CySA+

Cybersecurity Analyst

CCI
Post Office Box 9627
Mississippi State, MS 39762

CySA+

Part 1

Threat Management

Applying Reconnaissance Techniques

Chapter 1

Outline

- Open Source Intelligence
- Active Reconnaissance
- Special Considerations
- Tools of the Trade

Open Sources Intelligence

- If possible, adversaries will get as much information indirectly before attempting any type of direct approach
- Passive Reconnaissance
  - Process of obtaining information without coming in direct interaction with the network or device
- Open Source Intelligence (OSINT)
  - Information from third parties that have been obtained legitimately
    - E.g. Job sites
    - E.g. Social Media sites

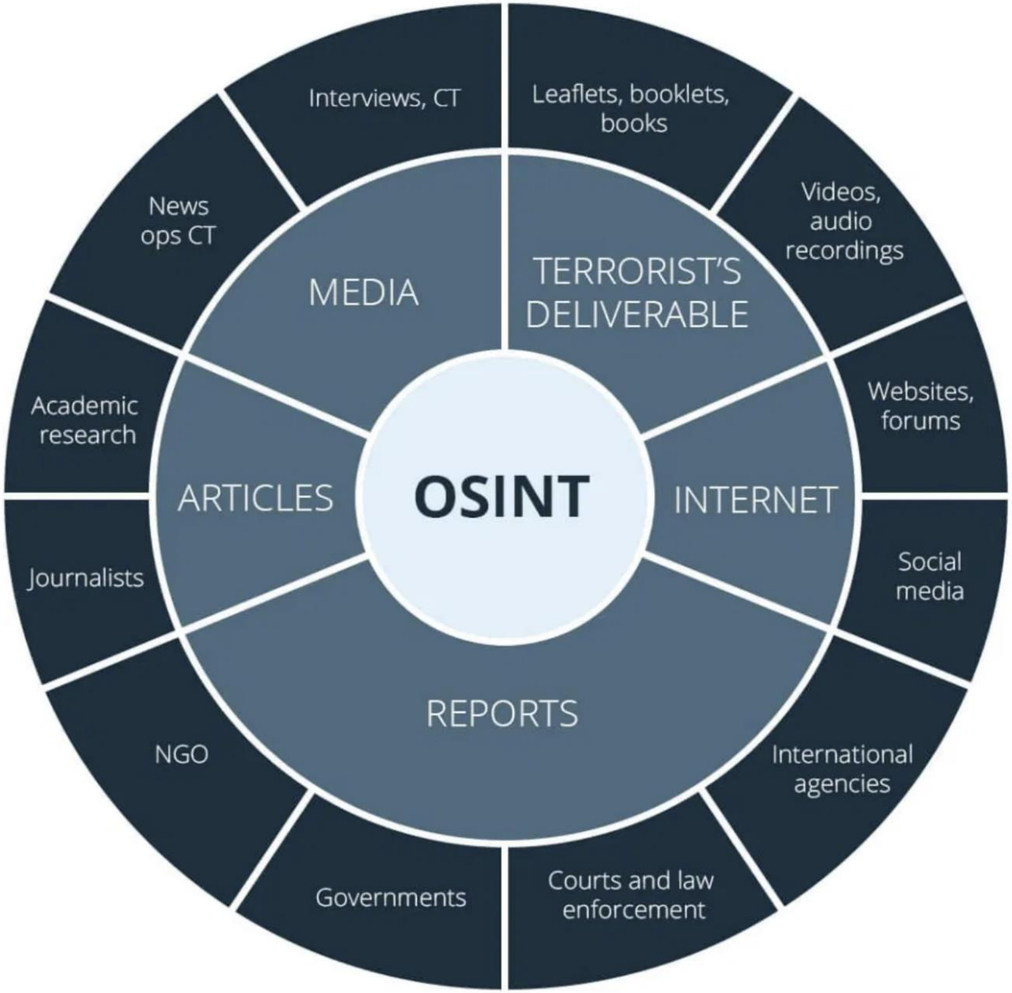
[1]

Open Sources Intelligence

- There are several different Google operators that make searching for open-source information easier
  - Here are a few
    - "site:"
      - Restricts search results to the specified domain or site
      - E.g. site:apache.org
    - "intitle:"
      - Restricts search results to pages with the indicated text in their title
      - E.g. intitle:vitae
    - "cache:"
      - Restricts search results to Google's latest cached copies of the results
      - E.g. cache:www.eff.org

[1]

Open Sources Intelligence Examples



[7]

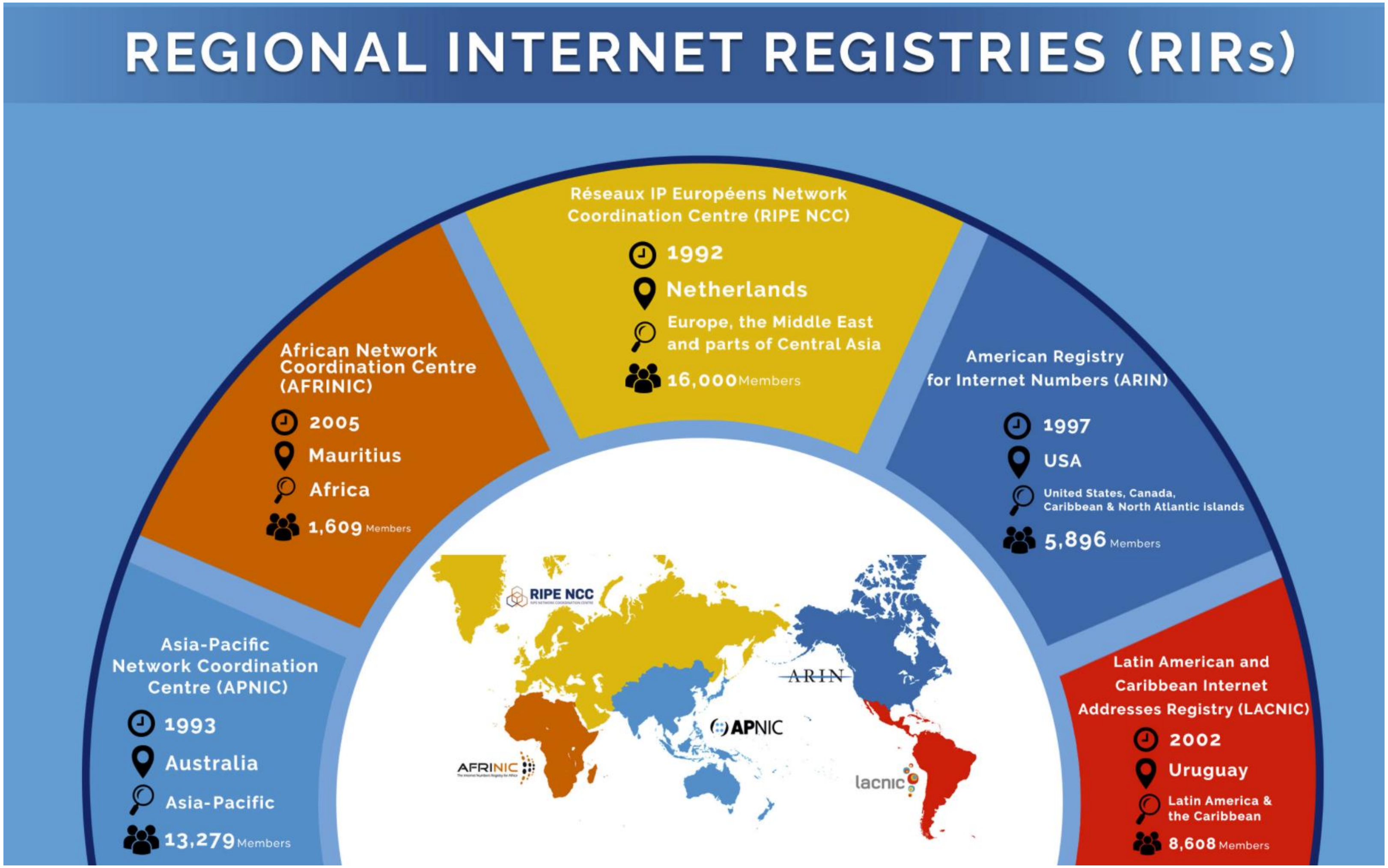
Various OSINT information sources

Regional Internet Registries

- Internet Registries ensure IP addresses and domain names are globally unique
- Regional Internet Registries (RIRs) consist of five separate corporations that control the assignment of IP addresses throughout the world
- Each is responsible for a geographical area
  - For example, the American Registry for Internet Numbers (ARIN) is responsible for Canada, the United States, and most of the Caribbean
- Domain Name System (DNS)
  - this system maps domain names to their server's IP address and vice versa

[1]

(RIRs) MAP



REGIONAL INTERNET REGISTRIES (RIRs)

Réseaux IP Européens Network Coordination Centre (RIPE NCC)

- 1992
- Netherlands
- Europe, the Middle East and parts of Central Asia
- 16,000 Members

African Network Coordination Centre (AFRINIC)

- 2005
- Mauritius
- Africa
- 1,609 Members

American Registry for Internet Numbers (ARIN)

- 1997
- USA
- United States, Canada, Caribbean & North Atlantic islands
- 5,896 Members

Asia-Pacific Network Coordination Centre (APNIC)

- 1993
- Australia
- Asia-Pacific
- 13,279 Members

Latin American and Caribbean Internet Addresses Registry (LACNIC)

- 2002
- Uruguay
- Latin America & the Caribbean
- 8,608 Members

[8]

Domain Name System

- DNS data can be used to map an entire network
  - Ensure only authorized hosts are allowed to request full transfers
- DNS harvesting
  - Command-line tools such as nslookup, host, and dig are used by admin to troubleshoot DNS and network problems
  - These same tools can be automated by advisories to harvest DNS server data
- Zone transfer
  - Replicate the contents of a DNS server across multiple DNS servers
  - Never allow zone transfers to unrecognized devices

[1]

Domain Name System

- A registered domain has publicly alleviable details about its registrant's organization
  - Such as name, telephone number, email contact information, domain name system details, and mailing address
- A registered domain's information can be acquired using WHOIS
  - WHOIS is available as a command-line tool and has a web-based version too
  - Useful tool for incident responders and network engineers
  - Also a useful tool for adversaries to gather personal and technical information

[1]

Open Sources Intelligence

- Job Sites
  - Usually have user-provided personal data
  - Email harvesting from these sites allows advisories to craft more convincing phishing emails
  - Companies are also at risk due to the information they provide about the listed jobs needed
- Social Media sites
  - Media Profiling
    - Gathering information from personal social media pages and using that information to build a profile of the target's preferences and patterns to determine the user's actions
  - Social engineering attacks
    - Uses the data from media profiling to trick the target into giving out sensitive information

[1]

Active Reconnaissance

- Unlike OSINT, Active Reconnaissance engages with the target to gain more information
- Here are a few active reconnaissance techniques
  - Scanning
  - Network Mapping
  - Port Scanning
  - Web App Vulnerability Scanning
  - Packet Capturing

[1]

Scanning

- Scanning
  - Used to gather more details about a target system
  - Such as pinging a device and noting its response
- War Dialing
  - A scanning method used at the beginning of the internet to find weaknesses
  - This method would automatically call a list of phone numbers and listen to the response to determine if it was human or machine
  - This method exploited unprotected modems and was one of the easiest ways at the time to gain access to a system

[1]

Scanning

- Host Scanning
  - Is an effective way to inventory and discover details of a system
  - This is done by sending a message to a system and depending on the response of that system if more exploratory measures are taken or if it is inventoried
- Scanners
  - Network Mappers
  - Host or Port Scanners
  - Web app vulnerability Scanners

[1]

Network Mapping

- The purpose of network mapping is to understand the topology of the target network
  - Such as the perimeter networks, the demilitarized zones, and key network devices
- Topology Discovery
  - Actions that are used to map out a network
- Nmap
  - A tool that finds existing device on the target network
  - Default behavior is to send a
    - ICMP Echo Request
    - TCP SYN to port 443
    - TCP ACK to port 80
    - ICMP Timestamp Request

[1]

Port Scanning

- **Port Scanner**
  - These types of programs probe servers and/or hosts for open ports
  - Devices often run services from common ports, such as port 80 and port 25
- **Service Discovery**
  - By using a port scanner an admin can discover the different service ports a host has to offer
  - Attackers can use these same tools for service discovery
- **OS fingerprinting**
  - Some port scanning tools can identify the operating system of the target device, but this is not reliable

[1]

Web App Vulnerability Scanning

- **Web application vulnerability scanner**
  - A tool that automatically scans web apps for security vulnerabilities
  - Useful for developers to test the security of their web app before deployment
  - Also useful for an attacker to find weaknesses in a target web application
- **Common Vulnerability Scans**
  - SQL injection
  - Command injection
  - Cross-site scripting
  - Improper server configurations

[1]

Capturing Packets

- Packets
  - A packet consists of a header and the payload
    - The header of a packet contains information about
      - The data in transition
      - The source and destination of the communicating hosts
    - The payload contains
      - A portion of the data that is in transition
      - Passwords, images, text, and sound can all be exposed if not encrypted
- IPv4 and IPv6
  - IPv4 header size various between 20 and 60 bytes
  - IPv6 header has a fixed size of 40 bytes
  - Total max packet size for IPv4 and IPv6 is 65,535 bytes

[1]

Capturing Packets

- Full Capture vs. Header Capture
  - More storage space is necessary for full packet capture than header capture
  - Cannot reconstruct data with just header information such as text, video, audio, or images
- Network Analyzer (aka packet sniffer)
  - Wireshark is a popular network analyzer
  - TShark is the command-line version of Wireshark
  - Promiscuous mode allows the host machine to listen to all network traffic
  - Captures the raw traffic on a network
  - Can log and store the packet header or the full packet

[1]

Special Considerations

- **Before conducting an active reconnaissance several variables that must be considered first**
  - **Is the target on a wired or wireless network**
  - **Is the target on a virtual or physical infrastructure**
  - **Is the target on an internal or external host**
  - **Does the target have an on-premises setup or a cloud environment**

[1]

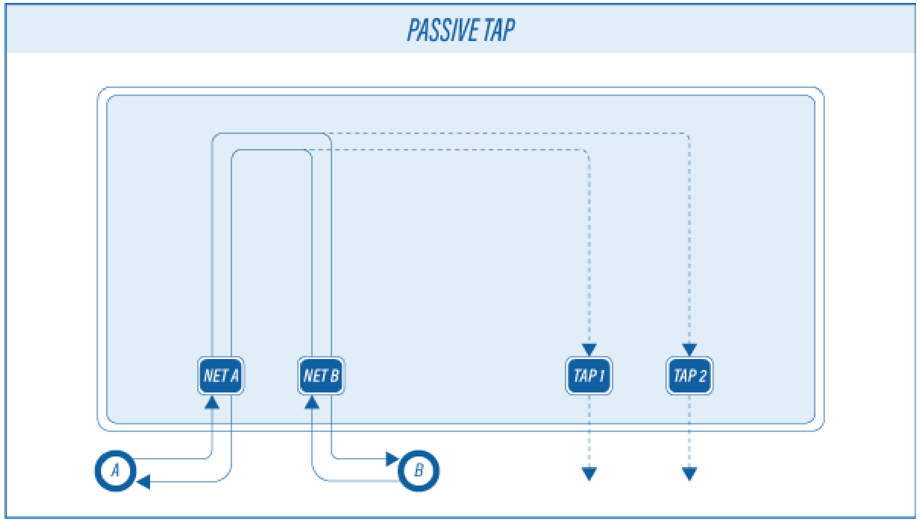
Wired Network Considerations

- Wired networks require physical proximity to gather information from them and are more secure than wireless networks because of this
  - However, hosts connected to a wired network are vulnerable through the open internet
- Wired Network Consideration
  - Taps
  - Hubs
  - Switches

[1]

Taps

- **Passive Tap**
  - **Requires no additional power**
  - **Has a direct connection to the wires in the copper cable**
  - **Power still flows to the intended destination, but enough of the signal is split to be useful to a sniffer**
- **Passive Optical Tap**
  - **The light beam in the fiberoptic cable is split so that the signal is diverted to a sensor**
  - **When on a Gigabit speed line there can be a high error rate, distortion, or failure**

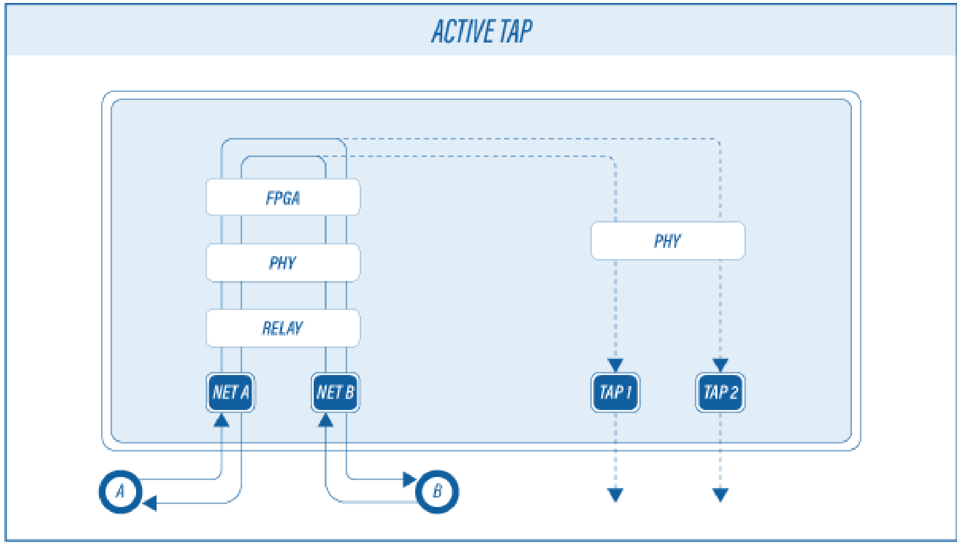


[2]

[1]

Taps

- Active Tap (Active Relay)
  - Requires extra power
  - The two destinations, A and B, are physically separated
  - Creates a copy of the signal sends it to the tap
  - Sends the original signal to its destination
  - If the tap fails, this will alert the admin



[2]

[1]

Hubs

- Hub
  - A network device that connects multiple host machines
  - All messages sent through a Hub are; also sent to any host machine connected to that Hub
  - Hubs are rare and are being replaced by Switches
- Exploits
  - Can connect a monitoring machine to the Hub and start the capturing software to collect data
  - An attacker might introduce a Hub at the chokepoint of a network to capture the network traffic.

[1]

Switches

- Switch
  - Much like a Hub, sends messages from one host to another
  - Unlike a Hub, a Switch knows where to send the packages by using MAC addresses
- Address Resolution Protocol (ARP) tables
  - Are used to map MAC addresses to their IP addresses
  - Are maintained by each host machine
  - Are inherently trusted
- When a host machine sends a message to an IP address, it looks up the corresponding MAC address in the host's ARP table.
- If a host does not know the MAC address for a given IP address the Switch will send an ARP request to each host machine.

[1]

Switches

- **ARP Poisoning**
  - Two methods to sniff traffic in a switched environment
    - Sending a stream of ARP replies to stress the Switch
    - Changing the mapped MAC address in a host’s ARP table to the attacker’s MAC address
  - Can be used for a Man-in-the-middle(MITM) Attack
    - Where an attacker captures data from host A modifies the data and sends it to host B
- **Mirroring**
  - Port mirroring replicates traffic from one or more ports and the data to separate output ports
  - Used to troubleshoot network problems
  - An attacker with Switch access can use port mirroring to collect all traffic passing through the Switch

[1]

Wireless Network Considerations

- **Wireless Network**
  - **Uses radio frequency (RF) data communication to access the network**
  - **Not as secure as wired networks because**
    - **There is no way to limit the admitted network signal**
    - **Any network traffic flowing over the signal can be observed**
- **Secure Wireless Networks**
  - **By encrypting any traffic passing between network devices**
    - **This method is not costly to employ**
    - **Any data collected by an attacker is useless**

[1]

Wireless Network Considerations

- Capturing traffic inside the wireless network
  - Must understand the relationship between host-to-access-point
  - Can use Wireshark to capture traffic
  - Promiscuous mode
    - Supported by many wireless cards
    - Allows clients to see all network traffic
- Capturing traffic outside the wireless network
  - Monitor mode
    - Wireless card must be able to operate in monitor mode for capture software to see 802.11 packets
    - Without being associated with any access points, an attacker can observe all 802.11 activity over multiple channels with monitor mode.

[1]

Virtualization Technologies

- Virtualization
  - Allows for multiple simulated environments on one physical device
  - Simulated environment can include CPUs, memory, networking, operating system, etc.
- Virtualization Technologies
  - Hypervisors
  - Containers
  - Cloud Computing

[1]

Hypervisors

- Hypervisors
  - Manages the physical hardware and handles sharing those resources across multiple virtual instances
- Type-1 hypervisor (aka. bare-metal hypervisors)
  - The hypervisor software runs directly on the host machine
  - The hypervisor manages guest operating systems and has access to the host machines hardware
  - Popular Type-1 hypervisors:
    - VMware vSphere with ESX, Microsoft Hyper-V, Kernel-based Virtual Machine(KVM)
- Type-2 hypervisor
  - Run within an existing operating system
  - Are like any other software application
  - Popular Type-2 hypervisor
    - VMware Player, VirtualBox, Parallels

[1]

Containers

- What are Containers
  - Virtual runtime environment
  - Runs on top of the OS kernel
  - Does not emulate the hardware but rather emulates an OS
  - Shares the resources provided by the host OS
- Use Cases
  - Allows for rapid development, giving developers a means to test code in multiple environments more quickly
  - Container Engines manage the deployment of containerized applications

[1] [3]

Docker Containers

[4]

Network Function Virtualization and Software-Defined Networking

- **Network Function Virtualization (NVF)**
  - Replacing custom hardware for network function with virtual clones
  - Essential component of high-volume servers and cloud computing resources
  - Relies on the automatic configuration and management of virtual resources, such as the management of traffic analysis and optimization
- **Software Defined Networks (SDN)**
  - The core of SDN is the management of network functionality, traffic analysis, and optimization
  - Pairs well with NVF since SDN is the management, while the NVF is the network architecture.

[1]

Cloud Computing

- Cloud Computing
  - Available hardware and software services enabled by high-performance distributed computing
  - These services are accessible through a network connection to the cloud service provider
  - These services are not physically located at the location of the organization
- Three Cloud Computing Types
  - Infrastructure as a Service (IaaS)
  - Platform as a Service (PaaS)
  - Software as a Service SaaS

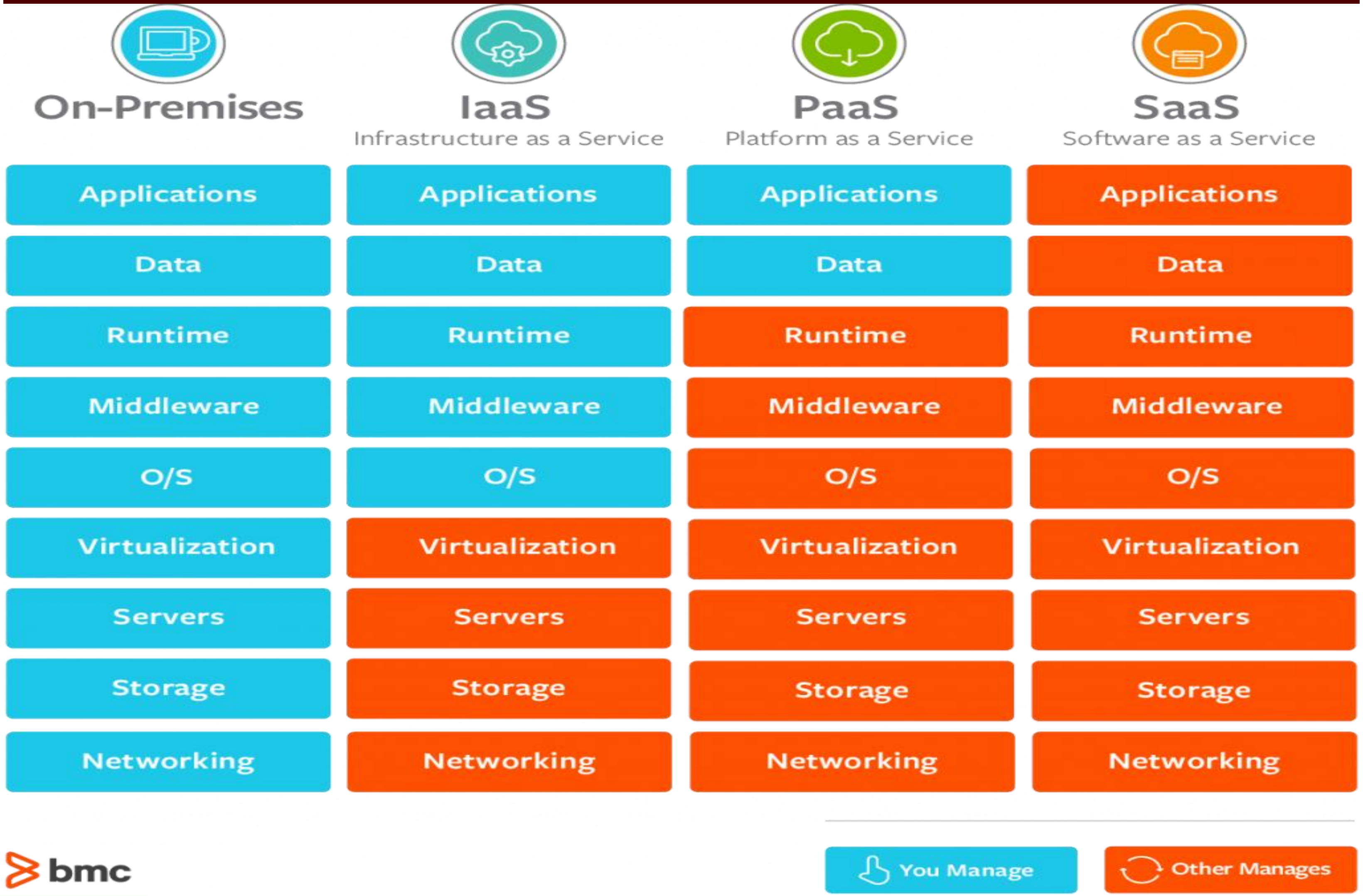
[1]

Cloud Computing

- IaaS
  - Complete admin control over the computing platform hosted by the cloud service provider
  - Cheaper for an organization to maintain
  - Organizations can more easily scale
- PaaS
  - Does not have complete admin control over the platform
  - The service provider is responsible for securing the platform
  - Great for development teams to develop, test, deploy, and maintain applications on a common environment
- SaaS
  - Users have access to the application hosted by the cloud service provider
  - Users are not responsible for installation, performing patches, or applying for updates
  - Software is managed by the service provider at a central location

[1]

Cloud Computing Chart



On-Premises	IaaS Infrastructure as a Service	PaaS Platform as a Service	SaaS Software as a Service
🟦 Applications	🟦 Applications	🟦 Applications	🟧 Applications
🟦 Data	🟦 Data	🟦 Data	🟧 Data
🟦 Runtime	🟦 Runtime	🟧 Runtime	🟧 Runtime
🟦 Middleware	🟦 Middleware	🟧 Middleware	🟧 Middleware
🟦 O/S	🟦 O/S	🟧 O/S	🟧 O/S
🟦 Virtualization	🟧 Virtualization	🟧 Virtualization	🟧 Virtualization
🟦 Servers	🟧 Servers	🟧 Servers	🟧 Servers
🟦 Storage	🟧 Storage	🟧 Storage	🟧 Storage
🟦 Networking	🟧 Networking	🟧 Networking	🟧 Networking

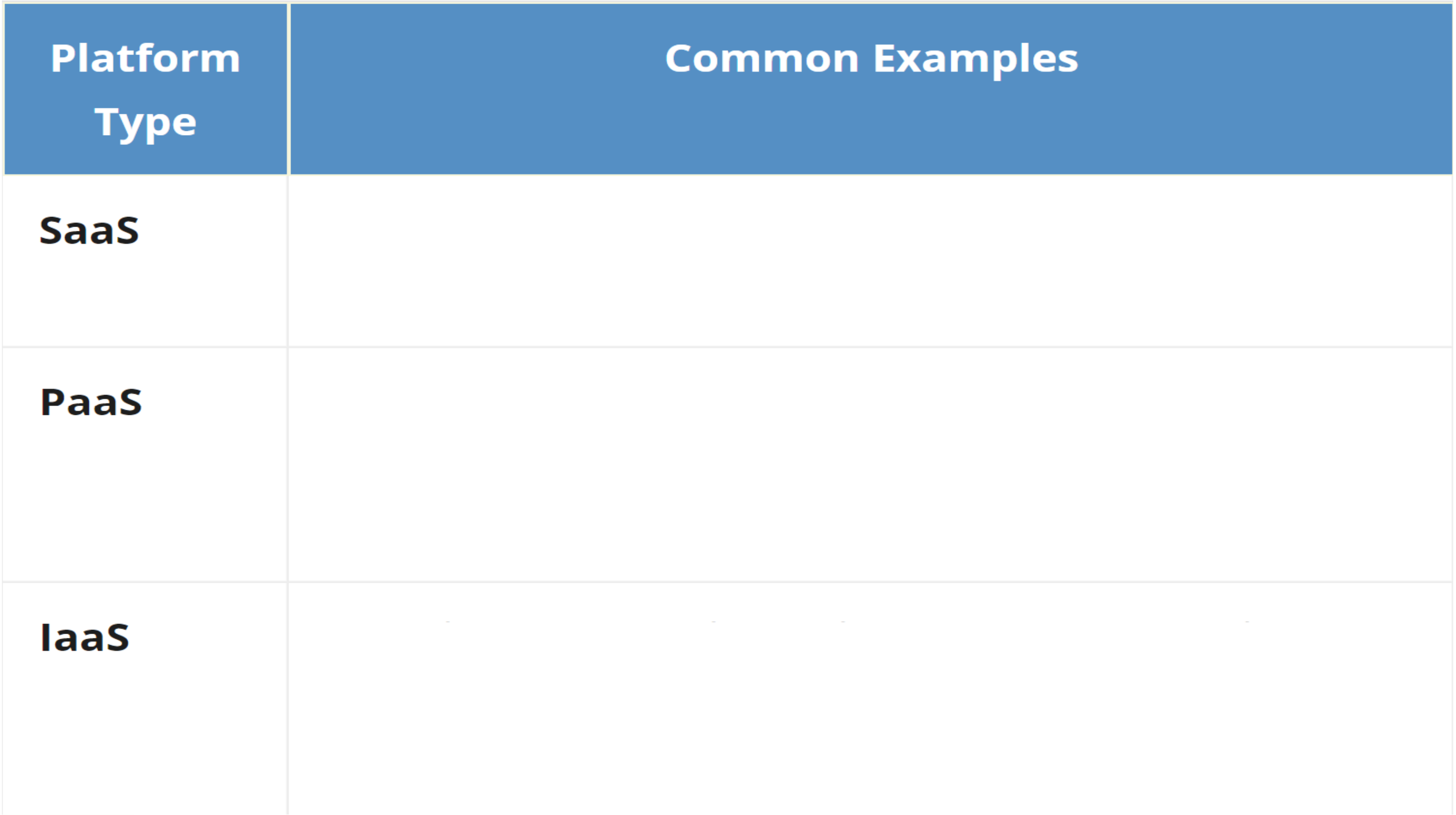
🟦 You Manage

🟧 Other Manages

[6]

Cloud Computing Interactive Ex

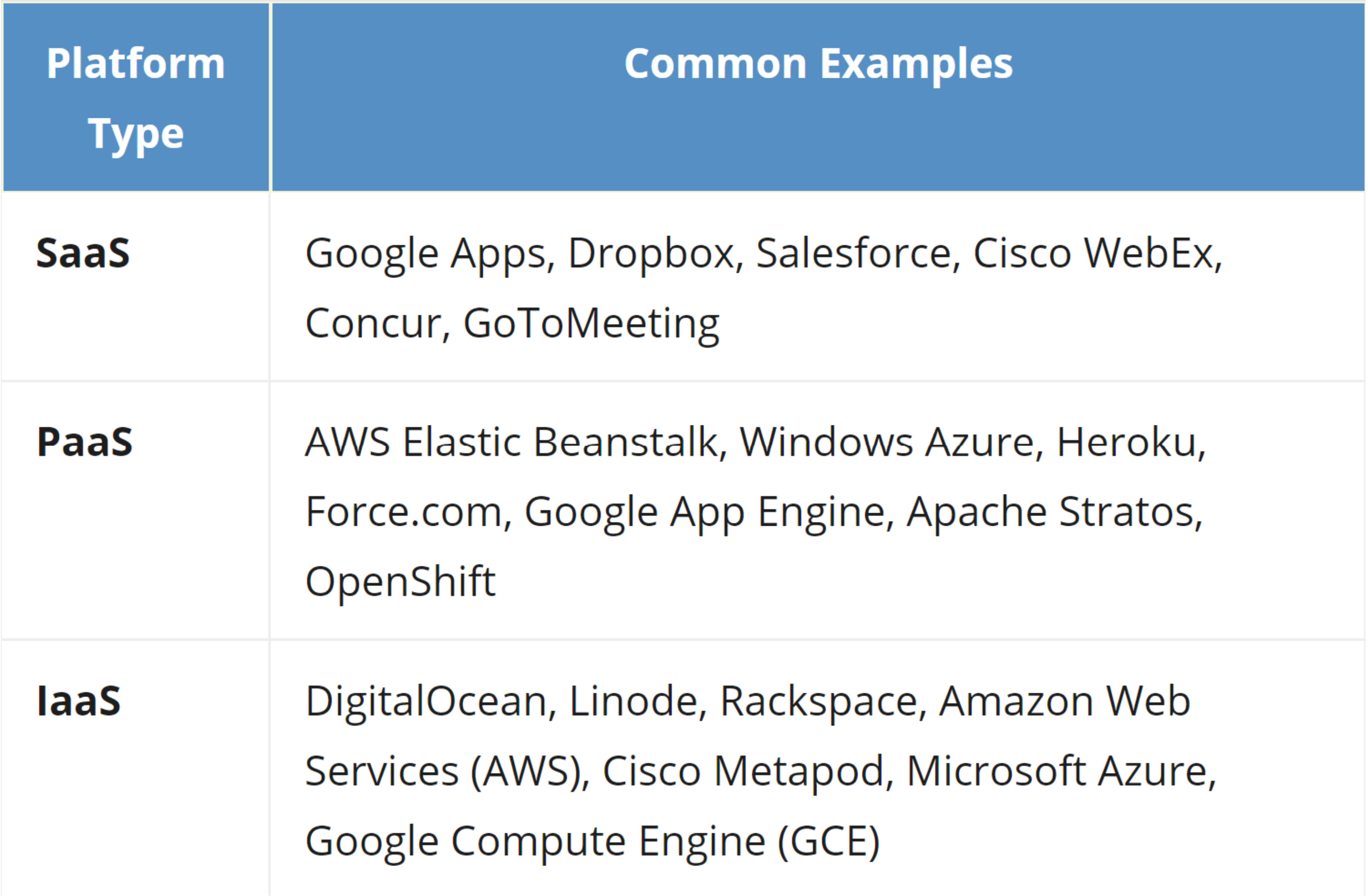
Brainstorm and list some of the common examples of each cloud computing types.



Platform Type	Common Examples
SaaS	
PaaS	
IaaS	

[6]

Cloud computing Interactive answers



Platform Type	Common Examples
SaaS	Google Apps, Dropbox, Salesforce, Cisco WebEx, Concur, GoToMeeting
PaaS	AWS Elastic Beanstalk, Windows Azure, Heroku, Force.com, Google App Engine, Apache Stratos, OpenShift
IaaS	DigitalOcean, Linode, Rackspace, Amazon Web Services (AWS), Cisco Metapod, Microsoft Azure, Google Compute Engine (GCE)

[6]

Defending Against Reconnaissance

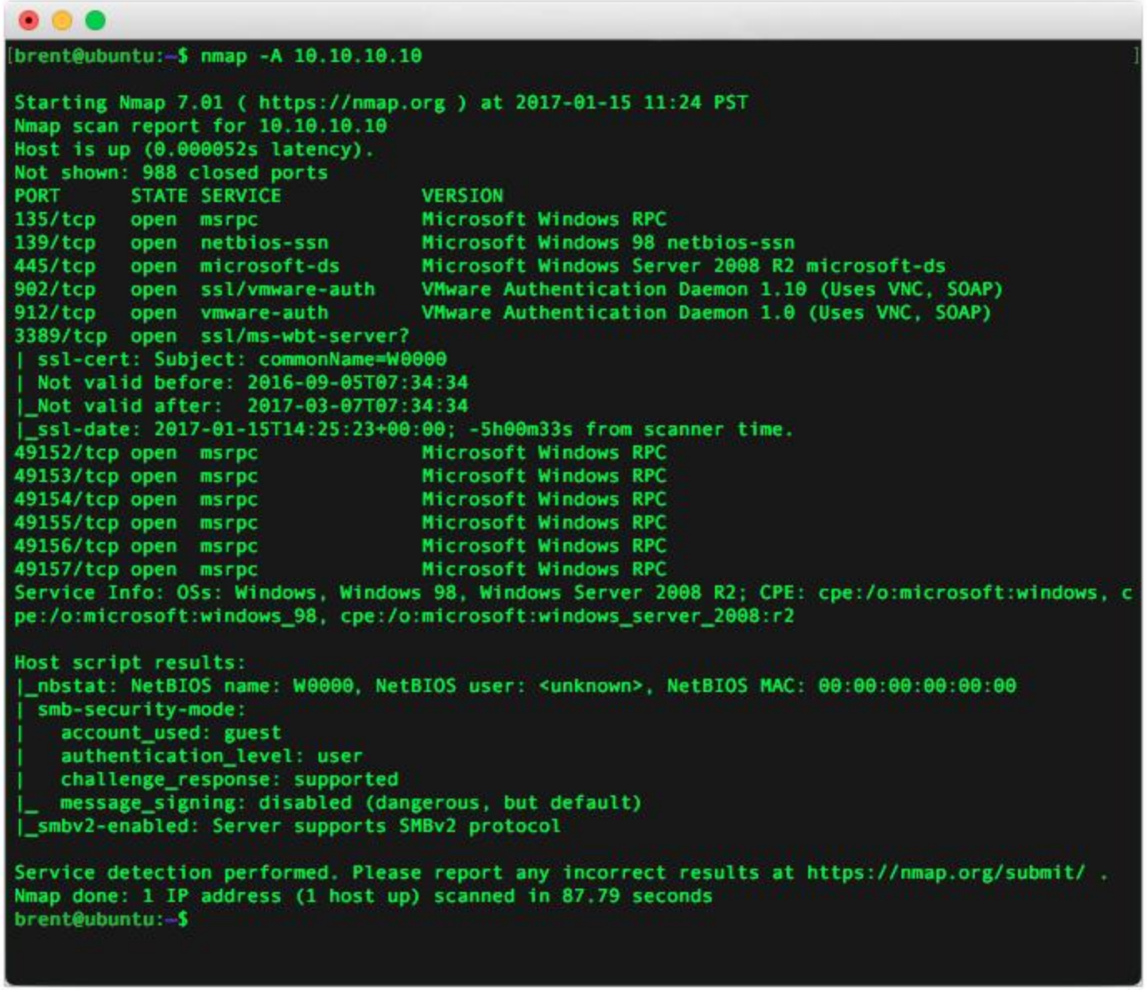
- **Vulnerability Scans**
  - **Finding vulnerabilities and remediating the risk**
- **Log Reviews**
  - **Looking for suspicious activity**
  - **Inspecting firewalls**
  - **Inspecting access-control list (ACL)**
  - **Syslogs**
    - **Thousands of system logs can be produced in a day**
    - **SIEM systems can assist in monitoring Syslogs**
- **Security Information and Event Management (SIEM)**
  - **Aggregates device logs**
  - **Detail monitoring**
  - **Correlates events**
  - **Provides a dashboard for users**

[1]

Tools of the Trade

- **Environmental reconnaissance tools**
  - **The listed tools are some of the more notable tools**
  - **Need to know these tools for the CySA+ exam**
- **Nmap**
  - **The standard for network scanning**
  - **Free software license for Linux, Windows, Mac OS, and various other systems**
  - **Features include port scanning, host discovery, version detection, and OS identification**

[1,10]



```
[brent@ubuntu:~$ nmap -A 10.10.10.10

Starting Nmap 7.01 ( https://nmap.org ) at 2017-01-15 11:24 PST
Nmap scan report for 10.10.10.10
Host is up (0.000052s latency).
Not shown: 988 closed ports
PORT      STATE SERVICE           VERSION
135/tcp   open  msrpc             Microsoft Windows RPC
139/tcp   open  netbios-ssn       Microsoft Windows 98 netbios-ssn
445/tcp   open  microsoft-ds      Microsoft Windows Server 2008 R2 microsoft-ds
902/tcp   open  ssl/vmware-auth   VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
912/tcp   open  vmware-auth       VMware Authentication Daemon 1.0 (Uses VNC, SOAP)
3389/tcp  open  ssl/ms-wbt-server?
| ssl-cert: Subject: commonName=W0000
| Not valid before: 2016-09-05T07:34:34
|_Not valid after:  2017-03-07T07:34:34
|_ssl-date: 2017-01-15T14:25:23+00:00; -5h00m33s from scanner time.
49152/tcp open  msrpc             Microsoft Windows RPC
49153/tcp open  msrpc             Microsoft Windows RPC
49154/tcp open  msrpc             Microsoft Windows RPC
49155/tcp open  msrpc             Microsoft Windows RPC
49156/tcp open  msrpc             Microsoft Windows RPC
49157/tcp open  msrpc             Microsoft Windows RPC
Service Info: OSs: Windows, Windows 98, Windows Server 2008 R2; CPE: cpe:/o:microsoft:windows, c
pe:/o:microsoft:windows_98, cpe:/o:microsoft:windows_server_2008:r2

Host script results:
|_nbstat: NetBIOS name: W0000, NetBIOS user: <unknown>, NetBIOS MAC: 00:00:00:00:00:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smbv2-enabled: Server supports SMBv2 protocol

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 87.79 seconds
brent@ubuntu:~$
```

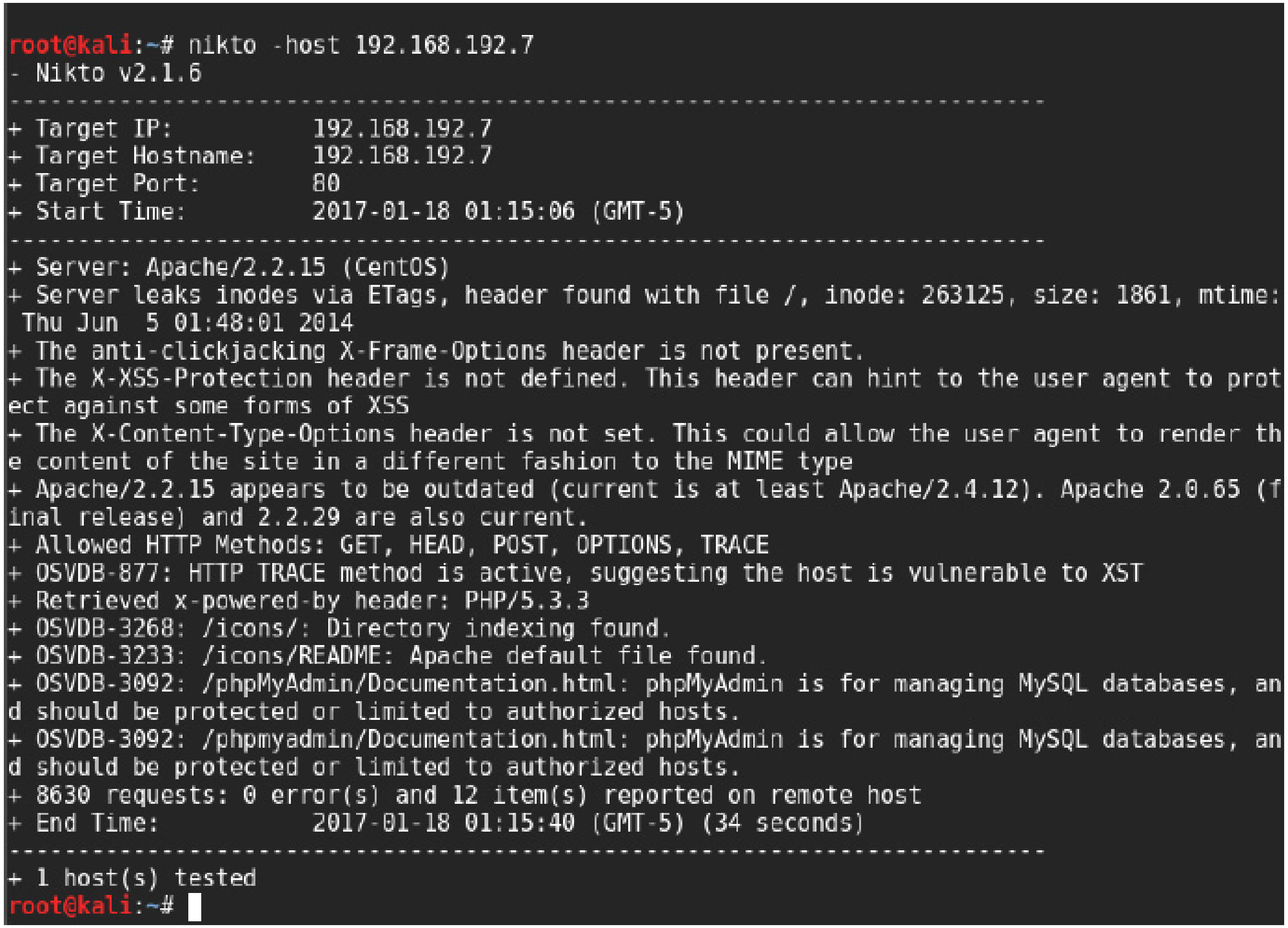
Nmap

In the above example shows nmap searching a device for open ports using command-line

Tools of the Trade

- **Nikto**
  - Open-source software that is well supported
  - Active reconnaissance tool
  - Runs thousands of tests to scan for web server vulnerabilities
  - Provides an assessment of offending files and a reference to the OSVDB
- **Open Source Vulnerability Database (OSVDB)**
  - Gives detail information on open source vulnerabilities
  - OSVDB has since been disbanded, but referential materials and commercial licenses are still available

[1]



```
root@kali:~# nikto -host 192.168.192.7
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.192.7
+ Target Hostname:    192.168.192.7
+ Target Port:        80
+ Start Time:         2017-01-18 01:15:06 (GMT-5)
---------------------------------------------------------------------------
+ Server: Apache/2.2.15 (CentOS)
+ Server leaks inodes via ETags, header found with file /, inode: 263125, size: 1861, mtime:
 Thu Jun  5 01:48:01 2014
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to prot
ect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render th
e content of the site in a different fashion to the MIME type
+ Apache/2.2.15 appears to be outdated (current is at least Apache/2.4.12). Apache 2.0.65 (f
inal release) and 2.2.29 are also current.
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ Retrieved x-powered-by header: PHP/5.3.3
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ OSVDB-3092: /phpMyAdmin/Documentation.html: phpMyAdmin is for managing MySQL databases, an
d should be protected or limited to authorized hosts.
+ OSVDB-3092: /phpmyadmin/Documentation.html: phpMyAdmin is for managing MySQL databases, an
d should be protected or limited to authorized hosts.
+ 8630 requests: 0 error(s) and 12 item(s) reported on remote host
+ End Time:           2017-01-18 01:15:40 (GMT-5) (34 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
root@kali:~# 
```

Nikto

In the above example Nikto has reported several possible vulnerabilities on a web server.

Tools of the Trade

- OWASP Zed Attack Proxy(ZAP)
  - Open source web application vulnerability scanner
  - As a web proxy, it can also capture and manipulate web traffic coming through it
  - OWASP is a non-profit organization that promotes and maintains best use practices for web application deployment

nessus

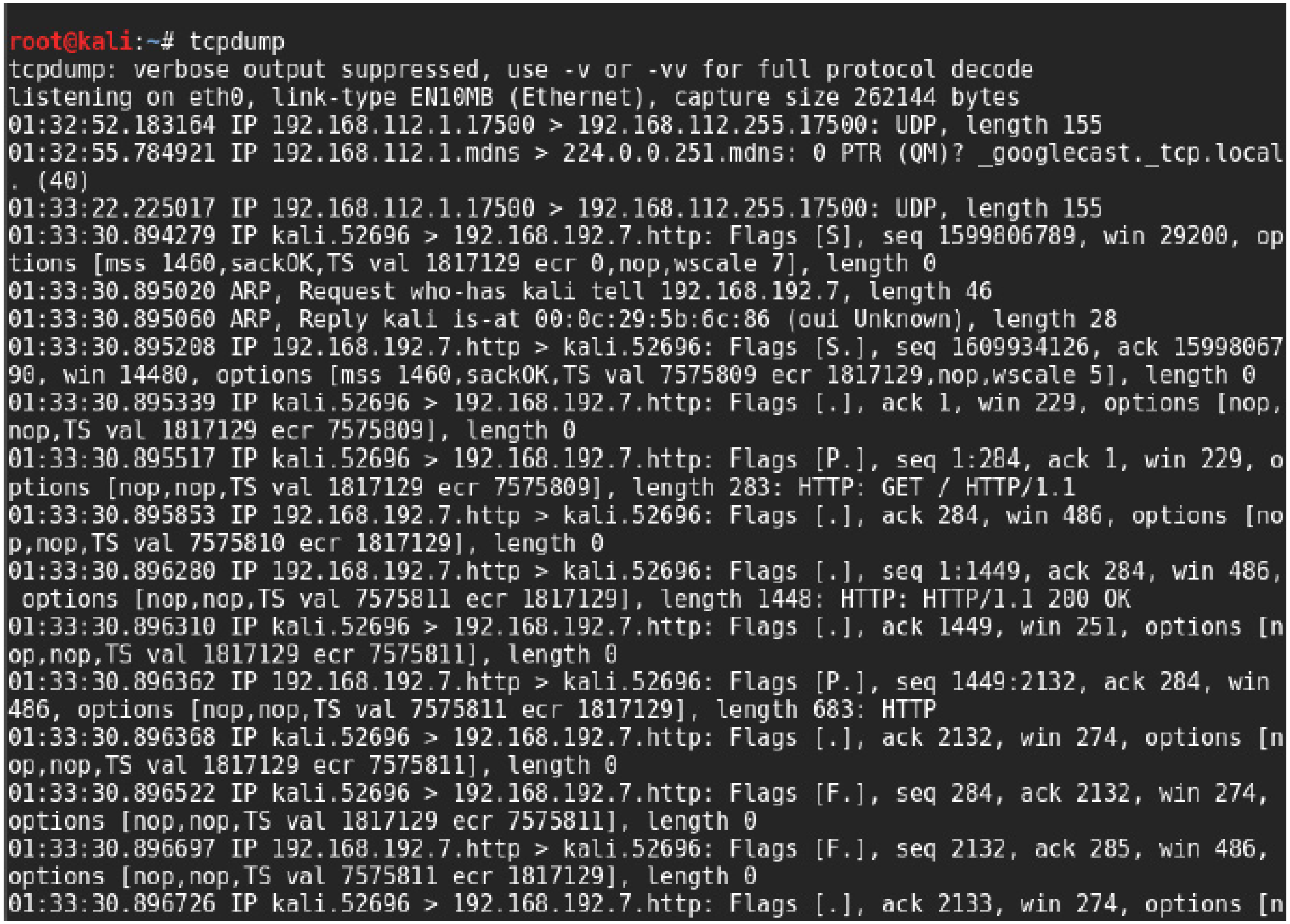
  - Vulnerability scanner
  - Proprietary software with an expansive suite of plug-ins
  - Has basic port scanning capabilities
  - Has comprehensive configuration checks and reporting
    - It will check for vulnerabilities, common misconfigurations, default passwords usage, and compliance level

[1,5,9]

Tools of the Trade

- **Netstat**
  - Command-line tool found in every major OS
  - Can displays network connections, interface statistics, listening ports, and process identifies
- **Tcpdump**
  - Command-line tool
  - Displays raw network packets
  - Requires admin privileges to capture traffic promiscuously

[1]



```
root@kali:~# tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
01:32:52.183164 IP 192.168.112.1.17500 > 192.168.112.255.17500: UDP, length 155
01:32:55.784921 IP 192.168.112.1.mdns > 224.0.0.251.mdns: 0 PTR (QM)? _googlecast._tcp.local
. (40)
01:33:22.225017 IP 192.168.112.1.17500 > 192.168.112.255.17500: UDP, length 155
01:33:30.894279 IP kali.52696 > 192.168.192.7.http: Flags [S], seq 1599806789, win 29200, op
tions [mss 1460,sackOK,TS val 1817129 ecr 0,nop,wscale 7], length 0
01:33:30.895020 ARP, Request who-has kali tell 192.168.192.7, length 46
01:33:30.895060 ARP, Reply kali is-at 00:0c:29:5b:6c:86 (oui Unknown), length 28
01:33:30.895208 IP 192.168.192.7.http > kali.52696: Flags [S.], seq 1609934126, ack 15998067
90, win 14480, options [mss 1460,sackOK,TS val 7575809 ecr 1817129,nop,wscale 5], length 0
01:33:30.895339 IP kali.52696 > 192.168.192.7.http: Flags [.], ack 1, win 229, options [nop,
nop,TS val 1817129 ecr 7575809], length 0
01:33:30.895517 IP kali.52696 > 192.168.192.7.http: Flags [P.], seq 1:284, ack 1, win 229, o
ptions [nop,nop,TS val 1817129 ecr 7575809], length 283: HTTP: GET / HTTP/1.1
01:33:30.895853 IP 192.168.192.7.http > kali.52696: Flags [.], ack 284, win 486, options [no
p,nop,TS val 7575810 ecr 1817129], length 0
01:33:30.896280 IP 192.168.192.7.http > kali.52696: Flags [.], seq 1:1449, ack 284, win 486,
 options [nop,nop,TS val 7575811 ecr 1817129], length 1448: HTTP: HTTP/1.1 200 OK
01:33:30.896310 IP kali.52696 > 192.168.192.7.http: Flags [.], ack 1449, win 251, options [n
op,nop,TS val 1817129 ecr 7575811], length 0
01:33:30.896362 IP 192.168.192.7.http > kali.52696: Flags [P.], seq 1449:2132, ack 284, win
486, options [nop,nop,TS val 7575811 ecr 1817129], length 683: HTTP
01:33:30.896368 IP kali.52696 > 192.168.192.7.http: Flags [.], ack 2132, win 274, options [n
op,nop,TS val 1817129 ecr 7575811], length 0
01:33:30.896522 IP kali.52696 > 192.168.192.7.http: Flags [F.], seq 284, ack 2132, win 274,
options [nop,nop,TS val 1817129 ecr 7575811], length 0
01:33:30.896697 IP 192.168.192.7.http > kali.52696: Flags [F.], seq 2132, ack 285, win 486,
options [nop,nop,TS val 7575811 ecr 1817129], length 0
01:33:30.896726 IP kali.52696 > 192.168.192.7.http: Flags [.], ack 2133, win 274, options [n
```

tcpdump

In the above example tcpdump is capturing packets. This shows raw output of network packets transmitted over the network.

Tools of the Trade

- **Wireshark**
  - **Opensource software**
  - **Graphical representation of packet types**
  - **Can use promiscuous mode for a closer complete network capture**
  - **Provides a statistical analysis summary for captured data**
- **Tshark**
  - **Command-line version of Wireshark**

[1]

Intrusion Detection and Prevention Systems

- Intrusion Detection System (IDS)
  - There are Hardware and software IDS products
  - Passively reviews network events and analyzes them for signs of intrusion
  - Can detect anomalies or be set up to alert the admin of any known malicious activity
- Intrusion Prevention Systems
  - Actively reviews network events
  - Will stop or quarantine the host if any malicious activity is detected
- Network IDS (NIDS)
  - Used to monitor a network
- Host IDS (HIDS)
  - Used to monitor an individual host

[1]

Quiz

Chapter 1

Question #1

- 1. Which of the following is not considered a form of passive or open source intelligence reconnaissance?
  - A. Google hacking
  - B. Nmap
  - C. ARIN queries
  - D. Nslookup

[1]

Answer #1

- B
  - Nmap is a scanning tool that requires direct interaction with the system under test.
  - All the other responses allow a degree of anonymity by interrogating intermediary information sources.

[1]

Question #2

- **2. Which of the following transmissions are part of nmap’s default host-scanning behavior?**
  - A. ICMP Echo Response
  - B. TCP FIN to port 80
  - C. TCP ACK to port 80
  - D. UDP SYN to port 53

[1]

Answer #2

- C
  - Nmap’s default behavior is to send an ICMP Echo Request(not a response), a TCP SYN to port 443(not to port 80), a TCP ACK to port 80, and ICMP Timestamp Request.

[1]

Question #3

- **Why is operating system (OS) fingerprinting imprecise?**
  A. **Hosts can run multiple OSs**
  B. **Some hosts run both IPv4 and IPv6**
  C. **It is impossible to distinguish major OSs**
  D. **Variants of OS families (such as Linux) can be hard to differentiate**

[1]

Answer #3

- D
  - Although scanning tools such as nmap will likely infer the correct major version of an OS (such as Windows or Linux), it is difficult to ascertain the specific variant (for example, the service pack of Windows, or CentOS versus Ubuntu for Linux).
  - Sophisticated defenders can configure their externally accessible hosts to report the wrong OS

[1]

Question #4

- **Email harvesting is useful for all the following reasons except which?**
  A. **The inbox name is commonly the same as an active user account name.**
  B. **Publicly visible addresses are likelier to receive phishing emails.**
  C. **Email addresses can help yield additional personal information for targeting.**
  D. **It is difficult to find email addresses for specific individuals or organizations.**

[1]

Answer #4

- D
  - Several techniques and tools can be leveraged to obtain email addresses, either individually or in bulk, so this is not a difficult thing to do.

[1]

Question #5

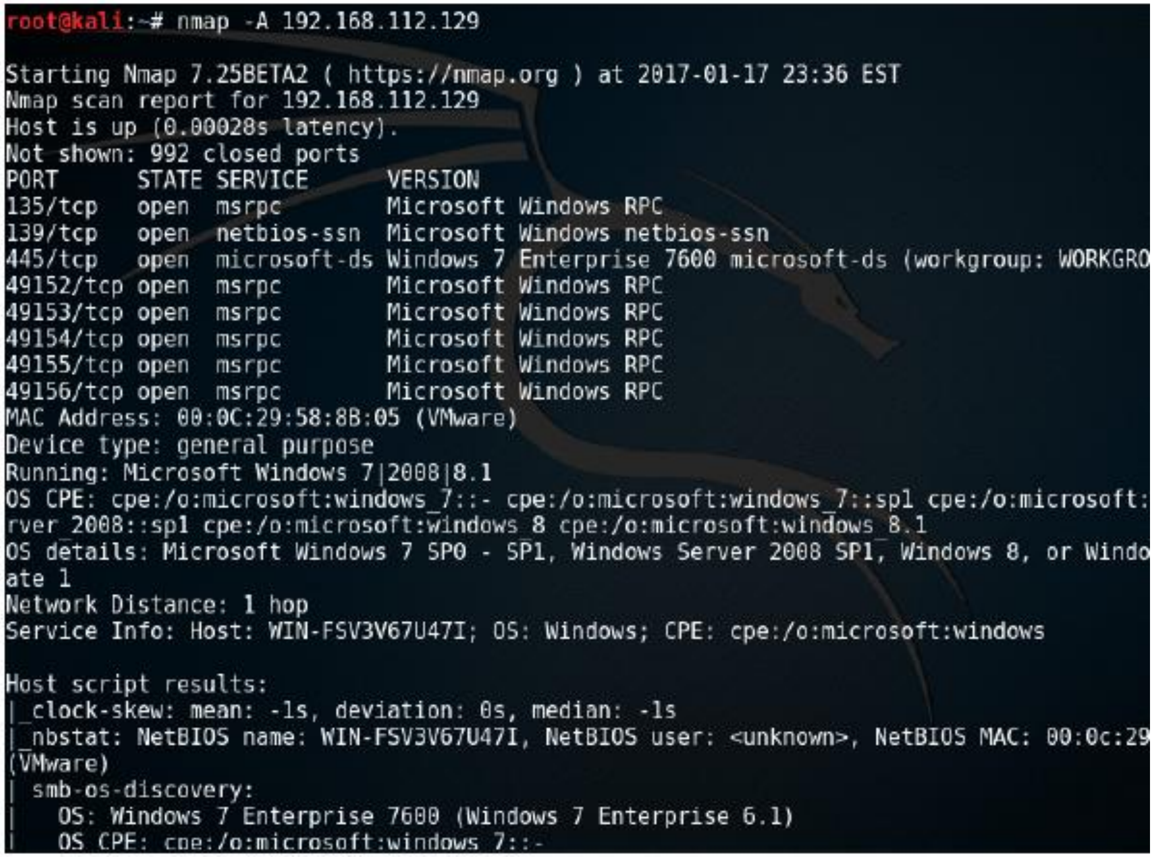
- What is key consideration when conducting wired versus wireless reconnaissance?
  A. Wireless reconnaissance requires physical access.
  B. Wireless reconnaissance can be performed thousands of feet away.
  C. Wired reconnaissance requires user credentials.
  D. Wired reconnaissance will yield less information than wireless.

[1]

Answer #5

- B
  - A key difference between wired and wireless reconnaissance is that the former requires physical connectivity whereas the latter can be done over the airwaves from a distance.
  - In fact, by using a hi-grain direction al antenna, it is possible to connect to wireless network from miles away.

[1]



```
root@kali:~# nmap -A 192.168.112.129

Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2017-01-17 23:36 EST
Nmap scan report for 192.168.112.129
Host is up (0.00028s latency).
Not shown: 992 closed ports
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Windows 7 Enterprise 7600 microsoft-ds (workgroup: WORKGRO
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 00:0C:29:58:8B:05 (VMware)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:
rver_2008::sp1 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows 8, or Windo
ate 1
Network Distance: 1 hop
Service Info: Host: WIN-FSV3V67U47I; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: -1s, deviation: 0s, median: -1s
|_nbstat: NetBIOS name: WIN-FSV3V67U47I, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29
(VMware)
| smb-os-discovery:
|   OS: Windows 7 Enterprise 7600 (Windows 7 Enterprise 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::-
```

Question #6

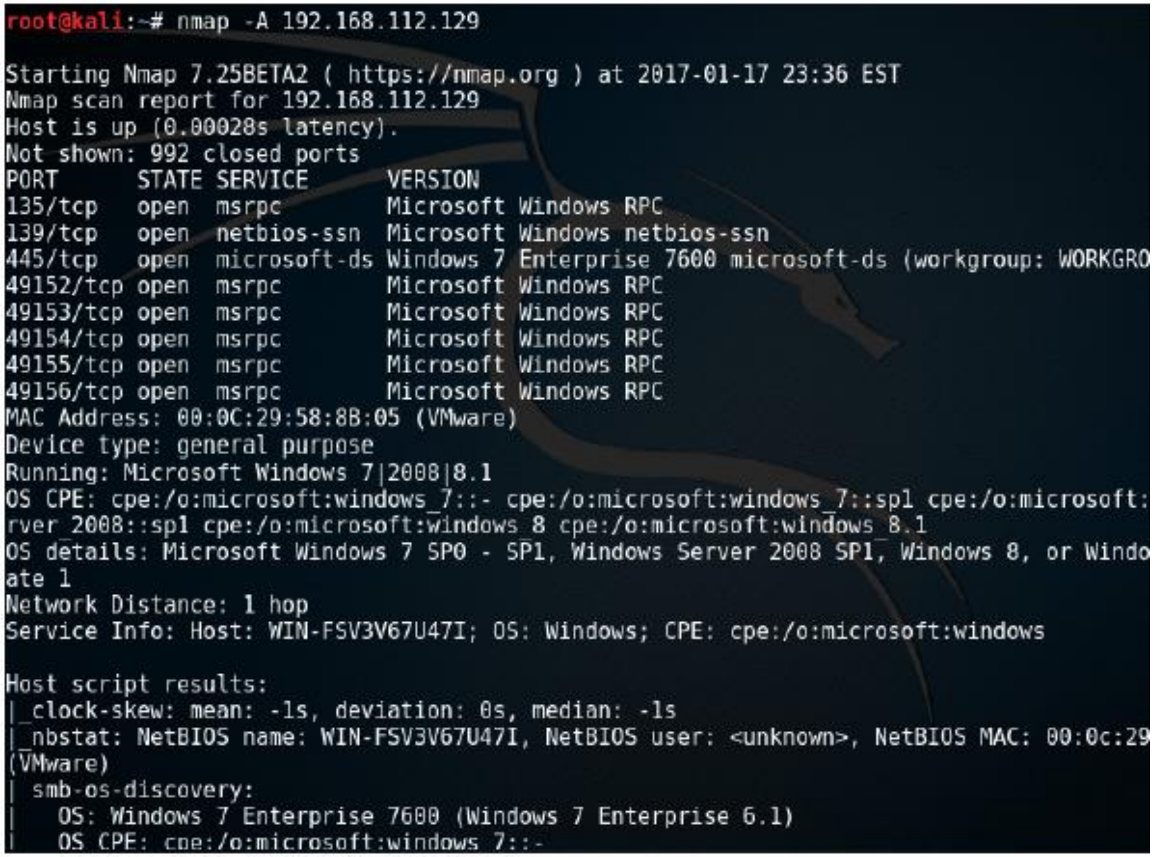
- **All the following statements are likely true about the above scan except which?**
  - **A. There is firewall between the scanner and the host**
  - **B. The scan was preformed using Kali Linux**
  - **C. An ICMP Echo Request was part of the scan**
  - **D. The scanner is attempting to identify the OS of the target host.**

[1]

Answer #6

- A
  - The scan shows that the target host is likely running Windows 7.
  - The default behavior for that system's firewall is to block unsolicited access to all ports.
  - This means that the scan would have not reported any open ports had the firewall been enabled.

[1]



```
root@kali:~# nmap -A 192.168.112.129

Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2017-01-17 23:36 EST
Nmap scan report for 192.168.112.129
Host is up (0.00028s latency).
Not shown: 992 closed ports
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Windows 7 Enterprise 7600 microsoft-ds (workgroup: WORKGRO
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 00:0C:29:58:8B:05 (VMware)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:
rver_2008::sp1 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows 8, or Windo
ate 1
Network Distance: 1 hop
Service Info: Host: WIN-FSV3V67U47I; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: -1s, deviation: 0s, median: -1s
|_nbstat: NetBIOS name: WIN-FSV3V67U47I, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29
(VMware)
| smb-os-discovery:
|   OS: Windows 7 Enterprise 7600 (Windows 7 Enterprise 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::-
```

Question #7

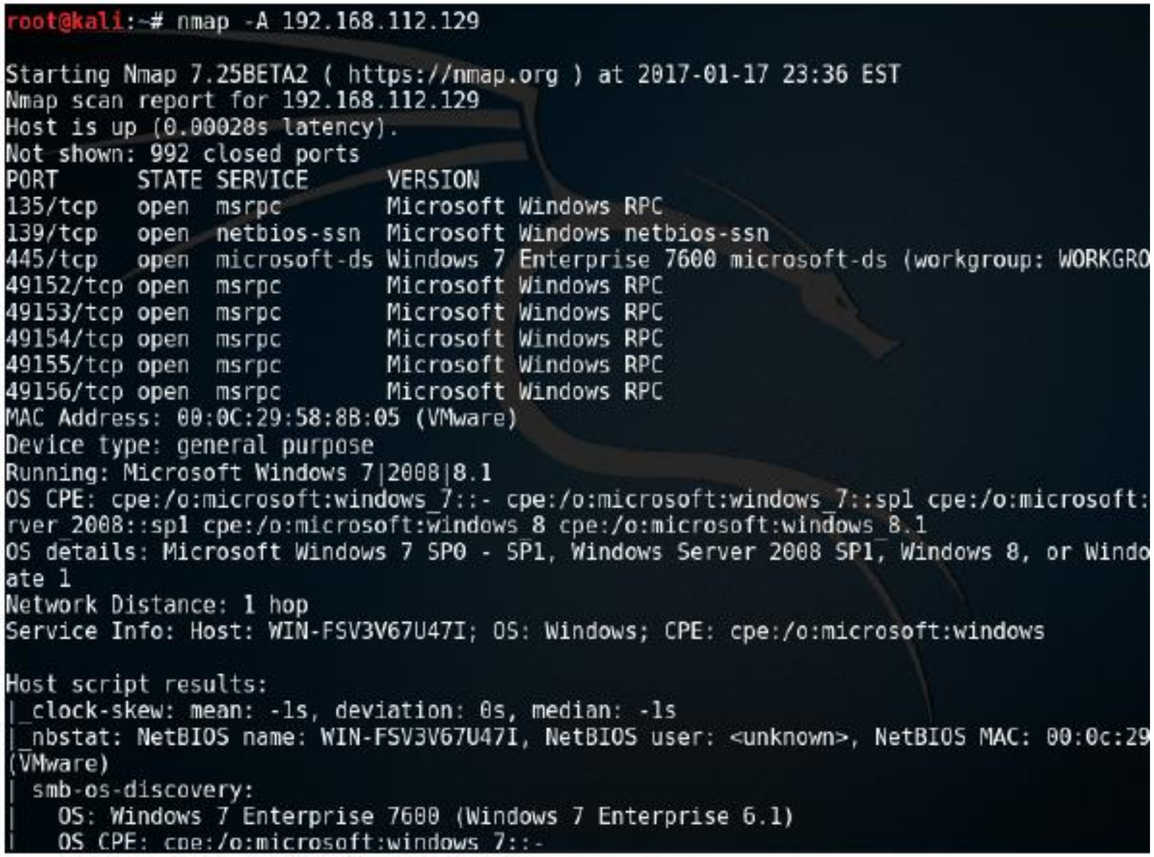
- **Which service is running on the target host?**
  - **A. HTTP**
  - **B. RPC**
  - **C. POP**
  - **D. CPE**

[1]

Answer #7

- **B**
  - **You can tell that the Remote Procedure Call (RPC) service is running because TCP port 135 is open, but also because this service is identified by name as running on several other ports.**

[1]



```
root@kali:~# nmap -A 192.168.112.129

Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2017-01-17 23:36 EST
Nmap scan report for 192.168.112.129
Host is up (0.00028s latency).
Not shown: 992 closed ports
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Windows 7 Enterprise 7600 microsoft-ds (workgroup: WORKGRO
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 00:0C:29:58:8B:05 (VMware)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:
rver_2008::sp1 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows 8, or Windo
ate 1
Network Distance: 1 hop
Service Info: Host: WIN-FSV3V67U47I; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: -1s, deviation: 0s, median: -1s
|_nbstat: NetBIOS name: WIN-FSV3V67U47I, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29
(VMware)
| smb-os-discovery:
|   OS: Windows 7 Enterprise 7600 (Windows 7 Enterprise 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::-
```

Question #8

Which of the following statements probably not true about the target host?

- **A. It is in the same subnet as the scanner.**
- **B. It is running as a virtual machine.**
- **C. It is far away from the scanner.**
- **D. It is running Windows 7 Service Pack 1.**

[1]

Answer #8

- C
  - The scan states that the network distance to the host is one hop, which means the target and the scanner are directly connected.

[1]

Question #9

- **Netstat can provide all the following information except which?**
  A. Listening ports
  B. Remotely connected host IP addresses
  C. Name of the program that opened the socket
  D. Name of the user who opened the socket

[1]

Answer #9

- D
  - Although it is possible to associate running processes or ports with specific users, this is not a feature offered by netstat.

[1]

Scenario for Questions 10 – 12

- Robbie is the security administrator of a company that needs to ensure its employees are practicing good operational security (OPSEC). All employees have received training on social engineering (phishing in particular) and how to control their personal profile on the Internet. Robbie wants to verify externally that his teammates are putting into practice what they have learned.

[1]

Question #10

- **When testing his teammates' online OPSEC, Robbie could do which of the following?**
  A. **Search employees' Facebook and LinkedIn pages, looking for sensitive personal or work information.**
  B. **Attempt to guess employees' passwords on Facebook or LinkedIn.**
  C. **Monitor employees' use of social media site while at work.**
  D. **Create fake profiles on Facebook and LinkedIn and attempt to befriend employees.**

[1]

Answer #10

- A
  - Searching for openly available information is the only one listed approaches that would be permissible for Robbie. All other options, at a minimum, violate terms of service or, at worst, violate the law (for example, guessing passwords).

[1]

Question #11

- What is the best way to assess Robbie's teammates' vulnerability to phishing?
  A. Send simulated phishing emails to work addresses and provide additional training to those who fall victim to it.
  B. Monitor inbound phishing emails and note which individuals fall victim to them.
  C. Block phishing attempts at the email gateway.
  D. Send simulated phishing emails to personal addresses and provide additional training to those who fall victim to it

[1]

Answer #11

- A
  - Conducting internal simulated phishing campaigns is a common way to assess the security posture of an organization regarding this type of threat.
  - This approach should never be used with personal email address without the users' explicit consent.

[1]

Question #12

- **Robbie could test his teammates' responses to social engineering attempts by all the following except which?**
  A. Pretexting
  B. Spear-phishing
  C. Footprinting
  D. Tailgating

[1]

Answer #12

- C
  - Footprinting is reconnaissance and not a social engineering technique.

[1]

References

1. Maymí Fernando, and Brent Chapman. CompTIA CSA+ Cybersecurity Analyst Certification All-in-One Exam Guide (Exam CS0-001). McGraw-Hill Education, 2018.
2. Profitap, 10 October 2018. [Online]. Available: https://insights.profitap.com/passive-vs-active-network-taps#.
3. D. Firesmith, "CMU Software Engineering Institute," September 25 2017. [Online]. Available: https://insights.sei.cmu.edu/sei_blog/2017/09/virtualization-via-containers.html.
4. T. S. Engineer, "YouTube," 9 February 2019. [Online]. Available: https://youtu.be/JSLpG_spOBM.
5. Tenable, 2020.

References

6. J. 15, S. Watts, and M. Raza, “SaaS vs PaaS vs IaaS: What's The Difference and How To Choose,” *BMC Blogs*, 15-Jun-2019. [Online]. Available: https://www.bmc.com/blogs/saas-vs-paas-vs-iaas-whats-the-difference-and-how-to-choose/. [Accessed: 30-Sep-2020].

7. Guest, “Graph-based intelligence analysis,” *Linkurious*, 05-Nov-2019. [Online]. Available: https://linkurio.us/blog/graph-based-intelligence-analysis/. [Accessed: 30-Sep-2020].

8. “Regional Internet Registries (RIRs) - An Overview: Infographic,” *IPv4Mall*, 17-May-2019. [Online]. Available: https://ipv4mall.com/technology/regional-internet-registries-rirs-an-overview-infographic/. [Accessed: 30-Sep-2020].
9. “The ZAP Homepage,” OWASP ZAP, 22-Sep-2020. [Online]. Available: https://www.zaproxy.org/. [Accessed: 30-Sep-2020].
10. Nmap. [Online]. Available: https://nmap.org/. [Accessed: 30-Sep-2020].