Internet Scale Scanning

## Summary

Attackers do not need to do broad scans when others are doing for them.

This lab looks at how attackers can manage reconnaissance and build an initial inventory of their target without ever sending a packet to the target.

## Tools/Resources

Website: <https://bgp.he.net/>

Website: <https://www.shodan.io>

## Tasks

Using: <https://bgp.he.net/> try the following searches against UNH:

1. Search unh.edu. Determine CIDR and AS.  This informs you of the IP address space and ISP providers.
2. Search the UNH CIDR. How many DNS entries?  Anything interesting or unusual?  Looking for a job or someone to phish?  How many AS’s are propagating AS11745 addresses?

Using: <https://www.shodan.io> try searching UNH’s CIDR, “net:132.177.0.0/16”

1. How many publicly exposed: web and ssh servers?
2. Are any servers running older (maybe unpatched) versions? Should UNH IT shut these down?
3. What is available on: hostname:"cs.unh.edu"

## Submission

Upload to Canvas a docx or pdf containing screenshots showing a reconnaissance of a domain you find interesting (not unh.edu).

DO NOT ATTACK, you do not have permission.

## Walkthrough

1. Using: <https://bgp.he.net/> try the following searches against UNH:
   1. Search unh.edu. Determine CIDR and AS. This informs you of the IP address space and ISP providers.

A screenshot of a computer

Description automatically generated

* 1. Search the UNH CIDR. How many DNS entries? More than 1000 entries

A screenshot of a computer

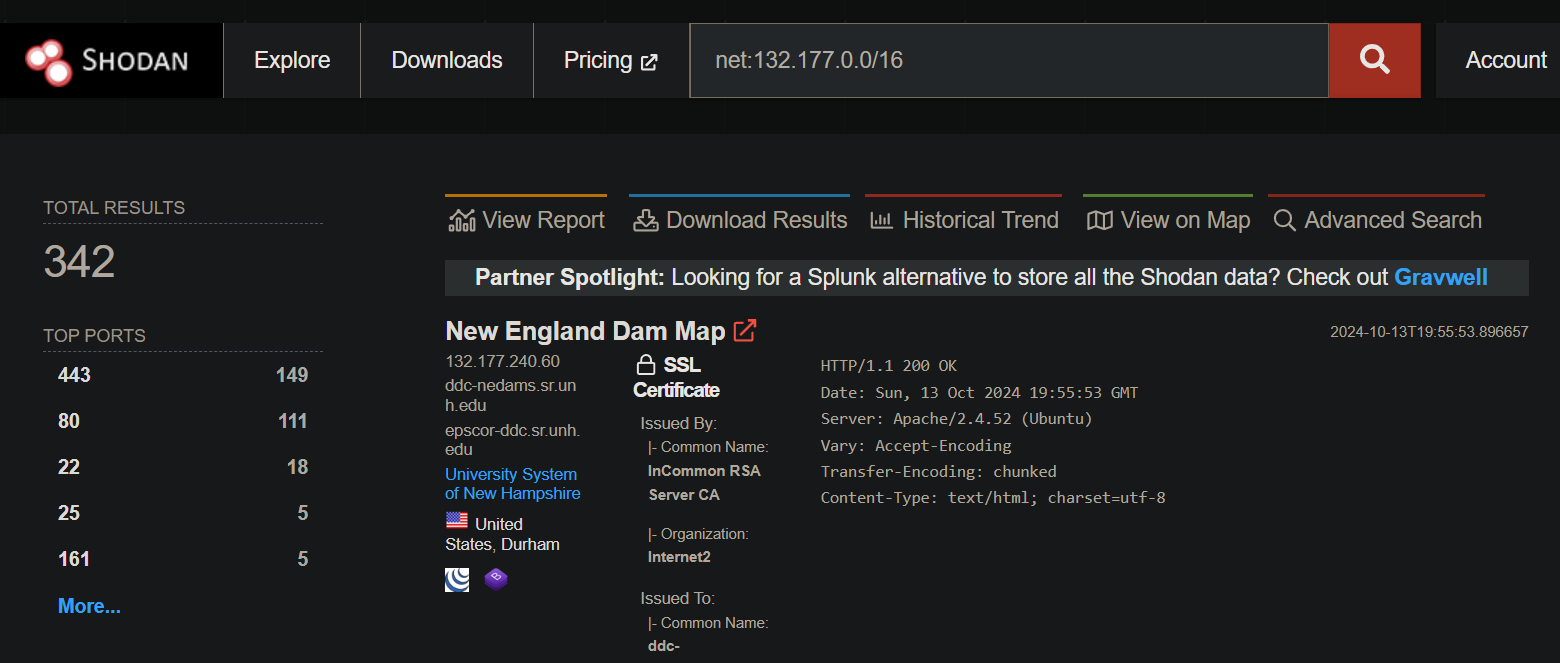
Description automatically generated

* 1. Anything interesting or unusual? “cs.unh,edu” 132,177,{4,5,8,10,11,14}.0/24 are these sites separately managed from unh.edu? How many AS’s are propagating AS11745 addresses?

A screenshot of a computer

Description automatically generated

1. Using: <https://www.shodan.io> try searching UNH’s CIDR, “net:132.177.0.0/16”. Searches are free, but you do need to establish an account.
   1. How many publicly exposed: web and ssh servers?



* 1. Are any servers running older (maybe unpatched) versions? Should UNH IT shut these down?

A screenshot of a computer

Description automatically generated

* 1. What is available on: hostname:"cs.unh.edu"

A screenshot of a computer

Description automatically generated

Upload to Canvas a docx or pdf containing screenshots showing a reconnaissance of a domain you find interesting (not unh.edu).DO NOT ATTACK, you do not have permission.

## Additional Thoughts

Why does cs.unh.edu need to run a DNS server?

* This is a management control issue rather than a technical issue?
* How are dev, test, and staging hosts managed?

How does IPv6 impact Shodan scanning?

* There is vast amount of empty IPv6 space, brute force is not viable.
* Can you translate an IPv4 CIDR to IPv6?
  + 1.2.3.4/32 -> ::ffff:1.2.3.4/128
  + 1.2.3.0/24 -> ::ffff:1.2.3.0/120