Lab 2: Services, Logging and Intrusions

A Challenge

Our challenge is to test services for their operation and to log network event for **MyBank Incorp**, where each of you will be allocated a network and hosts to configure and get on-line (Figure 1). For this you will be allocated your own network (GROUP001, GROUP002, and so on) which you can access from the DFET Cloud infrastructure. Table 1 outlines your challenges and how you might achieve them. You have a pfSense firewall, a Linux host, and a Windows host to achieve your objectives. **The WAN port of the firewall should always be set to DHCP**.

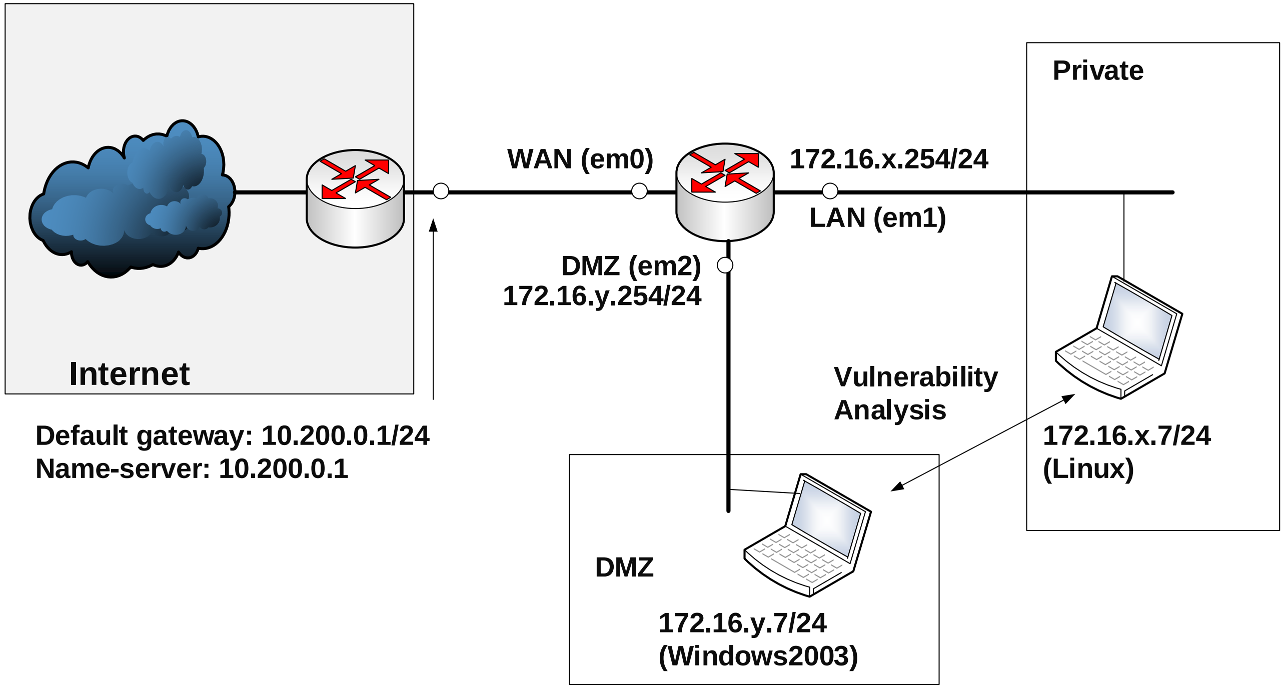


Figure 1: My Bank architecture

Table 1: Your challenges

Challenge	Description	How will I do this?	Completed
1	You should be able to setup your network with the required setup. Test: Ping all the ports and be able to communicate as required.		
2	Examine the Log files for Web access on Linux and Windows **Test:** Examine the log files	Locate the log file locations.	
3	Examine various application protocols for their traces, including remote access and FTP. **Test:** Examine network traces	Run TELNET and Wireshark	
4	Discover host information **Test:** Use WMIC to discover details from Windows hosts	Run WMIC	
5	Enable Syslog. **Test:** Exercise the firewall and view the Syslog messages	Enable remote Syslog on the firewall.	
6	Use Snort to detect complex rules. **Test:** Probe network to trigger events.	Run Snort and test.	

B Setting up the network

In this lab we will connect multiple firewalls to the main gateway, and be able to complete the challenges in Table 1. You will be given two things:

Network Number:	Your networks will be: 172.16.*x*.0/24 172.16.*y*.0/24
Demo:	https://youtu.be/75zEAMV5v0s https://youtu.be/cFYTHXZwGPQ

You should have been allocated in a group. In this case we will use **ALLOCATIONB** addressing:

http://asecuritysite.com/csn11128/nets

User logins: Ubuntu (User: napier, Password: napier123), Windows: (User: Administrator, Password: napier), Vyatta (User: vyatta, Password: vyatta), pfsense (User: admin, Password: pfsense), Metasploitable (User: user, Password: user), Kali (User: root, Password: toor).

C Network Setup

Setup your network, and allow all IP traffic between the DMZ and LAN, and vice-versa, and for the host in the DMZ to connect to Google.com. Next we will do a system audit of our network:

- You can determine your MAC address on Ubuntu with `ifconfig`, and on Windows with `ipconfig /all`.
- You can determine the MAC address of the gateways by ping'ing them and looking at your ARP cache (`arp -a`).

LAN GATEWAY IP address/subnet mask:	
LAN GATEWAY MAC address:	

LAN UBUNTU IP address/subnet mask:	
LAN UBUNTU MAC address:	

DMZ GATEWAY IP address/subnet mask:	
DMZ GATEWAY MAC address:	
DMZ WINDOWS IP address:	
DMZ WINDOWS MAC address:	

WAN GATEWAY IP address/subnet mask:	
WAN GATEWAY MAC address:	

What could you observe from the MAC address, related to the manufacturer:

DWeb Services (Linux)

We will first be testing the UBUNTU Web server, and examine the logs. **For all the following run Wireshark on WINDOWS.**

From → To	**Command**	**Observation**
LAN	To list the running network services in the UBUNTU server, use this (-l listening, -t TCP, -u UDP): `netstat –ltu`	List some of the services (and their port numbers) which are running on the server:

DMZ to LAN	From WINDOWS, using a browser, connect to the Web Server running on UBUNTU using: `http://172.16.x.7`	Do it connect? [Yes] [No]
DMZ	On your Wireshark trace, find the initial connection to the Web server (using the filter of `tcp.flags.syn==1`).	Can you determine the following: MAC Address of the Source: MAC Address of the Destination: Is this the MAC address of the UBUNTU Web server: Source IP of the TCP SYN: Destination IP of the TCP SYN: Source TCP port of the TCP SYN: Destination TCP port of the TCP SYN:
DMZ	On your Wireshark trace, find the initial connection to the Web server (using the filter of `tcp.flags.syn==1`) and then **right click** on it and **follow the stream**.	Can you see the HTML code of the response? Pick of one of the words in the rendered page: What is the significance of the blue and red text in the stream?
DMZ	On your Wireshark trace, run the following filters: `http.request.method=="GET"`	What is the function of these filters:

	`http.response.code==200`	

DMZ to LAN	Using Telnet from WINDOWS, access the Web server on UBUNTU using:
	`telnet 172.16.x.7 80`
	and then:
	`OPTIONS / HTTP/1.1`
		Determine the Web server type:

LAN	On UBUNTU, navigate to the **/var/www** folder, and edit the **index.html** file with the following (you can use nano as an editor):
	`<html><body>`
	`<h1>My Home Page (Ubuntu)</h1>`
	`<p>This is my home page and the next page is`
	`<a href=”page01.html”>here</a></p>`
	`</body></html>`
		What are the names of the files in this directory, and what type of files are they:
		Reload your browser from WINDOWS. Can you access the newly created page?

LAN	On UBUNTU, go to **/var/log/apache2** and list the contents of the folder (ls).	Outline the contents of the folder?
LAN	On UBUNTU, examine the contents of the **access.log** file.	What information can you determine from one of the accesses: Client IP: User agent: HTTP Method: HTTP Status:

		TCP Source Port: TCP Destination Port:
DMZ to LAN	From WINDOWS, now access a page which does not exist on the UBUNTU Web server, such as: `http://172.16.x.7/nopage.html`	Examine the log. What is the HTTP Status response code: Can you determine the row numbers of the data packet in your Wireshark trace is the HTTP request (GET) and the HTTP response (404):

DMZ to LAN	Now create a page with the following:
	`<form name="input" action="demo_form_action.asp" method="post">`
	`Username: <input type="text" name="user">`
	`<input type="submit" value="Submit">`
	`</form>`
		Access the page from WINDOWS and examine the log on UBUNTU. What can you observe from the log:

E Web Services (Windows)

We will now test the WINDOWS Web server, and examine the logs. **For all the following run Wireshark on WINDOWS.**

From → To	**Command**	**Observation**
DMZ	To list the running network services on the WINDOWS server, use this (-l listening, -t TCP, -u UDP): `netstat -a`	List some of the services (and their port numbers) which are running on the server:

LAN to DMZ	From UBUNTU, using a browser, connect to the Web Server running on WINDOWS using: `http://172.16.y.7`	Do it connect? [Yes] [No]
DMZ	On your Wireshark trace, find the initial connection to the Web server (using the filter of `tcp.flags.syn==1`).	Can you determine the following: MAC Address of the Source: MAC Address of the Destination: Is this the MAC address of the WINDOWS Web server: Source IP of the TCP SYN: Destination IP of the TCP SYN: Source TCP port of the TCP SYN: Destination TCP port of the TCP SYN:
DMZ	On your Wireshark trace, find the initial connection to the Web server (using the filter of `tcp.flags.syn==1`) and then **right click** on it and **follow the stream**.	Can you see the HTML code of the response? Pick of one of the words in the rendered page:
LAN to DMZ	Using Telnet from UBUNTU, access the Web server on WINDOWS using: `telnet 172.16.y.7 80`	Determine the Web server type:

	and then: `OPTIONS / HTTP/1.1`	

DMZ	On WINDOWS, navigate to the **c:\inetpub\wwwroot** folder, and edit the **iisstart.htm** file with the following (you can use Notepad as an editor):
	`<html><body>`
	`<h1>My Home Page (Windows)</h1>`
	`<p>This is my home page and the next page is`
	`<a href=”page01.html”>here</a></p>`
	`</body></html>`
		What are the names of the files in this directory, and what type of files are they:
		Reload your browser from UBUNTU. Can you access the newly created page?

DMZ	On WINDOWS, go to **C:\WINDOWS\system32\LogFiles\W3SVC1**.	What are the contents of the folder? What do the files contain?
DMZ	On WINDOWS, examine the contents of the most recent log.	What information can you determine from one of the accesses: Client IP: User agent: HTTP Method: HTTP Status: TCP Source Port: TCP Destination Port:
LAN to DMZ	Perform an NMAP scan from UBUNTU to WINDOWS using: -sT	Are there any traces in the logs for these scans:

	and -sV	
DMZ to LAN	From WINDOWS, now access a page which does not exist on the UBUNTU Web server, such as: `http://172.16.x.7/nopage.html`	Examine the log. What is the HTTP Status response code: Can you determine the row numbers of the data packet in your Wireshark trace is the HTTP request (GET) and the HTTP response (404):

DMZ to LAN	Now create a page with the following:
	`<form name="input" action="demo_form_action.asp" method="post">`
	`Username: <input type="text" name="user">`
	`<input type="submit" value="Submit">`
	`</form>`
		Access the page from WINDOWS and examine the log on UBUNTU. What can you observe from the log:

DMZ	**ACCESS FROM WAN (Web).** From the knowledge gained in a previous lab (1:1 NAT), expose your WINDOWS Web site to the WAN, and get someone else from another network to access from a Web browser (otherwise to the test network and access it from there).	By examining the log file, can you determine the IP of the host which accessed your Web site:

F Services: Remote Access

We will now test the UBUNTU Telnet server. **For all the following run Wireshark on WINDOWS.**

From → To	Command	Observation
DMZ to LAN	From WINDOWS, using a browser, connect to the Telnet Server running on UBUNTU using: `telnet 172.16.x.7`	What is the default home folder for the Telnet session on the UBUNTU host:
DMZ	On your Wireshark trace, find the initial connection to the Web server (using the filter of `tcp.flags.syn==1`) and then following the stream.	For the connection: Source IP of the TCP SYN: Destination IP of the TCP SYN: Source TCP port of the TCP SYN: Destination TCP port of the TCP SYN: Can you see the username and password that you entered?

And now repeat:

From → To	Command	Observation
LAN to DMZ	From UBUNTU, using a browser, connect to the Telnet Server running on WINDOWS using: `telnet 172.16.y.7`	What is the default home folder for the Telnet session on the WINDOWS host:
DMZ	On your Wireshark trace, find the initial connection to the Web server (using the filter of `tcp.flags.syn==1`) and then following the stream.	For the connection: Source IP of the TCP SYN: Destination IP of the TCP SYN:

		Source TCP port of the TCP SYN: Destination TCP port of the TCP SYN: Can you see the username and password that you entered?
DMZ	**ACCESS FROM WAN (Telnet).** From the knowledge gained in a previous lab (1:1 NAT), expose your WINDOWS Telnet site to the WAN, and get someone else from another network to access from a Web browser (otherwise to the test network and access it from there).	Get them to put a file in the home folder for the Telnet connection, and see if you can find it.

G Services: Remote Desktop

Run Wireshark on your WINDOWS host.

From → To	**Command**	**Observation**
DMZ to LAN	Using the VNC client on WINDOWS, connect to you UBUNTU host, and make sure you can connect.	From your Wireshark trace, determine the following: Transport protocol: [UDP] or [TCP] Source Port: Destination Port:

H Services: FTP

Run Wireshark on your WINDOWS host.

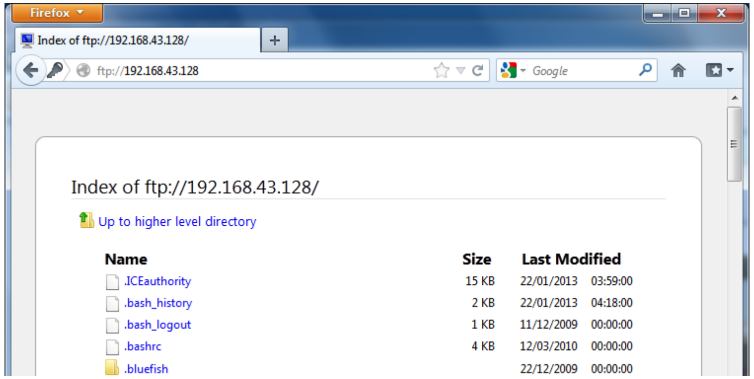
From → To	Command	Observation
LAN	View the contents of **`/etc/inetd.conf`** file.	How is this used to enable services?
DMZ to LAN	From your host, connect to the FTP Server from WINDOWS, via a web browser using: `ftp://172.16.x.7`	Can you connect? [Yes] [No]

DMZ to LAN	Open a command line window from WINDOWS, and connect to the FTP Server using the command:
	`telnet 172.16.x.7 21`
	
	`USER napier`
	`331 Password required for napier.`
	`PASS napier123`
	`230- Linux ubuntu 2.6.31-14-generic #48-Ubuntu SMP Fri Oct 16`
	`     14:04:26 UTC 2009 i686`
	`230-`
	`230- To access official Ubuntu documentation, please visit:`
	`230- http://help.ubuntu.com/`
	`230-`
	`230 User napier logged in.`
	`HELP`
	`214- The following commands are recognized (* =>'s unimplemented).`
	`   USER    PORT    STOR    MSAM*   RNTO    NLST    MKD     CDUP`
	`   PASS    PASV    APPE    MRSQ*   ABOR    SITE    XMKD    XCUP`
	`   ACCT*   TYPE    MLFL*   MRCP*   DELE    SYST    RMD     STOU`
	`   SMNT*   STRU    MAIL*   ALLO    CWD     STAT    XRMD    SIZE`
	`   QUIT    RETR    MSOM*   RNFR    LIST    NOOP    XPWD`
	`PWD`
	`257 "/home/napier" is current directory.`
	`TYPE I`
	`200 Type set to I.`
	`PASV`
		Did the LIST command succeed? [Yes][No]

	`227 Entering Passive Mode (192,168,75,136,146,31)`
	`LIST`	

DMZ to LAN	The PASV FTP command opens up a different port for the data transfer. This is calculated from the last two digits of the Passive Mode response (227 response). It is calculated as, the second last (146) digital multiplied by 256, plus the last digital (31). So, in this case, it would be: Port = 146*256 + 31 = 37397 Next, open up the data transfer channel by creating a new Telnet connection, in a second command line window, such as with the command: `telnet 172.16.y.7 37397` Now try the LIST command again, in the 1st command window.	Did the LIST command succeed? [Yes][No]
DMZ to LAN	Now try a correct login for FTP on UBUNTU, and then an incorrect one.	Go to **/var/log/vsftpd.log** file and examine the log, which information can you determine from the good and the bad login:
DMZ to LAN	Run a Hydra scan on the UBUNTU FTP server. An example of a Hydra scan is (for an IP address of w.x.y.z): `hydra -L user.txt -P pass.txt w.x.y.z ftp` where user.txt is a list of login names and pass.txt a list of passwords.	Did it manage to crack a user name and password?

DMZ to LAN	Re-examine the log. What do you observe:	Observation on log:
DMZ to LAN	Examine the Hydra trace in Wireshark, and implement the following filter: ftp.response.code==530	Which FTP response code are defined in the trace: Which code is used for a successful login, and by tracing the stream, which was a successfully entered username and password:



Index of ftp://192.168.43.128/

Up to higher level directory

Name	Size	Last Modified
.ICEauthority	15 KB	22/01/2013 03:59:00
.bash_history	2 KB	22/01/2013 04:18:00
.bash_logout	1 KB	11/12/2009 00:00:00
.bashrc	4 KB	12/03/2010 00:00:00
.bluefish		22/12/2009 00:00:00

Figure 2: FTP listing

I Syslog

The Windows server has been setup for a Syslog server (if not, download the Kiwisoft Syslog Server). Now we will setup the firewall to send its logs to the Syslog server.

From → To	**Command**	**Observation**
FIRE	From your firewall, go to Status -> System Logs -> Settings Then: Check Enable Remote Logging Remote Syslog Servers 172.16.y.7	Do you receive Syslog messages on the Syslog server on WINDOWS [Yes] [No]
FIRE	Now disable the Allow IPv4 on the LAN interface. Now try and ping the 172.16.x.254 port, and examine your Syslog server.	What message do you get on the Syslog server?

FIRE	Re-enable the Allow IPv4 rule, and ping the gateway port.	Do you get any messages related to it?

J Enumeration – Windows WMIC

Windows Management Instrumentation Command-line (WMIC) allows the use of Windows Management Instrumentation (WMI) from the Windows command line. WMI is a model for accessing management information, which can be used by applications.

From → To	Command	Observation

DMZ	Enumerate your host with the following:
	`wmic.exe CPU list brief`
	`wmic.exe NIC list brief`
	`wmic.exe OS list brief`
	`wmic.exe SHARE list brief`
		What is the MAC address of the windows host?
		Which Shares are found on the host?
		Outline some other details:
		What other options are available in WMIC?

K Snort IDS Detection

Snort is a useful Intrusion Detection Agent, and we often use it to detect content in data packets. The following detects some file formats, and also uses regular expressions to detect things like credit card details and email addresses in network flows.

<table>
<tr><th>From → To</th><th>Command</th><th>Observation</th></tr>
<tr><td><b>DMZ</b></td><td>We now want to detect some content in network packages using Snort. Create the following rules:
alert tcp any any -> any any (content:"GIF89a"; msg:"GIF";sid:10000)
alert tcp any any -> any any (content:"%PDF"; msg:"PDF";sid:10001)
alert tcp any any -> any any (content:"|89 50 4E 47|"; msg:"PNG";sid:10002)
alert tcp any any -> any any (content:"|50 4B 03 04|"; msg:"ZIP";sid:10003)
Start Snort and get it to read your rules. Then access the Internet, and access pages with a GIF file, a PDF file, a PNG graphic and a ZIP file.</td><td>Did your IDS detect the all of the content, and what details did it log on these:</td></tr>
<tr><td><b>DMZ</b></td><td>Create a rule which detects a DoS on your WINDOWS server:
alert tcp any any -> any 80 (msg:"DOS flood denial of service attempt"; flow:to_server; \
detection_filter:track by_dst, count 60, seconds 60; \
sid:25101; rev:1;)
Now scan the WINDOWS server from UBUNTU on port 80 with hping.</td><td>Did it detect it?</td></tr>
<tr><td><b>DMZ</b></td><td>Create a Web page on your UBUNTU server with some credit card details, such as:
Here is my credit card: 5555-5555-5555-5555
Now create a Snort rule to detect credit card details in the data packets:
alert tcp any any <> any any (pcre:"/5\d{3}(\s|-)?\d{4}(\s|-)?\d{4}(\s|-)?\d{4}/"; \
msg:"MasterCard number detected in clear text"; \
content:"number";nocase;sid:9000003;rev:1;)</td><td>Access the Web page, and see if the IDS detects the credit card.</td></tr>
<tr><td><b>DMZ</b></td><td>Create a Web page on your UBUNTU server with some credit card details, such as:</td><td>Access the Web page, and see if the</td></tr>
</table>

	`Here is my email address: fred@home`
	Now create a Snort rule to detect credit card details in the data packets:
	`alert tcp any any <> any 25 (pcre:"/[a-zA-Z0-9._%+-]+@@[a-zA-Z0-9._%+-]/"; \`
	`msg:"Email in message";sid:9000000;rev:1;)`
		IDS detects the email address.

Note you may have to add the following at the start of your Snort file:

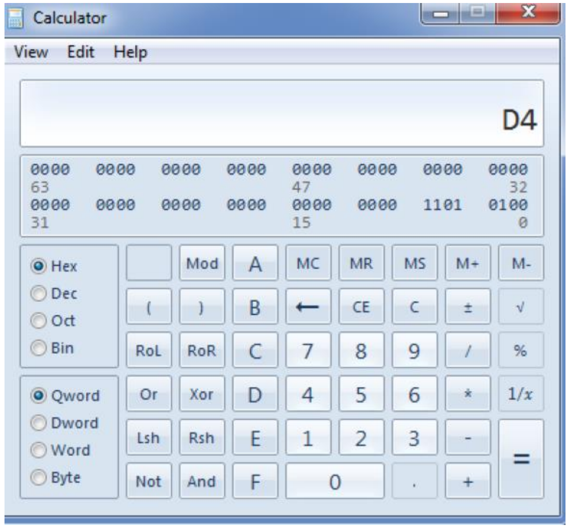
Link: https://dl.dropboxusercontent.com/u/40355863/snort.txt

```
preprocessor stream5_global: track_tcp yes, \
track_udp yes, \
track_icmp no, \
max_tcp 262144, \
max_udp 131072, \
max_active_responses 2, \
min_response_seconds 5
preprocessor stream5_tcp: policy windows, detect_anomalies, require_3whs 180, \
overlap_limit 10, small_segments 3 bytes 150, timeout 180, \
ports client 21 22 23 25 42 53 70 79 109 110 111 113 119 135 136 137 139 143 \
161 445 513 514 587 593 691 1433 1521 1741 2100 3306 6070 6665 6666 6667 6668 6669 \
7000 8181 32770 32771 32772 32773 32774 32775 32776 32777 32778 32779, \
ports both 80 81 82 83 84 85 86 87 88 89 90 110 311 383 443 465 563 591 593 631 636 901 989 992 993 994 995 1220
1414 1830 2301 2381 2809 3037 3057 3128 3443 3702 4343 4848 5250 6080 6988 7907 7000 7001 7144 7145 7510 7802 7777
7779 \
7801 7900 7901 7902 7903 7904 7905 7906 7908 7909 7910 7911 7912 7913 7914 7915 7916 \
7917 7918 7919 7920 8000 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180 8222 8243 8280 8300 8500 8800 8888 8899
9000 9060 9080 9090 9091 9443 9999 10000 11371 34443 34444 41080 50000 50002 55555
preprocessor stream5_udp: timeout 180
```

L Link Obfuscation

One way to confuse the user is with a hexadecimal address. For example www.bbc.co.uk is 212.58.246.95, so we can convert each of these digits to D4.3A.F6.5F.

From → To	Command	Observation
DMZ to WAN	A malicious link in a page has the following format (Figure 3 for conversion): http://0x812a2601	Where does this link go: Which is an obfuscated link for cisco.com: Which is an obfuscated link for www.napier.ac.uk:
DMZ to WAN	A certain site is blocked for its domain name and associated IP address, but an intruder creates on in the form: http://0110.0243.04.0241/	Where does this link go: Which is an obfuscated link in a similar form for apple.com: Which is an obfuscated link in a similar form for bbc.co.uk:



```
D4
```

```
0000   0000   0000   0000   0000   0000   0000   0000
63                          47                       32
0000   0000   0000   0000   0000   0000   1101   0100
31                          15                        0
```

● Hex
○ Dec
○ Oct
○ Bin

● Qword
○ Dword
○ Word
○ Byte

Figure 3: Hex to decimal