Colby Heilner

Professor Torres

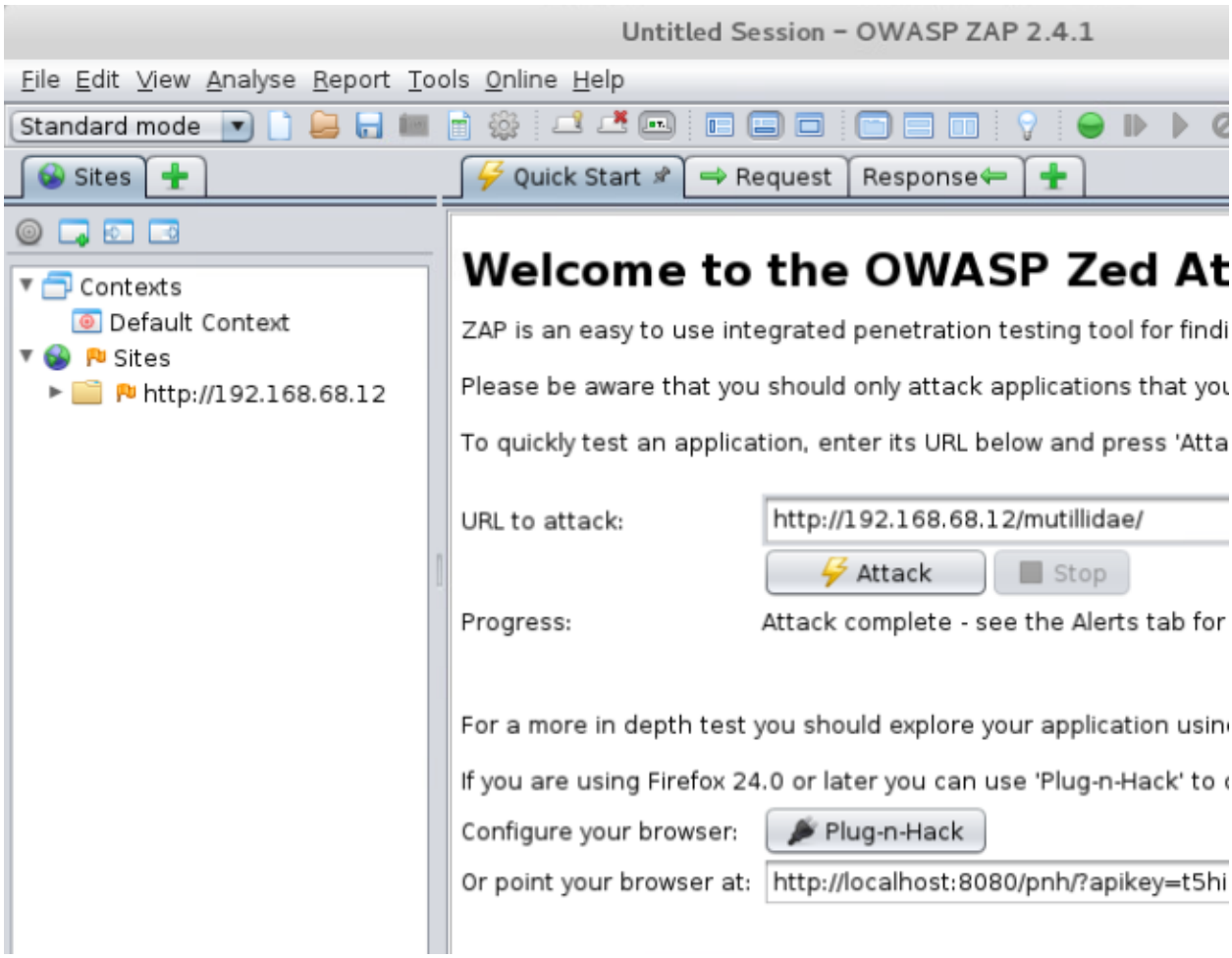
IT 120

Lab 6

Part A: Netlab1 NDG Ethical Hacking Links to an external site.Links to an external site.

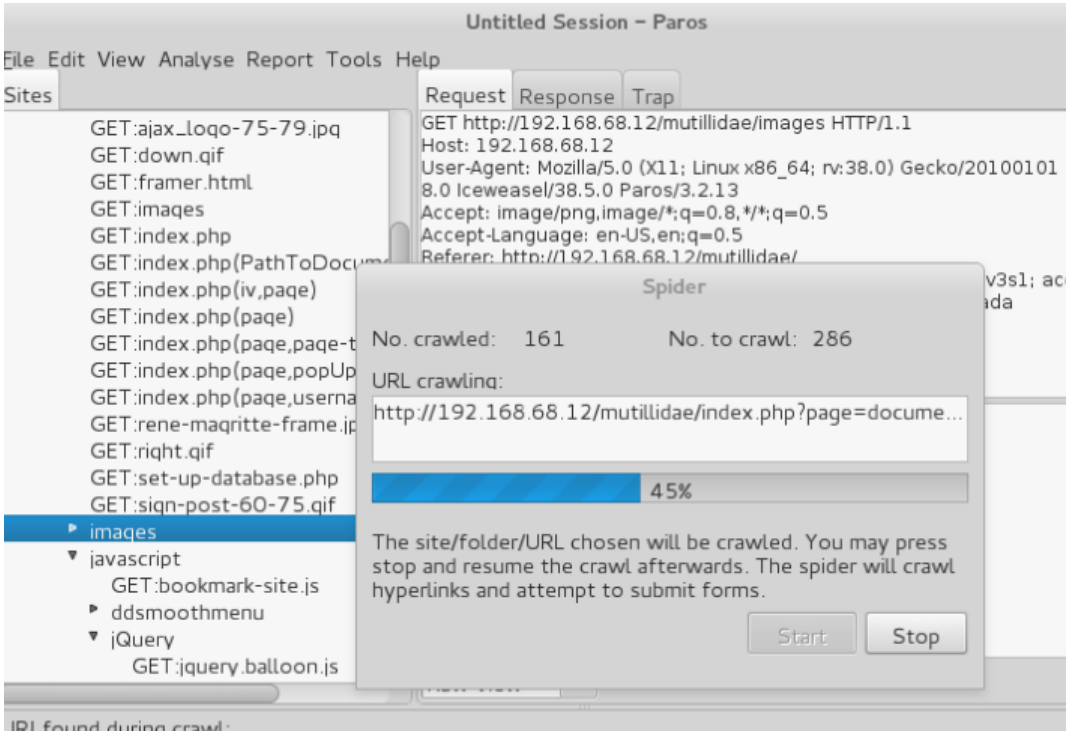
Applications

- OWASP Zap

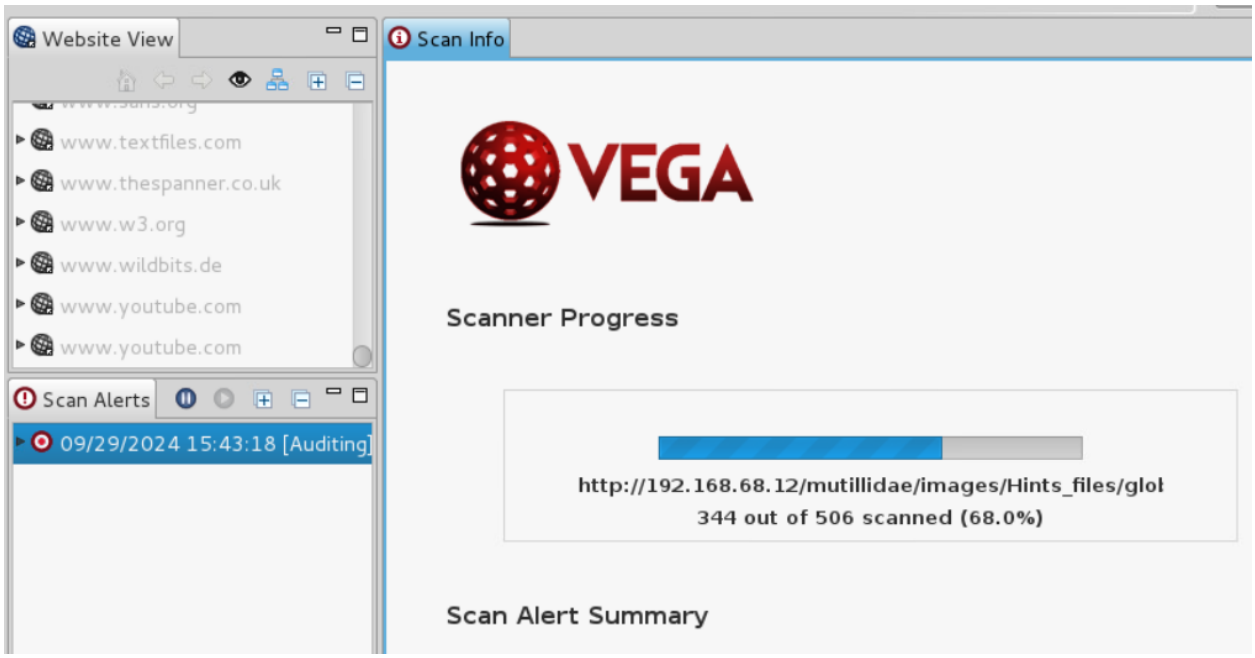


- Nikto

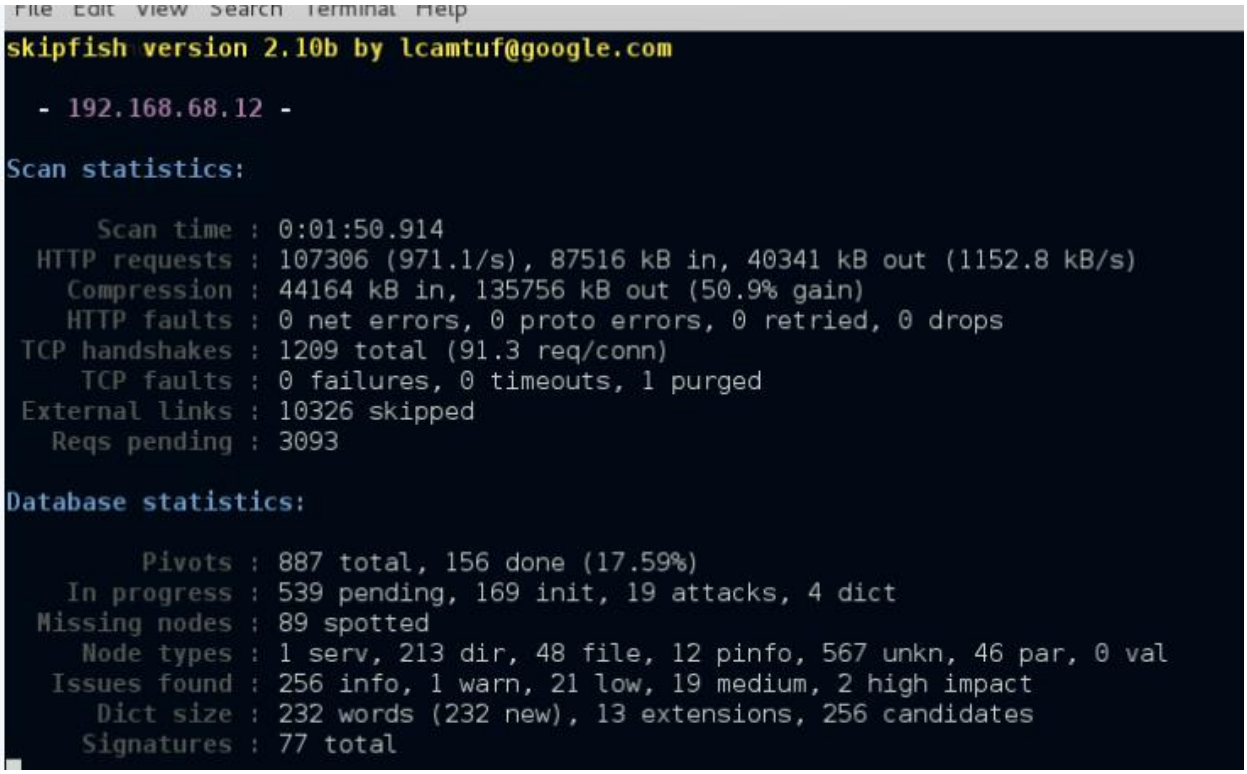
- Paros Proxy



- Vega Scanner

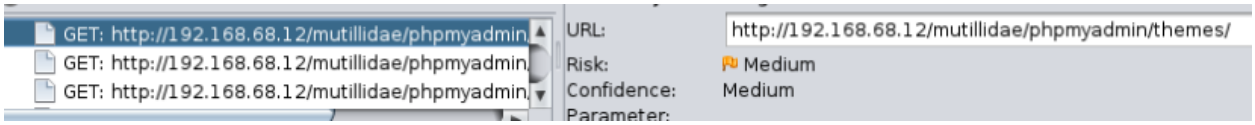


- Skipfish

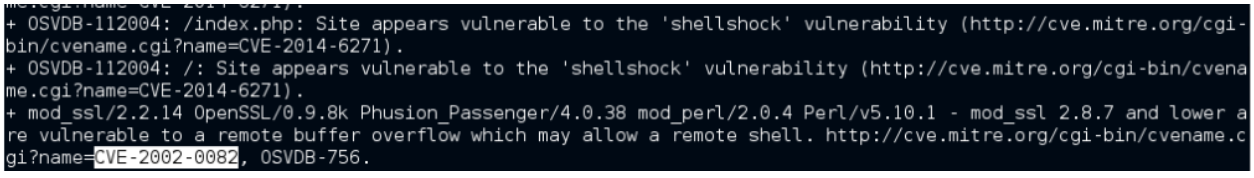


After you scan your applications with the above tools:

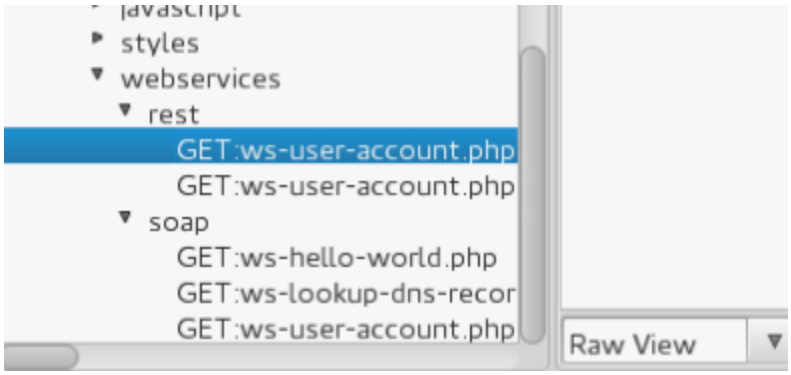
- Discuss your findings.
- What was the most critical vulnerability found by each tool?
  For zap: I found alot of directory throught directory traversal/fuzzing



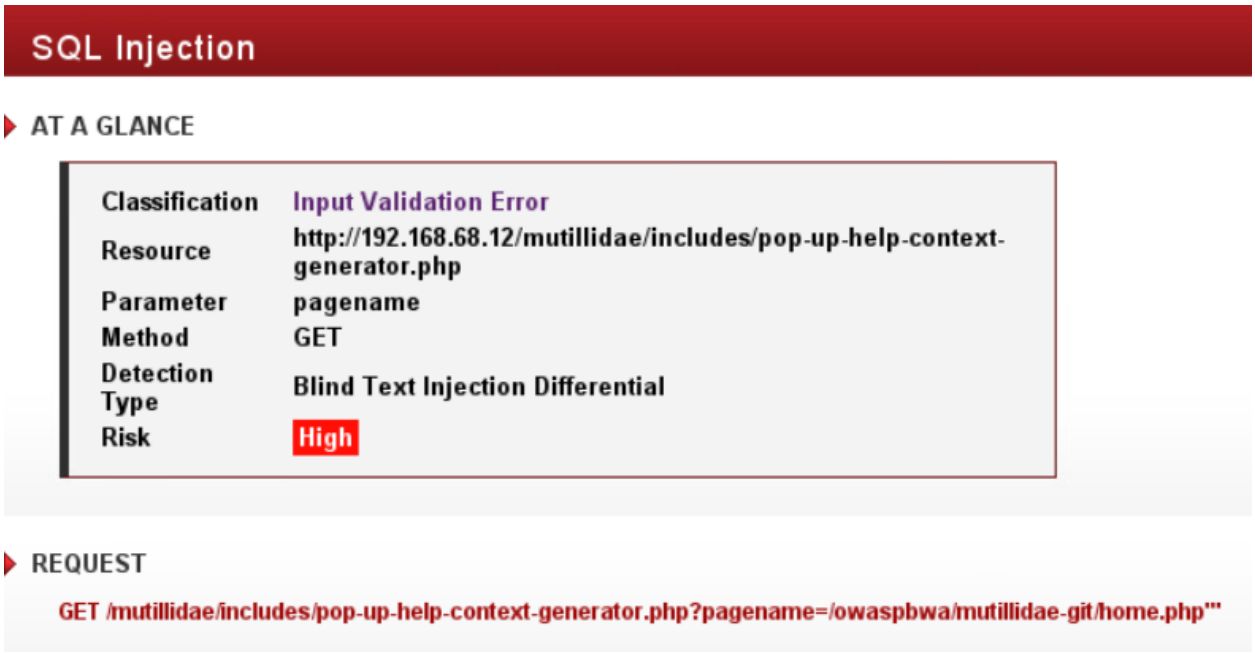
  Nikto:



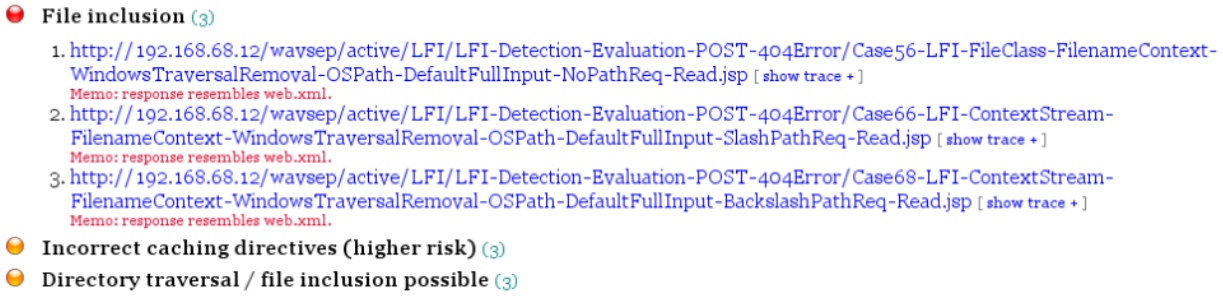
  Paros:



Vega: Sql injections are serious and can be used to get sensitive info out of databases



Skipfish: Weirdly I dont rember seeing these anywhere else before.

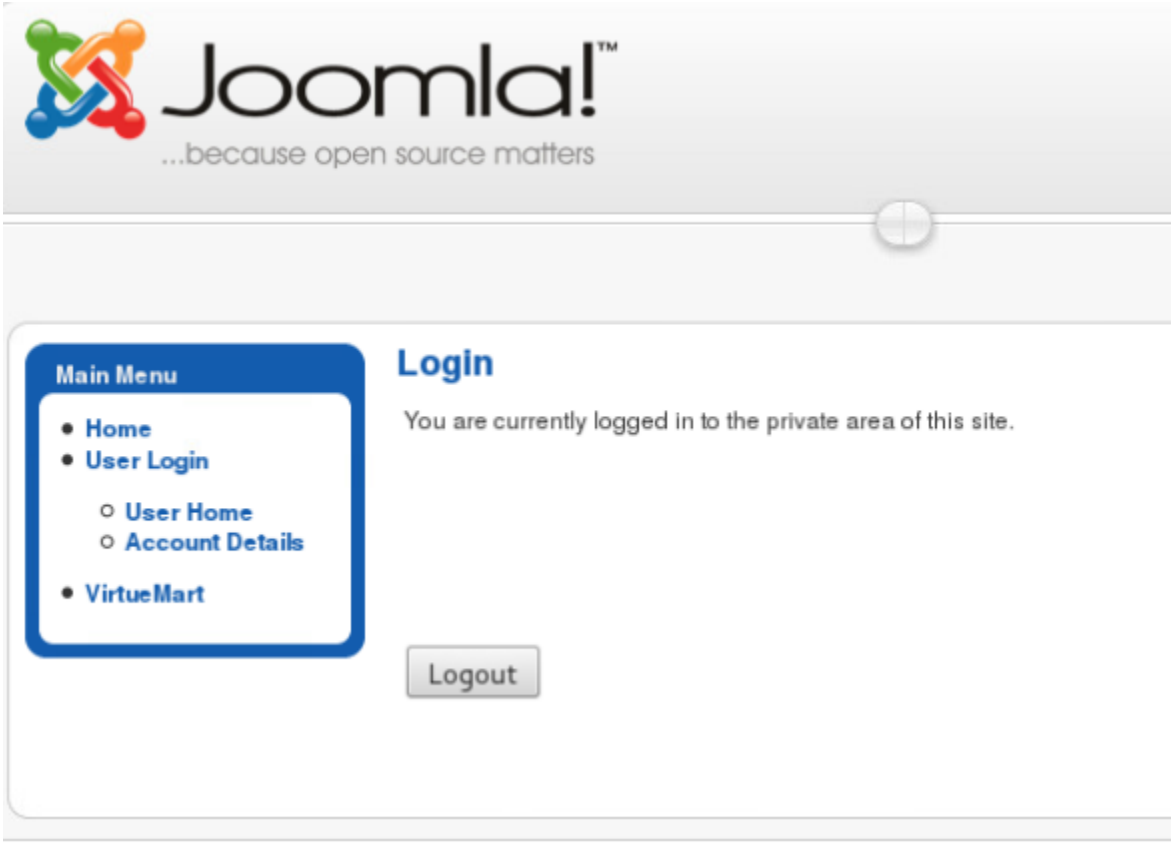


What vulnerability was flagged as being severe or critical in one tool and not in another?

In nikito I saw that cve for remote buffer overflow, but it did not catch it in vega. This shows me that even thought vega gave me alot of good output its always good run multiple things. Or just use **burpsuite** :)

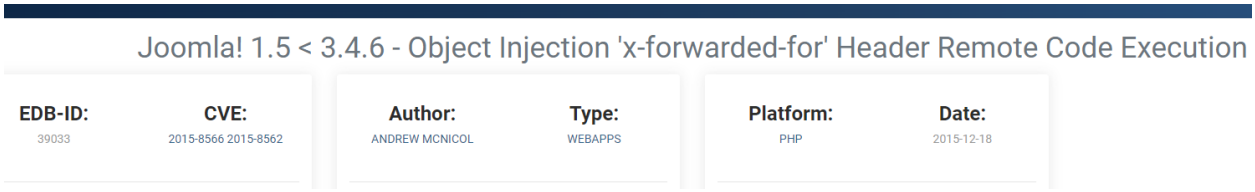
- Which tool gave you the best results
  I would say VEGA, it took the longest but it had alot of results.

- Attempt to locate every website that requires authentication using the above tools.
- Research and attempt the "default credentials" for the websites found.
- What is the name and version of the web application?
  I had alot of trouble with this. Im not sure why but i was unable to identify or access any of the webapp I found.
  So i switched over to bricks and tried scanning it to try my luck elsewhere. It had alot of login pages but im not sure about webapps.
  I ended up finding joomla login and found the defult password of admin admin and logged in



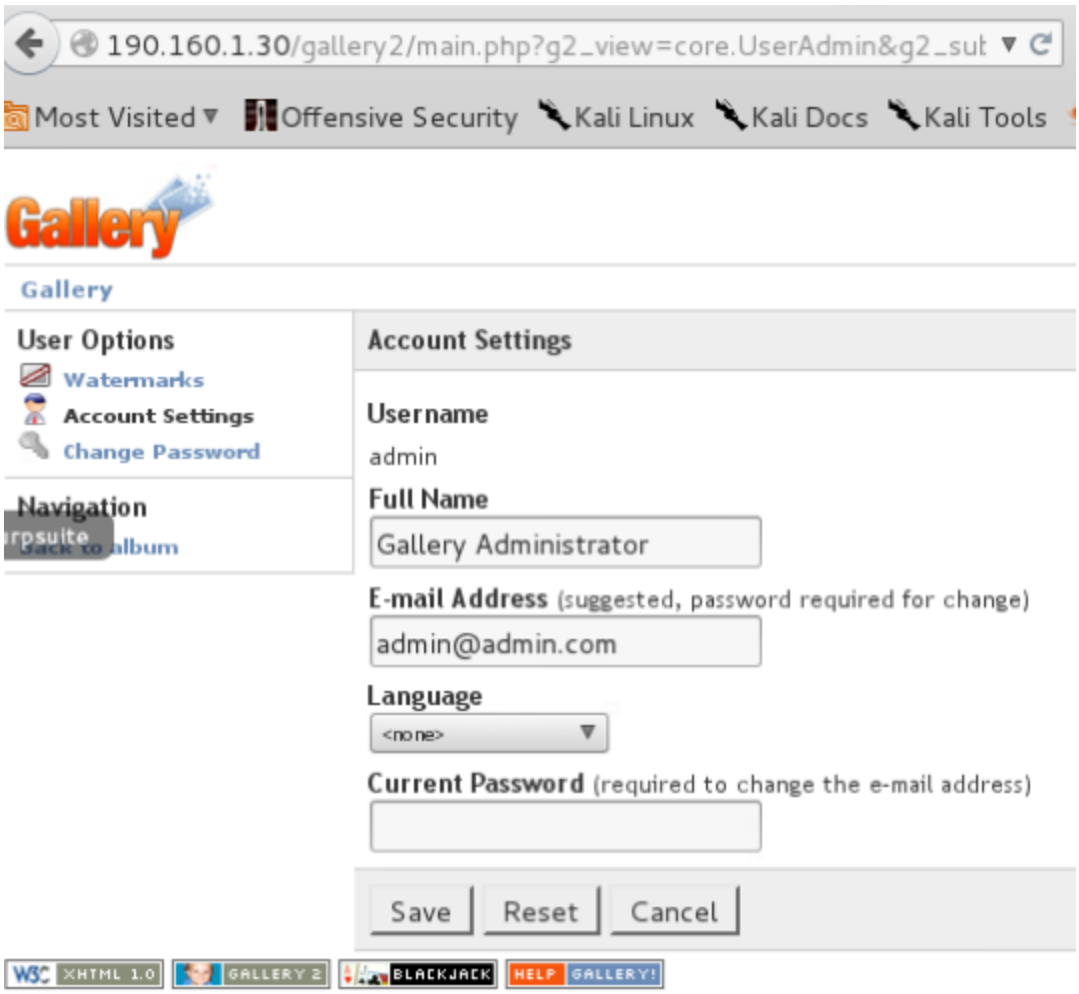
Here is my version!

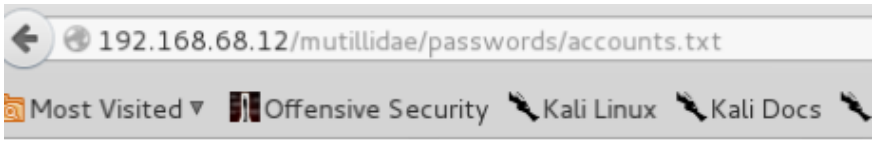
Quick trip to exploit dB will tell me that, this one looks good



Found with dirb buster

I also found this and logged in with admin admin


190.160.1.30/gallery2/main.php?g2_view=core.UserAdmin&g2_sut
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Gallery
Gallery
User Options
Watermarks
Account Settings
Change Password
Navigation
Back to album
Account Settings
Username
admin
Full Name
Gallery Administrator
E-mail Address (suggested, password required for change)
admin@admin.com
Language
<none>
Current Password (required to change the e-mail address)
Save
Reset
Cancel
XHTML 1.0
GALLERY 2
BLACKJACK
HELP GALLERY!



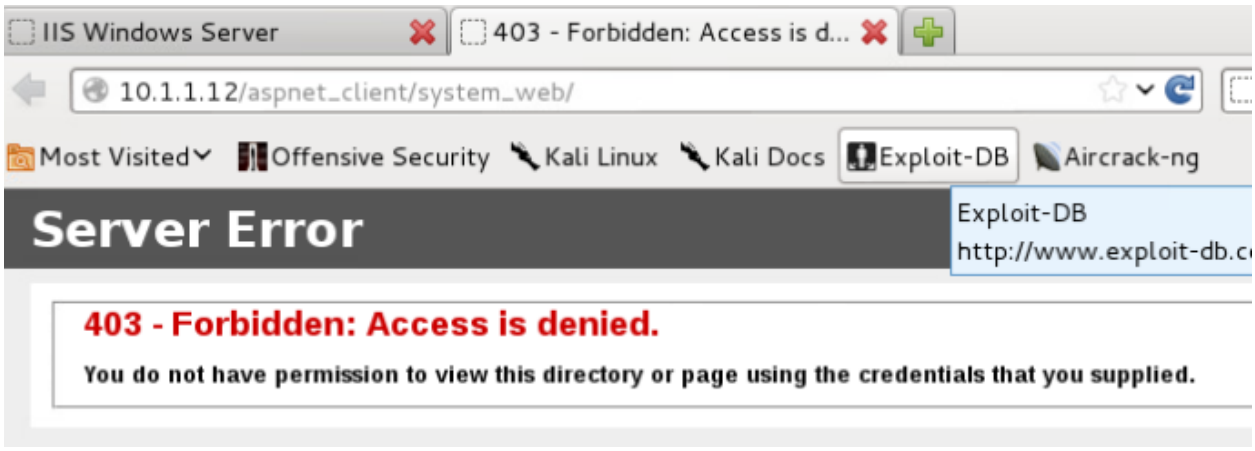

```
1,admin,admin,g0t r00t?,Admin
2,adrian,somepassword,Zombie Films Rock!,Admin
3,john,monkey,I like the smell of confunk,Admin
4,jeremy,password,d1373 1337 speak,Admin
5,bryce,password,I Love SANS,Admin
6,samurai,samurai,Carving fools,Admin
7,jim,password,Rome is burning,Admin
8,bobby,password,Hank is my dad,Admin
9,simba,password,I am a super-cat,Admin
10,dreveil,password,Preparation H,Admin
11,scotty,password,Scotty do,Admin
12,cal,password,C-A-T-S Cats Cats Cats,Admin
13,john,password,Do the Duggie!,Admin
14,kevin,42,Doug Adams rocks,Admin
15,dave,set,Bet on S.E.T. FTW,Admin
16,patches,tortoise,meow,Admin
17,rocky,stripes,treats?,Admin
18,tim,lanmaster53,Because reconnaissance is hard to spell,Admin
19,ABaker,SoSecret,Muffin tops only,Admin
20,PPan,NotTelling,Where is Tinker?,Admin
21,CHook,JollyRoger,Gator-hater,Admin
22,james,i<3devs,Occupation: Researcher,Admin
23,user,user,User Account,Admin
24,ed,pentest,Commandline KungFu anyone?,Admin
```

Part B: NDG Security+V3

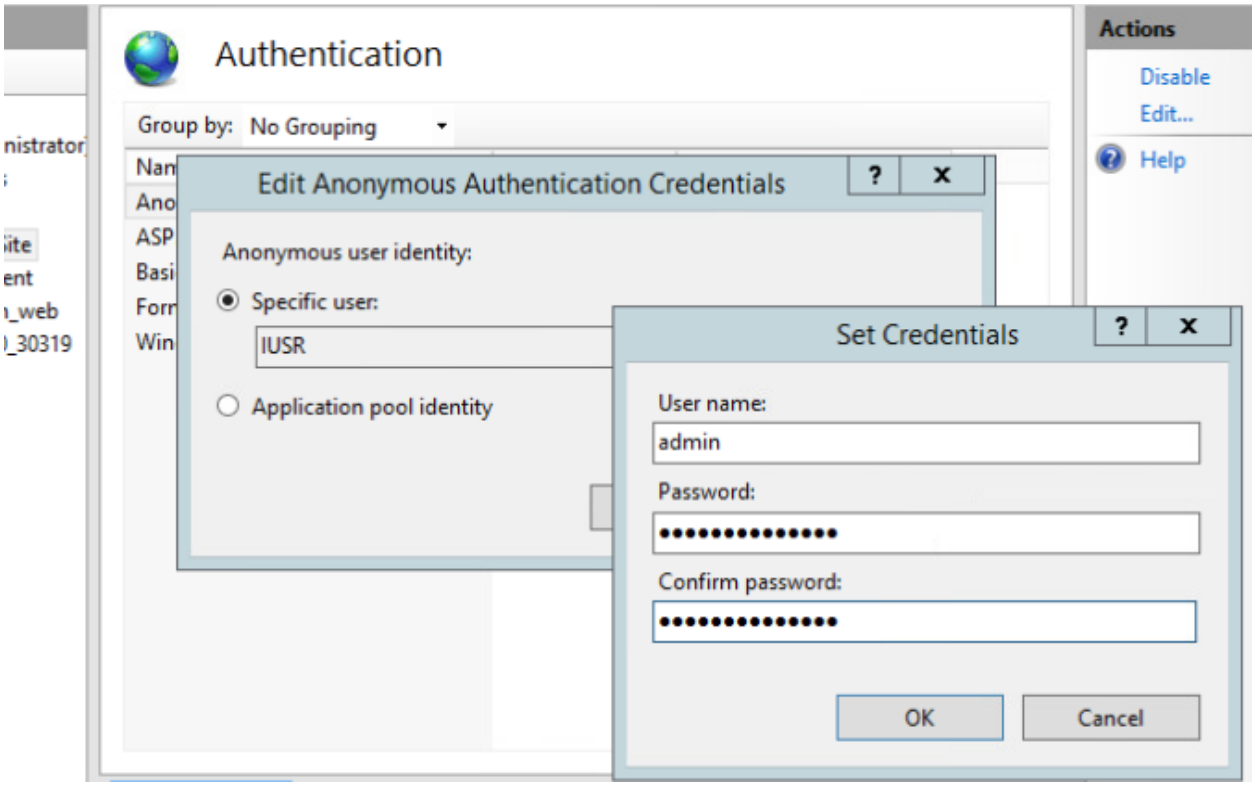
- Analyze the NDG Security+V3 network

  - Fix the firewalls. All ports should be closed
  - Fix the DMZ. DMZ should be accessed by the public IP and should be the only port open. Within the DVL box, activate the HTTP web server. This web server should be accessible on the Kali box.
  - On the DVL network find every website requiring authentication (if any exist)
    - Change the default credentials

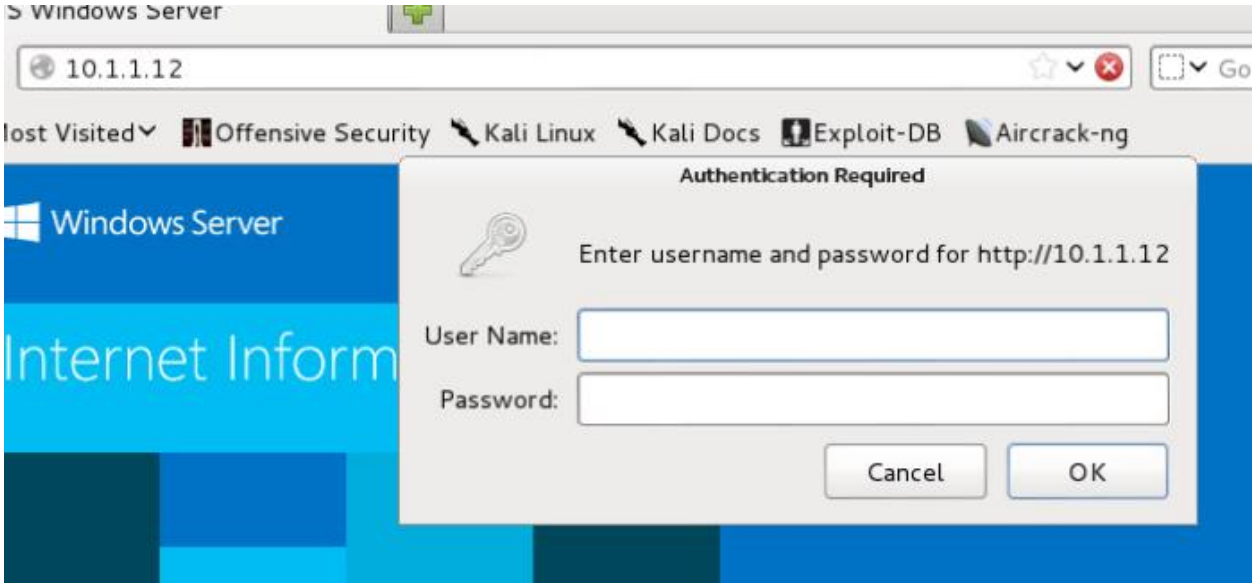
    Website login for Win box on dvl network



So, I went to change them from anonymous to uname admin password



Now I get this



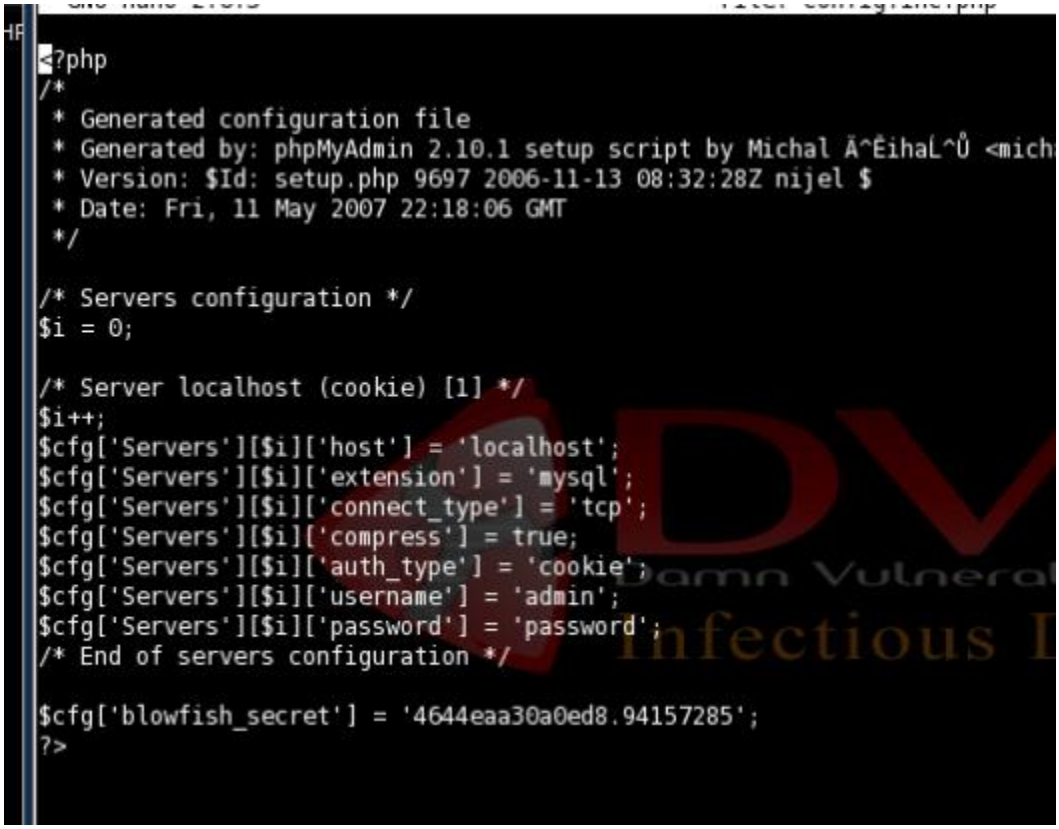
Okay now for the Logins/WEBSITES in DVL box They have an Apache version 1.3

Defult is
username : username
Password :

I could not figure out how to change this password.

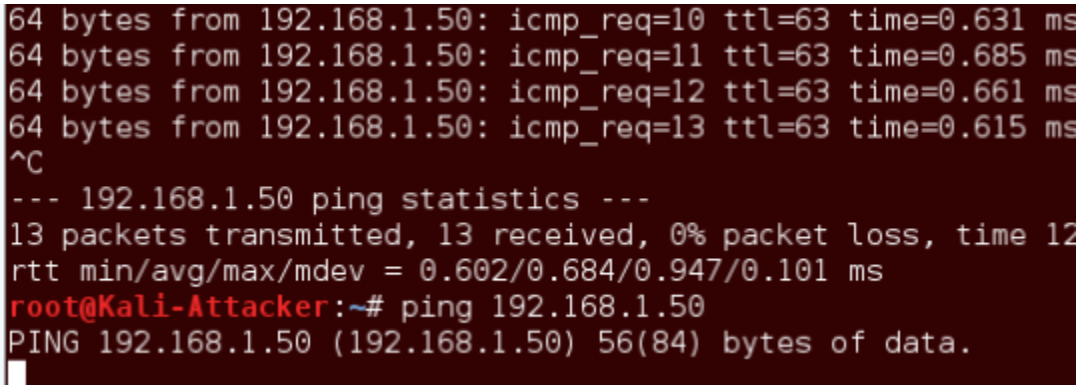
I tried everything from going into the config file and adding entries to changing Apache login directly.

And nothing seemed to save or change.



Now to correctly setup the network,

I cleaned up all the rules and now kali cannot ping into the internal network.



Lastly, I made sure the ports were good, and that kali can reach the website still on the DMZ.

If	Proto	Src. addr	Src. ports	Dest. addr	Dest. ports	NAT IP	NAT Ports	Description
EXTERNAL_GW	TCP	EXTERNAL_GW net	*	DMZ_GW net	80 (HTTP)	10.1.1.10	80 (HTTP)	Allow NAt for Http

ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
	IPv4 TCP	EXTERNAL_GW net	*	10.1.1.10	80 (HTTP)	*	none		NAT Allow NAt for Http

More screenshots of my rules

ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
	*	*	*	INTERNAL_GW Address	80	*	*		Anti-Lockout Rule
	IPv4 *	INTERNAL_GW net	*	EXTERNAL_GW net	*	*	none		Default allow LAN to WAN any rule
	IPv6 *	INTERNAL_GW net	*	EXTERNAL_GW net	*	*	none		Default allow LAN IPv6 to any rule

Part C: NDG Ethical Hacking

- Analyze the NDG Ethical Hacking network
  - Fix the firewalls. All ports should be closed
  - Fix the IP addresses (public/private)
  - Fix the DMZ. DMZ should be accessed by the public IP and should be the only port open
    Initial thought is that kali should not have a private Ip address. (this may be a netlab thing) The DMZ and LAN should not be able to talk for maximum security purposes.
  -
    First before anything I will make the ip address(es) correct

My ip on kali and firewall wan interface changed now to public ips

```
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_
oup default qlen 1000
    link/ether 00:50:56:9a:e2:b9 brd ff:ff:ff:ff:ff:ff
    inet 190.160.1.40/24 brd 190.160.1.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::250:56ff:fe9a:e2b9/64 scope link
       valid_lft forever preferred_lft forever
root@Kali2:~# ping 190.160.1.30
PING 190.160.1.30 (190.160.1.30) 56(84) bytes of data.
64 bytes from 190.160.1.30: icmp_seq=1 ttl=64 time=0.479 ms
64 bytes from 190.160.1.30: icmp_seq=2 ttl=64 time=0.243 ms
64 bytes from 190.160.1.30: icmp_seq=3 ttl=64 time=0.246 ms
64 bytes from 190.160.1.30: icmp_seq=4 ttl=64 time=0.232 ms
^C
--- 190.160.1.30 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2999ms
rtt min/avg/max/mdev = 0.232/0.300/0.479/0.103 ms
root@Kali2:~#
```

Now I made a rule(s) to block lan to DMZ

	IPv4 *	LAN net	*	WAN net	*	*	none		Default allow LAN to WAN ANY

ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
	IPv4 *	LAN net	*	DMZ net	*	*	none		Block all lan on DMZ

```
osboxes@osboxes:~> ping 190.160.1.40
PING 190.160.1.40 (190.160.1.40) 56(84) bytes of data.
64 bytes from 190.160.1.40: icmp_seq=1 ttl=63 time=0.589 ms
64 bytes from 190.160.1.40: icmp_seq=2 ttl=63 time=0.470 ms
64 bytes from 190.160.1.40: icmp_seq=3 ttl=63 time=0.472 ms
^C
--- 190.160.1.40 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2000ms
rtt min/avg/max/mdev = 0.470/0.510/0.589/0.058 ms
osboxes@osboxes:~> ping 190.160.1.30
PING 190.160.1.30 (190.160.1.30) 56(84) bytes of data.
64 bytes from 190.160.1.30: icmp_seq=1 ttl=64 time=0.292 ms
64 bytes from 190.160.1.30: icmp_seq=2 ttl=64 time=0.264 ms
64 bytes from 190.160.1.30: icmp_seq=3 ttl=64 time=0.294 ms
64 bytes from 190.160.1.30: icmp_seq=4 ttl=64 time=0.279 ms
^C
--- 190.160.1.30 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3000ms
rtt min/avg/max/mdev = 0.264/0.282/0.294/0.016 ms
osboxes@osboxes:~> ping 192.168.68.12
PING 192.168.68.12 (192.168.68.12) 56(84) bytes of data.
```

I made a nat rule and i can now access the website on the firewalls IP (public)

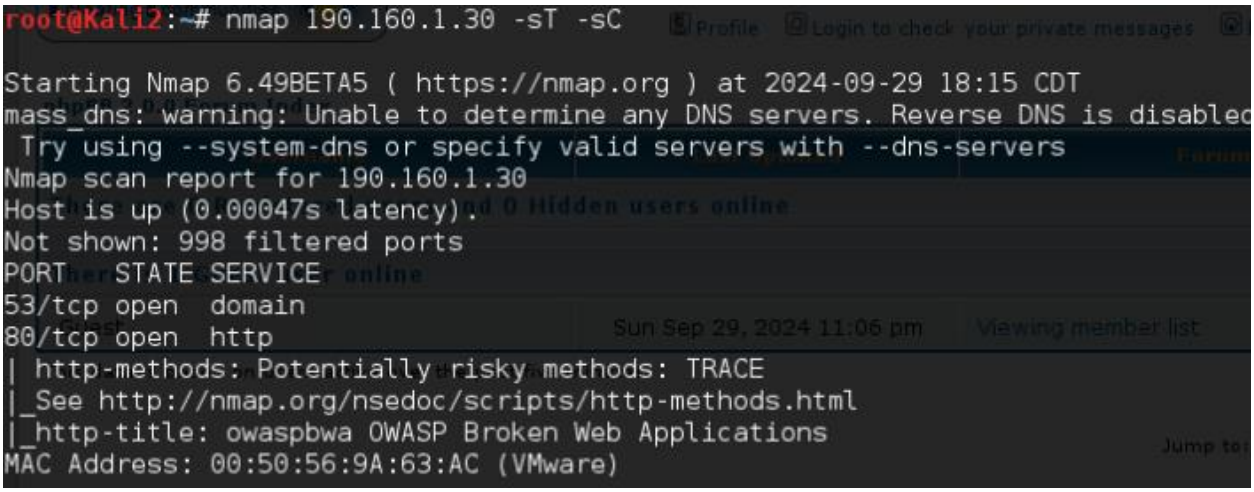
Another important security thing to check, can My LAN ping DMZ?

They can't.

Can WAN ping LAN directly?

No.

Nmap scan of firewall



DNS open I do not believe has any security issues.

And of course, out http open because it is a business required item!

I love firewalls and would like more things with them. It is like a mini puzzle trying to get the rules right for it to work if it does not work the first try. :)