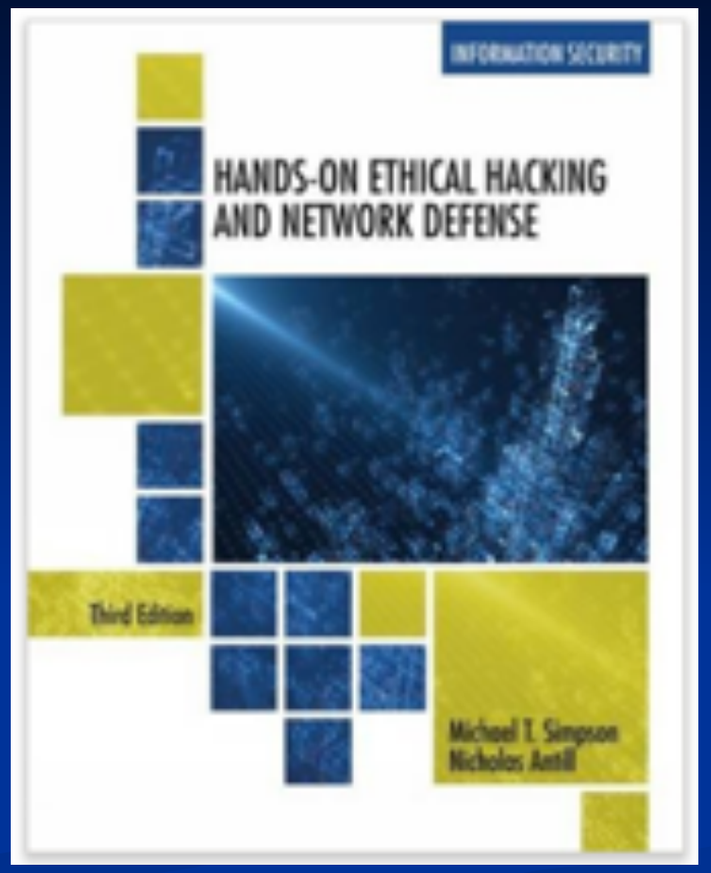
THOMSON

COURSE TECHNOLOGY

Hands-On Ethical Hacking and Network Defense



Chapter 2
TCP/IP Concepts Review

Last modified 1-11-17

Objectives

- Describe the TCP/IP protocol stack
- Explain the basic concepts of IP addressing
- Explain the binary, octal, and hexadecimal numbering system

Overview of TCP/IP

- Protocol
  - Common language used by computers for speaking
- Transmission Control Protocol/Internet Protocol (TCP/IP)
  - Most widely used protocol
- TCP/IP stack
  - Contains four different layers
    - Network
    - Internet
    - Transport
    - Application

Application layer

This layer includes network services and client software.

Transport layer
TCP/UDP services

This layer is responsible for getting data packets to and from the application layer by using port numbers. TCP also verifies packet delivery by using acknowledgments.

Internet layer

This layer uses IP addresses to route packets to their appropriate destination network.

Network layer

This layer represents the physical network pathway and the network interface card.

Figure 2-1 The TCP/IP protocol stack

The Application Layer

- Front end to the lower-layer protocols
- What you can see and touch – closest to the user at the keyboard
- HTTP, FTP, SMTP, SNMP, SSH, IRC and TELNET all operate in the Application Layer

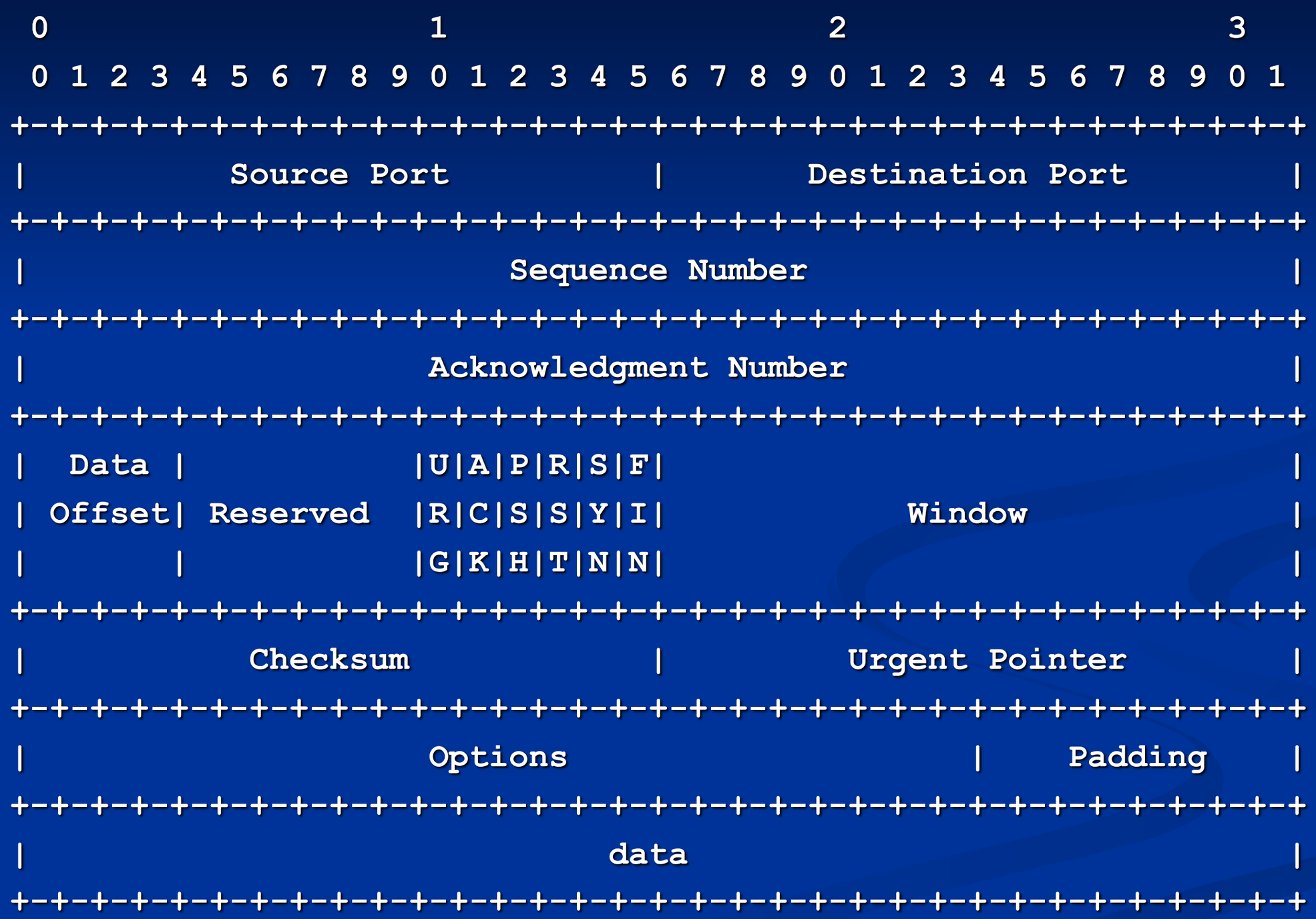
Table 2-1 Application layer programs

Application	Description
Hypertext Transfer Protocol (HTTP)	The primary protocol used to communicate over the World Wide Web (see RFC-2616 at *www.ietf.org* for details)
File Transfer Protocol (FTP)	Allows different operating systems to transfer files between one another
Simple Mail Transfer Protocol (SMTP)	The main protocol for transmitting e-mail messages across the Internet
Simple Network Management Protocol (SNMP)	Primarily used to monitor devices on a network, such as remotely monitoring a router's state
Secure Shell (SSH)	Enables a remote user to log on to a server and issue commands
Internet Relay Chat (IRC)	Enables multiple users to communicate over the Internet in discussion forums
Telnet	Enables users to remotely log on to a server

The Transport Layer

- Encapsulates data into segments
- Segments can use TCP or UDP to reach a destination host
  - TCP is a connection-oriented protocol
- TCP three-way handshake
  - Computer A sends a SYN packet
  - Computer B replies with a SYN-ACK packet
  - Computer A replies with an ACK packet

TCP Header Format



TCP Segment Headers

- Critical components:
  - TCP flags
  - Initial Sequence Number (ISN)
  - Source and destination port
- Abused by hackers finding vulnerabilities

TCP Flags

- Each flag occupies one bit
- Can be set to 0 (off) or 1 (on)
- Six flags
  - SYN: synchronize flag
  - ACK: acknowledge flag
  - PSH: push flag
  - URG: urgent flag
  - RST: reset flag
  - FIN: finish flag

Initial Sequence Number (ISN)

- 32-bit number
- Tracks packets received
- Enables reassembly of large packets
- Sent on steps 1 and 2 of the TCP three-way handshake
  - By guessing ISN values, a hacker can hijack a TCP session, gaining access to a server without logging in

TCP Ports

- Port
  - Logical, not physical, component of a TCP connection
  - Identifies the service that is running
  - Example: HTTP uses port 80
  - A 16-bit number – 65,536 ports
  - Each TCP packet has a source and destination port

Blocking Ports

- Helps you stop or disable services that are not needed
  - Open ports are an invitation for an attack
- You can’t block all the ports
  - That would stop all networking
  - At a minimum, ports 25 and 80 are usually open on a server, so it can send out Email and Web pages

TCP Ports (continued)

- Only the first 1023 ports are considered well-known
- List of well-known ports
  - Available at the Internet Assigned Numbers Authority (IANA) Web site (www.iana.org)
- Ports 20 and 21
  - File Transfer Protocol (FTP)
  - Use for sharing files over the Internet
  - Requires a logon name and password
  - More secure than Trivial File Transfer Protocol (TFTP)

Figure 2-2 Connecting to an FTP site

TCP Ports (continued)

- Port 25
  - Simple Mail Transfer Protocol (SMTP)
  - E-mail servers listen on this port
- Port 53
  - Domain Name Service (DNS)
  - Helps users connect to Web sites using URLs instead of IP addresses

TCP Ports (continued)

- Port 69
  - Trivial File Transfer Protocol
  - Used for transferring router configurations
  - Had the "Sorcer's Apprentice Syndrome" Denial-of-Service vulnerability (link Ch2i)
  - (image from luharu.com)

TCP Ports (continued)

- Port 80
  - Hypertext Transfer Protocol (HTTP)
  - Used when connecting to a Web server
- Port 110
  - Post Office Protocol 3 (POP3)
  - Used for retrieving e-mail
- Port 119
  - Network News Transfer Protocol
  - For use with newsgroups

TCP Ports (continued)

- Port 135
  - Remote Procedure Call (RPC)
  - Critical for the operation of Microsoft Exchange Server and Active Directory
- Port 139
  - NetBIOS
  - Used by Microsoft's NetBIOS Session Service
  - File and printer sharing

TCP Ports (continued)

- Port 143
  - Internet Message Access Protocol 4 (IMAP4)
  - Used for retrieving e-mail
  - More features than POP3

Demonstration

- Telnet to hills.ccsf.edu and netstat to see the connections
  - Port 23 (usual Telnet)
  - Port 25 blocked off campus, but 110 connects
  - Port 21 works, but needs a username and password

Command Prompt

```
E:\Documents and Settings\Sam>telnet hills.ccsf.edu 110
```

Command Prompt

```
E:\Documents and Settings\Sam>netstat -n

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:1047         127.0.0.1:1048         ESTABLISHED
  TCP    127.0.0.1:1048         127.0.0.1:1047         ESTABLISHED
  TCP    192.168.2.14:1129      72.5.124.55:80         CLOSE_WAIT
  TCP    192.168.2.14:1130      208.59.201.18:80       CLOSE_WAIT
  TCP    192.168.2.14:1175      147.144.1.2:110        ESTABLISHED
```

Demonstration

- Wireshark Packet Sniffer
  - TCP Handshake: SYN, SYN/ACK, ACK
  - TCP Ports
  - TCP Status Flags

o	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.2.14	82.165.134.55	TCP	1157 > http [SYN] Seq=0 Len=0 MSS=1
2	0.100187	82.165.134.55	192.168.2.14	TCP	http > 1157 [SYN, ACK] Seq=0 Ack=1
3	0.100281	192.168.2.14	82.165.134.55	TCP	1157 > http [ACK] Seq=1 Ack=1 Win=1
4	0.100656	192.168.2.14	82.165.134.55	HTTP	GET /235/s214.html HTTP/1.1
5	0.214045	82.165.134.55	192.168.2.14	TCP	http > 1157 [ACK] Seq=1 Ack=701 Win
6	0.218748	82.165.134.55	192.168.2.14	TCP	[TCP segment of a reassembled PDU]
7	0.220002	82.165.134.55	192.168.2.14	TCP	[TCP segment of a reassembled PDU]

```
⊞ Frame 1 (62 bytes on wire, 62 bytes captured)
⊞ Ethernet II, Src: AcctonTe_0e:5c:8a (00:10:b5:0e:5c:8a), Dst: BelkinCo_02:ed:7b (00:3
⊞ Internet Protocol, Src: 192.168.2.14 (192.168.2.14), Dst: 82.165.134.55 (82.165.134.5
⊟ Transmission Control Protocol, Src Port: 1157 (1157), Dst Port: http (80), Seq: 0, Le
    Source port: 1157 (1157)
    Destination port: http (80)
    Sequence number: 0    (relative sequence number)
    Header length: 28 bytes
  ⊟ Flags: 0x02 (SYN)
      0... .... = Congestion Window Reduced (CWR): Not set
      .0.. .... = ECN-Echo: Not set
      ..0. .... = Urgent: Not set
      ...0 .... = Acknowledgment: Not set
      .... 0... = Push: Not set
      .... .0.. = Reset: Not set
      .... ..1. = Syn: Set
      .... ...0 = Fin: Not set
    Window size: 16384
    Checksum: 0x6033 [correct]
  ⊞ Options: (8 bytes)
```

User Datagram Protocol (UDP)

- Fast but unreliable protocol
- Operates on transport layer
- Does not verify that the receiver is listening
- Higher layers of the TCP/IP stack handle reliability problems
- Connectionless protocol

The Internet Layer

- Responsible for routing packets to their destination address
- Uses a logical address, called an IP address
- IP addressing
- Packet delivery is connectionless

Internet Control Message Protocol (ICMP)

- Operates in the Internet layer of the TCP/IP stack
- Used to send messages related to network operations
- Helps in troubleshooting a network
- Some commands include
  - Ping
  - Traceroute

ICMP Type Codes

Table 2-2 ICMP type codes

ICMP Type Code	Description
0	Echo Reply
3	Destination Unreachable
4	Source Quench
5	Redirect
6	Alternate Host Address
8	Echo
9	Router Advertisement
10	Router Solicitation

Wireshark Capture of a PING

No.	Time	Source	Destination	Protocol	Info
1	0.00	192.168.2.14	192.168.2.30	ICMP	Echo (ping) request
2	0.00	192.168.2.30	192.168.2.14	ICMP	Echo (ping) reply

```
⊞ Frame 1 (74 bytes on wire, 74 bytes captured)
⊞ Ethernet II, Src: AcctonTe_0e:5c:8a (00:10:b5:0e:5c:8a), Dst: Trigem
⊞ Internet Protocol, Src: 192.168.2.14 (192.168.2.14), Dst: 192.168.2.
⊟ Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x405c [correct]
    Identifier: 0x0400
    Sequence number: 0x0900
    Data (32 bytes)
```

Warriors of the Net

- Network+ Movie
- Warriorsofthe.net (link Ch 2d)

IP Addressing

- Consists of four bytes, like 147.144.20.1
- Two components
  - Network address
  - Host address
    - Neither portion may be all 1s or all 0s
- Classes
  - Class A
  - Class B
  - Class C

Table 2-3 TCP/IP address classes

Address Class	Range	Address Bytes	Number of Networks	Host Bytes	Number of Hosts
Class A	1–127	1	127	3	16,777,214
Class B	128–191	2	16,128	2	65,534
Class C	192–223	3	2,097,152	1	254

IP Addressing (continued)

- Class A
  - First byte is reserved for network address
  - Last three bytes are for host address
  - Supports more than 16 million host computers
  - Limited number of Class A networks
  - Reserved for large corporations and governments (see link Ch 2b)
  - Format: *network.node.node.node*

IP Addressing (continued)

- Class B
  - First two bytes are reserved for network address
  - Last two bytes are for host address
  - Supports more than 65,000 host computers
  - Assigned to large corporations and Internet Service Providers (ISPs)
  - Format: *network.network.node.node*
    - CCSF has 147.144.0.0 – 147.144.255.255

IP Addressing (continued)

- Class C
  - First three bytes are reserved for network address
  - Last byte is for host address
  - Supports up to 254 host computers
  - Usually available for small business and home networks
  - Format: *network.network.network.node*

IP Addressing (continued)

- Subnetting
  - Each network can be assigned a subnet mask
  - Helps identify the network address bits from the host address bits
- Class A uses a subnet mask of 255.0.0.0
  - Also called /8
- Class B uses a subnet mask of 255.255.0.0
  - Also called /16
- Class C uses a subnet mask of 255.255.255.0
  - Also called /24

Planning IP Address Assignments

- Each network segment must have a unique network address
- Address cannot contain all 0s or all 1s
- To access computers on other networks
  - Each computer needs IP address of **gateway**

Planning IP Address Assignments

- TCP/IP uses subnet mask to determine if the destination computer is on the same network or a different network
  - If destination is on a different network, it relays packet to gateway
  - Gateway forwards packet to its next destination (routing)
  - Packet eventually reaches destination

IPv6

- Modern operating systems like Windows 7 use IPv6 in addition to IPv4
- IPv6 addresses are much longer: 128 bits instead of the 32 bits used by IPv4

```
Ethernet adapter Local Area Connection 2:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:c08:3700:ffff::1:955b
   Link-local IPv6 Address . . . . . : fe80::8c65:684e:a10e:c9f%17
   Autoconfiguration IPv4 Address. . : 169.254.12.159
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . : ::
```

Binary

Binary Games for CNIT 123

Play each game till you have 10 correct. Then email the image showing 10 correct to cnit.123@gmail.com to get 5 points extra credit.

1: Nybbles

Lesson (pdf) (ppt)
Game 1: Nybbles (5 pts.)

2: Bytes

Lesson (pdf) (ppt)
Abigail Bornstein's Video Lessons: Part 1 Part 2
Game 2a: Bytes (5 pts.) Game 2b: Bytes (5 pts.)

3: Hexadecimal

Lesson (pdf) (ppt)
Game 3a: Hexadecimal (5 pts.)

Binary, Hexadecimal, and Base64

- Binary: uses only 0 and 1
  - Eight bits per byte
- Hexadecimal: uses 0-9 and a-f
  - 4 bits per character
  - Two characters per byte
- Base64
  - 6 bits per character
  - 4 characters for 3 bytes

Base 64 Encoding

- Used to evade anti-spam tools, and to obscure passwords
- Encodes six bits at a time (0 – 63) with a single ASCII character
  - A - Z: 0 – 25
  - a – z: 26 – 51
  - 1 – 9: 52 – 61
  - + and - 62 and 63
    - See links Ch 3a, 3b

Base64 Example

Input String	O	R	A	C	L	E	.	.
Binary Representation	01001111_2	01010010_2	01000001_2	01000011_2	01001100_2	01000101_2	.	.
After regrouping into 6-bit groups. *[Binary and decimal equivalents are shown.]*	010011_2 $[19_{10}]$	110101_2 $[53_{10}]$	001001_2 $[9_{10}]$	000001_2 $[1_{10}]$	010000_2 $[16_{10}]$	110100_2 $[52_{10}]$	110001_2 $[49_{10}]$	$000101\backslash_2$ $[5_{10}]$
After mapping the above eight 8-bit bytes using Table 1	T	1	J	B	Q	0	x	F

Base64 encoded string : **T1JBQ0xF**

- ORACLE -> T1JBQ0xF
  - Link Ch 3r