NETWORK ADAPTER

EXPOSED IP: 143.198.217.245

NAME	IP
DIRTY DMZ	10.10.111.0/24
DIRTY LAN	192.168.111.0/24
DIRTY SERVER	172.16.111.0/24
MAIN 208	192.168.111.0/24

BOX IP ADDRESS

NAME	IP	LOCAL CRED	DOMAIN CRED	NOTE
AD	172.16.111.60	Administrator:admin@123987 adminRDP:Testing12345	SQLService:MYpassword123#	SQLService - for kerberoast attack
WIN-IIS	192.168.8.130/10.10.111.71	Administrator:Testing12345	WebServer:Testing1234567	local - Administrator:Testing12345
WIN-RDP	10.10.111.70	Administrator:P@ssw0rd1234 RemoteAdmin:Testing123456	adminRDP:Testing12345	Local administrator: - weak password for bruteforce Local2: RemoteAdmin:Testing123456 - backup local admin D user: adminrdp:Testing12345
U1 - workstation	192.168.111.80	admin_1:No password required	iqbal:Testing12345	uitm-info\iqbal - local admin
U2 - workstation	192.168.111.90	admin_2:No password required	badrul:Testing12345	UITM-INFO\Badrul - local admin
SPLUNK	172.16.111.102:8000 172.16.0.51:8000	splunk:SplunkIntern123	ubuntu: internubuntu!@#	ssh root@172.16.0.51

MySQL Server	
PASS	root

Wordpress Admin	
Email :	Uitm.info000@gmail.com
Password email :	uitm@123
Username (Wordpress) :	admin
Password (Wordpress) :	Admin@WebServer123

DOMAIN USER IN AD
amin : Testing123
abu : Test12345678
Badrul : Testing12345
Iqbal : Testing1234
syahmi : Makan12345
aufa : Testing1234
hazim : Playstore1234
nur : Playstore12
bakar : Aircond1234
fitri : Aircond123
imran : Makan123
fakri : Abu12345678

PRIV	Account
Domain Admin	administrator badrul faisalfs
Enterprise Admin	administrator badrul faisalfs
DNS Admin	iqbal