CALIFORNIA STATE UNIVERSITY
LONG BEACH
College of Engineering

CECS 303: Networks and Network Security

Penetration Testing (cont'd)

Chris Samayoa

Week 8 – 2nd Lecture
3/10/2022

Course Information

- CECS 303
  - Networks and Network Security – 3.0 units
- Class meeting schedule
  - TuTH 5:00PM to 7:15PM
  - Lecture Room: VEC 402
  - Lab Room: ECS 413
- Class communication
  - chris.samayoa@csulb.edu
  - Cell: 562-706-2196
- Office hours
  - Thursdays 4pm-5pm (VEC-404)
  - Other times by appointment only

Objectives

- Types of penetration tests
- Intro to Penetration Testing
  - Stages
- Rules of Engagement
- Reconnaissance techniques

Why Pen Test?

- Compliance
  - Some industries have specific frameworks that they must adhere to legally
    - Payment card industry (PCI DSS)
    - North American utility companies (NERC CIP)
    - Medical Industry (HIPAA)
    - Department of Defense (CMMS [Cybersecurity Maturity Model Certification])
  - Other organizations may have a self imposed compliance requirement
    - Good publicity
    - ISO 27001
    - NIST-CSF
- Risk Management
  - Cybersecurity insurance will often require penetration testing
  - Acceptable risks can be calculated if needed
- Baselines
  - Regular penetration tests can serve as baselines for needed remediations
  - Set future architecture roadmaps
- Stay informed!

Penetration Testing Types

- White Box
  - Internal structure of network environment is known
  - Tester can view source code and have access to applications and systems
  - Test from developer’s / administrators point of view
- Black Box
  - Internal structure is unknown for network environment
  - Little to no information provided to testers
  - Can most closely resemble external actors
    - Time restraints are different
- Grey Box
  - Combination of white box and black box
  - Tester can partially “see” inner working of a network environment
    - Allows for more of the network to be tested within a given time frame
    - Tester granted some permissions or internal access on the network
  - Typically where most penetration tests land

Penetration Testing Stages

- Planning (scoping)
- Reconnaissance
- Gaining Access (exploitation) – Lateral Movement
- Maintaining Access / Escalation
- Analysis / Reporting
- Remediation

Planning

- Identify what threats cause the most concern
    - Insider threats
    - External threats
    - Unknown
- What devices?
    - Cloud vs on-premises
        - What about cloud service policies?
    - IP address ranges / domain names
    - Servers / workstations / network devices
- Length of engagement
    - Cost vs scope
    - Can help determine what type of testing would be best
- Rules of Engagement document solidifies the scope

Rules of Engagement

- Rules of Engagement (ROE)
  - Written document that specifies the scope and allowable actions during a penetration test
  - Specifies level of communication during engagement
- Type and scope of engagement
  - White box / black box / grey box
  - What attack surfaces can be tested
  - What methods are allowed?
    - Intrusive vs. non-intrusive
    - Physical vs remote engagements
- Client contact details
  - Who knows about the testing?
  - Who should be contacted and in what order?
  - Preferred methods of communication

Rules of Engagement

- IT Team Notifications
  - When should the IT team be engaged?
  - Establish levels of criticality
- Sensitive data
  - Special provisions for regulated data (e.g. HIPAA)
- Meetings and report
  - Pre-determined meeting dates and frequency
  - What types of reports are needed (e.g. technical, executive, sanitized)

Rules of Engagement

- Hours of engagement
  - 24/7
  - After-hours only
  - Who needs to know these?
- Handling of a sensitive / critical vulnerability
- Essential to legally protect penetration testers

Reconnaissance

- Goals
  - Discover attack surfaces (physical and network)
  - Discover overall cybersecurity environment
  - Gain information to assist with vulnerability exploitation
- Publicly available information
  - Company employee directories
  - Whois information
  - DNS information
  - ARIN
- Physical visits
  - What can be learned about the facilities?
  - Lobby officers?
  - Server room locations?
  - Access control?

Reconnaissance (cont’d)

- Social engineering
  - Tailgating
  - Phishing
  - Discover overall cybersecurity environment
  - Gain information to assist with vulnerability exploitation
- Social media or other employee profiles
  - Potential usernames
  - Potential passwords
  - Vacations
  - Insider information
  - Many of this information can help to impersonate individuals

Reconnaissance (cont’d)

- Plant devices
    - Raspberry Pis
    - Keyloggers
- Passive data collection
    - Monitor online traffic
    - Monitor internal network traffic
    - Learn employee schedules
- Active data collection
    - ICMP (ping) sweeps
    - Service identification
    - Vulnerability scans
    - RFID cloning

Tools Overview

- Network Scanners
  - Nmap
  - Masscan
- Vulnerability Scanners
  - Nessus
  - OpenVAS
  - Tripewire IP360
  - Retina

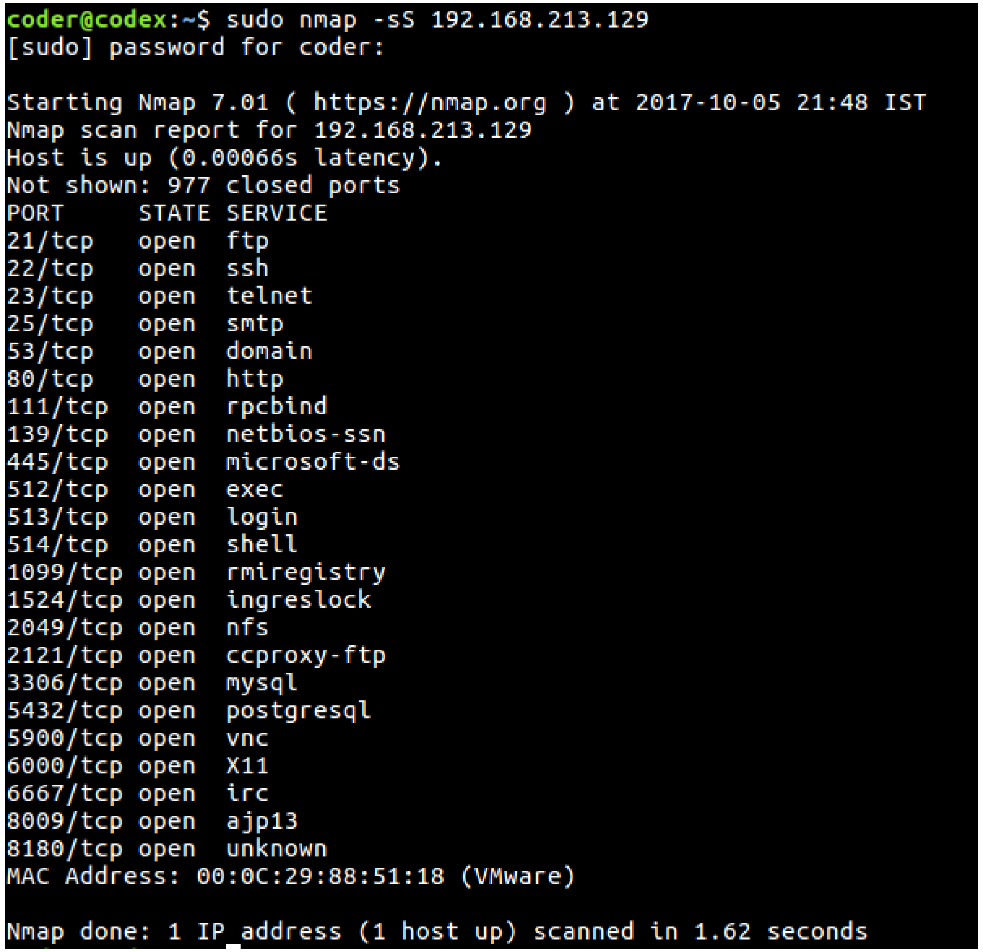
NMAP

- GUI Available
  - Zenmap
- Options
  - Port Scanning
    - Default: Scans the most common 1,000 ports for each protocol
    - Fast flag: Scan the 100 most common
  - Ping Scanning
    - IP address ranges
    - Subnet masks
    - Single IPs
  - Host Scans
    - Sends ARP requests (MAC address collection)
    - DNS queries
    - Latency information
  - Output to files

NMAP (cont'd)

- Port scans
  - TCP SYN: TCP handshake is not completed (avoids suspicion)
  - TCP connect: TCP handshake is completed (more reliable)
  - UDP: Identify DNS, SNMP, and DHCP ports
    - Frequently targeted by hackers
- OS Scans
  - Uses TCP and UDP Ports
  - Compares responses to database of over 2500 operating systems
    - Can return information about OS and version for each host

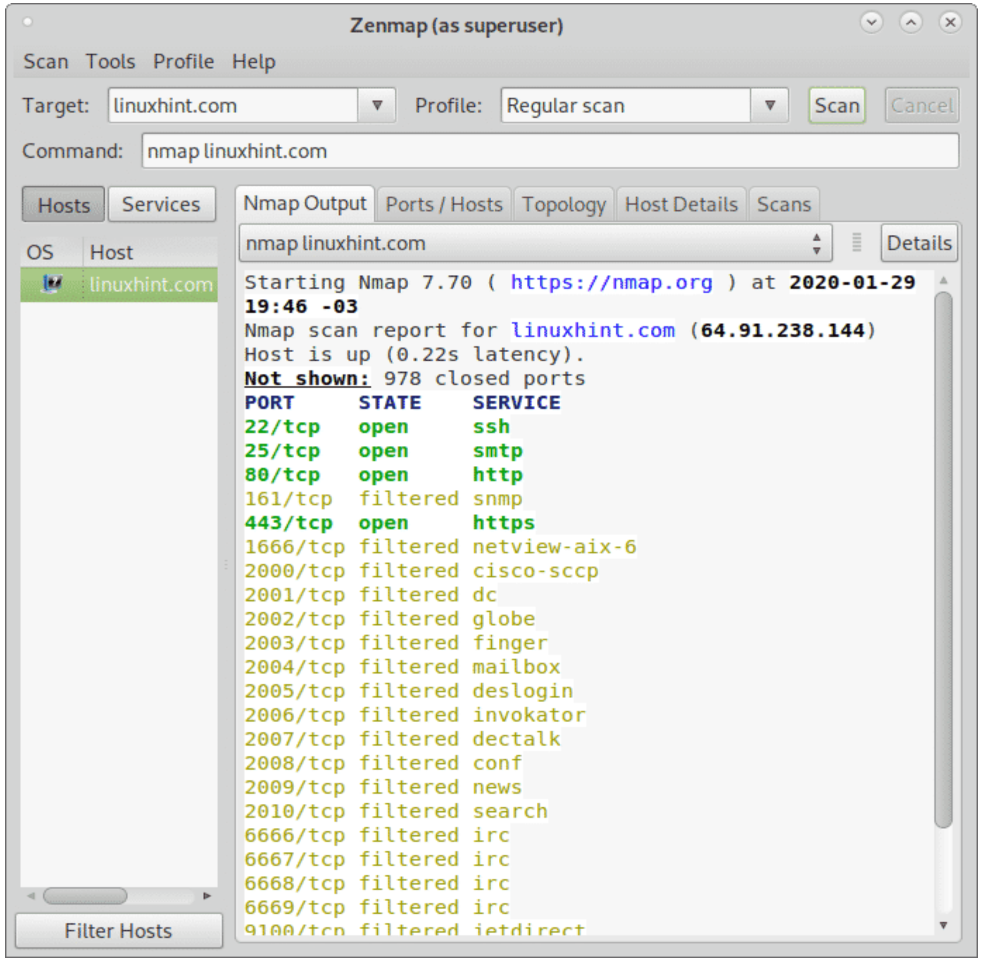
NMAP vs Zenmap



```
coder@codex:~$ sudo nmap -sS 192.168.213.129
[sudo] password for coder:

Starting Nmap 7.01 ( https://nmap.org ) at 2017-10-05 21:48 IST
Nmap scan report for 192.168.213.129
Host is up (0.00066s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 00:0C:29:88:51:18 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.62 seconds
```



Target: linuxhint.com

Profile: Regular scan

Command: nmap linuxhint.com

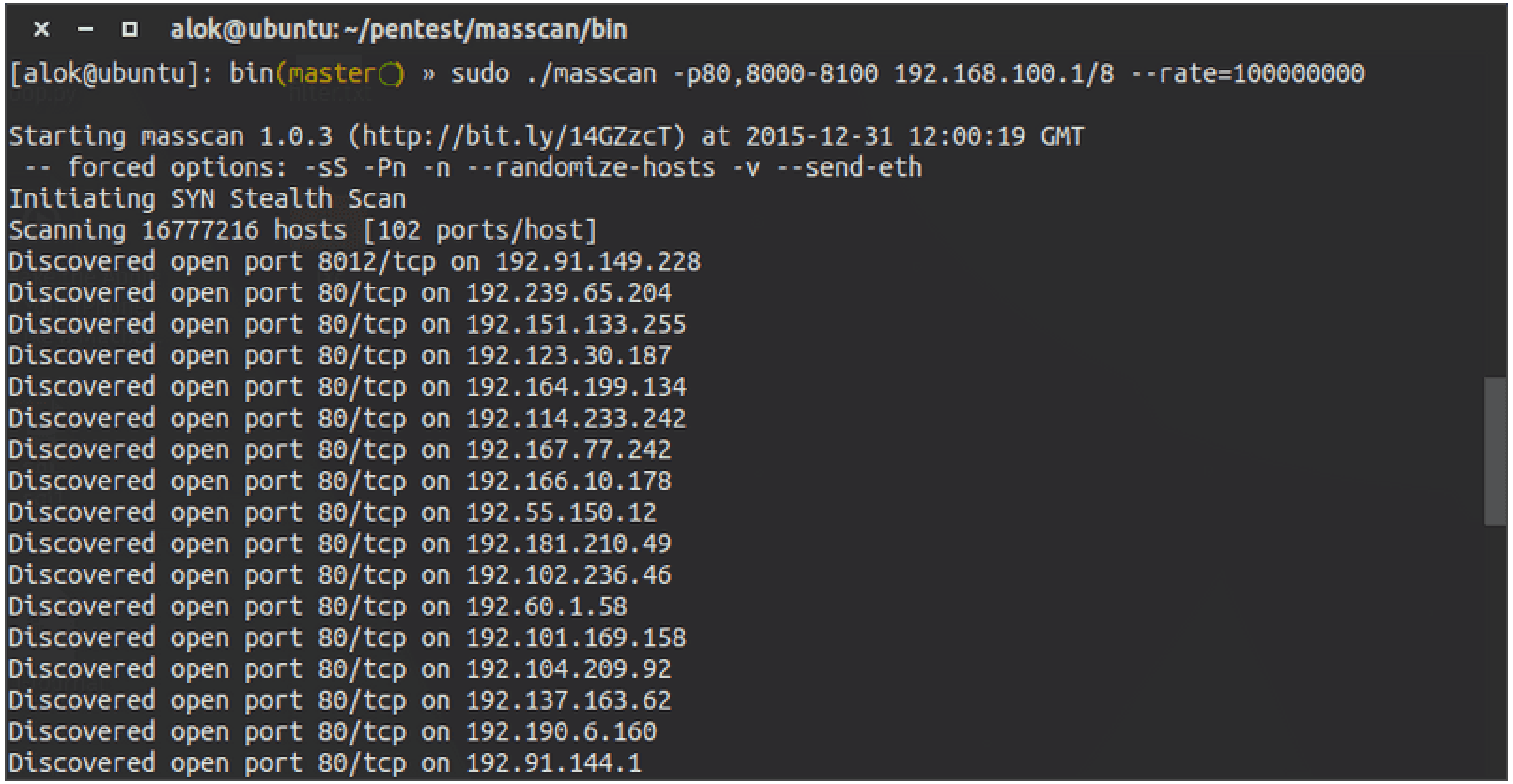
nmap linuxhint.com

```
Starting Nmap 7.70 ( https://nmap.org ) at 2020-01-29
19:46 -03
Nmap scan report for linuxhint.com (64.91.238.144)
Host is up (0.22s latency).
Not shown: 978 closed ports
PORT      STATE    SERVICE
22/tcp    open     ssh
25/tcp    open     smtp
80/tcp    open     http
161/tcp   filtered snmp
443/tcp   open     https
1666/tcp filtered netview-aix-6
2000/tcp filtered cisco-sccp
2001/tcp filtered dc
2002/tcp filtered globe
2003/tcp filtered finger
2004/tcp filtered mailbox
2005/tcp filtered deslogin
2006/tcp filtered invokator
2007/tcp filtered dectalk
2008/tcp filtered conf
2009/tcp filtered news
2010/tcp filtered search
6666/tcp filtered irc
6667/tcp filtered irc
6668/tcp filtered irc
6669/tcp filtered irc
9100/tcp filtered jetdirect
```

Masscan

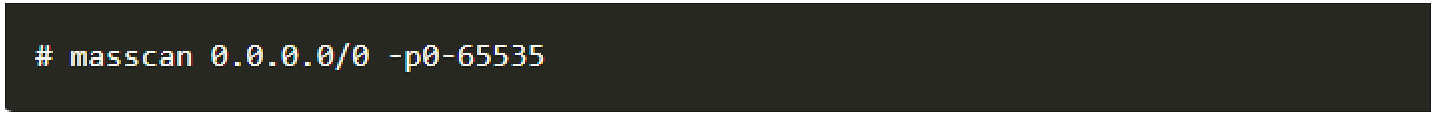
- Two types of port scanners
  - Synchronous (connection-oriented)
    - Send request to target port and waits for response or time-out
    - Slower
    - More accurate
  - Asynchronous (connectionless
    - Does not wait for response prior to sending out next port probe
    - Less accurate – can’t detect dropped packets
- Masscan is incredibly fast (asynchronous scanner)
  - Can facilitate DoS attacks
  - Said to be able to scan the entire internet in 6 minutes
    - 10 million packets per second

Masscan Examples



```
[alok@ubuntu]: bin(master○) » sudo ./masscan -p80,8000-8100 192.168.100.1/8 --rate=100000000

Starting masscan 1.0.3 (http://bit.ly/14GZzcT) at 2015-12-31 12:00:19 GMT
 -- forced options: -sS -Pn -n --randomize-hosts -v --send-eth
Initiating SYN Stealth Scan
Scanning 16777216 hosts [102 ports/host]
Discovered open port 8012/tcp on 192.91.149.228
Discovered open port 80/tcp on 192.239.65.204
Discovered open port 80/tcp on 192.151.133.255
Discovered open port 80/tcp on 192.123.30.187
Discovered open port 80/tcp on 192.164.199.134
Discovered open port 80/tcp on 192.114.233.242
Discovered open port 80/tcp on 192.167.77.242
Discovered open port 80/tcp on 192.166.10.178
Discovered open port 80/tcp on 192.55.150.12
Discovered open port 80/tcp on 192.181.210.49
Discovered open port 80/tcp on 192.102.236.46
Discovered open port 80/tcp on 192.60.1.58
Discovered open port 80/tcp on 192.101.169.158
Discovered open port 80/tcp on 192.104.209.92
Discovered open port 80/tcp on 192.137.163.62
Discovered open port 80/tcp on 192.190.6.160
Discovered open port 80/tcp on 192.91.144.1
```



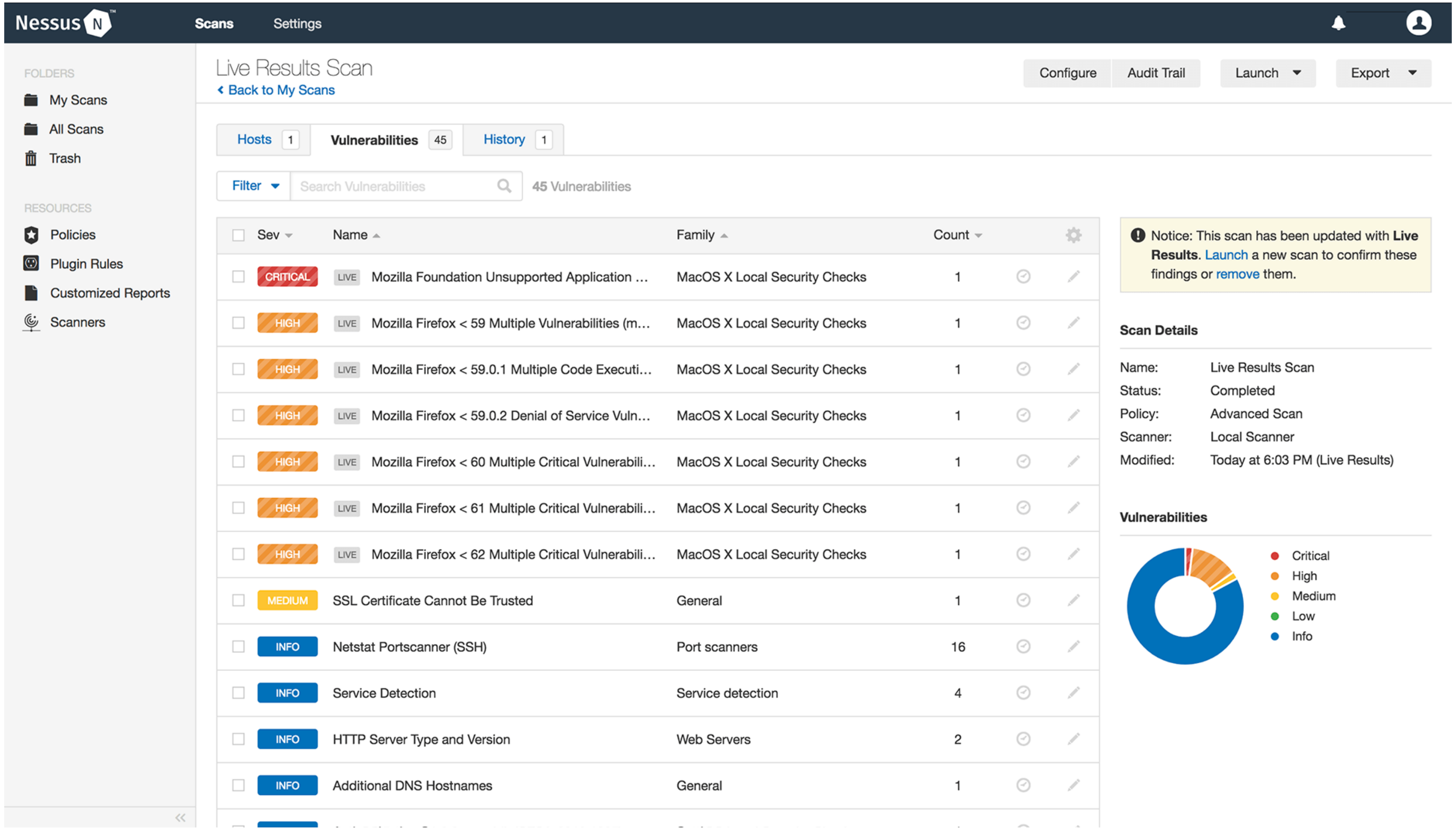
```
# masscan 0.0.0.0/0 -p0-65535
```

Source: https://www.computersnyou.com/5390/scan-whole-network-quickly/

Vulnerability Scanners

- More focused search
  - Use information from other reconnaissance to specify targets
  - Identify known vulnerabilities on hosts and network devices
- OpenVAS options
  - Full Scan
  - Web Server Scan
  - WordPress Scan
  - Joomla Scan

Nessus Example



Live Results Scan

‹ Back to My Scans

45 Vulnerabilities

Sev	Name	Family	Count
CRITICAL	LIVE Mozilla Foundation Unsupported Application ...	MacOS X Local Security Checks	1
HIGH	LIVE Mozilla Firefox < 59 Multiple Vulnerabilities (m...	MacOS X Local Security Checks	1
HIGH	LIVE Mozilla Firefox < 59.0.1 Multiple Code Executi...	MacOS X Local Security Checks	1
HIGH	LIVE Mozilla Firefox < 59.0.2 Denial of Service Vuln...	MacOS X Local Security Checks	1
HIGH	LIVE Mozilla Firefox < 60 Multiple Critical Vulnerabili...	MacOS X Local Security Checks	1
HIGH	LIVE Mozilla Firefox < 61 Multiple Critical Vulnerabili...	MacOS X Local Security Checks	1
HIGH	LIVE Mozilla Firefox < 62 Multiple Critical Vulnerabili...	MacOS X Local Security Checks	1
MEDIUM	SSL Certificate Cannot Be Trusted	General	1
INFO	Netstat Portscanner (SSH)	Port scanners	16
INFO	Service Detection	Service detection	4
INFO	HTTP Server Type and Version	Web Servers	2
INFO	Additional DNS Hostnames	General	1

Notice: This scan has been updated with **Live Results**. Launch a new scan to confirm these findings or remove them.

Scan Details

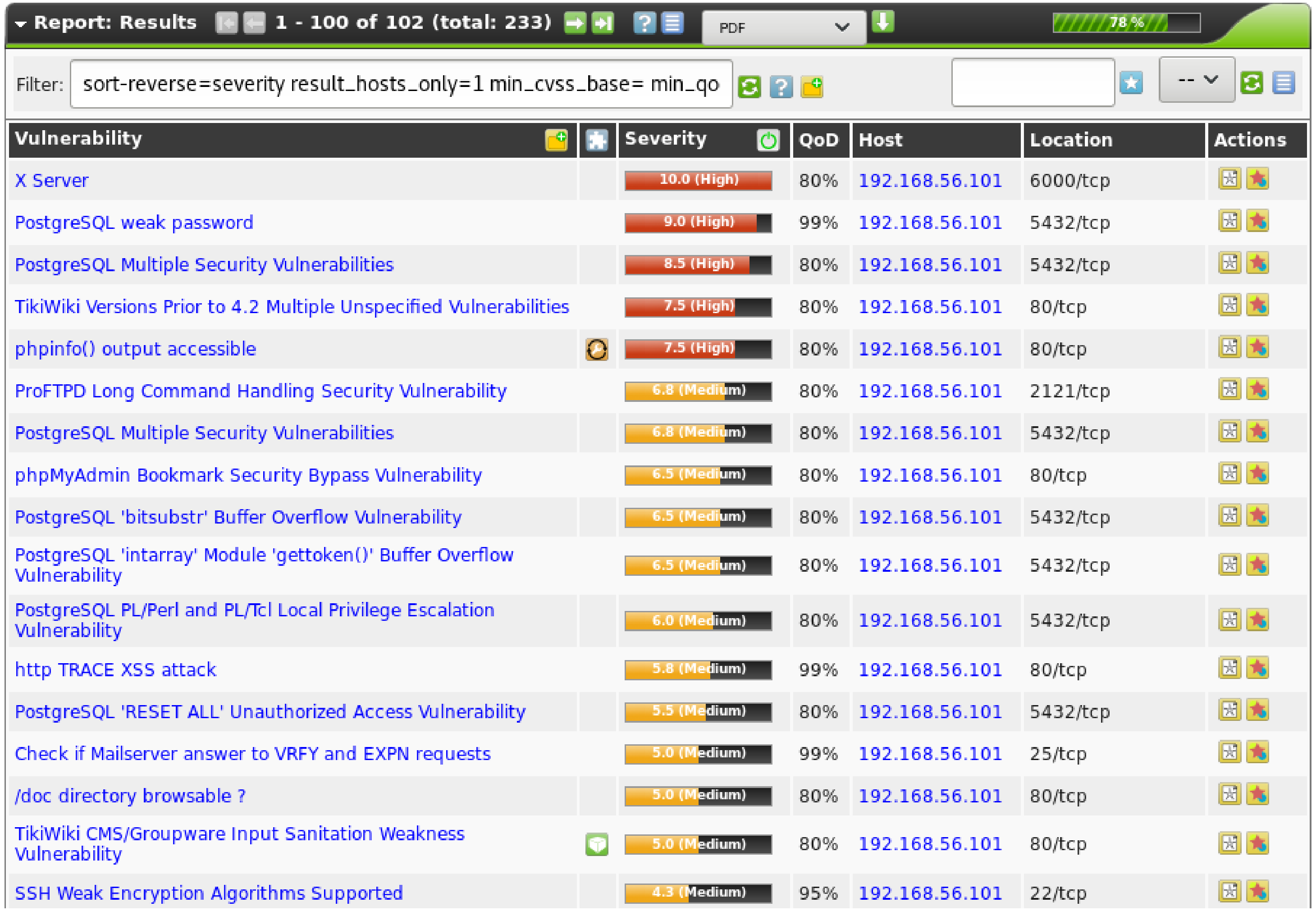
Name:	Live Results Scan
Status:	Completed
Policy:	Advanced Scan
Scanner:	Local Scanner
Modified:	Today at 6:03 PM (Live Results)

Vulnerabilities

- ● Critical
- ● High
- ● Medium
- ● Low
- ● Info

Source: https://tanable.com/products/nessus

OpenVAS Example



Report: Results 1 - 100 of 102 (total: 233)

Filter: sort-reverse=severity result_hosts_only=1 min_cvss_base= min_qo

Vulnerability		Severity	QoD	Host	Location	Actions
X Server		10.0 (High)	80%	192.168.56.101	6000/tcp	
PostgreSQL weak password		9.0 (High)	99%	192.168.56.101	5432/tcp	
PostgreSQL Multiple Security Vulnerabilities		8.5 (High)	80%	192.168.56.101	5432/tcp	
TikiWiki Versions Prior to 4.2 Multiple Unspecified Vulnerabilities		7.5 (High)	80%	192.168.56.101	80/tcp	
phpinfo() output accessible		7.5 (High)	80%	192.168.56.101	80/tcp	
ProFTPD Long Command Handling Security Vulnerability		6.8 (Medium)	80%	192.168.56.101	2121/tcp	
PostgreSQL Multiple Security Vulnerabilities		6.8 (Medium)	80%	192.168.56.101	5432/tcp	
phpMyAdmin Bookmark Security Bypass Vulnerability		6.5 (Medium)	80%	192.168.56.101	80/tcp	
PostgreSQL 'bitsubstr' Buffer Overflow Vulnerability		6.5 (Medium)	80%	192.168.56.101	5432/tcp	
PostgreSQL 'intarray' Module 'gettoken()' Buffer Overflow Vulnerability		6.5 (Medium)	80%	192.168.56.101	5432/tcp	
PostgreSQL PL/Perl and PL/Tcl Local Privilege Escalation Vulnerability		6.0 (Medium)	80%	192.168.56.101	5432/tcp	
http TRACE XSS attack		5.8 (Medium)	99%	192.168.56.101	80/tcp	
PostgreSQL 'RESET ALL' Unauthorized Access Vulnerability		5.5 (Medium)	80%	192.168.56.101	5432/tcp	
Check if Mailserver answer to VRFY and EXPN requests		5.0 (Medium)	99%	192.168.56.101	25/tcp	
/doc directory browsable ?		5.0 (Medium)	80%	192.168.56.101	80/tcp	
TikiWiki CMS/Groupware Input Sanitation Weakness Vulnerability		5.0 (Medium)	80%	192.168.56.101	80/tcp	
SSH Weak Encryption Algorithms Supported		4.3 (Medium)	95%	192.168.56.101	22/tcp	

Source: https://www.rapid7.com/blog/post/2016/11/22/how-to-use-openvas-to-audit-the-security-of-your-network-22/

Exploitation

- Can begin while reconnaissance is still ongoing
  - More reconnaissance is needed after successful exploitation
  - Time constraints are always of concern
- Opportunistic approach
  - Chase whatever leads become available
  - Prioritize based on sensitivity and criticality
- Human-hacking
  - Use information gained from reconnaissance to guess passwords or used exposed ones
  - Use known personal information to fool an employee or one of their relations
- Find lateral avenues to continue testing

Escalation

- Privilege escalation
  - e.g. Dirty Pipe
  - Allows for additional lateral or local movement
- Continually search for new opportunities
  - Access to new devices or credentials offer potential pathways
  - Different VLANs, IP addresses, or devices have access to different network resources
- Establish persistent access
  - Reverse shells
  - VNC servers
  - Firewall rule changes
  - “Malicious” software

Summary

- Stages of a penetration test
  - You must protect yourself and your organization by properly scoping and agreeing to terms with your customer
  - There are many different reconnaissance techniques that can be used by a penetration tester depending on the established RoE
- Creativity is key
- There are open source versions of most penetration testing tools