SPORTS MANAGEMENT

Team 5

Demetrio Marruffo
Felix Vargas
Timothy Pavone

Building Our Network

Website Plugins

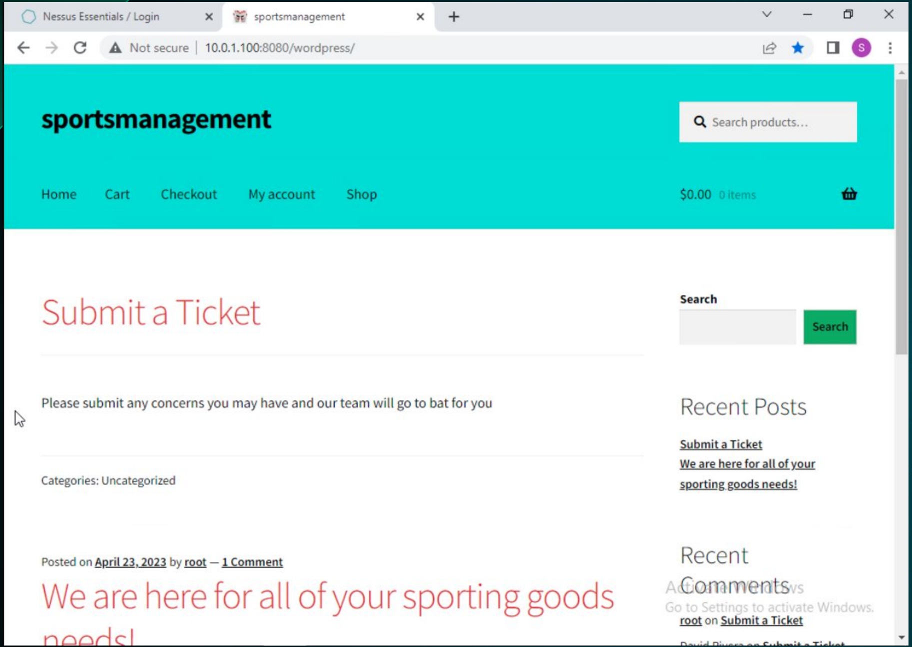
- WooCommerce - Shopping Cart
- WATS - Support Ticketing

Software Installed - Email

- Hmail
- Mozilla Thunderbird

Software Installed - Website/Database

- Xampp
- PHP
- MariaDB
- MySQL
- Wordpress
- Apache



sportsmanagement

Submit a Ticket

Please submit any concerns you may have and our team will go to bat for you

Categories: Uncategorized

Posted on April 23, 2023 by root — 1 Comment

We are here for all of your sporting goods needs!

Recent Posts

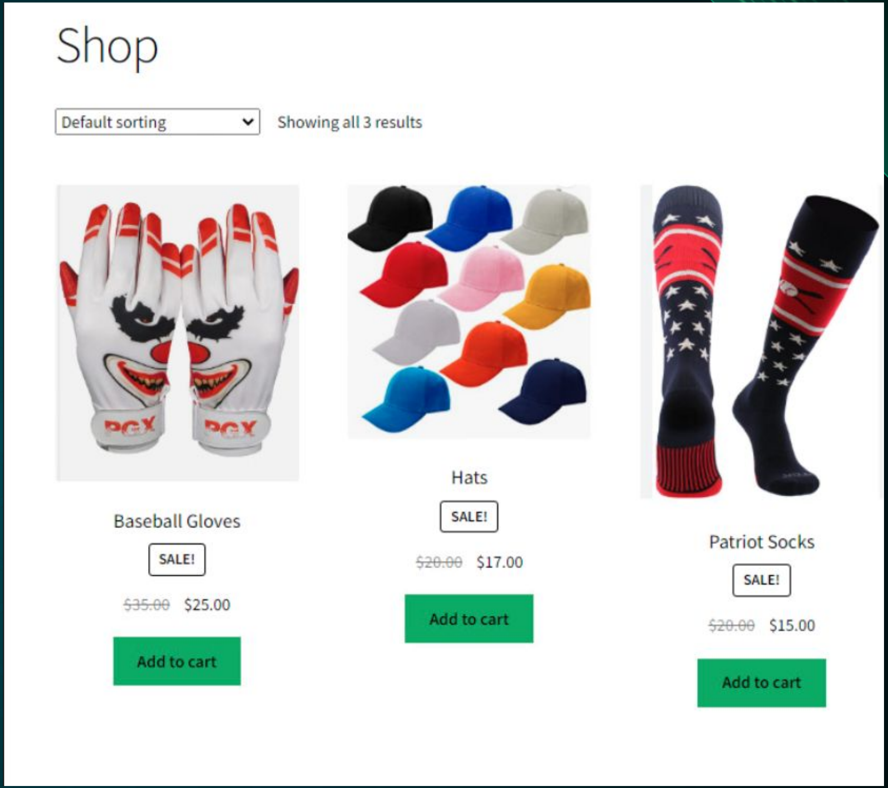
Submit a Ticket

We are here for all of your sporting goods needs!

Recent Comments

root on Submit a Ticket

David Rivera on Submit a Ticket



Shop

Showing all 3 results

Baseball Gloves
SALE!
~~$35.00~~ $25.00

Hats
SALE!
~~$20.00~~ $17.00

Patriot Socks
SALE!
~~$20.00~~ $15.00

TABLE OF CONTENTS

01

Gantt Chart

Screenshot of Gantt chart

02

Network Diagram

What changes were made

03

CSET Compliance

CSET score and charts
Vulnerability scan

04

Pentest Week Analysis

Evidence of attacks or lack thereof

05

Customer Service Perspective

Ticket Responses
Email responses
Items purchased

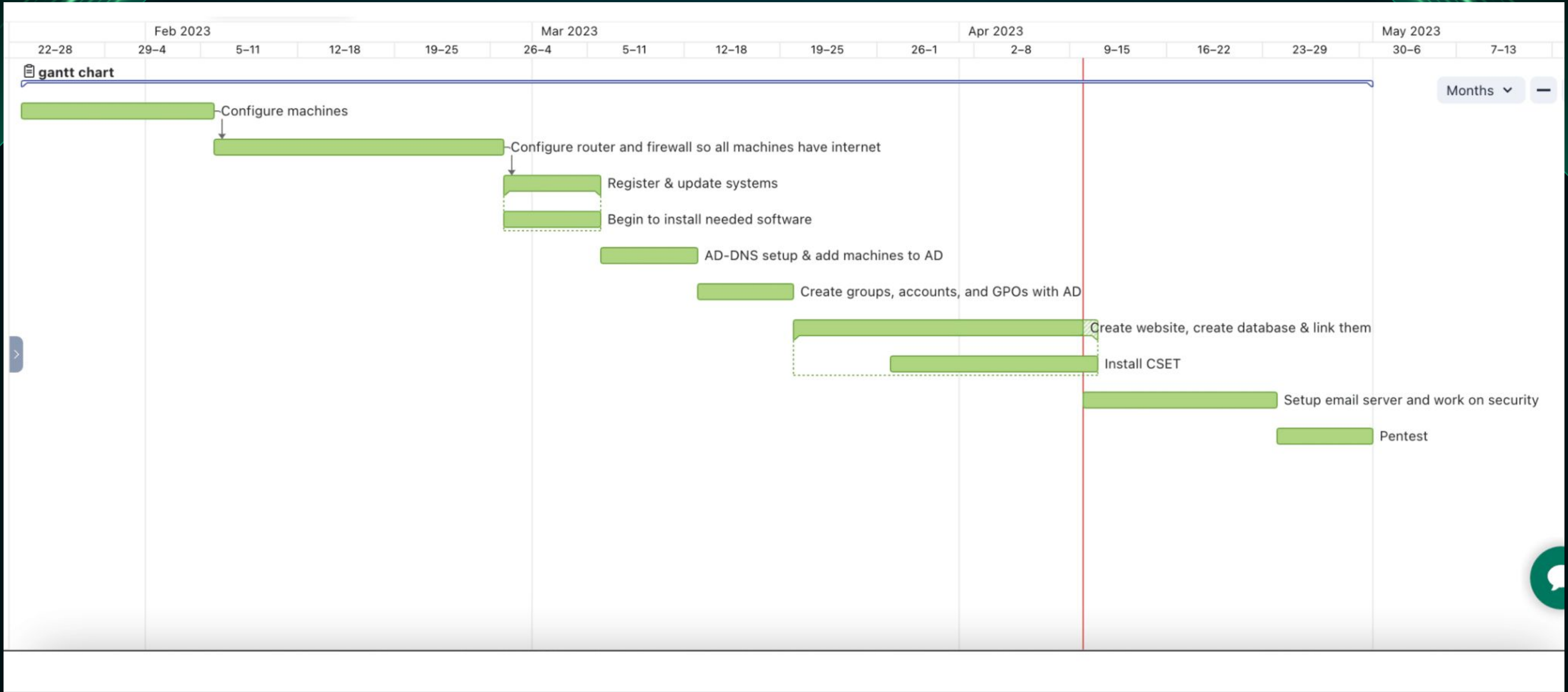
06

Lessons Learned

Things we could improve on

01

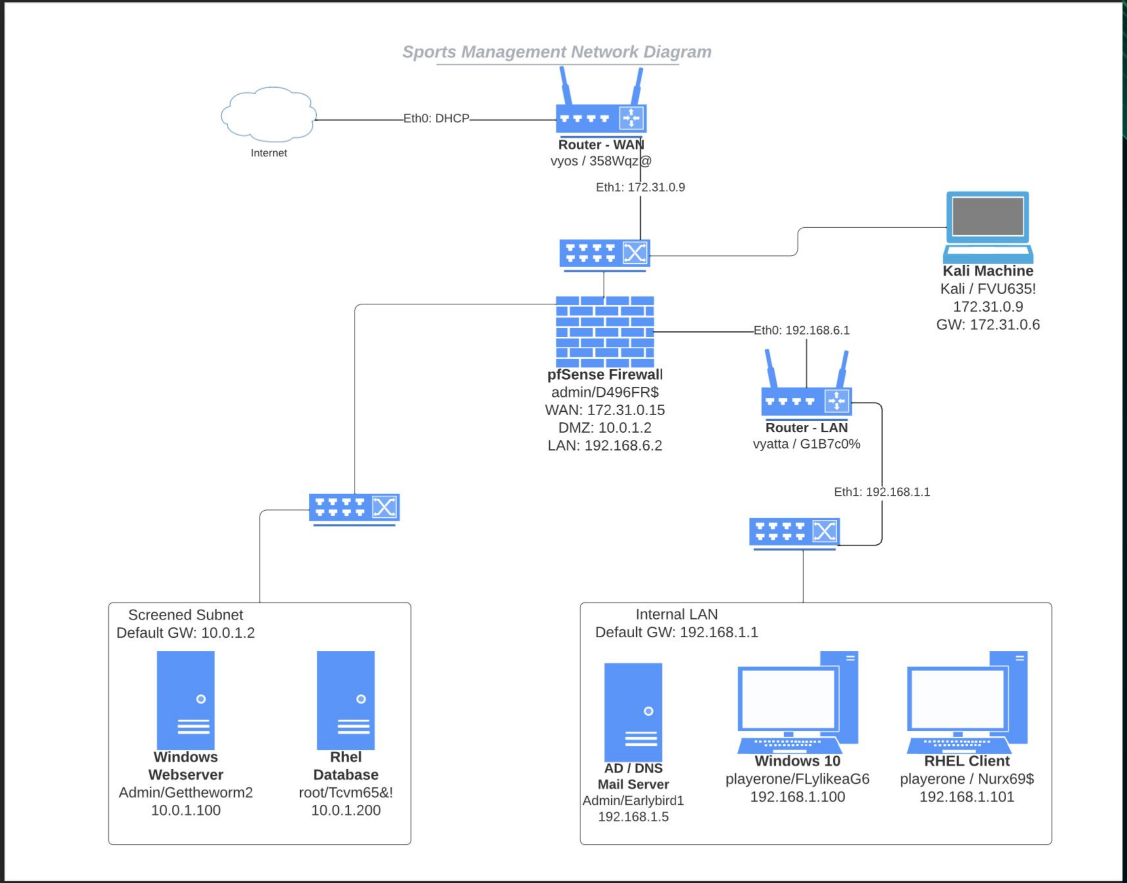
GANTT CHART


Feb 2023
Mar 2023
Apr 2023
May 2023
22–28
29–4
5–11
12–18
19–25
26–4
5–11
12–18
19–25
26–1
2–8
9–15
16–22
23–29
30–6
7–13
gantt chart
Months
Configure machines
Configure router and firewall so all machines have internet
Register & update systems
Begin to install needed software
AD-DNS setup & add machines to AD
Create groups, accounts, and GPOs with AD
Create website, create database & link them
Install CSET
Setup email server and work on security
Pentest

02 NETWORK DIAGRAM

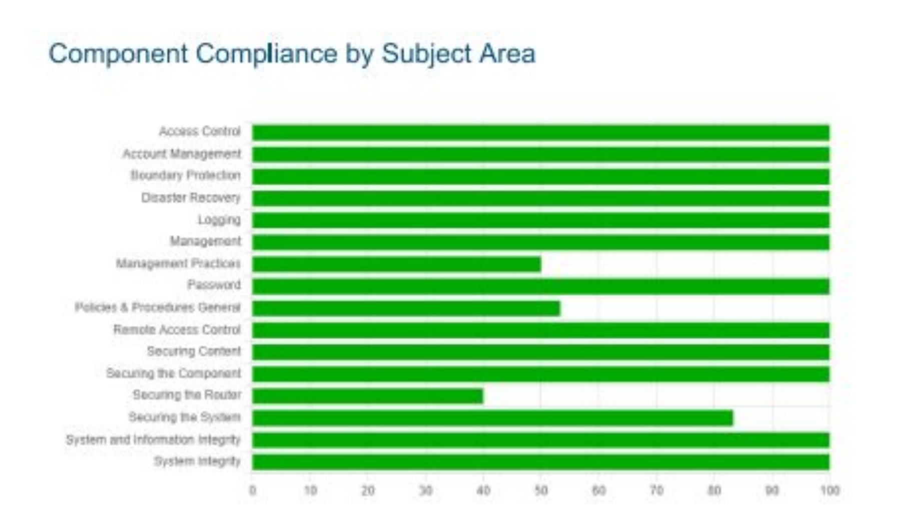
Network Setup

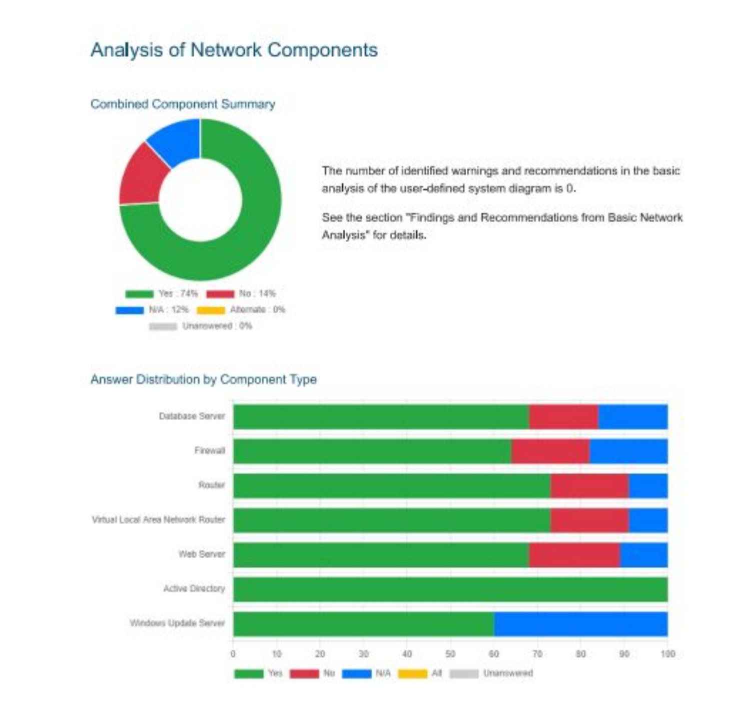
- Changed IP addresses
- DHCP on WAN
- Similar to kanban
- Mail server added to AD
- Database configured or Windows



CSET COMPLIANCE 03

- Passed the CSET compliance tool
- Helped pinpoint areas we could work on
- 0 identified warnings during final assessment


Component Compliance by Subject Area


Analysis of Network Components

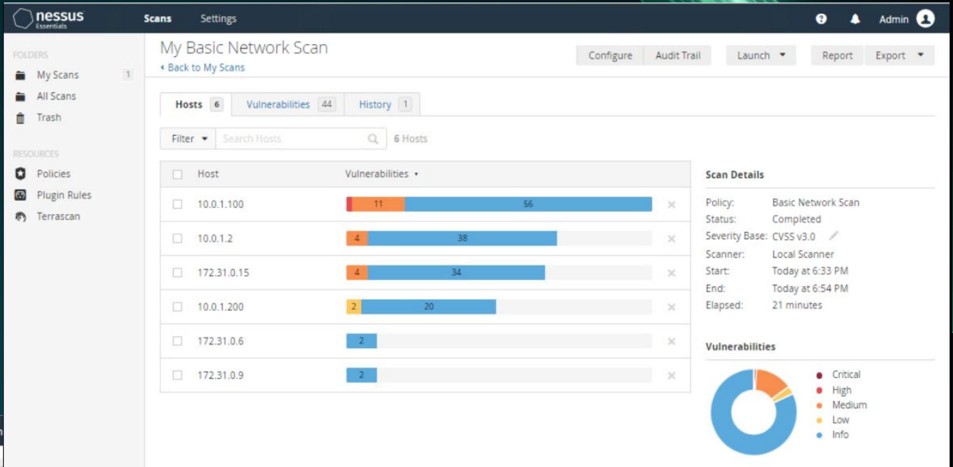
Combined Component Summary

The number of identified warnings and recommendations in the basic analysis of the user-defined system diagram is 0.

See the section "Findings and Recommendations from Basic Network Analysis" for details.

Answer Distribution by Component Type

- Passed a vulnerability scan as well
- Over 80% with no critical marks
- 2 scans - 1 from outside of Lan and 1 from inside
- Used Nessus Essentials



My Basic Network Scan

‹ Back to My Scans

Hosts 6 | Vulnerabilities 44 | History 1

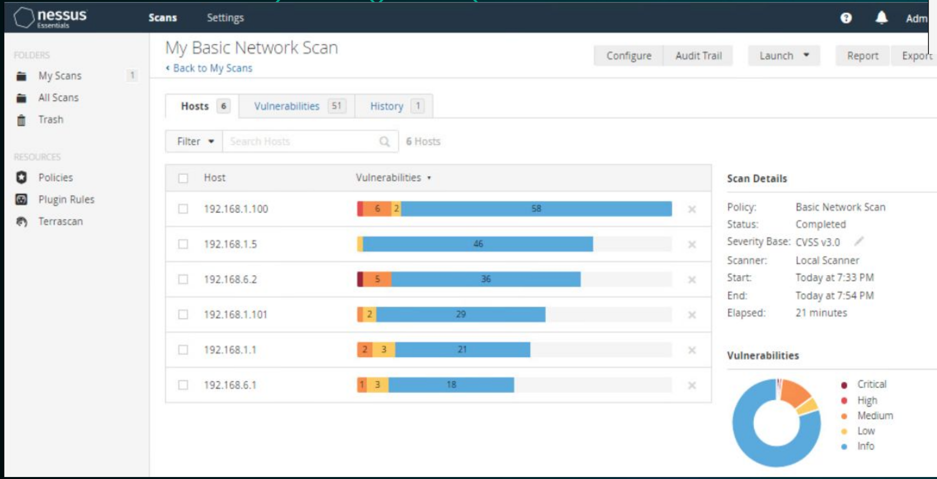
6 Hosts

Host	Vulnerabilities
10.0.1.100	11 56
10.0.1.2	4 38
172.31.0.15	4 34
10.0.1.200	2 20
172.31.0.6	2
172.31.0.9	2

Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 6:33 PM
End: Today at 6:54 PM
Elapsed: 21 minutes

Vulnerabilities



My Basic Network Scan

‹ Back to My Scans

Hosts 6 | Vulnerabilities 51 | History 1

6 Hosts

Host	Vulnerabilities
192.168.1.100	6 2 58
192.168.1.5	46
192.168.6.2	5 36
192.168.1.101	2 29
192.168.1.1	2 3 21
192.168.6.1	1 3 18

Scan Details

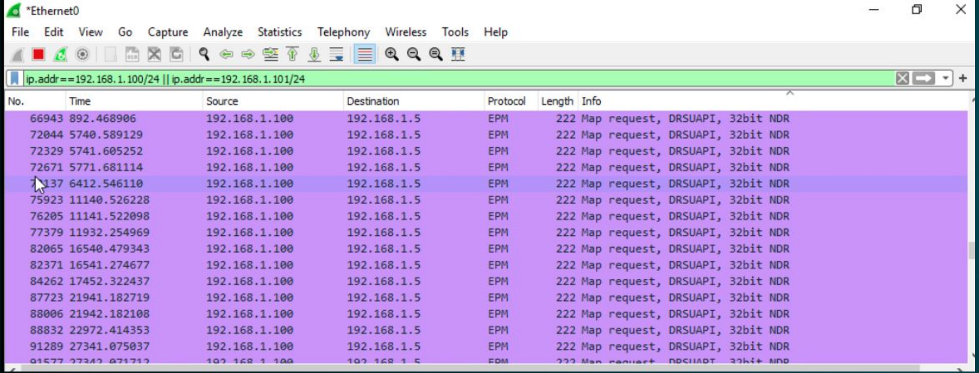
Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 7:33 PM
End: Today at 7:54 PM
Elapsed: 21 minutes

Vulnerabilities

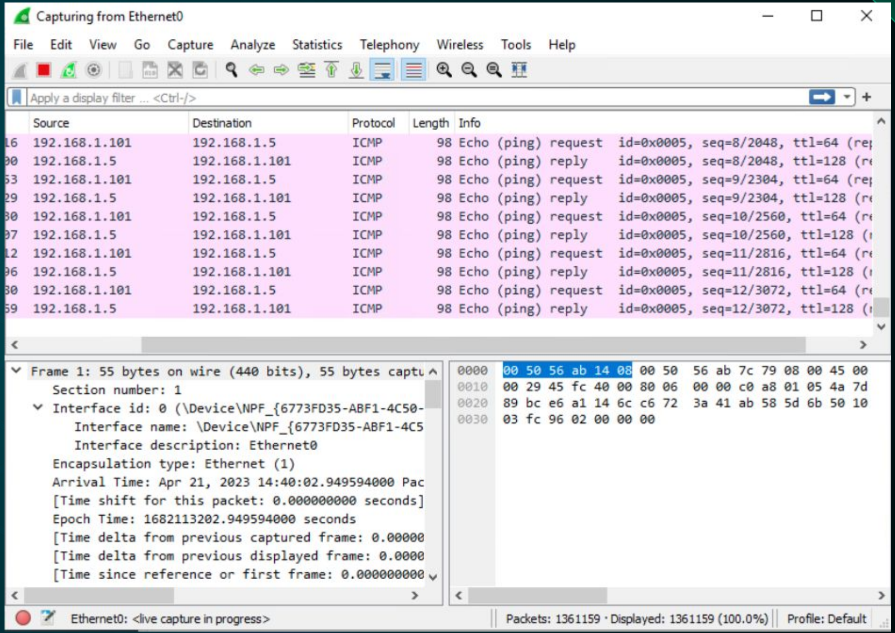
04

PENTEST WEEK ANALYSIS

- Used Wireshark as monitoring tool and IDS
- Saw pings and map requests


*Ethernet0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
ip.addr==192.168.1.100/24 || ip.addr==192.168.1.101/24

No.      Time            Source          Destination    Protocol  Length  Info
   66943 892.468906      192.168.1.100   192.168.1.5    EPM          222  Map request, DRSUAPI, 32bit NDR
   72044 5740.589129     192.168.1.100   192.168.1.5    EPM          222  Map request, DRSUAPI, 32bit NDR
   72329 5741.605252     192.168.1.100   192.168.1.5    EPM          222  Map request, DRSUAPI, 32bit NDR
   72671 5771.681114     192.168.1.100   192.168.1.5    EPM          222  Map request, DRSUAPI, 32bit NDR
   7 137 6412.546110     192.168.1.100   192.168.1.5    EPM          222  Map request, DRSUAPI, 32bit NDR
   75923 11140.526228    192.168.1.100   192.168.1.5    EPM          222  Map request, DRSUAPI, 32bit NDR
   76205 11141.522098    192.168.1.100   192.168.1.5    EPM          222  Map request, DRSUAPI, 32bit NDR
   77379 11932.254969    192.168.1.100   192.168.1.5    EPM          222  Map request, DRSUAPI, 32bit NDR
   82065 16540.479343    192.168.1.100   192.168.1.5    EPM          222  Map request, DRSUAPI, 32bit NDR
   82371 16541.274677    192.168.1.100   192.168.1.5    EPM          222  Map request, DRSUAPI, 32bit NDR
   84262 17452.322437    192.168.1.100   192.168.1.5    EPM          222  Map request, DRSUAPI, 32bit NDR
   87723 21941.182719    192.168.1.100   192.168.1.5    EPM          222  Map request, DRSUAPI, 32bit NDR
   88006 21942.182108    192.168.1.100   192.168.1.5    EPM          222  Map request, DRSUAPI, 32bit NDR
   88832 22972.414353    192.168.1.100   192.168.1.5    EPM          222  Map request, DRSUAPI, 32bit NDR
   91289 27341.075037    192.168.1.100   192.168.1.5    EPM          222  Map request, DRSUAPI, 32bit NDR
   91577 27342.071712    192.168.1.100   192.168.1.5    EPM          222  Map request, DRSUAPI, 32bit NDR
```


Capturing from Ethernet0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
    Source          Destination     Protocol  Length  Info
16  192.168.1.101   192.168.1.5     ICMP          98  Echo (ping) request  id=0x0005, seq=8/2048, ttl=64 (rep
90  192.168.1.5     192.168.1.101   ICMP          98  Echo (ping) reply    id=0x0005, seq=8/2048, ttl=128 (re
53  192.168.1.101   192.168.1.5     ICMP          98  Echo (ping) request  id=0x0005, seq=9/2304, ttl=64 (rep
29  192.168.1.5     192.168.1.101   ICMP          98  Echo (ping) reply    id=0x0005, seq=9/2304, ttl=128 (re
30  192.168.1.101   192.168.1.5     ICMP          98  Echo (ping) request  id=0x0005, seq=10/2560, ttl=64 (re
97  192.168.1.5     192.168.1.101   ICMP          98  Echo (ping) reply    id=0x0005, seq=10/2560, ttl=128 (r
12  192.168.1.101   192.168.1.5     ICMP          98  Echo (ping) request  id=0x0005, seq=11/2816, ttl=64 (re
96  192.168.1.5     192.168.1.101   ICMP          98  Echo (ping) reply    id=0x0005, seq=11/2816, ttl=128 (r
30  192.168.1.101   192.168.1.5     ICMP          98  Echo (ping) request  id=0x0005, seq=12/3072, ttl=64 (re
59  192.168.1.5     192.168.1.101   ICMP          98  Echo (ping) reply    id=0x0005, seq=12/3072, ttl=128 (r
```

```
Frame 1: 55 bytes on wire (440 bits), 55 bytes captu
    Section number: 1
    Interface id: 0 (\Device\NPF_{6773FD35-ABF1-4C50-
        Interface name: \Device\NPF_{6773FD35-ABF1-4C5
        Interface description: Ethernet0
    Encapsulation type: Ethernet (1)
    Arrival Time: Apr 21, 2023 14:40:02.949594000 Pac
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1682113202.949594000 seconds
    [Time delta from previous captured frame: 0.00000
    [Time delta from previous displayed frame: 0.0000
    [Time since reference or first frame: 0.000000000
```

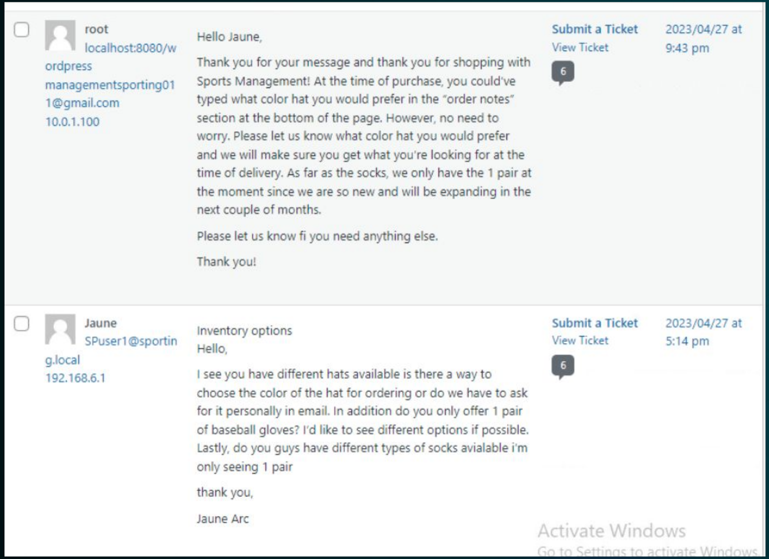
```
0000  00 50 56 ab 14 08 00 50  56 ab 7c 79 08 00 45 00
0010  00 29 45 fc 40 00 80 06  00 00 c0 a8 01 05 4a 7d
0020  89 bc e6 a1 14 6c c6 72  3a 41 ab 58 5d 6b 50 10
0030  03 fc 96 02 00 00 00
```

Ethernet0: <live capture in progress>   Packets: 1361159 · Displayed: 1361159 (100.0%)   Profile: Default

05

CUSTOMER SERVICE

- Took us no longer than 7 hours to respond to each ticket
- Responded to every single ticket respectfully and professionally



□ root localhost:8080/wordpress managementsporting01 1@gmail.com 10.0.1.100

Hello Jaune,

Thank you for your message and thank you for shopping with Sports Management! At the time of purchase, you could've typed what color hat you would prefer in the "order notes" section at the bottom of the page. However, no need to worry. Please let us know what color hat you would prefer and we will make sure you get what you're looking for at the time of delivery. As far as the socks, we only have the 1 pair at the moment since we are so new and will be expanding in the next couple of months.

Please let us know fi you need anything else.

Thank you!

Submit a Ticket · View Ticket · 6 · 2023/04/27 at 9:43 pm

□ Jaune SPuser1@sporting.local 192.168.6.1

Inventory options

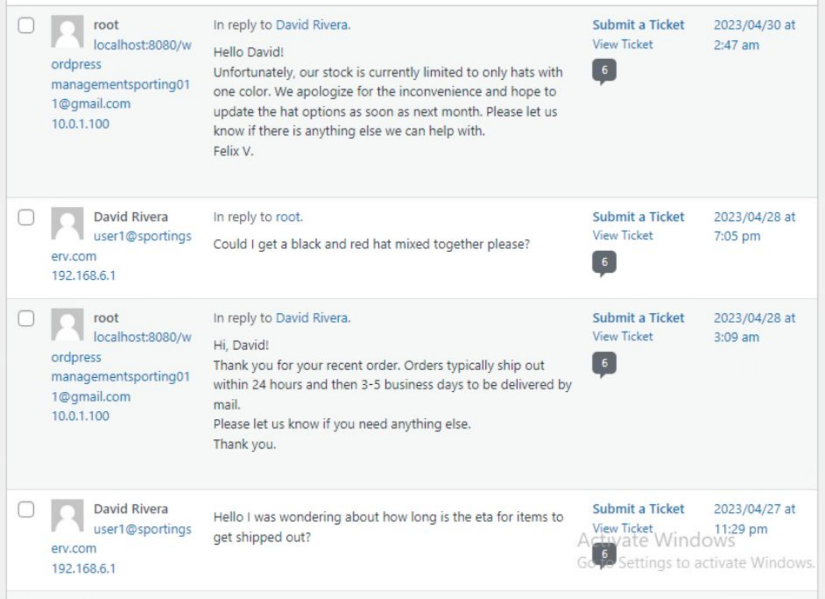
Hello,

I see you have different hats available is there a way to choose the color of the hat for ordering or do we have to ask for it personally in email. In addition do you only offer 1 pair of baseball gloves? I'd like to see different options if possible. Lastly, do you guys have different types of socks avialable i'm only seeing 1 pair

thank you,

Jaune Arc

Submit a Ticket · View Ticket · 6 · 2023/04/27 at 5:14 pm



□ root localhost:8080/wordpress managementsporting01 1@gmail.com 10.0.1.100

In reply to David Rivera.

Hello David!
Unfortunately, our stock is currently limited to only hats with one color. We apologize for the inconvenience and hope to update the hat options as soon as next month. Please let us know if there is anything else we can help with.
Felix V.

Submit a Ticket · View Ticket · 6 · 2023/04/30 at 2:47 am

□ David Rivera user1@sportingserv.com 192.168.6.1

In reply to root.

Could I get a black and red hat mixed together please?

Submit a Ticket · View Ticket · 6 · 2023/04/28 at 7:05 pm

□ root localhost:8080/wordpress managementsporting01 1@gmail.com 10.0.1.100

In reply to David Rivera.

Hi, David!
Thank you for your recent order. Orders typically ship out within 24 hours and then 3-5 business days to be delivered by mail.
Please let us know if you need anything else.
Thank you.

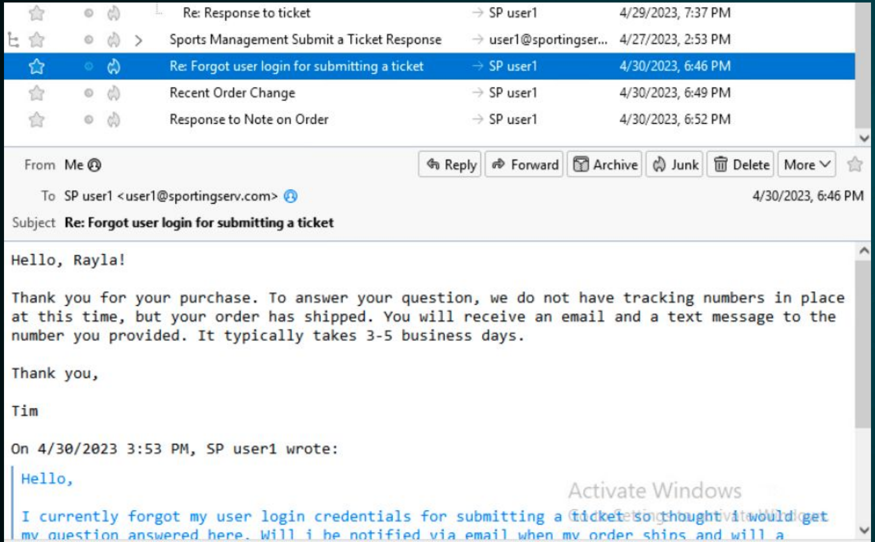
Submit a Ticket · View Ticket · 6 · 2023/04/28 at 3:09 am

□ David Rivera user1@sportingserv.com 192.168.6.1

Hello I was wondering about how long is the eta for items to get shipped out?

Submit a Ticket · View Ticket · 6 · 2023/04/27 at 11:29 pm

- Responded through the website and email
- All emails were also responded to in no more than 7 hours



Re: Response to ticket	→ SP user1	4/29/2023, 7:37 PM
Sports Management Submit a Ticket Response	→ user1@sportingser...	4/27/2023, 2:53 PM
Re: Forgot user login for submitting a ticket	→ SP user1	4/30/2023, 6:46 PM
Recent Order Change	→ SP user1	4/30/2023, 6:49 PM
Response to Note on Order	→ SP user1	4/30/2023, 6:52 PM

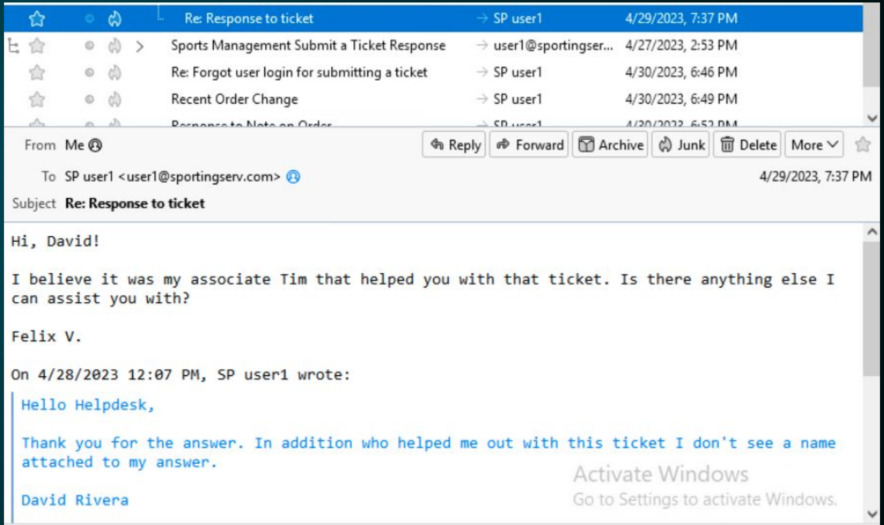
From Me

To SP user1 <user1@sportingserv.com>

4/30/2023, 6:46 PM

Subject **Re: Forgot user login for submitting a ticket**

```
Hello, Rayla!

Thank you for your purchase. To answer your question, we do not have tracking numbers in place
at this time, but your order has shipped. You will receive an email and a text message to the
number you provided. It typically takes 3-5 business days.

Thank you,

Tim

On 4/30/2023 3:53 PM, SP user1 wrote:
  Hello,

  I currently forgot my user login credentials for submitting a ticket so thought i would get
  my question answered here. Will i be notified via email when my order ships and will a
```



Re: Response to ticket	→ SP user1	4/29/2023, 7:37 PM
Sports Management Submit a Ticket Response	→ user1@sportingser...	4/27/2023, 2:53 PM
Re: Forgot user login for submitting a ticket	→ SP user1	4/30/2023, 6:46 PM
Recent Order Change	→ SP user1	4/30/2023, 6:49 PM
Response to Note on Order	SP user1	4/30/2023, 6:52 PM

From Me

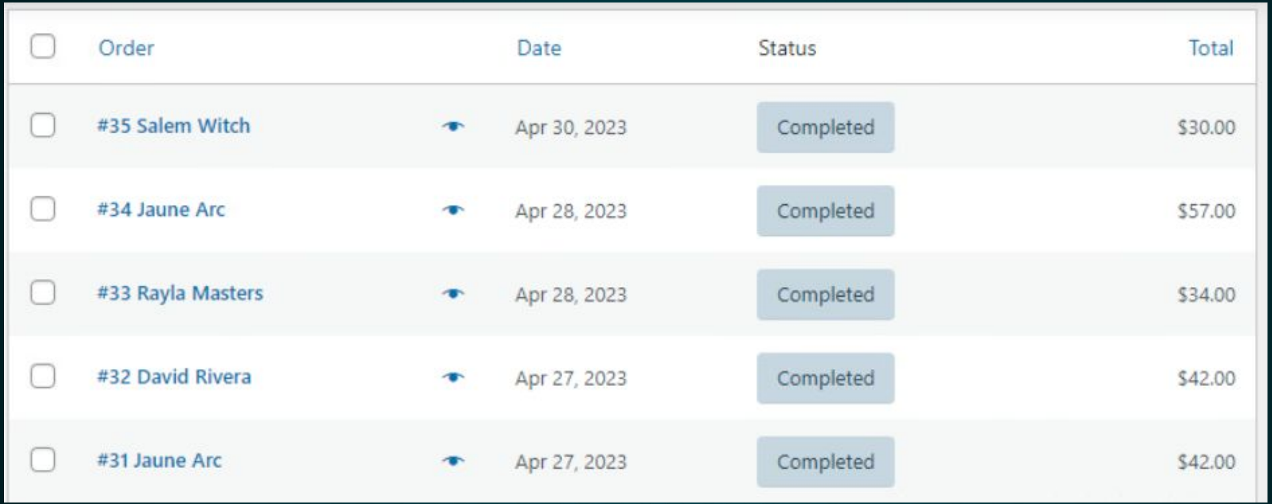
To SP user1 <user1@sportingserv.com>

4/29/2023, 7:37 PM

Subject **Re: Response to ticket**

```
Hi, David!

I believe it was my associate Tim that helped you with that ticket. Is there anything else I
can assist you with?

Felix V.

On 4/28/2023 12:07 PM, SP user1 wrote:
  Hello Helpdesk,

  Thank you for the answer. In addition who helped me out with this ticket I don't see a name
  attached to my answer.

  David Rivera
```

- Once orders were acknowledged, responded to, and "shipped" the order was marked as complete



□	Order	Date	Status	Total
□	#35 Salem Witch	Apr 30, 2023	Completed	$30.00
□	#34 Jaune Arc	Apr 28, 2023	Completed	$57.00
□	#33 Rayla Masters	Apr 28, 2023	Completed	$34.00
□	#32 David Rivera	Apr 27, 2023	Completed	$42.00
□	#31 Jaune Arc	Apr 27, 2023	Completed	$42.00

06 LESSONS LEARNED

- Fully upgrade PFSense sooner than later. No access to Snort IDS because it would've been too late to re-configure the firewall
- At first, couldn't get Apache to listen to port 80. Figured out how to update the conf file to listen on port 8080
- At first, couldn't get our website off of localhost so wasn't able to reach our other machines. While figuring out how to change the conf file, the site was broken twice and had to be redone. Got it fully working by the end
- Since we were also using the machines, it was tough to know which traffic was from us and which traffic was from the red team. Adding a signature to our traffic could've helped

THANKS!