International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-5, January 2020

Capability of Wireshark as Intrusion Detection System

Sakshi Singh, Suresh Kumar

Abstract*: The rise of networks has increased very fastly in this modern world. Our day to- day life mostly depends on the internet. It can be in the form of education, banking, research, business, journalism and many more. This dependency also leads to various types of intrusions. To identify intrusions on the grid, the system must have a detection engine that can detect intrusions automatically without any human intervention. Wireshark is an important tool for the analysis of network packets. But Wireshark lacks the feature of intrusion detection. In this paper, we will show that Wireshark can be considered not only as troubleshooting tool, network analyzer, protocol analyzer, packet sniffer but also a network intrusion detection tool because if the user has appropriate knowledge about attacks and data packets, then he could easily identify an attack by observing a specific data packet patterns. In this paper, an attack pattern dictionary will be created using which captured live data packets will be manually mapped in order to detect intrusions. We will also identify various attacks captured by Wireshark using this process.

***Keywords*: Attacks, Attack pattern dictionary, Intrusion, Intrusion detection, Wireshark**

I. INTRODUCTION

The intrusion detection system is the system that tracks any security policy breaches. It is a software application that scans a malicious operation or regulation violation network or device. These are categorized into the Network Intrusion Detection System (NIDS) and the Host Intrusion Detection System (HIDS). Wireshark is a software tool that uses a network interface to track network traffic. It is the most widely used method for tracking the network. Wireshark is commonly used by the following:

- Network administrators use it to review TCP retransmission, troubleshoot network problems, visually understand packet loss and graph high latency packet responses.
- Network Security controller uses it to inspect security problems like detecting anomalous behavior that could indicate malware, searching for unusual domains or IP address endpoints, using the IO graph to discover regular connections to command and control servers and extracting large DNS responses and other oddness which may indicate malware.
- Quality Assurance engineers use it to validate network applications
- Engineers use it to test the implementation of protocols
- People use it to understand internal network protocol

It is used to develop and enlighten protocols for troubleshooting, analysis, software, and communications. It runs on Linux, OS X, BSD, Solaris and some other operating systems like UNIX and Windows like Microsoft. Wireshark supports a wide range of protocols such as TCP, UDP, HTTP, and even specialized AppleTalk protocols. It has a range of advance choices such as packet filtering, packet export, and name resolutions. Wireshark is capable of capturing live network data. The sniffing [1] of the Wireshark network uses the promiscuous mode. Next, Wireshark converts the code of the network into a promiscuous mode where it can collect raw binary data that flows through the network. Then the chunks of the captured binary data will be translated into a readable form. Depending on their numbers, the packets are also re-assembled. Eventually, it analyzes the data collected and reassembled. The initial analysis includes defining the type of protocol [2], the medium of communication, port numbers, etc.

II. LITERATURE REVIEW

Vivens Ndatinya [3] demonstrated network protocol analysis on Wireshark and discovered various attacks using conventional network attack discovery methods, such as hidden FTP and IRC channels, port inspection, ICMP attacks, Bit Torrent services, etc. He also showed that a wide range of security threats and attacks on networked computer networks can be found in Wireshark's packet review. Sameena Naaz [4] used Wireshark to study and investigate the DHCP and DNS protocols. Using cisco packet tracer student, she had configured two computers with DHCP and DNS servers and dynamically assigned them network parameters with the servers. She also researched the Rogue DHCP server identification. She studied all LAN and home network DNS packets and observed delays in DNS errors. Wolf-Bastian and Lars Wolf [5] demonstrated without hardware modifications the modification of the sky wireless sensor node into a packet sniffer. The critical timing parameters were evaluated by them.

Manuscript published on January 30, 2020.
* Correspondence Author
Sakshi Singh*, Department of CSE , Ambedkar Institute of Advanced Communication Technologies & Research, Delhi (India) , Email : 010sakshisingh@gmail.com
Dr. Suresh Kumar, Department of CSE, Ambedkar Institute of Advanced Communication Technologies & Research, Delhi (India), Email : sureshpoonia@aiactr.com

In Wireshark, which offers a wide range of existing dissectors for different protocols, packets obtained by the sniffer node can be analyzed according to them. Therefore, for a custom MAC protocol, they developed their dissector. Mohsin Khan [6] had researched and examined that when an IP address is allocated using DHCP, what exactly happened in the back panel.

He introduced the DHCP client-server model and then captured DHCP packets exchanged between DHCP client and server using Wireshark. He studied and examined their contents thoroughly to promote and appreciate the entire contact process. In packet data interpretation and data handling, Usha Banerjee [7] highlighted the capabilities of Wireshark. She reiterated the need for IDS / IPS devices in any network in her experiment. In ACL (Access Control List) scanning, she used Wireshark. According to her, Wireshark can be built into a comprehensive program for intrusion detection by using filtering commands and supplementing utilities properly. Rashmi Hebbar [8] collected live network traffic and used Wireshark and Snort to conduct a detailed analysis of captured packets. She spoke about Wireshark alone being unable to produce an alert or take security measures against unauthorized access. The Snort intrusion detection tool will prevent the device from any intrusion, and warnings for these suspicious activities will be created. The graph of captured files shows the network structure information and insight into the issues.

S. Pavithirakini [9] addressed Wireshark's work briefly, its benefits, and the Wireshark tool improved. By using the ping command on the OS (Operating System), his idea triggered a ping flood scenario. Wireshark was installed on the victim's network to calculate the number of ping packets identified over a given timeline with a threshold orientation dependent on the identification of a flood attack. Ming-Hsing Chin [10] has shown an aggressive attack, i.e. Man in the Middle (MITM). Wireshark collects and analyzes the MITM behaviors in his experiment. From the results, the characteristics of the MITM attack were established. He also addressed preventive measures and stressed the importance of abnormality awareness. He found Wireshark to be an indispensable tool in disseminating the MITM assault knowledge. S. Choudhary et al. [11] used the snort NIDS for the auto detection of SQL injection attacks and moloch approach to analyze the captured packets (pcap) for the prototype system. K. Sinha [12] et al. proposed the secret shared key mythology to prevent from MITM attack during the transfer of multimedia data in cloud storage over the internet.

III. WIRESHARK AS INTRUSION DETECTION SYSTEM

Since Wireshark is not an intrusion detection tool but the user with expert knowledge can detect intrusions on the network. Wireshark consists of some expert features which can help the user to detect any intrusion [13] and suspicious activities on the network. Here is a list of some advanced features of Wireshark:

A. Display filter

Wireshark has two types of filters: filter capture and display filter. A capture filter cannot be modified. Display filters are used according to certain requirements to display packets in Wireshark. Display filters enable us to focus on the packets in which we are interested in while hiding uninteresting ones at the moment. Packets are displayed based on protocol, field presence, field values, and field comparison.

B. I/O graph

Wireshark has the function of an I/O graph that summarizes the flow of the packet. Wireshark I / O Graphs display the total traffic in the capture file, usually measured in bytes or packets per second.

C. Network conversation window

Contact between two separate endpoints is a connection on the network. The contact window comprises four columns together with names, packet counters and byte counters: the start time of the chat, the length of the conversation in seconds, and the average bits in each direction.

D. Coloring rules

It is possible to apply the coloring rules that reflect an infringement. The coloring rules require a word, a list (based on the view filter format), a foreground color and a background color.

E. Expert information

Expert knowledge is a compilation of exceptions in the Wireshark capture log. The general idea behind the following "Expert Info" is to have a more "uncommon" or simply notable perception of network activity. The quantity of expert knowledge depends largely on the protocol used.

IV. RESEARCH METHODOLOGY

To identify intrusions on the grid, the system must have a detection engine that can detect intrusions. But Wireshark lacks this feature. We have designed a general architecture of manual attack detection using Wireshark.

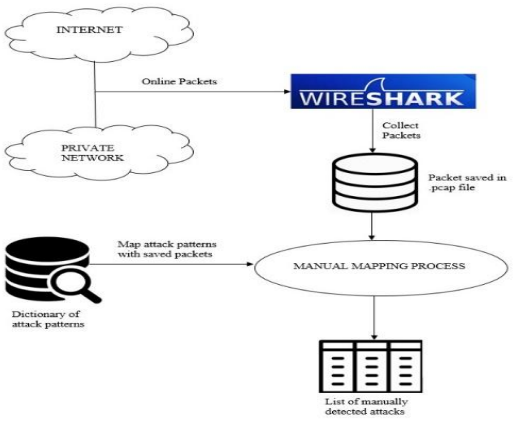

Fig. 1. General Architecture of Manual Attack Detection using Wireshark

According to this architecture, data packets from the internet or private network are captured by Wireshark.

After capturing, data packets are saved in a .pcap file in the system. A dictionary will be created which consists of all the attack patterns that can be identified by the Wireshark. Attack patterns will be mapped manually with the saved file of captured packets to detect attacks. Once the mapping process will complete, the list of manually detected attacks is created as the output.

In this architecture, the mapping process will be done manually. Wireshark is not able to detect attacks automatically because it does not contain any detection engine, so we are developing a mapping process in which a manually created dictionary of attack patterns will be compared with the data packets captured by Wireshark. After comparison, a list of attacks will be created which are identified in the mapping process.

V. DICTIONARY OF ATTACK PATTERNS

To implement the defined model and detect intrusions manually, a dictionary of attack patterns has to be maintained. Here is a list or various attack patterns that can help in detecting intrusions on the network.

A. Attack – DDOS (Distributed Denial of Service)

When a large number of data packets with the same source address and destination address are captured then it can be considered as a DDOS attack [14]. The data packets captured by the Wireshark will have the unknown protocol and the length of each packet will be the same. All these features indicate that it is a DDOS attack. When the DDOS attack takes place, a large number or similar packets are captured within a short period.

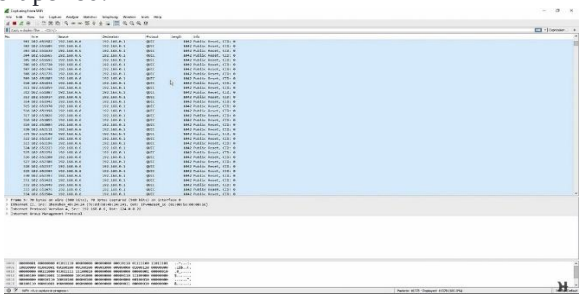

Fig. 2. Screenshot of DDOS attack

B. Attack – MITM

When the source MAC address of the captured data packets changes from normal address to unusual address then the MITM attack takes place. The ARP packets are sent back and forth, but in packet 56, the intruder sends another ARP packet with a separate MAC address from the router, delivering the data to the attacker and then the router. So hence MITM attack [15].

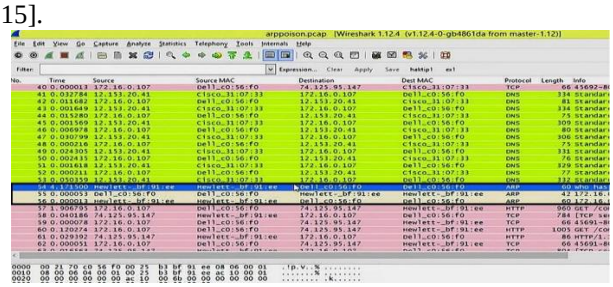

Fig. 3. Screenshot of Man -in –the- Middle attack

C. Attack – ARP Cache Poisoning Attack

In the figure, in packet number 57, the destination IP is .147, the MAC ID shows up as Hewlett- Packard i.e. it is an HP computer. But if we look at an earlier packet that is supposed to be sent to the router like packet 40 it's also being sent to IP .147 but the MAC address is for Cisco router. This shows that it is an ARP Cache Poisoning attack. Therefore, in short when two packets with the same source address, same destination address but different destination MAC addresses are captured then the attack is ARP Cache Packet Poisoning attack [15].

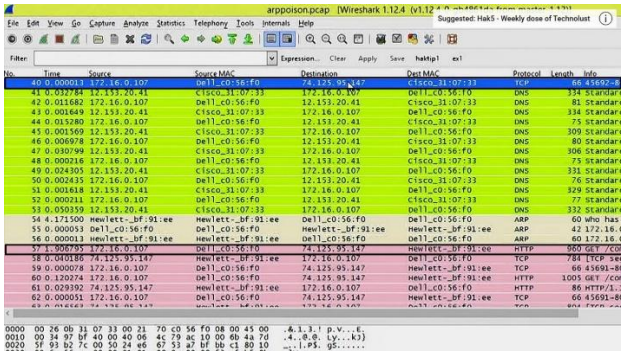

Fig. 4. Screenshot of ARP Cache Packet Poisoning attack

D. Attack – Exploitation (Malicious Sites)

In the figure, packet 6 has a "302 moved" response. This response is unusual and can be a malicious site. The location of the packet in packet detail pane is also not readable. In follow TCP stream of the same packet, script command consists of gibberish data and after scrolling down the follow TCP stream, iframe attack is taking place. In this scenario, it is an attack that is sent to the user.

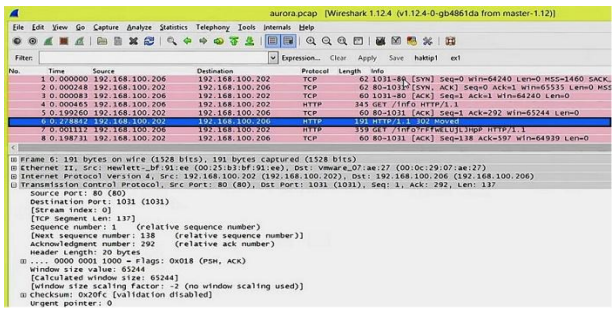

Fig. 5. Screenshot of malicious packet

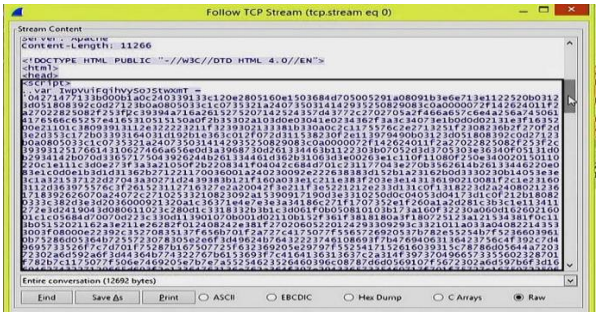

Fig. 6. Screenshot of TCP Stream of malicious packet

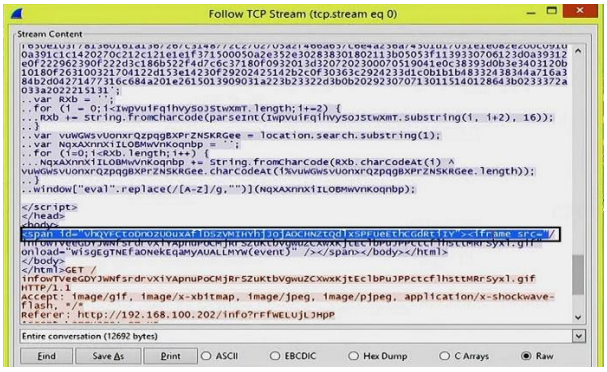

Fig. 7. Screenshot of iframe attack

At the follow TCP stream of packet 25, window command shell and attacker is getting admin privileges to the user's files like there is a password.txt. This is also an exploit.

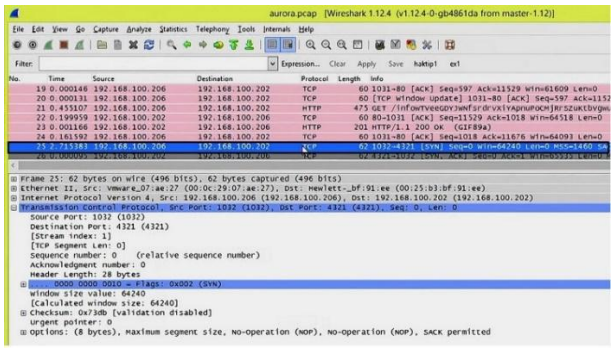

Fig. 8. Screenshot of exploitation -1

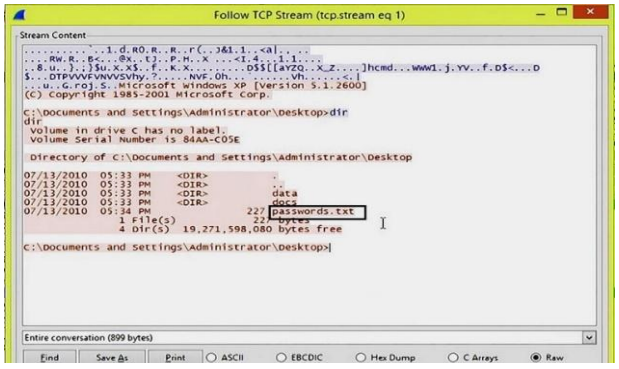

Fig. 9. Screenshot of exploitation -2

E. Port Scanning

To check the open ports in the network, first of all, check the conversation window and see which protocol's data packets are received the most. In the figure, the most packets are of TCP. Select any TCP packet and check the destination port from packet detail pane. Write a filter command of that port in-display filter and it shows all the packets with the same destination port. The figure shows that the server is trying to reach out to the intruder, but the attacker rejects the link ending with the TCP handshake. So it seems like the DNS port is already accessible.

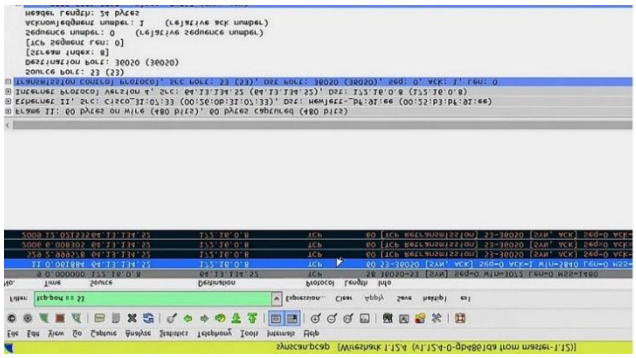

Fig. 10. Screenshot of Port Scanning

F. Attack - Packet sniffing (Username and Password)

In order to sniff password and username [17], Right-click on the suspect packet and open the next packet to navigate the follow TCP stream. The follow TCP stream shows the username and password.

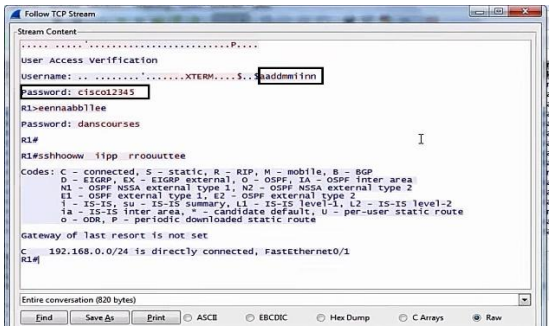

Fig. 11. Screenshot of Packet Sniffing

VI. RESULT AND DISCUSSION

Wireshark captures live data packets from the network and the packets are saved in .pcap format file. The file is then mapped with the attack patterns saved in the attack pattern dictionary. If the same packet pattern is found in the saved packet file as defined in the attack pattern dictionary then we can say that the following attack takes place on the home networked computer system. After mapping the dictionary and the captured data packet file, a list of attacks is identified in our home network.

Table I: List of Manually Detected Attacks on Lab Network

S.No.	Attack Name	Detection
1.	DDOS attack	Not Detected
2.	MITM attack	Not Detected
3.	ARP Cache Poisoning attack	Not Detected
4.	IFrame attack	Not Detected
5.	Exploitation 1- Malicious Site	Detected
6.	Exploitation 2- Unauthorized Access	Not Detected
7.	Port Scanning	Open Port Detected
8.	Sniff username and password	Detected

VII. CONCLUSION

Wireshark is a very important tool that has several advanced features like display filters, I/O graphs, color coding, expert information, etc. that can be used to detect various types of attacks on the networked computer systems. The paper introduced a model of a manual attack detection process using Wireshark. The defined model consists of an attack pattern dictionary in which a list of attack patterns are introduced. In the defined model, Wireshark captured live data packets from the network that are manually mapped with the attack pattern dictionary. Wireshark can identify a number of attacks like DDOS attack, Man-in-the-Middle attack, ARP cache poisoning attack etc. The model is used for the identification of various attacks on the network. This experiment showed that the Wireshark can not only be used as a packet analyzer, troubleshooting tool but also as an intrusion detection tool. A user with expert knowledge of data packets, protocols, etc. can detect intrusion using Wireshark.

REFERENCES

1. Alia yahia, Eric Atwell, "Evaluation of Capabilities of Wireshark as Intrusion Detection System", Journal of Global Research in Computer Science, Volume 9, No. 8, August 2018.
2. Santosh Kumar, "Detect/Analyze Scanning Traffic using Wireshark",PenTest Magazine, June 2013.
3. Vivens Ndatinya, Zhifeng Xiao, Ke Meng, "Network Forensic Analysis using Wireshark", International Journal of Sensor Networks, vol. 10, Issue No. 2, 2015.
4. Sameena Naaz, Firdoos Ahmad Badroo, "Investigating DHCP and DNS Protocols using Wireshark", IOSR Journal of Computer Engineering, vol. 18, Issue No. 3, May- June 2016.
5. Wolf- Bastian Pottner, Lars Wolf, "IEEE 802.15.4 Packet Analysis with Wireshark and Off- Shelf Hardware", Institute of Operating System and Computer Networks.
6. Mohsin Khan, Saleh Alshomrani, Shahzad Qamar, "Investigation of DHCP Packets using Wireshark", International Journal of Computer Application, vol. 63, Issue No. 4, Feb 2013.
7. Usha Banerjee, Ashutosh Vashishtha, Mukul Saxena, "Evaluation of Capabilities of Wireshark as a tool for Intrusion Detection System" International Journal of Computer Application, vol. 6, Issue No. 7, September 2010.
8. Rashmi Hebbar, Mohan K., "Packet Analysis with Network Intrusion Detection System" International Journal of Science and Research, vol. 4, Issue 2, Feb. 2015.
9. S. Pavithirakini, D.D.M.M. Bandra, C.N. Gunawardhana, "Improve the Capabilities of Wireshark as a tool for Intrusion Detection in DOS attacks" International Journal of Scientific and Research Publications, vol. 6, Issue 4, April 2016.
10. Ming- Hsing Chiu, Kuo- Pao Yang, R. Meyer, T. Kidder, "Analysis of a Man-in-the-Middle Experiment with Wireshark",http://worldcomp-proceedings.com/proc/p2011/SAM4991.pdf
11. Sandeep Choudhary, Nanhay Singh "Safety Measures and Auto Detection against SQL Injection Attacks", International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-9 Issue-2, December, 2019 pp. 2827 – 2833
12. K Sinha, S Choudhary, S Paul, P Paul "Security of Multimedia in Cloud using Secret Shared Key", International Conference on Computing, Power and Communication Technologies, 2018, pp. 908-912
13. Haroon Iqbal, Sameena Naaz, "Wireshark as a tool for detection of various LAN attacks", International Journal of Computer Science and Engineering, vol. 7, issue 5, May 2019
14. https://link.springer.com/referenceworkentry/10.1007%2F978-1-4419-5906-5_635
15. C. Calvert, Taghi M. Khoshgoftaar, Maryam M. Najafabadi, C. Kemp, "A Procedure of Collecting and Labeling MITM attack Traffic", International Journal of Relaibility, Quality and Safety Engineering, 2017, vol. 24, No. 01.
16. H Awang Mangut, Ameer Al- Nemrat Chafika Benzaid, Abdel- Rehman "ARP Cache Poisoning Mitigation and Forensics Investigation", IEEE, August 2015.
17. Pallavi Asrodia, Hemlata Patel, "Analysis of various Packet Sniffing tools for Network Monitoring and Analysis", International Journal of Electrical, Electronics and Computer Engineering, ISSN No.: 2277-2626.

AUTHORS PROFILE

Sakshi Singh, received her B.Tech degree in computer science and engineering from Guru Gobind Singh Indraprastha University (GGSIPU), New Delhi, India, in 2016 and M.Tech (P) degree in information security from Ambedkar Institute of Advanced Communication Technology and Research (AIACT&R), Delhi (India). Her research interests include digital forensics and information security.

Dr. Suresh Kumar, received his PhD degree in computer science and engineering from Maharshi Dayanand University, Haryana, India and the M.Tech and M. Sc degree in computer science from Kurukshetra University, Haryana, India. His major field of research is Semantic Web. His area of specialization are semantic web, operating system, Information retrieval, Database management system, etc. He is currently working as an associate professor at the department of Computer Science and Engineering, Ambedkar Institute of Advanced Communication Technology and Research (AIACT&R), Delhi (India). He is the author, co- author of more than 41 publications in International, National Journals and Conferences.