



BITS PILANI DUBAI CAMPUS
CS F266 STUDY PROJECT
CYBERSECURITY
SECOND SEMESTER 2019-2020

Submitted by:

Anukriti Jaiswal

2018A7PS0254U

ACKNOWLEDGEMENTS

The success of this project required immense guidance and support from a number of people and I am honoured to be able to express it here.

Firstly, I must thank Dr. Nilesh Goel, for providing me an opportunity to work on this project and for giving all of his students valuable assistance all throughout the course of the project. I am extremely thankful to him for pushing us and taking time out even during the course of this difficult time.

I owe my deepest gratitude to my friends and most of all to my parents for putting up with my project submissions and distorted sleep schedules. They have been a constant source of motivation to me and without them, this project would lack soul.

I would also like to thank our instructor-in-charge, Dr. Vilas Gaidhane for his inspiring presence.

Anukriti Jaiswal

CONTENTS

1. Cybersecurity

- 1.1. Introduction to Cybersecurity
- 1.2. Elements of Cybersecurity
- 1.3. Types of Threats
- 1.4. Benefits
- 1.5. Career Possibilities
- 1.6. Cyber Crime

2. **Cryptography**

- 2.1. Introduction to Cryptography
- 2.2. Symmetric Cryptography
 - 2.2.1. Transposition Cipher
 - 2.2.2. Substitution Cipher
 - 2.2.2.a. Caesar Cipher
 - 2.2.2.b. Monoalphabetic Cipher
 - 2.2.2.c. Polyalphabetic Cipher
 - 2.2.2.d. Polygram Cipher
 - 2.2.2.e. Playfair Cipher
 - 2.2.2.f. Hill Cipher
- 2.3. Encryption
 - 2.3.1. RSA Encryption
 - 2.3.2. Euclid's Algorithms
 - 2.3.3. Advanced Encryption Standard
 - 2.3.3.a. Key Generation
 - 2.3.3.b. Encryption
- 2.4. Authentication
 - 2.4.1. Message Authentication Code
 - 2.4.2. Hash Functions
- 2.5. Firewalls
 - 2.5.1. Packet Filtering Firewall
 - 2.5.2. Application Level Gateway
 - 2.5.3. Circuit Level Gateway
- 2.6. Digital Signature

2.7. Shannon's Theory of Confusion and Diffusion

3. Introduction to Ethical Hacking

3.1. Hacking and Hackers

3.2. Security Attacks

3.3. Security Threats

3.4. Hacking Tools

3.5. Password Cracking

3.6. IP and MAC Addresses

3.6.1. ARP Poisoning

3.7. Network Sniffing

3.7.1. Implementation

3.7.2. Counter Measures

3.8. Wireless Networks

3.8.1. Wired Equivalent Privacy

3.8.2. Wi-fi Protected Access

3.9. Web Servers

3.9.1. Web Attacks

4. Network Penetration Testing

4.1. Linux Commands

5. Harry Potter Cipher Game

6. Conclusion

7. Bibliography

1. Cybersecurity

1.1. Introduction to Cybersecurity

To understand what cybersecurity really is, we must realize the need for it. In the past, data was stored in centrally managed closed systems, but now it is stored in distributed devices with immense processing power. We now find the need to protect all our internet-connected systems including hardware, software from cyberattacks. Cybersecurity threat vectors such as USB sticks, personality tests and infected websites serve as primary paths of access to hackers. All essential information held by banks, governments and corporate records may result in fraud, data theft, loss of reputation and money. The goal today is to defend systems against unauthorized access, malicious intent and mitigate as well as respond to cyberattacks better and more efficiently.

1.2. Elements of Cybersecurity

There are six basic elements of cybersecurity:

1. Application Security- minimizing unauthorized code by embedding security into the system.
2. Information Security- safeguarding sensitive information by maintaining data confidentiality, integrity and availability.
3. Network Security- thwarting and monitoring all kinds of misuse, alteration and access through security policies.
4. Operation Security- classifying information and determining the required controls for protection
5. Business Continuity Planning- carrying out already well-planned procedures while an emergency/disaster is in effect.
6. End-user Education- providing directives for actions to be taken by employees to protect their assets.

1.3. Types of Threats

Malware- It is a kind of malicious software like worms, viruses and trojan horses that may contain files that can be used to harm computer systems.

Ransomware- It is a kind of malware that involves an attacker locking a user's files through encryption techniques and demanding payment to unlock the same.
Phishing- It involves sending falsified emails or messages that resemble reputed sources in order to steal sensitive personal data.

1.4. Benefits

The benefits of cybersecurity implementation are many but the most important ones include protection of data and networks and improvement of recovery time post breach. In fact, many world-renowned organizations such as Gartner have predicted that cash flow due to information security will increase by at least 8.7% in the next year. The most popular cybersecurity vendors of the decade are Cisco, McAfee and Trend Micro, responsible for VPNs, firewalls, cloud-based security and anti-malware works.

1.5. Career Possibilities

This field of the cyber world proves to offer a range of high-paying jobs such as:

1. Chief Information Security Officer-responsible for implementing security programs and overseeing the organization's IT operations.
2. Security Engineer- responsible for protecting company assets from threats and regulating quality control.
3. Security Analyst- responsible for planning security measures, audits, and controls.

1.6. Cyber Crime

In this era of growing technology and its misuses, cyber crime is a word not unfamiliar to most in the world. Cybercrime has found its roots in fraud, trafficking, pornography and violation of privacy. Computing devices may be used as target (to gain network access), weapon (to launch service attacks) or accessory (to store illegally obtained data) in the process of committing a crime online.

2. **Cryptography**

2.1. Introduction to Cryptography

Cryptography is the process associated with storing and transmitting data in a specific form so that the data is readable to only those for whom it is intended. We use it as a means of protection from data theft and also for user authentication. There are three types of cryptographic techniques that we will be discussing further:

- 1) Symmetric key cryptography

- 2) Hash Functions
- 3) Public key cryptography

2.2. Symmetric Cryptography

2.2.1. Transposition Cipher

Suppose we have a string or a sentence stored in the form of a matrix. Let this string be 'MEET ME AFTER PARTY'.

1	2	3	4	5	6
M	E	E	T	M	E
A	F	T	E	R	P
A	R	T	Y		

Let us come up with a random number sequence incorporating all numbers from 1 to 6 that will serve as our key. Let this key be 421635. Rearrange the letters of the original matrix according to the column key sequence. For example, if our first column is 4, then all values under 4 in the original matrix must be written under it. Now our cipher text (data transmitted) is 'TEEMEEMEFAPTRYRAT'.

4	2	1	6	3	5
T	E	M	E	E	M
E	F	A	P	T	R
Y	R	A	T		

2.2.2. Substitution Cipher

2.2.2.a. Caesar Cipher

This is probably the most commonly used symmetric cipher technique. All we need to do is shift every letter in the plain text by a specific count. For example, if we have a shift of 1, then a becomes b and c becomes d.

Let plaintext be 'happy' and shift be 2. Then ciphertext will be 'jcrra'.

Mathematically, the encryption function can be denoted with $E(x)=(x+k) \bmod 26$ and the decryption function with $D(x)=(x-k) \bmod 26$ where x is the plaintext and k is the key or the shift.

2.2.2.b. Monoalphabetic Cipher

This type involves assigning any one letter to another letter. So, a becomes x, b becomes g, c becomes y and so on. One exclusive letter is assigned to another without repetition. For example, 'abcde' is encrypted to 'xgyfk'.

2.2.2.c. Polyalphabetic Cipher

It is a little difficult to explain this cipher in words, but an example should do the job. Let's assume our plaintext to be 'YOU CAN TRUST ME' and the key 'COMPUTER'. Now we must shift the letters of the text by as many spaces as represented by the corresponding letter in the key. So, Y shifts by 3 letters (since C is the 3rd letter in the English Alphabet) and becomes B.

	Y	O	U	C	A	N	T	R	U	S	T	M	E
+	C	O	M	P	U	T	E	R	C	O	M	P	U
	B	D	H	S	V	H	Y	J	X	H	G	C	Z

2.2.2.c. Polygram Cipher

Polygram cipher simply replaces a block of letters with another. Hence, 'EDUC' may be replaced by 'XYQZ' and 'EDU' may still be replaced by 'LOD' and 'ED' may be further replaced by 'BE'. This is one of the most difficult ciphers to crack as it can have many combinations.

2.2.2.d. Playfair Cipher

Take a 5x5 matrix which makes 25 letters. Let our key be 'monarchy' and plaintext be 'instruments'. We first write our key down in the matrix and write the remaining letters of the English alphabet.

m	o	n	a	r
c	h	y	b	d

e	f	g	i	k
l	p	q	s	t
u	v	w	x	z

We have removed j from the matrix since it can contain only 25 letters. In case, we have a j in the plaintext, we must always replace it with i. Now, split all the letters in text into pair. In case of odd letters, add a z at the end. If both letters in the pair are in the same column, replace with letter below each. If both letters are in same row, take the letter to the right of each. Similarly, if pair does not satisfy either of the above, form a rectangle with the 2 letters as corners and replace with letters on the horizontal opposite corners of rectangle.

So, i=g,

n=a,

s=t,

t=l,

r=m,

u=z,

m=c,

e=l,

n=r,

t=q,

s=t,

and z=x.

Thus, 'instruments' becomes 'gatlmzclrqtx'.

2.2.2.e. Hill Cipher

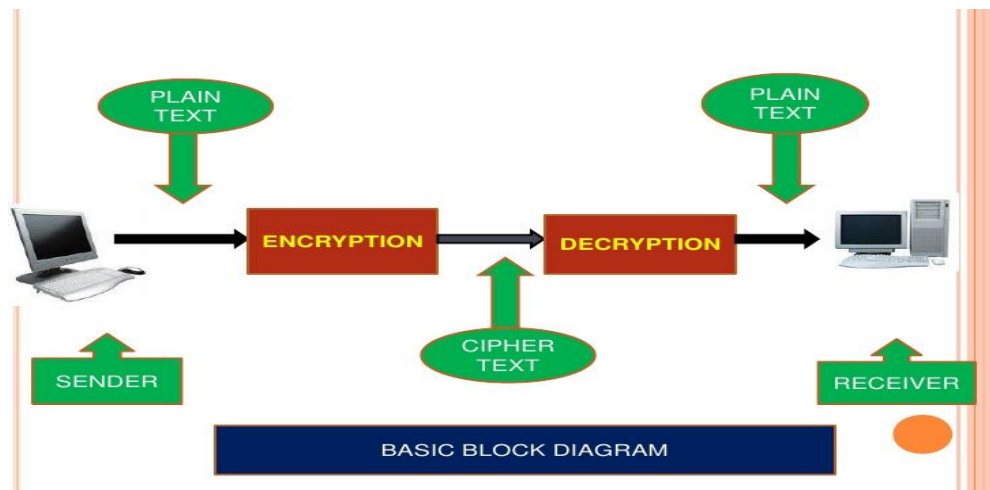
Suppose we take plaintext 'ACT' and key 'gybnqkurp'. Place the corresponding numbers of letters in the key in a nxn matrix, a is 0, b is 1, c is 2 and so on. We now form a 3x3 matrix with the 9-letter key (in green) and multiply it with a 3x1 matrix (in blue) comprising of plaintext corresponding numbers. The resultant matrix is denoted in orange, but these numbers are not between 0 to 25. Hence, we find the denoted these numbers using mod 26.

6	24	1		0		67		15 mod 26
13	16	10		2		222		14 mod 26
20	17	15		19		319		7 mod 26

The numbers 15, 14 and 7 represent the letters 'POH', our ciphertext.

2.3. Encryption

Encryption is basically the conversion of normal messages into meaningless (as seen) messages. The process of converting these so to say meaningless messages back to meaningful or normal messages is called decryption. This can be depicted with the image below.



2.3.1. RSA Encryption

All techniques mentioned above were examples of symmetric cryptography. Now, we must explore the topic of asymmetric cryptography starting with RSA Encryption. This kind of encryption involves message encryption using a public key and decryption using a private key. It uses a trap door function, that develops a relationship between numbers that it is easy to compute in one direction but impossible to compute backwards. For example, 701111 is a product of 2 prime numbers that are impossible to guess or compute, but if we were given the 2 prime numbers, 907 and 773, then it is very easy to compute the result $907 \times 773 = 701111$.

There are 5 steps to follow for encryption and decryption:

Step 1: Generate keys using primality test algorithm to find 2 random prime numbers. The numbers must be large and have a huge difference in them. For explanation's sake, we will take two relatively small numbers $p=907$ and $q=773$. Find the product n .

$$n=p*q=907*773=701111$$

Step 2: Find Carmichael's Totient function denoted by,

$$\pi(n)=lcm(p-1, q-1), \text{ i.e.,}$$

$$\pi(701111) = lcm(906, 772) = 349,716$$

Step 3: Generate a public key and ciphertext 'c' by finding a random number 'e' between 1 and $\pi(n)$. Here, let $e=11$. Then our ciphertext 'c' in terms of plaintext 'm', random number 'e' and product 'n' will be,

$$c = m^e \bmod n = m^e \% n$$

For example, let $m=4$,

Then, $c = 4^{11} \bmod 701111 = 688,749$ will be our ciphertext or encrypted message that is sent to the receiver with private key. The public key is shared.

Step 4: Generate private key 'd' using formula,

$$d = (1/e) \bmod \pi(n) = (1/e) \% \pi(n)$$

$$d = (1/11) \bmod 349,716 = 254,339$$

Step 5: Decrypt ciphertext 'c' using all the available information using,

$$m = c^d \bmod n$$

$$m = 688,749^{254,339} \bmod 701111 = 4 \text{ is our original message (plaintext).}$$

Note: We can also use an RSA decryption calculator where supply $\text{mod}=n$, decryption key= d , and ciphertext= c .

2.3.2. Euclid's Algorithms

Euclid's algorithms or Euclidean's algorithms are an essential part of modular arithmetic and cryptographic protocols, specifically in factoring large composite numbers.

Euclid(a,b)

1. **A=a**
2. **B=b**
3. **if B=0**
4. **return A= gcd (a, b)**
5. **R=A mod B**
6. **A=B**
7. **B=R**
- goto 2**

This can be depicted by the example given below:

GCD (1970, 1066)

$1970 = 1 \cdot 1066 - 904$ returns gcd (1066,904)

$1066 = 1 \cdot 904 - 162$ returns gcd (904,162)

$904 = 5 \cdot 162 - 94$ returns gcd (162,94)

$162 = 1 \cdot 94 - 68$ returns gcd (94,68)

$94 = 1 \cdot 68 - 26$ returns gcd (68,26)

$68 = 2 \cdot 26 - 16$ returns gcd (26,16)

$26 = 1 \cdot 16 - 10$ returns gcd (16,10)

$16 = 1 \cdot 10 - 6$ returns gcd (10,6)

$10 = 1 \cdot 6 - 4$ returns gcd (6,4)

$6 = 1 \cdot 4 - 2$ returns gcd (4,2)

$4 = 2 \cdot 2 - 0$ returns gcd (2,0)

Hence, the GCD for 1970 and 1066 is 2.

Euclid defined another algorithm or trick to find the multiplicative inverse of a number. Suppose we have to find the multiplicative inverse of 11 in Z_{26} . This means that our inverse will be a number between 1 and 26 since we are using mod 26. We will have a number of variables that will be the column heads.

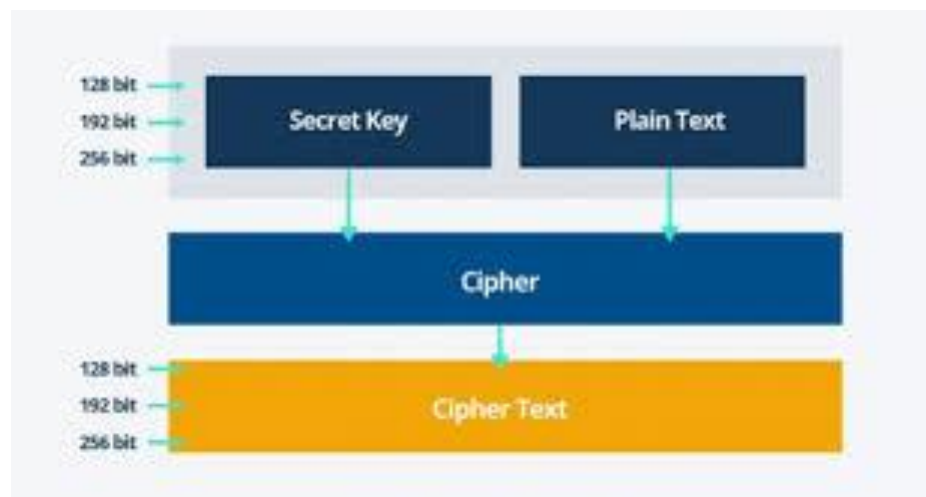
Assume $t_1=0$, $t_2=1$, $r_1= \max (11,26)$, $r_2= \min (11,26)$, $t=t_1-t_2 \cdot q$, $q=r_1/r_2$ and $r=r_1 \% r_2$. We keep repeating the division till we get an undefined value for r_1/r_2 .

q	r1	r2	r	t1	t2	t
2	26	11	4	0	1	-2
2	11	4	3	1	-2	5
1	4	3	1	-2	5	-7
3	3	1	0	5	-7	26
	1	0		-7	26	

The numbers in red, 1 and -7 are the GCD and MI of 11 respectively.

2.3.3. Advanced Encryption Standard (AES)

Why use the AES when you have techniques such as the RSA Encryption method? The reason we use the Advanced Encryption Standard is because it provides better security and efficiency in terms of algorithm. The AES comprises of three block ciphers- AES-128, AES-192, and AES-256. Each 128-bit plaintext undergoes AES Encryption using a 128-bit key to produce a 128-bit ciphertext and the same goes for the other block ciphers.



The number of rounds the encryption takes is determined by the key size:

Number of Rounds	Key Size
10	128



12	192
14	256

Step 1: Key Generation

T	E	A	M	S	C	O	R	P	I	A	N	1	2	3	4
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

Convert each letter to its hexadecimal equivalent ASCII value-

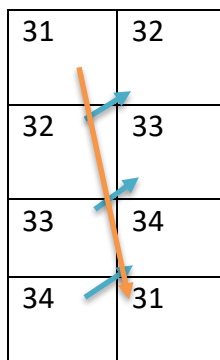
54	45	41	4D	53	43	4F	52	50	49	41
----	----	----	----	----	----	----	----	----	----	----	---	---	---	---	---

Take four elements at once and convert them to a cubic matrix. We will give us an 8x16=128-bit key state that make the 10 subkeys for each round. This is our SUBKEY 0. We can generate 10 more such subkeys with the method below.

54	53	50	31
45	43	49	32
41	4F	41	33
4D	52	43	34

Take the last column and do rot word on it.

31	32
32	33
33	34
34	31



Use the pre-defined sub-byte table in AES and change values accordingly. If the element is 32, replace it with the element in Row 3, Column 2.

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Similarly, the rot word of the last column and convert into sub-byte column.

32	23
33	C3
34	18
31	C7

Use the predefined RCON table in AES to perform the next step. This table can be used to generate the next 10 subkeys for the encryption. Column 1 for subkey 1, column 2 for subkey 2 and so on.

01	02	04	08	10	20	40	80	1b	36
00	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	00

Rcon

We will use the following formula to compute each subkey:

Column XOR Sub-byte column XOR Rcon Column

For column 1:

54		23		01		76
45	XOR	C3	XOR	00	=	86
41		18		00		59
4D		C7		00		8A

For column 2:

53		23		01		25
43	XOR	C3	XOR	00	=	C5
4F		18		00		16
52		C7		00		D8

For column 3:

50		23		01		75
49	XOR	C3	XOR	00	=	8C
41		18		00		57
4E		C7		00		96

For column 4:

31		23		01		44
32	XOR	C3	XOR	00	=	BE

33		18		00		64
34		C7		00		A2

Combining all the resultant columns we can form our subkey 1.

76	25	75	44
86	C5	8C	BE
59	16	57	64
8A	D8	96	A2

Step 2: Encryption

Suppose we have a 16 byte or 128 bit message MESSAGE CRYPTO N.

Convert each character into its hexadecimal ASCII value.

M	E	S	S	A	G	E	N	C	R	Y	P	T	I	O	N
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

4D	41	4E	54	4D	41	4E	54	4D	41	4E	54	4D	41	4E	54
----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----

Convert the ASCII values into an NxN matrix, here a 4x4 matrix.

4D	41	4E	54
45	47	43	49
53	45	52	4F
53	45	50	4E

Add round key by computing *Hexadecimal Matrix XOR Subkey 0* of corresponding positions to find the resultant matrix.

4D	41	4E	54		54	53	50	31		19	12	1E	65
45	47	43	49	XOR	45	43	49	32	=	00	04	0A	7B

53	45	52	4F		41	4F	41	33		12	0A	13	7C
53	45	50	4E		4D	52	43	34		1E	17	1E	7A

Use sub-byte table to replace each element in the resultant matrix to get the after sub-byte matrix.

D4	C9	72	4D
63	F2	67	21
C9	67	7D	10
72	F0	72	DA

Shift each row of the matrix by 0, 1, 2, and 3 positions. Shift the first row by 0 i.e. don't shift the first row at all, shift the second row by 1, third row by 2 and the fourth row by 3. The shifted matrix is represented in orange below.

			D4	C9	72	4D
		63	F2	67	21	63
	C9	67	7D	10	C9	67
72	F0	72	DA	72	F0	72

Multiply every column of shift matrix with the pre-defined Mixed Column in AES. This multiplication yields the dot product and addition yields XOR sum.

$$\begin{array}{|c|c|c|c|} \hline a_{0,0} & a_{0,1} & a_{0,2} & a_{0,3} \\ \hline a_{1,0} & a_{1,1} & a_{1,2} & a_{1,3} \\ \hline a_{2,0} & a_{2,1} & a_{2,2} & a_{2,3} \\ \hline a_{3,0} & a_{3,1} & a_{3,2} & a_{3,3} \\ \hline \end{array} \times \begin{array}{|c|c|c|c|} \hline 2 & 3 & 1 & 1 \\ \hline 1 & 2 & 3 & 1 \\ \hline 1 & 1 & 2 & 3 \\ \hline 3 & 1 & 1 & 2 \\ \hline \end{array} = \begin{array}{|c|c|c|c|} \hline b_{0,0} & b_{0,1} & b_{0,2} & b_{0,3} \\ \hline b_{1,0} & b_{1,1} & b_{1,2} & b_{1,3} \\ \hline b_{2,0} & b_{2,1} & b_{2,2} & b_{2,3} \\ \hline b_{3,0} & b_{3,1} & b_{3,2} & b_{3,3} \\ \hline \end{array}$$

This will be our encrypted matrix.

(2.D4)xor(3.F2)xor(1.7D)xor(1.DA)
(1.D4)xor.....
...
...

NOTE: How to find the dot product?

Suppose we have to find the dot product of 2 and D4. Convert both numbers to binary and turn them into polynomials (only for the 1s). Multiply the polynomials and convert them back to binary. We can see that our polynomial contains x^8 which is more than a byte, hence we need to reduce the polynomial. AES has a pre-defined reduce polynomial $x^8+x^4+x^3+x^7+x^0$ with the binary value 100011011. Add the binary values of reduce polynomial and resultant polynomial till you get the MSB to be 0. Convert this value back to hexadecimal. That is our dot product.

2.D4

*=10 * 11010100*

*= $x^1 * x^7+x^6+x^4+x^2$*

=110101000

110101000+100011011=010110011

=19_H

Hence, the dot product is 19_H.

2.4. Authentication

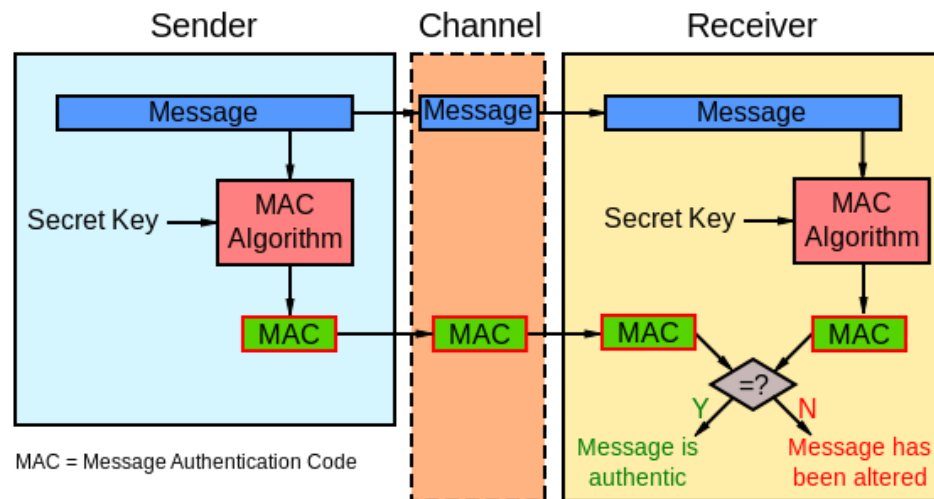
Authentication is the one of the five major principles of security. It is the process that is used in verifying the identity of the persons involved in a message transaction as well as the authenticity of the message itself. Usually, it uses an authenticator to do so. There are three techniques for authentication:

1. Encryption
2. Message Authentication Code (MAC)
3. Hash Functions

2.4.1. Message Authentication Code (MAC)

This method of authentication involves using a secret key to generate a fixed block of data called the MAC or cryptographic checksum. This code is then appended to the message and the secret key is sent to the receiver. MAC can be used to either obtain authentication or both authentication and confidentiality. It ensures that receiver knows whether message has been altered or not and verifies identity of sender.

Case 1: For Authentication



The message M from sender is passed through a MAC function C to obtain the message authentication code or MAC. The MAC and M are appended together and sent to the receiver along with the secret key used with C. The receiver then extracts the MAC from the appended message and also finds the MAC from C using the key. If both MACs on comparison are equal, the message is unaltered and authentic. If not, then our message is unauthentic. This method has only one disadvantage; there is no confidentiality if a third party comes in between of the message transaction.

Case 2: For Authentication and Confidentiality

This method is very similar to the previous one, except that it adds confidentiality by using encryption.

- a. *Authentication tied to plain text*- The message M is passed through MAC function C using key K_1 to obtain the MAC. M is then appended with the MAC obtained and encrypted using key K_2 . Since we are following symmetric encryption, the receiver will have K_2 already. The receiver will obtain M+MAC on decryption, which can then be extracted for comparison.
- b. *Authentication tied to cipher text*- This is slightly different from the previous one. Here, we encrypt the message M first using key K_1 and pass the derived cipher text through C using key K_2 to find the MAC. Then, append the cipher text and MAC and send it to the receiver. We can observe that confidentiality is achieved since it is difficult for attacker to decrypt and comprehend the message as it contains ciphertext and MAC. The receiver can now decrypt using K_1 and extract accordingly to authenticate.

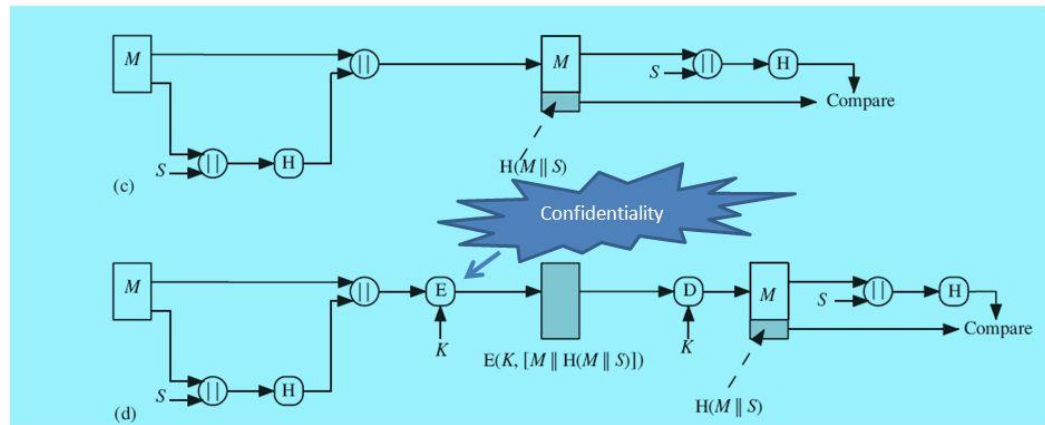
2.4.2. Hash Functions

Hash functions implementation is similar to that of MAC. The only difference is that hash functions do not use a key. It takes in a variable size input and produces a fixed output or hash code as depicted by the diagram below.

$H(M)$ =fixed length code h

Cryptographic Hash Functions

Message Authentication



Case 1: For authentication and confidentiality

Sender must pass the message M through hash function H . This will generate hash code h that will be appended to M and encrypted using a key. This combination of ciphertext and hash code is sent to the receiver who decrypts and passes extracted message M through $H(M)$ for comparison. If hash code from extraction is equal to hash code from $H(M)$, then the message is authentic.

Case 2: For authentication only

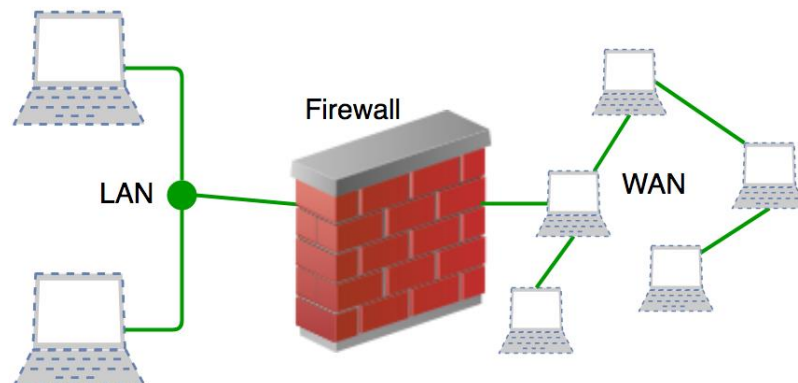
In this method, instead of encrypting the combination of h and M , we only encrypt h using key k . The message and encrypted hash code are then sent to user and the same procedure is followed as before. Note that both these methods do not involve using a key when passing through hash function $H(M)$.

2.5. Firewalls

A firewall is a network security device that acts like a barrier between secured internal networks and the outside world as shown below. It monitors and controls incoming and outgoing network traffic based on predefined protocols.

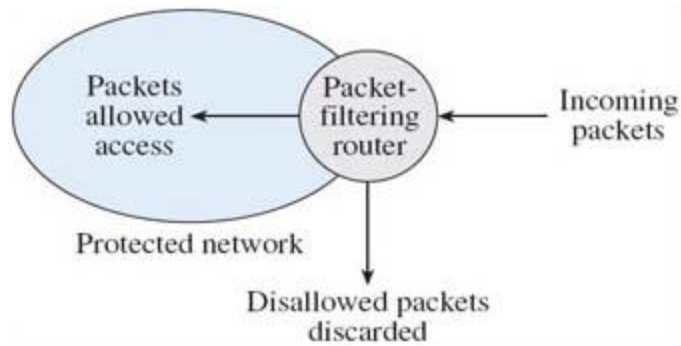
There are three types of firewalls-

1. Packet-filtering firewalls
2. Application Level Gateway
3. Circuit Level Gateway



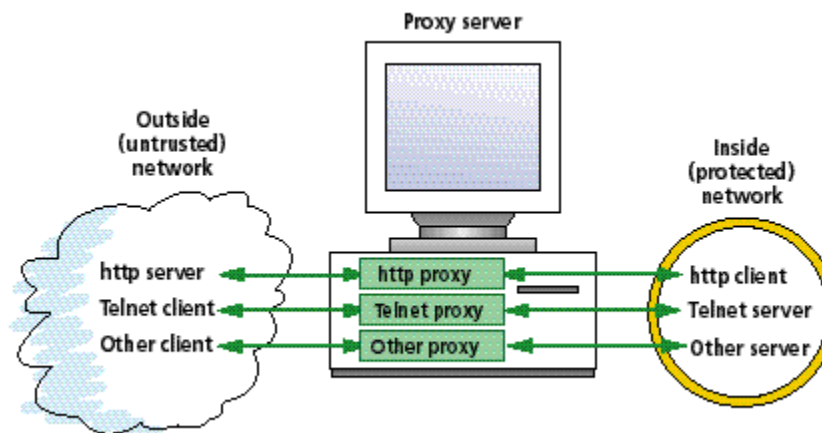
2.5.1. Packet-filtering firewalls

These kind of firewalls apply a set of rules to each incoming packet and takes actions accordingly. The rules are based on source input, destination input, protocols and ports. If the incoming or outgoing data satisfies the set rules, corresponding actions such as accept, reject and drop are taken. If not, default action is taken. Packet-filtering routers analyze traffic at the transport level. A filtering table is maintained which decides the action to be taken upon matching. For example, a rule might say that if Source IP= '192.168.21.0.', accept the information, else deny. Here is a nice diagram to explain it.



2.5.2. Application Level Gateways

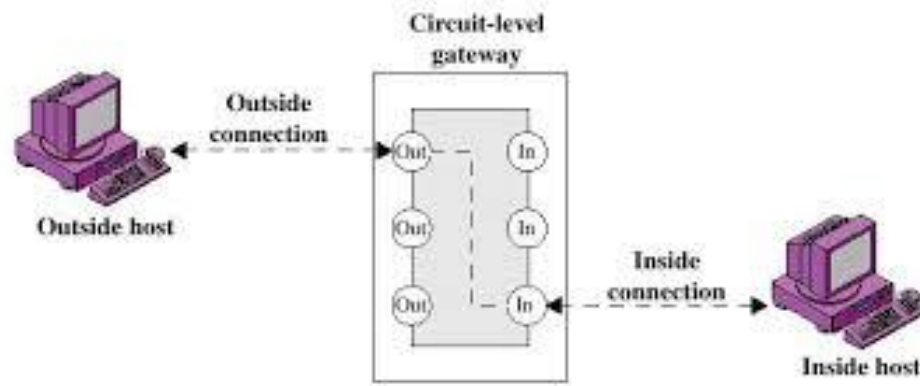
Application level gateways or host to proxy servers are used to contact users through TCP/IP applications such as TELNET and HTTP. It is more secure than Packet-filtering routers since all data must first pass through proxy servers before being transmitted. This can be explained with an example. Suppose some internal host xyz.com requests for data. This request is transferred to the proxy server which checks if source and request are valid. If valid, request is sent to external host where it is processed. The data obtained is sent back to the proxy server where it is verified again, If valid and safe as per pre-defined rules, data is sent to system. This process however, has a disadvantage. It is more time-consuming due to the processing overhead. A lot of time is taken by the transfer and processing of requests.



2.5.3. Circuit Level Gateways

These type of firewalls use two kinds of TCP connections, one between internal host and gateway and another between external host and gateway. All security checks are done before setting the connection up. Once the

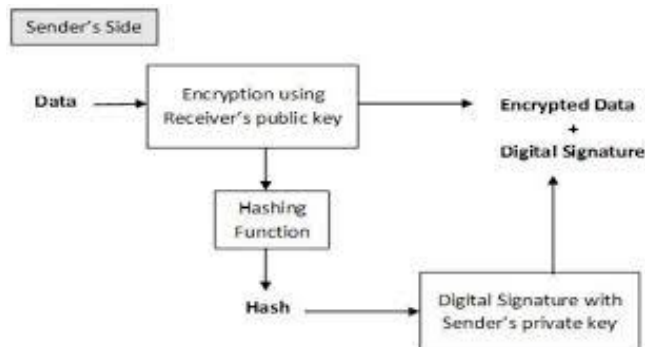
connection is established, all data transmitted passes without any hindrances. This process gives us the advantage of speed and time due to less number of evaluations.



2.6. Digital Signature

Digital signature is the process of guaranteeing the authenticity and integrity of a message. It helps us to verify identities, especially in online transactions and e-commerce dealings. It uses the concept of asymmetric cryptography and maintains non-repudiation of message. This process used three important algorithms for key generation for private key, signing by inputting message and private key and verification using public key and generated signature.

The signature must use some information that is unique to the sender in order to prevent forgery and denial. It must be easy to produce and verify. The digital signature is sent as a separate document along with actual message. One can verify if message is authentic and has integrity by checking for hash values and public key.



2.7. Shannon's Theory of Confusion and Diffusion

Claude Shannon's theory of confusion and diffusion is a fundamental part of cryptography. It was developed to essentially prevent any kind of cryptanalysis

done statistically and to create a secure cipher. It follows the below mentioned technique:

Diffusion- When a symbol or character in the plaintext is altered, several or all symbols in the ciphertext will also change. This hides the relationship between ciphertext and plaintext.

Confusion- When a bit or a symbol is altered in the key, most or all bits of ciphertext is changed.

Example 1, we use the theory of diffusion to depict a change in bits.

- a. Let our initial text be 'HELLO'
- b. We take the positions of each letter in the English alphabet for encryption
- c. Let us use the algorithm to get the encrypted values;
for($i=1; i < n; i++$)
 $A[i] = (A[i] + A[i+1]) \bmod 26$
 $A[n] = (A[n] + A[0]) \bmod 26$
- d. We now have the encrypted letters as per the English alphabet
- e. Suppose we change the first element in the plaintext (H becomes G)
- f. We repeat step b
- g. Repeat step c to get new encrypted values
- h. We can see that this change has only affected the first and last bits of the plaintext.

(a)	H	E	L	L	O
(b)	8	5	12	12	15
(c)	13	17	24	1	23
(d)	M	Q	X	A	W
(e)	G	E	L	L	O
(f)	7	5	12	12	15
(g)	12	17	24	1	22
(h)	L	Q	X	A	V

Example 2,

- a. Let our initial text be 'HELLO'
- b. We take the positions of each letter in the English alphabet for encryption

- c. Let us use the algorithm to get the encrypted values using a new empty array B;
for(i=1;i<n-1;i++)
for(j=1;j<=i;j++)
B[i]=(B[i]+B[j]) mod26
- d. We now have the encrypted letters as per the English alphabet
- e. Suppose we change the first element in the plaintext (H becomes G)
- f. We repeat step b
- g. Repeat step c to get new encrypted values
- h. We can now see that this change has affected all the bits of the plaintext.

(a)	H	E	L	L	O
(b)	8	5	12	12	15
(c)	8	13	25	12	11
(d)	H	M	Y	L	K
(e)	G	E	L	L	O
(f)	7	5	12	12	15
(g)	7	12	24	10	8
(h)	G	L	X	J	H

3. Introduction to Ethical Hacking

3.1. Hacking and Hackers

Ethical hacking refers basically to identifying the shortcoming and weaknesses in a computer system or network and counteracting them with the intention of protection with certain measures. Persons who carry out hacking are called hackers. There are four main types of hackers:

1. Ethical or White hat hackers- These gain access to fix the weakness of the system through various methods such as penetration testing, etc.
2. Cracker or black hat hacker- These gain unauthorized access for personal gain and the intent of theft.
3. Grey hat hackers- These are the in-betweens of white and black hat hackers. They gain unauthorized access only to identify the weaknesses of the system.
4. Hacktivist- These hackers use their skill set to send social, religious and political messages across the network by hijacking websites, accounts, etc. A very recent and popular example of these are the [Anonymous International](#).

Why is there a need for Ethical Hacking?

Today, all information is stored online or in computer databases. Losing such essential information can result in a loss of valuable assets for all organization and persons. Hence, ethical hacking prevents a computer network or system from being compromised by protecting it against malicious hackers.

What are the rules that must be followed by an Ethical Hacker?

1. Hacker must have written permission from the holder of the system to be accessed.
2. He/She must report all the identified shortcomings of the system transparently to the owner.
3. He/She must always protect the data of the organization or person at all costs.
4. In case of hardware or software weakness, respective vendors must be informed.
5. Following the above-mentioned rules makes ensures the legality of hacking.

What are the most commonly used programming languages by hackers?

Most commonly used are HTML, PHP and SQL mainly for web hacking. C and C++ for writing exploits and Python for building scripts and tools.

3.2. Security Attacks

There are two types of security attacks mainly:

1. Passive Attacks that attempt to make use of data and information from systems without really affecting system resources. These can easily be prevented using good encryption techniques. There are two types of passive attack:
 - a. Release of message content- which means that due to weak encryption techniques, hacker is able to understand the message easily.
 - b. Traffic analysis- by observing the pattern of messages through frequency of messages, length hacker is able to determine location and hosts in the network.
2. Active attacks basically attempt to alter the system's resources and data. These are of four types:
 - a. Replay-hacker captures the message such that the transmission happens repeatedly generating an unauthorized effect.
 - b. Masquerade- hacker pretends to be an entity it is not in reality,

- c. Modification of messages- messages sent over are altered, deleted or re-ordered.
- d. Denial of Service (DOS)- The most common type of attack done by disrupting the entire network by disabling it or by overloading it with messages in order to degrade its performance and make it unavailable for serious users and customers.

3.3. Security Threats

Security Threats range from physical threats that threaten to damage or harm the system to spyware that monitors activities or installs programs without owner's consent. Here, we will only discuss non-physical threats pertaining to computers.

- 1. Virus- perhaps, the most commonly known type of threat to our systems, attaches itself to existing authorized programs and files without consent, much like its biological namesake. It slows down the network.
- 2. Trojan horse- program that allows attack in order to gain control of the computer system from any remote location without being physically present. It is responsible for data theft and spying.
- 3. Worm- program that works by replicating itself over the network. It corrupts and disrupts working greatly.

3.4. Hacking Tools

There are a number of tools available online in the form of web applications and softwares that help detect weaknesses and manipulate through them. Below are the few tools that are considered most useful in this field of work:

- 1. Acunetix is a functional software that mimics hacker and his/her activities and follows an algorithm such that it is always one step ahead of the intruders. It is also equipped to scan for SQL, HTML5 and JavaScript vulnerabilities.
- 2. Netsparker is a very user-friendly web application that detects URL rewrites, SQL injections and customized (fake) error 404 pages.
- 3. IKECrack allows users to perform cryptography tasks using open authentication tools.
- 4. SaferVpn is a fast speed tool that checks anonymous file transfers.



netsparker



SaferVPN



QualysGuard

3.5. Password Cracking

Password cracking requires solving some algorithms and obtaining authentication and hence access to certain accounts and data. Normally, efficiency of a password is determined by its length, complexity and unpredictability. For example, *got1234* is shorter and easier to predict than *Godzilla2078\$*. This is elaborated further with the use of a password strength meter <https://howsecureismypassword.net/>.

Image 1 displays the time taken by a computer to crack *got1234*. Image 2 lists down the predictability of the password and suggestions to make it stronger.



Image 3(below) displays the time taken by a computer to crack *Godzilla2078\$*. It is obvious that a combination of non-sequenced alphanumeric characters make better passwords.



Now, we will be discussing the top 5 password cracking techniques used by professionals today.

1. Dictionary Attack- uses a wordlist of most commonly used words as user passwords and matches it against the password to be cracked.
2. Brute-force Attack- similar to dictionary attack but it focuses on detecting non-dictionary alphanumeric characters and symbols.
3. Rainbow Table Attack- uses pre-computed passwords and their hashes.
4. Phishing- one of the most commonly used methods of cracking passwords. Hackers ask user to enter log in details on a fake log in page and hence, acquire all the details.
5. Keylogger- this can be installed on any device with the help of malware and records on typing processes and login processes and sends them to the hacker involved.

3.6. IP and MAC addresses

IP and MAC addresses are very integral components of networking. Internet Protocol addresses are used to identify devices connected on a network, something very similar to a postal address. Basically, whenever a user requests for a page, the request is sent to the page identified by its IP address. It has two version: IPv4 and IPv6. IPv4 uses 32 bits and looks something like this- 127.0.0.1 while IPv6 uses 128 bits and can be written as- 2001:0db8:85a3:8a2e:370:7334. Media Access Control addresses on the other hand, are used to uniquely identify network interfaces for communication usually embedded into the network adapter's card. It can be thought of more simply as the characteristics of the user's mailbox.

We can clearly find out all the network connections available on a system through Windows Command Prompt. The command `ipconfig/all` displays MAC address, IPv4 and IPv6 of the network used as displayed below.

```
Mobile Broadband adapter Mobile Broadband Connection 3:
Connection-specific DNS Suffix . :
Description . . . . . : HUAWEI Mobile Connect - Network Adapter #
3
Physical Address. . . . . : 58-2C-80-13-92-63 ← MAC Address
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . : Yes
IPv4 Address. . . . . : 10.131.70.186(Preferred)
Subnet Mask . . . . . : 255.255.255.252 ← IPv4 Address
Default Gateway . . . . . : 10.131.70.185
DNS Servers . . . . . : 41.223.4.97
                        41.223.5.33
NetBIOS over Tcpip. . . . . : Enabled
```

3.6.1. ARP Poisoning

“Address Resolution Protocol (ARP) is a procedure for mapping a dynamic Internet Protocol address (IP address) to a permanent physical machine address in a local area network (LAN).” It is used to convert 32-bit addresses to 48-bit addresses since IPv4 is 32-bits long but MAC addresses used are 48-bit long.

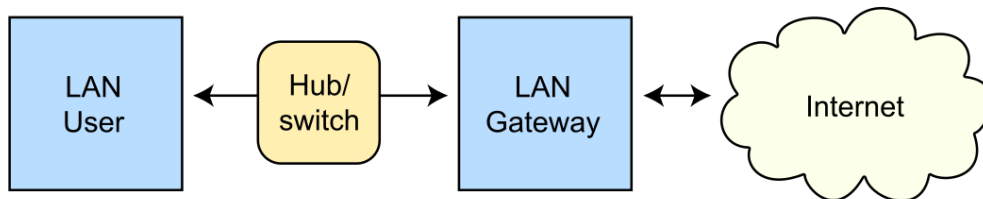
How does ARP work?

Normally, the host computer sends an ARP broadcast on the network and recipient computer responds to the query with its MAC address. That is, a computer is assigned a unique IP address on joining a network or LAN. The ARP program is supposed to find a suitable MAC address for incoming data packets that match the given IP address as per the ARP cache, which stores a list of IP addresses with their MAC counterparts.

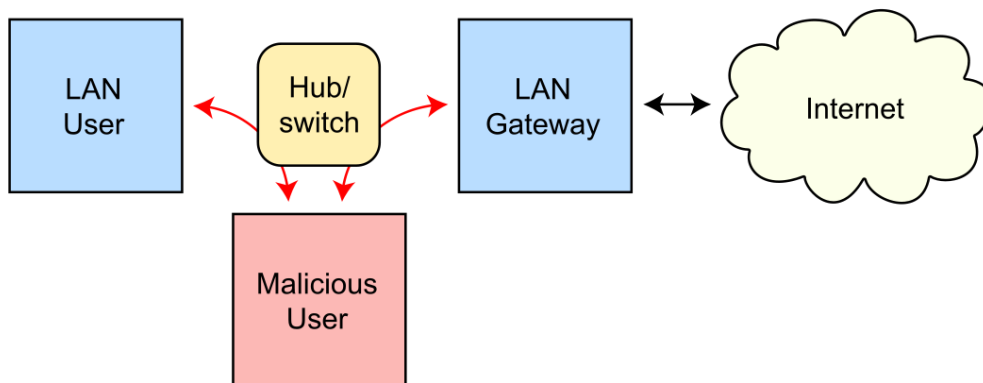
What is ARP Poisoning?

ARP Poisoning occurs when a middle-man or hacker sends fake ARP messages across the LAN or network in order to establish a legitimate link between the hacker's MAC address and the real IP address. This way all the data to be transmitted from the real IP address goes to the hacker's IP address instead.

Routing under normal operation



Routing subject to ARP cache poisoning

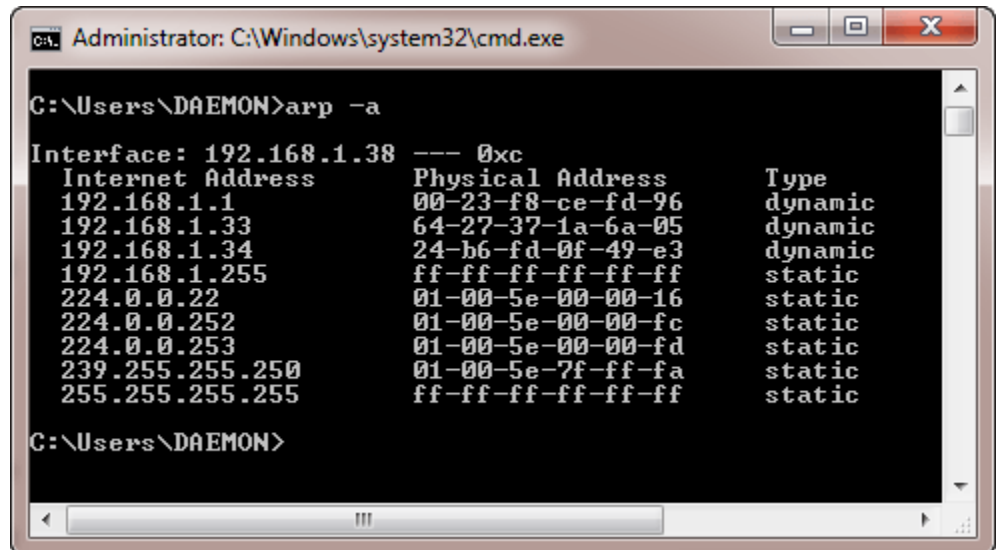


There are two types of ARP entries:

1. Static ARP entries- These are defined in the system's local ARP cache and are programmed to ignore all automated ARP reply packets. They can be added manually and are deleted when system restarts(volatile).

Command Prompt –

a. *arp -a* displays all the entries in ARP cache



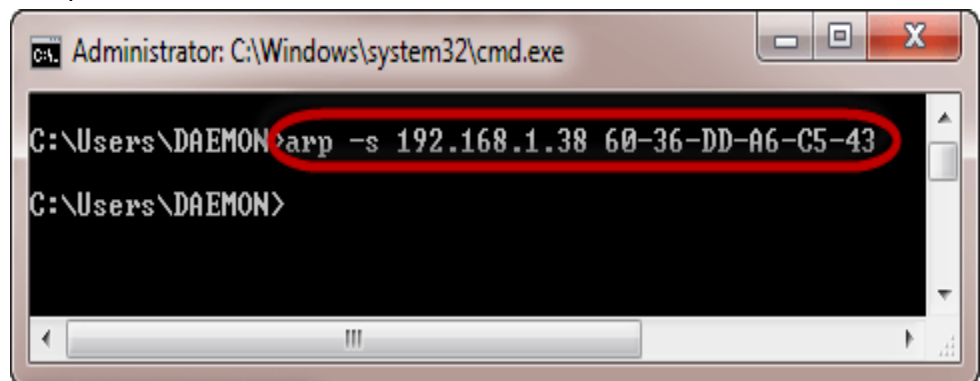
A screenshot of a Windows Command Prompt window titled "Administrator: C:\Windows\system32\cmd.exe". The prompt shows the command `arp -a` being executed. The output displays the ARP table for the interface 192.168.1.38. It lists several entries with their Internet Address, Physical Address, and Type. The types include dynamic and static.

```
C:\Users\DAEMON>arp -a

Interface: 192.168.1.38 --- 0xc
Internet Address      Physical Address      Type
192.168.1.1           00-23-f8-ce-fd-96    dynamic
192.168.1.33          64-27-37-1a-6a-05    dynamic
192.168.1.34          24-b6-fd-0f-49-e3    dynamic
192.168.1.255         ff-ff-ff-ff-ff-ff    static
224.0.0.22            01-00-5e-00-00-16    static
224.0.0.252           01-00-5e-00-00-fc    static
224.0.0.253           01-00-5e-00-00-fd    static
239.255.255.250       01-00-5e-7f-ff-fa    static
255.255.255.255       ff-ff-ff-ff-ff-ff    static

C:\Users\DAEMON>
```

b. *arp -s* adds static entries

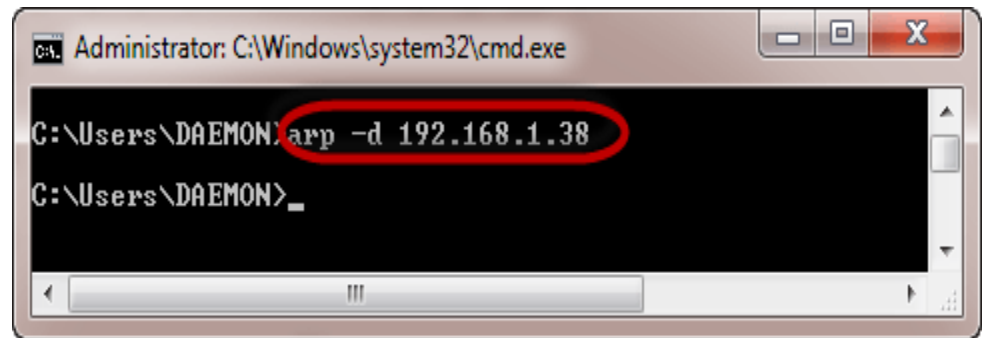


A screenshot of a Windows Command Prompt window titled "Administrator: C:\Windows\system32\cmd.exe". The prompt shows the command `arp -s 192.168.1.38 60-36-DD-A6-C5-43` being entered. The command is highlighted with a red oval.

```
C:\Users\DAEMON>arp -s 192.168.1.38 60-36-DD-A6-C5-43

C:\Users\DAEMON>
```

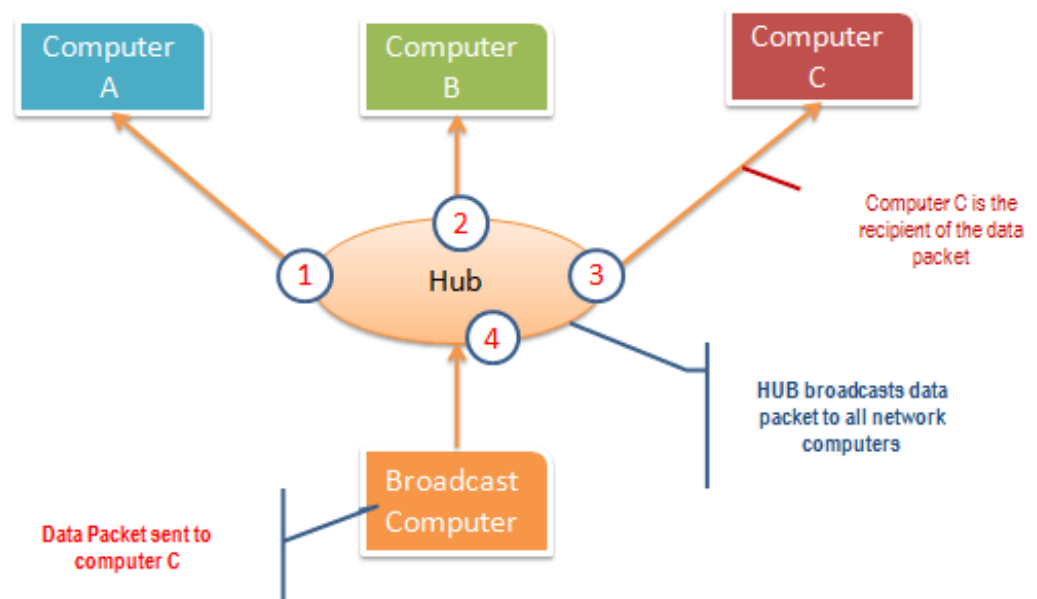
c. *arp -d* deletes static entries



3.7. Network Sniffing

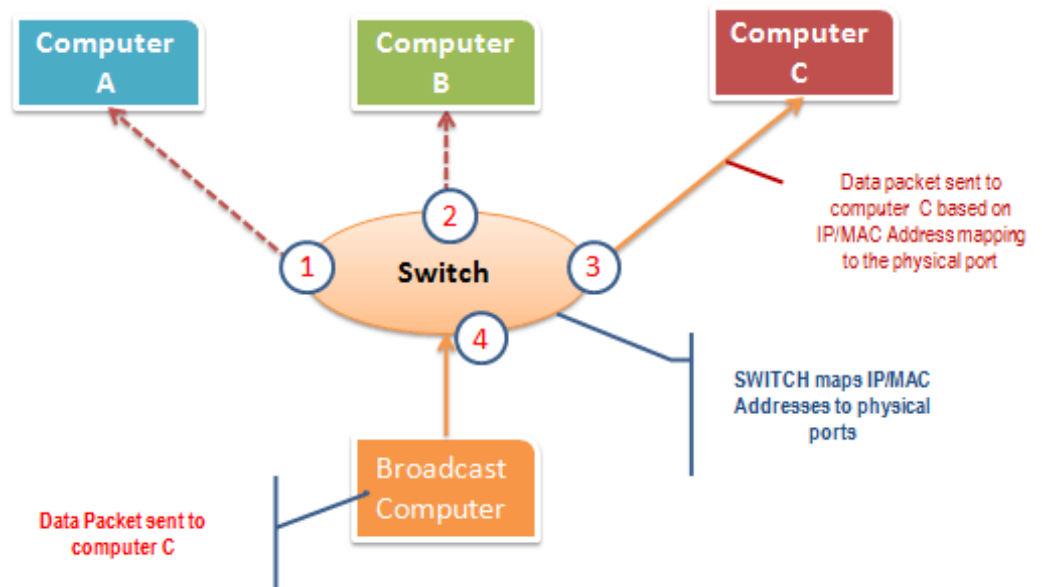
Network Sniffing is the process of capturing data transmitted over a network by intercepting packets mid-air. Network Sniffers usually intercept messages and record them without altering them. These can capture everything from network credentials to chat messages. There are two kinds of network sniffing:

1. Passive Sniffing- This involves intercepting packages transmitted over a network that uses a hub. A hub is device that receives broadcasts from a computer and transmits the packets to all the computers on that network. This method is both difficult to detect and easy to perform, since the hub broadcasts data to all computers.



2. Active Sniffing- This technique involves intercepting packages transmitted over a network that uses a switch. A switch is a device that transmits data

only to computer whose IP/MAC addresses match that of the physical ports. This is used more often than passive sniffing.



The following protocols are vulnerable to sniffing attacks if packages are sent in plaintext:

HTTP
Telnet
NNTP
SMTP
and POP etc.

3.7.1. Implementation

Several kinds of attacks can be implemented to carry out network sniffing.

1. MAC Flooding- Probably the most popular approach to network sniffing. This involves flooding the cache table with false MAC addresses to overload the switch which in turn begins acting like a hub and sending data packets all over the network.
2. DNS Cache Poisoning- DNS (Domain Name System) cache records are altered in such a way that the request is directed to a genuine-looking malicious website.

3. Evil Twin Attack- The attacker sets up a similar DNS to that of the user that responds to all the requests instead.
4. MAC Spoofing- The attacker acquires the MAC addresses associated with the switch and sets the device used in sniffing to the same address. Hence, all the messages intended for the actual recipient's computer are redirected to the attacker's system.

3.7.2. Counter Measures

1. Limit the number of MAC addresses associated with the ports.
2. Authenticate servers
3. Careful transmission of encrypted messages
4. Change the network to a Secured Shell Network (SSH)
5. Restrict networking of physical media

3.8. Wireless Networks

What makes wireless networks different is that they “use radio waves to link computers and other devices at physical layer 1.” They are mostly password-protected and require authentication for access.

There are four types of wireless networks:

1. Wireless Local Area Network (WLAN): Connects two or more devices using a wireless distribution method.
2. Wireless Metropolitan Area Networks (WMAN): Connects a number of wireless LANs.
3. Wireless Wide Area Network (WWAN): Connects devices over large areas such as cities.
4. Wireless Personal Area Network (WPAN): Connects devices within a certain range in a very short time.

3.8.1. Wired Equivalent Privacy

WEP is a security protocol for wireless local area networks that provides the same level of security to that of wired LANs. It is required since as compared to LANs, WLANs work over radio waves and cannot be protected from unauthorized access by a physical structure. WEP works by encrypting transmitted data, i.e. it performs end-to-end encryption of messages. But latest research has observed that WEP does not actually succeed in encrypting all data from end-to-end as it operates at the two

lowest layers of the OSI (Open Systems Interconnection) Model -Data link and Physical Layer.

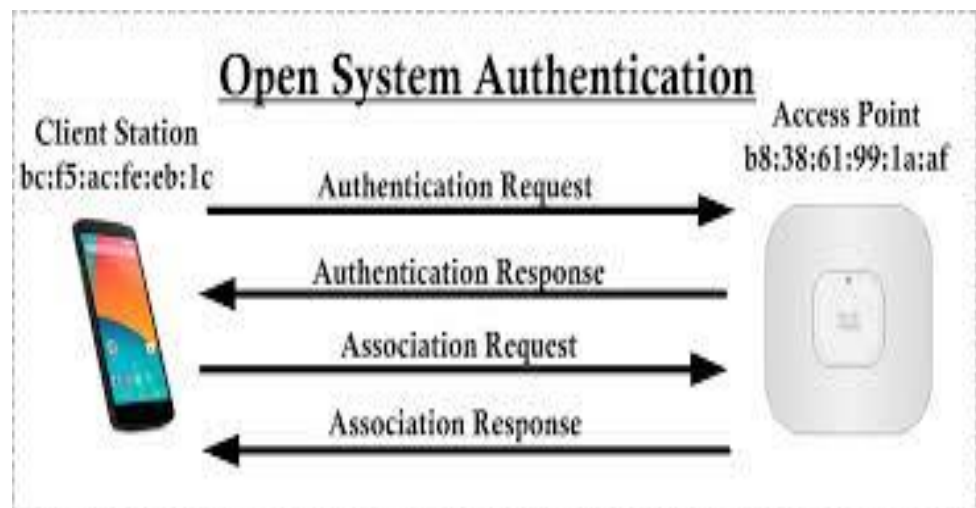
More about OSI Model:

<https://www.networkworld.com/article/3239677/the-osi-model-explained-how-to-understand-and-remember-the-7-layer-network-model.html>

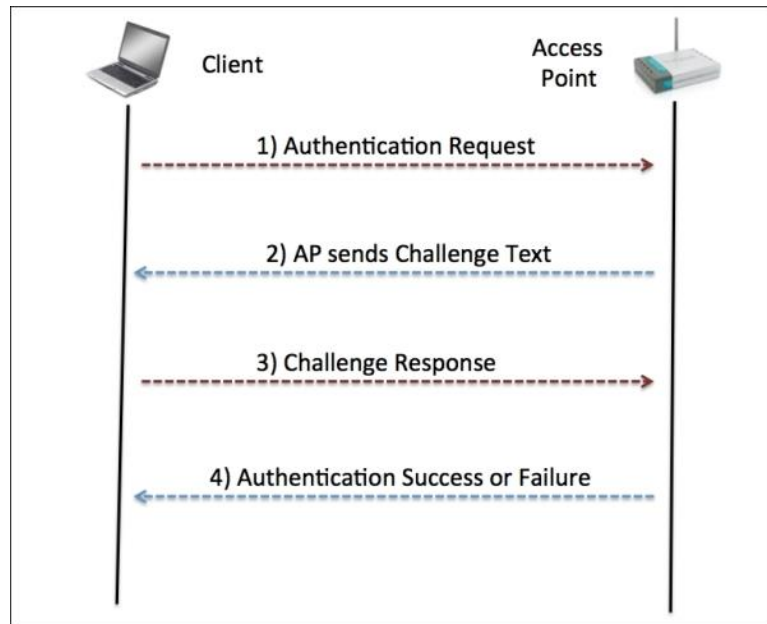
What is WEP Authentication?

WEP authentication simply refers to the methods used to ensure access to authorized users only. The following are the two main types used:

- a) Open System Authentication (OSA)- It is a method that grants access to requested authentication based on the existing access policy of the system. It can be better explained with the help of a diagram.



- b) Shared Key Authentication (SKA)- It is a process that begins with the user sending a authentication request to the network access point, which in turn sends as encrypted file to the user that must be decrypted using password. The access point then verifies if the decrypted file returned by the user exists and grants access accordingly.



What are the shortcomings of WEP?

For starters, WEP uses the RC4 algorithm which is easy to decode as it uses a smaller number of bits, 40 to be precise for the key. It is based on passwords that are vulnerable to dictionary attacks. Furthermore, it uses the CRC32 algorithm to carry out integrity checks, which is not the best choice for computing cryptographic hashes as it can easily be compromised by capturing just two data packets.

How to crack WEP?

WEP cracking refers to exploiting weaknesses of the wireless network in order to gain access. This can be done in two ways:

1. Passive Cracking- gaining access without affecting network traffic making it more difficult to detect.
2. Active Cracking- gaining access and increasing load on network traffic as a result. It is easy to detect but more effective.

A number of online tools and software can be used to crack WEP like Aircrack, Kismet and WEPCrack.

3.8.2. Wi-Fi Protected Access

WPA is another security protocol that functions to secure wireless networks using improved encryption techniques as compared to WEP. The reason that it is better than WEP is because it uses a Temporal Key Integrating Protocol (TKIP) that regularly changes the key used instead of using the same key as done in WEP. This prevents attackers from discovering the encryption key. WPA also moves away from the conventional MAC address mapping for authentication to using Extensible Authentication Protocol (EAP) which makes even more difficult to gain access to the network.

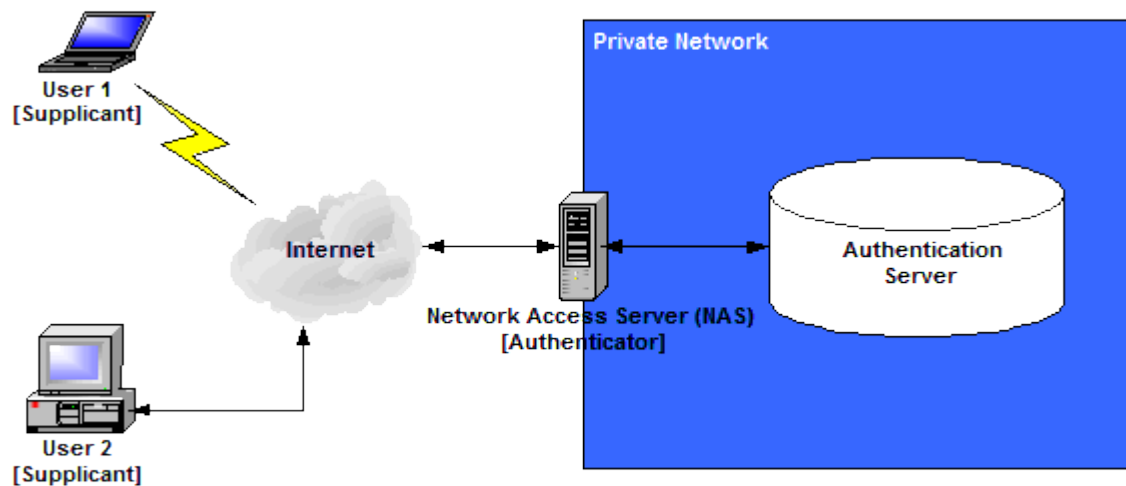
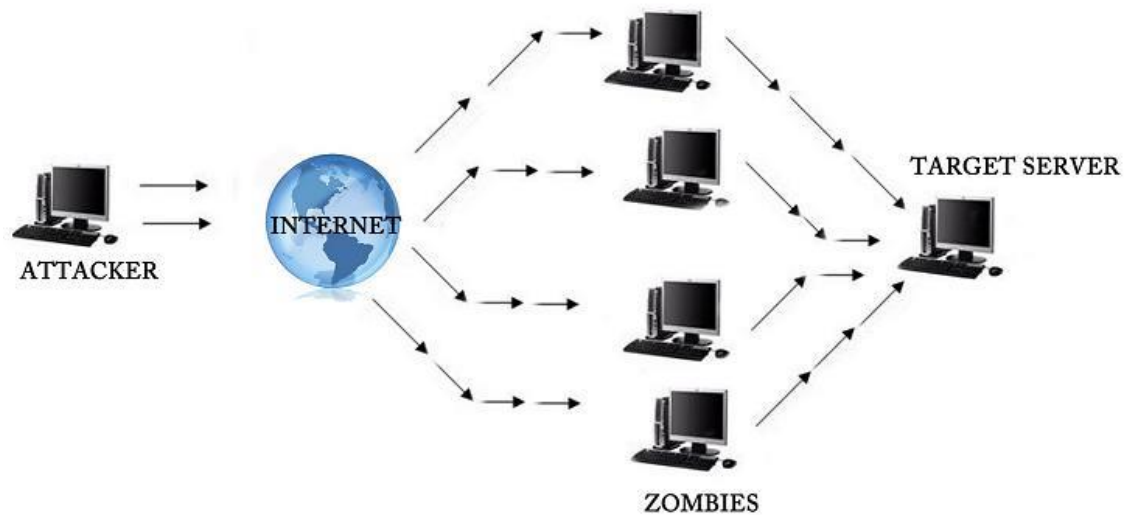


Figure 1: EAP Architecture

Does WPA have weaknesses too?

Yes, since nothing can ever be perfect, WPA too has its drawbacks. Firstly, it is vulnerable to denial of service or DOS attacks. Secondly, the passphrases or passwords used by the keys are vulnerable to dictionary attack. It is also not compatible with a number of operating systems and older systems.

DENIAL OF SERVICE ATTACK



How can we crack WPA?

We already know that WPA uses a 256-bit pre-shared key and that makes it vulnerable to dictionary attacks. A number of tools such as CowPatty, Cain and Abel can be used to exploit this.

Finally, how can we secure wireless networks?

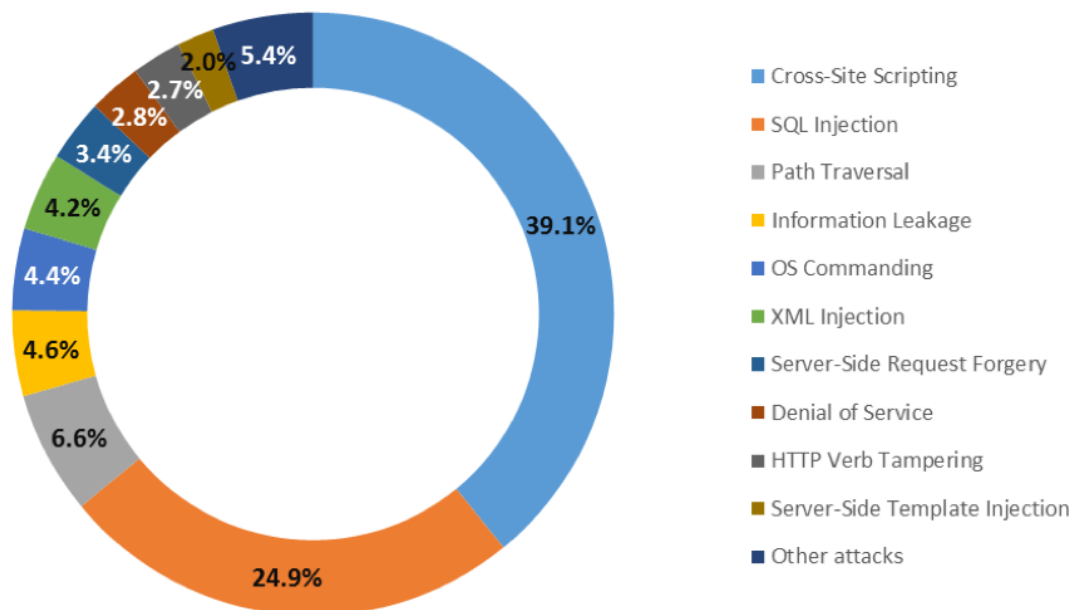
1. Set up authentication mechanisms
2. Change default passwords
3. Change passwords frequently
4. Allow only registered MAC addresses access
5. Use strong keys to prevent attacks
6. Set up firewalls

3.9. Web Servers

Web Servers are software or hardware that use protocols such as HyperText Transfer Protocol (HTTP) to respond to web queries or requests. They store web pages as files that can be accessed upon requesting.

In the recent times, many web server vulnerabilities have come under the notice of specialists. Click on the links below for more details.

- [SQL Injection](#)
- [Cross Site Scripting](#)
- [Broken Authentication and Session Management](#)
- [Insecure Direct Object References](#)
- [Cross Site Request Forgery](#)
- [Security Misconfiguration](#)
- [Insecure Cryptographic Storage](#)
- [Failure to restrict URL Access](#)
- [Insufficient Transport Layer Protection](#)
- [Unvalidated Redirects and Forwards](#)



There are three basic types of web servers:

1. Apache- It is an HTTP server developed by Apache that is used by IBM, Cisco and Adobe.
2. Apache Tomcat- It is the web server that hosts most websites written in Java.
3. Internet Information Server- IIS is a creation by Microsoft and runs on Windows. It hosts asp and aspx sites.

3.9.1. Web Attacks

Numerous web attacks are conducted to steal sensitive and private information not available publicly. These attacks include Denial of Service, Phishing, Sniffing, DNS hijacking and Defacement. The first four terms have been explained before, but defacement remains unexplained.

Defacement is an attack that replicates original websites and poses as an organization's actual page.

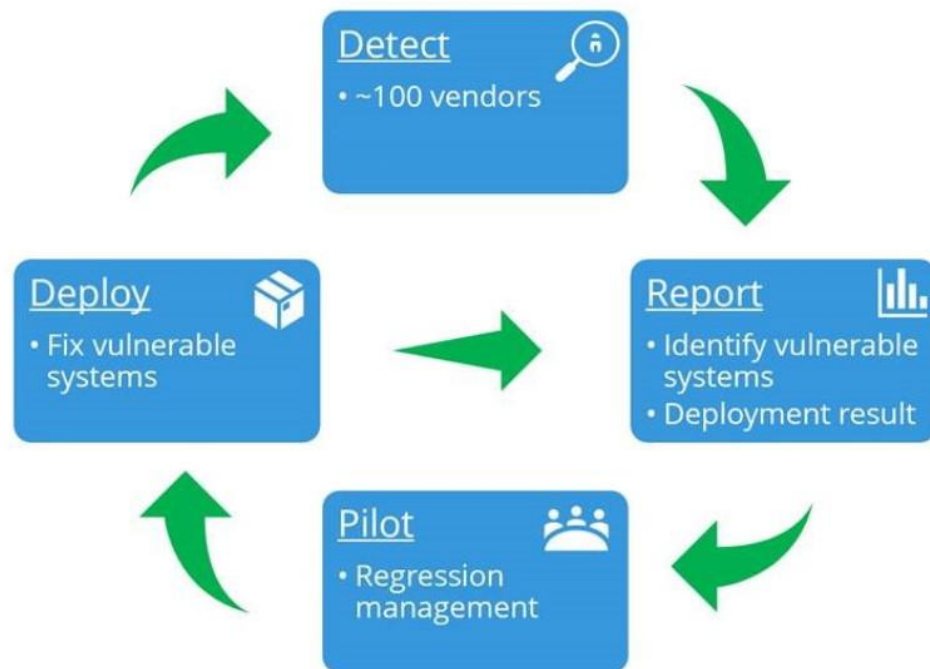
These attacks can have massive after-effects in various ways:

- a. Gaining access to valuable data
- b. Installing malicious bugs, software on the system
- c. Altering website contents, leading to loss of reputation
- d. Using acquired data illegally

How can prevent web attacks?

1. Antivirus- popularly used software used to get rid of unwanted files on the system
2. Firewall- device used to block traffic from attacker's end
3. Patch Management- installing patches or updates to fix bugs in a system
4. Use secure vulnerability scanners
5. Change custom ports settings

The image below depicts the patch management process applied by Windows.



4. Network Penetration Testing

Also known as pentesting, this method involves testing sites, applications, devices such as routers and switches and systems in order to find any kind of vulnerabilities or weaknesses that may be exploited by hackers. The reason pen test is carried out is to find and fix security issues in a way to prevent hacker attacks in the future.

How is penetration testing different from usual vulnerability assessments? Usual vulnerability tests aim only at evaluating systems and their security features, while penetration testing actually performs exploits on a network to find its flaws and correct them if any. It is a kind of replication of the steps performed by a hacker when attacking the network.

4.1. Linux Commands

Kali Linux is a software or tool designed mainly for the works of ethical hacking and network penetration testing. Below are a few commands written in Linux using Kali Linux VMware Workstation Player 15.

1. pwd- Stands for print working directory. Shows location of directory
2. cd- Stands for change directory and allows moving from one directory to another.
For example,
cd Desktop/ moves user to desktop
cd.. moves user back to the directory he/she was in previously
3. ls – lists all files and folders in the directory
4. cd<foldername>/- displays all files in that particular folder
5. cd /root/- moves back to root folder
6. mkdir <name>- creates a new directory with the mentioned name
7. rmdir <name>- removes a directory
8. ls -la- lists all hidden files as well
9. “xyz” new.txt- creates a file
10. cp new.txt Desktop/new.txt- copies the new file created to Desktop
11. rm Desktop/new.txt- removes the copied file from desktop
12. mv new.txt Desktop/new.txt- moves file to desktop
13. locate <filename>- locates file mentioned

When you list all files, you will notice the following syntax:

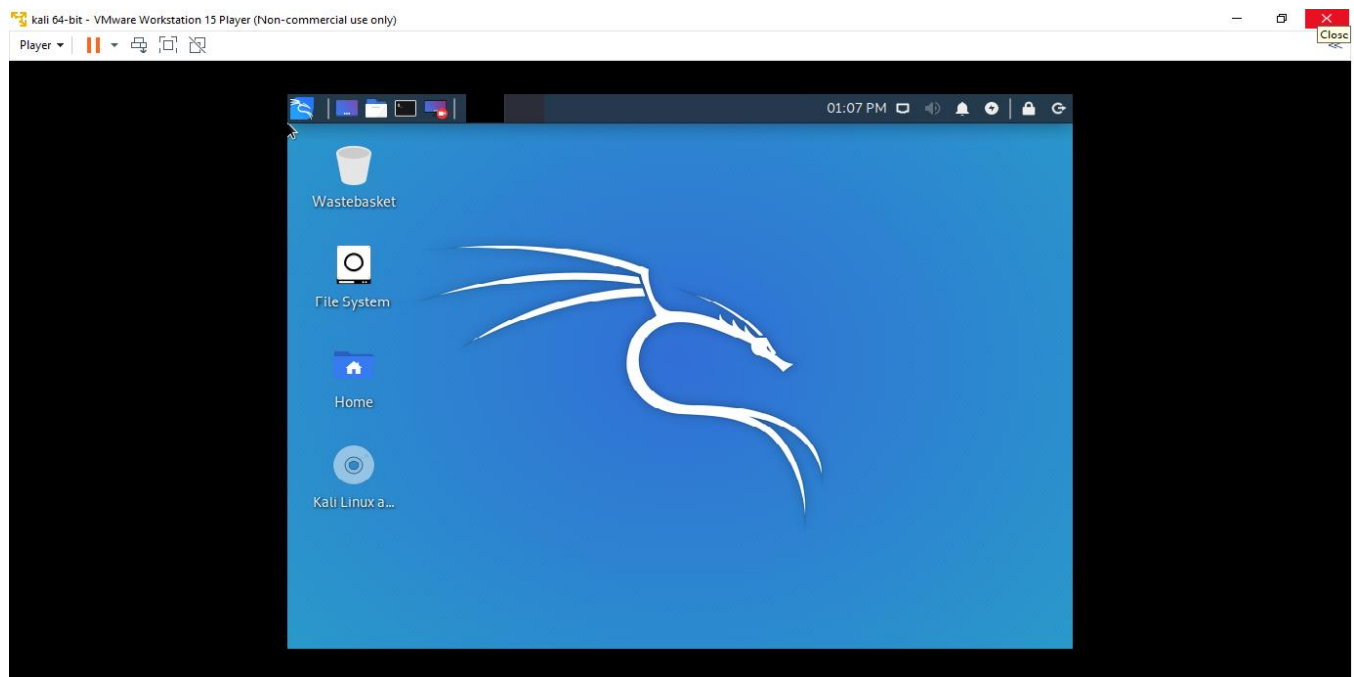
drwxr-xr-x : Here, *d* stands for directory, *r* for read, *w* for write and *x* for execute. If a dash – replaces the *d*, we can say that it is file. The first three set of letters(*rw**x*) decide the file owner’s permissions, the next three for

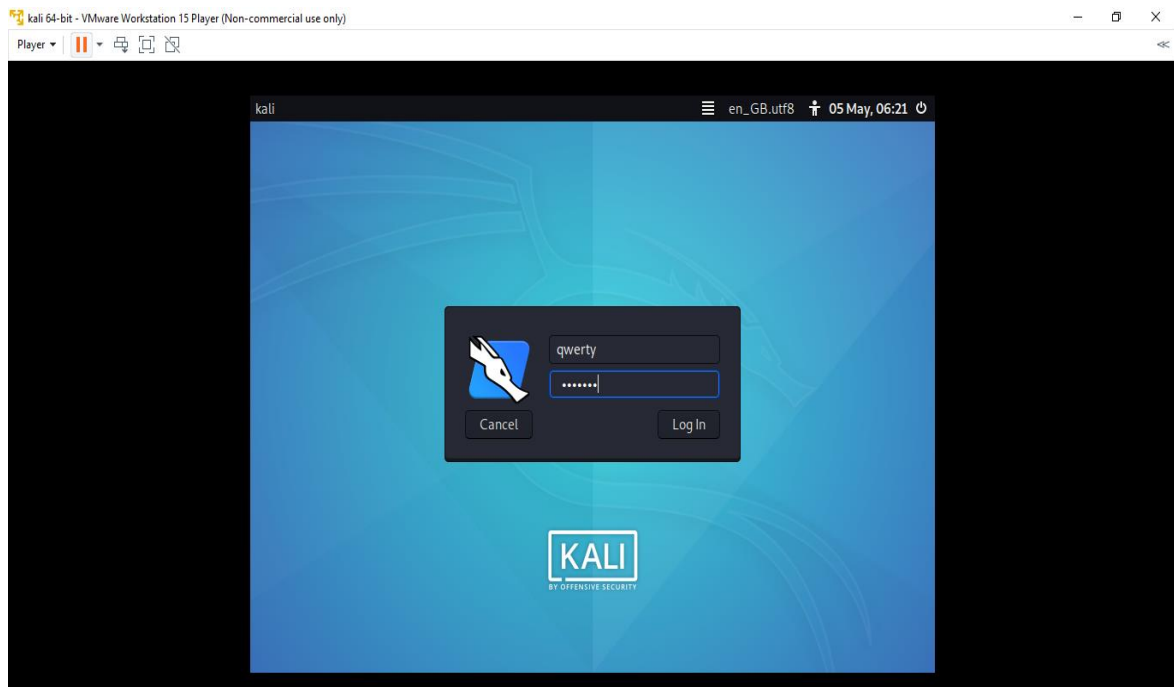
group owner's permissions (*r-x*) and the last three for all other permissions.

We must also know that for any permission, value of the bit must be 1. For example, if the selected group is to be given the permission to execute, then value of *x* *should be 1*.

14. `chmod 777 <filename>`- this command changes permissions to read, write, execute for all three sets. The hexadecimal value of 7 is 111. Hence, for all sets to be able to perform all three operations, they should all have the value 7 or 111.
15. `chmod +x <filename>`- adds the execute permission for sets
16. `adduser <name>`- creates and adds another user for access
17. `cat /etc/shadow`- displays all passwords with hashes
18. `cat /etc/passwd`- shows all details of users
19. `su <name>`- switches user
20. `sudo cat /etc/shadow`- checks if user is authorized
21. `cd /var/log`- goes to log directory
22. `ifconfig`- displays all configuration details
23. `iwconfig`- displays all wireless connections
24. `arp -a`- displays all IP and MAC addresses
25. `netstat -ano`- displays all open ports and their details
26. `history`- displays all recent commands

The images given below display a few of these commands:





```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# pwd  
/root  
root@kali:~# cd  
.cache/ Desktop/ Downloads/ .local/ Music/ Public/ Videos/  
.config/ Documents/ .gnupg/ .mozilla/ Pictures/ Templates/  
root@kali:~# cd Desktop/  
root@kali:~/Desktop# cd ..  
root@kali:~# cd ..  
root@kali:/# cd ..  
root@kali:/# pwd  
/  
root@kali:/# ls  
bin home lib32 media root sys vmlinuz  
boot initrd.img lib64 mnt run tmp vmlinuz.old  
dev initrd.img.old libx32 opt sbin usr  
etc lib lost+found proc srv var  
root@kali:/# cd home/  
root@kali:/home# ls  
root@kali:/home# cd /root/  
root@kali:~# ls  
Desktop Documents Downloads Music Pictures Public Templates Videos  
root@kali:~# ls Desktop/  
mount-shared-folders restart-vm-tools  
root@kali:~# mkdir new
```



```
root@kali: ~  
File Edit View Search Terminal Help  
Documents Music Pictures Templates  
root@kali:~# ls -la  
total 116  
drwxr-xr-x 15 root root 4096 Mar 20 20:42 .  
drwxr-xr-x 19 root root 36864 Feb 11 03:09 ..  
-rw-r--r-- 1 root root 1 Feb 11 03:30 .bash_history  
-rw-r--r-- 1 root root 3391 Jan 30 02:03 .bashrc  
drwx----- 8 root root 4096 Feb 11 03:06 .cache  
drwxr-xr-x 11 root root 4096 Mar 20 20:22 .config  
drwxr-xr-x 2 root root 4096 Mar 20 20:42 Desktop  
drwxr-xr-x 2 root root 4096 Feb 11 02:43 Documents  
drwxr-xr-x 2 root root 4096 Feb 11 02:43 Downloads  
drwx----- 3 root root 4096 Feb 11 02:43 .gnupg  
-rw----- 1 root root 1228 Mar 20 20:20 .ICEauthority  
drwx----- 3 root root 4096 Feb 11 02:43 .local  
drwx----- 5 root root 4096 Feb 11 02:49 .mozilla  
drwxr-xr-x 2 root root 4096 Feb 11 02:43 Music  
-rw-r--r-- 1 root root 6 Mar 20 20:42 new.txt  
drwxr-xr-x 2 root root 4096 Feb 11 02:43 Pictures  
-rw-r--r-- 1 root root 148 Nov 29 08:49 .profile  
drwxr-xr-x 2 root root 4096 Feb 11 02:43 Public  
drwxr-xr-x 2 root root 4096 Feb 11 02:43 Templates  
drwxr-xr-x 2 root root 4096 Feb 11 02:43 Videos  
root@kali:~# chmod 777 new.txt
```

```
root@kali: ~  
File Edit View Search Terminal Help  
-rwxr-xr-x 1 root root 6 Mar 20 20:42 new.txt  
drwxr-xr-x 2 root root 4096 Feb 11 02:43 Pictures  
-rw-r--r-- 1 root root 148 Nov 29 08:49 .profile  
drwxr-xr-x 2 root root 4096 Feb 11 02:43 Public  
drwxr-xr-x 2 root root 4096 Feb 11 02:43 Templates  
drwxr-xr-x 2 root root 4096 Feb 11 02:43 Videos  
root@kali:~# adduser bob  
Adding user `bob' ...  
Adding new group `bob' (1000) ...  
Adding new user `bob' (1000) with group `bob' ...  
Creating home directory `/home/bob' ...  
Copying files from `/etc/skel' ...  
Enter new UNIX password:  
Retype new UNIX password:  
passwd: password updated successfully  
Changing the user information for bob  
Enter the new value, or press ENTER for the default  
Full Name []:  
Room Number []:  
Work Phone []:  
Home Phone []:  
Other []:  
Is the information correct? [Y/n]  
root@kali:~# cat /etc/pass
```



```
File Edit View Search Terminal Help
bob@kali: /root
speech-dispatcher:!:17926:0:99999:7:::
pulse:!:17926:0:99999:7:::
king-phisher:!:17926:0:99999:7:::
Debian-gdm:!:17926:0:99999:7:::
dradis:!:17926:0:99999:7:::
beef-xss:!:17926:0:99999:7:::
systemd-coredump:!!:17938:::::
bob:$6$TJUmf7$nsyXkIrysJy2h3Ibns9D5Dhyvbk2c/UYZAhv0UZ3IzobeH0dqAGXjMviA0j8/nI
ejEhrzKqMIL.i0efek6A0/:17976:0:99999:7:::
root@kali:~# su bob
bob@kali:/root$ cat /etc/shadow
cat: /etc/shadow: Permission denied
bob@kali:/root$ sudo cat /etc/shadow

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

#1) Respect the privacy of others.
#2) Think before you type.
#3) With great power comes great responsibility.

[sudo] password for bob:
bob is not in the sudoers file. This incident will be reported.
bob@kali:/root$
```

```
File Edit View Search Terminal Help
root@kali: /var/log
Mar 20 20:55:04 kali CRON[2994]: pam_unix(cron:session): session opened for user
root by (uid=0)
Mar 20 20:55:04 kali CRON[2994]: pam_unix(cron:session): session closed for user
root
root@kali:/var/log# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.56.129 netmask 255.255.255.0 broadcast 192.168.56.255
    inet6 fe80::20c:29ff:fe9e:978d prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:9e:97:8d txqueuelen 1000 (Ethernet)
    RX packets 1050970 bytes 1573476386 (1.4 GiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 61772 bytes 4052287 (3.8 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 18 bytes 1038 (1.0 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 18 bytes 1038 (1.0 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
root@kali:/var/log#
```

```

Applications ▾ Places ▾ Terminal ▾ Player ▾
root@kali: ~/Downloads

File Edit View Search Terminal Help

192.168.56.0 0.0.0.0 255.255.255.0 U 100 0 0 eth0
root@kali:/var/log# history
 1 cd /var/log/
 2 ls
 3 ls -la
 4 cat syslog
 5 cat syslog | grep bob
 6 cat syslog | grep sudo
 7 cat auth.log
 8 ifconfig
 9 iwconfig
10 ping 192.168.1.254
11 ping -c 1 192.168.1.254
12 arp -a
13 netstat -ano
14 route
15 history
root@kali:/var/log# history | grep ping
 10 ping 192.168.1.254
 11 ping -c 1 192.168.1.254
 16 history | grep ping
root@kali:/var/log# ls
alternatives.log  daemon.log      gdm3            mysql           speech-dispatcher  user.log          vmware-vmtoolsd.log
apache2          debug          inetsim         nginx           sslsplit          vmware-network.1.log  vmware-vmtoolsd.log
apt              dpkg.log       installer       ntpstats       stunnel4          vmware-network.2.log  wtmp
auth.log         dradis         kern.log        openvpn        syslog            vmware-network.3.log  Xorg.1.log
bootstrap.log    exim4          lastlog         postgresql     sysstat           vmware-network.log    Xorg.1.log.old
btmptmp          faillog        macchanger.log  private        tallylog          vmware-vmtoolsd.1.log
chkrootkit       fontconfig.log  messages       samba           unattended-upgrades  vmware-vmtoolsd.2.log

root@kali:/var/log# cd /root/Downloads/
root@kali:~/Downloads# cd ~/Downloads/
root@kali:~/Downloads# ls
root@kali:~/Downloads#

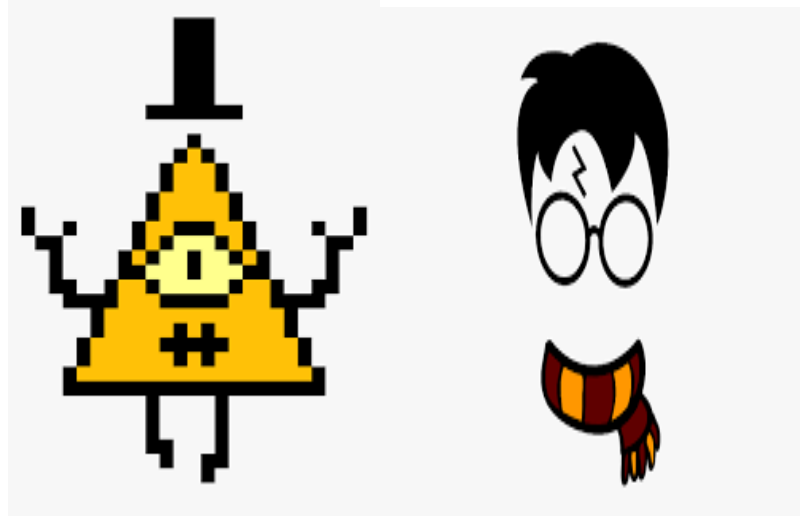
```

5. Harry Potter Cipher Game

I designed an encryption game in Java on Blue J that uses a given key to decrypt the given ciphertext.

Given here, is a link to the same.

<https://youtu.be/p0Gw5qqvpyk>



6. Conclusion

All in all, the topics of cybersecurity and ethical hacking have immense application of programming and networking. A strong hold on networking is essential along with good coding skills. This project explores all the fundamentals of both topics in the hope that it will inspire readers to further delve into it. The world of security still has a number of shortcomings and flaws and a massive scope for discovery. Mastering all required skills will definitely be a career accelerator for those interested.

7. Bibiliography

Websites:

<https://searchsecurity.techtarget.com/>
<https://www.britannica.com/tooic/cybercrime>
<https://www.youtube.com/>
<https://www.cloudwards.net/cybercrime/>
<https://www.geeksforgeeks.org/>
<https://economictimes.indiatimes.com/>
[https://cryptography.fandom.com/wiki/Confusion and diffusion](https://cryptography.fandom.com/wiki/Confusion_and_diffusion)
<https://www.webroot.com/gb/en/resources/tips-articles/computer-security-threats>
<https://www.itpro.co.uk/security/34616/the-top-ten-password-cracking-techniques-used-by-hackers>
<https://howsecureismypassword.net/>
<https://askleo.com/>
<https://www.erg.abdn.ac.uk/users/gorry/course/inet-pages/arp.html>
<https://searchnetworking.techtarget.com/definition/Address-Resolution-Protocol-ARP>
<https://www.lifewire.com/definition-of-sniffer-81799>
<https://www.greycampus.com/blog/information-security/what-is-a-sniffing-attack-and-how-can-you-defend-it>
<https://www.techopedia.com/definition/26186/wireless-network>
<https://www.webopedia.com/TERM/W/WEP.html>

<https://www.networkworld.com/article/3239677/the-osi-model-explained-how-to-understand-and-remember-the-7-layer-network-model.html>
<https://smallbusiness.chron.com/>
<http://www.opus1.com/www/whitepapers/whatswrongwithwep.pdf>
<https://whatis.techtarget.com/definition/Web-server>
<https://www.redteamsecure.com/services>

Text References:

Cryptography and Network Security Principles and Practices, Third Edition.
Author: William Stallings. Publisher: Prentice Hall. 2003.