The Cyber Time

An initiative towards cyber

Message to the readers

I felicitate the young and exuberant students of Master of Science, Cyber Security who are coming out with their magazine "The Cyber Time". The magazine would deal with diverse areas pertaining to Cyber Crimes, Cyber Terrorism, Cyber Security and how to deal with these problems in a rapidly changing digital world. I warmly appreciate their efforts despite the handicaps of a fledging institution. I wish them good luck and hope that their diligent research, sincere efforts and enthusiasm will go a long way in building a critical mass of well-equipped professionals who will provide expertise in their domain. I sincerely hope that the Centre for Cyber Security will develop into a Centre of Excellence that would provide pivotal and critical services to the State and other organizations.

Dr. Bhupendra Singh (I.P.S.)

Pro-Vice Chancellor

Editorial

Cyber security is one of the most emerging fields today. In these days we are seeing that every country is trying to perform cyber-attacks on rival countries and their organizations and when we talk about their countermeasures formation of cyber armies and establishments of CERT,s are just the part of these. There are lot of questions that are striking in our mind like is it the starting of cyber warfare and if it is, then where we stand in the cyber warfare. This edition of "The Cyber Time" is dedicated to Cyber Warfare in which we have introduced some biggest attacks of year 2014 as well as the biggest attacks in the history of cyber space. From this edition we will also discuss some of the greatest players of cyber space and in this issue we have discussed about cyber capabilities of Russia.

I wish you **Happy Republic Day**.

Enjoy the issue, and please send your Article and Quiz Answer!

All the best, and keep in touch!

Nitish Vyas

spu1311218@policeuniversity.ac.in

Google Faced Fines in Netherlands

-Nitish Vyas

The authorities of the Netherlands may fine Google about €15 million over Internet privacy breaches. It turned out that Google is failing to abide by the data protection law of the country by collecting users' private data including browsing history and location for targeting advertisement.

The Dutch Data Protection Authority (DPA) has given the tech giant two months to fix the way it handles the information collected from individual users of its services. Besides Netherlands, the company has alsobeen under investigation in the UK, Spain, Germany, France, and Italy over the way it handles user information after enforcing new company guidelines 2 years ago. The tech giant collects information from search engine queries, users' emails, intermediary websites tracking or "cookies", location information and even YouTube browsing in order to target users with ads in future. The Dutch regulator claims such data collection is taking place without Google adequately informing the Internet users in advance. Moreover, Google doesn't ask for consent, which is a violation of the country's legislation. According to DPA's head, the practices of the tech giant catch the country in an invisible web of their personal details, without telling them or asking their permission. The Data Protection Authority ordered Google to start informing Internet users of its actions and to ask for consent. Otherwise, the company would face fines of up to €15 million. In response, Google said it was very disappointed with the order of the Dutch regulator, because the tech giant had already made a number of changes to its privacy policy when trying to address DPA's concerns. Nevertheless, Google has already introduces some proposals for further changes in its policy to the group of EU data protection authorities.

Q.1.Which one of the following characteristics is true regarding the use of hubs and switches?

a) Hubs can have their ports be configured with VLANs.
b) Using hubs is costly with regard to bandwidth availability.
c) Switches cannot forward broadcasts.
d) Switches increase the number of collision domains in the network.

Top 5 cyber-attacks of past year

- Vikash Saini

The cyber-attacks are just becoming more and more common every day and it's not looking like that this will slow down in coming time. In the year 2014 we have seen a number of data breaches of large corporations and companies due to which a great loss to both the financial status and reputation of the companies have been seen. Criminals are stepping up their game and data breaches are becoming both common and devastating.

Types of major attacks of year 2014:-

According to hackmageddon.com Cyber Crime ranks at number one with 62.3% (it was 47% last year) followed by Hacktivism (24.9%, was 44% last year). It is interesting to notice the rise of Cyber Espionage that doubled its percentage (10.2% vs. 5% in 2014). Defacement leads the chart of known Attack Techniques (16.4%, was 14% last year) ahead of SQL-injection (14.3%, down from 19% last year) and Account Hijacking (10.9%, a value slightly higher than last year when it was at 9%). It's also worth to mention the Influence of Targeted Attacks (10.5%) and Malware, which in practice rank on top if one consider also the PoS Malware (the aggregated value is 17.3%).

Top 5 attacks of year 2014 are:-

eBay's 233 million accounts hacked:- Cyber-attacks in late February and early March led to the compromise of eBay employee log-ins, allowing access to the contact and log-in information for 233 million eBay customers. eBay issued a statement asking all users to change their passwords.

Sony Pictures Entertainment Systems: - In November 2014, there was a breach by a group of hackers who had completely shut the server of Sony Pictures Entertainment down. This was the second attack that took place on Sony entertainment, previously in August there was an attack on Sony entertainment in this attack the Play-station networks were disabled and a false bomb threat was spread by the attackers on a plane on which high-profile Sony members were present. Also the attackers claimed that they had access to all the bad deeds of Sony and if the company didn't comply with the attacker's requirement then they would leak all the secrets of Sony.

Evernote & Feedly: -There was attack in these two companies Evernote and Feedly, and it was not made clear that if these two attacks were connected or not. Evernote was taken down by the DDoS attack in the month of June. But the website

was restored soon. And then there was an attack made on Feedly on the next day.

P.F. Chang's China Bistro (restaurant): - Between September 2013 and June 2014, credit and debit card information from 33 P.F. Chang's restaurants was compromised and reportedly sold online.

Domino's Pizza (Restaurant):- Over 600,000 Belgian and French customer records are hacked by Hacking group Rex Mundi. In exchange for the personal data, which included names, addresses, emails, phone numbers and even favorite pizza toppings, Mundi demanded $40,000 from the fast-food chain.

Conclusion:-

The recent increases in the rate and the severity of cyber-attacks. Companies indicate a clear threat to businesses and customers. As businesses come to terms with the increasing threat of hackers, instituting the right policies is critical to harnessing the power of the private sector. In a cyber-environment with ever-changing risks and threats, the government needs to do more to support the private sector in establishing sound cyber-security while not creating regulations that hinder businesses more than help them.

TOP 25 CYBER ATTACKS

Hetram Yadav

(Editor)

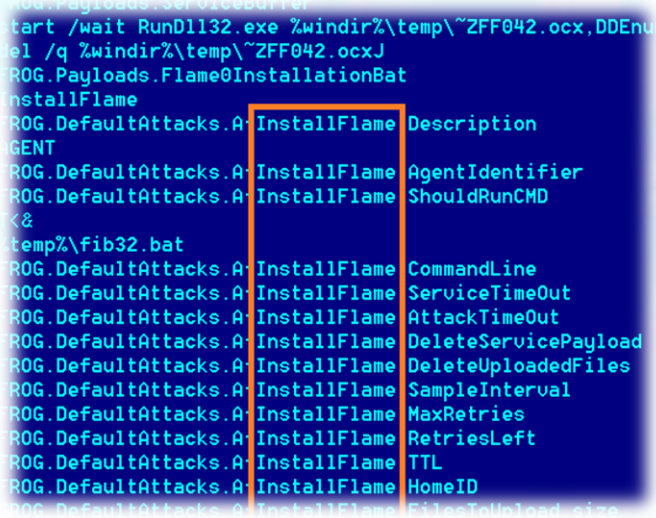
The cyber space is a growing community where everyone can reach out to one another regardless of time and distance.

It has become a new way of life, but has its negative repercussions as well. Some individuals use the cyberspace for their own dubious schemes, as they target unsuspecting individuals, companies, banks and even the military and government agencies. Here are the 25 biggest cyber-attacks in history that were launched as large-scale cyber terrorism and affected whole sovereign nations.

25. Flame

Also known as Skywiper and Flamer, Flame is a modular computer malware that was discovered in 2012 as a virus used to attacks computer systems in Middle Eastern countries that run on Microsoft Windows as their operating system.Used by hackers for espionage purposes, it infected other systems over a local network (LAN) or USB stick including

over 1,000 machines from private individuals, educational institutions, and government organizations. It also recorded audio, including Skype conversation, keyboard activity, screenshots, and network traffic. It was discovered on May 28, 2012 by the MAHER Center of Iranian National Computer Emergency Response Team (CERT), the CrySys Lab and Kaspersky Lab.



24. July 2009 Cyber attacks

These were a series of coordinated attacks against major government, financial websites and news agencies of both the United States and South Korea involving the activation of botnet. This involved a number of hijacked computers that caused servers to overload due to the flooding of traffic called DDoS attack. The numbers of hijacked computers varied depending on the sources and include 50,000 from the Symantec's Security Technology Response Group, 20,000 from the National Intelligence Service of South Korea, and more than 166,000 from Vietnamese computer security researchers as they analyzed the two servers used by the invaders.

23. Canadian Government hacking

The Canadian government has revealed in news sources that they became a victim of cyber-attacks in February 2011 from foreign hackers with IP addresses from China. These hackers were able to infiltrate three departments within the Canadian government and transmitted classified information back to themselves. Canada eventually cut off the internet access of the three departments in order to cut off the transmission towards China.

22. PayPal

PayPal became a victim of cyber-attack in December 2010 after it permanently restricted the account used by WikiLeaks to raise fund, citing their violation of the Acceptable Use of Policy as their reason. However, it did not only result in multiple boycotts from individual users but also caused hackers to move in.

Contd. In next issue…

Data Loss Prevention – Log & Event Manager

Pragya Johari

(Editor)

In today's world your network is subject to a multitude of vulnerabilities and potential intrusions and it seems like we see or hear of a new attack weekly. A **data breach** is arguably the most costly and damaging of these attacks and while loss of data is painful the residual impact of the breach is even more costly. The loss or leakage of sensitive data can result in serious damage to an organization, including:

- Loss of intellectual property
- Loss of copyrighted information
- Compliance violations
- Damage to corporate reputation/brand
- Loss of customer loyalty
- Loss of future business opportunities
- Lawsuits and ongoing litigation
- Financial and criminal penalties

To help you protect sensitive data and reduce the risk of data loss, we recommend using a Security Information and Event Management (SIEM) technology such as Solar Winds Log & Event Manager.

Feature #1 Real-Time Event Correlation

Solar Winds LEM employs a proactive approach to help you identify and respond to threats in real time. LEM automatically collects and aggregates log data from network devices, systems, and applications throughout the IT infrastructure. It then normalizes this data into a consistent format and performs multiple event correlation, along with the distinct ability to set independent activity thresholds per event or per group of events. The end result is security intelligence you can count on and reduced false positives.

- Instantly detect security, operational, and compliance issues, including external breaches, insider abuse, policy violations, application availability, performance problems, and more
- Get alerted in real time and contain threats at network speed

Feature #2 Unauthorized Network Access Prevention

SolarWinds LEM can help protect your network from unauthorized access in multiple ways, including the ability to monitor user activity, such

as logon attempts, and then correlate events with other log activity to identify suspicious behavior and malicious activity. LEM can then automatically disable user access. Another key way LEM can prevent access to sensitive data is through its real-time detection and automatic detachment of unauthorized USB devices. Plus, LEM enables you to monitor what files and processes are accessed on the device.

Feature #3 Stay Compliant, Stay Secure

Being in line with IT compliance regulations, such as PCI DSS, GLBA, SOX, NERC CIP, and HIPAA require businesses to protect, track, and control access to and usage of confidential/proprietary information and private customer data. Unfortunately, many organizations treat compliance as just a "checkbox" to pass an audit, instead of focusing on putting truly effective controls in place to better secure their network resources and critical data. With SolarWinds Log & Event Manager's real-time log analysis and powerful cross-device/cross-event correlation, you can quickly uncover policy violations that could leave your network vulnerable to a breach. And, with over 300 predefined, customizable reporting templates, you can ensure the right controls are in place to not only maintain compliance, but keep your network and the data it holds secure.

Lady to Saint – I doubt my Husband has been cheating on me….I have doubt on a woman….what to do?

Saint – Take your Husband to that woman's doorstep…and see if his

Wi-Fi connects automatically

Q.2 When comparing and contrasting the similarities and differences between bridges and switches, which of the following are valid statement?

a) Bridges are faster than switches because they have fewer ports.
b) A switch is a multiport bridge.
c) Bridges and switches learn MAC addresses by examining the source MAC address of each frame received.
d) A bridge will foreword a broadcast but a switch will not.

Smartphone with Android 4.3 or earlier, No WebView Vulnerability Patch for You

Vikas Yadav

(Editor)

Owning a smartphone running *Android 4.3 Jelly Bean* or an earlier versions of Android operating system??*Then you are at a great risk, and maybe this will never end. Yes, you heard right.* If you are also one of millions of users still running Android 4.3 Jelly Bean or earlier versions of the operating system, you will not get any security updates for WebView as Google has decided to end support for older versions of Android WebView – a default web browser on Android devices.

WebView is the core component used to render web pages on an Android device, but it was replaced on Android 4.4 KitKat with a more recent Chromium-based version of WebView that is also used in the Chrome web browser.

Just a day after Google publicized a bug in Windows 8.1 before Microsoft could do anything about it, a security analyst from Rapid7 who oversees the Metasploit project, discovered a serious bug in the WebView component of Android 4.3 and earlier that possibly left millions of Android smartphone users vulnerable to malicious hackers.

Android KitKat 4.4 and Lollipop 5.0 are not affected by the vulnerability, but over 60 percent of Android users – close to a billion people (950 Million) – still use the older version of Android 4.3 or below, which clearly states that the bug still affects more than a lot of people.

However, the response from Google after security analyst notified the vulnerability made him and every one of us stunned. Well, the tech giant won't patch the vulnerability in the WebView at all. As a result, only devices running KitKat 4.4 and Lollipop 5.0 will receive security updates for WebView from Google and the remaining Android versions will remain unpatched or rely on fixes from third party developers. The company has said that it will welcome third-party patches.

in case if a hacker or a cyber-criminal finds a way to exploit WebView on older versions of Android OS, Google will not release any patch for the vulnerability itself. However, if any outsider develops a patch, Google will incorporate those patches into the Android Open Source Project code and will further provide them to handset makers. This is where the company's responsibility get over.

Though, Google says that WebView support in older versions of Android operating system is baked firmly into the operating system in such a way that it makes much harder for Google to create a patch to affected devices. This issue has been mitigated by the search engine giant in newer versions of Android by dropping WebView from the core OS and incorporating it into the Google Play Services app.

Q.3.While troubleshooting a connectivity problem on the network, you issue the ping command from your PC command prompt, but the output shows "request times out."

At which OSI layer is this problem associated with?

a) the application layer
b) the access layer
c) the data link layer
d) the network layer

Sony Pictures Cyber Attack

- Nishant Grover

The *Sony Pictures Entertainment cyber hack* was a release of confidential data belonging to Sony Pictures Entertainment on *November 24, 2014*. The data included personal information about Sony Pictures employees and their families, e-mails between employees, information about executive salaries at the company, copies of unreleased Sony films, and other information.

The hackers called themselves the *"Guardians of Peace"* or *"GOP"* and demanded the cancellation of the planned release of the film *The Interview*, a comedy about a plot to assassinate North Korean leader Kim Jong-Un. United States intelligence officials, evaluating the software, techniques, and network sources used in the hack, allege that the attack was sponsored by *North Korea*. North Korea has denied all responsibility, and some cyber security experts have cast doubt on the evidence, alternatively proposing that current or former Sony Pictures employees may have been involved in the hack. The alleged document leak came a week after Sony employees reportedly were met with computers displaying images of a neon red skull and a message proclaiming the company had been hacked by "G.O.P".

Pirated versions of several films, including some

which have yet to be released, were also leaked online over the weekend.

The *duration of the hack* is yet *unknown*, though evidence suggests that the intrusion had been occurring *for more than a year*, prior to its discovery in November 2014. The hackers involved claim to have taken over *100 terabytes of data from Sony*. Following the breach, the hackers implanted Wiper on Sony's computer infrastructure, a malware software program designed to erase data from the servers. The malware also led to the discovery of the hack in late November 2014, as many Sony employees' computers were rendered inoperable by the software with the warning by the Guardians of Peace and *several Sony-related Twitter accounts were also taken over*. North Korean officials had previously expressed concerns about the film to the United Nations, stating that "*to allow the production and distribution of such a film on the assassination of an incumbent head of a sovereign state should be regarded as the most undisguised sponsoring of terrorism as well as an act of war.*"

After failing to stop the release of *The Interview* diplomatically, North Korea may have been motivated to escalate its efforts in the hopes of forcing Sony Pictures to yield. What other country or organization is demanding that Sony Pictures halt the release of a film? And consider: *While the hackers provided open Internet access to five recent or about to be released Sony films, The Interview was not among them. North Korea has known about the movie for at least five months, giving it ample opportunity to plot and carry out a cyber-attack.*

Assessing North Korean means for such a hack is a more difficult proposition. North Korean hackers apparently took down the internal networks of both South Korean TV broadcasters and several banks in 2013, having previously threatened the broadcasters for “defaming” North Korea. ***North Korea is reported to have a cadre of 6,000 or so hackers, over 1,000 of whom are reportedly very skilled.*** The character of North Korean cyber-attacks has evolved over the years in many other ways, and this type of attack could represent another step in that evolution.

Q.4 CISCO is the leader in router market space. What basic function do their routers perform in a network?

a) The micro-segmentation of broadcast domain.

b) Path selection

c) Packet Switching

d) Bridging b/w LAN segments

In this edation we introducing a new segment where we introduce some improtant tool which are play an important role in Cyber Security.

This time we indroduce **WIRESHARK – A Network Analysis Tool.**

Wireshark is a free and open source packet analyzer. Formerly known as Ethereal, captures packets in real time and display them in human-readable format. It is used for network troubleshooting, analysis, software and communications protocol development, and education. Wireshark is cross-platform, using the GTK+ widget toolkit in current releases, and Qt in the development version, to implement its user interface, and using pcap to capture packets; it runs on GNU/Linux, OS X, BSD, Solaris, some other Unix-like operating systems, and Microsoft Windows. There is also a terminal-based (non-GUI) version called TShark. Wireshark includes filters, color-coding and other features that let you dig deep into network traffic and inspect individual packets.

We can download Wireshark for Windows or Mac OS X from its official website. If we are using Linux or another UNIX-like system, we will probably find Wireshark in its package repositories. For example, if we are using Ubuntu, we will find Wireshark in the Ubuntu Software Center.

Features-

Wireshark is software that "understands" the structure of different networking protocols. It can parse and display the fields, along with their meanings as specified by different networking protocols. Wireshark uses pcap to capture packets, so it can only capture packets on the types of networks that pcap supports.

- Data can be captured "from the wire" from a live network connection or read from a file of already-captured packets.
- Live data can be read from a number of types of network, including Ethernet, IEEE 802.11, and PPP.
- Captured network data can be browsed via a GUI, or via the terminal (command line) version of the utility, TShark.
- Data display can be refined using a display filter.
- VoIP calls in the captured traffic can be detected. If encoded in a compatible encoding, the media flow can even be played.

Q.5. You download a file from an FTP site on the Internet. What is the highest layer in the OSI model used in this FTP operation?

a) Application b) Presentation

c) Session d) Internet

Call for articles:

Students are invited to get involved in the Tech Newsletter activities by providing articles and other related materials. Suggestions and feedbacks for the improvement of the newsletter are most welcome and contributions are invited from the faculty and students of the department. Contributions can be from any of the whole gamut of activities in the department like any special achievement, an admirable project, a publication, and Cyber Crime case, Quiz, puzzles or even the fun section material like jokes, cartoons, interesting facts or poems. You can also report any interesting workshops or talks taking place in the department.

You can send your material on: -

editors@policeuniversity.ac.in

Note: - If any of the articles is found to be copied, the writer himself/herself will be responsible for copyright issues. Editor or University will not be liable for any issue.

"The key to social engineering is influencing a person to do something that allows the hacker to gain access to information or your network."

Kevin Mitnick

Brought out by the Department of Computer Science & Cyber Security

Sardar Patel University of Police, Security & Criminal Justice, Jodhpur