly in bullet points if possible)

How to improve the current firewall or antivirus to protect ourselves? to detect the thing? Or maybe use any other tool or detecting it? Brief idea on how it would work and what it would detect and any sample detection tool name

Current stage of firewall and antivirus setup, will it detect it? Why or why not?

Any tools it can use to support this detection?

Possible solutions used: <https://www.hacking.reviews/2017/03/how-to-set-and-bypass-outbound-rule-in.html?m=0> (setting rule to prevent access to that port, but that can eb bypassed by using different port

---so best case scenario---close down all ports excepts ones which are currently in use ---ie white listing method ig (block everything other than that which you absolutely need)/)--+ reference the course materials as well for the topic mentioned

(like say it had been mentioned in the topic in week… by…. in this course….and then you decided to look it up more and found out that it was for… and meant…. And thus can be used as the most effective solution to this type of issues as it prevents the payload from communicating with culprit PC and thus prevents malware from having any effect )

Thoughts or words for the future? (both attacker hiding and defender detecting)

(brief one line or two line for concluding the entire thing)

1. Reference