Wuhan University of Technology

School of Computer Science and Technology

Report - Network Security

Gouasmia Zakaria

Master 2018/2019   information security

ID: 2018GF189

E-MAIL: GOUASMIA.ZAKARIA1@gmail.com

I. Introduction:

1. Terminology

Internet is one of the most important advancements in the history of mankind. It allowed communication to reach a new high. Initially internet was used for military purposes for a message to pass through few computers. The universities came to know that it will send messages faster than any other means for the researches that were conducted in the universities.

Then the business world became very curious about this and later it has become common in every field and to everyone. It has become more applicable for all the communities. The main aim for the internet to grow is to make communications faster.

Internet made information accessible to everyone very easily. The growth and vastness of the Internet was accepted worldwide and became a necessity rather than a utility. Many significant changes took place in the world of internet. The TCP/IP addressing is almost over and a new version of addressing has been introduced called IPV6. The number of hosts getting connected is increasing exponentially.

The TCP/IP is called a four-layer protocol. This is responsible for the data flow across the network. This network is unreliable because there is know no acknowledgement that is there is no guarantee that the packet has reached the destination. However, TCP is a reliable network where it sends the acknowledgement to the host

Talking about the **IP addressing** system, it is a **32-bit** internet addressing system. If an interface has to participate in the internet then it should have an ip address. An ip address has a Network address and the host address. There are five different classes in addressing: class A, class B, class C, class D, class E. A browser is software that allows a user to view the information that is available on the internet. The appropriate address field will take the user to the requested web browser or to the destination. A DNS server is one that changes/resolves the host name to its respective IP addresses.

Attacks: Attacks include

1. **Reconnaissance attacks**: -The process of collecting data which is further used to

compromise the network.

2. **Access attacks**: - In order to gain access to database servers, e-mail servers one can

compromise a network which exploits network vulnerabilities.

3. **Denial-of-service attacks**: - It prevents and blocks access to the computer system.

Social Engineering: In Social Engineering, obtaining confidential network security information through non-technical means, such as posing as a technical support person and asking for people's password is causing a threat to security of personal data.

2. What is security?

Dictionary.com says:

. Freedom from risk or danger; safety.
. Freedom from doubt, anxiety, or fear; confidence.
. Something that gives or assures safety, as:

1. A group or department of private guards: Call building security if a visitor acts suspicious.
2. Measures adopted by a government to prevent espionage, sabotage, or attack.
3. Measures adopted, as by a business or homeowner, to prevent a crime such as burglary or assault: Security was lax at the firm's smaller plant.

3. Why do we need security?

Protect vital information while still allowing access to those who need it

- Trade secrets, medical records, etc.

Provide authentication and access control for resources

- Ex: AFS

Guarantee availability of resources

- Ex: 5 9's (99.999% reliability)

4. Who is vulnerable?

- Financial institutions and banks
- Internet service providers
- Pharmaceutical companies
- Government and defense agencies
- Contractors to various government agencies
- Multinational corporations

II. Network Security:

1. Introduction

Network Security consists of the provisions and policies adopted by a network administrator to prevent and monitor **unauthorized access**, **misuse**, **modification**, or **denial of a computer network** and **network-accessible resources**.

Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority.

Network security covers a variety of computer networks, both public and private, that are used in everyday jobs conducting transactions and communications among businesses, government agencies and individuals. Networks can be private, such as within a company, and others which might be open to public access. Network security is involved in organizations, enterprises, and other types of institutions. It does as its title explains: It secures the network, as well as protecting and overseeing operations being done. The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password.

2. Security Management:

Security management for networks is different for all kinds of situations. A home or small office may only require basic security while large businesses may require high-maintenance and advanced software and hardware to prevent malicious attacks from hacking and spamming.

3. Threats to Network Security

1. Viruses:

Computer viruses can be defined as software programs that are written to spread from one network node to another computer node and to corrupt and interfere with network nodes and computer operations.
The virus threat might corrupt or delete data on your PC and can be spread to other computers by email, program and even delete all data on your hard disk.

2. Vandals:

Software applets or applications that is responsible for destroying data.

3. Data Interception:

Data interception involves eavesdropping or spoofing the packets in communication systems and altering data packets that are being transmitted.

4. Trojan horse programs:

A destructive software program that acts as a genuine application is called a Trojan horse program. Unlike Viruses, Trojan horses do not replicate themselves among network but they can be just as destructive as viruses. Trojan horse claims to wipe out the virus in your computer but instead introduces viruses onto your computer.

5. Social Engineering:

In Social Engineering, obtaining confidential network security information through non-technical means, such as posing as a technical support person and asking for people’s password is causing a threat to security of personal data.

6. Attacks include

Reconnaissance attacks: The process of collecting data which is further used to compromise the network.

Access attacks: In order to gain access to database servers, e-mail servers one can compromise a network which exploits network vulnerabilities.

Denial-of-service attacks: It prevents and blocks access to the computer system.

4. Types of Attacks:

Networks are subject to attacks from malicious sources. Attacks can be from two categories: "Passive" when a network intruder intercepts data traveling through the network, and "Active" in which an intruder initiates commands to disrupt the network's normal operation.

Types of attacks include:

□ **Passive**

1. Network

a. Wiretapping

b. Port scanner

c. Idle scan

□ **Active**

1. Denial-of-service attack

2. Spoofing

3. Man in the middle

4. ARP poisoning

5. Smurf attack

6. Buffer overflow

7. Heap overflow

8. Format string attack

9. SQL injection

10. Cyber attack

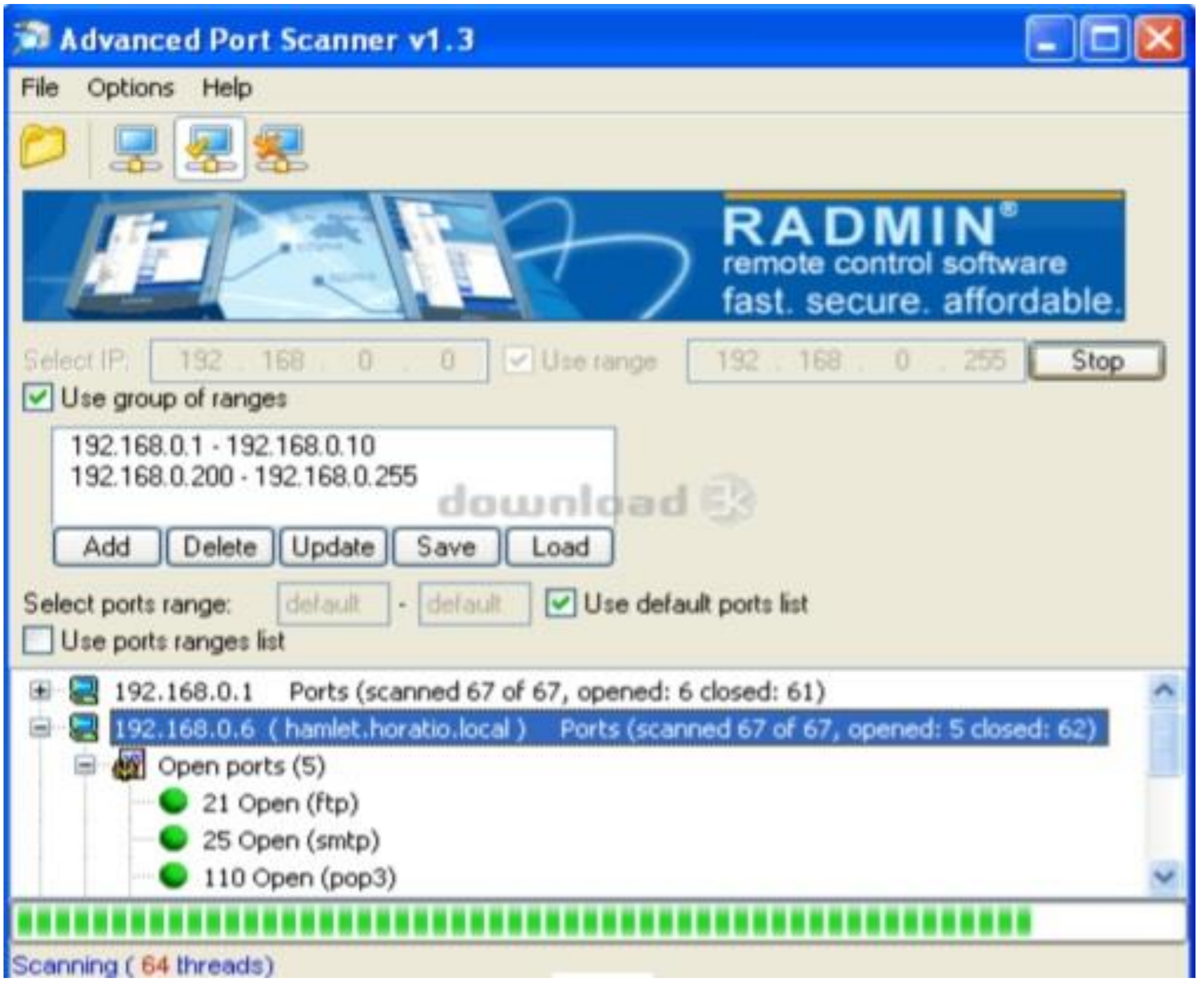
1. Passive:

❖ Wiretapping:

Telephone tapping (also wiretapping or wiretapping in American English) is the monitoring of telephone and Internet conversations by a third party, often by covert means. The wiretap received its name because, historically, the monitoring connection was an actual electrical tap on the telephone line. Legal wiretapping by a government agency is also called lawful interception. Passive wiretapping monitors or records the traffic, while active wiretapping alters or otherwise affects it.

❖ Port Scanner:

A port scanner is a software application designed to probe a server or host for open ports. This is often used by administrators to verify security policies of their networks and by attackers to identify running services on a host with the view to compromise it.



Select IP: 192 . 168 . 0 . 0 ☑ Use range 192 . 168 . 0 . 255

☑ Use group of ranges

192.168.0.1 - 192.168.0.10
192.168.0.200 - 192.168.0.255

Select ports range: default - default ☑ Use default ports list

□ Use ports ranges list

```
⊞ 192.168.0.1     Ports (scanned 67 of 67, opened: 6 closed: 61)
⊟ 192.168.0.6 ( hamlet.horatio.local )     Ports (scanned 67 of 67, opened: 5 closed: 62)
    ⊟ Open ports (5)
        ● 21 Open (ftp)
        ● 25 Open (smtp)
        ● 110 Open (pop3)
```

Scanning (64 threads)

A **port scan** or **portscan** can be defined as a process that sends client requests to a range of server port addresses on a host, with the goal of finding an active port. While not a nefarious process in and of itself, it is one used by hackers to probe target machine services with the aim of exploiting a known vulnerability of that service. However, the majority of uses of a port scan are not attacks and are simple probes to determine services available on a remote machine.

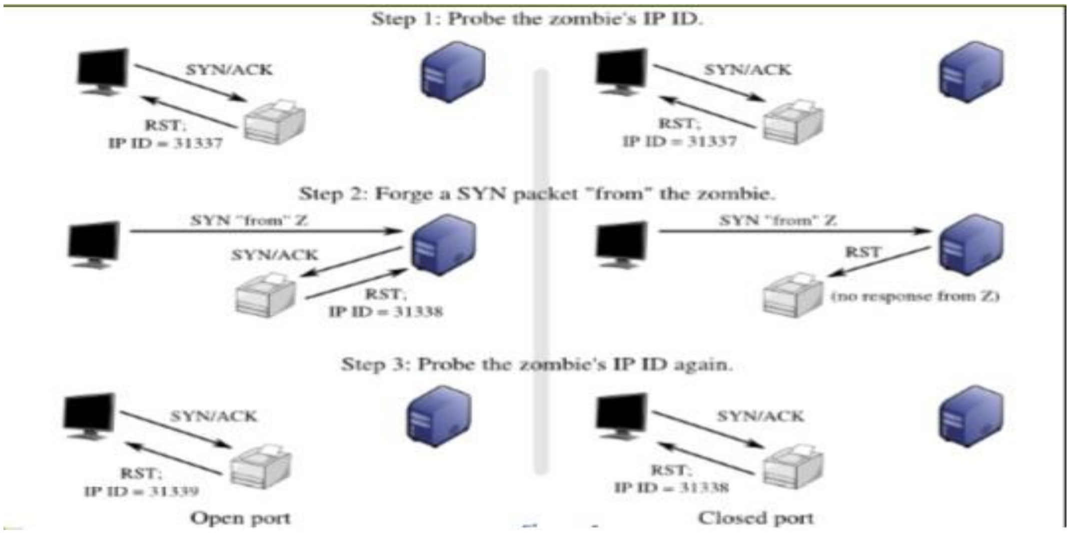
To port sweep is to scan multiple hosts for a specific listening port. The latter is typically used to search for a specific service, for example, an SQL-based computer worm may port weep looking for hosts listening on TCP port 1433.

Types:

1. TCP scanning
2. SYN scanning
3. UDP scanning
4. ACK scanning
5. Window scanning
6. FIN scanning
7. Other scan types

❖ Idle Scan:

The idle scan is a TCP port scan method that consists of sending spoofed packets to a computer to find out what services are available. This is accomplished by impersonating another computer called a "zombie" (that is not transmitting or receiving information) and observing the behavior of the "zombie" system.



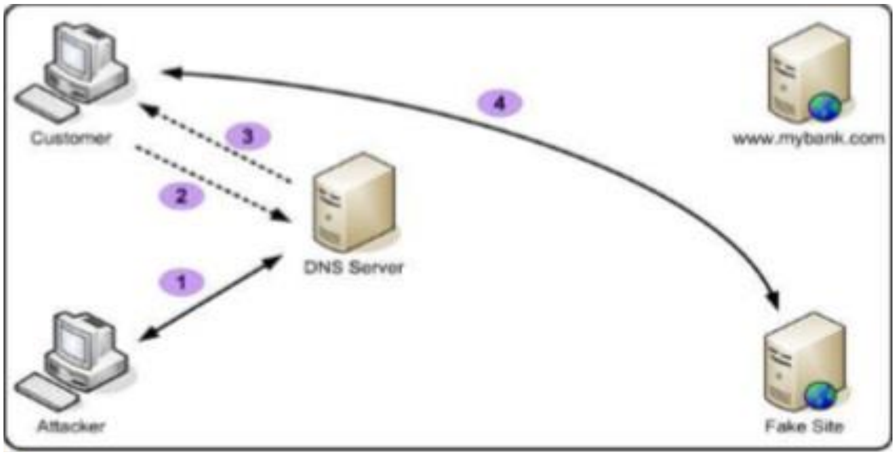
2. Active:

❖ Denial-of-Service Attack:

Denial-of-Service (DoS) or distributed denial-of-service (DDoS) attack is an attempt to make a machine or network resource unavailable to its intended users. Although the means to carry out, the motives for, and targets of a DoS attack vary, it generally consists of efforts to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet.

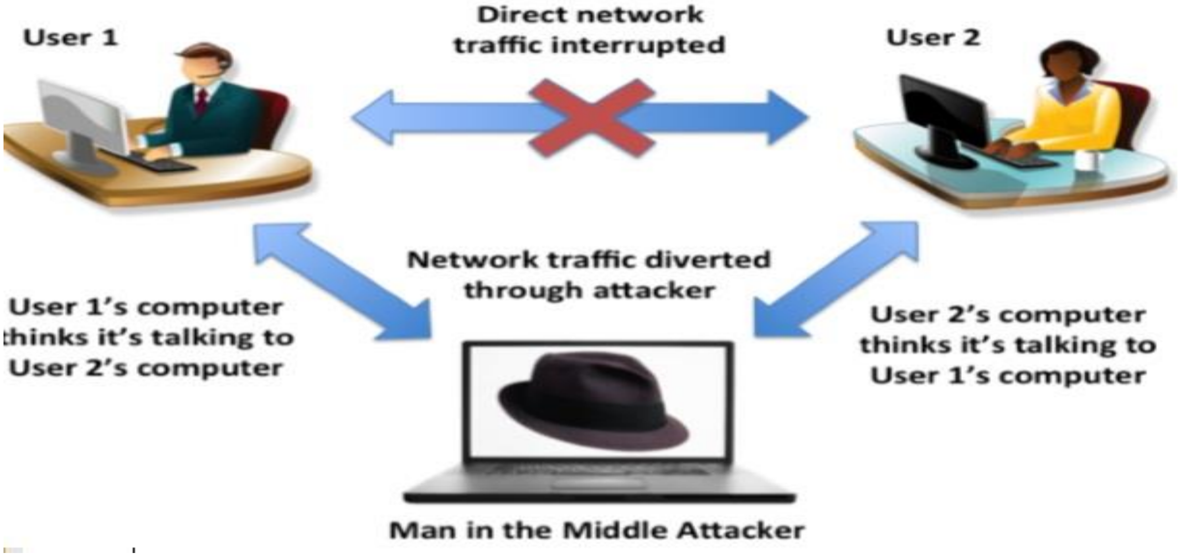
❖ Spoofing

A spoofing attack is a situation in which one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage.



❖ Man in the Middle

Man-in-the-middle attacks are a common type of cybersecurity attack that allows attackers to eavesdrop on the communication between two targets. The attack takes place in between two legitimately communicating hosts, allowing the attacker to “listen” to a conversation they should normally not be able to listen to, hence the name “man-in-the-middle.”.


User 1
Direct network traffic interrupted
User 2
Network traffic diverted through attacker
User 1’s computer thinks it’s talking to User 2’s computer
User 2’s computer thinks it’s talking to User 1’s computer
Man in the Middle Attacker

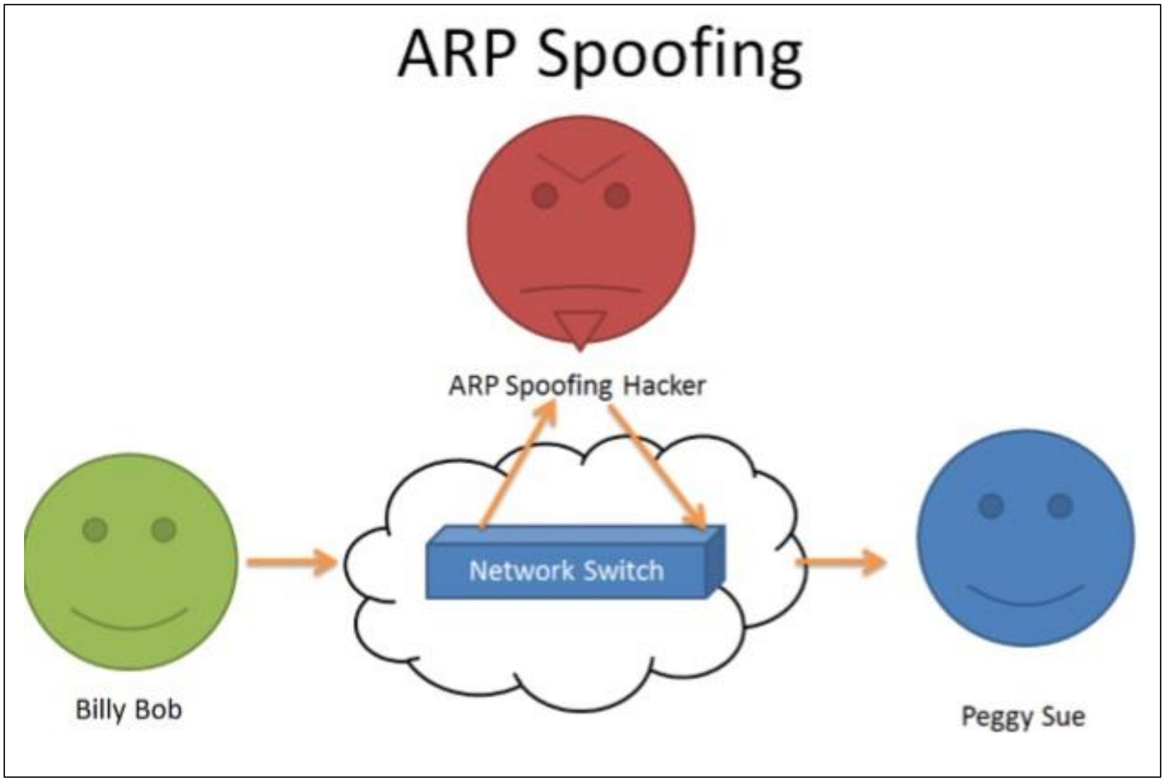
❖ heap overflow

A heap overflow is a type of buffer overflow that occurs in the heap data area. Heap overflows are exploitable in a different manner to that of stack-based overflows. Memory on the heap is dynamically allocated by the application at run-time and typically contains program data. Exploitation is performed by corrupting this data in specific ways to cause the application to overwrite internal structures such as linked list pointers. The canonical heap overflow technique overwrites dynamic memory allocation linkage (such as malloc meta data) and uses the resulting pointer exchange to overwrite a program function pointer.

❖ ARP Poisoning

ARP Spoofing/ Poisoning is a technique whereby an attacker sends fake ("spoofed") Address Resolution Protocol (ARP) messages onto a Local Area Network. Generally, the aim is to associate the attacker's MAC address with the IP address of another host (such as the default gateway), causing any traffic meant for that IP address to be sent to the attacker instead.

ARP spoofing may allow an attacker to intercept data frames on a LAN, modify the traffic, or stop the traffic altogether. Often the attack is used as an opening for other attacks, such as denial of service, man in the middle, or session hijacking attacks.



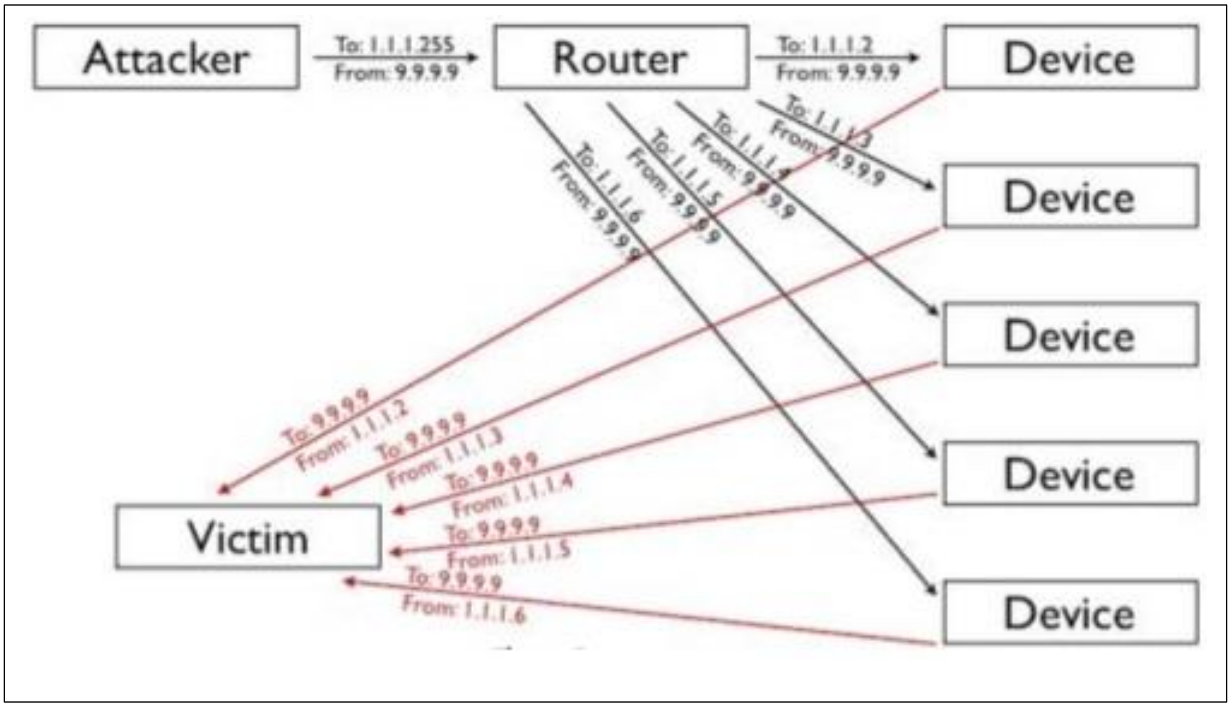
The attack can only be used on networks that make use of the Address Resolution Protocol (ARP), and is limited to local network segments.

Defenses

- Static ARP entries
- .ARP spoofing detection software
- OS security

❖ Smurf Attack

The Smurf Attack is a distributed denial-of-service attack in which large numbers of Internet Control Message Protocol (ICMP) packets with the intended victim's spoofed source IP are broadcast to a computer network using an IP Broadcast address. Most devices on a network will, by default, respond to this by sending a reply to the source IP address. If the number of machines on the network that receive and respond to these packets is very large, the victim's computer will be flooded with traffic. This can slow down the victim's computer to the point where it becomes impossible to work on.

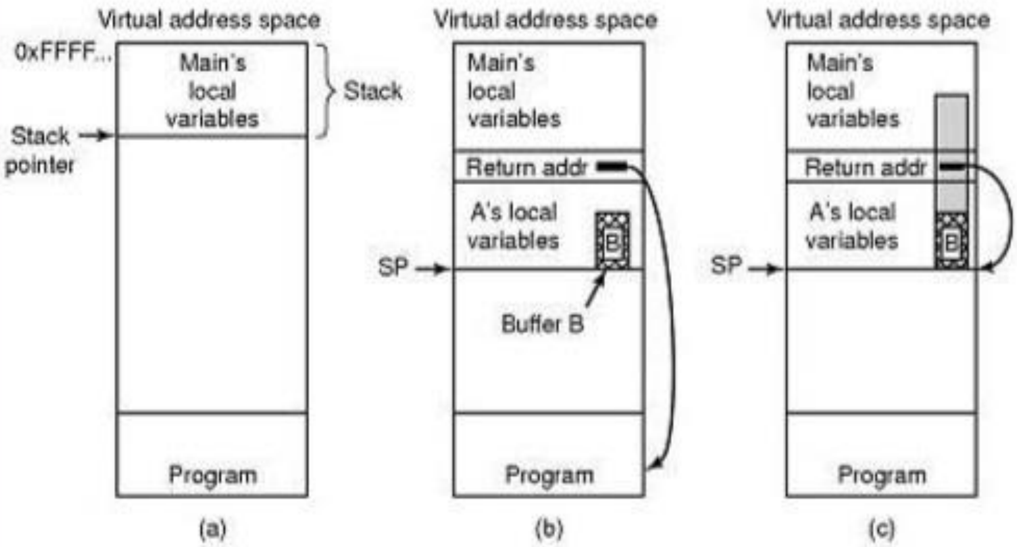


❖ Buffer Overflow

In computer security and programming, a buffer overflow, or buffer overrun, is an anomaly where a program, while writing data to a buffer, overruns the buffer's boundary and overwrites adjacent memory. This is a special case of violation of memory safety.

Buffer overflows can be triggered by inputs that are designed to execute code, or alter the way the program operates. This may result in erratic program behavior, including memory access errors, incorrect results, a crash, or a breach of system security. Thus, they are the basis of many software vulnerabilities and can be maliciously exploited.

Programming languages commonly associated with buffer overflows include C and C++, which provide no built-in protection against accessing or overwriting data in any part of memory and do not automatically check that data written to an array (the built-in buffer type) is within the boundaries of that array. Bounds checking can prevent buffer overflows.



- (a) Situation when main program is running
- (b) After program *A* called
- (c) Buffer overflow shown in gray

- **Exploitation**

1. Stack-based exploitation
2. Heap-based exploitation
3. Barriers to exploitation
4. Practicalities of exploitation
    a. NOP sled technique
    b. The jump to address stored in a register technique

- **Protective Countermeasures**

    1. Choice of programming language
    2. Use of safe libraries
    3. Buffer overflow protection
    4. Pointer protection
    5. Executable space protection
    6. Address space layout randomization
    7. Deep packet inspection

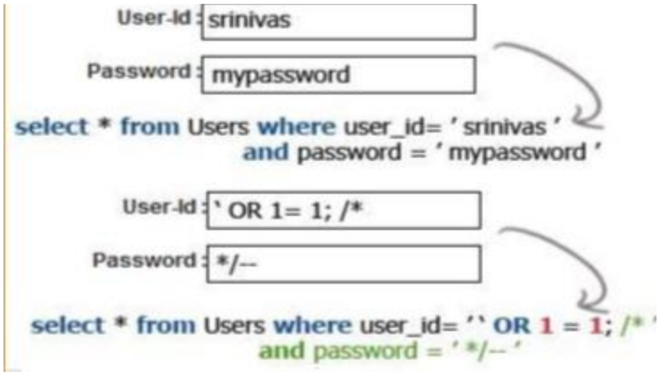
❖ Format String Attack

Uncontrolled format string is a type of software vulnerability, discovered around 1999, that can be used in security exploits. Previously thought harmless, format string exploits can be used to crash a program or to execute harmful code. The problem stems from the use of unchecked user input as the format string parameter in certain C functions that perform formatting, such as “printf()”.A malicious user may use the “%s” & “%x” format tokens, among others, to print data from the stack or possibly other locations in memory. One may also write arbitrary data to arbitrary locations using the “%n” format token, which commands “printf()”and similar functions to write the number of bytes formatted to an address stored on the stack.

❖ SQL Injection

‘ SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). SQL injection must exploit a security vulnerability in an application's software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL database

In a 2012 study, security company Imperva observed that the average web application received 4 attack campaigns per month, and retailers received twice as many attacks as other industries



User-Id : srinivas

Password : mypassword

```
select * from Users where user_id= ’ srinivas ’
                    and password = ’ mypassword ’
```

User-Id : ‘ OR 1= 1; /*

Password : */--

```
select * from Users where user_id= ’‘ OR 1 = 1; /* ’
                    and password = ’ */-- ’
```

III. Cyber Attack & Network Security tools

1. Cyber Attack

Cyber-attack is any type of offensive maneuver employed by individuals or whole organizations that targets computer information systems, infrastructures, computer networks, and/or personal computer devices by various means of malicious acts usually originating from an anonymous source that either steals, alters, or destroys a specified target by hacking into a susceptible system. These can be labelled as either a Cyber campaign, cyberwarfare or cyberterrorism in different context. Cyber-attacks can range from installing spyware on a PC to attempts to destroy the infrastructure of entire nations. Cyberattacks have become increasingly sophisticated and dangerous as the Stuxnet worm recently demonstrated.

2. Factors for cyber-attacks

1. Fear factor
2. Spectacular factor
3. Vulnerability factor

3. Network Security tools:

1. Antivirus software packages:

These software packages counter most virus threats if updated and correctly maintained regularly.

2. Virtual Private networks:

These networks provide access control and data encryption between two different computers on a same network or different, which allows hosts to have remote access to the network without the risk of a hacker or any intruder corrupting the data.

3. Secure network infrastructure:

Switches and routers have hardware and software features that support secure connectivity, intrusion protection, perimeter security, identity services and security management.

Dedicated network security hardware and software –Tools such as firewalls and intrusion detection systems provide protection for all areas of the network and enable secure connections.

4. Encryption:

Encryption is defined as the process of converting the plain input text to cipher text using a key. The encrypted text cannot be intercepted or read by any other user except the authorized recipient.

5. Identity Services:

Identity Services help to identify users and control their activities and transactions on the network. Services include digital certificates, passwords and digital authentication keys.

6. Security Management:

Security management is the centralized management solution that holds together all other building blocks of a strong security solution.

None of above approaches alone to secure a network will be sufficient in protecting the network, but when they are layered together, they can be highly effective in keeping a network safe from attacks and other threats to security.

Each network Security rule consists of conditions for network traffic and of actions

which are taken when conditions are met.

IV. Research on Network Security Situational Awareness System:

Keywords: Network Security, Security Situational Awareness

Abstract: With the popularity of computers, the Internet has entered the production and all aspects of social life, but the attendant problem of network security has become the focus of widespread concern. **Network security situation awareness** to effectively respond to network security issues provide a viable solution: for complex network environments and malicious attacks, a comprehensive analysis of attacks against various parts of the network system, from a macro point of view of network security situation be assess and predict the future of network security situation based on this information. For the predictive accuracy of prediction system for network security situation has improved significantly, and network security situation prediction method based on machine learning for the network security situation prediction have a high degree feasible, in the real network security situation awareness applications have certain research and practical value.

1. Introduction of Network Security Situational Awareness:

Network security situation is the current status and trends of the entire information from a variety of factors operating conditions of various network devices, network behavior and user behavior constituted. Network security situational awareness can acquire, understand and display the network environment of security elements. Through a series of technical means in time and space, are fully aware of network security and access and associated elements as possible in a pluralistic, and the establishment of a network based on complex behaviors modeling and simulation situational analysis and pre-side system, and then integrate and analyze vast amounts of security associated with the network-related data.

Network security situation awareness is a scientific and effective network security situation assessment and use of relevant technologies to make reasonable predictions about trends over time network security, network management personnel in advance to remind the network system for network equipment, network peer node hosts and data resources to make reasonable adjustments, upgrades and backup, network environment to address the risk of possible future harm to the network system, losses may result down to an acceptable range [1].

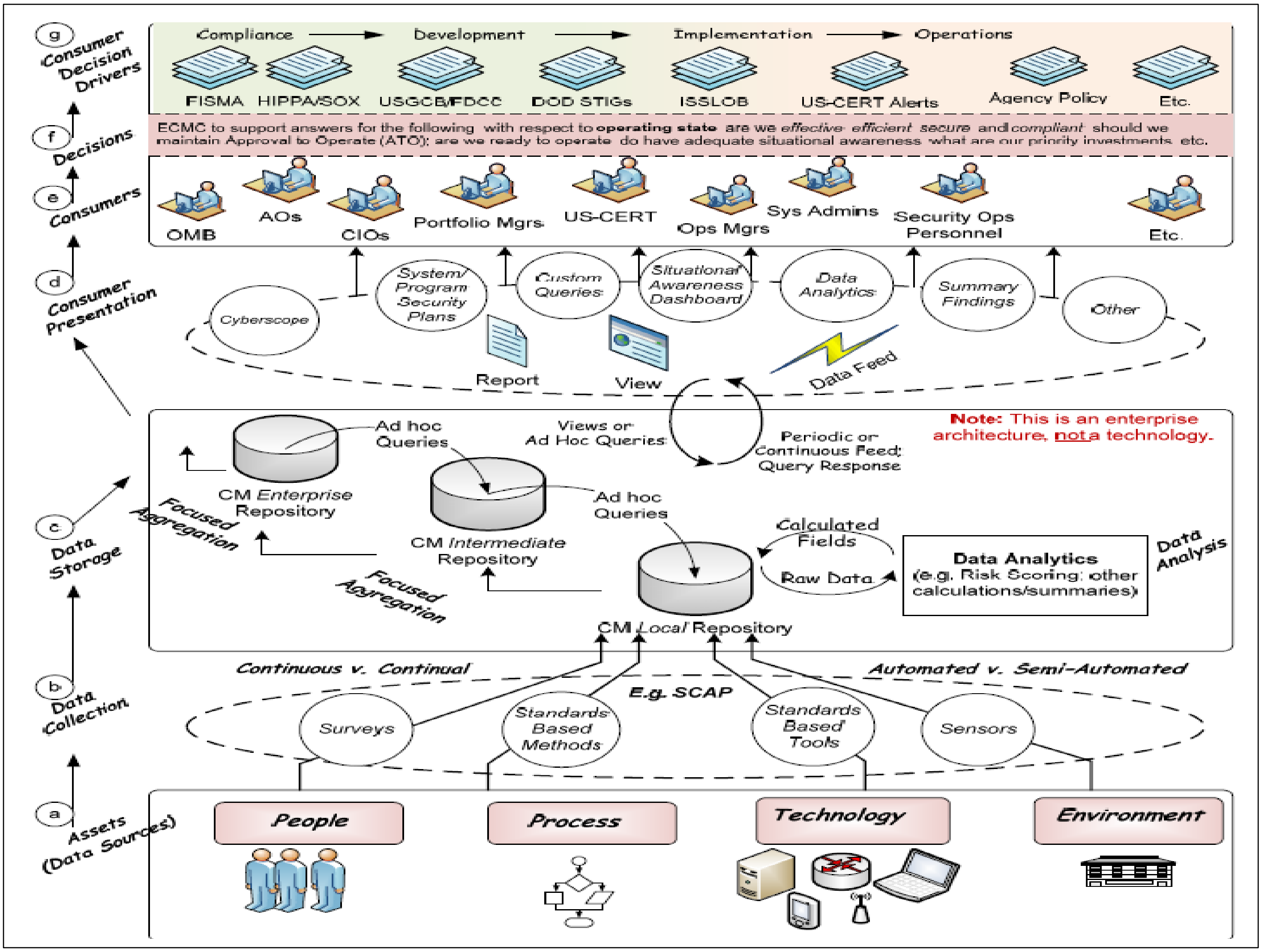
Extract information network security situation is carried out on the basis of situational awareness that only a comprehensive collection of data and the use of sophisticated index system, to ensure the correctness of the results of the assessment. Therefore, in the design process model or system must pay attention to select a metric system. Network security situation is a source of diverse, different collection methods, different devices collect data formats, network security situation letter from mainly contains configuration, operating status, traffic, user behavior and other information.

2. The concept of Situational Awareness:

The concept of Situational Awareness is an extremely important one in information security cyber security operations. Situational Awareness is defined as: "*Within a volume of time and space, the perception of an enterprise's security posture and its threat environment; the comprehension/meaning of both taken together (risk); and the projection of their status into the near future*."

The National Institute of Standards and Technology (NIST) has a draft publication for Interagency Report (IR) numbered 7756 that outlines the CAESARS (Continuous Asset Evaluation, Situational Awareness and Risk Scoring) Framework.

On aspect introduced within the NIST IR 7756 is continuous monitoring, which is defined and presented as in an architectural diagram. The diagram presents the interrelation and ecology of the multiple layers of continuous monitoring elements.



The following definition is provided: "*Continuous monitoring is ongoing observance with intent to provide warning. A continuous monitoring capability is the ongoing observance and analysis of the operational states of systems to provide decision support regarding situational awareness and deviations from expectations*." As well there are eleven domains that have to be considered for situational awareness in information security; they are:

- Vulnerability Management
- Patch Management
- Event Management
- Incident Management
- Malware Detection
- Asset Management
- Configuration Management
- Network Management
- License Management
- Information Management
- Software Assurance

There can be much debate on the merit and methods of philosophies such as Situational Awareness in network security. One fundamental aspect of Situational Awareness is its dynamicity. The ability to be dynamic and respond to new and evolving threat models. This is in direct contrast with the paradigm of classic information security, which is similar to fortress and castle building and somewhat static in design.

Traditional information security can use risk management to prescribe a set of controls to achieve a security baseline. For application development Threat Modeling is an approach for analyzing and mitigating the security of an application. However, in a dynamic threat landscape a new way of thinking may be to seek dynamic threat modeling for the network as the 'application'. To respond to the needs of the dynamic landscape of network attacks, the following characteristics are fundamental for the network to possess:

- Monitoring activated on all network hosts.
- Monitoring information written to local log files and log data shipped to a Security Information and Event Management (SIEM) system.
- The SIEM will then correlate and analyze the incoming log data for possible attack patterns.
- The SIEM should contrast and compare the incoming log data to the Common Vulnerability & Exposures (CVE) and the Common Configuration Errors (CCE) databases available from Miter and NIST, as well as threat-based databases for the purposes of providing insights into any incoming attacks.
- Network hosts should be classified in an asset database that can then be used to carry out vulnerability scans and track of the results of the scans for remediation.

3. Design of Network Security Situation Awareness System:

Support vector machine is a machine learning statistical learning theory, the latest theoretical achievements for outstanding practicality, currently used as statistical learning theory in the field of research focus, and in constantly evolving. Linear support vector machine is classified based and developed. Linear classifier basic theory in two-dimensional space represents. Fig.1 shows theory of linear classifier.

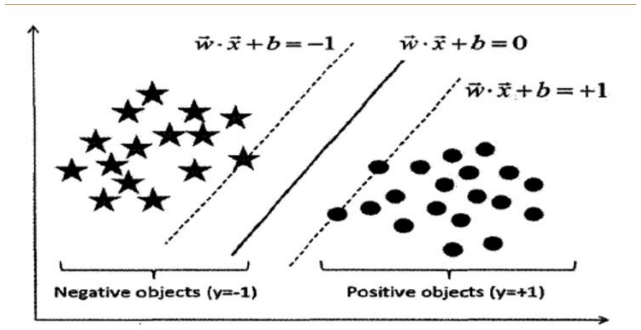

$\vec{w}\cdot\vec{x}+b=-1$
$\vec{w}\cdot\vec{x}+b=0$
$\vec{w}\cdot\vec{x}+b=+1$
Negative objects (y=-1)
Positive objects (y=+1)

Figure 1 The theory of linear classifier

Five-pointed star and the dots represent the two kinds of points, the hyperplane symmetry exists in the classification hyper plane around both sides, respectively, through two types of sample points from the hyperplane nearest sample points three straight line parallel to the middle, the distance between them is called a class interval, two sample points is a straight line through the SVM (support vector). Solving linear classifier is to the n-dimensional data space for training set to find a hyperplane to the sample point be classified separately, and the classification of the maximum distance in n-dimensional space. Inherited proposed machine learning method based on binary tree of many small sub-classifiers training methods, the advantages of faster decision-making, and to overcome each sub-classifier training needs of the entire sample, the disadvantage caused by the slow training, while drawing on the advantages of fewer training samples and advantages of one algorithm directed acyclic graph method of decision-making speed etc. In this paper, simulated annealing algorithm to optimize the parameters of SVM used to obtain the approximate optimal solution. Simulated annealing algorithm is introduced Monte Carlo iterative strategy for solving stochastic optimization algorithm. Since the physics of solids and the annealing process optimization process has many similarities. Physical principles of simulated annealing algorithm corresponding to: solid after being heated from a higher initial temperature of the starting temperature at a temperature falling to ambient temperature process, the binding characteristics of the probability of the sudden jump in the solution space in the form of random find the global objective function optimal solution, namely local optimal solution can be in the form of probabilistic jumping out of local, and find the most optimal solution to a final approximate approaches to the global optimal solution [4].

4. Achievement of Network Security Situation Awareness System:

In order to improve accuracy and generalization ability of machine learning, select the appropriate kernel function is very important. Seen from the introduction, the most commonly used kernel functions include linear kernel, polynomial kernel and Gaussian kernel of three. Using their default parameters set using the training data set of nuclear tests respectively linear kernel, polynomial kernel function and Gaussian kernel. Using the optimal parameters of simulated annealing algorithm, the optimal parameters will be used to establish the appropriate network security situation prediction model, and extract data normalized concentration in the first seven weeks as a training data set, function prediction model training. In order to test the perceptual model based on machine learning network security situation prediction accuracy and generalization capability obtained from the normalized data after a process of centralized data extracted after two weeks, the security situation to get a time series that contains 336 hours, and sliding window of size 7 time series reconstructed. The test dataset input support vector machine prediction model, to predict the beginning of the test data, and get the security situation time series forecasting [5]. Fig.2 shows network security situation forecast result compare.

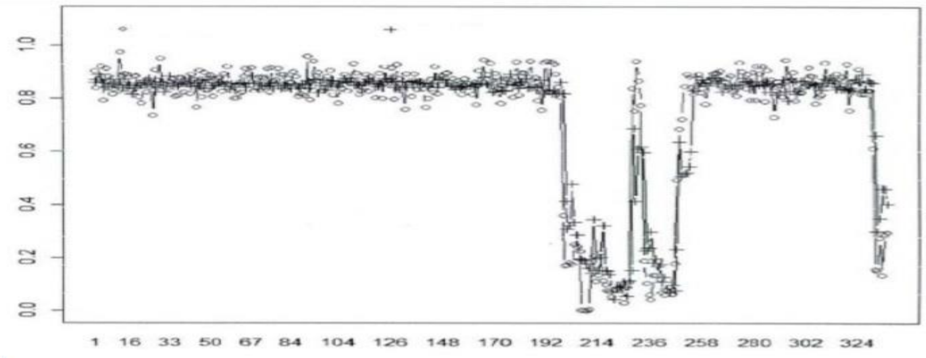


Figure 2 The network security situation forecast result compare

The horizontal axis represents the time in hours, and the ordinate represents the normalized subsequent to the [0, 1] interval of trend value, hollow red dot indicates the actual security situation for each time interval, while the blue dots represent hollow corresponding to the time interval by the value of the security situation prediction model results. As can be seen from the figure, the actual security situation and predicted trends broadly in line, when the value of the security situation mutation, predictive values and the real deviation is larger. Simulated annealing algorithm is a state transition factor contains a position distribution so that it can be seen as a continuous random parameter values within the range, set the proper cooling rule, fast convergence, to find global optimal solution. The grid size is based on cross-validation state transition step, easy to skip the global optimal solution, and the optimization process required for each point on the grid within the range of parameters to calculate the objective function value many times, when the training data set is too large, or fine-grid search optimization too long.

5. Conclusion:

With the growing size of the network, the network structures are becoming increasingly complex, which gives the network viruses and other security risks in the intangibles to opportunity, and threat of loss of its network system consisting of growing. In this context, the proposed network security situation and build a framework for modeling based on machine learning, constitute the network security situation awareness system, an important part of network security assessment, emergency response network, network security early warning, through a series of analysis, it shows that the system can support network security situational awareness of evolving. Network security situation awareness can analyze the overall state of the network from a macro perspective, according to the contact between the various security events, integrated network security status given to the evaluation system, to make effective and accurate predictions.

References

[1] Yih-Lon Lin, Jer-Guang Hsieh, Hsu.-Kun Wu.et. Three-parameter sequential minimal optimization for support vector machines [J].Neuro computing. 2011, 72: 3467-3475.

[2] Stephane, Alexandre Lucas. Visual Intelligence for Crisis Management[D]. Florida: Florida Institute of Technology.2013.

[3] Haoliang Zhang, Jinqiao Shi, Xiaojun Chen. A Multi-Level Analysis Framework in Network Security Situation Awareness [J].Procedia Computer Science, 2013, 17: 530-536.

[4] Tiago P. F. Lima; Teresa B, Ludermir. An automatic method for construction of ensembles to time series prediction [J]. International Journal of Hybrid Intelligent Systems.2013, 10 (4):191-203.

[5] Song-song Lu, Xiao-feng Wang, Li Mao. Network security situation awareness based on network simulation [C]. Electronics, Computer and Applications, 2014 IEEE Workshop Ji-Nan, China. 2014.