Enumeration

Module-4


Enumeration
INFOSAVVY

Active and Passive Data Collection

- Collecting information about the target company from the Internet, climbing through trashcans, walking the halls, or talking to friends is considered passive information collection because there is little direct interaction with the target.

- Active information involves direct interaction with the target.
- Enumeration can be defined as a crossover between passive to active attack

Enumeration Techniques

- Various Information can be collected through scanning,and various protocols has its own weaknesses for exploitation
- **Connection Scanning**-TCP COnnection Establishment -connect request is where whether port is listening?
- Unless the port is controlled by an intermediate device (e.g., firewall) that authenticates the session, the system will usually respond to the request (if the port is active).
- Once the session is established it is up to the service to authenticate, but by then we know the service is running.
- Detectable

TCP communication Flags

Data contained in the packet should be processed immediately

URG
(Urgent)

There will be no more transmissions

FIN
(Finish)

Resets a connection

RST
(Reset)

PSH
(Push)

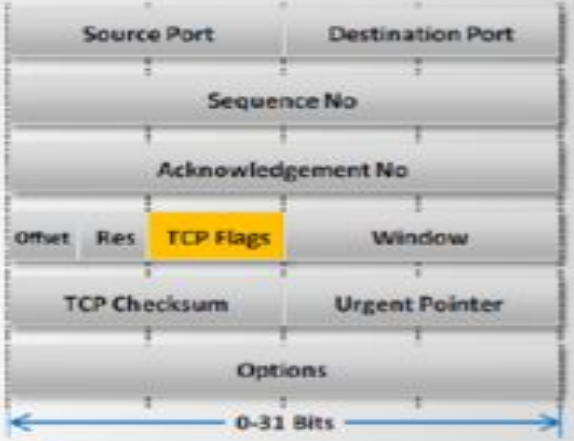
Sends all buffered data immediately

ACK
(Acknowledgement)

Acknowledges the receipt of a packet

SYN
(Synchronize)

Initiates a connection between hosts



Three-way Handshake

TCP uses a **three-way handshake** to establish a connection between server and client

Three-way Handshake Process

1. The Computer A (10.0.0.2) initiates a connection to the server (10.0.0.3) via a packet with only the **SYN** flag set
2. The server replies with a packet with both the **SYN** and the **ACK** flag set
3. For the final step, the client responds back to the server with a single **ACK** packet
4. If these three steps are completed without complication, then a TCP connection is established between the client and the server

Step 1

Step 2

Step 3

Enumeration Techniques

- **SYN Scanning**. Briefly described earlier, during a session initiation the source system sends a SYN packet requesting a connection on an interesting port. If the port is active and accepting connections the service willrespond with a SYN/ACK, effectively acknowledging the connection.

- When the SYN/ACK is received you immediately respond with an RST (reset) to tear down the connection.

- The advantage is that some filteringdevices, especially ones that do not monitor sessions, may let this get through.

Stealth Scan/ Half Open Scan

Attackers use stealth scanning techniques to **bypass firewall rules, logging mechanism**, and hide themselves as usual network traffic

Stealth Scan Process

1. The client sends a single SYN packet to the server on the appropriate port
2. If the port is open then the server responds with a SYN/ACK packet
3. If the server responds with an RST packet, then the remote port is in the "closed" state
4. The client sends the RST packet to close the initiation before a connection can ever be established

Enumeration Techniques

- **FIN Scanning.** Opening connections or performing a “half-open” scan,such as the SYN scan, can be noisy and draw attention to the process.
- **FIN (FINish) packets,** on the other hand, have the potential to bypass several types of controls if not configured properly. First identified and documented by Uriel Maimon, **the technique is founded on a TCP RFC requirement that if a closed port** (one without a corresponding service) receives a FIN packet the response will be an RST packet.
- If an open port or listening port receives a FIN packet it may not respond at all **depending on the type of OS employed**. Therefore, this technique can be used to bypass firewalls and routers to gain a better understanding of operating systems and, in some cases, what ports are potentially in use.


FIN
No Response
Attacker
10.0.0.6
Server
10.0.0.8:23
Port is open


FIN
RST/ACK
Attacker
10.0.0.6
Server
10.0.0.8:23
Port is closed

Enumeration Techniques

- **Fragment Scanning.**To scan a system behind a firewall or through another box acting as a gateway, you can break up the probing packet into tiny little ones in an effort to confuse the security systems.
- . However, over the past couple of years hackers have been sending fragments at certain intervals to slightly overlap the session state table of firewalls and IDSs, but not so long that the targeted system gives up.
- Therefore, a fragment is sent through the firewall and to the target computer. The computer may wait X seconds for the next packet before dropping the session. In contrast, the firewall may only monitor the session for Y seconds. By setting the interval to less than X and greater than Y, the technique has a better chance of going undetected. Keep in mind that today's firewalls or IDSs usually queue the fragments before sending, but there is always a chance for a misconfiguration.

Enumeration Techniques

- **TCP Reverse IDENT Scanning.** The IDENT protocol is used to identify the owner of a connection.
- By sending the system a port pair, the IDENT service will respond with the owner of the connection and ultimately the owner of the process. Therefore, this technique is best used on internal systems, or when there is a clear path into the internal network.
- As noted by Dave Goldsmith in a 1996 Bugtraq post, the ident protocol (rfc1413) allows for the disclosure of the username of the owner of any process connected via TCP, even if that process didn't initiate the connection. So you can, for example, connect to the http port and then use ident to find out whether the server is running as root. This can only be done with a full TCP connection to the target port (i.e. the -t option). nmap's -i option queries ident d for the owner of all listen()ing ports.

Enumeration Techniques

- **FTP Bounce Scanning.** The FTP protocol uses a **control connection and a data connection to support the entire session**. The control connection is for commands and other user interaction, whereas the data connection is specifically for data transfer.

- An interesting protocol feature is that the d**ata and control connections do not have to be to or from the same system.**Therefore, it is feasible to connect to a system and send data to any other system: However, this can provide an opportunity to use an FTP server to proxy scans on behalf of the tester by manipulating the control and data channels.

- For example, you connect to an FTP server and use the PORT command to declare a listening port on a target system and then run a LIST forcing the control channel to request data from a remote system on the port specified. If the port is listening, the system may respond; if not you'll receive a data error. To test the next port, you specify the new one and run LIST again.

FTP Bounce Attack

Intermediate Server

Step 2 :
The Intermediate Server connects to the Target Server

Step 3 : Sensitive file is transferred to the Intermediate Server

Target Server

Step 1 :
Attacker opens a connection with the Intermediate Server

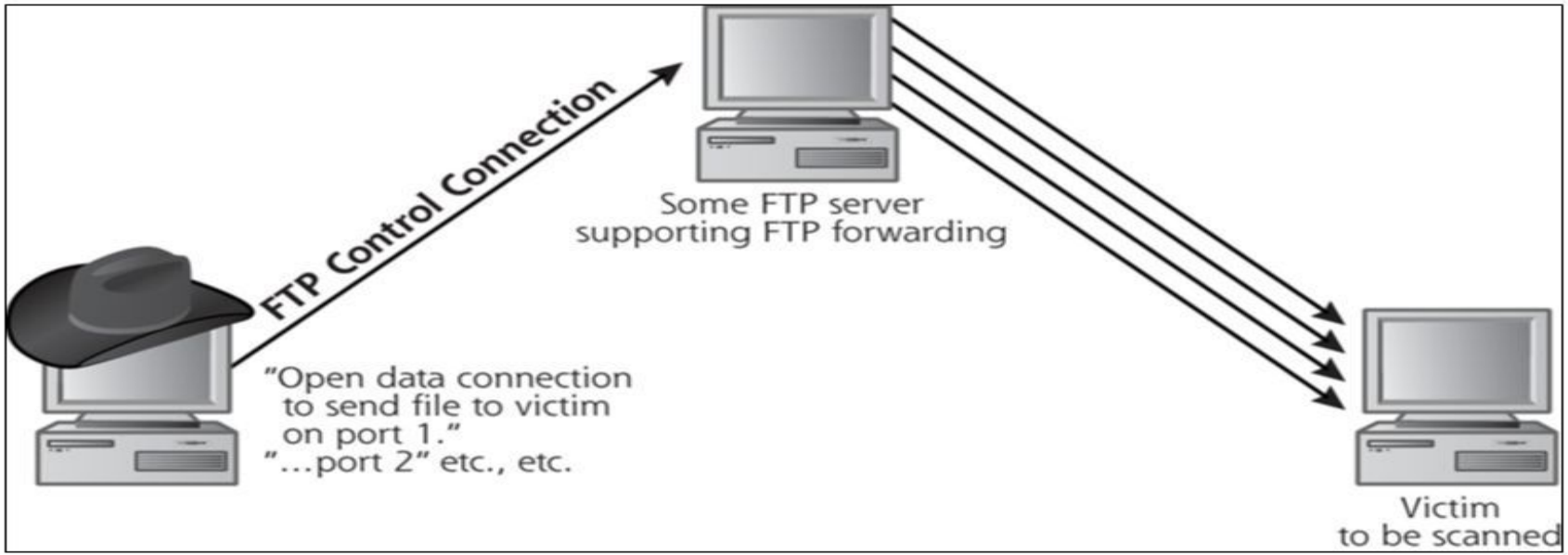
Step 4 :
Data is transferred back to the Attacker

Attacker

The Security Buddy
https://www.thesecuritybuddy.com/

FTP Bounce Scan

- FTP server informs attacker of result



Enumeration Techniques

- **UDP Scanning.**
- UDP, on the other hand, is connectionless and is not required to acknowledge a session. Even though UDP scans will not receive a reply from a remote port, in the event there is no service listening some systems will send an ICMP message stating the port is unreachable.
- Therefore, one can conclude the **nonresponsive ports are open.** Of course, when you rely on ICMP for penetration testing you're going to be disappointed because nearly every firewall and router will block ICMP messages making it look like all the ports are open.
- The one true advantage to UDP scanning is **finding high UDP ports associated with known vulnerabilities in services or even a Trojan hiding on a previously compromised system.**

UDP Scan (User Datagram Protocol)

UDP Port Open

- There is no three-way TCP handshake for UDP scan
- The system does not respond with a message when the port is open

UDP Port Closed

- If a UDP packet is sent to closed port, the system responds with ICMP port unreachable message
- Spywares, Trojan horses, and other malicious applications use UDP ports

Enumeration Techniques

- **ACK Scanning.** Sometimes you may want to know the type of filtering devices between you and the target. Is it a stateful firewall monitoring all the sessions or is it a router just performing port filtering?

- By sending a packet with the port defined and the ACK bit set, a router will typically pass the packet and you will receive an RST from the system.

- If the gateway is a firewall, you probably won't get anything in return.
- The goal is to get as much information as possible,

Attacker

Stateful Firewall is Present

Probe Packet (ACK)

No Response

Target Host

Attacker

No Firewall

Probe Packet (ACK)

RST

Target Host

Soft Objective

- **Enumeration is focused on the act of investigating various characteristics about the target's technical elements by interacting with operating systems, applications, services, and anything that can be used to gain more data about the target.**
- **The enumeration phase is the last opportunity, prior to developing an attack plan .**
- **Therefore, at the completion of the enumeration phase, the tester has a collection of data from querying the technical environment in addition to other forms of information collected from the reconnaissance phase.**
- **it is necessary to look at the data in a manner that will expose vulnerabilities that are not directly identified.**
- **Enumeration and vulnerability analysis are inherently linked**

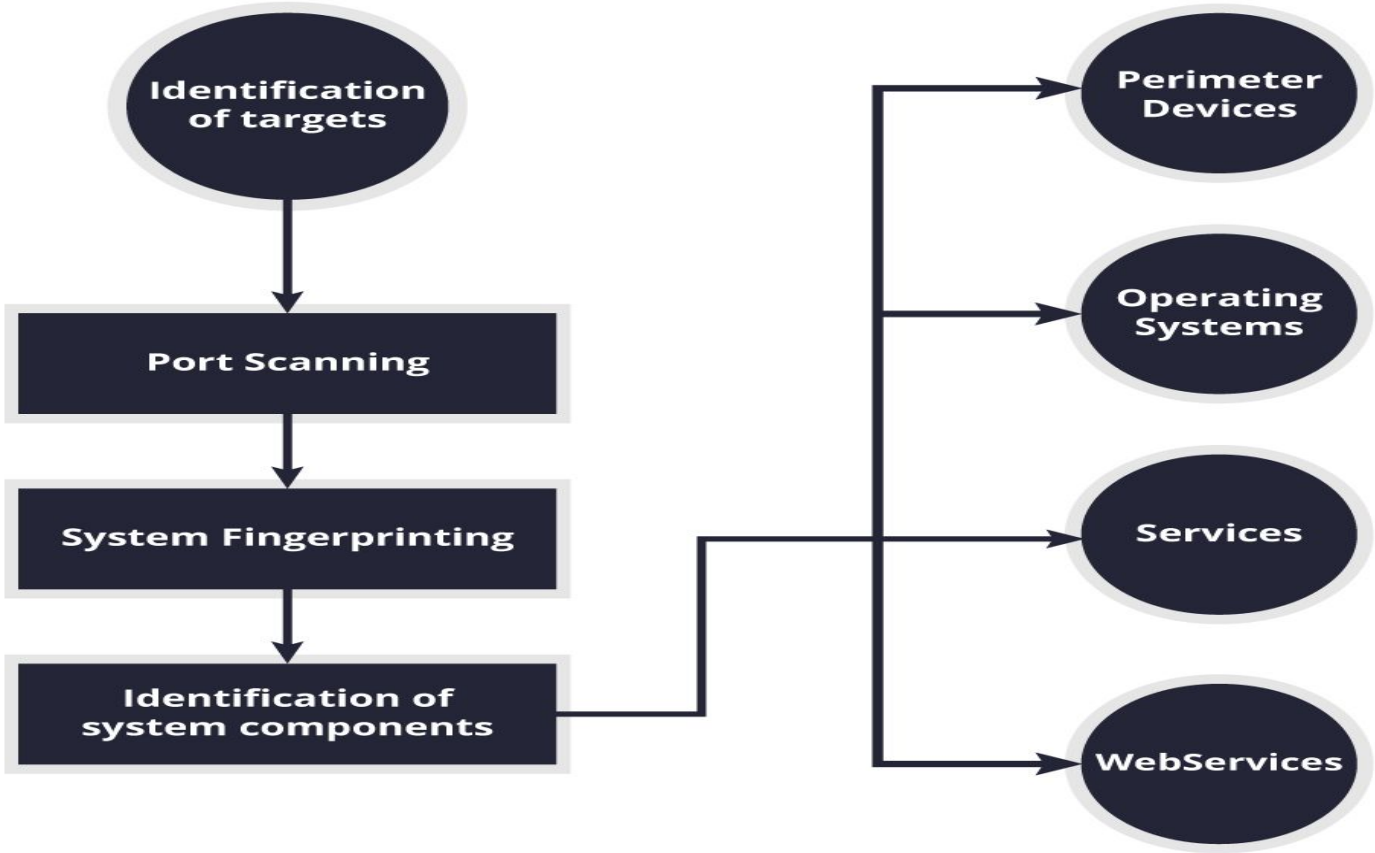
LOOKING AROUND OR ATTACK?

- **Active and interactive scanning are used to pull information about the target system by sending packets to the target system in an effort to determine the status of the system and what services it is offering.**
- **It is important to consider the potential impact on systems and networks when aggressive tactics are used to survey systems.**
- **For example, a firewall may permit fragmented packets to pass, allowing the tester to query the targeted server undetected.**
- **Port scan and targeted port scan-case study**

ELEMENTS OF ENUMERATION

- Depending on the system type, such as a server, router, switch, remote
- access system, or phone system, there is data that can be pulled to be used later during the vulnerability analysis phase. Following are some examples of data and system types:
  - Account Data
  - Architecture
  - Operating System
  - Wireless Network
  - Applications-logo case study
  - Custom Applications-poor security,legacy programming language,password field data check,pull parts/whole web for offline analysis

Elements of Enumeration



PREPARING FOR THE NEXT PHASE

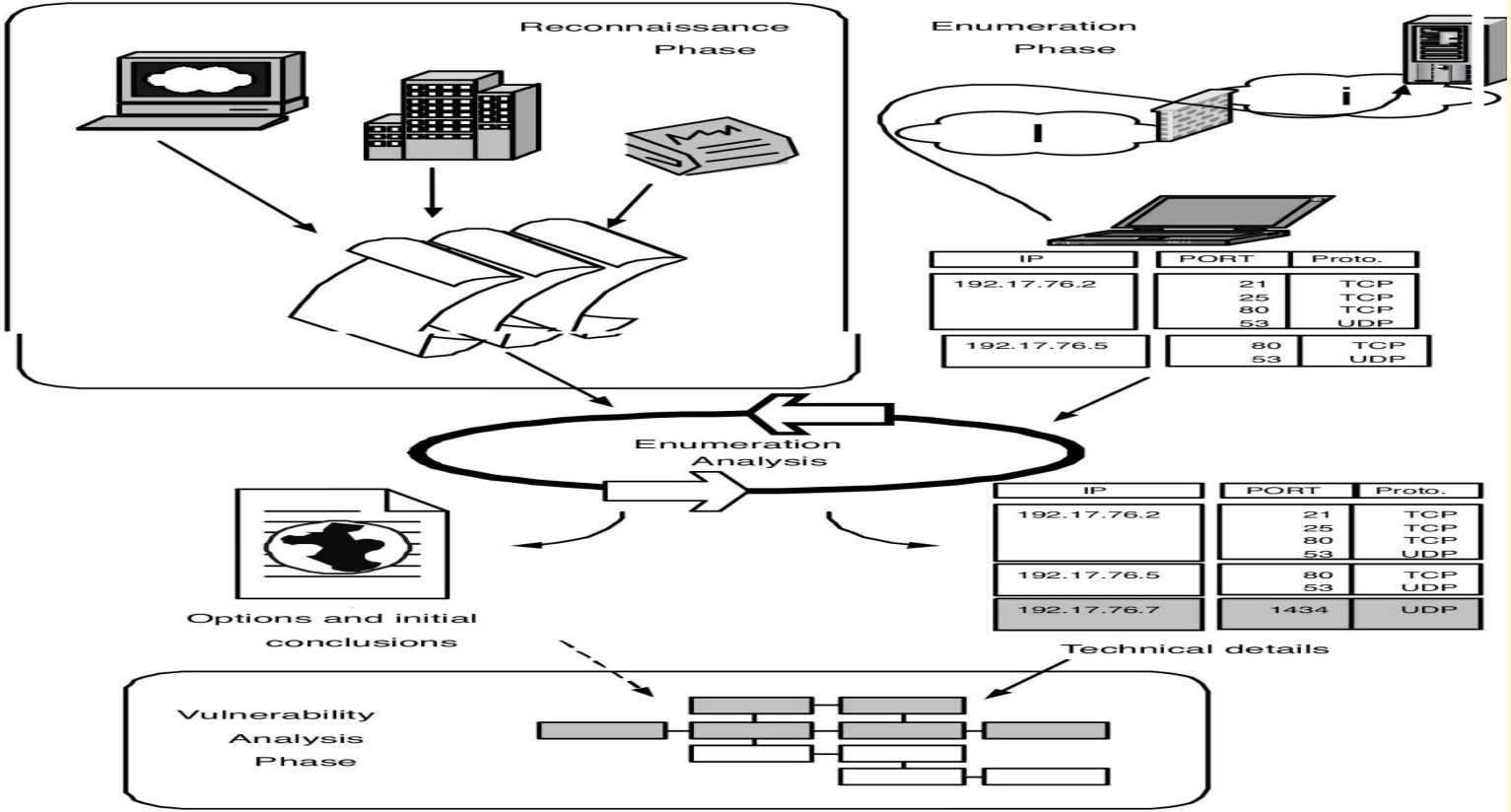
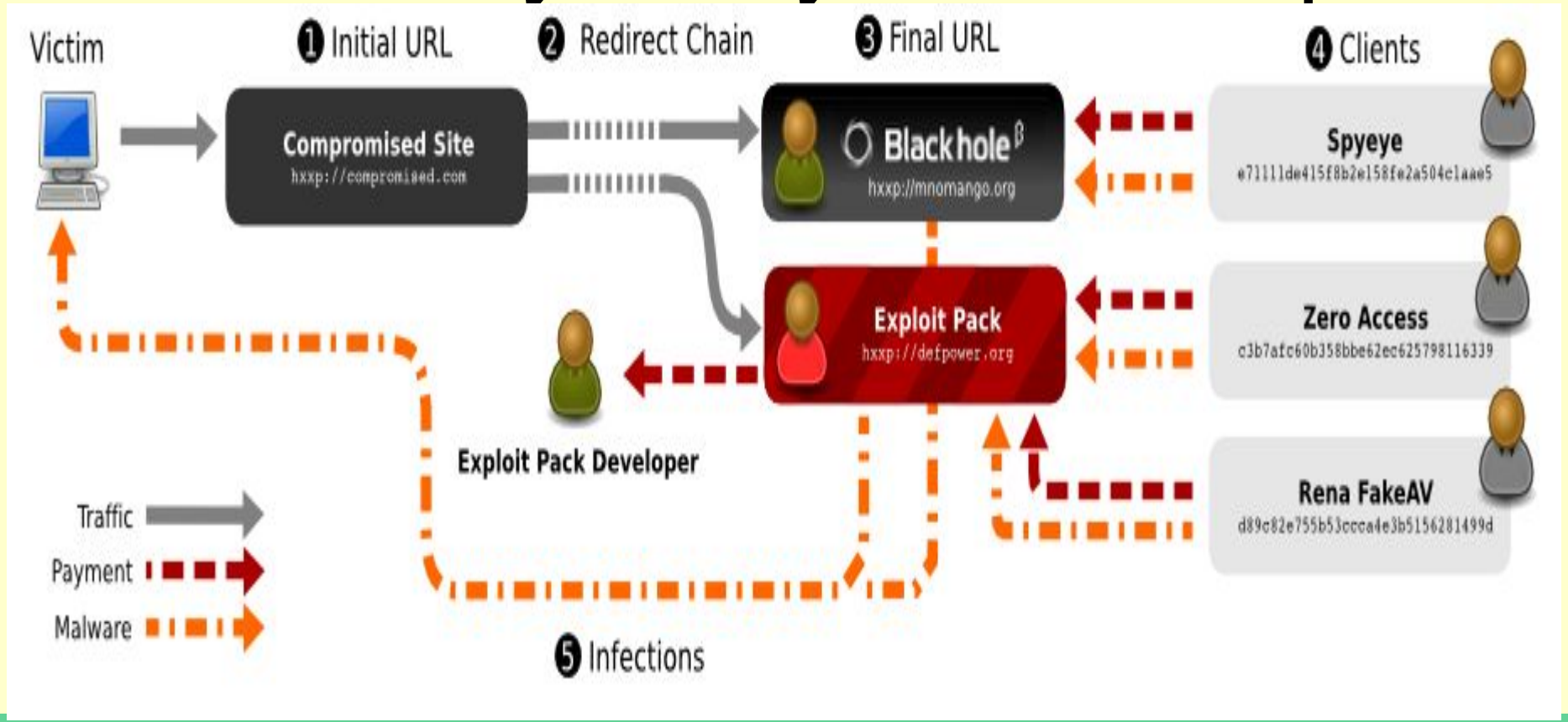


FIGURE 10.1 Process Overview for Enumeration Moving into Vulnerability Analysis

Vulnerability Analysis&Exploitation

- **Vulnerability Analysis-scan open ports,password cracker,Vulnerabilities in OS,Applications**
- **The difference between a penetration test and vulnerability scanning is the act of exploitation**
- **A vulnerability scanning (or analysis) service is engineered to identify vulnerabilities and determine a level of risk based on the potential of the vulnerability without regard for other environmental conditions on the network that may enhance or cancel out the vulnerability altogether**
- **By exploiting the vulnerability, a company can determine the impact of not rectifying the problem as opposed to assuming the level of risk is bearable given a specific vulnerability.**

Vulnerability Analysis and Exploit



Vulnerability Analysis&Exploitation

- Vulnerability Analysis-scan open ports,password cracker,Vulnerabilities in OS,Applications
- The difference between a penetration test and vulnerability scanning is the act of exploitation
- A vulnerability scanning (or analysis) service is engineered to identify vulnerabilities and determine a level of risk based on the potential of the vulnerability without regard for other environmental conditions on the network that may enhance or cancel out the vulnerability altogether
- By exploiting the vulnerability, a company can determine the impact of not rectifying the problem as opposed to assuming the level of risk is bearable given a specific vulnerability.
- A system in the DMZ that provides services to the general Internet public is exposed to all types of threats that can exploit even the most hidden vulnerability

INTUITIVE TESTING

- **The issue is not all vulnerabilities can be quickly surmised, and the ones that can be determined as high risk without exploitation are identified well into a test.**
- **This goal is to expose and rate as many vulnerabilities as possible to provide a clear picture and the various levels of risk related to them.**
- **Intuitive testing allows the target to gain as much value from the attack thread while promoting the search for other vulnerabilities.**
- **The primary argument against this type of testing is the assumption that why would a hacker not go for the throat than spend more time looking for other avenues of access**

INTUITIVE TESTING

- **Intuitive testing allows the target to gain as much value from the attack thread while promoting the search for other vulnerabilities.**
- **The tester can avoid spending valuable time and effort leveraging that one set of vulnerabilities to gain singular access, when that time can be spent looking for another, which could be potentially broader and more effective in the long run.**
- **Eg :once rootkit is successfully installed ,one can gain access to system at later stage also,so can spend time in looking around for more attack threads.**
- **Move from one point to another without committing to a single point.**

INTUITIVE TESTING

- **Intuitive testing allows the target to gain as much value from the attack thread while promoting the search for other vulnerabilities.**
- **The tester can avoid spending valuable time and effort leveraging that one set of vulnerabilities to gain singular access, when that time can be spent looking for another, which could be potentially broader and more effective in the long run.**
- **Eg :once rootkit is successfully installed ,one can gain access to system at later stage also,so can spend time in looking around for more attack threads.**
- **Move from one point to another without committing to a single point.**

EVASION

- One of the main goal of a tester is to remain anonymous/undetected during the observation,unless there’s a requirement to prove to blue team about the attack.
- Covering up the attack takes lot of time and working way low below the radar will not fetch more information about the vulnerabilities.
- There are several ways for an attacker or tester to be detected in the network.

EVASION-WAYS FOR A TESTER TO GET DETECTED IN THE NETWORK

- **Intrusion Detection System. IDS can exist as a network device, monitoring the network for malicious packets and communications. It can also run on a server that is being used for other services.**
- **Most types of IDS detect attacks in one of three basic ways.**
- **Signature Analysis-Most of the attacks have a predictable structure.**
- **A signature is a rule simply stating if there is an application level request that is known to be used as part of an attack, then the administrator needs to be notified or the event logged.**
- **Protocol Analysis-To check the inherent vulnerabilities in the protocol itself.Eg:FRAG Attack-Illegal Offset values causing overwriting of packets during Reassembly.**

Continued..

Anomaly-based Method:

Anomaly-based IDS was introduced to detect unknown malware attacks as new malware is developed rapidly.
In anomaly-based IDS there is the use of machine learning to create a trustful activity model and anything coming is compared with that model and it is declared suspicious if it is not found in the model.

EVASION-WAYS FOR A TESTER TO GET DETECTED IN THE NETWORK

- **Anomaly Detection-Anything outside an acceptable standard operating envelope.**
- **There are several types of anomaly Detection**

  Anomaly Signature-Define the normal operating conditions
  Statistical Modeling-To Detect whether it is an attack or not.
  Observation. By monitoring system activity, log files, and system status a hacker can be detected based on the reaction the environment has to a typical interference.
  Evasion: Sending packets with limited Time to Live (TTL), with excessive time between each to bypass IDA but not lose the attention of the target system, injecting malicious data through URLs that may not be detectable, or using invalid characters, are only a few examples of evasion techniques that have the potential to expose the attacker.

THREADS AND GROUPS

- **The concept of threads and groups are used to evaluate the success and tactics of an attack.**
- **Attacks during the exploitation phase can be broken into two categories: threads and groups.**

- **Threads are a single collection of linked actions with a focal point and a traceable path.**

- **Groups are combinations of similar or seemingly unrelated threads to meet a greater goal.**

THREADS

- A thread is a related set of actions leading to a conclusion.
- The conclusion can be an exploited vulnerability allowing the implantation of a trophy and obtaining sensitive data, essentially proving the impact of the vulnerability found on a system.
- Following a thread also can reach a dead end.
- Threads are a basic form of attack. They use information available to move through each layer of the security infrastructure with little consideration for the success or failure of previous threads exercised in the past.
- It is the act of attacking a set of systems with the intent to go as far as one can while meeting the planned objectives. This method promotes the search for more vulnerabilities, but does not ignore the need to exploit an opportunity.

THREADS

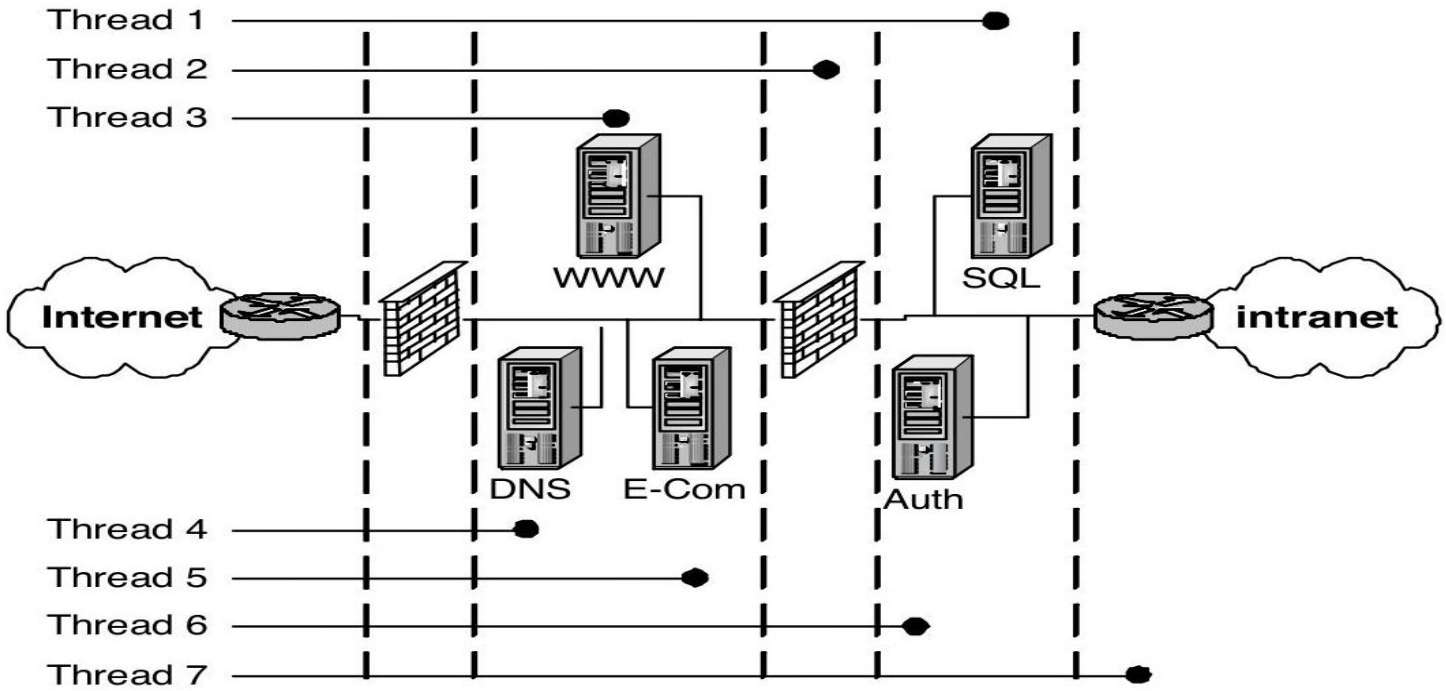


FIGURE 12.1 Each Attack Has Its Own Set of Hurdles and Targets

THREADS

- **Thread 3,4,5-Attack on DMZ**
- **Thread 2-inner firewall**
- **Thread 1,6-Interacting with servers behind the inner firewall**
- **Thread 7-made to internal network-false packets, manipulating one of the servers in the DMZ or inner servers, or simply taking advantage of poor security practices.**
- **Because each thread is a unique set of tasks potentially employing different tools there is the opportunity to spread the attack out over multiple sources in addition to lengthening the time between packets, ultimately dipping farther under the radar.**

GROUPS

- Groups are a representation of two concepts.
- Each thread is independent, but may leverage an aspect of a previously used thread to branch off and logically jump a layer.
- For instance, a thread resulting in a deeper attack, such as thread 7, may diverge from a previous attack by branching from a point well before the layer required to be bypassed.
- Thread 5 gains access to the E-commerce server and thread 2 makes it to the inner firewall. However, the success of thread 1 is based on a Trojan implanted in the E-commerce server thanks to thread 5 ?

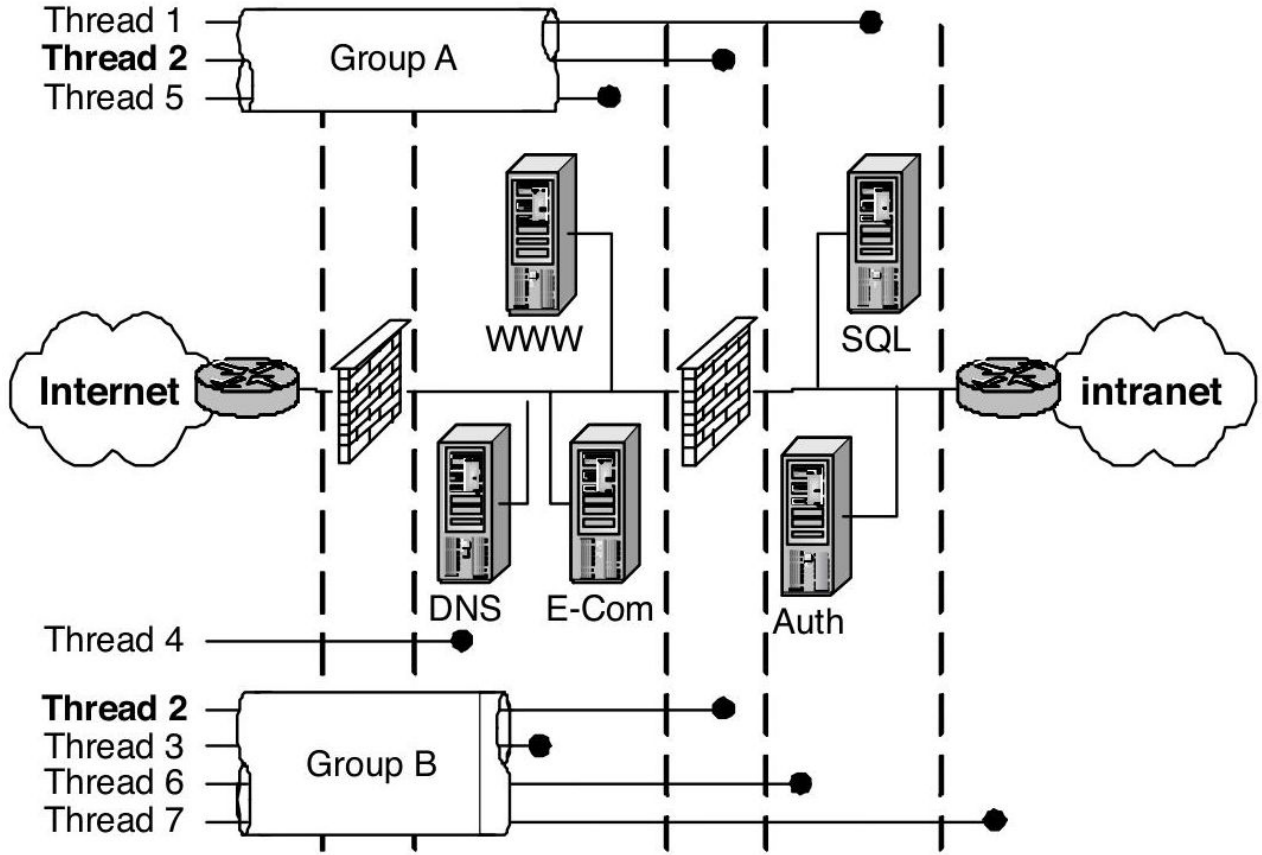


FIGURE 12.2 Threads Can Be Combined to Build Highly Successful and Aggressive Attacks That Are Fast Moving and Productive

OPERATING SYSTEMS

- **Attempts /attacks on operating system are most commontactics used by attacker/penetration tester**
- **Windows-Most user friendly OS,but not much secure**
- **Wireless NW issue**
- **UNIX-MOst secure,of late some vulnerabilities are found without timely updation of patch releases.**

- **Solaris system-Standard installation-unnecessary services**

Large Scale Cyber Attack Targets

Outdated Versions of Windows OS

PASSWORD CRACKERS

- Password crackers operate on the theory that eventually, given enough time, combinations, and permutations, the tool will eventually determine the password.
- Once a password is “cracked” it allows the tester (or hacker) to assume the user’s identity,thereby granting them access to all the data they are normally permitted to access
- eg:Lophtcrack
- A password cracker tool uses different methods to achieve
- its objective: some use word lists, phrases, or other combinations, including numbers and symbols to find out what the user has set as a password.
- Algorithm Based Attack

Phishing

Social Engineering

Dictionary Attack

Rainbow Tables

Brute Force

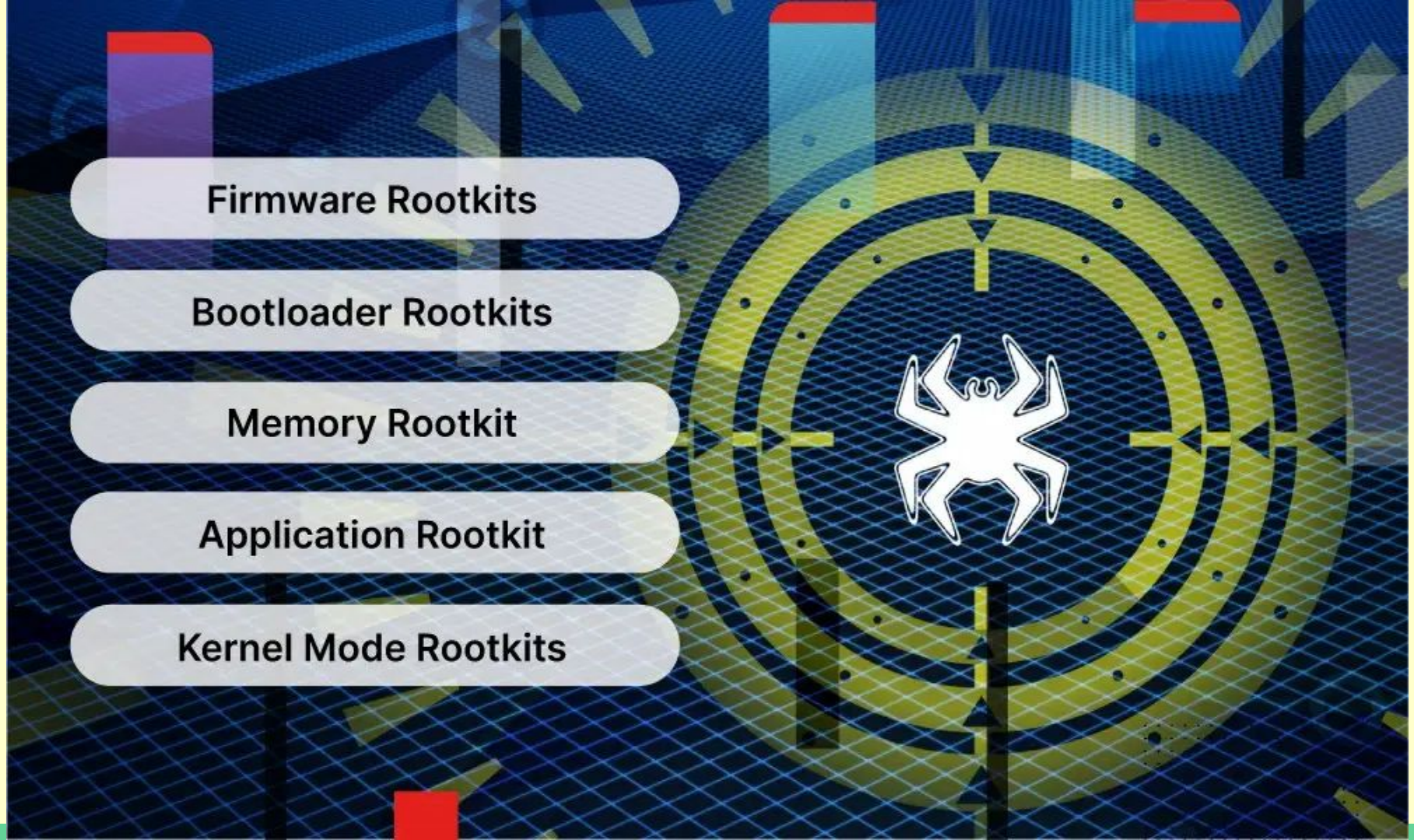
PASSWORD CRACKERS

- Password crackers operate on the theory that eventually, given enough time, combinations, and permutations, the tool will eventually determine the password.
- Once a password is “cracked” it allows the tester (or hacker) to assume the user’s identity,thereby granting them access to all the data they are normally permitted to access
- eg:L0phtcrack
- A password cracker tool uses different methods to achieve
- its objective: some use word lists, phrases, or other combinations, including numbers and symbols to find out what the user has set as a password.
- Algorithm Based Attack

ROOTKIT

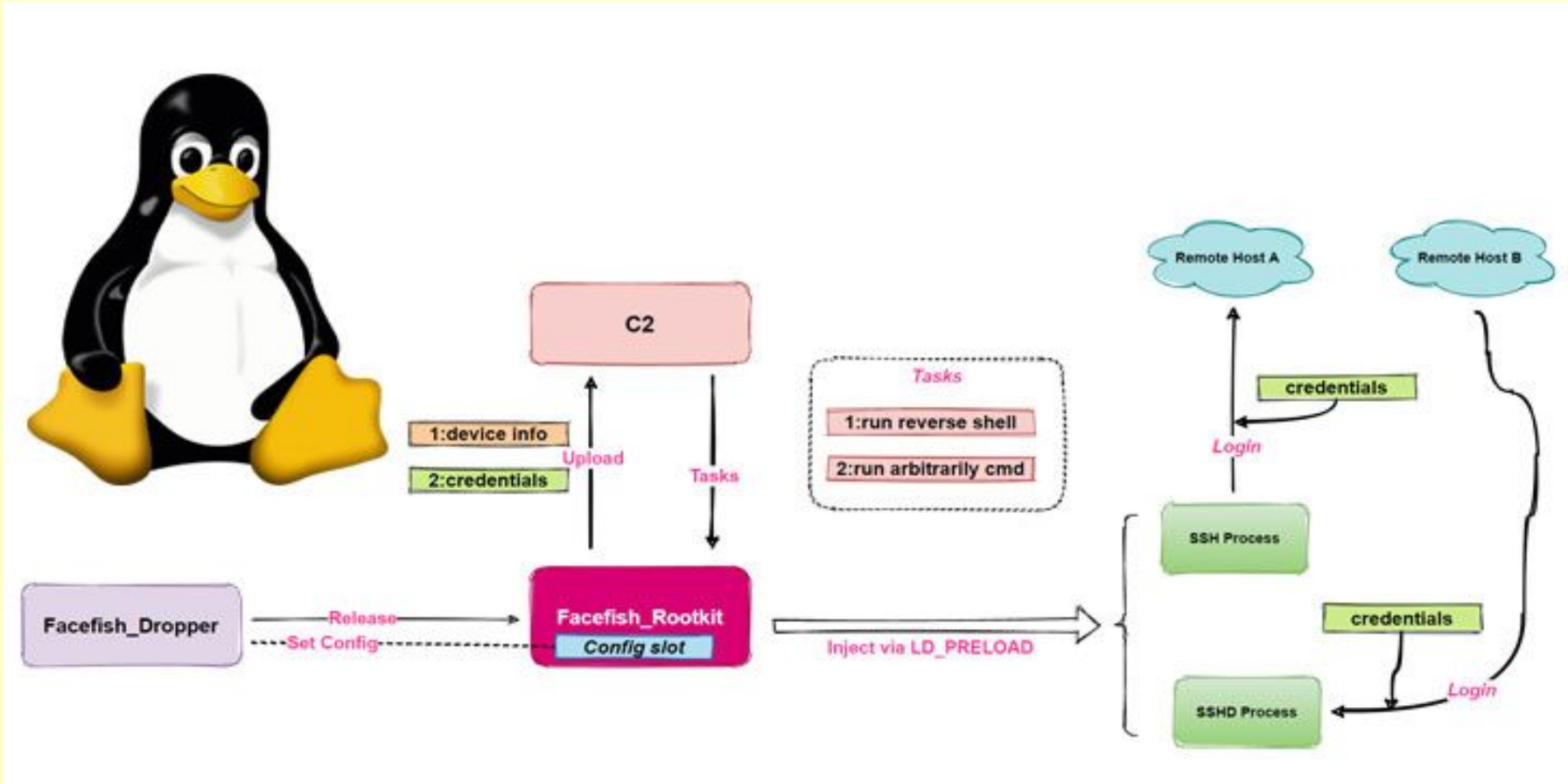
- A rootkit is a collection of tools, or a program itself, a hacker installs on a system once she has gained initial access to that system.
- A rootkit allows a hacker to come back to the compromised system at a later time, or to run services remotely on the system without being detected. This is done by installing a backdoor daemon, stemmed from the rootkit itself, which usually runs on a different port than the typical service they utilize.
- Rootkits typically contain such subprograms as network sniffers, log cleanup scripts, and Trojan backdoor daemons within the tool.
- The rootkit uses binaries, which it replaces, making the hacker invisible to monitoring tactics and system administrators.

Types of malware


Firmware Rootkits
Bootloader Rootkits
Memory Rootkit
Application Rootkit
Kernel Mode Rootkits

ROOTKIT

- **One of the most popular rootkits is the Linux rootkit. This rootkit has undergone massive changes throughout history. Stemming from April 1996 with version 1, these massive changes have morphed into rootkits such as the T0rn rootkit and the lion worm.**
- **The most common method of identification of a rootkit is by utilizing a file integrity checker such as Tripwire to identify system changes**

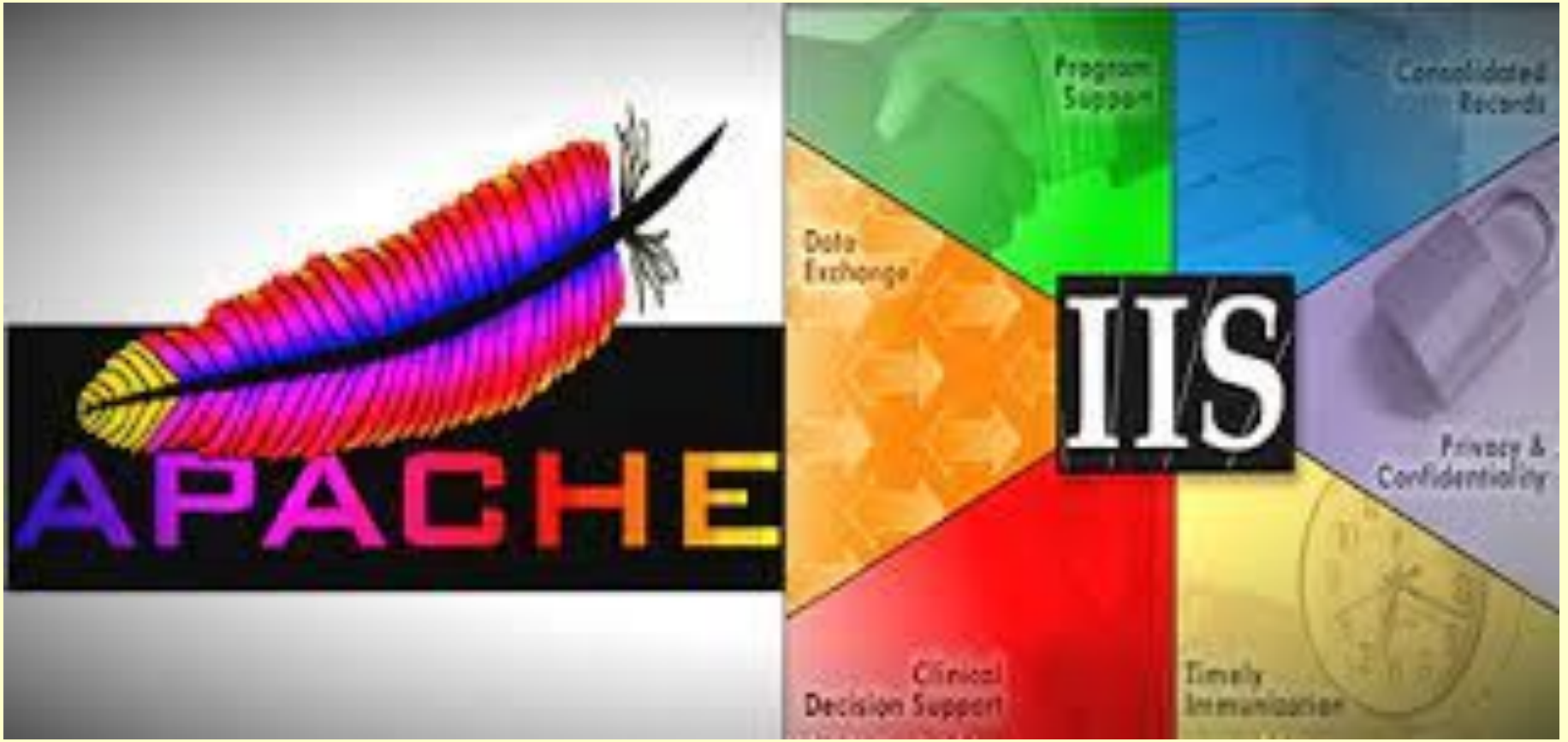

C2
1:device info
2:credentials
Upload
Tasks
Tasks
1:run reverse shell
2:run arbitrarily cmd
Remote Host A
Remote Host B
credentials
Login
SSH Process
Facefish_Dropper
Release
Set Config
Facefish_Rootkit
Config slot
Inject via LD_PRELOAD
credentials
Login
SSHD Process

APPLICATIONS

- **Applications can open a system up to a plethora of vulnerabilities. This is due to two main reasons: the application itself is not configured securely, thus allowing a hacker to gain access to a system through the misconfigured application,**
- **The system itself is not secure, thereby making the application run in a nonsecure manner.**
- **During a penetration test, three main types of applications are assessed for the level of threat they expose the organization to:**
  - **Web, distributed, and customer applications.**

WEB APPLICATIONS

- Three popular Web server applications used in many companies today are Apache,IIS, and iPlanet
- Attempt to exploit a vulnerability through the CGI scripts
- Scripts can present two security vulnerabilities:
    - they can leak information about the host system itself, helping a malicious user to break in, and scripts that process remote user input, such as contents of a form or a “searchable index” command, may be vulnerable to attacks in which the malicious user tricks it into executing commands.
- Whisker, an open source tool, is often used to scan Web servers for CGI script vulnerabilities.

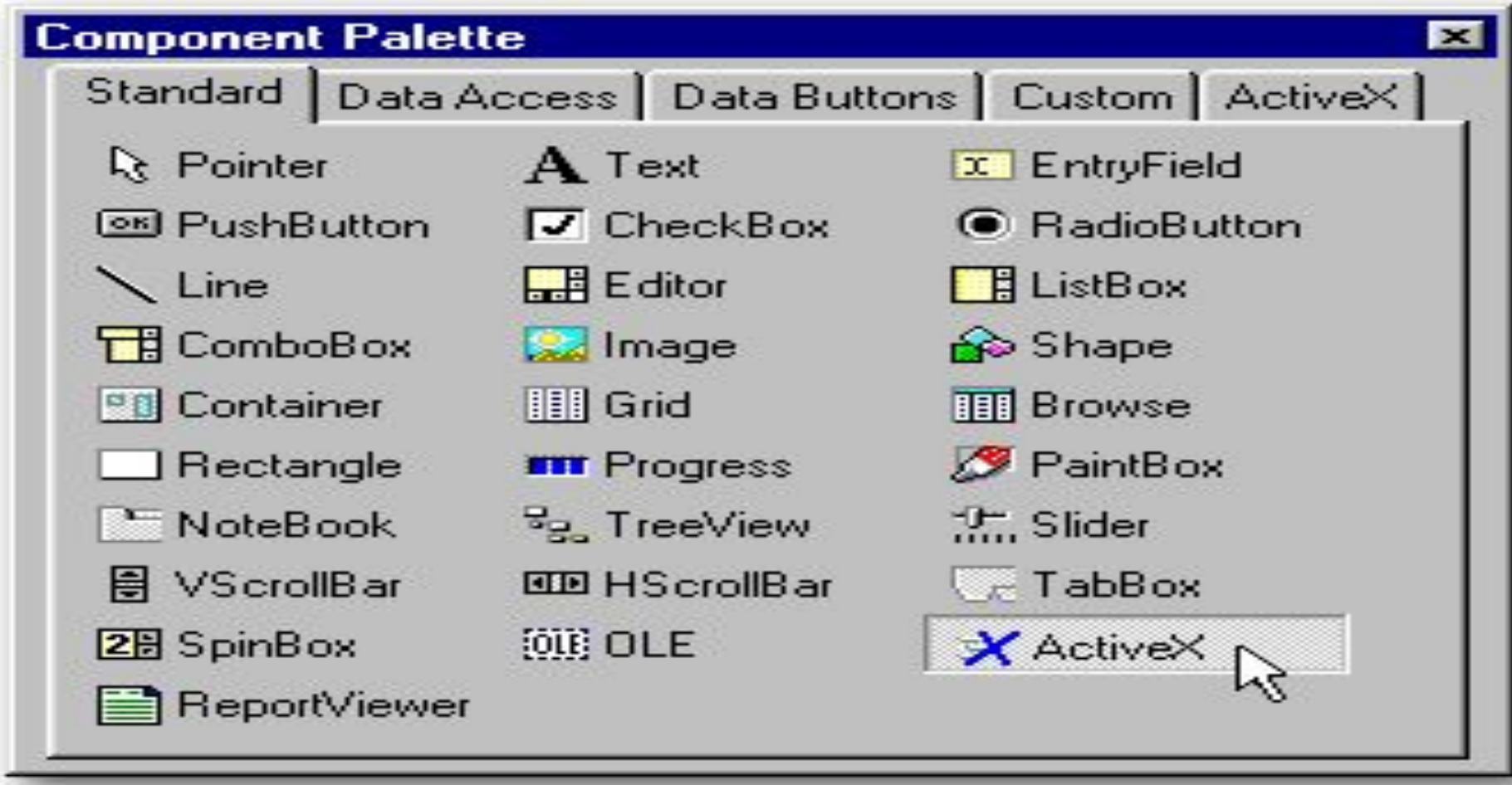

APACHE
IIS
Program Support
Consolidated Records
Data Exchange
Privacy & Confidentiality
Clinical Decision Support
Timely Immunization

WEB APPLICATIONS

- Another popular tactic in attempting to exploit a vulnerability on a Web serveris to try to execute a command through the HTML directory itself.
- A tester may attempt to enter in a random URL with specific attributes to exploit the Web server. These URLs typically include suffixes such as .exe, .sh, or login.pl. This would permit the tester to execute potentially destructive commands remotely.
- **ActiveX** is another area of concern with Web applications. There have been several instances allowing code execution on another user's machine.
- **ActiveX** and workstation builds should have their browsers set with security in mind

DISTRIBUTED APPLICATIONS

- **Distributed applications** include those that permit users throughout the company to access them in order to do their jobs properly.
- Distributed applications are those that include a database, mail, or collaboration server.
- A database server may contain sensitive HR information about the employees within the organization, and another that contains highly sensitive financial data on the organization itself may be used by finance.
- **Access control List**
- A tester finding the database server can attempt to exploit a vulnerability either by attempting to gain a user's password, or using a password cracker, and then accessing the system to retrieve the highly sensitive information.

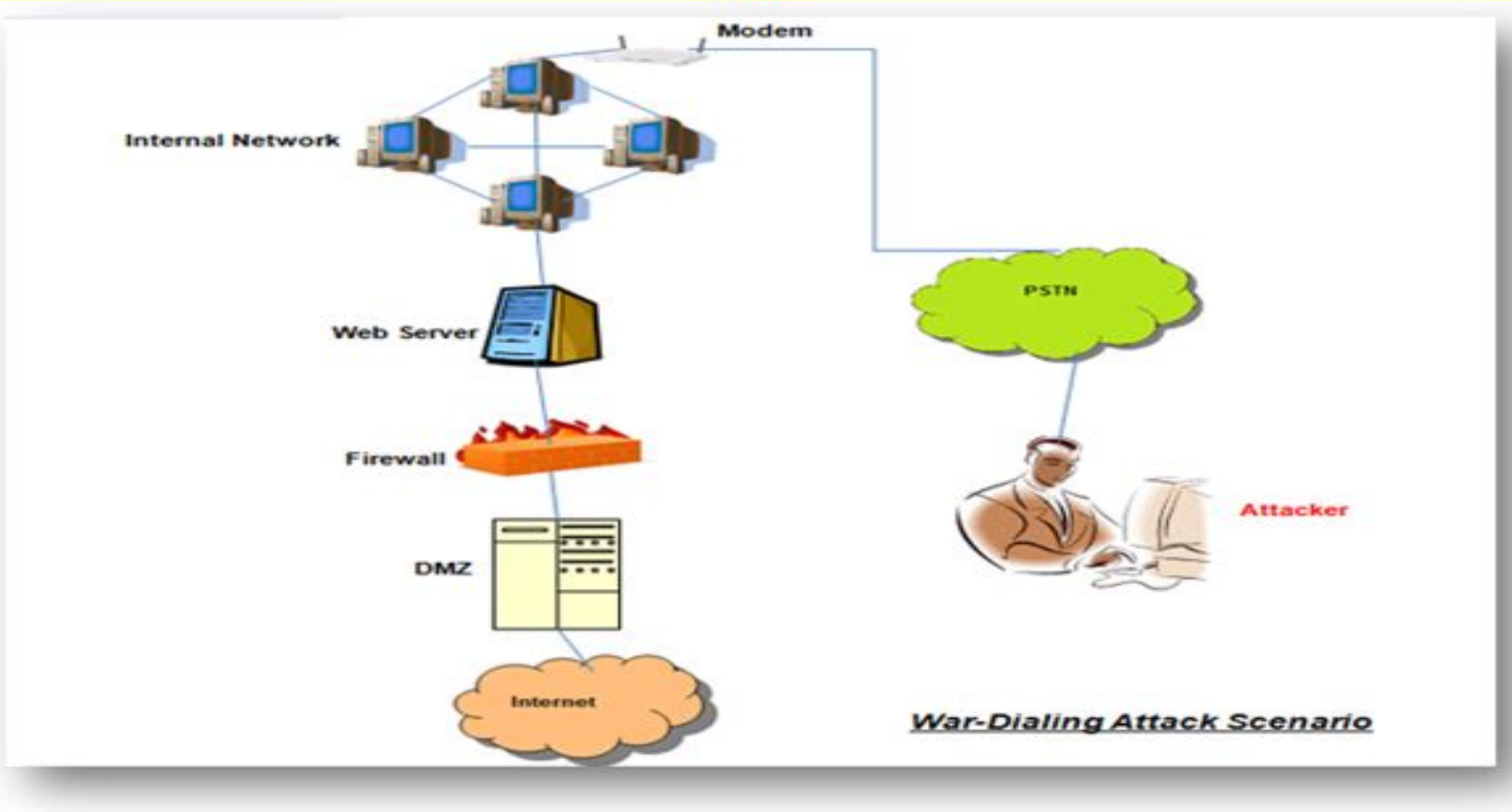

Component Palette
Standard
Data Access
Data Buttons
Custom
ActiveX
Pointer
Text
EntryField
PushButton
CheckBox
RadioButton
Line
Editor
ListBox
ComboBox
Image
Shape
Container
Grid
Browse
Rectangle
Progress
PaintBox
NoteBook
TreeView
Slider
VScrollBar
HScrollBar
TabBox
SpinBox
OLE
ActiveX
ReportViewer

CUSTOMER APPLICATIONS

- Customer applications are those to which the organization’s customers need access,either through a partner agreement or an end-user agreement.
- Eg:Retrieve bank statements through Internet.
- Web server and database server should be separated by atleast a firewall.
- Secure configuration would ensure the traffic between the two devices is configured so that any traffic coming from the Internet to the Web server resides over HTTP(s)
- when the Web server queries the database server, it must transfer to the database protocol (e.g., MySQLTCP 3306), and all traffic from the Web server to the Internet is only over HTTP(s).
- This ensures that the Web server cannot be used as a stepping stone to get to the database server maliciously.

WARDIALING

- The usage of modems
- The test simply involves dialing numbers in search of a system that may be exploited in some manner to gain access.
- Randomize-If we try sequentially various nos,-alarm.So randomization is done


Modem
Internal Network
PSTN
Web Server
Firewall
Attacker
DMZ
Internet
War-Dialing Attack Scenario

WARDIALING STEPS

- Number Scanning-Find out telephone numbers are connected to computers, fax machines, modems, or simply do not answer.
- System Type Scanning.-Find if any modern fis
- ’Banner Collection-For every number that answered with a modem tone,There is the possibility that the system will provide a banner communi- cating the type of system and status.
- Default Access. There are some situations where the system is configured to allow access simply based on a username or group name without a password. This is sometimes used to accommodate maintenance access or poorly configured systems.

WARDIALING STEPS

- **Brute Force.** When a username and password combination is required, this is the act of testing as many passwords as possible. Typically this is supported by a collection of commonly used passwords passed to th remote system sequentially until one of them works.

- Another aspect is simply defining the scope of characters to use and the assumed length of the password and allowing the system to step through each until the password is cracked.

Network

- It is important to attempt to exploit the network devices that are critical to the overall security posture of the organization.

- This includes the network infrastructure, the routers and gateways between the Internet and intranet, intranet and extranet (client networks), and internal gateways to more secure networks.

PERIMETER

- The perimeter of a company's network is responsible for protecting the network behind it from external entities. This can be the Internet, intranet, or extranet.
- Firewalls are the most popular way to ensure the perimeter of any network is secure.
- During a penetration test, firewalls are often closely examined in order to ensure a high level of threat does not exist due to a misconfigured firewall. One tactic is to ensure compartmentalization exists on the firewalls.
- Each interface on the firewall should be assigned a security level.

Perimeter

- **The DMZ, which houses Internet applications,and an internal segment, which contains the server holding company-sensitive data, should not be connected to same interface of the firewall.**
- **This design flaw is easily detected, because access to and from the DMZ and internal segment would not pass**
- **Through the firewall, allowing all services through.**
- **Another exploit usually identified during the penetration test would be to ensure that any service not needed is prohibited through the firewall to another segment.**
- **Usually HTTP(s) should be the only service permitted inbound to the Web servers in a DMZ. If an exploit were attempted from the Internet, and the tester identified that not only was HTTP accessible, but also such ulnerability-filled services such as NTP, SNMP, and even FTP, this would be considered a high-level threat to the company.**

NETWORK NODES

- **Routers are devices to gain access to networks.**
- **During the penetration test, the tester needs to ensure that at a minimum the following characteristics have been implemented on the routers.**
- **Do the routers inspect traffic on the TCP/IP layer with packet filters, and do they drop any malformed or fragmented packets?**
- **Has NAT been implemented to hide IP addresses for all systems, or at least the critical systems? A security vulnerability within a router is allowing source routing of a packet, which is enabled by default on some systems. Meaning, if a hacker knows the company's network is a private range of IP addresses, it can't route over the Internet, but the hacker can traceroute to the edge device and then sourceroute the packet to attack the private net from the Internet.**

SERVICES OR AREAS OF CONCERN

- Hackers can infiltrate your networks and systems by leveraging weaknesses in applications, operating systems, and services.
- Hackers have the time, patience, and resources to discover these vulnerabilities long before developers.
- Configuration by inexperienced administrators could also lead to a higher level of exploitation by leaving unnecessary or often vulnerable services enabled.
- These services, if not configured properly, could lead to a system compromise from a source both internal and external.
- By establishing baseline builds for both Windows and UNIX environments, companies can reduce the risks associated with these unnecessary services

Continued..

How is access to the routers permitted?
Is it username/password based, or two-factor authentication, such as through the user of SecurID?
If the answer to any of these is “No,” then the tester has a multitude of tests to perform in order to attempt an exploit against a router within the network infrastructure.
Perhaps the edge router has a modem attached to it, which has been left enabled. During the wardialing exercise, access to this router would be identified, and then the process of attempting to gain access would be followed.

SERVICES

- Services are necessary to allow the system to function, and to provide business functionality.
- Services can be exploited through a variety of methods during a penetration test. Prior to testing the systems for exploits, a clear understanding of the system's functionality is helpful to avoid testing services that shouldn't be running in the first place.
- In some cases, FTP may not be a required service to be running on a system, so the removal of it would be the recommendation instead of stating a specific exploit against the FTP service.
- Often the administrators of a large network are not sure what services are running on a system. For this purpose, the tester should run a tool against all the systems in question in order to clearly identify what services the system is running; such tools include **NMAP, Nessus, and ISS scanner**.

SERVICES (Started by Default)

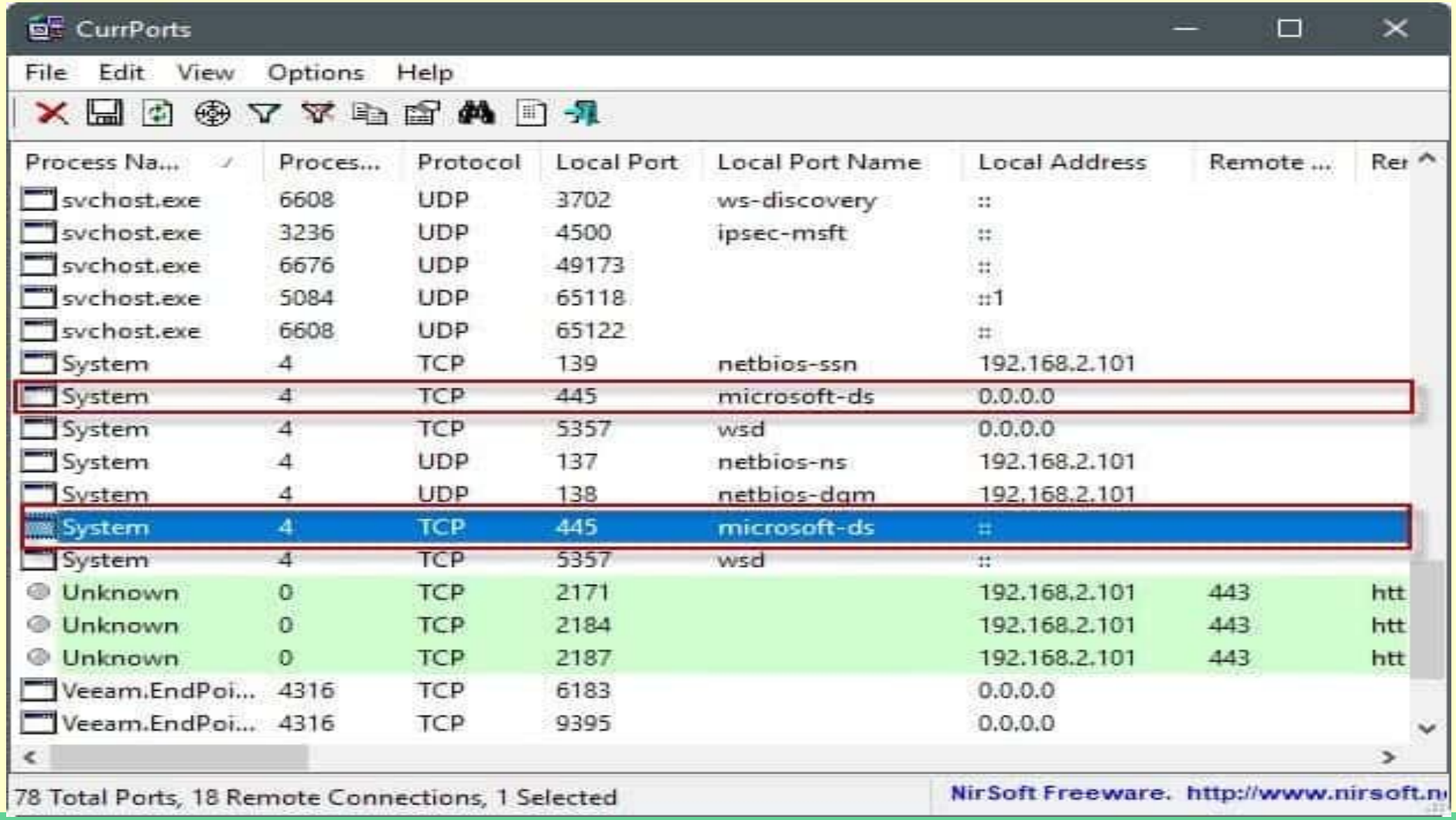
- **Many operating systems install and start unnecessary services by default. Although these services do serve a purpose, most are not needed for the system and applications to function properly.**
- **Eg:sendmail, savecore, rpcbind, FTP, telnet for UNIX, and Internet Information Server (IIS) for Windows NT/2000/XP.**
- **Every effort should be made to contain these services and disable them if not needed.**
- **The creation of a “standard” base build for both UNIX and Windows systems has many of the security recommendations already configured.**
- **This will make the administrator job easy to manage the security aspects.**

WINDOWS PORTS

- The Server Message Block (SMB) and the Common Internet File System (CIFS) protocols are the mechanisms that permit a system to modify remote files as if they were locally stored.
- The Sircam virus (CERT Advisory,2001-22) and Nimba worm (CERT Advisory 2001-26) were spread rapidly by discovering unprotected network shares and placing a copy of themselves there.
- Many systems, especially desktop users, open their systems up to co-workers for convenience, or sharing of files, when in fact they are opening them up to hackers that turn the convenience into malicious activity.

WINDOWS PORTS

- **The tester should determine whether sharing is necessary before attempting any exploits.**
- **A scanning tool such as ISS, NMAP, or Nessus can determine which systems have file sharing enabled; then it is best to evaluate whether it is needed.**
- **If sharing files across the network is a business requirement then the tester can attempt to authenticate a system without being required to enter a username and password.**
- **They should be configured to require a user to authenticate before connecting.**
- **All ports used for Windows sharing should also be blocked at the network perimeter; these ports include TCP and UDP 137-139 and TCP and UDP 445. These ports should also be restricted internally through the firewalls, only permitted when a source and destination IP address is included, along with the user authentication.**


CurrPorts
File Edit View Options Help
Process Na... Proces... Protocol Local Port Local Port Name Local Address Remote ... Rer
svchost.exe 6608 UDP 3702 ws-discovery ::
svchost.exe 3236 UDP 4500 ipsec-msft ::
svchost.exe 6676 UDP 49173 ::
svchost.exe 5084 UDP 65118 ::1
svchost.exe 6608 UDP 65122 ::
System 4 TCP 139 netbios-ssn 192.168.2.101
System 4 TCP 445 microsoft-ds 0.0.0.0
System 4 TCP 5357 wsd 0.0.0.0
System 4 UDP 137 netbios-ns 192.168.2.101
System 4 UDP 138 netbios-dgm 192.168.2.101
System 4 TCP 445 microsoft-ds ::
System 4 TCP 5357 wsd ::
Unknown 0 TCP 2171 192.168.2.101 443 htt
Unknown 0 TCP 2184 192.168.2.101 443 htt
Unknown 0 TCP 2187 192.168.2.101 443 htt
Veeam.EndPoi... 4316 TCP 6183 0.0.0.0
Veeam.EndPoi... 4316 TCP 9395 0.0.0.0
78 Total Ports, 18 Remote Connections, 1 Selected
NirSoft Freeware. http://www.nirsoft.n

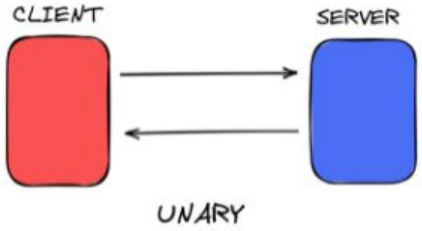
NULL CONNECTION

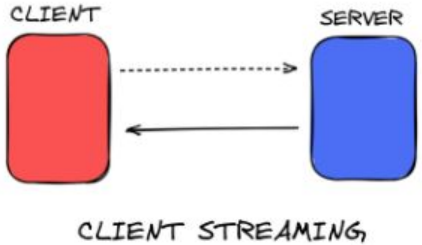
- **Microsoft built an “administrator” backdoor, into their Windows products. This default “backdoor” is an anonymous connection called an interprocess connection share or IPC$.**
- **It is called a “null” connection because it is available for any Microsoft Windows machine to access that share.**
- **Why is this a “bad” thing to have?**
    - **Because it allows any other Microsoft computer to access your “C:” drive; the main partition for your operating environment. Hackers can place Trojans and viruses and even obtain password files that are contained in this “default” share.**

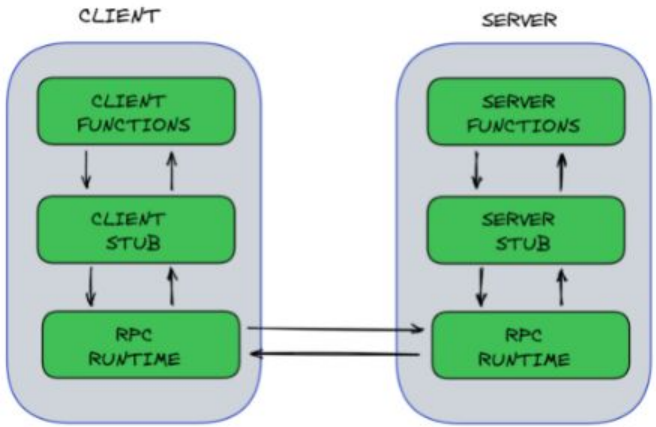
REMOTE PROCEDURE CALLS (RPC)

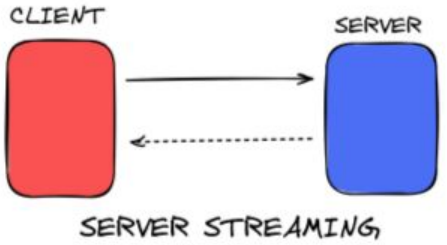
- Remote Procedure Calls is a service that allows programs on one system to execute procedures on a second system by passing data and retrieving the results.
- It is a widely used service for distributed network services such as remote administration, NFS, and NIS.
- In most cases, RPC services execute with root privileges, therefore,when an RPC service is exploited, it can provide the hacker with root access to the system.

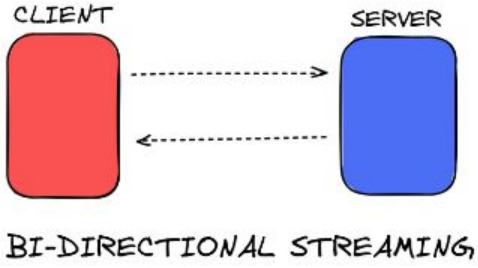
Remote Procedure Call (RPC)











REMOTE PROCEDURE CALLS (RPC)

- RPC services are usually exploited through buffer overflow attacks because the RPC services do not perform sufficient error checking or input validation.
- Some examples of RPC services include **rcp.ttdbserverd, rpc.cmsd, rpc.statd, rpc.mountd, sadmind, cachefs, and snmpXdmid.**
- In order to ensure exploitation is not possible, the tester should check to make sure that RPC TCP Port 111 and the RPC loopback TCP and UDP Ports 32770 to 32789 are blocked at the network perimeter.
- Specifically on systems that require the use of NFS, the tester should ensure that host/IP-based export lists are implemented, file systems should only be read Only, or no-suid, and “nfsbug” should be used to scan for vulnerabilities.
- If one of the above is not implemented, chances are the tester will find an exploit on the NFS server using the RPC service.

SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP)

- The Simple Network Management Protocol is used extensively in all organizations to remotely monitor and configure almost all types of TCP/IP-enabled devices.
- SNMP communication consists of exchanged messages between the management systems and the devices that run the SNMP agent
- SNMP is used by network management systems to determine the “health” of a networked device. These devices range from routers and switches to servers and desktops.
- SNMP is a cleartext protocol as discussed earlier. The information gathered by this protocol can be used by hackers to gain valuable knowledge such as the OS version, failed hardware, the managing NMS server IP, subnet mask, and internal and external IP information.
- There are two “default” network paths for SNMP, public (read only) and private (read/write).

BERKELEY INTERNET NAME DOMAIN (BIND)

- BIND is an application used to provide users and applications with domain name service.
- It is a very popular and common target for attacks because it is the most widely distributed DNS software and the servers running BIND are usually accessible from the Internet.
- The exploits typically involve buffer overflows and denial-of-service attacks.
- BIND should not be installed on servers running applications other than DNS.
- For those needing to run BIND, system administrators should keep up to date on the latest versions and/or patches for BIND. BIND should also be configured to run as a non privileged account and in a secured environment such as “chroot.”

BERKELEY INTERNET NAME DOMAIN (BIND)

- **BIND is an application used to provide users and applications with domain name service.**
- **It is a very popular and common target for attacks because it is the most widely distributed DNS software and the servers running BIND are usually accessible from the Internet.**
- **The exploits typically involve buffer overflows and denial-of-service attacks.**
- **BIND should not be installed on servers running applications other than DNS.**
- **For those needing to run BIND, system administrators should keep up to date on the latest versions and/or patches for BIND. BIND should also be configured to run as a non privileged account and in a secured environment such as “chroot.”**

COMMON GATEWAY INTERFACE (CGI)

- **CGI scripts are used by Web servers as a means to provide collecting Web user information, execution of programs, and accessibility to files requested by users of the Web site.**
- **CGI programs normally run with the same permissions as the Web server software. Sometimes, if not configured correctly, these permissions are of a privileged user such as “root.”**
- **Hackers can exploit vulnerable CGI programs, most of which are installed by default**

COMMON GATEWAY INTERFACE (CGI)

- Elements such as running the programs with least-privilege or using valid buffers to prevent overflows.
- Ensure data arrays process their data correctly.
- A program accepts data entry from a user, places it in an array or variable that stores the information in memory, and then proceeds to process the data without checking first if the entry was valid.
- Eg:A cross-scripting vulnerability that interprets the data input and forces it out to the shell for execution, thus allowing a user or attacker to execute other binary code available on the system such as an FTP session or a remote shell.

COMMON GATEWAY INTERFACE (CGI)

- Elements such as running the programs with least-privilege or using valid buffers to prevent overflows.
- Ensure data arrays process their data correctly.
- A program accepts data entry from a user, places it in an array or variable that stores the information in memory, and then proceeds to process the data without checking first if the entry was valid.
- Eg:A cross-scripting vulnerability that interprets the data input and forces it out to the shell for execution, thus allowing a user or attacker to execute other binary code available on the system such as an FTP session or a remote shell.

CLEARTEXT SERVICES

- **Services that use unencrypted data present another challenge for administrators.**
- **Eg:FTP, telnet, and e-mail are frequently used by everyday users especially e-mail.**
- **Alternatives:OpenSSH (freeware) or Secure Shell (commercial software)**

NETWORK FILE SYSTEM (NFS) SERVICES

- **UNIX systems utilize NFS to share files and directories and drives across the network.**
- **NFS is insecure in its natural state. Most administrators allow read and write access to everyone rather than narrow down the list to a select few.**
- **Since NFS runs on an Internet-facing server,the attackers, or anyone really, is provided with access to the files, directories, or drives on that system.**
- **The attacker is only limited to the actual permissions applied to the mounted system.**
- **Once permission is obtained,attacker can place any files or remove files from your NFS share.**
- **There are other vulnerabilities within an unpatched “nfsd,” the daemon that runs NFS, that gives an attacker root privileges.**

DOMAIN NAME SERVICE (DNS) SERVICES

- DNS does the name resolution portion of BIND.
- It translates a domain name into an IP address and vice versa.
- Applications use DNS exclusively to look up address information when they need to send information over the Internet.
- Without DNS, users would have to know the exact IP address every time they wanted to surf the Web or send an e-mail. Hence,DNS is critical to the Internet.
- Attackers can deny access to or manipulate data from the DNS servers. Due to the fact that most DNS servers exist outside a firewall, it is very easy for attackers to employ a DoS attack by flooding the server with DNS requests.

DOMAIN NAME SERVICE (DNS) SERVICES

- DNS does the name resolution portion of BIND.
- It translates a domain name into an IP address and vice versa.
- Applications use DNS exclusively to look up address information when they need to send information over the Internet.
- Without DNS, users would have to know the exact IP address every time they wanted to surf the Web or send an e-mail. Hence,DNS is critical to the Internet.
- Attackers can deny access to or manipulate data from the DNS servers. Due to the fact that most DNS servers exist outside a firewall, it is very easy for attackers to employ a DoS attack by flooding the server with DNS requests.

DOMAIN NAME SERVICE (DNS) SERVICES

- **Attackers can also “hijack” a DNS server IP address and respond to legitimate requests from unsuspecting users sending them to Web sites containing Trojans, or worse, they are able to obtain usernames and passwords, credit card information, or bank account information.**

- **Zone transfer-Seeing that DNS has all the IP addresses associated with names of systems, it can be helpful for the attacker to have the IP addresses of systems accessible from the Internet. If not configured properly, the DNS system will provide all the IP addresses to a general request, revealing all the addresses of the systems supported by that DNS server.**

- **DNS information can be helpful in formulating an attack and assisting with the identification of the overall structure of the Internet connection. For example, there may be several IP addresses defined in DNS supporting systems behind a firewall. If some of the IP address ends up at a firewall, a hacker knows which systems are behind a firewall or directly accessible to the Internet.**

FILE AND DIRECTORY PERMISSIONS

- Files and directories are owned by users on a system. This means for other users to access or execute these files, the owner must assign the appropriate level of permission to his files and directories.
- Permissions are very similar between UNIX and Windows. There are three basics: read, write, and execute.
- Although there are many more in Windows, UNIX offers a “special” one called “setuid/setguid.”
- Vulnerabilities exist in file and directory permissions. They can lead to elevated privileges, buffer overflows, and worse, the compromise of your server. Find a balance between keeping your servers secure and application/user functionality.

FTP AND TELNET

- Problems:sends Information in cleartext,
- buffer overflows and brute force password attacks
- System administrators need to ensure the latest patches have been applied to those systems running these services.
- Another issue with FTP is the fact that some administrators fail to remove or lock down the anonymous or guest account.

INTERNET CONTROL MESSAGE PROTOCOL (ICMP)

- ICMP is used mainly by administrators as a quick way to determine if a server or,more appropriately, if an interface on a server is up or down.
- Ping provides a very simple answer and is one of the most common denial-of-service attacks.
- One of the first tools created to perform the denial-of-service attack is POD or ping of death.
- Traceroute on the Windows platform utilizes ICMP and actually provides the path a packet takes to reach that interface, usually in great detail. That detail is used by hackers to find out the IP of your firewall or Internet router.
- Other ICMP requests include timestamps, network masks, and other useful information.
- By disabling this protocol at the Internet router and firewall you prevent anyone, not just hackers,from being able to clearly identify your network.

IMAP AND POP

- Commonly used by Internet e-mail applications, these protocols allow remote users to access their e-mail over the Internet. This means ports have to be open on the firewall to permit this access.
- Hackers using a firewall scanning tool such as “firewalk” can determine all the open ports and using known exploits for IMAP and POP can gain access to your network and/or e-mail systems.
- Traffic is not usually encrypted, unless you are using SSL.

NETWORK ARCHITECTURE

- **A poorly designed network can allow “unprotected” Internet access into your network. Multi-homed servers and servers in a DMZ are two of the most common sources for intrusion. This is due to the fact that these servers have interfaces that do not pass through a firewall.**
- **So Network security is very important**