Case Project 9-3: Application Patch Management

Select four applications (not OSs) that you frequently use. How does each of them address patch management? Visit their websites to determine what facilities they must alert users to new vulnerabilities. Are the patch management systems adequate? Write a one-page paper on your findings.

- Gmail

When we use our own Google accounts and click on the promotional or social tabs in Gmail, we'll see advertisements that have been selected to be the most beneficial and pertinent for us. Targeted advertisement selection and presentation in Gmail are both fully automated. These adverts are shown to us depending on how we behave online when logged into Google; they do not, however, go through email content to show us ads for work or school accounts.

Google protects our account from fraudulent activity and unauthorized logins by monitoring a number of security indicators. Additionally, for accounts that are most susceptible to targeted attacks, they offer the Advanced Protection Program.

- Snapchat

The principles and features of Snapchat are listed below in accordance with its privacy statement.

-Unless otherwise required by law, Snap Inc. deletes Snaps from servers once they have been viewed by each Snapchat user to whom it was sent.

- For a longer amount of time, Snap Inc. can store information shared on a user's Story, Live, Local, and other crowd-sourced services.

- Users of Snapchat can add friends using their usernames, the contacts list, Snapcodes, while utilizing nearby, and Quick Add, which uses mutual friends.

- Instagram

The Instagram comments of other users were successfully deleted by the hacker from Helsinki going by the moniker Jani. The Facebook vulnerability management team built a test account with comments on it to confirm the breach, but he was able to get rid of them. A representative stated that the payment was made in March after the vulnerability was patched in February. The incident serves as a reminder of the importance of effective vulnerability management procedures for companies in charge of cloud-based services or consumer-facing software, as well as for the corporate users that use them. While the big social networks are usually rather safe, there is a risk when allowing employees to use BYOD or company-issued devices to access other potentially unsafe programs. By employing a mobile device management (MDM) solution to control which programs are installed or by using a containerization solution to separate personal and professional data on the device, these risks can be substantially decreased. Being alert and implementing the right solutions are crucial since security vulnerabilities can occur in both consumer and enterprise applications.

- Mozilla

This security-enhancing feature requires that all connections to websites use HTTPS, a secure, encrypted connection. Currently, HTTPS is accepted by the majority of websites, and some even support both. You may be sure that all of your website connections will be updated to HTTPS and become secure if you enable this mode. Find out more about the benefits of HTTPS-Only Mode and how to enable it.

Firefox's Enhanced Tracking Protection automatically protects your privacy while you browse. It blocks trackers and cookies that track your online activity and collect information about your interests and browsing habits. Turn on Total Cookie Protection in the Enhanced Tracking Protection options to prevent tracking by tracking businesses while you navigate between websites. But site breaking happens when a website stops working properly.

Source:

https://courses.csail.mit.edu/6.857/2017/project/1.pdf

https://support.mozilla.org/en-US/kb/https-only-prefs

Case Project 9-1: Antivirus Comparison

Select four antivirus products, one of which is a free product, and compare their features. Create a table that lists the features. How do they compare with the AV software you currently use? Which would you recommend to others? Why? Create a report on your research.

	TotalAV Antivirus	Kaspersky Antivirus	Norton Antivirus	Avast
Price (1 year)	$29-$49	$27-$45	$40-$55	free
Number of Devices	1-6	3-10	1-10	1-7
Free Trial Version	Free version capable of manual smart scans is available	Free trial of full version for 30 days	Free trial for seven days	Free
OS	Windows	Windows	Windows	Windows, MAC, Android
Virus Detection	Yes	Yes	Yes	Yes
Malware Detection	Yes	Yes	Yes	Yes
On-Demand Malware scan	Yes	Yes	Yes	Yes

I definitely recommend Avast free, which I now use on my computer. It is a quiet service that operates continuously in the background. My PC is not slowed down by it, and it routinely updates its virus definitions. The UI has been completely redesigned, and the newest version of Avast Free Antivirus now has an automatic gaming mode that mutes pop-ups and reduces system stress when you launch a processor-intensive game. There is also a password manager, which is unquestionably a wise addition to your security arsenal. It continues a clean sweep against 0-day assaults and performs well on AV-widely TEST's used malware benchmark, indicating that the increased detection network is undoubtedly contributing.

Case Project 9-4: UEFI

Use the Internet to research UEFI. What are its advantages? What are its disadvantages? What criticisms have been leveled against it? Do you agree with the criticism? Write a one-page paper on your findings.

The Unified Extensible Firmware Interface (UEFI) is a specification for a piece of software that links an operating system's firmware to a machine (OS). Future BIOS replacement is anticipated to be UEFI. Similar to BIOS, UEFI is preinstalled during manufacturing and is the first application to launch when a machine is powered on. It determines which hardware components are present on the computing device, wakes them up, and then transfers control to the operating system. The new specification addresses a number of BIOS drawbacks, such as constraints on the size of hard drive partitions and the processing speed of BIOS. UEFI can operate as a light operating system because it is programmable, allowing original equipment manufacturer (OEM) developers to add drivers and apps.

Your boot procedure will be quicker with UEFI since it has greater addressable address space than BIOS and can operate in 32-bit or 64-bit modes. Additionally, it implies that UEFI configuration panels, which include graphics and mouse cursors, may be sleeker than BIOS setup windows. This is optional, though. Many computers still come with text-mode UEFI setup screens that resemble the old BIOS setup screen.

There are many additional features in UEFI. Since Secure Boot is supported, the operating system may be verified for authenticity to make sure malware hasn't interfered with the boot process. The UEFI firmware itself may be able to provide networking functionality, which can help with remote configuration and troubleshooting. You can only configure a classic BIOS while physically in front of a computer. It goes beyond simply replacing the BIOS. A lot more functions than a BIOS are available with UEFI, which is essentially a mini operating system that runs on top of the PC's firmware. It might be loaded from a hard drive or network share upon boot instead of being saved in flash memory on the motherboard.

Source:

https://www.techtarget.com/whatis/definition/Unified-Extensible-Firmware-Interface-UEFI

https://www.howtogeek.com/56958/htg-explains-how-uefi-will-replace-the-bios/

Case Project 9-5: Application Whitelisting/Blacklisting

Research the Internet to find three tools that are available for application whitelisting/ blacklisting for a client computer and for a network server. Create a table that lists their advantages, disadvantages, ease of use, etc. Would you recommend using these tools? Why or why not? Write a one-page paper on your findings.

Application Whitelisting: The whitelisting of applications is one sort of endpoint security. Its goal is to prevent harmful software from running on a network. It regularly scans the operating system to prevent any undesirable files from starting. Application whitelisting allows organization managers, rather than the end user, to determine which apps are allowed to run on a user's computer or over a network. Blocking is applied to programs that have not been specifically whitelisted.

Application Blacklisting: Blacklisting, often referred to as refuse listing, is a security measure that restricts access to a computer or network for specific persons, websites, or programs. To put it another way, it refers to the action of preventing unauthorized users from accessing system resources. Firewalls and antivirus software typically employ a blacklist, which is a list of hosts that are forbidden from accessing a specific service. Blacklists can be created manually or automatically by looking at data flow and identifying dangerous or illegal connections. In order to remove unwanted content from websites and social networks, blacklisting is a frequent strategy.

	AppLocker	AirLock Digital	Faronics Anti-Executable
License/ Free Trial	Its free to use	Full version free 30 day trial available.	Full version free 30-day trial available.
Pros	Its free to use for windows devices. It prevents users from installing software.	Emergency workaround to prevent company-wide lockouts. Centralized controls	Mass approvals for trusted software brands. Quick graylisting for short-term access allowance.
Cons	It can be bypassed programmatically It operates only on Windows OS.	Control workaround feature could weaken the security of the service.	Graylisting feature could be abused to defer decision making.
Key Features	Controls Operating system access control. Automatic access permission Built into windows	It has feature of emergency bypass. Blocklisting against attacks Networked controls.	It has features of extensive activity logging. Default permission rules.

One of the company's most crucial resources is security. The blacklisting/whitelisting tools I've shown in the table above only compare one particular component of end-point security suites, not all the features included in each suite. Administrators can deploy these technologies, albeit doing so may need additional skill depending on the security settings. Blacklisting software, in my opinion, would give an extra layer of security, although it might take longer than expected. In contrast to application blacklisting tools, application whitelisting tools are simpler to set up and may take less time, however omitting potential hosts and applications from the list could lead to security flaws.

Source:

https://www.itprotoday.com/security/comparative-review-application-restriction-products

https://www.comparitech.com/net-admin/application-whitelisting-guide/

Case Project 10-1: Mobile Device Management Tools

Use the Internet to identify and compare three different mobile device management (MDM) tools. Create a table that lists their various features for on-boarding, off-boarding, configuration, quarantine, modification of device settings, etc. Which of the tools would you recommend for a small business with 10 employees who use smartphones but has a single person managing IT services? Why?

Using mobile device management (MDM) software, IT managers may control, secure, and enforce policies on smartphones, tablets, and other endpoints. IT managers can configure policies on the MDM server's management interface, and the server then wirelessly transfers those settings to the device's MDM agent. The agent applies the policies to the device by interacting with application programming interfaces (APIs) that are directly built into the operating system of the device.

	Microsoft Endpoint Manager	Trend Micro Mobile Security	Jamf Pro
Pros	Microsoft Endpoint Manager includes native access integration capabilities with a number of leading security and workplace management systems.	It includes mobile device management and mobile application reputation services.	Self-service enterprises version allows users to install secure app without submitting a ticket.
Con	Some clients feel that Microsoft's MDM reporting features are constrained when compared to some of the other leading solutions.	Some users believe that it lags while using this solution and also there are some users who complained about high memory consumption.	Some users have complained regarding the difficulties to setup self-service options on their mobile devices.
Quarantine	Device analysis	Threat detection	Alert and notifications

Modification of device setting	Applying device permission	Threat identification	Easy administration
On-boarding	Easy setup	Increasing productivity	Easy integration
Off-boarding	Helps in administration	Application access and identity management	Device management remotely
Key features	Group management for users, devices and mobile apps. Selective data wiping feature to remove organizational data only.	Cross-device and group policy management. Device location and inventory management support.	It has policies and scripts for device management and customization. It has custom report feature for inventory management and it also supports alerts and license management.
Pricing/Trial	Price depends on the type of license.	A free trial is available and pricing is directly offered by trend micro sales team.	$3.33/month per iOS and $7.17/month per Mac.

In light of the comparison just made, I would advise choosing Trend Micro Mobile Security due to its abundance of practical features. It is appropriate for small businesses and offers a trial version to the customer for assessment. It offers security for devices running Windows, MacOS, Android, iOS, and even ChromeOS. I consider the $49.95/year price to be pretty fair and acceptable for 5 devices.

Source:

https://www.educba.com/mobile-device-management-software/

https://www.enterprisenetworkingplanet.com/guides/mdm-software/

Case Project 10-3: Rooting and Jailbreaking

Research rooting and jailbreaking. What are the advantages? What are the disadvantages? How frequently is this technology used? Can a device that has been broken return to its default state? If so, how? Finally create a list of at least seven reasons why rooting and jailbreaking is considered harmful in a corporate environment.

An Android smartphone can be "rooted" to gain easy, unrestricted access to the system files. Making the appropriate additions, deletions, or alterations is part of access. like how IOS's JAIL breaking functions. It enables the device's software to be modified or new software to be installed, both of which are advised for mobile security. While rooting an ordinary Android phone or tablet can have many advantages, it also has some risks for the user and the Android device.

Advantages:

- Your Android device will operate much better if you install a custom ROM that has been optimized for performance after rooted it.
- Some smartphones may require rooting before software can be installed on a microSD card. Android 2.2 has such feature, however some carriers might turn it off.
- After jailbreaking your iPhone, you have more options for organizing and managing your data. With iFile, you may move and copy files, send files through a web server, and modify file permissions.
- Jailbreaking an iPhone is the first step in unlocking it so that it will accept a SIM card from a different GSM carrier. If you want to use your iPhone while traveling abroad but don't want to pay AT&T's exorbitant international roaming fees, this is especially useful.

Disadvantages:

- Unofficial apps have the potential to be poorly made or to include malicious code, both of which could cause your phone's operating system to crash. Applications with root access have extensive control over the operating system on your phone.
- Many reputable and secure applications cannot be loaded on your smartphone once it has been rooted. Most importantly, perhaps, is that your device's warranty will run out.
- If you jailbreak or root your device, all of your data and any apps you have installed will be removed. Make a backup of your personal data at all times, whether or not you jailbreak or root your phone.

The frequency of rooting and jailbreaking your phone is not specified. When a device's warranty has expired and the system default programs begin using up too much memory, most users start using this technology. Overusing the memory occasionally causes the phone to hang. At that point, we can jailbreak or root our phones and install a custom ROM.

It's highly likely that we will be able to fix the broken gadget and restore it to working order. Before rooting our device, we should have a complete backup of it. The simplest and quickest way to return to the original condition of our gadget is to restore it using the system backup.

Why rooting is harmful:

- Increased security vulnerabilities.

- Disruptions of services

- Carriers may deny service to rooted devices

- Possibility of losing access to manufacturer updates

Case Project 10-4: Security for Missing Mobile Devices

If a mobile device is lost or stolen, several security features can be used to locate the device or limit the damage. Many of these can be used through an installed third-party app. Use the Internet to identify four apps, two each for iOS and Android, and create a table that compares their features. Use the information in Table 10-8 as a starting point. Create your own table comparing their different features. Include a paragraph that outlines which app you would prefer for iOS and Android

Applications for phone trackers include a ton of functionality. The most basic function of a phone tracker app is to track the device's location. Some apps also offer complex features like geo-fencing, phone logs, text messages, and social media tracking. The following list of device finder applications' security features:

	Find my Iphone	Life360	Find my device	Where’s my Droid
Remote erase	Yes	Yes	Yes	Yes
Last known location	Yes	Yes	Yes	Yes
Remote lockout	Yes	Yes	Yes	Yes
Photo of convict	Yes	Yes	No	No
Price	Free	Subscription	Free	Free
Locate	Yes	Yes	Yes	Yes

Some of the devices, as shown in the table, include capabilities that make it easy to find lost or stolen devices. These functions do, however, have certain special capabilities, such as overlaying text messages on the screen of a misplaced smartphone, photographing prisoners, and leaving audio messages. I personally advise individuals who need to locate their gadgets to use Find my iPhone and Find my device. These programs are practical and simple to use. These come with a ton of handy features and are free. These programs have received several years of excellent reviews and are well regarded.

Case Project 10-5: Internet of Things

Use the Internet to research the Internet of Things (IoT). In your own words, what is IoT? How is it being used today? How will it be used in the near future? What impact will IoT have on technology, society, and the economy over the next five years? What are its advantages and disadvantages? Finally, visit the IoT List site (iotlist.co) and identify five of the most unusual IoT devices. Write a one-page paper on the information that you find.

The term "Internet of Things," or "IoT," refers to the entire network of interconnected devices as well as the technology that makes it possible for such devices to communicate both with one another and with the cloud. Due to the creation of low-cost computer processors and high-bandwidth telephony, there are currently billions of devices online. This suggests that everyday devices like vacuum cleaners, automobiles, and robots may use sensors to collect data and wryly respond to users.

It has already been established that IoT technology is one of the most important technological developments to have emerged in recent years. Over the years, IoT has influenced several business procedures, technological advancements, and consumer trends. In present, IOT has been used in various sectors:

- IoT in retail

With the help of smart gadgets and connected equipment, stores and supermarkets will probably become safer and more efficient. Additionally, businesses can create innovative use cases to raise customer satisfaction while reducing operating costs.

- IoT in healthcare

Due to the global pandemic, modern healthcare facilities are urgently needed. The benefits of IoT technology are now being actively utilized by the healthcare sector. The firm will benefit from increased customer satisfaction, top-notch service, round-the-clock accessibility, off-clinic patient monitoring, and many other factors.

- IoT in automative

One industry where IoT has a lot of potential is the automotive industry. Applications for the internet of things can be used during the implementation of V2X technology, often known as "vehicle to everything technology."

Advantages:

- Time savings: By reducing the quantity of human effort, it allows us to save a lot of time. Time savings are one of the key advantages of adopting the IoT platform.
- Better security: An integrated system will make it possible for our homes and towns to be more intelligently controlled by mobile phones. It increases security and provides safety for the individual.
- helpful for the healthcare sector: Without a doctor's visit, real-time patient care can be delivered more successfully. It enables them to base choices and provide care on the greatest evidence currently available.

Disadvantages:

- Privacy concern: Without the user's involvement, the Internet of Things system divulges very detailed personal information.
- High reliance on the internet: They are totally unable to function without it.
- Reduced mental and physical activity: People who use the internet and technology excessively become indifferent and inactive as a result of their dependency on smart devices rather than pushing themselves physically.

Five most unusual IoT devices:

Smart toaster

Smart flip flops

Smart snoring solution

Smart deodorant

Smart belt

3. Watch the 3 firewall tutorials (posted here in week 12) and write a summary for each one.

1. Palo Alto

A Palo Alto Next Generation Firewall is a security system that prioritizes prevention and views the user, application, and content as the three most important components of any commercial setting. These three components can be incorporated into your network's business policies thanks to this firewall, whose two primary features are user identification and password management. We may develop policy roles that take this information into account with the aid of this firewall. As opposed to merely IP addresses and port numbers, as is the case with traditional filtering systems, we may choose from hundreds of programs and enforce our regulations based on groups or even single users.

It also incorporates some kind of content filtering, comparable to the url filtering. Palo Alto Networks also offers some more advanced technologies, such as Wildfire Uh Palo Alto Devices, which have a variety of logging features. Even cloud-based logging systems are an option with Cortex Data Lake, and the Palo Alto Firewall is simple to include into the SD1 Architecture.

The web interface will undoubtedly be the primary method for connecting to the firewall when it comes to management options. Either local configuration or local access allows us to use merely a browser to establish a direct connection between our machine and the firewall.

This implies that the firewall should work with almost any browser. The centralized strategy, which is the second option, is actually advised to be used with networks that have at least six distinct firewalls, although this first option is obviously quite easy to set up in comparison. Panorama is the name of the program that develops the hardware and software, as well as maybe the physical appliance, that serve as the centralized management system for configuring several firewalls.

2. Cisco Firewall

A firewall is a system with rules to manage network traffic going in and out. There are numerous firewall setups that the network might utilize. Firewalls can act as an enforcement point for networks that are both trusted and untrusted. Where firewalls are used most frequently is between internal networks and the internet.

Types of Firewall:

- Traffic proxy firewalls: These firewalls can be used either forward or backward. The traffic is delivered to the proxy firewall, which examines it. This type of firewall can be used if we need to control network traffic at a location without an inline firewall.

- Application firewalls: These are required for deep inspection in order to block or allow traffic at the application level due to the dynamic nature of today's traffic and the diversity of apps that are available.
- Personal firewalls: are software applications that can be set up using IP and program rules. They are essential because, if a user's personal firewall is active, they will at least have some level of security on whatever network they join, even if the network's main firewall is not constantly protecting them.

Firewalls can be stateful or stateless. Stateful firewalls keep track of the statuses of connections, while stateless firewalls do not. When firewalls can monitor connection states and keep a closer eye on what is traveling through their zones, stateful firewalls become the preferred option. Status tables are used to keep track of each connection's current state. As a result, the firewall has the ability to allow or reject traffic based on whether a connection has been made and the origin of the traffic.

3. IPtables

Simply put, Iptables is a firewall program for Linux. To monitor traffic to and from your server, tables will be used. These tables contain chains of rules for filtering data packets coming in and leaving out. When a packet fits a rule, a target is assigned to it; this target could be another chain or one of the following unique values:

- The packet can proceed if the command ACCEPT is given.

-The packet cannot pass through by using the - DROP command.

- RETURN prevents the packet from moving on via a chain and instructs it to go back to the first chain.

It is common practice to add an INPUT or OUTPUT when creating a new rule. Both INPUT rules and OUTPUT rules apply to traffic entering and exiting the protected system. I don't know why INCOMING and OUTGOING or INBOUND and OUTBOUND were chosen instead of the more descriptive Feedback and OUTPUT, but like so many other decisions in life, I wasn't asked for input before it was implemented.

Syntax:

INPUT rule:

```
$ iptables –I INPUT <options>
```

OUTPUT rules

```
$ iptables –I OUTPUT <options>
```

Iptables rules can be added in one of two methods. We only use append (-A) once per system for the first method. The second choice, insert (-I), is how we add all extra rules to a system. RHEL asserts that adding the rule to the list places it at the bottom, and there is only one rule we want to be included at the very bottom: the conventional DENY ALL rule. Adding is simple.

Syntax: $ sudo iptables –A INPUT –j DROP