Homework #2

Mike Pendleton

John Hulett

West Texas A@M University

**CIDM 6340 Network Management & Information Security – Fall 2021**

**West Texas A&M University**

Homework #4

***[N.B: You can work with a team/group of MAX 5 students, but you need to submit your own Homework report. Also, please mention all group members name in the cover page]***

**Name : \_\_\_\_\_\_\_\_\_\_\_Mike Pendleton\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Id:\_\_\_\_** **1058201\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Rubrics:**

*Full points:* Correct and complete answer.

*Partial points:* Correct but not complete answer.

*No points:* No answer or Incorrect AND incomplete answers.

**Q1. [10 points]** What kind of information can you gather with Kali? List top five tools for security information gathering. <https://resources.infosecinstitute.com/topic/kali-linux-top-5-tools-for-information-gathering/>

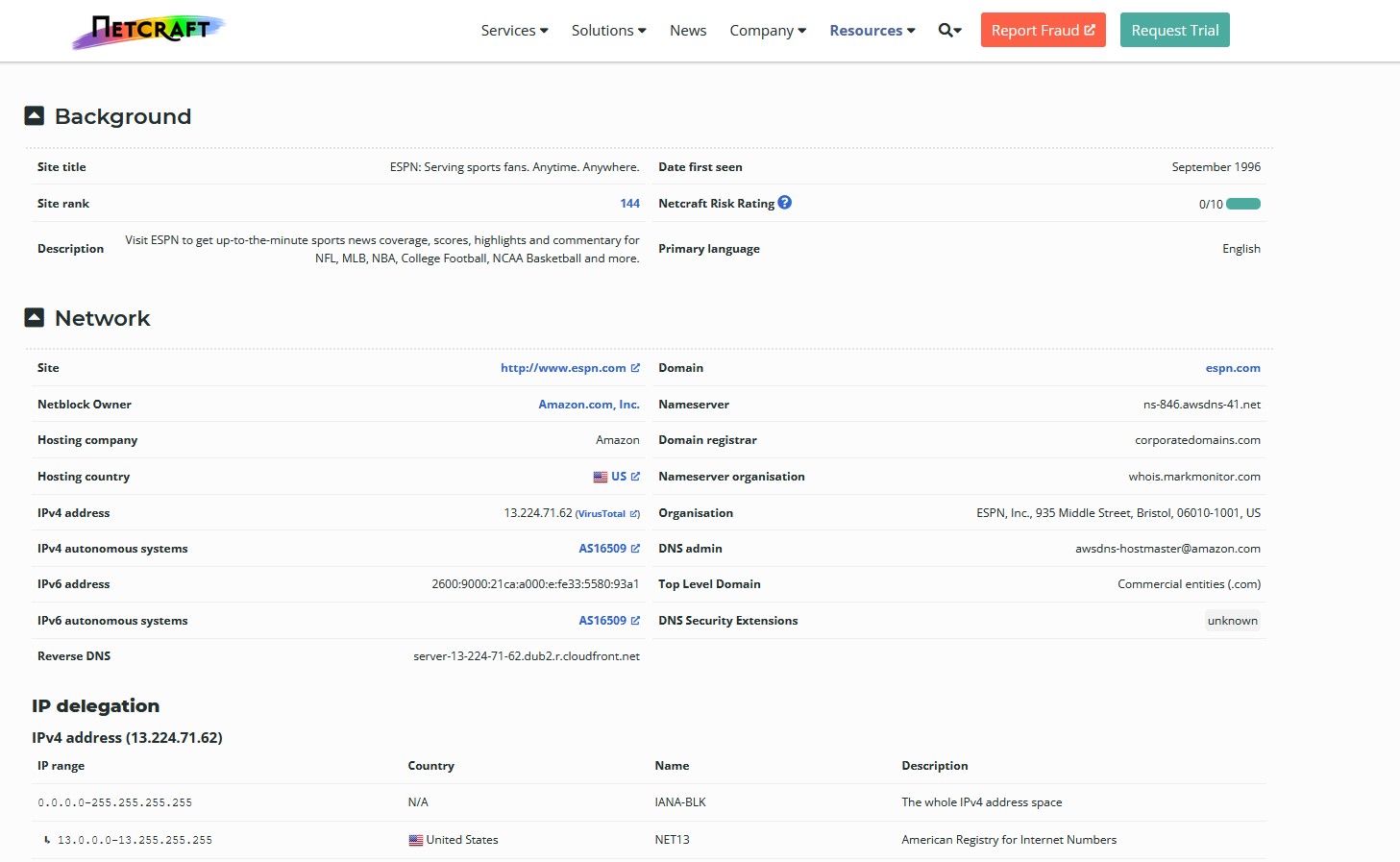
Visit [www.netcraft.com](http://www.netcraft.com/) and do a search on at least three different websites of your choosing. Note/screenshot what information you can gather about each website. You can use Site Neighbours or Search DNS results.

The top 5 tools are:

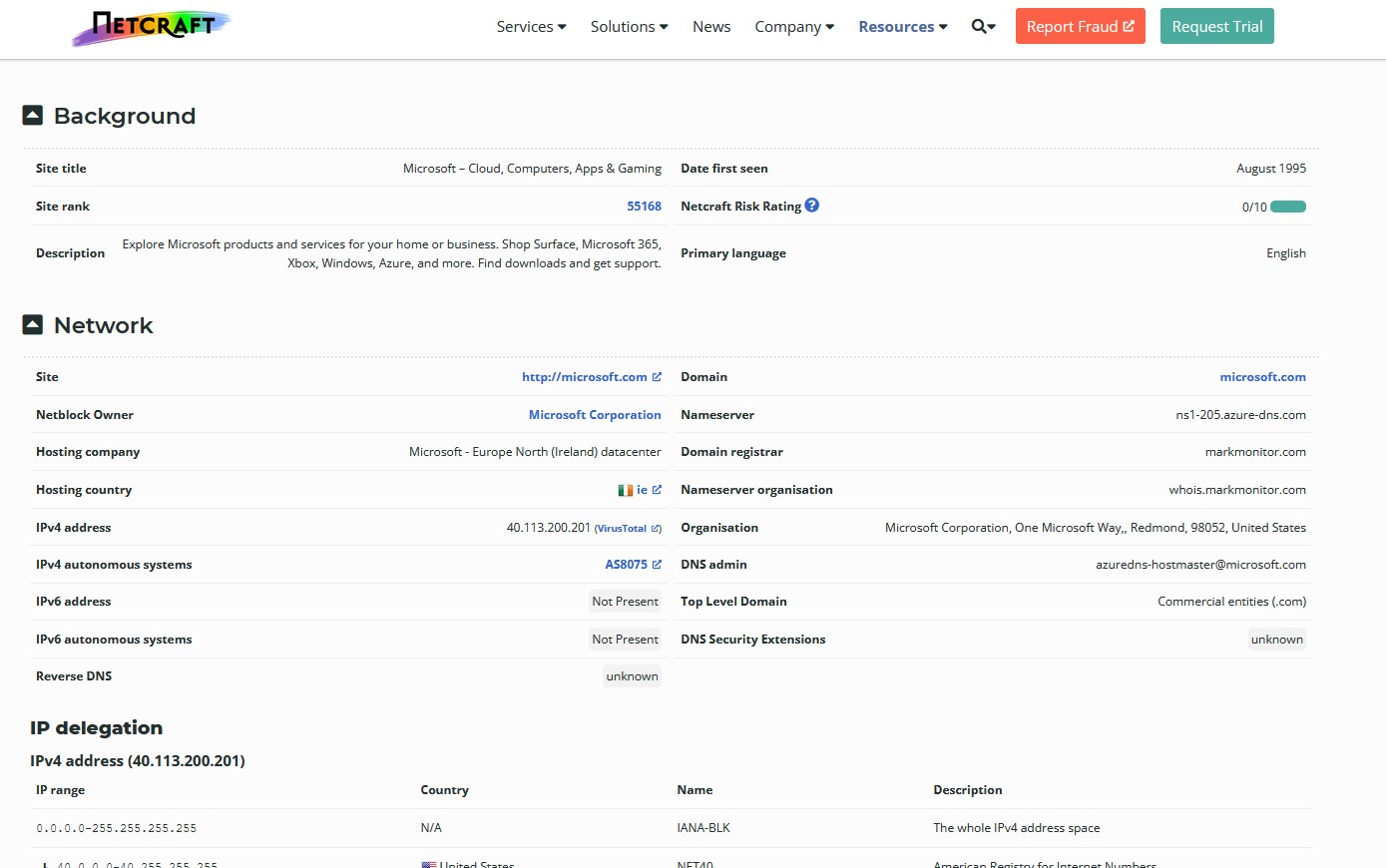
1. NMAP – port scanning for live host on the network
2. Metasploit – used to determine vulnerabilities
3. Maltego – graph-based data mining that can gather ip ranges, domains and devices on the network
4. Wireshark – packet sniffer to look at traffic on the network
5. Netcat – can be used to establish connections between hosts on the network

Search 3 different sites. You will see the hosting company, ip address, domain registrar, top level domains, the country the ip address is registered in… and more.

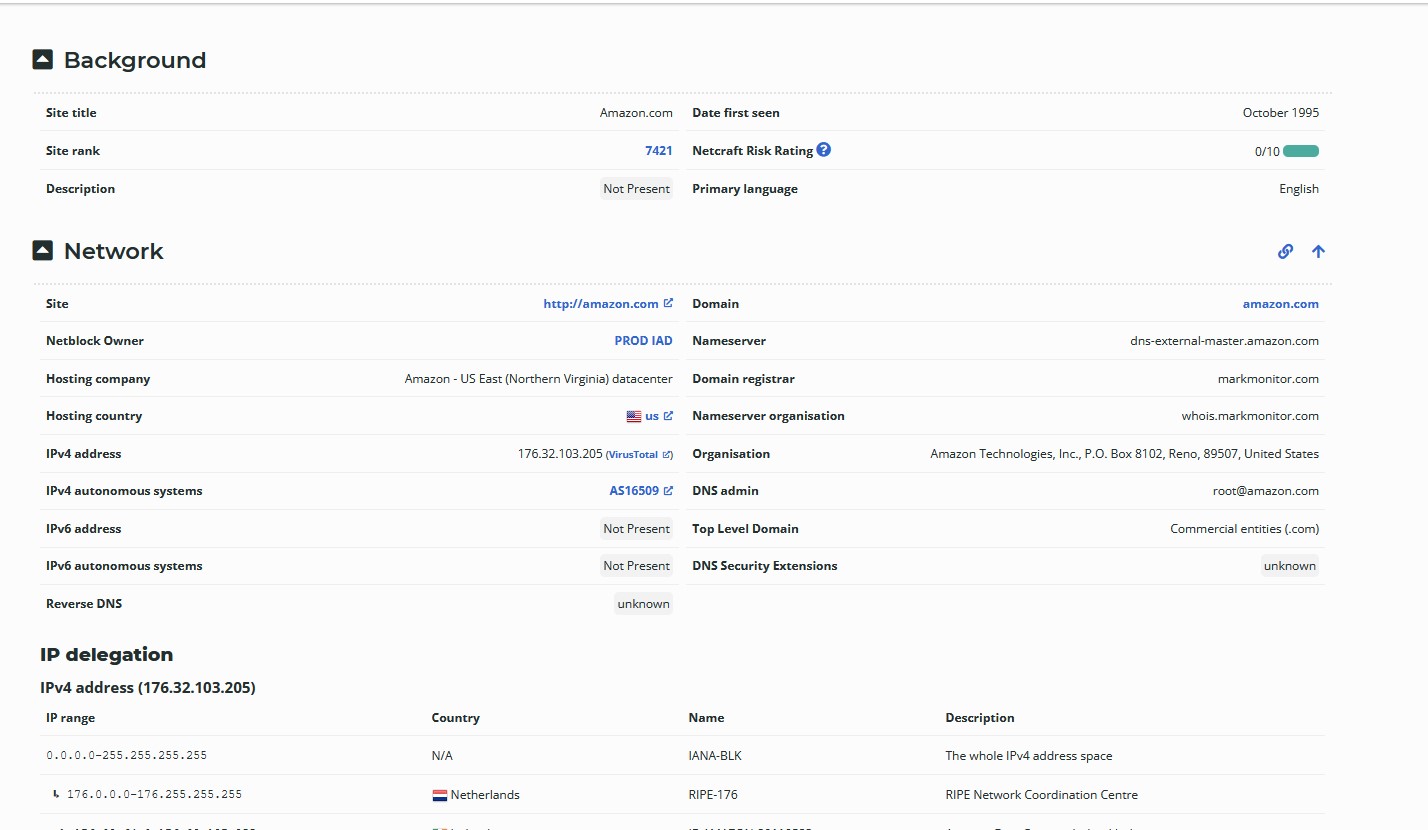
Espn:



Microsoft:



Amazon:



**Q2. [10 points]** List (you can also make a table) top cybersecurity companies and their functions. <https://www.thesoftwarereport.com/the-top-25-cybersecurity-companies-of-2020/>

Select a local organization and conduct passive reconnaissance on it. This should include searching job boards, the organization’s own website, user groups/bulletin boards, social networking sites, [www.archive.org](http://www.archive.org/), and more. Gather as much information about the target network as you can.

**Answer:**

**Part 1: List of Top companies and their functions**

|  |  |
| --- | --- |
| Company Name | **Function** |
| McAfee | California-based security software company also works with governments around the globe, relying on its McAfee Global Threat Intelligence to keep businesses, governments, and consumer’s one step ahead of hackers. On the business front, McAfee’s endpoint and mobile security products protect end-user devices from attacks, while its network security products and services protect company servers, databases, and data centers. For home users, McAfee provides security software to protect mobile devices and personal computers |
| Palo Alto Networks | The company’s core Security Operating Platform helps keep hackers out by utilizing analytics to automate routine tasks and enforcement, simplifying security so customers can focus on securing users, applications, and data. The platform is optimized for a variety of industries, including financial services and healthcare. The global cybersecurity company also provides cloud security, advanced firewall, endpoint protection, and threat detection and prevention. |
| LexisNexis Risk Solutions | Provides content-enabled workflow solutions in risk management. Its risk solutions give customers decision tools that combine public and industry content with analytics that help evaluate and predict risk. |
| CrowdStrike | cloud-native endpoint security platform on the market |
| SecureWorks | offers network, IT, and managed security solutions focusing on information security services |
| Infoblox | Helping customers secure their networks, including Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), and IP address management (IPAM), collectively known as DDI. |
| Darktrace | Cyber AI company that created Autonomous Response technology. Its machine learning AI is modeled on the human immune system and is used by more than 4,000 organizations to ward off threats to the cloud, email, IoT, and network systems. |
| Code42 | Dedicated to securing the collaboration culture for enterprises and building its services around insider risk detection and response. |
| Generali Global Assistance | identity theft resolution services, and since then, has expanded their identity/cyber product line to offer a comprehensive suite of services |
| Hack The Box | platform that lets organizations experiment with their penetration testing skills and exchange methodology information with the community |
| A-LIGN | technology-enabled cybersecurity and compliance firm that specializes in helping companies to navigate their security needs and mitigate cybersecurity risks |
| Sonatype | cybersecurity-focused open-source automation also scales DevOps through open-source governance and software supply chain automation |
| Cybrary | platform for cybersecurity professional development, offering content from top experts and leading organizations |
| Deep Instinct | Applies advanced AI and deep learning to the prevention and detection of malware. |
| White Ops | detects, prevents, and outwits bot populations at every level of sophistication. The "pro-privacy and pro-human organization" uses privacy-sensitive code to detect bots without tracking humans |
| ThreatQuotient | helps organizations achieve a successful threat management and security operations program. By enabling responsible automation, improved defenses, and overall security efficiency and effectiveness |
| SlashNext | cyber-attack detection and IT solutions. protecting users from phishing through its proprietary technology that detects zero-hour phishing threats |
| Intezer | Malware Analysis technology to focus on cyber threat detection and response |
| Red Sift | Helps organizations defend against costly cyberattacks using its Open Cloud data analytics platform. It uses AI to compute and visualize data from thousands of individual signals to optimize cybersecurity |
| GTB Technologies | provides data protection cybersecurity solutions preventing loss of data from malware, competitors, and insiders. It blocks sensitive data in real-time on- and off-site, in the cloud, or as a managed service. |
| TrueFort | uses an application-centric approach to protect cloud, hybrid, and legacy environments from hidden risks. |
| CTM360 | Fully managed Digital Risk Protection (DRP) platform that detects and manages vulnerabilities and threats across the surface, deep, and dark web |
| ThreatLocker | is a tool for endpoint security that gives companies control over what applications run on their networks. It protects companies from ransomware, malware, viruses, and other types of security threats from permissions to applications. |
| Gray Analytics | Focuses on a broad spectrum of cybersecurity needs for government and commercial customers. It offers personalized, end-to-end support services from supply chain risk management to enterprise cybersecurity. |
| RevBits | provides the marketplace with four robust security solutions and a full range of cybersecurity services. RevBits product range covers Email Security, Endpoint Security, Privileged Access Management and Deception Technology. |

**Part 2:** We chose [Mid-City Custom Pools, Inc](https://www.manta.com/c/mm5kft4/mid-city-custom-pools-inc).

Address: 7700 Precinct Line Road Hurst, TX

Website: <https://www.midcitypools.com/>

Blog: <https://www.midcitypools.com/blog/>

Facebook Page: <https://www.facebook.com/midcitypools/>

Instagram: <https://www.instagram.com/midcitycustompools/>

Email: [**sales@midcitypools.com**](mailto:sales@midcitypools.com)

Social Site Statistics 🡪 Instagram [126 posts](https://www.instagram.com/accounts/login/?next=%2Fmidcitycustompools%2F&source=profile_posts), [193 followers](https://www.instagram.com/accounts/login/?next=%2Fmidcitycustompools%2Ffollowers%2F&source=followed_by_list), [523 following](https://www.instagram.com/accounts/login/?next=%2Fmidcitycustompools%2Ffollowing%2F&source=follows_list). Facebook 682 people follow, Yelp rating is 2 ½ stars with 28 reviews

Facebook newsletter page does not work

Owners Don & Tina Pierce, no other information on the staff found

No API’s found as this is a service company

**Q3. [10 points]** What do you mean by demystifying a keylogger? <https://home.sophos.com/en-us/security-news/2019/what-is-a-keylogger.aspx>

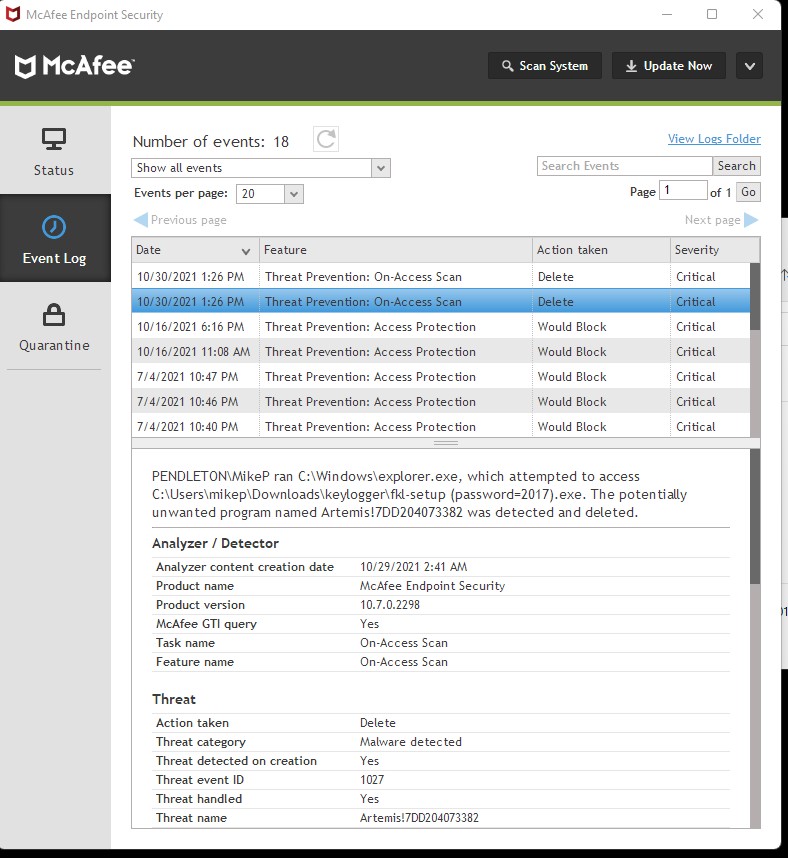
Note that this exercise may only be completed on machines where you have explicit permission to do so (not on public computers).

1. Using any website, find and download a key logger. The following websites might help you locate a key logger: [www.kmint21.com/familykeylogger/](http://www.kmint21.com/familykeylogger/) and [www.blazingtools.com/bpk.html](http://www.blazingtools.com/bpk.html) .
2. Install the key logger on your PC.
3. Examine how the key logger behaves on your machine. Do you notice anything that might indicate the presence of illicit software?
4. Run an antispyware software. Does the antispyware software detect the key logger?

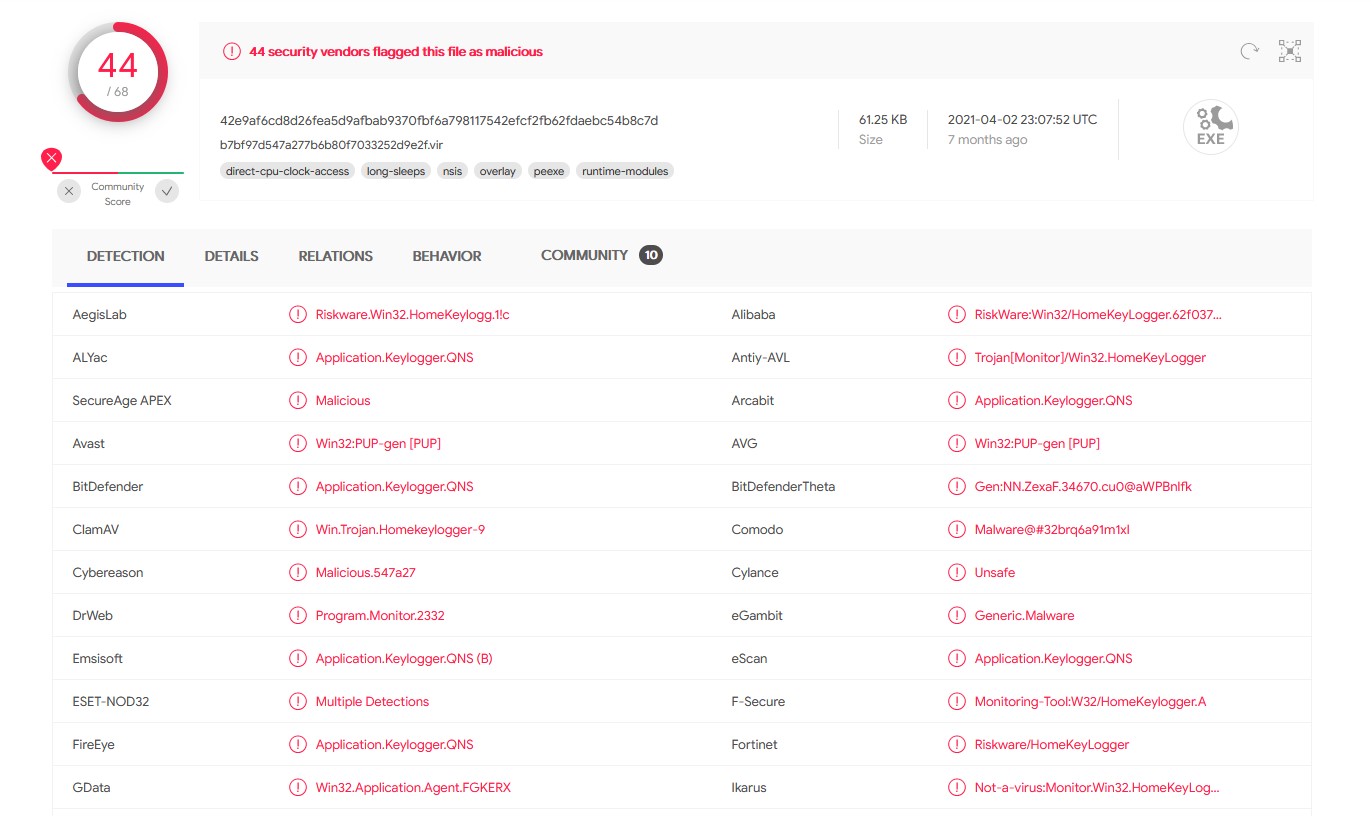
I downloaded home KeyLogger

Immediately after extracting the file, McAfee Endpoint Security detected the threat with the analyzer method on access scan. This logger is detected threats in two ways:

1. This threat is covered in the dat
2. There is also an artemis detection. An artemis detection is detected through McAfee’s global threat intelligence database. All threats detected here are artemis!(Generic letters are then added to create the detection name)



1. The detection type for this is a PUP (potentially unwanted program)
2. Due to the amount of vendors that do not trust this pup, I prefer to not move forward and disable on access scan as without knowing exactly what it can do, or is coded for would possibly leave the system is an undesireable state. Though the AV can potentially clean it later, I would like to avoid the attempt because the coded behavior could have changed on remediation from the first instance on what Malware Labs was able to determine what registry and file level changes this software makes.
3. Below is a screen shot of virus total:



**Q4. [10 points]** Google has uncovered espionage malware, which monitors and steals information about the target --including emails, messages and calls**.**  Using the Web, find and download a screen-capturing spyware application. <https://www.zdnet.com/article/this-android-spyware-can-record-calls-take-screenshots-and-video-targets-gmail-linkedin-snapchat/>

The following website might be helpful to you in selecting an appropriate product: <http://en.softonic.com/s/screen-capture-spy-software>. Warning: Since you are downloading spyware, it is likely that your system’s antivirus/antispyware will give you a warning.

1. Install and configure the application on your computer.
2. Run the application and note what it finds.
3. Run the antispyware and see whether it detects your spyware program.
4. Take screenshots and write ½ page critic on this software.

**Answer:** We chose not to download and install Employee Desktop Live Viewer

This software is designed to be used by employers to monitor their employee’s activities secretly by recording the screen. This monitoring is Invisible, with Uninterrupted Surveillance.

From the security perspective of the organization this can be a key tool in preventing or detecting employees that are potentially doing things to harm the network. This can also help with building security training programs to better inform the staff on potential network security threats. The tool can also assist in investigation of certain types of attacks as long as the network and data was not encrypted and the recordings are available. The bad side of this is that it adds to the complex issue of privacy and whether the employer trusts its employees. As I.T. professionals we are very aware of cyber security threats and understand that security monitoring is required to help maintain a secure network, however non I.T. folks seem to fall in the “you invaded my privacy” by monitoring what I am doing on the company network.

**Q5. [10 points]** How Does the Microsoft Firewall Work? Using Microsoft documentation, the Web, and other resources, find out what methodologies the Microsoft Windows (whichever version you are using) firewall uses. Write a brief essay explaining the strengths and weaknesses of that approach. Also discuss situations in which you feel that approach is adequate and those in which it might be inadequate.

I do not believe that windows firewall is adequate.

1. Since working at McAfee in Security and supporting our firewall product there are several advantages that McAfee firewall does that windows firewall cannot do.
2. Windows firewall is stateful, but will allow the connection from the client system if the communication started from the client, to the server and the communication back. This alone is dangerous depending on what is in the traffic returned from the destination.
3. All firewalls allow rules to be configured to harden the firewall further.
4. Software firewall, even McAfee’s should never be leveraged alone as a firewall is not also an IPS/IDS by default. Hardware firewalls are essential and should be used in conjunction with software firewalls.
5. McAfee firewall also includes additional options that windows firewall is not efficient with.
   1. Location based awareness
      1. You can implement a location based on gateway/dns/epo server availability
      2. This enables two rule sets to be enabled.
         1. Less strict rules can be in place while connected to the vpn or if the client is in the office.
         2. Strict rules will be enforced when the client is off vpn and not in the office.
6. While it is highly possible that I am biased due to working with McAfee firewall solutions over five years, I am attempting to explain my clarification on why and there are better software for firewall’s than what comes with the operating systems install.

**Q.6** **[10 points]** Briefly explain a Network Intrusion Detection & Prevention System. Go to the Snort.org website ([www.snort.org](http://www.snort.org/)) and download Snort. Using the vendor documentation or other resources, configure Snort. Then use port scanners on the machine that has Snort configured and note whether Snort detects the scan.

**Answer:** A network intrusion detection and prevention system is a combination of software that automates the intrusion detection process as well as the ability to attempt to stop possible security threat incidents. IDPS technologies use many methodologies to detect attacks. The primary classes of detection methodologies are signature-based, anomaly-based, and stateful protocol analysis, respectively. The IDPS system has the following components. Sensor or Agent, Management Server, Database Server, and a Console. IDPS offer broad detection capabilities, with some configurations or tuning to increase the detection ability. Thresholds, Blacklists, Whitelists, Alert Settings, and Code Viewing and editing. There are different types of IDPS technologies such as Network-based, Wireless, Network Behavior Analysis and Host-Based. Organizations can utilize a combination of the IDPS technologies.

Snort did not find a port scanner using Microsoft IP Port Scanner software

**Q7. [10 points]** What is IT/Cyber Disaster Recovery Plan? Using the knowledge you have gained far, create an IT disaster recovery plan for an organization. You may use a fictitious organization, but a real organization would be better. You may find the following resources helpful: www.cert.org [www.sans.org](http://www.sans.org)

Disaster recovery plain should include the business analysis.

1. The cost of a down situation on how much it would cost if all I.T services are down per hour.
2. The cost of a cold site should be considered as there are greater risks that could damage the integrity of the organization if down time exceeds expectations.
   1. I have designed disaster recovery plans in the past, so I will explain what I implemented.
      1. Cold sites though are expensive is an easy way for plug and play for disaster situations. Adding a cold site will create a separate data center, so that if datacenter A was hit by a tornado for instance, then all traffic would be routed to datacenter B limiting the amount of downtime.
      2. Backups are crucial. Create backups daily and then move the backups to the cold site. I prefer to do full backups bi-weekly and the other 13 days would be incremental backups. This insures that the incrementals would not be corrupt and simply not knowing until they are needed is important to maintain several types. Always create backups for the backup.
      3. Carriers can be leveraged for secure movement from site to site backup delivery, if the cold site is not connected to the wan where a data transfer could be done otherwise.
      4. Maintain the full network in the cold site. DC’s. DNS, IPS/IDS, management applications and server os/Hardware…etc. The cold site should mimic the primary site so there is a smooth transition if needed.
      5. Additionally cold sites are not meant to sustain longevity as the primary goal is to get the primary site back to normal conditions and then route the traffic back to the primary site when those conditions are met.
      6. In the present, cold sites also offer a greater value of return due to the expansion and preferred malware being used today with “ransomware”.
         1. If the primary sites primary servers go down, simply transition over the backups and restore the OS’s. Since backups were maintained then once the exploit is taken care of, simply move back to the primary site after the backups have been restored and the malicious payloads have been resolved in the environment.
      7. Disaster recovery methodology is also the reason why organizations pay for pen tests. This way exploits can be resolved before a malicious author can find and infiltrate them.

**Q8. [10 points]** What do you mean by the ethics of investigation?

Write an essay discussing the ethics of online investigations (e.g. finding phone numbers, criminal records, court cases etc.). Do you feel these investigations are an invasion of privacy? Why or why not? If you do feel they are an invasion of privacy, what do you think can be done about it? Are there problems with getting inaccurate information?

Answer: A) Ethics of investigations are the moral principles that define how an investigation should be conducted. Investigators must know the laws of the land to be able to conduct an ethical investigation. While investigating it’s important that the investigator is not breaking laws or circumventing processes that would lead to an unjust result.

B) The ethics of online investigations at its core is similar to other types of investigations in regards to how and why the investigation is being conducted. Regardless of the type of investigation both legal and ethical practices must be followed. Consider that the online investigation is being done as part of a criminal or civil case then the federal and local laws, and statues on how to conduct the investigation must be followed. Since most states make phone numbers, criminal records and court cases public information that are not protected by the patriot act then there is no invasion of privacy as this information can be obtained by going to the appropriate department and requesting the information. If the investigators use social media websites or other websites to obtain protected information such as contact lists, health records, and financial information without the proper warrants then yes these tactics are an invasion of privacy. The reasoning for the stance is that, the investigators should only need to focus on information vital to the case and not gather information that can persuade a judge or jury on the ruling. If it’s a criminal offense that does not involve financial liabilities or gains then the accused should have the right to privacy on how much money they have in their accounts. If the person is wealthy and the news publishes it this could sway people to be unfair. The invasion of privacy is a subject is a topic that is more and more prevalent in conversations around the country. With social media sites, cell phones, emails, cameras in stores and on streets, organizations using software monitoring tools to capture employee’s activities it’s difficult to evade to have complete privacy. On one side of the argument you have people who conclude that we don’t need big brother monitoring our every move with social media site scanning, camera’s and phone tapping, and on the other side people believe that if you are doing something wrong then what is the harm. For me I fall somewhere in the middle, privately I don’t want my privacy invaded, however when I am at work I realize that the company must employ security measures to protect their employees, network and financial assets. There are many potential problems with getting inaccurate information, especially from social media sites. Do we really assume that John Doe lives where indicated on the site, is the age stated, is even the gender indicated. A general assumption in my experience is that investigators should be like software developers, verify (validate) data often, and re-verify as well as don’t assume the data gathered at that point tells the entire story of the investigation.

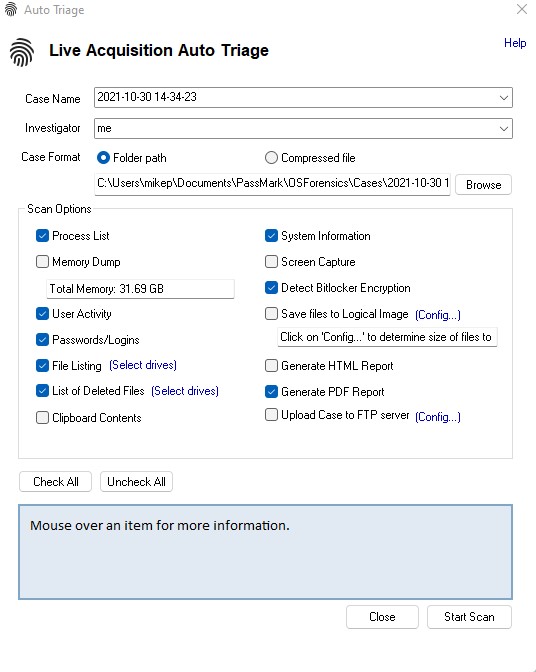
**Q9. [10 points]** What do you mean by computer forensics? OSForensics : Download a trial copy of OSForensics from <https://www.osforensics.com/osforensics.html>.

Using tutorials at <https://www.osforensics.com/faqs-and-tutorials/video_demonstrations.html>, perform basic forensics on your own computer with OSForensics.

OS Forensics is used a lot by policing bodies such as local law enforcement, all the way up to the FBI. The tool is able to provide a forensic analysis of systems and determine what passwords are (the tool can decrypt and display the passwords), determining files that have been deleted and restore them, memory dumps and more.

This is so that a deep dive into the the system in order to find information on what someone may be hiding in order to help complete an investigation. Case numbers assignments are created in order to separate one case investigation from others.

The software has been crashing on me for some reason, but I have used the software previously in my white hacking class at Tarleton State, were I have my bachelor’s degree with that university.

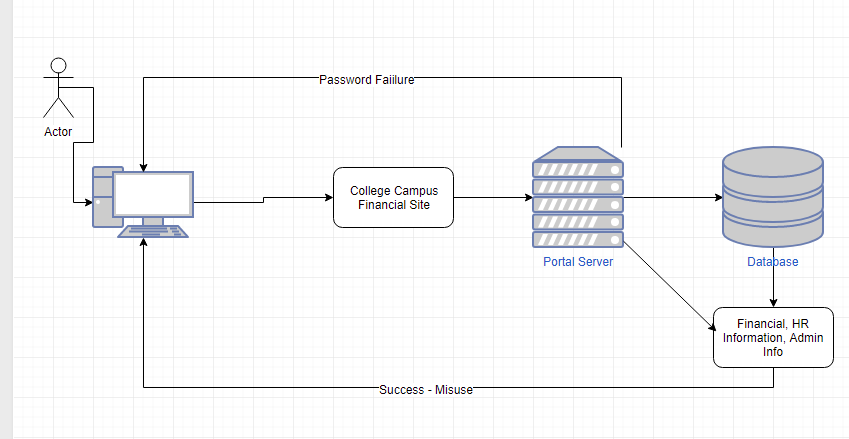


**Q.10 [10 points]** Name some cybersecurity analysis and modeling tools. Consider the cybersecurity requirements of a college campus. Create a misuse-case diagram for a specific type of attack. Also, Create a requirements traceability matrix for penetration testing a campus computer network. You can choose any attack described in this book.

**Answer:**

1. Analysis tools are Wireshark, Nmap, Ncat, Metasploit, Nikto, and Nessus.
2. In a brute force attack a hacker tries millions of most common password combinations in only a couple of seconds. This is known as a brute force attack. To avoid such attacks, a system should ensure that they set up a difficult and complex password, enable multi-factor authentication, and configure remote access.

Misuse Diagram for Brute Force Attack



Penetration Testing Matrix

