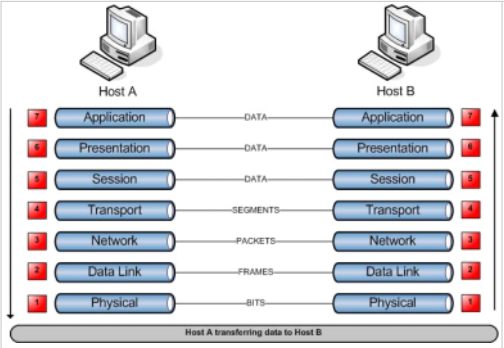
Key Concepts

25 February 2021 08:57

OSI

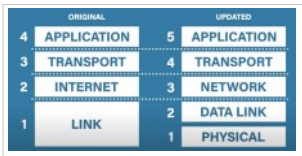


Bottom to Top : "**P**eople **D**on't **N**eed **T**hose **S**tupid **P**ackets **A**nyway".
Top to Bottom : "**A**ll **P**eople **S**eem **T**o **N**eed **D**ata **P**ackets"

- This was introduced to standardize computer networking, basically to allow communication to happen between two different vendor's devices
- Mostly this is not used in REAL WORLD - TCP/IP model
- Layers are numbered. 1 means Physical to 7 means Application
- Physical Layer : Cable, Network Interface Cards (NIC), Hubs
- Data Link Layer : MAC address, Switches
- Network Layer : IP address, Routers
- Transport Layer : TCP, UDP, Port Numbers
- Session Layer : Start & Stop Sessions
- Presentation Layer : Format, Data Encryption
- Application : SMTP, FTP, TelNet

During communication, each layer will add some of its own data (headers) to the information, this is known as encapsulation

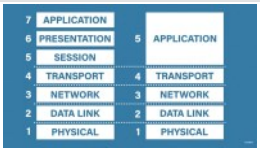
TCP/IP Model



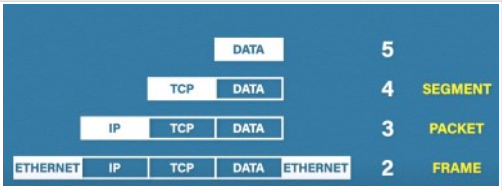
- Original Model has 4 layers, updated model has 5
  - Links layer is split between Data Link and Physical layer
  - Internet layer is renamed to network layer

Protocols are each layers

5. Application : SMTP, FTP, HTTP
4. Transport : TCP , UDP - port numbers will be added here
3. Network : IP, Routers
2. Data Link : Ethernet, Switches
3. Physical : NIC, Cable - touch and feel

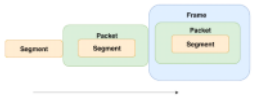


- Compared with OSI - top three OSI layers are combined into one application layer



During communication, each layer will add some of its own data (headers) to the information, this is known as encapsulation
e.g.

5. Application : will have DATA only - DATA
4. Transport : TCP header will be included - SEGMENT
   - that contains information e.g. Source and destination port, sequence no. etc.
3. Network : IP Header - PACKET
   - Source & Destination IP address
2. Data Link : Data Link Header and Trailer both added - FRAME
   - Header : Destination & Source MAC address
   - Trailer : Error checking information that receiver side can check that data is received correctly
1. Physical : Data will be physically transmitted

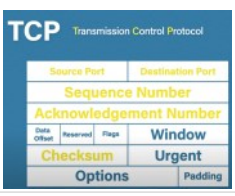
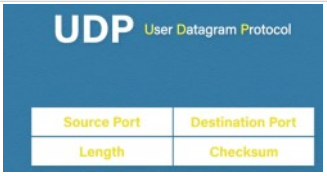


On the receiving part

- The computer checks the Frame destination MAC address - if it matches with own MAC address, it will further process it
- Checks IP address and matches with own
- Transport information will be read further
- Then the application data will be given to receiving application

TCP vs UDP

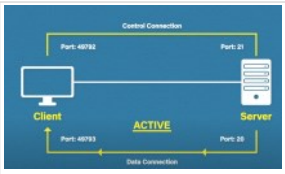
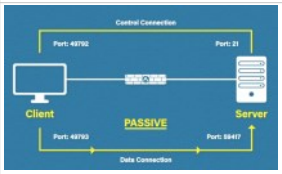
- Depends on application Layers (Application) on how those data to be transmitted - RELIABLE (TCP) or UNRELIABLE (UDP)

TCP	UDP
• Transmission Control Protocol • TCP is resource extensive and have latency because of processing • Good for File transfer, Web page, • Uses three way hand-shaking before transferring data - before & After the connection 1. SYN : send sync signal to the receiver 2. SYN - ACK : receiver respond with his ACK but also sends his own SYN 3. ACK : Sender responds with ACK of SYN of receiver • TCP makes sures packets get delivered by Adding acknowledgement nos. • Sequence nos. ○ Each Data will be sequenced so that receiver can organize them • Acknowledgement ○ Each data sequence will be acknowledged by received • Checksum ○ Receiver validates the checksum ○ In case of invalid Checksum - the corresponding segment will be discarded	• User Datagram Protocol • Machine Gun of Data - Only Firing the data without worry about the receiver's acknowledgement or anything • Used in Voice calls, video calls, Gaming etc. where we need live, real time data where latency is not acceptable • Small header means less information • But it is lighter and quicker
Typical TCP Header 	

FTP

- File transfer protocol, used in file downloading
- Works in client server model where,
  - Server hosts the file
  - Client can access, upload or delete the files
- To access FTP server ftp://192.168.0.8 via Browser or File Explorer
- Can also be using FTP client like Filezilla
- FTP uses TCP

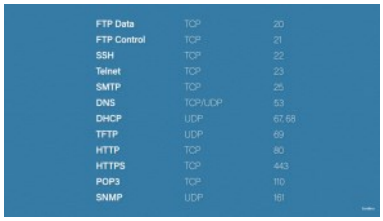
- Disadvantages
  - Lacks basic security features such as encryption - all data will be transmitted in plain text , including the username and password of the FTP server - Wireshark can capture it
- FTPS to be used , FTPS uses TLS internally
- SFTP - SSH File transfer protocol - is part of SSH protocol - not a part of FTP protocol
- TFTP - Trivial File Transfer
  - Use UDP
  - Provides simple and quicker way to transfer a file
  - No security , no authentication, no encryption
  - Helpful in local network e.g. backup configuration file
- FTP server uses two different connections
  - Control connection : GET PUT commands
  - Data Connection :

• ACTIVE data connection • Server initiating the session • in case of firewall it is likely to be blocked as by default rule of the Firewall • Server uses port 20 and client uses randomly generated port	
• Passive data Connection • client initiating the session - Firewall can allow • Client and server both uses randomly generated ports	

Port Numbers

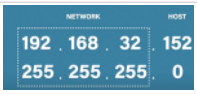
- Port numbers will be choose by Layer 4. Transport layer - where UDP or TCP decision will be made
- Analogy of a letter box in the house - gives access to the postman to your house
- Mostly on the machine (Server) all running applications are having assigned (standard) port number - well known port number
  e.g. HTTP - 80 , SMTP - 25, FTP -21
- port is a logical construct that identifies a specific process or a type of network service.
- A port is identified for each transport protocol and address combination by a 16-bit unsigned number, known as the port number. **2^16 = 65536 ports available in total**
- IP address get data to the computer but the port number is used to send data to the right application
- 0 - 1023 are well known port numbers
- 1024 - 49151 are registered port numbers - companies have registered
- 49152 - 65535 are dynamically assigned port numbers - used to randomly generate unique port numbers for a given computer which it will passes as source port to the server
- For TCP, port number 0 is reserved and cannot be used
- for UDP, the source port is optional and a value of zero means no port

- To see connections - netstat -n



IP Address

- Unique Identifier Assigned to a device connected to the computer network e.g. the way postal service works
- e.g. IPV4 address looks like 192.168.32.152 - AKA Dotted Decimal notation
- No more allocated IPV4 address available :(
- That is why the new IPV6 is designed to give us more expansion to cover other devices
- IP Addresses are linked with interfaces (connections) and not the host or the router

• Total 32 bits - total 32 binary digits • 4 blocks/section (octets) separated by '.' • Each octets goes from 0-255	
Address is separated in two parts • Network ○ Often supplied with subnet mask address (e.g. 255.255.255. 0) to locate the network where the host (individual machine) belongs to. ○ Mostly the network will have 0th at last e.g. 192.168.5.0 • Host	
To send particular message to a given host, use both subnet mask and network and individual pc • Looking at the subnet mask **255.255.255**.0 - the network is located at **192.168.5 where the 3 is our host number within the given network**	

Type A and AAAA

• To make IP address allocation scalable, address are divided into classes • A : 3 octets available for host allocation • B : 2 octets available for host allocation • C : 1 octet available • D : Multi cast address • E : Reserved for Experiment • Easiest way to memorize the IP address class is to look for the first octet • e.g. 10.0.0.0 is A • If starts with anywhere between 1 to 126 then it is A	
• Solution to prolonged the life of IP address by separating out in public and private IP addresses • Both uses same subnet mask, having same no. of hosts • Diff. is public IP is unique but the private IP can be used again and again, saving millions of public IP available to use • The local network uses private IP whereas the ISP will provide 1 public IP to entire network of devices To check IP • Private - ipconfig in command prompt • Public - Google -> what is my ip	 

Mac Address

- At 2. Data link layer - Ethernet
- Media Access Control - Unique identifier assigned to a network interface card (NIC)

- Physical addresses - Unique & can't be changed
- Mac address is of 6 bytes or 48 bits long e.g. 08-00-27-EC-10-61
- Two part
  - First 3 bytes = OUI Organizationally unique Identifier (Vendor) 08-00-27
  - Last 3 bytes = Unique Identifier assigned by a vendor EC-10-61
- Can be displayed in multiple ways
  - 08-00-27-EC-10-61 - Microsoft
  - 08:00:27:EC:10:61 - Linux or Apple convention
  - 0800.27EC.1061 - Cisco display
- LAN communicates through MAC address AKA Layer 2 communication . MAC are for local communication
- Routers (Internet) requires IP address as means of globally locate the device and communicate

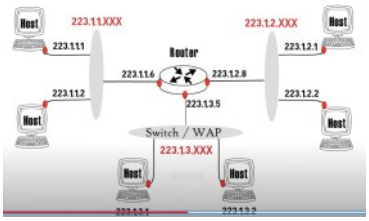
- Ipconfig /all - look for physical address
- ifConfig - look for ether address

Subnet

- The CIDR (classless Interdomain routing) has define the generic form of Subnet Address as a.b.c.d/x
- X represents how many bits will be command for given org. AKA network prefix

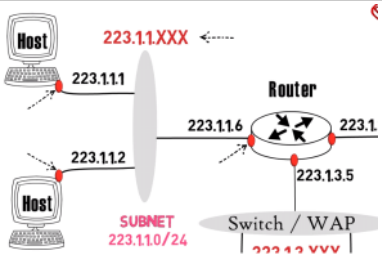
The RED Dot represents Interface
If multiple hosts are connected with a router then each interface will have separate IP Address
But the format of the IP address would remain the same

Subnet :
- The Host and the Router interfaces through which the hosts are connected follows the same IP address format (RED)
- This is known as Subnet



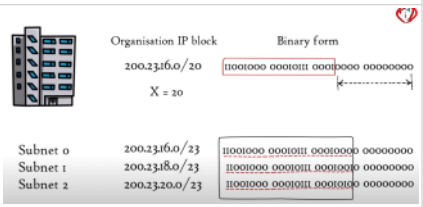
Subnet Mask :

223.1.1.0 / 24 - where 24 is the subnet mask,
meaning all the interfaces of this subnet (host and routers) have same initial 24 bits (223.1.1)



For example, if Org. has assigned subnet address as 200.23.16.0/20 means
- First 20 bits will represent the network prefix meaning all devices in the company will have same left most 20 bits
- So last 12 bits can be divided further into multiple subneting

So the org. can create multiple subnet within the itself



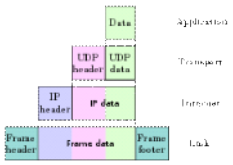
Firewall

- Firewall protects the bad traffic (hacker) coming into the network through routers
- Allows good traffic
- Network Firewalls
  - Traditional Firewalls (rule based)
    - By Default the firewall will simply block everything - No Incoming - No outgoing.
    - We have to configure Firewall rules - mostly for incoming traffic it should be always block
    - However, for application such as web server, SMTP server etc. we need to open incoming traffic
    - Stateful firewall - monitor the state of the active connection which means we don't have to create rules for incoming traffics
  - Next Gen Firewall
    - Application level Inspection
      - Identify and block risky application traffic
    - Intrusion prevention system (IPS)
      - Checks for the contents of the packet, signature etc.
      - Detect anomalies and unusual traffic
    - Threat Intelligence
      - External T.I so that it can update itself externally for brand new threat
    - Unified Threat Management includes features such as URL Filtering, Email scanning, Data Loss Prevention (DLP)
- Software Firewalls
  - AKA endpoint firewalls
  - Computer can have software firewalls
  - Windows Firewall uses same rule based methods
- For layer security posture, it is advisable to add both firewalls (network and software) so that we can have multiple check p oints of security

Hub - Switch - Router

- https://community.fs.com/blog/do-you-know-the-differences-between-hubs-switches-and-routers.html

template	Hub	Switch	Router
Layer	Physical layer	Data link layer	Network layer
Function	To connect a network of personal computers together, they can be joined through a central hub	Allow connections to multiple devices, manage ports, manage VLAN security settings	Direct data in a network
Data Transmission form	electrical signal or bits	frame & packet	packet
Port	4/12 ports	multi-port, usually between 4 and 48	2/4/5/8 ports
Transmission type	Frame flooding, unicast, multicast or broadcast	First broadcast, then unicast and/or multicast depends on the need	At Initial Level Broadcast then Uni-cast and multicast
Device type	Non-intelligent device	Intelligent device	Intelligent device
Used in(LAN, MAN, WAN)	LAN	LAN	LAN, MAN, WAN
Transmission mode	Half duplex	Half/Full duplex	Full duplex
Speed	10Mbps	10/100Mbps, 1Gbps	1-100Mbps(wireless); 100Mbps-1Gbps(wired)
Address used for data	MAC address	MAC address	IP address

	transmission
Ethernet	• IEEE 802.3 (Institute of Electrical and Electronics Engineers (IEEE)) • standards produced by the working group defining the physical layer and data link layer's media access control (MAC) of wired Ethernet. • family of wired computer networking technologies commonly used in local area networks (LAN), metropolitan area networks (MAN) and wide area networks (WAN). • The Internet Protocol is commonly carried over Ethernet and so it is considered one of the key technologies that make up the Internet. • It was commercially introduced in 1980 and first standardized in 1983 as IEEE 802.3. • Ethernet has since been refined to support higher bit rates, a greater number of nodes, and longer link distances, but retain s much backward compatibility. • Over time, Ethernet has largely replaced competing wired LAN technologies such as Token Ring, FDDI and ARCNET. • Systems communicating over Ethernet divide a stream of data into shorter pieces called frames. • Each frame contains source and destination addresses, and error-checking data so that damaged frames can be detected and discarded; most often, higher-layer protocols trigger retransmission of lost frames. • Ethernet provides services up to and including the data link layer
Internet Protocol	• The Internet Protocol (IP) is the principal communications protocol in the Internet protocol suite for relaying datagrams acr oss network boundaries. • Internet Protocol suite ○ is the conceptual model and set of communications protocols used in the Internet and similar computer networks. ○ It is commonly known as TCP/IP because the foundational protocols in the suite are the Transmission Control Protocol (TCP) and the Internet Protocol (IP). ○ end-to-end data communication specifying how data should be packetized, addressed, transmitted, routed, and received. ○ The technical standards underlying the Internet protocol suite and its constituent protocols are maintained by the Internet Engineering Task Force (IETF) • IP has the task of delivering packets from the source host to the destination host solely based on the IP addresses in the pa cket headers. • For this purpose, IP defines packet structures that encapsulate the data to be delivered. • It also defines addressing methods that are used to label the datagram with source and destination information • first major version of IP, Internet Protocol Version 4 (IPv4), is the dominant protocol of the Internet • successor is Internet Protocol Version 6 (IPv6), which has been in increasing deployment on the public Internet since c. 2006 • IP is responsible for • addressing host interfaces (connection point addressing via IP address) • encapsulating data into datagrams (including fragmentation and reassembly) • routing datagrams from a source host interface to a destination host interface across one or more IP networks. • For these purposes, the Internet Protocol defines the format of packets and provides an addressing system. • Datagram • It has two components ○ Header ▪ The IP header includes source IP address, destination IP address, and other metadata needed to route and deliver the datagram ○ Payload ▪ The payload is the data that is transported. • This method of nesting the data payload in a packet with a header is called encapsulation 
ICANN	• Core functions of the Internet are managed by a non-profit organization, the Internet Corporation for Assigned Names and Numbers (ICANN, icann.org) • It does assignment on – Internet domain names – IP address numbers – Protocol parameters and port numbers • Three subdivisions ○ Address Supporting Organization (ASO): aso.icann.org ○ Generic Names Supporting Organization (GNSO): gnso.icann.org • reviews and develops recommendations on domain-name policy for all generic top-level domains (gTLDs) • not responsible for domain name registration, but is responsible for the generic top-level domains (for example, .com, .net, .edu, .org, and .info) • iana.org/gtld/gtld.htm - list of top level domains ○ Country Code Domain Name Supporting Organization (CCNSO): ccnso.icann.org • reviews and develops recommendations on domain-name policy for all country-code top-level domains (ccTLDs): • does not handle domain name registrations • iana.org/cctld/cctldwhois.htm - list of country codes • Regional Internet Registries (RIRs) ○ manage, distribute, and register public Internet number resources within their respective regions ○ allocate IPs to organizations, Internet service providers (ISPs), or, in some cases, National Internet Registries (NIRs) or L ocal Internet Registries (LIRs) if particular governments require it (mostly in communist countries, dictatorships, etc.) ○ 5 RIR • APNIC (apnic.net): East Asia, Oceania, South Asia and South East Asia • ARIN (arin.net): USA, Canada, Parts of caribbean and Antarctica • LACNIC (lacnic.net): Latin America and most of Caribbean • RIPE (ripe.net): Europe, Central Asia, Russia and West Asia • AfriNIC (afrinic.net): Whole of Africa – iana.org/assignments/ipv4-address-space IPv4 allocation – iana.org/assignments/ipv6-address-space IPv6 allocation – iana.org/ipaddress/ip-addresses.htm IP address services – rfc-editor.org/rfc/rfc3330.txt Special-use IP addresses – iana.org/assignments/port-numbers Registered port numbers – iana.org/assignments/protocol-numbers Registered protocol numbers

Introduction

06 February 2021 21:26

Some key sites:

- https://www.broadcom.com/support/security-center/protection-bulletin
- https://thehackernews.com/
- https://cybermap.kaspersky.com/

- Spokeo – Social Data aggregator: www.spokeo.com
- Common Vulnerabilities and Exposures (CVE): http://cve.mitre.org
- National Vulnerability Database (NVD): http://nvd.nist.gov
- NVD Full Listing: https://nvd.nist.gov/vuln/full-listing

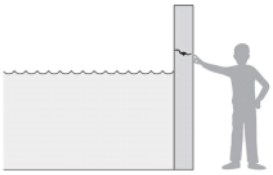
Computer Security

- Computer security is protection of items or ASSETS of a computer or computer system
- ASSETS are of following types:
  - **Hardware:** Computers, Devices (disk drives, memory cards, printers etc), Networks
  - **Software:** Operating system, utilities, commercial applications (MS-Office, Oracle apps, SAP etc), individual applications
  - **Data:** Documents, photos, emails, projects, corporate data etc
- ASSETS have a value to an individual
  - Has an owner or user perspective
  - May be monetary or non-monetary
  - Is personal, time dependent & often imprecise
- ASSETS are target for an attack and require security protection

Vulnerability – Threat - Control Paradigm

- '**Vulnerability**' is a weakness in the system that might be exploited to cause loss or harm
- '**Threat**' is a set of circumstances that has a potential to cause loss or harm to system
- A person who exploits the vulnerability perpetrates an '**Attack**'
- '**Control**' is an action, device, procedure of technique that removes or reduces the vulnerability

Example: Vulnerability - Threat - Control



- **Vulnerability:** Crack in the wall
- **Threat:** Rising water level
- **Attack:** Someone pumping more water
- **Control:** Fill the gap, strengthen the wall

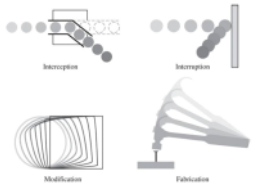
Security Triad - CIA

- **Confidentiality:** Ability of a system to ensure that an asset is viewed by only authorized parties
- **Integrity:** Ability of a system to ensure that an asset is modified by only authorized parties
- **Availability:** Ability of a system to ensure that an asset can be used by any authorized parties

Additional two properties:

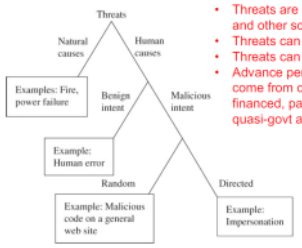
- **Authentication:** Ability of a system to validate the identity of a sender
- **Non-repudiation or Accountability:** Ability of a system to confirm that a sender can not convincingly deny having sent something

Acts of Harm



- **Interception:** Confidentiality lost
- **Interruption:** Availability lost
- **Modification:** Integrity lost
- **Fabrication:** Integrity lost

Security Threats



- Threats are caused both by human and other sources
- Threats can be malicious or not
- Threats can be random or targeted
- Advance persistent threat attacks come from organized, well financed, patient and often govt or quasi-govt affiliated groups

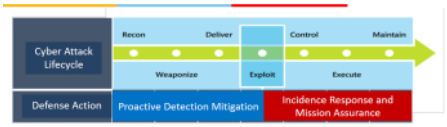
Who are the Attackers?

- Individual
- **Hackers**
- Terrorist
- Criminal for hire
- Loosely connected group
- Organized crime member
  - cyber crime is lucrative

Vulnerabilities Exploited by Hackers

- Systems with inadequate border protection
- Systems with weak authentication credentials
- Systems with out of date patching
- Remote Access Servers (RASs) with weak access controls.
- Applications with known vulnerabilities
- Open source applications with no protection
- Poorly protected data and websites
- Mis-configured or default configured systems

Cyber Attack Lifecycle (Kill Chain)



The cyber attack lifecycle, first articulated by Lockheed Martin as the "kill chain," depicts the phases of a cyber attack:

- **Recon**—the adversary develops a target;
- **Weaponize**—the attack is put in a form to be executed on the victim's computer/network;
- **Deliver**—the means by which the vulnerability is weaponized;
- **Exploit**—the initial attack on target is executed;
- **Control**—mechanisms are employed to manage the initial victims;
- **Execute**—leveraging numerous techniques, the adversary executes the plan;
- **Maintain**—long-term access is achieved.

Cyber Attack Lifecycle

Reconnaissance	Harvest email addresses, company information, etc.
Weaponization	Couple exploit with backdoor into deliverable payload
Delivery	Deliver weaponized bundle to the victim via email, web, usb, etc.
Exploitation	Exploit vulnerability to execute code on victim system
Installation	Install malware on the asset
Command & Control	Command channel for remote manipulation of victim
Actions on Objectives	With "Hands on Keyboard" access, intruders accomplish their original goal

Hacking

- Act committed toward breaking into a computer and/or network
- Hacking is any technical effort to manipulate the normal behavior of network connections and connected systems
- A hacker is any person engaged in hacking
- Purpose
  - Greed
  - Power
  - Publicity
  - Revenge
  - Adventure
  - Desire to access forbidden information
  - Destructive mindset

What is Ethical Hacking?

- Ethical hacking involves an authorized attempt to gain unauthorized access to a computer system, application, or data.
- Ethical hack involves duplicating strategies and actions of malicious attackers.
  - Helps to identify security vulnerabilities which can then be resolved before a malicious attacker has the opportunity to exploit them.
- Ethical hackers ("white hats") are security experts that perform these assessments.
  - The proactive work they do helps to improve an organization's security posture.
  - With prior approval from the organization or owner of the IT asset, the mission of ethical hacking is opposite from malicious hacking.

Hacker Types

White Hat	Black Hat	Gray Hat
• Ethical Hackers • They use their knowledge and skill to thwart the black hats and secure the integrity of computer systems or networks • They use hacking to identify vulnerabilities and inform the owners of systems so that the vulnerabilities can be	• Bad guys • Black hats may also share information about the "break in" with other black hat crackers so they can exploit the same vulnerabilities before the victim becomes aware and takes appropriate measures	• Bit of both White and Black hat • Their main objective is not to do damage to a system or network, but to expose flaws in system security • The black hat part of the mix is that they may very well use illegal means to gain access to the targeted system

plugged-in • If a black hat decides to target you, it's a great thing to have a white hat around	•	or network, but not for the purpose of damaging or destroying data • They want to expose the security weaknesses of a particular system and then notify the "victim" of their success • this is done with the intent of then selling their services to help correct the security failure so black hats can not gain entry and/or access for more devious and harmful purposes
Ethical Hackers • Use their knowledge to secure and improve the technology of organizations. • They provide an essential service to these organizations by looking for vulnerabilities that can lead to a security breach. • An ethical hacker reports the identified vulnerabilities to the organization. Additionally, they provide remediation advice. • With the organization's consent, the ethical hacker performs a re-test to ensure the vulnerabilities are fully resolved.	Malicious Hackers • Intend to gain unauthorized access to a resource (the more sensitive the better) for financial gain or personal recognition. • Deface websites or crash backend servers for fun, reputation damage, or to cause financial loss. • The methods used and vulnerabilities found remain unreported. • They aren't concerned with improving the organizations security posture.	

Key Concept of Ethical Hacking

- Stay Legal
  - Obtain proper approval before accessing and performing a security assessment
- Define the scope
  - Determine the scope of the assessment so that the ethical hacker's work remains legal and within the organization's approvedboundaries.
- Report Vulnerabilities
  - Notify the organization of all vulnerabilities discovered during the assessment.
  - Provide remediation advice for resolving these vulnerabilities
- Respect Data Sensitivity
  - Depending on the data sensitivity, ethical hackers may have to agree to a non-disclosure agreement, in addition to other terms and conditions required by the assessed organization

Key Limitations on Ethical Hacking

- Limited Scope
- Resource Constraints
  - Limited time
  - Limited Computer power and budget constraints
- Restricted Methods
  - Org. asks experts to avoid tests that may crash the system i.e. DDoS

Security Threats

06 February 2021 21:34

Malware	• Malicious Software • catch-all term for any type of malicious software designed to harm or exploit any programmable device, service or network • A wide variety of malware types exist, including computer viruses, worms, Trojan horses, ransomware, spyware, adware, rogue software, wiper and scareware.
Phishing	• fraudulent attempt to obtain sensitive information or data, such as usernames, passwords and credit card details or other sensitive details, by impersonating oneself as a trustworthy entity in a digital communication
Password Attacks	<See another page for the same>
DDoS	• Distributed Denial of Service • network attack wherein threat actors force numerous systems (usually infected with malware) to send requests to a specific web server to crash, distract, or disrupt it enough that users are unable to connect to it
MITM	• cyberattack where the attacker secretly relays and possibly alters the communications between two parties who believe that they are directly communicating with each other. • example of a MITM attack is active eavesdropping, in which the attacker makes independent connections with the victims and relays messages between them to make them believe they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker.
Drive-By Downloads	• unintentional download of a virus or malicious software (malware) onto your computer or mobile device. • A drive-by download will usually take advantage of (or “exploit”) a browser, app, or operating system that is out of date and has a security flaw
Maladvertising	• Malvertising (a portmanteau of "malicious advertising") is the use of online advertising to spread malware. • Typically involves injecting malicious or malware-laden advertisements into legitimate online advertising networks and webpages
Rouge Software	• internet fraud that misleads users into believing there is a virus on their computer and aims to convince them to pay for a fake malware removal tool that actually installs malware on their computer

OWASP Top 10 : https://owasp.org/www-project-top-ten/

1. Injection
2. Broken Authentication
3. Sensitive Data exposure
4. XML External Entities (XEE) : Older or poorly configured XML processors evaluate external entity references within XML documents
5. Broken Access Control :
6. Security Misconfiguration :
7. Cross-site scripting XSS : XSS flaws occur whenever an application includes untrusted data in a new web page without proper validation or escaping, or updates an existing web page with user supplied data using a browser API that can create HTML or JavaScript
8. Insecure Deserialization : Insecure deserialization often leads to remote code execution
9. Using Components with known vulnerabilities :
10. Insufficient Logging and Monitoring :

Malware

06 February 2021 21:45

- https://comtact.co.uk/blog/what-are-the-different-types-of-malware/

Computer Virus	• viruses need an already-infected active operating system or program to work • Viruses are typically attached to an executable file or a word document. • But there are hundreds of other file extensions that denote an executable file except .exe that causes virus • Usually spread via infected websites, file sharing, or email attachment downloads, a virus will lie dormant until the infected host file or program is activated • the virus is able to replicate itself and spread through your systems.	https://uk.norton.com/norton-blog/2016/02/the_8_most_famousco.html

Worms	• Worms are spread via software vulnerabilities or phishing attacks.
	• Worms doesn't need infected operating systems to work
	• Once a worm has installed itself into your computer's memory, it starts to infect the whole machine and in some cases… your whole network. They can
	  • Modify and delete files
	  • Inject malicious software onto computers
	  • Replicate themselves over and over to deplete system resources
	  • Steal your data
	  • Install a convenient backdoor for hackers
	  • They can infect large numbers of computers fast, consuming bandwidth and overloading your web server as they go.
		https://blog.eccouncil.org/9-of-the-biggest-botnet-attacks-of-the-21st-century/
		
		Stuxnet

Bots & Botnets	• A bot is a computer that's been infected with malware so it can be controlled remotely by a hacker
	• That bot (aka a **zombie** computer), can then be used to launch more attacks or to become part of a collection of bots (aka a botnet).
	• Botnets are popular with hacker show-offs (the more bots you collect, the mightier a hacker you are) and cyber criminals spreading ransomware.
	• Botnets can include millions of devices as they spread undetected.
	• It can cause
	  • DDoS attacks
	  • Keylogging, screenshots and webcam access
	  • Spreading other types of malware
	  • Sending spam and phishing messages	

Cutwail Botnets	Cutwail botnet, founded around 2007,[1] is a botnet mostly involved in sending spam e -mails. The bot is typically installed on infected machines by a Trojan component called Pushdo.[2] It affects computers running Microsoft Windows.[3]	
Zeus botnets	• Zeus, ZeuS, or Zbot is a Trojan horse malware package that runs on versions of Microsoft Windows. • While it can be used to carry out many malicious and criminal tasks, it is often used to steal banking information by man-in-the-browser keystroke logging and form grabbing.	

Trojan Horses	• Trojan Horse is a malicious program that disguises itself as a legitimate file
	• Trojans themselves are a doorway. Unlike a worm, they need a host to work.
	• Once you've got the Trojan on your device, hackers can use it to…
	  • Delete, modify and capture data
	  • Harvest your device as part of a botnet
	  • Spy on your device
	  • Gain access to your network	

Ransomware	• denies or restricts access to your own files. Then it demands payment (usually with crypto-currencies) in return for letting you back in • May 2017, a ransomware attack spread across 150 countries and compromised over 200k computers within just one day. • Aptly named WannaCry, the attack caused damage estimated in the hundreds of millions to billions of dollars	
Spyware	• Spyware secretly records your online activity, harvesting your data and collecting personal information such as usernames, passwords and surfing habits • Spyware is a common threat, usually distributed as freeware or shareware that has an appealing function on the front end with a covert mission running in the background that you might never notice. • It's often used to carry out identity theft and credit card fraud • spyware installs additional malware that make changes to your settings.	
Adware & Scams	• One of the better-known types of malware • It serves pop-ups and display ads that often have no relevance to you. • the ads link to sites where malicious downloads await unsuspecting users. • Adware can also deliver Spyware and is often easily hacked, making devices that have it installed a soft target for hackers, phishers and scammers	
Rouge Software	• internet fraud that misleads users into believing there is a virus on their computer and aims to convince them to pay for a fake malware removal tool that actually installs malware on their computer. • e.g. BraveSentry and SpySheriff •	
wiper	• whose intention is to wipe the hard drive of the computer it infects. • Originally designed by Jeffrey Allen as a way to infect locally stored computers in evidence lockup	
scareware	• uses social engineering to cause shock, anxiety, or the perception of a threat in order to manipulate users into buying unwanted software.	

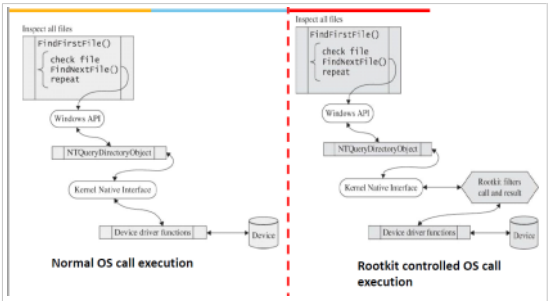
Tool and Techniques

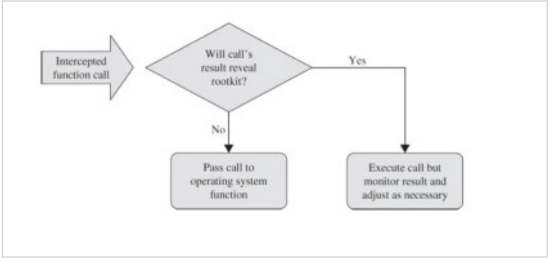
07 February 2021 05:34

Rootkit

- Malware - specially virus that has capabilities to modify OS code such that it can hide others Malwares from display (either as process or as application)
- RootKit does required installation - and it has command based utility
- Attacker usually finds a way to deliver the rootkit to the system under attack via either open port or social engineering and then first installs the root kit. Then he executes commands to hide other malware (worms, trojan, virus etc.) so that it doesn't get captured on process list
- Rootkit can hide files, registry, processes, bypass personal firewall, undetectable by anti-virus,
- It works at kernel level
- Root kit detection tools
  - ICE Swords, F-secure Blacklight, Rootkit Revealer, Dark Spy, system virginity verifier, RK Detector
- Sony Music story
- There are several rootkit classifications depending on whether the malware survives reboot and whether it executes in user mode or kernel mode.

Persistent Rootkits	• A persistent rootkit is one associated with malware that activates each time the system boots. • Because such malware contain code that must be executed automatically each system start or when a user logs in, they must store code in a persistent store, such as the Registry or file system, • configure a method by which the code executes without user intervention
Memory-Based Rootkits	Memory-based rootkits are malware that has no persistent code and therefore does not survive a reboot
User-mode Rootkits	• user-mode rootkit might intercept all calls to the Windows FindFirstFile/FindNextFile APIs
Kernel-mode Rootkits	• can be even more powerful since, not only can they intercept the native API in kernel-mode, but they can also directly manipulate kernel-mode data structures • A common technique for hiding the presence of a malware process is to remove the process from the kernel's list of active processes • Since process management APIs rely on the contents of the list, the malware process will not display in process management tools like Task Manager or Process Explorer



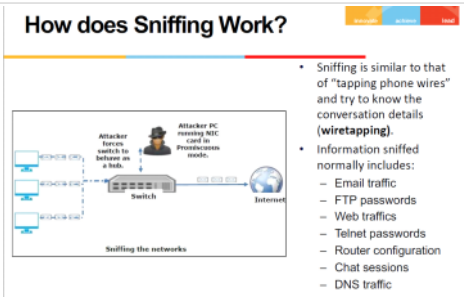


Covert Channel

- Any form of communication channel that can be exploited by the attacker e.g. Port 80 can be used to mount attack
- communication of information by transferring objects through existing information channels or networks using the structure of the existing medium to convey the data in small parts
- Tunneling :
  - Basically carried out one protocol over another
- ICMP (Internet Control Message Protocol) <TBD>
  - Echo request / reply message to deliver payload
- LOKI Tool <TBD>
- https://www.hackingarticles.in/covert-channel-the-hidden-network/
- https://www.spammimic.com/
- Steganography <TBD>

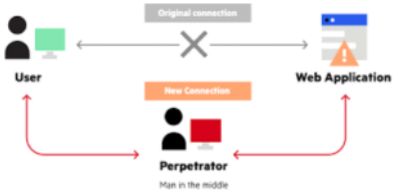
Sniffing

- Active Sniffing
  - By Injecting traffics to switches
  - What is Switch <TBD>
- Passive Sniffing
  - Hubs <TBD> instead of switches
  - Attackers simply needs to connect with LAN to observe the traffic
- What is MSN ? - Microsoft Network
- NIC , Switches, Hub
- Promiscuous mode
- Wire shark - <TBD> Home work
- BetterCAP <TBD>
- Ways to detect Sniffing : <Check the PDF Downloaded externally>
  - Ping method :
  - ARP (Address Resolution Protocol) <TBD> method
  - On Local host - using logs
  - Latency Method : Faster pings becomes slower by sniffer if the load is too high
  - ARP Watch: Duplicate caches of ARP
  - Using IDS (Intrusion detection system)



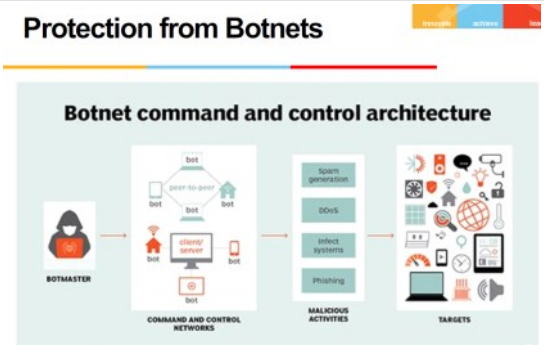
MITM

- Proxy <TBD>
- DNS <TBD>
- DNS poisoning <TBD>
- Attack tools
  - Pocket Creator
  - EtterCap
  - Dsniff <TBD>
  - Cain e Able
- Attack Types
  - IP Spoofing: target server IP spoofing to which the victim wants to connect
  - DNS spoofing: Forces users to a fake website instead of the real one
  - HTTPS Spoofing: Attacker fools browsers to believe that this is the correct website
  - SSL Hijacking: Attacker uses another computer and secure server and intercepts all the information passing between the server and the user's computer.
  - Email Hijacking: Hijacking bank's email server
  - WIFI Eavesdropping <TBD> Public WIFI
  - Stealing Browser's cookies <TBD>:



Botnets

- Collection of infected Internet-connected devices (systems, mobile, anything) - allows hackers to use them
- Botnets can be used to
  - Email spam - Cutwail botnet
  - DDoS attack
  - Financial Breach - Zeus botnet
  - Targeted Intrusion : Smaller botnets designed to compromise specific highvalue systems of organizations (R&D, Financials, IP etc) from which attackers can penetrate and intrude further into the network



Covering the tracks	• Hiding of digital footprints is the final stage of penetration testing.
	• Ethical hackers cover their tracks to maintain their connection in the system and to avoid detection by incident response teams or forensics teams
	• How
	  • Reverse HTTP Shells <TBD>
	  • Using ICMP (Internet control Message Protocol) Tunnels <TBD>
	  • Clearing the event logs : Metasploit's meterpreter <TBD>
	  • Erasing or Shredding command History : export HISTSIZE=0	

Camouflage	• the act, means, or result of obscuring things to deceive an enemy by painting or screening objects so that they are lost to view in the background, or by making up objects that from a distance have the appearance of fortifications
	• Deception: false appearance or statements
	• Defence Strategy :
	  • Predicting attacks
	  • Detecting activities
	  • Disrupting and Responding to TTPs (Tactics, techniques and procedures)
	• Server Decoys <TBD>	

Anti-Forensics	• criminal hacking with an objective – Make it hard for them to find you and even harder for them to prove they found you
	  • Data hiding : encryption, steganography, hardware/software based concealment
	  • Artifact hiding :
	  ○ Disk cleaning utilities (Cyber scrub, CyberCide, KillDisk)
	  ○ File wiping utilities (BC wipe, Eraser Cyber scrub)
	  • Trail obfuscation : log cleaners, timestamp modification, misinformation, spoofing, trojan command
	  • Attacks against computer forensics
	  • Attacks against computer forensics
	  • Counter forensic tools
	• Techniques for Anti-Forensic
	  • – Encryption
	  • – Steganography
	  • – Tunnelling
	  • – Onion routing <TBD> :
	  ○ Onion routing is a technique for anonymous communication over a computer network.
	  ○ The client has access to all the keys but the servers only have access to the keys specific for encryption/decryption to that server. Since this process wraps your message under layers of encryption which have to be peeled off at each different hop just like an onion that's why its called an onion router
	  • – Obfuscation
	  • – Spoofing: IP. & MAC spoofing	

Vulnerabilities

10 February 2021 10:19

- Vulnerability Assessment
  - process of identifying, quantifying, and prioritizing (ranking) the vulnerabilities in a system - RISK PROFILING
  - vulnerability assessment is a systematic review of security weaknesses in an information system
  - Evaluates if the system is susceptible to any known vulnerabilities, assigns severity levels to those vulnerabilities, and re commends remediation or mitigation, if and Whenever needed
  - process of identifying, quantifying, and prioritizing (ranking) the vulnerabilities in a system

- Threats can be prevented by Vulnerabilities assessments are :
  - SQL injection, XSS and other code injection attacks.
  - Escalation of privileges due to faulty authentication mechanisms.
  - Insecure defaults – software that ships with insecure settings, such as a guessable admin password
- Types of Vulnerability Assessment
  - Host Assessment : **The assessment of critical servers**, which may be vulnerable to attacks if not adequately tested or not generated from a tested machine image
  - Network and Wireless Assessment : **The assessment of policies and practices** to prevent unauthorized access to private or public networks and network-accessible resources
  - Database Assessment : The assessment of databases or big data systems for vulnerabilities and misconfigurations, identifying rogue databases or insecure dev/test environments, and classifying sensitive data across an organization's infrastructure
  - Application Scans : security vulnerabilities in web applications and their source code by automated scans on the front -end or static/dynamic analysis of source code

Vulnerability Assessment process

- Vulnerability assessment is an on-going activity - repeat it at regular intervals (recommended once in a year)
- **critical to foster cooperation between security, operation and development teams – a process known as DevOps**

Identification	Analysis	Risk assessment	Remediation

• How each of the threats that are possible or likely could be perpetrated, and list the organization's assets and their vulnerabilities
• draft a comprehensive list of an application's vulnerabilities
• Done by **Security Analyst** using automated tools or manually testing
  • Also rely on vulnerability database, vendor vulnerability announcements, asset management systems and threat intelligence feeds to identify security weaknesses
Methodology
• Start with commonly available vulnerability lists.
• Work with the system owners or other individuals with knowledge of the system or organization, start to identify the vulnerabilities that apply to the system.
• Specific vulnerabilities can be found by reviewing vendor web sites and public vulnerability archives
• Common Vulnerabilities and Exposures (CVE -http://cve.mitre.org)
• National Vulnerability Database (NVD - http://nvd.nist.gov)
	• identify the source and root cause of the vulnerabilities identified in step one
	• identification of system components responsible for each vulnerability, and the root cause of the vulnerability
	• RCA provides clear path of remediation
		• this step is the Prioritizing of vulnerabilities
		• Quantifying the risk
		• assign a rank or severity score based on
		– Which systems are affected.
		– What data is at risk.
		– Which business functions are at risk.
		– Ease of attack or compromise.
		– Severity of an attack.
		– Potential damage as a result of the vulnerability
			• this step is the closing of security gaps
			• joint effort by security staff, development and operations teams, who determine the most effective path for remediation or mitigation of each vulnerability
			• remediation steps include
			  • Introduction of new security procedures, measures or tools.
			  • Update of operational or configuration changes.
			  • Development and implementation of a vulnerability patch
			•

Vulnerability assessment tools

- Tools design to automatically scan
  - Web application scanners
  - Protocol scanners
  - Network scanners
- Popular open source tools are:
  - – OpenVAS - by Greenbone Networks
  - – Nexpose or InsightVM (cloud-based) – by Rapid7
  - – Retina CS Community – by BeyondTrust
  - – Burp Suite Community Edition - by PortSwigger

- – Nikto - by Netsparker
- – OWASP Zed Attack Proxy (ZAP)

- Popular Licensed tools are:
  - – Acunetix
  - – beSecure (AVDS)
  - – Comodo HackerProof
  - – Intruder
  - – Netsparker
  - – Tenable Nessus Professional
  - – Tripwire IP360

Advantage	Disadvantages
• Clearly defined scope • – Which systems are evaluated • – What potential problems are evaluated • Identifies most common technical issues • Cheapest of the assessment options • Repeatable and quantitative	Can identify a lot of issues Often lacks contextual risk information – Generic risk rankings – May not indicate the severity in your environment May not include expert advice/involvement

There are many online repositories with databases of vulnerabilities and exploits. The following are the most popular:

- Exploit Database – Exploits for Penetration Testers, Researchers, and Ethical Hackers
- Packet Storm Security
- SecurityFocus
- National Vulnerability Database
- CVE – Common Vulnerabilities and Exposures (CVE)
- Secunia Research Advisories
- Snyk Vulnerability Database

Password Cracking

10 February 2021 16:19

Brute Force	• One of the most common forms of password attack methods, and the easiest for hackers to perform. In fact, inexperienced hackers favor this method precisely because of this • a hacker uses a computer program to login to a user's account with all possible password combinations • Brute force accounts don't start at random; instead, they start with the easiest-to-guess passwords • Don't forget, if a hacker ever gains access to your employee list, guessing your usernames tends to present no challenge
Dictionary Attack	• Conversely, a dictionary attack allows hackers to employ a program which cycles through common words • A brute force attack goes letter by letter, whereas a dictionary attack only tries possibilities most likely to succeed • rely on a few key factors of users' psychology. • For example, users tend to pick short passwords and base their passwords off common words. So a dictionary attack starts with those words and variations (adding numbers at the end, replacing letters with numbers, etc.).
Phishing	As above
Rainbow Table Attack	• enterprises often hash their users' passwords; • hashing entails mathematically converting caches of passwords into cryptographic, random-looking strings of characters to prevent them from being misused. • If hackers can't read the passwords, they can't abuse them. • rainbow table compiles a list of pre-computed hashes. • It already has the mathematical answers for all possible password combinations for common hash algorithms. Like many identity management threats, this one uses time to its advantage
Credential Stuffing	• In a credential stuffing attack, hackers use lists of stolen usernames and passwords in combination on various accounts, automatically trying over and over until they hit a match. • Credential stuffing relies on users' tendency to reuse their passwords for multiple accounts, often to great success • hackers share stolen passwords on the Dark Web or sell them, so this information proliferates among threat actors • credential stuffing falls under the umbrella of brute force password attack methods. Yet it proves incredibly effective because it uses known passwords
Password Spraying	• member of the brute force password attack methods family • Password spraying tries thousands if not millions of accounts at once with a few commonly used passwords • If even one user has a weak password, your whole business may end up at risk • Most brute force methods focus on a singular account. By contrast, password spraying expands the potential targets exponentially. • Thus, it helps hackers avoid account lockout policies which would trigger on repeat login failures. At the very least, it mitigates their effectiveness • These password attack methods tend to move slowly. Hackers prefer to attack methodically from account to account, trying different passwords. • This allows the timers on account lockout detection tools to revert before moving back with a different password. • Password spraying can be particularly dangerous for single sign-on or cloud-based authentication portals.
Keylogger Attack	• keylogger attacks install a program on users' endpoints to track all of a users' keystrokes • user types in their usernames and passwords, the hackers record them for use later. • This technically falls under the category of malware or a digital virus, so it must first infect the users' endpoints (often through a phishing download).
Traffic interception	• In this attack, the cybercriminal uses software such as **packet sniffers** to monitor network traffic and capture passwords as they're passed. • Similar to eavesdropping or tapping a phone line, the software monitors and captures critical information, where the attack is made easier when passed on the network without any encryption • encrypted information may be decrypted, depending on the strength of the encryption method used.
Social Engineering	
Man-in-the-middle	• the hacker's program doesn't just monitor information being passed but actively inserts itself in the middle of the interaction, usually by impersonating a website or app • This allows the program to capture the Password attacks user's credentials and other sensitive information, such as account numbers, social security numbers, etc. • Man in the middle (MITM) attacks are often facilitated by social engineering attacks which lure the user to a fake site.
Malware	
Shoulder Surfing	• cybercriminals steal personal information or confidential information by peering over the target's shoulders

Kali : Crunch	• wordlist generator where you can specify a standard character set or a character set you specify
	• crunch can generate all possible combinations and permutations
	• Features:
	  • crunch generates wordlists in both combination and permutation ways
	  • it can breakup output by number of lines or file size
	  • resume support
	  • pattern now supports number and symbols
	  • pattern now supports upper and lower case characters separately
	  • adds a status report when generating multiple files
	  • new -l option for literal support of @,%^
	  • new -d option to limit duplicate characters see man file for details
	  • unicode support
	Generate a dictionary file containing words with a minimum and maximum length of 6 ***(6 6)*** using the given characters ***(0123456789abcdef)***, saving the output to a file ***(-0 6chars.txt)***:
	`root@kali:~# crunch 6 6 0123456789abcdef -o 6chars.txt`
	`Crunch will now generate the following amount of data: 117440512 bytes`
	`112 MB`
	`0 GB`
	`0 TB`
	`0 PB`
	`Crunch will now generate the following number of lines: 16777216`

Kali: Rainbow Crack	• general propose implementation of Philippe Oechslin's faster time-memory trade-off technique. • It crack hashes with rainbow table • RainbowCrack uses time-memory tradeoff algorithm to crack hashes • It differs from brute force hash crackers.

Memory Trapping

10 February 2021 17:33

https://googleprojectzero.blogspot.com/2021/01/windows-exploitation-tricks-trapping.html

https://media.ccc.de/v/36c3-10497-messenger_hacking_remotely_compromising_an_iphone_through_imessage#t=3645

Log Analysis

10 February 2021 20:11

https://en.wikipedia.org/wiki/Security_information_and_event_management

Privilege Escalation

10 February 2021 20:20

- https://www.cynet.com/network-attacks/privilege-escalation/
- act of exploiting a bug, design flaw or configuration oversight in an operating system or software application to gain elevated access to resources that are normally protected from an application or user
- In some cases, attackers attempting privilege escalation find the "doors are wide open" – inadequate security controls, or failure to follow the principle of least privilege, with users having more privileges than they actually need
- Privilege escalation is a technique of exploiting a vulnerability, or configuration on a web application or operating system to gain elevated access to permissions (normally root) that should not be available to that user.

Horizontal privilege escalation— **access rights of same privileged user**

- an attacker expands **their privileges by taking over another account** and **misusing the legitimate privileges granted to the other user**. To learn more about horizontal privilege escalation see our guide on lateral movement.

Vertical privilege escalation— **access rights to more privileged users**

- an attacker attempts to gain more permissions or access with an existing account they have compromised. For example, an attacker takes over a regular **user account on a network and attempts to gain administrative permissions.** This requires more sophistication and may take the shape of an Advanced Persistent Threat.

Reverse Engineering

11 February 2021 08:13

Reverse engineering is the process of **uncovering**

- principles behind a piece of hardware or software, such as its architecture and internal structure.
- program's components and functionalities in order to find vulnerabilities in the program
- original software design is recovered by analyzing the code or binary of the program, in order to hack it more effectively

Why ?

- Research network communication protocols
- Find algorithms used in malware such as computer viruses, trojans, ransomware, etc.
- Research the file format used to store any kind of information, for example emails databases and disk images
- Check the ability of your own software to resist reverse engineering
- Improve software compatibility with platforms and third-party software
- Find out undocumented platform features

Protection against Reverse Engineering :

- Proguard Assistance :
  - This is an open-source cross-platform tool written in Java
  - It is a command-line tool that shrinks, optimizes, obfuscates and even pre-verifies the code.
    - Shrink Method: identify the unused classes, fields, methods attributes of the mobile app and remove them.
    - Optimization: analyze and optimize the bytecode of various methods.
    - Obfuscation: short meaningless names are given to the rest of classes, fields, and methods
    - Pre verification: this process involves adding pre-verification information to the classes that are required by JME, Java 6 or higher
- Save important code chunks on the server:
  - remove the code from the application and move it to any web service that is encrypted server-side language
  - e.g. company is having a unique code or algorithm for their application, they would not allow their code to be stolen
- Use C/C++ to write important codes
  - A code written in Java is easy to decompile than the one written in C/C++
  - use NDK to write crucial parts of their code natively into the .so files and they add those files as a compiled library.
  - The code can be disassembled to assembly language code but the process of reverse engineering of a huge library can be cumbersome and time-consuming
- Be careful while applying SSL:
  - SSL based apps are candidate for MITM where attacker can easily breach the connection and get valuable data by simply providing a self-signed certificate
- Avoid storing values in raw format
  - values are to be saved in encoded form - e.g. store them in algorithm
- Securing User credentials:
  - The username and passwords should not be stored on the device
  - It is advisable to complete the initial authorization and use a short-lived authorization token
- Hide API Keys
  - Use either NDK or Private/public key exchange to protect the API key.
- Hashing Algorithm
  - Most of the hash functions MD2, MD5, SHA1 are vulnerable and prone to attacks
  - Instead, use secure functions such as SHA-2.
  - A typical hash function should be resistant to collisions and not too fast. If a hash function is too fast, it complicates the attack by exhaustive search. For this specific purpose, specialized hash functions are developed such as PBKDF2, bcrypt, scrypt
- Use of reflection in an insecure manner
- Try not to use External storage
- Use Database Encryption : SQLCipher

https://www.apriorit.com/dev-blog/366-software-reverse-engineering-tools

https://www.apriorit.com/dev-blog/364-how-to-reverse-engineer-software-windows-in-a-right-way

Binary Auditing	De-Compiler https://www.hex-rays.com/products/decompiler/compare/compare_vs_disassembly/	De-Assembler

Binary Auditing deals with the analysis of binary files
developing strategies to understand, analyze and interpret native code
	• Machine code to high-level language - mostly pseudo code or program language like Java
	
	PSEUDOCODE
	
	`__int64 __cdecl mod_ll(__int64 a1)`
	`{`
	`  return a1 % 2;`
	`}`
		• Machine code to human readable assembly language instructions
		
		ASSEMBLER CODE
		
		`; =============== S U B R O U T I N E =======================================`
		`; Attributes: bp-based frame`
		`; mod_ll(long long)`
		`public __Z6mod_llx`
		`__Z6mod_llx proc near`
		`var_10 = dword ptr -10h`
		`var_C = dword ptr -0Ch`
		`arg_0 = qword ptr 8`
		`push ebp`
		`mov ebp, esp`
		`push ebx`
		`sub esp, 0Ch`
		`mov ecx, dword ptr [ebp+arg_0]`
		`mov ebx, dword ptr [ebp+arg_0+4]`
		`mov eax, ecx`
		`mov edx, ebx`
		`mov eax, edx`
		`mov edx, eax`
		`sar edx, 1Fh`
		`sar eax, 1Fh`
		`mov eax, edx`
		`mov edx, 0`
		`shr eax, 1Fh`
		`add eax, ecx`
		`adc edx, ebx`
		`shrd eax, edx, 1`
		`sar edx, 1`
		`mov [ebp+var_10], eax`
		`mov [ebp+var_C], edx`
		`mov eax, [ebp+var_10]`
		`mov edx, [ebp+var_C]`
		`shld edx, eax, 1`

Android iOS Security

11 February 2021 09:16

Jailbreaking and Rooting

- Jailbreaking is the process of removing the limitations imposed by Apple on devices running the iOS operating system.
- Jailbreak allows the phone's owner to gain full access to the root of the operating system and access all the features.
- Rooting is the term for the process of removing the limitations on a mobile or tablet running the Android operating system.
- Jailbreaking and Rooting can potentially open security holes that may have not been readily apparent, or undermine the device's built-in security measures.
- Jailbroken and Rooted phones are much more susceptible to viruses and malware because users can avoid Apple and Google application vetting processes that help ensure users download virus-free apps.

Primary Google Security Services

- **Google play:** a collection of services that allow users to discover, install, and purchase apps from their Android device or the web
- **Android updates:** update service delivers new capabilities and security updates to selected Android devices,
- **App services:** Frameworks that allow Android apps to use cloud capabilities such as data backup
- **Verify apps:** Warn or automatically block the installation of harmful apps, and continually scan apps on the device, warning about or removing harmful apps
- **SafetyNet:** A privacy preserving intrusion detection system to assist Google tracking, mitigate known security threats, and identify new security threats
- **SafetyNet attestation:** Third-party API to determine whether the device is CTS compatible
- **Android device manager:** To locate a lost or stolen device

Android Kernel Security

• Linux kernel is the base for a Android computing environment. • Linux kernel provides Android with several key security features including: – A user-based permissions model – Process isolation – Extensible mechanism for secure IPC – Ability to remove unnecessary and potentially insecure parts of the kernel • **Application Sandbox** – Android's application security is enforced by the application sandbox, which isolates apps from each other and protects apps and the system from malicious apps.	• **System Partition and Safe Mode** – Contains Android's kernel and operating system libraries like application runtime, application framework, and applications. – This partition is set to read-only. – In Safe Mode booting of device third-party applications are not launched automatically however device owner can launch these manually. • **Filesystem Permissions** – Follows UNIX-style filesystem permissions to ensure that one user cannot alter or read another user's files. – Each application runs as its own user. – Unless the developer explicitly shares files with other applications, files of one application cannot be read or altered by another application. • **Security-Enhanced Linux** – Uses Security-Enhanced Linux (SELinux) to apply access control policies and establish mandatory access control (mac) on processes.	• **Verified boot** – Android 6.0 and later supports verified boot and device-mapper-verity. – Verified boot guarantees the integrity of the device software starting from a hardware root of trust up to the system partition. – During boot, each stage cryptographically verifies the integrity and authenticity of the next stage before executing it. – Android 7.0 and later supports strictly enforced verified boot, which means compromised devices cannot boot. • **Cryptography** – Android provides a set of cryptographic APIs for use by applications. – APIs include implementations of standard and commonly used cryptographic primitives such as AES, RSA, DSA, and SHA. – Specific APIs are provided for higher level protocols like SSL and HTTPS. – Android 4.0 provides the KeyChain class to allow applications to use the system credential storage for private keys and certificate chains.

Android User Security Features

File System Encryption	• Android 3.0 and later provides full filesystem encryption at kernel level. • Android 5.0 and later supports full-disk encryption. Full-disk encryption uses a single key—protected with the user's device password—to protect the whole of a device's user data partition. • Android 7.0 and later supports file-based encryption. File-based encryption allows different files to be encrypted with different keys.
Password Protection	Android can be configured to verify a user-supplied password prior to providing access to a device. – Use of a password and/or password complexity rules can be required by a device administrator.
Device Administration	Android 2.2 and later provide the Android Device Administration API – Administrators can also remotely wipe lost or stolen handsets. – APIs are available to third-party providers of Device Management solutions

- **Tools**
- APK Tool
- Drozer
- SSL Pinning
- Frida

Footprinting

11 February 2021 14:42

- Casing (Covering) the Establishment
  - Just like a bank robber will stake out a bank before making the big strike, your Internet adversaries will do the same
  - They will systematically poke and prod until they find the soft underbelly of your Internet presence
  - footprinting, scanning, and enumeration are vital concepts in casing the establishment

3 Pre-Attack phases

FootPrinting

• To know the landscape
• blue printing of the security profile of an organization undertaken in a structured manner
• It results in a unique organization profile with respect to networks (internet, Intranet, Extranet, Wireless) and systems involved
• attackers can take an unknown entity and reduce it to a specific range of domain names, networks, subnets, routers, IP addresses and other details about its security posture
• An attacker will spend **90% of his time in profiling** an organization and **10% in launching the attack**

• Determine the scope of activities
  • Are you going to footprint the entire organization, or limit your activities to certain subsidiaries or locations ?
  • What about business partner connections (extranets), or disaster recovery sites?
  • Are there other relationships or considerations ?
  • Are you going to exploit the weaknesses in whatever forms they manifest themselves ?
  • What are the potential crack in your system ?

• Information Gathering Methodology
  • Discover initial information
    • Domain name lookup
    • Locations
    • Contacts (telephone, mails etc)

  • Locate the network range
  • Ascertain active machine
  • Discover open ports / access points
  • Detect operating systems
  • Uncover services on ports
  • Map the network

• Main information sources are:
– Open source
– Whois
– Nslookup
• Hacking tools
– Sam spade

Good trusted website mirroring tools:
– Wget (gnu.org/software/wget/wget.html) for UNIX/Linux
– Teleport Pro (tenmax.com) for Windows

Use brute-force techniques to enumerate “hidden” files and
directories on a website:
– Use OWASP’s DirBuster to do this automatically

Paros: Tool to Analyze Website **http://www.parosproxy.org/'**

Dumpster diving : In the world of information technology, dumpster diving is a technique used to retrieve information that could be used to carry out an attack on a computer network. Dumpster diving isn't limited to searching through the trash for obvious treasures like access codes or passwords written down on sticky notes

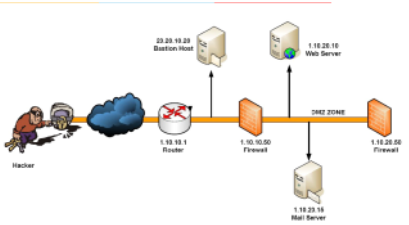
Tools
– Athena,
– SiteDigger
– Wikto
– FOCA analyses metadata associated with a document

Whois https://www.whois.com/whois/mit.edu	Host	NSLookup
• Gathers IP address and domain Information e.g. whois mit.edu **Commands on mac**	• Can look up one IP address, or the whole DNS Zone file (All the servers in the domain) e.g. host mit.edu	• Nslookup is a program to query Internet domain name servers • Displays information that can be used to diagnose Domain Name System (DNS) infrastructure • Helps find additional IP addresses if authoritative DNS is known from whois • MX record reveals the IP of the mail server • Both Unix and Windows come with a Nslookup client. Third party clients are also available e.g. Sam Spade

Traceroute : <see Additional PDF>>

- works by exploiting a feature of the Internet Protocol called TTL, or Time To Live
- reveals the path IP packets travel between two systems by sending out consecutive UDP packets with ever increasing TTLs
- As each router processes a IP packet, it decrements the TTL. When the TTL reaches zero, it sends back a "TTL exceeded" messag e (using ICMP) to the Originator
- Routers with DNS entries reveal the name of routers, network affiliation and geographic location
- can be used to determine the path from source to destination so that an attacker can determine the layout of a network and lo cation of devices

- traceroute 1.10.10.20, second to last hop is 1.10.10.1
- traceroute 1.10.20.10, third to last hop is 1.10.10.1
- traceroute 1.10.20.10, second to last hop is 1.10.10.50
- traceroute 1.10.20.15, third to last hop is 1.10.10.1
- traceroute 1.10.20.15, second to last hop is 1.10.10.50



Path Analyzer Pro

Tools

- Whois & SmartWhois
- Nslookup
- ARIN
- Neo Trace
- Visual Route Trace
- Path Analyzer Pro
- EmailTrackerPro
- Email Spider
- Geo Spider
- Website Watcher
- HTTrack Web Copier
- Google Earth

Cookies

11 February 2021 18:40

Cookie
– Text file generated by a Web server
– Stored on a user's browser
– Information sent back to Web server when user returns
– Used to customize Web pages
– Some cookies store personal information: Security issue

View cookies (Chrome): Website -> Inspect -> Application -> Cookies

What Is A Cookie?	• You can think of cookies as tiny bits of data. It stores information about your interaction with a website. For example, an e Commerce site would like to track a customer's journey – the products searched for, products purchased, items abandoned in the cart, or which pages they visit. • This gives the store analytical information on what customers prefer, which pages are being visited the most, how long users stay on a page, etc. They can then use this information to tailor what's displayed on the website according to the customer's preferences. • Cookies give website owners insight into what works and what doesn't. This helps them determine what they need to change or i mprove on their site. • Cookies are also used to display relevant ads to users. When you visit websites, you would notice advertisements being displa yed. • These ads usually reflect your recent search history. For example, if you searched for 'laptops' on Google, you'll notice that ads on all websites show you ads for dell. These ads are not a part of the website but are handled by services like Google Adsense. • Cookies make things convenient for both the website owner and the user. • It can boost engagement and lead to more sales which is great for website owners. As for the buyer, cookies help them get a more personalized experience on a website or see ads that are more relevant.
What Is A Browser Session and Session ID?	• When you log into a website, a session between your computer and this website is created • For example, when you log into Facebook, a session begins. This allows you to keep using Facebook (even if you close and reopen the web browser) until you click on 'log out' and end the session. • If the session wasn't created, you would need to keep logging in every time you wanted new data. For example, if you wanted to leave your Facebook news feed and view a friend's profile page, you will be logged out of Facebook and would need to enter your credentials again to log in and view the friend's profile. • This is why sessions are needed. It keeps you logged in so that you can continue to browse through different web pages and na vigate the website. • What's important to note here is that every session generates a set of cookies. • We can call these session cookies. • And each session cookie has a unique session ID. • A website uses this ID to authenticate the user and establish a trusted connection. • For example, to log in to Facebook, you need to enter your username and password. Next, a session is created with a unique ID. Any requests you make to the Facebook website will be authenticated with this ID. • So, when you want to view a different page, you would be sending a request to the Facebook server to display that page. Facebook verifies the ID and displays the content you wish to see. • Now, hackers can hijack your session and abuse this trusted connection. They can send malicious requests on your behalf. Let' s see how.
What Are The Security Concerns With Cookies?	• When cookies are generated, they can only be viewed by you – the site owner. • No other website can view your cookies. They belong solely to you • But these cookies travel across the internet. • They are used by ad services and analytics services. So these cookies bounce around from server to server all across the glob e. • If the connection is not secure, a hacker can easily intercept and steal these cookies. • The problem is cookies stored more than just information about your shopping preferences. It also stores bank details and per sonal information such as your shipping address and contact details. • If this kind of information falls into the wrong hands, it can be misused for fraudulent activities. • One of the most common ways hackers steal cookies is if they are using the same wifi as you. This kind of wifi hacking is cal led man-in-the-middle attacks and can take place only if both are connected to the same wireless network. • This is why it's advised to never use public wifi that is unsecured or used by many
How Hackers Use Cross-site Scripting (XSS) To Steal Cookies & Hijack Sessions?	Let's use example • Let's assume you visit a website that has a comments section on it. • Any comment you make will be sent to the website's database. Ideally, this comments section should be configured to accept only text in plain English. • But if it accepts special characters as well, this makes it vulnerable to XSS. • A hacker can enter their own malicious codes which will be sent to the database. • Once inside, the code will get executed. There are numerous codes hackers can insert into the website to run all sorts of malicious activities like creating a new website admin or stealing cookies.
How To Prevent Cookie Stealing And Session Hijacking?	1. Install an SSL Certificate • Data is transferred constantly between the user's browser and your web server. • Without SSL, this data (cookies) is sent in plain text. If a hacker intercepts this data, they can simply read it. So if it c ontains login credentials, it will be exposed. • SSL (Secure Sockets Layer) will encrypt the data before it's transferred. So even if a hacker manages to steal it, they can't read the data. 2. Install a Security Plugin • Keep a WordPress security plugin such as MalCare active on your website • The plugin's firewall will prevent hack attempts on your website and block malicious IP addresses. • it will scan your site regularly and alert you if any malicious code has been entered by a hacker. 3. Update Your Website • Always keep your website up to date - this includes the WordPress installation, themes, and plugins. • Running on outdated software opens many vulnerable spots on your website that hackers can exploit. 4. Harden Your Website • using strong and unique usernames and strong passwords, • blocking PHP execution in unknown folders, • disabling the file editor in themes and plugins and more.
For Visitors	• Install an Effective Anti-virus • Never Click on Suspicious Links • Avoid Storing Sensitive Data • Clear Cookies

Scanning

11 February 2021 16:05

- Scanning is a **set of procedures** for identifying **live hosts, ports, and services, discovering Operating system and architecture of target system, Identifying vulnerabilities and threats in the network**
- used to collect more information using complex and aggressive reconnaissance techniques
- hackers to identify vulnerabilities such as missing patches, unnecessary services, weak authentication, or weak encryption algorithms

Network Scanning	Port Scanning	Vulnerability Scanning
• used to create a profile of the target organization • To discover live hosts/computer, IP address, and open ports of the victim. • To discover services that are running on a host computer. • To discover the Operating System and system architecture of the target. • To discover and deal with vulnerabilities in Live hosts. **Methods** – Hackers and Pen-testers check for Live systems. – Check for open ports (also known as Port Scanning) – Scanning beyond IDS (Intrusion Detection System) **– Banner Grabbing:** method for obtaining information regarding the targeted system on a network and services running on its open ports. **Telnet and ID Serve** are the tools used mainly to perform a Banner-grabbing attack. • Scan for vulnerability • Prepare Proxies	• conventional technique used by penetration testers and hackers to search for open doors from which hackers can access any organization's system • hackers need to find out those live hosts, firewalls installed, operating systems used, different devices attached to the system, and the targeted organization's topology • Hacker fetches the victim organization's IP address by scanning TCP and UDP ports, the Hacker maps this organization's network under his/her grab • **NMAP** Techniques SYNScan: XMASScan: FINScan: IDLEScan: Inverse TCP Flag Scan: ACK Flag Probe Scan:	• performed by pen-testers to detect the possibility of network security attacks • Proactive identification of the system's vulnerabilities within a network in an automated manner to determine whether the system can be exploited Tools Nmap: Angry IP Scanner: Hping2/Hping3: Superscan: ZenMap: Net Scan Tool Suite Pack: Wireshark and Omnipeak

Enumeration

11 February 2021 19:36

- Probing the identified services for potential weakness - this process is known as Enumeration (ganatari)
- attack and obtains connectivity to hosts and segments he previously did not have access to, he will often return to this phas e to find ways to greatly expand his foothold and work toward specific targets
- key difference between the previously discussed information-gathering techniques and enumeration is in the **level of intrusiveness**
- Enumeration involves active connections to systems and directed queries
- information attackers seek via enumeration includes
  - user account names (to inform subsequent password-guessing attacks)
  - often misconfigured shared resources (for example,unsecured file shares)
  - older software versions with known security vulnerabilities (such as web servers with remote buffer overflows)
- Once a service is enumerated, it's usually only a matter of time before the intruder compromises the system in question to s ome degree, if not completely
- port scanning and enumeration functionality are often bundled into the same tool e.g. SuperScan
- Enumeration is the third step of information gathering about target
  i. Footprinting: act of gathering information about target systems (active & passive footprinting)
  ii. Scanning: using tools to find openings in target systems
  iii. Enumeration: gaining complete access to the system by compromising the vulnerabilities identified in the first two steps

1. https://www.youtube.com/c/Certbros/videos
2. https://resources.infosecinstitute.com/topic/what-is-enumeration/

<table>
<tr><td>Enumeration can give following details</td><td>Enumeration is used to gather the following:
– Usernames, group names
– Hostnames
– Network shares and services
– IP tables and routing tables
– Service settings and audit configurations
– Application and banners
– SNMP and DNS details</td></tr>
<tr><td>How to exploit</td><td>
<table>
<tr><th>Enumeration on (Types)</th><th>Enumeration using (Information Enumerated)</th></tr>
<tr><td>- NTP enumeration
– NetBIOS enumeration
– Windows enumeration
– LDAP enumeration
– Linux/Windows enumeration
– SMB enumeration
– RPC enumeration
– SNMP enumeration
– IPSec enumeration
– VOIP enumeration</td><td>– Network source
– Users and groups
– Routing tables
– Audit settings
– Service configuration settings
– The various machine names
– Applications
– Banners
– SNMP details
– DNS details</td></tr>
</table>
</td></tr>
<tr><td>NTP Enumeration</td><td>
<table>
<tr><td>What is NTP</td><td>• https://en.wikipedia.org/wiki/Network_Time_Protocol
• protocol for synchronizing time across your network, this is especially important when utilizing Directory Services
• There exists a number of time servers throughout the world that can be used to keep systems synced to each other
• NTP utilizes UDP port 123.</td></tr>
<tr><td>How to find NTP Server list</td><td>• https://helpdeskgeek.com/how-to/how-to-find-ntp-server-in-a-domain-to-sync-all-pcs/
• Command prompt
• w32tm /register - this is to register with window's time service
• sc start w32time - to start this service
• w32tm /query /status - to see the status of the service
• w32tm /query /status /verbose - verbose description
• w32tm /query /source - source of the time
• w32tm /query /configuration - runtime configuration and setting
• w32tm /query /peers - list of people using your system</td></tr>
<tr><td>Enumeration</td><td>• Through NTP enumeration you can gather information such as
• lists of hosts connected to NTP server
• IP addresses
• System names, and OSs running on the client system in a network
• All this information can be enumerated by querying NTP server as shown in above</td></tr>
<tr><td>Tools</td><td>• Ntptrace :Query to determine from where the NTP server updates its time and traces the chain of NTP servers from a source.
• Ntpdc : Query the NTP daemon about its current state and to request changes in the state.
• Ntpq : Monitors NTP daemon NTPD operations and determines performance.</td></tr>
</table>
</td></tr>
<tr><td>NetBios Enumeration</td><td>
<table>
<tr><td>What is NetBios</td><td>• NetBIOS stands for Network Basic Input Output System
• It Allows computer communication over a LAN and allows them to share files and printers
• NetBIOS names: - nbtstat -n
• used to identify network devices over TCP/IP (Windows)
• It must be unique on a network, limited to 16 characters where
○ 15 characters are used for the device name and the 16th character is reserved for identifying the type of service running orname record type.</td></tr>
<tr><td>Enumeration</td><td>Attackers use the NetBIOS enumeration to obtain:
• List of computers that belong to a domain
• List of shares on the individual hosts on the network
• Policies and passwords</td></tr>
<tr><td>Tools</td><td>Nbtstat : Windows default
Superscan: SuperScan is a connect-based TCP port scanner, pinger, and hostname resolver
Hyena :
• Hyena is a GUI product for managing and securing Microsoft operating systems. It shows shares and user logon names for Window s servers and domain controllers.
• It displays graphical representation of Microsoft Terminal Services, Microsoft Windows Network, Web Client Network, etc.
WinFingerPrint:
• Winfingerprint determines OS, enumerate users, groups, shares, SIDs, transports, sessions, services, service pack and hotfix level, date and time, disks, and open TCP and UDP ports.
Netview: command line tool to identify shared resources on a network</td></tr>
</table>
</td></tr>
<tr><td>Windows Enumeration</td><td>
<table>
<tr><td>What ?</td><td>• Used for Windows OS</td></tr>
<tr><td>Enumeration</td><td>• This is the most basic enumeration and the hackers attack desktop workstations
• confidentiality of the files is no longer maintained Any file can be accessed and altered.
• In some cases, hackers may also change the configuration of the desktop or operating system.
• It can be prevented by using Windows firewall, etc</td></tr>
<tr><td>Tool</td><td>• Sysinternals :
• The Sysinternals web site was created in 1996 by Mark Russinovich to host his advanced system utilities and technical information.
• Sysinternals Live is a service that enables you to execute Sysinternals tools directly from the Web without hunting for and manually downloading them.</td></tr>
</table>
</td></tr>
<tr><td>LDAP Enumeration</td><td>
<table>
<tr><td>What is LDAP ?</td><td>• Lightweight Directory Access Protocol
• LDAP is a protocol used to access directory listings within Active Directory or from other Directory Services
• directory is compiled in a hierarchical and logical format like the levels of management and employees in a company.</td></tr>
</table>
</td></tr>
</table>

		• LDAP tends to be tied into the Domain Name System to allow integrated quick lookups and fast resolution of queries. • Default port is 389 •

	Enumeration	• possible to query the LDAP service, sometimes anonymously to determine a great deal of information
		  • e.g. valid usernames, addresses, departmental details that could be utilized in a brute force or social engineering attack
		• Use NTLM or Basic authentication to limit access to known users only.
		  • Windows NT LAN Manager (NTLM) is a challenge-response authentication protocol used to authenticate a client to a resource on an Active Directory domain.
		  • When the client requests access to a service associated with the domain, the service sends a challenge to the client, requiring that the client to perform a mathematical operation using its authentication token, and then return the result of this operation to the service.
		  • The service may validate the result or send it to the Domain Controller (DC) for validation. If the service or DC confirm that the client's response is correct, the service allows access to the client
		• By default, LDAP traffic is transmitted unsecured; use SSL technology to encrypt the traffic.
		• Select a username different from your email address and enable account lockout.

	Tools	• Jxplorer - http://www.jxplorer.org/ • LDAP Admin Tool - http://www.ldapsoft.com

Linux / Unix Enumeration		
	What?	• Hackers who need to enumerate a target host whose operating system is Linux/UNIX use this type of enumeration. • It works in the same way as others and collects various sensitive data.

	Enumeration	• It is similar to Windows enumeration with just a change in operating systems
		• It can be prevented by configuring IPTables
		  • https://opensource.com/article/18/9/linux-iptables-firewalld
		  • iptables is a user-space utility program that allows a system administrator to configure the IP packet filter rules of the Linux kernel firewall, implemented as different Netfilter modules
		  • iptables is a tool for managing firewall rules on a Linux machine.
		  • The filters are organized in different tables, which contain chains of rules for how to treat network traffic packets. Different kernel modules and programs are currently used for different protocols; iptables applies to IPv4, ip6tables to IPv6, arptables to ARP, and ebtables to Ethernet frames

	Counter Measure	IP Tables
	Tools	<< See PDF >>
SMB Enumeration		

	What ?	• https://www.samba.org/cifs/docs/what-is-smb.html
		• SMB, which stands for Server Message Block, is a protocol for sharing files, printers, serial ports, and communications abstractions such as named pipes and mail slots between computers
		• Server Message Block (SMB), one version of which was also known as Common Internet File System (CIFS /sɪfs/),[1][2] is a communication protocol[3] for providing shared access to files, printers, and serial ports between nodes on a network.
		• It also provides an authenticated inter-process communication mechanism. Most usage of SMB involves computers running Microsoft Windows, where it was known as "Microsoft Windows Network" before the introduction of Active Directory
		• **convention** for sharing assets like records, printers, by and large, any asset which should be retrievable or made accessible by the server
		• It fundamentally runs on port **445** or port **139** relying upon the server
		• quite accessible in windows but for linux, you have to introduce a samba server since Linux locally doesn't utilize SMB convention
		• Some authentication like username and password will be there
		• Only certain resources made shareable
		• Some flaws
		  • default credentials or easily guessable and sometimes even no authentication for access of important resources of the server
		  • Samba servers are notorious for being tremendously insecure

	Enumeration	• use Nmap
		  • nmap -p445 — script smb-protocols <target ip>
		  • nmap -p139 — script smb-protocols <target ip>
		  • nmap -sC -p 139,445 -sV 10.0.2.30 (enumerate smb using default scripts of the NSE)
		• we found out the version of Samba running in the server. Now just go to google and search whether the given version is vulnerable or not.
		• but what if the samba server was patched, or didn't have a samba server to begin with.
		• Use Enum4linux Or smbclient and smbmap.

	Tools	• Nmblookup. • nbtscan. • SMBMap. • Smbclient. • Rpcclient. • Nmap. • Enum4linux
RPC Enumeration		

	What?	• Remote Procedure Call
		  • A procedure call is also sometimes known as a function call or a subroutine call.
		  • Most computer programs run procedures, or sets of instructions, using the computer's CPU. In other words, the instructions ar e processed locally on the same computer that the software is running from.
		  • Remote procedure calls, however, run procedures on other machines or devices connected to a network. Once the instructions ha ve been run, the results of the procedure are usually returned to the local computer
		  • e.g.
		  ○ computer without a hard drive may use an RPC to access data from a network file system (NFS)
		  ○ When printing to a network printer, a computer might use an RPC to tell the printer what documents to print.
		  ○ A client system connected to a database server may execute an RPC to process data on the server
		  • client-server model, where multiple client computers may connect to a server and retrieve data from it
		  • RPCs are typically written in a standard format, such as XML, so that the procedures can be understood by multiple computer p latforms
		  • e.g. XML-RPC sent by a Windows computer could be recognized by a Macintosh or Unix-based system.

	Enumeration	• Counting RPC endpoints empower aggressors to recognize any weak administrations on these administration ports • hackers filter high port reaches to recognize RPC administrations that are available to coordinate an assault

	Tools	• Nmap
		• Rpcbind
		  • utility is a server that converts RPC program numbers into universal addresses. It must be running on the host to be able to make RPC calls on a server on that machine
		• Rpcclient
		  • utility initially developed to test MS-RPC functionality in Samba itself.

SNMP Enumeration		

	What ?	• Simple Network Management Protocol
		  • Since 1988
		  • Developed for Adminstrators to remotely monitor networking equipments and change/modify the configuration and settings
		  • Initially developed for switches and routers - extended for Windows, Linux based pc, printers, power supplies etc.
		  • OID
		  ○ Object Identifier to all device - similar like ip address
		  ○ e.g. 1.3.6.1.2.1.2.2.1.8
		  • MIB
		  ○ Management Information Base
		  ○ Text file to translate OID to word based identifier
		  ○ e.g. 1.3.6.1.2.1.2.2.1.8 => SYNOLOGY-SYSTEM-MIB::temperature.0
		  • an application-layer protocol for managing TCP/IP based networks
		  • SNMP runs over UDP (which runs over IP)

	Enumeration	• used to enumerate user accounts, passwords, groups, system names, devices on a target system
		• Consist of three Major Components
		  1. Managed Device : device or a host (node) which has the SNMP service enabled. e.g. routers, switches, hubs, bridges, computer s etc.
		  2. Agent : piece of software that runs on a managed device. Its primary job is to convert the information into SNMP compatible format for the smooth management of the network using SNMP protocol

<table>
<tr><td></td><td></td><td>3. Network Management System (NMS) : These are the software systems that are used for monitoring of the network devices

• An agent running on every SNMP device will be providing access to a read and writable database.
• The database is referred to as the management information base (MIB) which is organized hierarchically and is a virtual database containing a formal description of all the network objects identified by a specific object identifier (OID) that can be managed using SNMP. It's a giant repository of values and settings. There is a manager involved in the process, and the manager will query the agent for various details.
• Community strings is a text string used to authenticate communications between the management stations and network devices on which SNMP agents are hosted.
• Community Strings travel in clear text over the network, hence are subject to network sniffing attacks. Community Strings are sent with every network packet exchanged between the node and management station. There are Two types of community strings:

1. Read only: This mode permits querying the device and reading the information, but does not permit any kind of changes to the configuration. The default community string for this mode is “public.”
2. Read Write: In this mode, changes to the device are permitted; hence if one connects with this community string, we can even modify the remote device ’s configurations. The default community string for this mode is “private.”

• when the community strings are left at the default settings, attackers take the opportunity and find the loopholes in it.</td></tr>
<tr><td></td><td>Counter Measure</td><td>• Remove or disable SNMP agents on hosts
• Block port 161 at all perimeter network access devices
• Restrict access to specific IP addresses
• Use SNMPv3 (more secure)
• Implement the Group Policy security option called "Additional restrictions for anonymous connections"
• Access to null session pipes, null session shares, and IPsec filtering should also be restricted</td></tr>
<tr><td></td><td>Tools</td><td>OpUtils Network Monitoring Toolset - http://www.manageengine.com
SolarWinds (best SNMP enumeration tool) - www.solarwinds.com
command line tools: SNMP-WALK, SNMP-CHECK</td></tr>
<tr><td>IPSec Enumeration</td><td>What ?</td><td>• Internet Protocol Security is a secure network protocol suite that authenticates and encrypts the packets of data to provide secure encrypted communication between two computers over an Internet Protocol network.
• It is used in virtual private networks.
• is a suite of protocols developed to ensure the integrity, confidentiality and authentication of data communications over an IP network
• IPsec utilizes following to make sure about the correspondence between virtual private organization (VPN).
• ESP (Encapsulation Security Payload)
• AH (Authentication Header)
• IKE (Internet Key Exchange)
• Most IPsec-based VPNs use the Internet Security Association and Key, Management Protocol, a piece of IKE, to establish, arrange, alter, and erase Security Associations and cryptographic keys in a VPN climate</td></tr>
<tr><td></td><td>Enumeration</td><td>• A straightforward checking for ISAKMP at the UDP port 500 can demonstrate the presence of a VPN passage
• Internet Security Association and Key Management Protocol (ISAKMP)
• protocol defined by RFC 2408 for establishing Security association (SA) and cryptographic keys in an Internet environment
• Hackers can research further utilizing an apparatus, for example, IKEoutput to identify the delicate information including encryption and hashing calculation, authentication type, key conveyance calculation, and so forth</td></tr>
<tr><td></td><td>Tool</td><td>IKEoutput</td></tr>
<tr><td>VoIP Enumeration</td><td>What ?</td><td>• Voice over Internet Protocol, also called IP telephony
• method and group of technologies for the delivery of voice communications and multimedia sessions over Internet Protocol networks, such as the Internet
• VoIP uses the SIP (Session Initiation Protocol) protocol to enable voice and video calls over an IP network
• UDP/TCP ports 2000, 2001, 5050, 5061</td></tr>
<tr><td></td><td>Enumeration</td><td>• VoIP enumeration provides sensitive information such as VoIP gateway/servers, IP-PBX systems, client software, and user extensions
• This information can be used to launch various VoIP attacks such as DoS, Session Hijacking, Caller ID spoofing, Eavesdropping, Spamming over Internet Telephony, VoIP phishing, etc.</td></tr>
<tr><td></td><td>Tools</td><td>• https://www.exploit-db.com/docs/english/18136-paper-enumerating-and-breaking-voip.pdf
• Smap
• scans a single IP or subnet of IP addresses for SIP enabled devices
• Svmap
• another powerful scanner from sipviciousv suite of tools. We can set the type of request being sent while enumerating SIP devices using this tool
• Swar
• identify the live SIP extensions</td></tr>
<tr><td>enum4linux</td><td colspan="2">• A Linux alternative to enum.exe for enumerating data from Windows and Samba hosts.
• Enum4linux is a tool for enumerating information from Windows and Samba systems. It attempts to offer similar functionality t o enum.exe formerly available from www.bindview.com.
• It is written in Perl and is basically a wrapper around the Samba tools smbclient, rpclient, net and nmblookup.
Key features:
• RID cycling (When RestrictAnonymous is set to 1 on Windows 2000)
• User listing (When RestrictAnonymous is set to 0 on Windows 2000)
• Listing of group membership information
• Share enumeration
• Detecting if host is in a workgroup or a domain
• Identifying the remote operating system
• Password policy retrieval (using polenum)</td></tr>
</table>

Sniffing

25 February 2021 08:20

Sniffing <Check Downloaded PDF>

What ?	• process of monitoring and capturing all data packets that are passing through a computer network using packet sniffers
Enumeration	• Tools were designed for Network administrators to keep track of data traffic passing through their network • However, Malicious attackers employ the use of these packet sniffing tools to capture data packets in a network. Which can be used to extract and steal sensitive information such as passwords, usernames, credit card information, etc. • Attackers sniff email traffic, FTP passwords, web traffics, telnet passwords, router configuration, chat sessions, DNS traffic etc. • Two types of Sniffing

Active Sniffing	Passive Sniffing
• Conducted on a switched network (switch connects two networks) • Switch has Content Addressable Memory (CAM) table containing MAC addresses of destinations to forward traffic to a right destination • Attacker sends huge fake traffic to a switch so that the CAM table gets full. • Once CAM table gets full, switch start sending traffic to all destinations • Attackers connects to one of the ports to carry out sniffing	• Passive sniffing uses hubs instead of switches (hubs redirects received traffic to all other ports) • All an attacker needs to do is to simply connect to LAN and they are able to sniff data traffic in that network

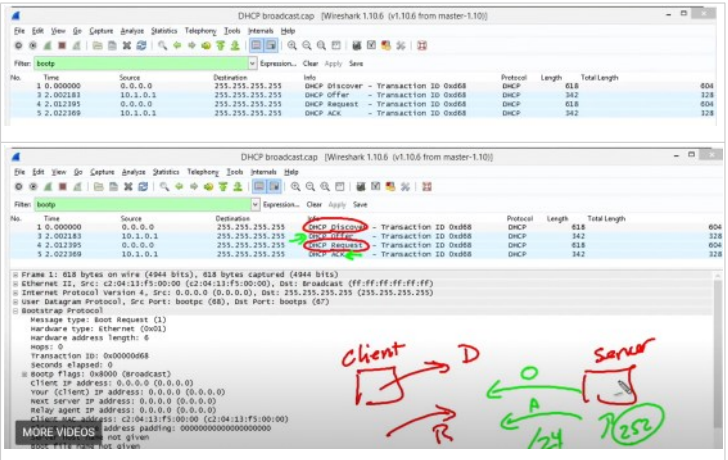
CAM Table	• Content Addressable Memory (CAM) table • system memory construct used by Ethernet switch logic which stores information such as • MAC addresses available on physical ports with their associated VLAN Parameters • present in all switches for layer 2 switching • This allows switches to facilitate communications between connected stations at high speed and in full-duplex regardless of how many devices are connected to the
Protocols Vulnerable	HTTP: Data sent in clear text. SMTP: Passwords and data sent in clear text. NNTP: Passwords and data sent in clear text. POP: Passwords and data sent in clear text. FTP: Passwords and data sent in clear text. IMAP: Passwords and data sent in clear text.
Tools	Wireshark, Ettercap, BetterCAP, Tcpdump, WinDump, dSniff, Debookee

How to Detect	• Ways to detect Sniffing : <Check the PDF Downloaded externally>
	  • Ping method :
	  • ARP (Address Resolution Protocol) <TBD> method
	  • On Local host - using logs
	  • Latency Method : Faster pings becomes slower by sniffer if the load is too high
	  • ARP Watch: Duplicate caches of ARP
	  • Using IDS (Intrusion detection system)

DHCP

25 February 2021 08:19

<table>
<tr><td>What ?</td><td>
• Dynamic Host Configuration Protocol
• It follows server - client architecture - works over UDP
• DHCP server
• Must be present in the network
• automatically assigns an IP address and other information to each host on the network so they can communicate efficiently wit h other endpoints
• the server assigns a unique address to the device, identifying it for TCP/IP communication, and supplies other network config uration parameters
• Keep records of assigned IP addresses and its lease time
<table>
<tr><td>Ip address</td><td>MAC address</td><td>Expiration Date (Least Time)</td></tr>
<tr><td>192.168.0.3</td><td>1111:2222:3333</td><td>1st Jan 12:00 AM</td></tr>
</table>
• Lease Time : Is the time by when the client needs to renew the IP address otherwise it would be discarded by the server and g iven to other client address
• Default UDP Port 67

• DHCP Client
• A device connected to the network requests an IP address from the DHCP server using the DHCP protocol;
• In the absence of a DHCP server, a device that needs an IP address must be manually assigned a static address by a network ad ministrator, or must assign itself an APIPA address (which will not enable it to communicate outside its local subnet).
• Default UDP Port 68
</td><td></td></tr>
<tr><td>Steps</td><td>
1. DHCP Discover
• Each client BRAODCAST a message saying I need DHCP server
• Other clients (apart from DHCP Server) will simply discard this broadcast message
• Default Broadcast destination is of 255.255.255.255 - meaning mostly the DHCP host will have this static IP
2. DHCP Offer
• When DHCP server receives a request - it sends one ip address as offer to the clients
• This one is also BROADCAST messages - other clients will simply discard it
• If more than one offer is given to the requested client, the client will choose the FIRST ONE
• DHCP server sends
○ proposed IP address for DHCP client
○ IP address of the server
○ MAC address of the client
○ subnet mask
○ default gateway
○ DNS address
○ lease information
3. DHCP Request
• Client will send lease request as BROADCAST to all for a offered IP
• DHCP server will receive it but other clients will simply discard it
4. DHCP Ack
• DHCP Sever will send the BROADCAST to all clients - the requesting client will accept it, others will simply discard it
• It has IP address (shared earlier), Subnet Mask and DNS server details
</td><td> 
</td></tr>
<tr><td>Some other terms</td><td>
• DHCP server: A networked device running the DCHP service that holds IP addresses and related configuration information.
• DHCP client: The endpoint that receives configuration information from a DHCP server.
• IP address pool: The range of addresses that are available to DHCP clients.
• Subnet: IP networks can be partitioned into segments known as subnets. Subnets help keep networks manageable.
• Lease Time: The length of time for which a DHCP client holds the IP address information.
• DHCP relay: A router or host that listens for client messages being broadcast on that network and then forwards them to a configured server.
</td><td></td></tr>
<tr><td>DHCP Starvation</td><td>
<table>
<tr><td>What ?</td><td>• Digital attack - targeting the DHCP server
• a hostile actor (Yersinia) floods a DHCP server with bogus DISCOVER packets until the DHCP server exhausts its supply of IP addresses.
• After this, an attacker can
• deny legitimate network users service - DoS
• even supply an alternate DHCP connection (Fake DHCP Server) that leads to a Man-in-the-Middle (MITM) attack
• It also sends malicious Gateway address which is usually attacker's machine
• Client will simply route all messages to the malicious gateway - causing MITM attack</td></tr>
<tr><td>Tools</td><td>Yersinia
• It can send tons of malicious DHCP Discover Packets using bogus mac addresses
• It can exhaust DHCP server IP address pool</td></tr>
<tr><td>Security Risk</td><td>• DHCP protocol requires no authentication so any client can join a network quickly - leads to malicious clients
• DHCP server has no way of authenticating a client, it will hand out IP address information to any device that makes a request
• Client has no way of validating the authenticity of a DHCP server meaning any rouge (Fake) DHCP servers can be used to provide incorrect network information.
•</td></tr>
<tr><td>Mitigation</td><td>• Port Security
•</td></tr>
</table>
</td><td></td></tr>
<tr><td></td><td>


</td><td></td></tr>
</table>

DNS

25 February 2021 08:41

What ?

- Domain Name System
- A system which resolves particular Domain name (Google.com) to the IP address of Web server where the website is hosted
- Packet sniffers can only see exchanges happening between client (pc) and the DNS Recursive Name Resolver.
- To check the local DNS
  - Ipconfig /displayDNS
- To flush the cache
  - of Browser = chrome://net-internals/#dns
  - Of local PC = ipConfig /flushdns - from cmd line
  - Of Local DNS server is hosted internally = Clear -DnsServerCache

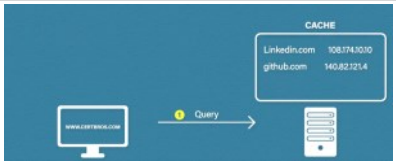
Steps

In local cache

- Both on the computer and browser
- There is also something called local configuration file that needs to be checked

To DNS Recursive Resolver

- Computer will connect to DNS recursive Resolver asking for ip address of given web server (certbors.com)
- Most of the cases, the DHCP will automatically configure our system to use the IP addresses of your ISP's domain name servers
- Most likely to be managed by ISP
- We can change it to Public DNS (e.g Google) or RUN our own DNS resolver
  - https://developers.google.com/speed/public-dns/docs/using
  - Google's Public DNS are IPV4 = 8.8.8.8 & 8.8.4.4 , IPV6 = 2001:4860:4860::8888 & 2001:4860:4860::8844
- Once it receives the request, it looks for an ip address into the local cache
- If it doesn't find entry then it sends it to the root server

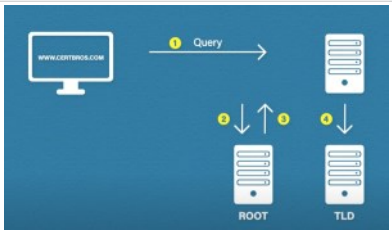


To Root Name Server

- Top of the DNS hierarchy
- Usually refers (diverts) the request to top level domain (TLD) servers e.g. .com, .org etc.
- In total, there are 13 main DNS root servers, each of which is named with the letters 'A' to 'M'.
- They all have a IPv4 address and most have an IPv6 address
- Managing the root server is ICANN's responsibility (Internet Corporation for Assigned Names and Numbers)
- operated by different institutions that ensure that data exchange in the root zone always remains correct, available, and secure
- https://www.ionos.com/digitalguide/server/know-how/what-is-a-root-server-definition-and-background/
- **Mostly the Root server is using UDP Port 53**

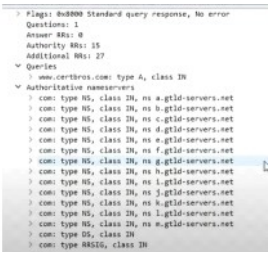
List of 13 Root servers

DNS-Root-Servers Letters	IPv4 address	IPv6 address	operator
A	198.41.0.4	2001:503:ba3e::2:30	VeriSign
B	192.228.79.201	2001:478:65::53	USC-ISI
C	192.33.4.12	2001:500:2::c	Cogent Communications
D	199.7.91.13	2001:500:2d::d	University of Maryland
E	192.203.230.10		NASA
F	192.5.5.241	2001:500:2f::f	ISC
G	192.112.36.4		U.S. DoD NIC
H	128.63.2.53	2001:500:1::803f:235	US Army Research Lab
I	192.36.148.17	2001:7FE::53	Autonomica
J	192.58.128.30	2001:503:c27::2:30	VeriSign
K	193.0.14.129	2001:7fd::1	RIPE NCC
L	199.7.83.42	2001:500:3::42	ICANN
M	202.12.27.33	2001:dc3::35	WIDE Project

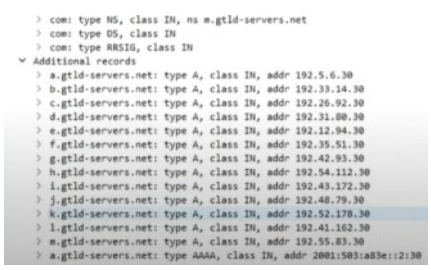


Querying the Root Server will show list of TLD with IP addresses in reply

See Query as CertBors.com and TLD as .Com

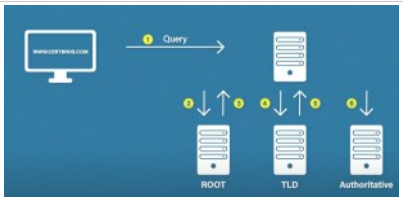


IP addresses - mostly first TLD server 192.5.6.30 will called later on

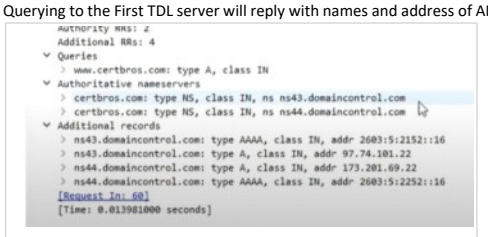


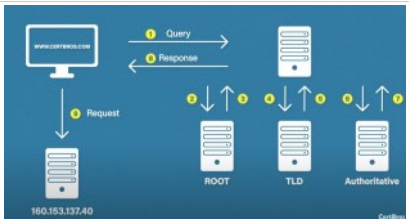
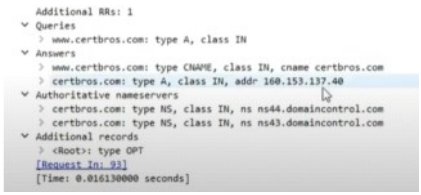
To TLD

- Top Level Domain Server
- Contains information about the domain e.g. .org, .com, .net etc.
- TLD holds the location of the **Authoritative Name server**
- As a result of request, TLD will refer it to the Authoritative Name Server



Querying to the First TDL server will reply with names and address of ANS



	To Authoritative Name Server	• Usually the Last step of the DNS lookup • Holds records of the DNS record information for the domain that they serve • If found, the ANS will send the IP address to the DNS recursive Resolver which in-tern send it back to the client • Using this IP address, the client can now connect with desired web server	 Query to the Authoritative Name server will reply back with IP address of the requested website It may not take the first ANS server record (e.g. 172.210.69.22 is picked) 

Attacks	Those who disable DNS mechanism	Those Who impacts the Data to be return

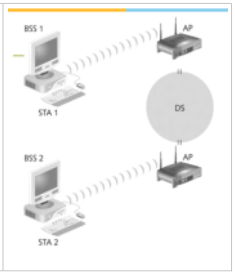
	• DOS (Amplification Attack - Resource Exhaustion of DNS servers)
	  • Overwhelmed the DNS server with large no. of queries
	  • Making DNS server to not to respond to legitimate queries
	  • Can be carried out by multiple malicious devices (BotNets)
	• DNS Reflection Attack (clogging Victim's machine)
	  • floods victims with high-volume messages from DNS resolver servers.
	  • Attackers request large DNS files from all the open DNS resolvers they can find and do so using the spoofed IP address of the victim
	  • When the resolvers respond, the victim receives a flood of unrequested DNS data that overwhelms their machines of the spoofed IP address (victim)
		• Change the DNS values such that it returns the malicious IP address of fake website
		• Cache Poisoning
		  • Intermediate DNS server connects with attacker instead of authentic DNS machine
		  • The attacker will supply wrong IP address
		  • Which gets cached within the intermediate DNS servers
		  • This cached response will spread across other DNS severs like a poison

Wireless Technology

25 February 2021 15:57

<table>
<tr><td>Wireless Technology</td><td></td></tr>
<tr><td>Components</td><td>
<table>
<tr><td>Access Points</td><td>• AP is transceiver
• combination transmitter/receiver in a single package
• Transmission is usually accomplished via radio waves, but communications satellites, wired connections, and optical fiber systems can also be used
• Connects the wireless network with the wired network But Not all wireless networks connect to a wired network
• Most companies have WLANs that connect to their wired network topology
• To configure AP
• Access the route admin console
• Provide username and password
• Change/update the default SSID name
• Provide WEP keys (password)</td></tr>
<tr><td>Wireless Network Interface Card (WNIC)</td><td>• Network Interface (connection) card
• each node or computer must have a wireless NIC
• NIC's main function is converting the radio waves it receives into digital signals the computer understands
• Two types
• Internal Network cards :
○ motherboard has a slot for the network card where it can be inserted
○ It requires network cables to provide network access.
○ Internal network cards are of two types.
▪ The first type uses Peripheral Component Interconnect (PCI) connection,
▪ second type uses Industry Standard Architecture (ISA)
• External Network cards :
○ desktops and laptops that do not have an internal NIC, external NICs are used.
○ External network cards are of two types:
▪ Wireless
□ Wireless network card needs to be inserted into the motherboard, however no network cable is required to connect to the network
□ They are useful while traveling or accessing a wireless signal.
▪ USB based</td></tr>
<tr><td>Ethernet Cable</td><td></td></tr>
</table>
</td></tr>
<tr><td>SSID</td><td>• SSID is the name to identify the wireless local area network (WLAN)
• Configured on the AP
• Unique 1- to 32-character case sensitive alphanumeric name
• Wireless computers must configure the SSID before connecting to a wireless network
• AP usually broadcasts the SSID
○ An AP can be configured to not broadcast its SSID until after authentication
• SSID is transmitted with each packet
○ Identifies which network the packet belongs
• Many Vendors have Default SSID values
• Usually the default SSID can be changed using admin console of the home router
• Most common is http://192.168.1.1.</td></tr>
<tr><td>Frequency Bands</td><td>
<table>
<tr><td>2.4 GHz</td><td>5 GHz</td></tr>
<tr><td>1 to 14 channels
Pros: Larger coverage area; better at penetrating solid objects
Cons: Lower data rate; more prone to interference; usually more devices using this frequency
Max connection speed: ~150 Mbps
Max signal range from router: ~410 ft
2.4 GHz band, this spectrum is the most widely used of the bands available for Wi-Fi.
Used by 802.11b, g, & n.
It can carry a maximum of three non-overlapping channels.
This band is widely used by many other non-licensed items including microwave ovens, Bluetooth, etc.

Lower Frequency : 2400
Higher Frequency : 2500</td><td>36 to 165 channels
Pros: Higher data rate; less prone to interference; usually fewer devices using this frequency
Cons: Smaller coverage area; worse at penetrating solid objects
Max connection speed: ~1 Gbps
Max signal range from router: ~410 ft amplified
5 GHz Wi-Fi band provides additional bandwidth, and being at a higher frequency, equipment costs are slightly higher, although usage, and hence interference is less.
It can be used by 802.11a & n.
It can carry up to 23 non-overlapping channels, but gives a shorter range than 2.4 GHz.
5GHz Wi-Fi is preferred because of the higher number of channels and available bandwidth.
There are also fewer other users of this band.

Lower Frequency : 5725
Higher Frequency : 5875</td></tr>
</table>
</td></tr>
<tr><td>IEEE 802.11</td><td>• First wireless technology standard defined by Institute of Electrical and Electronics Engineers (IEEE)
• Defined wireless connectivity at 1 Mbps and 2 Mbps within a LAN
• Applied to layers 1 and 2 of the OSI model
• Wireless networks cannot detect collisions
• Carrier sense multiple access/collision avoidance (CSMA/CA) is used instead of CSMA/CD
• 802.11 uses a Basic Service Set (BSS) as its building block
• Computers within a BSS can communicate with each others
• To connect two BSSs, 802.11 requires a distribution system (DS) as an intermediate layer
• An AP is a station that provides access to the DS
• Data moves between a BSS and the DS through the AP
 
</td></tr>
</table>

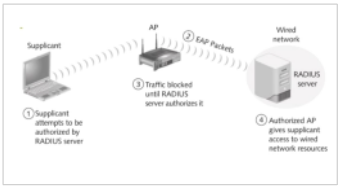
802.X Authentication Concepts

PPP Point to Point Protocol	EAP Extensible Authentication Protocol	WEP Wired Equivalent Protocol	WPA Wi-fi Protected Access
• Data link layer (layer 2) communication protocol between two routers directly without any host or any other networking in between • It can provide connection authentication, transmission encryption,[1] and data compression. • used over many types of physical networks,	• authentication framework frequently used in network and internet connections. • **EAP is not a wire protocol**; instead it only defines the information from the interface and the formats • **Enhancement of PPP** Allows a company to select its authentication method	• security standard for **wireless networks or WiFi**. • Intention was to provide data confidentiality comparable to that of a traditional wired network • It was implemented specifically to encrypt data that traversed a wireless network • Works well for home users or small businesses	• 802.11i standard • Replacement for WEP, developed by Wi-Fi Alliance • higher Initial Value of 48 bits (as against 24 bits of WEP) • improves encryption by using Temporal Key Integrity Protocol (TKIP) **Temporal Key Integrity Protocol (TKIP):**

including serial cable, phone line, trunk line, cellular telephone, specialized radio links, and fiber optic links, such as SONET
- (ISPs) have used PPP for customer **dial-up access to the Internet**, since IP packets cannot be transmitted over a modem line on their own without some data link protocol that can identify where the transmitted frame starts and where it ends
- Two derivatives of PPP, Point-to-Point Protocol over Ethernet (PPPoE) and Point-to-Point Protocol over ATM (PPPoA), are used most commonly by ISPs to establish a digital subscriber line (DSL) Internet service connection with customers.
  - DSL : family of technologies that are used to transmit digital data over telephone lines.
  - telecommunications marketing, the term DSL is widely understood to mean asymmetric digital subscriber line (ADSL)

– Certificates
– Kerberos : computer-network authentication protocol that works on the basis of tickets to allow nodes communicating over a non-secure network to prove their identity to one another in a secure manner

- EAP -Transport Layer Security (EAP-TLS)
- Protected EAP (PEAP)
- Microsoft PEAP
-



when combined with a Virtual Private Network (VPN)
- WEP has many vulnerabilities

Weakness

- **Weak Integrity Check**
- It uses CRC32 - which can be compromised by capturing at least two packets
- **Weak Encryption**
- RC4 is used with IV of 24 bits and secret key of 40 bits OR 104 bits
- The total length of both the initial value and secret can either be 64 bits or 128 bits long
- Easy to crack
- **Dictionary** attack is possible because it uses password
- **Poor key** management as it doesn't provide centralized KMS

- suite of algorithms that works as a "wrapper" to WEP
- TKIP uses the RC4 stream encryption algorithm as its basis. The new protocol, however, encrypts each data packet with a unique encryption key, and the keys are much stronger than those of its predecessor.
- To increase key strength, TKIP includes four additional algorithms:

1. A cryptographic **message integrity check** to protect packets
   - Cryptographic message integrity code
   - Main purpose is to prevent forgeries
2. An **initialization-vector sequencing** mechanism that includes hashing, as opposed to WEP's plain text transmission
   - Implemented to prevent replays
3. A **per-packet key-mixing** function to increase cryptographic strength
   - It helps defeat weak key attacks that occurred in WEP
   - MAC addresses are used in creating an intermediate key
4. A **re-keying mechanism** to provide key generation every 10,000 packets.
   - It provides fresh keys that help prevent attacks that relied on reusing old keys

How to secure Wireless Networks

- Use **Anti-warding** software e.g. Honeypots, Fake AP, Black Alchemy Fake AP
- Allow only **predetermined MAC** addresses and IP addresses
- **Limit the use** of wireless technology to people located in your facility
- Consider **using an authentication server** instead of relying on a wireless device to authenticate users
- Consider **using EAP**, which allows different protocols to be used that enhance security
- Consider placing the **AP in the demilitarized zone (DMZ)**
- If you use WEP, consider using **104-bit encryption** rather than 40-bit encryption
- Assign **static IP addresses to wireless clients** instead of using DHCP
- **Changing default passwords** that come with the hardware
- **Enabling the authentication** mechanism
- Access to the network can be restricted by allowing only **registered MAC addresses**.
- Use of **strong WEP and WPA-PSK keys**, a combination of symbols, number and characters reduce the chance of the keys been cracking using dictionary and brute force attacks.
- **Firewall Software** to help reduce unauthorized access

Wireless Hacking

27 February 2021 11:15

<table>
<tr><td>Warding</td><td>• Driving around with inexpensive hardware and software that enables them to detect access points that haven't been secured
•</td></tr>
<tr><td>Warflying</td><td>• Variant where an airplane is used instead of a car</td></tr>
<tr><td>How it works ?</td><td>• An attacker or security tester simply drives around with the following equipment
• Laptop computer
• Wireless NIC
○ Not all wireless NICs are compatible with scanning programs
• An antenna
• Antenna prices vary depending on the quality and the range they can cover
• Software that scans the area for SSIDs - that can identify
– Company's SSID
– Type of security enabled
– Signal strength indicates how close the AP is to the attacker

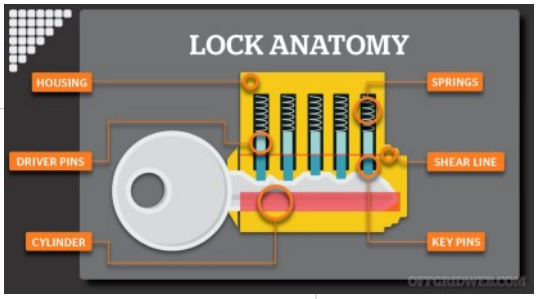
• It is similar to Wired network hacking
• Techniques for hacking wireless networks
• Port scanning
• Enumeration
• Two types of cracking:
• Passive cracking:
• this type of cracking has no effect on the network traffic until the WEP security has been cracked.
• It is difficult to detect.
• Active cracking:
• this type of attack has an increased load effect on the network traffic.
• It is easy to detect compared to passive cracking. It is more effective compared to passive cracking</td></tr>
<tr><td>Example</td><td>• wireless network adapter with the capability to inject/intercept packets
• Be within the target network's radius.
• users of the target network are actively using and connecting to it, then your chances of cracking it will be significantly improved.
• Capture packets specially users login steps – pcap files
• Pcap files
○ . pcap file extension is mainly associated with Wireshark;
○ They are data files created using the program and they contain the packet data of a network.
• captured packets (.pcap files) to find potential passwords using brute force technique
• Optionally you can use SaaS services like CloudCracker (seems It is out of service now. Alternate - https://www.onlinehashcrack.com/)</td></tr>
<tr><td>Cain & Able</td><td>• Password recovery tool for Microsoft Windows</td></tr>
<tr><td>Cracking tools</td><td>
<table>
<tr><td>NetStumbler</td><td>• NetStumbler logs the following information
– SSID
– MAC address of the AP
– Manufacturer of the AP
– Channel on which it was heard
– Strength of the signal
– Encryption
• Attackers can detect APs within a 350-foot radius
• with a good antenna, they can locate APs a couple of miles away</td></tr>
<tr><td>WEP Crack tools</td><td>• WEPCrack
• Open-source tool used to crack WEP encryption
• WEPCrack uses Perl scripts to carry out attacks on wireless systems
• Has features to conduct brute-force attack
• For details refer: http://wepcrack.sourceforge.net/
• Aircrack:
• network sniffer and WEP cracker.
• Can be downloaded from http://www.aircrack-ng.org/
• WebDecrypt:
• this tool uses active dictionary attacks to crack the WEP keys.
• It has its own key generator and implements packet filters.
• http://wepdecrypt.sourceforge.net/</td></tr>
<tr><td>WPA Cracking Tools</td><td>• WPA uses a 256 pre-shared key or passphrase for authentications.
• Short passphrases are vulnerable to dictionary attacks and other attacks that can be used to crack passwords.
• The following tools can be used to crack WPA keys.

• CowPatty:
• this tool is used to crack pre-shared keys (PSK) using brute force attack.
• http://wirelessdefence.org/Contents/coWPAttyMain.htm

• Cain & Abel:
• this tool can be used to decode capture files from other sniffing programs such as Wireshark.
• The capture files may contain WEP or WPA-PSK encoded frames. https://www.softpedia.com/get/Security/Decrypting-Decoding/Cain-and-Abel.shtml</td></tr>
</table>
</td></tr>
</table>

Hardware Hacking

19 March 2021 08:10



Lock Bumping

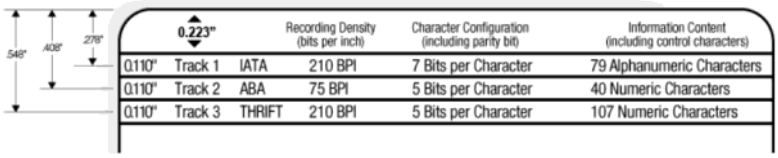
Driver Pins	• suspended by springs and push down on key pins •
Key Pins	• The key pushes the key pins against the driver pins to align a clear path for the mechanism • Once the pins have been aligned, the mechanism is clear and allows the lock to be turned
Bump Keys	• A specially constructed key (bump key) has teeth that sit below the key pins • When a bump key is inserted into any standard lock and then struck (“bumped”), each of the tips on the bump key transfers the force to the key pins causing them to “bump” into place temporarily for just a fraction of a second • Bumped locks leave no evidence of tampering

Magnetic Card Cloning

Cloning :

- Tool to clone the card : MSR605 (Magnetic Stripe Reader/Writer, Encoder for all 3 Tracks, ASI MSR 605)
- quick analysis of the data is enough to predict how to create a cloned card
- Analyze card data on three tracks is to read multiple cards of same type and then use "diff" tool to do a visual inspection on for contextual data verification
- Brute-forcing Card values can also help
- Writing data back on card
  - choose the track to write the data to
  - track may include checksum data to verify that the data on the card is valid or the card wasn’t damaged
  - Determine what checksum is being used and recalculate a new one before the card can be used.

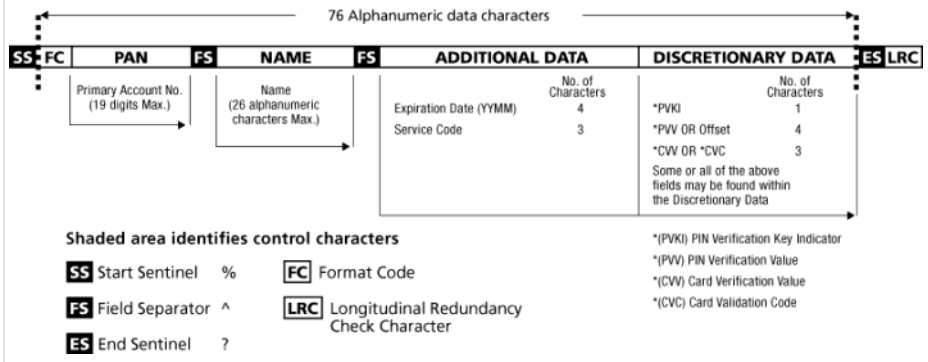
- magstripe cards use ISO standards 7810, 7811, and 7813
  - 7810: Physical characteristics
  - 7811-1 Embossing
  - 7811-2 Magnetic stripe - low coercivity
  - 7811-3 Location of embossed characters on ID-1 cards
  - 7811-6 Magnetic stripe - high coercivity
  - 7813: Financial transaction cards
- Most magstripe cards have no security measures to protect the data stored on the card and encode the data on the card in clear
- It has three tracks



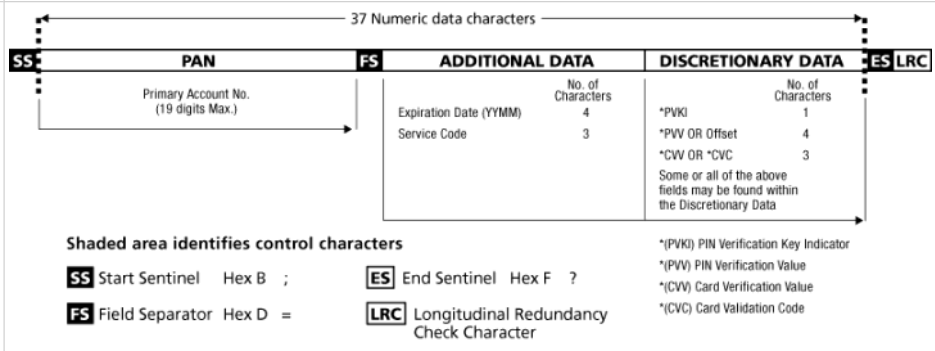
			Recording Density (bits per inch)	Character Configuration (including parity bit)	Information Content (including control characters)
0.110"	Track 1	IATA	210 BPI	7 Bits per Character	79 Alphanumeric Characters
0.110"	Track 2	ABA	75 BPI	5 Bits per Character	40 Numeric Characters
0.110"	Track 3	THRIFT	210 BPI	5 Bits per Character	107 Numeric Characters

- Track 1 : 76 + 3 = 79 **Alphanumeric** characters
  - IATA : Track 1 standards were created by the airlines industry - International Air transport Association
- Track 2 : 37 + 3 = 40 **Numeric** Characters
  - ABA : Track 2 standards were created by the banking industry (ABA) - American Bankers Association
- Track 3 : 104 + 3 = 107 **Numeric** Characters
  - THRIFT : Track 3 standards were created by the thrift-savings industry.

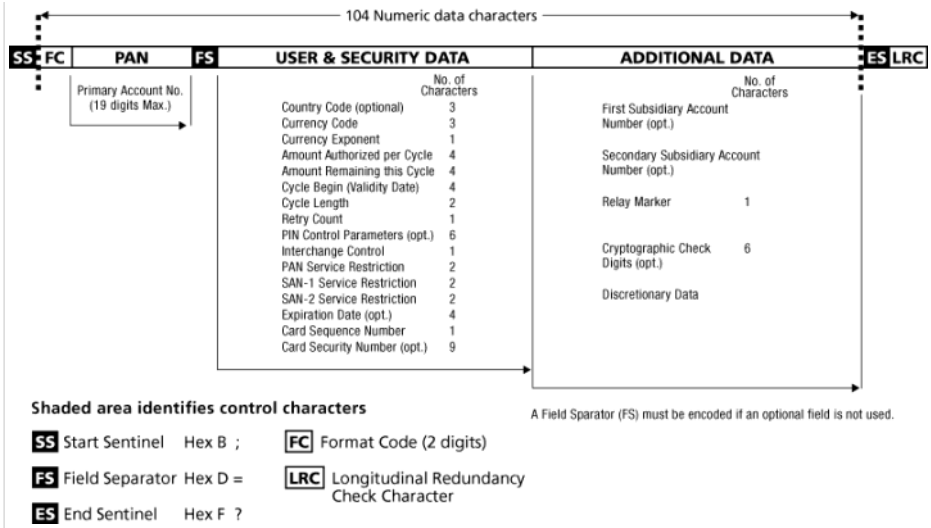
Track 1:



Track 2



Track 3



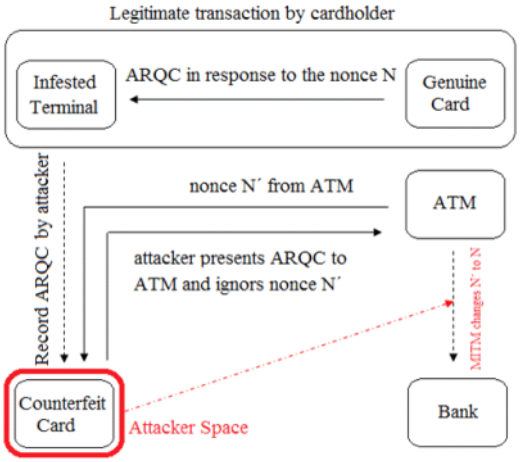
EMV Cards

- Europay, Mastercard and Visa
- Can be chip & signature (mainly US) or chip & PIN (most of the world)
- EMV cards are similar in data structures to Magstripe cards
- EMV cards track 1 and tarck2 data is almost same
- provision of PIN makes it much more secure

Pre-Play Attack

- pre-play attack is a cryptographic attack
- in which an attacker prepares for the attack in advance by carrying out a simulated transaction while pretending to be the device to be attacked,
- and then repeats the attack a second time with the real device at a time when it is likely to carry out the same series of operations as in the simulation
- The technique relies on being able to guess the content of the transaction in advance
- Something usually made possible by a poor choice of unpredictability within the system
- An EMV payment card authenticates itself with a MAC of transaction data, for which the freshly generated component is the unpredictable number (UN).
- If you can predict it, you can record everything you need from momentary access to a chip card to play it back and impersonate the card at a future date
- ATMs and POS have seriously defective random number generators (often simple counters)
- only four successive values of a terminal's "unpredictable number" have to be different for it to pass conformance testing.
- This enables a hacker with transient access to a payment card (a programmer of a terminal in a Mafia-owned shop) to harvest authentication codes which enable a "clone" of the card to be used later in ATMs and elsewhere.

- authorization request cryptogram (ARQC)
  - which is a cryptographic MAC calculated over the supplied data,
  - together with some card-provided data including the application transaction counter (ATC – a 16 bit number stored by the card and incremented on each transaction)
  - and the issuer application data (IAD – a proprietary data field to carry information from the card to its issuer)



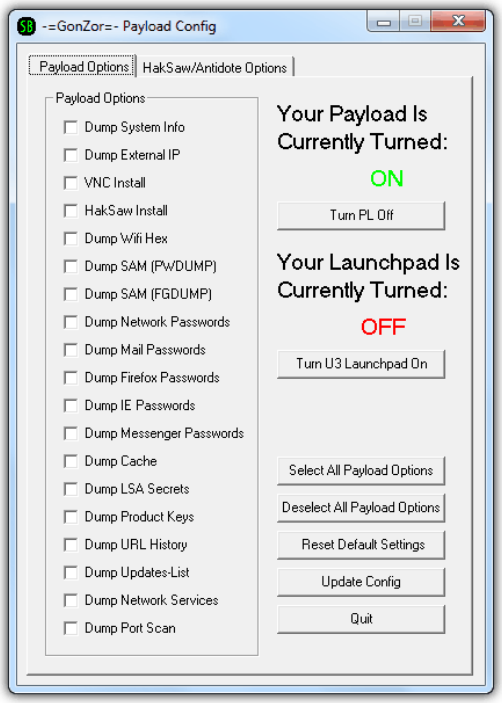
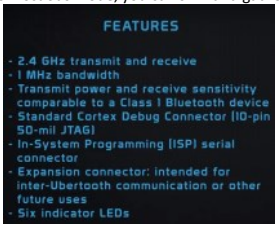
RFID Cards

- Radio-frequency identification (RFID) - uses electromagnetic fields to automatically identify and track tags attached to objects
- RFID Cards :
  - Badge cards, Smart cards used to get access of building,
  - tracking or identifying personnel is important or where access control is required
  - frequency bands :
    - 125 kHz low frequency proximity - Common proximity card format used for employee badges and door and gate access control
    - 13.56 MHz high frequency smart card - Higher security format used for credit cards and employee badges for physical and logical access control
    - 860-960 MHz ultra-high frequency (UHF) - UHF cards have a read range of up to 50 feet used for identification, access control and transaction processes
- RFID cards are normally unprotected and can be easily cloned for reuse
- Universal Software Radio Peripheral (USRP)

- Cloning using **proxmark3** - Cloning and Emulating RFID cards with Proxmark3
  - Read just about any RFID tag
  - Pretend to be a reader or a tag
  - Sniff communications between a reader and tag
  - Operate in standalone mode without a PC (USB battery required)

ATA Hard disk

- ATA security requires that the user type a password before a hard disk can be accessed by the BIOS
- Hot Swapping Drive

	• Boot the computer with unblocked hard drive and open BIOS menu that allows to reset ATA password • Carefully remove the unlocked drive from the computer and insert the locked drive • Set the hard-disk password using the BIOS interface • The drive will accept the new password
Hacking USB	• USB uses U3 standard • U3 was a joint venture between SanDisk and M-Systems,[1] producing a proprietary method of launching Windows software from special USB flash drives. • Flash drives adhering to the U3 specification are termed "U3 smart drives" • U3 partition is read only and partition menu is configured to auto execute when the USB stick is inserted into a computer • U3 hacking takes advantage of the autorun feature built into Windows • Hacking using Universal_Customizer - https://www.raymond.cc/blog/hack-u3-usb-smart-drive-to-become-ultimate-hack-tool/ • modify the content on the emulated CD-ROM such as the autorun.inf to instruct Windows to automatically run your payload instead of the U3 Launchpad when the drive is connected to a computer • One of the most popular and easy to use payload is called USB **SwitchBlade** • universal customizer tool that writes a custom ISO image file to the U3 partition and the payload that is copied to the stora ge drive can be configured by running the application and check the appropriate boxes 
Reverse Eng. H/W	<PDF>
Default Configuration	• how to communicate the initial default device password - Chicken & Egg problem • By default, devices are having standard passwords or insecure security settings • All default passwords - http://www.phenoelit.org/dpl/dpl.html • An attacker can log in to the router easily and change the settings to redirect the users to a malicious DNS and other services • Ubertooth • Ubertooth One is a cheap, open-source Bluetooth network sniffer by Michael Ossman • Ubertooth One is a USB plug with an antenna, and a ARM Cortex-M3 processor-based board in-between • Plug it into your computer and you can use it with various wireless monitoring tools like Kismet • This "promiscuous" mode makes the radio pass everything that it picks up onto the host computer • In promiscuous mode, you can sniff and gather data meant for other devices. ○ 
Router Compromise	• sophisticated form of data breach • Hackers conduct automated scans of routers to identify hardware that is vulnerable to an attack • extract configuration files enabling them to control or manipulate any devices that connect to your network, as well as the Internet connection. • Simple Network Management Protocol (SNMP) • default setting normally established during the setup of a network • Many organisations leave SNMP OPEN after the setup process • creating risk of compromise
Beacon Swarm (crowd, Group)	<step by step guide in PDF> • https://null-byte.wonderhowto.com/how-to/use-esp8266-beacon-spammer-track-smartphone-users-0187599/ • How to prevent ? ○
Evil Twin Attack	• Evil Twin attack takes advantage of the fact that most computers and phones will only 'see' the name of SSID of a wireless network as part of connection process. • hacker can take advantage of this vulnerability by setting up an Access Point with same name • This will trick a user into connecting if the network has the same name, same password, and same encryption • To get Password • Create a captive portal style phishing page similar to the login/password page of the network • Screen is similar to original one with T&C, other data and password entry fields • Can use **Airgeddon** or **Aircrack**-ng tools ○ Flood the actual trusted network with de-authentication requests so that the user is not able to connect and comes to join via the twin (but fake) name

	network ○ Upon connecting to phishing page, user will be asked for password with an plausible explanation (router has updated and requires password etc) • Advanced Social Engineering • previously captured password handshake from the actual network to validate the password entered by the user • If users enters wrong password, display appropriate message • Once user enters correct password, the network is hacked • technology assisted Social Engineering
MITM	• Attacker secretly captures and relays communication between two parties who believe they are directly communicating with each other • ARP spoofing or ARP poisoning • Alice and Bob are connected to a WiFi hotspot • They will use ARP requests and replies to find out the physical address (MAC address) to which to direct their traffic • Attacker (Mallory) will send a false ARP messages to Alice • giving its own MAC address as the physical address for Bob; • similar ARP messages to Bob, giving its own MAC address as the physical address for Alice;
Prevent WIFI hacking ?	• Purge networks not required in the preferred network list • Use VPN to keep local traffic encrypted • Disable auto-connect when joining networks • Never use hidden network • Disable WPS functionality on router • Never re-use password for Wi-Fi • Isolate clients to their own sub-net

VoIP

25 April 2021 11:18

What ?	• Voice Over IP
	• transport of voice on top of an IP network
	• basic setup for point-to-point communication between two users or can provide full carrier grade communication services.
	• Two common open signalling protocols
	  • **H.323 :**
	  • **Session Initiation Protocol (SIP)**
	• Propriety signalling protocols like Cisco SKINNY
	  • Skinny Client Control Protocol (SCCP)
	  • Proprietary network terminal control protocol originally developed by Selsius Systems, which was acquired by Cisco Systems
	  • lightweight IP-based protocol for session signaling with Cisco Unified Communications Manager, formerly named CallManager
	• Propriety Avaya Unified Networks IP Stimulus (UNIStim)
	  • deprecated Telecommunications protocol developed by Nortel (now acquired by Avaya) for IP Phone (terminals and soft phones) and IP PBX communications
	  • These protocols are being gradually replaced or complemented by standardized protocols, including H.323, especially SIP
	• Other protocols
	  • Real-Time Transport Protocol (RTP) transports encoded voice traffic
	  • Real-Time Control Protocol (RTCP)
	  ○ Provides call statistics like delay, packet loss, jitter etc
	  ○ Controls information for the RTP flow
	  ○ Used to monitor data distribution and adjust quality of service (QoS)parameters
	• VoIP setups are prone to a wide number of attacks, mainly due to the fact that they expose a large number of interfaces and protocols to the end user

H.323	• suite of protocols defined by the International Telecommunication Union (ITU) with ASN.1 encoding • Makes integration with the public switched telephone network (PSTN) easier • provides standards for equipment, computers and services for multimedia communication across packet based networks and specifies transmission protocols for real-time video, audio and data details

SIP	○ Signalling protocol is a type of communications protocol for encapsulating the signalling between communication endpoints and switching systems to establish or tear down a connection, and to identify the state of connection.
	○ Session Initiation Protocol (SIP) is a signalling protocol used for initiating, maintaining, and terminating real-time sessions that include voice, video and messaging applications
	○ SIP is a Internet Engineering Task Force (IETF) protocol and is becoming more popular
	○ protocol defines the specific format of messages exchanged and the sequence of communications for cooperation of the participants.
	○ SIP is a text-based protocol, incorporating many elements of the Hypertext Transfer Protocol (HTTP) and the Simple Mail Transfer Protocol (SMTP)
	  • Operates on TCP/UDP 5060 (similar to the HTTP protocol)
	  • implements different methods and response codes for session establishment and teardown
	○ Used by Enterprise voice products from Cisco, Avaya, and Microsoft
	• Handles voice/video traffic, instant messages, user location, user availability, user capability, session management etc

SIP Scanning	• discovery process of SIP proxies and other SIP devices
	• SiVus :
	  • general purpose SIP hacking tool for Windows and Linux
	  • perform SIP scanning via its point-and-click GUI
	• SIPVicious:
	  • Python based command-line SIP tool suite
	  • svmap.py tool within the SIPVicious suite is a SIP scanner
	  • identifying SIP systems within a provided network range
	https://www.rtcsec.com or sipvicious.org/

Hacking TFTP	• TFTP
	  • Trivial File Transfer Protocol (TFTP) is a protocol layered on the User Datagram transport Protocol (UDP) used over the Internet Protocol (IPv4 or IPv6).
	  • very simple file transfer protocol
	  • It was first specified in 1980 and provides functions to copy files across a network (a very basic form of FTP).
	• SIP phones use a TFTP server to retrieve their configuration settings during boot up process
	• TFTP server can be located on network (nmap –sU –p <IP Range>) and then attempt to guess the configuration file's name
	  • A list of common filenames is available on internet
	• Configuration files contain information such as usernames and passwords for administrative functions
	• To get the TFTP Server address, MAC address, Network settings
	  • Sniffing/Scanning the network and reviewing the web server on an IP phone
	  • Walking up to the phone and viewing the network settings under the menu

Enumeration on VoIP users	• Enumeration is the key to every successful attack/penetration test as it provides the much needed details and overview of the setup, VoIP is not different
	• In VoIP network, information useful to us as an attacker is VoIP gateway/servers, IP-PBX systems, client software (softphones)/VoIP phones and user extensions
	• For the sake of demonstration, let's assume that we know the IP addresses of devices already (i.e. 192.168.1.6)
	
	• Using smap
	  • Command : ./ smap -O 192.168.1.6
	 
	• Using Svmap
	  • powerful scanner from sipvicious suite of tools
	  • We can set the type of request being sent while enumerating SIP devices using this tool.
	  • The default request type is OPTIONS
	  • Let's run the tool on a pool of 20 devices (Figure 3). As we can see, svmap is able to detect IP addresses and their User-Agent details.
	  • Command : ./svmap.py 192.16.1.1 -20

```
root@bt:/pentest/voip/sipvicious# ./svmap.py 192.168.1.1-20
WARNING:DrinkOrSip:could not bind to 0.0.0.0:5060 - some process might already b
e listening on this port. Listening on port 5061 instead
| SIP Device       | User Agent                          | Fingerprint |
-------------------------------------------------------------------------
| 192.168.1.6:5060 | Asterisk PBX 1.6.0.26-FONCORE-r78 | disabled    |
| 192.168.1.4:5060 | Zoiper rev.11619                  | disabled    |
```

- Swar
  - During VoIP enumeration, extension enumeration is important to identify the live SIP extensions
  - Swar aides in scanning complete range of IP addresses
  - scan for user extensions from 200 to 300. The result is user extensions which were registered with IP-PBX server

```
root@bt:/pentest/voip/sipvicious# ./svwar.py -e200-300 192.168.1.6 -m INVITE
| Extension | Authentication |
-------------------------------
| 200       | reqauth        |
| 202       | reqauth        |
| 204       | reqauth        |
| 206       | reqauth        |
```

VoIP Attacks	• Denial of Service (DoS) attacks • Registration Manipulation and Hijacking • Authentication attacks • Caller ID spoofing • Man-in-the-middle attacks • VLAN Hopping • Passive and Active Eavesdropping • Spamming over Internet Telephony (SPIT) • VoIP phishing (Vishing)

VoIP attack types	• Unauthorised use:
	  • Hackers can use hacked phone system to use robocalling and auto-dialling software.
	  • People who answer the phone will hear a pre-recorded message asking them to do something— such as enter their credit card number to “confirm their account.”
	• Toll fraud:
	  • Hackers can make international calls from hacked phone.
	  • Toll charges for these long-distance calls can be expensive.
	• Caller Id spoofing:
	  • Caller ID isn’t always a reliable way to verify the person calling.
	  • Hackers can use fake caller IDs in coordination with another attack, like social engineering.
	• Eavesdropping:
	  • Eavesdropping allows hackers to collect information about a business and its customers.
	  • They can access every interaction the business has had including employee voice mails.
	• Social engineering:
	  • Hackers try to build relationships with their victims so they think it’s a genuine call, but it’s not.
	  • Caller is a hacker impersonating someone else to trick the called party into handing over sensitive information.

Defence	• Choose right VoIP provider • Control administrator access • Enable Network Address Translation (NAT) • Use VPN and enable end point filtering • Disable VoIP web interface • Monitor your call and access logs • Keep strong passwords • Use two factor authentication • Create cyber security awareness in your team • Have a mobile device policy • Create an incident response plan to handle VoIP hacking incidents

VPN

25 April 2021 12:23

<table>
<tr><td>What ?</td><td>• VPN gives online privacy and anonymity by creating a private network from a public internet connection
• mask your internet protocol (IP) address so your online actions are virtually untraceable
• establish secure and encrypted connections to provide greater privacy than even a secured Wi-Fi hotspot
• When you connect to the internet with a VPN, it creates a connection between you and the internet that surrounds your internet data like a tunnel, encrypting the data packets your device sends.
• technically created by a VPN, the tunnel on its own can’t be considered private unless it’s accompanied with encryption strong enough to prevent governments or ISPs from intercepting and reading your internet activity
• The level of encryption the tunnel has depends on the type of tunneling protocol used to encapsulate and encrypt the data going to and from your device and the internet</td></tr>
<tr><td>How ?</td><td><See PDF > pg no: 397</td></tr>
<tr><td>Types of Tunnelling</td><td><table>
<tr><td>Point to Point Tunnelling Protocol (PPTP):</td><td>• oldest protocols for VPN (Microsoft developed for W-95)
• Encrypts data in packets and sends them through a tunnel
• Easiest protocols to configure, requiring only a username, password, and server address to connect to the server
• Fastest VPN protocols because of low encryption level
• Low level of encryption makes it the least secure protocols</td></tr>
<tr><td>Layer 2 Tunnelling Protocol (L2TP/IPSec):</td><td>• conjunction with Internet Protocol Security (IPSec) to create a more secure tunnelling protocol than PPTP.
• L2TP encapsulates the data, but isn’t adequately encrypted until IPSec wraps the data again with its own encryption to create two layers of encryption
• L2TP/IPSec provides AES-256 bit encryption
• Double encapsulation makes highly secure but a little slower than PPTP
• It struggle with bypassing restrictive firewalls because it uses fixed ports
• making VPN connections with L2TP easier to block</td></tr>
<tr><td>Secure Socket Tunnelling Protocol (SSTP):</td><td>• Transports internet data through the Secure Sockets Layer or SSL
• Supported on Windows
• SSL provides internet data going through SSTP very secure
• No fixed Port so it is less likely to be blocked by firewalls than L2TP
• SSL can be used in conjunction with Transport Layer Security (TLS) on web browsers to add a layer to create a secure connection between devices</td></tr>
<tr><td>OpenVPN:</td><td>• relatively recent open source tunnelling protocol
• uses AES 256-bit encryption to protect data packets
• Because the protocol is open source
  • code is vetted thoroughly
  • regularly by the security community
  • constantly looking for potential security flaws
• supported by Windows, Mac, Android, and iOS
• Third-party software is required to set up the protocol - hard to configure
• provides a wide range of strong cryptographic algorithms that will allow users to keep their internet data secure and to even bypass firewalls at fast connection speeds</td></tr>
</table></td></tr>
<tr><td>What VPN can hide ?</td><td>• Browsing history
• IP address and location
• Private devices
• Web activity – maintains internet freedom
• Protects against identity theft</td></tr>
<tr><td></td><td><table>
<tr><th></th><th>Basic VPN
PPTP</th><th>STANDARD VPN
L2TP/IPsec</th><th>SECURE VPN
OpenVPN</th><th>SECURE VPN
SSTP (Very New!)</th></tr>
<tr><td>Encryption/Security</td><td>128 BIT Basic</td><td>256 BIT Standard</td><td>2048 BIT Very Strong</td><td>2048 BIT Very Strong</td></tr>
<tr><td>Supported OS</td><td>Windows
Mac OS X
Linux
iOS
Android
Windows Mobile
DD-WRT</td><td>Windows
Mac OS X
Linux
iOS
Android
Windows Mobile
DD-WRT</td><td>Windows
Mac OS X
Linux
iOS
Android
Windows Mobile
DD-WRT</td><td>Windows
Linux</td></tr>
<tr><td>Compatibility</td><td>desktops, laptops, tablets, smartphones</td><td>desktops, laptops, tablets, smartphones</td><td>desktops, laptops, tablets, smartphones</td><td>desktops, laptops</td></tr>
<tr><td>Speed</td><td>very fast due to the basic encryption</td><td>requires more CPU to encrypt data</td><td>best performance, very fast even on connection with high delay</td><td>best performance, very fast even on connection with high delay</td></tr>
<tr><td>Configuration</td><td>very simple, the protocol built into most devices, does not require additional software</td><td>simple, requires additional settings, the protocol built into most devices, does not require additional software</td><td>additional software required, optionally need to install certificates</td><td>protocol built into Windows 7, additional software required if used in other OS, need to install certificates</td></tr>
<tr><td>Ports</td><td>TCP 1723</td><td>UDP 500
UDP 1701
UDP 4500</td><td>ANY
(highly customizable, can use any ports available, can listen both TCP and UDP protocol)</td><td>TCP 443</td></tr>
<tr><td>Ability to Fuck GFW</td><td>least reliable, very easy to be blocked/filtered</td><td>not reliable, still very easy to be blocked/filtered</td><td>very flexible and customizable, very difficult to be blocked/filtered</td><td>the protocol is too new to be blocked/filtered</td></tr>
<tr><td>Summary</td><td>PPTP is very fast and very easy to set up. It is a good choice if your device does not support OpenVPN or SSTP VPN, and security is not one of your concerns.</td><td>L2TP/IPsec is a good choice if your device does not support OpenVPN or SSTP VPN and you care about the slightly higher security.</td><td>OpenVPN is the recommended protocol for all platforms, the highest performance, security and reliability.</td><td>SSTP is the recommended protocol for Windows (might improve in the future), the highest performance, security and reliability. FENG's BLOG</td></tr>
</table></td></tr>
</table>

	PPTP	L2TP	OpenVPN	SSTP	IKEv2
Pros	• Fast. • Client built-in to almost all platforms. • Easy to set up. •	• Typically considered secure. • Available on all modern devices and operating systems. • Easy to set up. •	• Has the ability to bypass most firewalls. • Highly configurable. • Since it is open source, it can be easily be vetted for backdoors. • It is compatible a variety of encryption algorithms. • Highly secure.	• Has the ability to bypass most firewalls. • The level of security depends on the cipher, but it is usually secure. • Entirely integrated into Windows operating system. • Microsoft support.	• Extremely secure – supports a variety of ciphers such as 3DES, AES, AES 256. • Comes with support for Blackberry devices. • It's stable, especially when reconnecting after losing a connection or switching networks. • It's easy to set up, at least from the user's end. • Relatively faster than L2TP, PPTP and SSTP.
Cons	• It's compromised by the NSA. • Not completely secure.	• Slower than OpenVPN. • May be compromised by the NSA. • Can be problematic if used with restrictive firewalls. • It's likely that the NSA has deliberately weakened the protocol. •	• Can be a little tricky to set up. • It requires third-party software. • Support for desktop is great, but on mobile devices, it needs improvement.	• Since it's a proprietary standard owned by the Microsoft Corporation, it cannot be vetted for backdoors. • Only works on Windows-only platforms	• Supported on limited platforms. • The UDP port 500 used is easy to block as compared to SSL based solutions, like SSTP or OpenVPN. • Not an open source implementation • At the server-end, implementing IKEv2 is tricky, which can cause a few potential issues.

	PPTP	L2TP/IPsec	OpenVPN ™
VPN Encryption	128-bit	256-bit	• 160-bit • 256-bit
VyprVPN Apps Supported	• Windows • Mac • Android	• Windows • Mac • Android • iOS	• Windows • Mac • Android
Manual Setup Supported	• Windows • Mac OS X • Linux • iOS • Android • DD-WRT	• Windows • Mac OS X • Linux • iOS • Android	• Windows • Mac OS X • Linux • Android
VPN Security	Basic encryption	Highest encryption. Checks data integrity and encapsulates the data twice.	Highest encryption. Authenticates data with digital certificates.
VPN Speed	Fast due to lower encryption.	Requires more CPU processing to encapsulate data twice.	Best performing protocol. Fast speeds, even on connections with high latency and across great distances.

Web Servers

25 April 2021 12:37

<table>
<tr><td>Exploits</td><td>
<table>
<tr><td>Code Red</td><td>• Computer Warm, July 15, 2001
• It attacked computers running Microsoft's IIS (Microsoft Internet Information Services) web server
• It contains the text string "Hacked by Chinese!", which is displayed on web pages that the worm defaces
• able to run entirely in memory, leaving no files on the hard drive or any other permanent storage
• attacker, from a remote location, to gain full system level access to any server that is running a default installation of Windows NT 4.0, Windows 2000 and Windows XP, IIS</td></tr>
<tr><td>Nimda</td><td>• Computer Virus, September 18, 2001
• caused traffic slowdowns as it rippled across the Internet
• spreading through four different methods
• Infecting computers containing Microsoft's Web server, Internet Information Server (IIS), and computer users who opened an e-mail attachment.
• Nimda's payload appears to be the traffic slowdown itself - DOS attack and doesn't create any other Harm
• Its name - backwards of admin refers to an "admin.dll" file that, when run, continues to propagate the virus</td></tr>
</table>
</td></tr>
<tr><td>Webserver Vulnerabilities</td><td>
<table>
<tr><td>Sample Files</td><td>• Vendor provided scripts and code snippet to demonstrate the features
• If poorly configured, these can leave holes in security
• Microsoft IIS4.0 - These files could be accessed by a remote attacker and could reveal the contents of just about every other file on the server
• showcode.asp
• codebrews.asp
• Sample files MUST be removed from production servers</td></tr>
<tr><td>Source Code Disclosure</td><td>• allow a malicious user to view the source code of confidential application files
• Under certain conditions, the attacker can combine this with other techniques to view important protected files such as /etc/passwd, global.asa etc
• <See PDF></td></tr>
<tr><td>Canonicalization</td><td>• The process of resolving a resource to a standard (canonical) name is called canonicalization (Computer and network resources can be addressed using more than one representation)
• For example, the file C:\text.txt may also be accessed by the syntax ..\text.txt or \\computer\C$\text.txt
• Applications that make security decisions based on the resource name can easily be fooled into performing unanticipated actions using so-called canonicalization attacks
• ASP::$DATA vulnerability - this vulnerability allows the attacker to download the source code of Active Server Pages (ASP), rather than having them rendered dynamically by the IISASP engine
• Unicode/Double Decode vulnerabilities</td></tr>
<tr><td>Server Extensions</td><td>• Additional functionalities are provided in the form of libraries (extensions) to the web server
• Features such as dynamic script execution, security, caching etc
• These extensions may have vulnerabilities like
- Microsoft Indexing extension had buffer overflows
– Microsoft Internet Printing Protocol (IPP) had buffer overflow attacks in IIS5
– Web Distributed Authoring and Versioning (WebDAV)
– Secure Sockets Layer (SSL) of Apache's mod_ssl had buffer overflow
– Netscape Network Security Services Library Suite had vulnerabilities
• Microsoft WebDAV 'Translate: f' vulnerability
- causes the web server to fork execution over to a vulnerable addon library when an unexpected input is sent
- <Check PDF></td></tr>
<tr><td>Input validation Buffer Overflow / SQL Injection</td><td>• provides ability to execute arbitrary commands on the victim machine, typically with very high privilege levels.
• Most of the vulnerability based on buffer overflows aim at forcing the execution of malicious code, mainly in order to give a root shell to the user.
• The malicious instructions are stored in a buffer, which is overflowed to allow an unexpected use of the process, by changing various memory sections.
• Buffer overflow attacks exploit a need of bounds checking on the size of input being stored in a buffer array
• By writing the data into the memory assigned to array, the attacker can make arbitrary changes to program state stored an adjacent to the array
• Buffer overflows types
• Stack based :
• Heap based :</td></tr>
<tr><td>Denial of Service</td><td></td></tr>
</table>
</td></tr>
<tr><td>Scanners</td><td>
<table>
<tr><td>Nikto</td><td>• Nikto is an Open Source (GPL) web server scanner which performs comprehensive tests against web servers for multiple items,
• including over 6700 potentially dangerous files/programs, c
• Checks for outdated versions of over 1250 servers,
• and version specific problems on over 270 servers
• also checks for server configuration items such as
• the presence of multiple index files,
• HTTP server options,
• identify installed web servers and software. Scan items and plugins are frequently updated and can be automatically updated</td></tr>
<tr><td>Nessus</td><td>• Network vulnerability scanner that contains a large number of tests for known vulnerabilities in web server software
• Nessus is a multiple platform network and host vulnerability scanner, supported on Window, Linux , Mac OS, UNIX</td></tr>
</table>
</td></tr>
<tr><td>Web App. Hacking</td><td>• attacks on applications
• <See PDF></td></tr>
<tr><td>Web Crawling</td><td>• <See PDF></td></tr>
<tr><td>Microsoft IIS Vulnerabilities</td><td>
<table>
<tr><td>Request Smuggling</td><td>• HTTP request smuggling is a technique for interfering with the way a web site processes sequences of HTTP requests that are r eceived from one or more users
• Request smuggling vulnerabilities are often critical in nature, allowing an attacker to bypass security controls, gain unauth orized access to sensitive data, and directly compromise other application users.
• <see link></td></tr>
</table>
</td></tr>
</table>

	Response Splitting	
	Privilege escalation	
	Denial of Service	
	XSS	

IBM WebSphere	Remote Code Execution
	• Issue occurs when serializing an object from an untrusted source
	• This could allow for a remote attacker to execute arbitrary code on the system with a specially-crafted sequence of serialized objects
	• This happens due to how the IBM WebSphere Application Server handles the Internet Inter-ORB Protocol.
	• vulnerability exists due to insecure input validation when processing serialized data.
	• Successful exploitation of this vulnerability could allow an attacker to execute remote code in the context of the affected application. Based on the privileges associated with the application, attack could
	  • install programs
	  • view, change, or delete data
	  • create new accounts with full user rights.
	• Failed exploitation could result in a denial-of-service condition.	

Database Exploits

25 April 2021 15:25

<table>
<tr><td>DB Hacking</td><td>• Database software vulnerabilities
• very complex piece of code that contains huge amounts of logic and thus a huge attack surface
• This is difficult to cover
• Application (executing inside the DB) logic vulnerabilities
• Unpatched version
• Default open ports
• SQL Slammer worm
• exploited a known buffer overflow in MS SQL Server resolution services running on port 1434
• managed to infect 75,000 computers in the first 10 minutes of its spreading
• Oracle listener process usage port 1521
• MS-SQL server usage port 1434</td></tr>
<tr><td>DB Discovery</td><td>• Nmap as network exploration tool that identifies hosts, open ports and the services running on them, service versions and OS.
• can be used to detect servers running popular databases with vulnerable versions
• It can run built-in and readily available scripts such as mysql-info.nse, ms-sql-info.nse, oracle-sid-brute.nse, and db2-info.nse</td></tr>
<tr><td>DB Vulnerabilities</td><td>
<table>
<tr><td>Network Attack</td><td>• All DB platform have network listening agent
• Listening agent has to be securely written to avoid the attack such as buffer overflows
• Attack chances are in direct proportion of complexity of the protocol used for the listening agent
• SQL Slammer was a buffer overflow exploit
• CVE-2012-0072 - Oracle listener vulnerability - can be exploited without any privileges
• Attacker can gain full control of the host running the database
• Trusting commands sent from a client and then executing them as a privileged user can lead to full database compromise

Countermeasure:
• Segment internal network and separate databases from other segments
• e.g. Valid node checking for Oracle
• select subset of internal IP addresses to access the database - DMZ
• DBMS vendor patches as soon as they are made available</td></tr>
<tr><td>DB Engine bugs</td><td>• most complex pieces of software
• different components let users create programs to execute inside the database , such as parsers and optimizers as well as running environments (PL/SQL, TSQL)
• bugs like improper permission validations and buffer overflows that allow an attacker to gain full control of the database
• incorrect permissions validation vulnerability in Oracle (patched in July 2007)
• allowed specially crafted SQL statements to bypass permissions granted to the executing user
• Allowing perform updates, inserts, and deletes on tables without appropriate privileges
• CVE-2008-0107 - attacker to take control of an MS SQL Server host via an integer underflow vulnerability on all MS SQL Server versions up to 2005 SP2

Countermeasure
• DBMS vendor patches as soon as possible
• Monitor database logs - audit user activity</td></tr>
<tr><td>Vulnerable built-in stored procedure</td><td>• A stored procedure is a group of SQL statements that has been created and stored in the database, A stored procedure will accept input parameters so that a single procedure can be used over the network by several clients using different input data
• DBMS provide a large number of built-in stored procedures and packages
• stored objects provide additional functionality to the database and help administrators and developers to manage the database system.
• Users can also write their own stored procedures and put inside the database
• Oracle database is installed with almost 30,000 publicly accessible objects that provide functionality like access OS files, make HTTP requests, manage XML/JSON objects, facilitate replication etc
• These has vulnerabilities like SQL injection, buffer overflow, application logic issues etc

Countermeasure
• DBMS vendor patches as soon as they are made available
• Follow the least privilege principle
• revoke access to dangerous database objects</td></tr>
<tr><td>Weak/Default password</td><td>• Oracle - default user & password of “Scott” and “tiger”.
• An Attacker
• Finds a vulnerable database using scanning techniques
• Usage a script that contains a few hundred combinations of credentials
• most cases, succeeds in gaining access to the database.
• Weak passwords are easy to crack using brute-force
• ‘Cain and Abel’ or ‘John the Ripper

Countermeasure
• Periodically scan your databases - discover and alert users to weak and default passwords.
• Monitor application accounts for suspicious activity not originating from the application servers.
• Steer clear of default passwords and institute tight password management and regular change-ups.</td></tr>
<tr><td>Mis-Configuration</td><td>• Database comes with default settings which are public knowledge or easy to crack
• Applications may be installed using default accounts which have default passwords are also easy to crack
• Insecure default settings left unchanged by administrators leave the database open to attack
• DB2 TRUST_ALLCLNTS if set to ‘yes’ - turns off all authentication authorization of the database.
• Most databases come with a set of applications installed, many of which are unnecessary to the organization</td></tr>
</table>
</td></tr>
</table>

	Countermeasure • Create a gold standard for each database platform setup/installation • alert on any deviations from this standard. • Periodically scan databases -

Indirect Attacks	• An attacker after gaining control of a DBA machine,
	  • install a keylogger on the DBA's machine to capture credentials
	  • can change a configuration files or modify database client binaries to inject his own malicious commands into the database
	  • e.g. change configuration such that allows an attacker to log into the database without an actual attack & action Logging
	
	Countermeasure
	• Monitor and alert on suspicious privileged user's behaviour
	• Restrict what is allowed to run on the DBA system to known good programs only.
	• Do not click untrusted/unknown links - specially on DBA system
	• Strictly control user access to the DBA system

Cloud Exploits

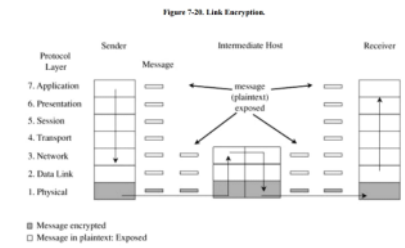
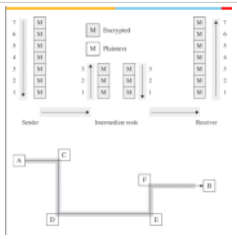
25 April 2021 16:20

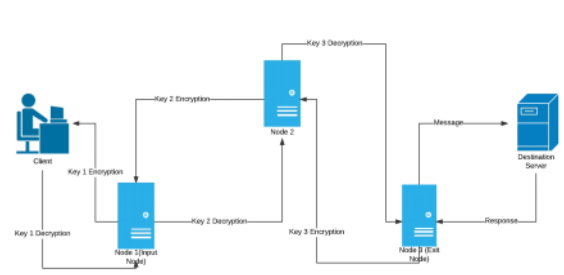
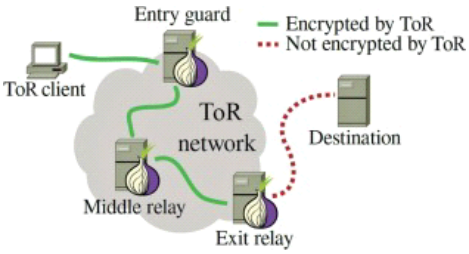
<table>
<tr><td>Cloud Threat Actors</td><td colspan="2">• Malicious CSP administrators
• Malicious Customer Cloud administrators
• Cyber criminals
• Nation State-sponsored actors
• Untrained of negligent customer administrators/users</td></tr>
<tr><td>Vulnerabilities</td><td>Cloud Misconfiguration</td><td>• Prevalence : High | Sophistication : Low
• Mainly due to cloud service policy mistakes or misunderstanding shared responsibility
• Impact can go to DOS to Account compromise
• Security principles such as least privilege and defense-in-depth should be applied during initial design and planning
• Well-organized cloud governance is critical</td></tr>
<tr><td></td><td>Poor Access Control</td><td>• Prevalence : Mid| Sophistication : Mid
• weak authentication/authorization methods or include vulnerabilities that bypass these methods.
• Weaknesses in access control mechanisms can allow an attacker to elevate privileges, resulting in the compromise of cloud resources
• Use multi-factor authentication with strong factors and require regular re-authentication
• Disable protocols using weak authentication
• Limit access to and between cloud resources with the desired state being a Zero Trust model
• Use automated tools to audit access logs for security concerns
• Do not include API keys in software CVS</td></tr>
<tr><td></td><td>Shared Tenancy Vulnerability</td><td>• Prevalence : Low | Sophistication : High
• Vulnerabilities in cloud hypervisors or container platforms could be severe
• Hypervisor vulnerabilities are difficult and expensive to discover and exploit - which limits their exploitation to advanced attackers
• Containerization
  • while being an attractive technology for performance and portability, should be carefully considered before deployment in a multi-tenant environment.
  • run on a shared kernel, without the layer of abstraction that virtualization provides
  • In a multi-tenant environment a vulnerability in the container platform could allow an attacker to compromise containers of other tenants on same host
• Enforce encryption of data at rest and in transit with strong encryption methods
• properly configured, managed and monitored key management systems
• sensitive workloads, use dedicated, whole-unit, or bare-metal instances</td></tr>
<tr><td></td><td>Supply Chain Vulnerability</td><td>• Prevalence : Low | Sophistication : High
• Presence of inside attackers and intentional backdoors in hardware and software
• Third-party/OEM cloud components may contain vulnerabilities intentionally inserted by the developer to compromise the application.
• Inserting an agent into the cloud supply chain, as a supplier, administrator or developer, could be an effective means for nation state attackers to compromise cloud environments
• Enforce encryption of data at rest and in transit with strong encryption methods
• Procure cloud resources pursuant to applicable accreditation processes
• Select cloud offerings that have had critical components evaluated against National Information Assurance Partnership (NIAP) Protection Profiles (PPs)
• Ensure that development and migration contracts stipulate adherence to internal standards or equivalent processes for mitigating supply chain risk</td></tr>
</table>

Defence Process / Tools

25 April 2021 17:35

<table>
<tr><td>What ?</td><td>•</td></tr>
<tr><td>Attack Points</td><td>
<table>
<tr><td>User Authentication</td><td>• Multiple layers of protection
• regular security policy enforcement for accounts
• strong password requirements, policy of frequent password changes etc
• Protect user identities using MFA
• Having increased callback feature, where the user initially authenticates using his/her credentials (username and password), and receives a call to enter their pin
• If both authentication factors succeed, they are authorized to access the system or network</td></tr>
<tr><td>Data Security</td><td>
<table>
<tr><th>State</th><th>Description</th><th>Threats</th><th>Countermeasures</th><th>Security triad affected</th></tr>
<tr><td>Data at rest on the user's device.</td><td>The data is currently located on the user's device.</td><td>The unauthorized or malicious process could read or modify the data.</td><td>Data encryption at rest. It could be file-level encryption or disk encryption.</td><td>Confidentiality and integrity.</td></tr>
<tr><td>Data in transit.</td><td>The data is currently being transferred from one host to another.</td><td>A man-in-the-middle attack could read, modify, or hijack the data.</td><td>SSL/TLS could be used to encrypt the data in transit.</td><td>Confidentiality and integrity.</td></tr>
<tr><td>Data at rest on-premise (server) or cloud.</td><td>The data is located at rest either on the server's hard drive located on-premise or in the cloud (storage pool).</td><td>Unauthorized or malicious processes could read or modify the data.</td><td>Data encryption at rest. It could be file-level encryption or disk encryption.</td><td>Confidentiality and integrity.</td></tr>
</table>
</td></tr>
<tr><td>Cont. Security Monitoring</td><td>Defence in Depth
• Network security control
• Antivirus software
• Analysing data integrity
• Behavioural analysis</td></tr>
</table>
</td></tr>
<tr><td>Network Security</td><td>• Network Encryption :
• Encryption protects only what is encrypted - At sender or receiver end once data is decrypted, it’s exposed to threats
• Encryption is no more secure than its key management. Once key is revealed, encryption is of no use
• Encryption types:
○ Link encryption: Host to Host
○ End to end encryption: Application to Application

<table>
<tr><td>• Link Encryption :
• Host to Host
• Useful when all hosts are reasonably secure but communication line is not
• Encryption occurs at layer 1 or 2 in OSI network model
• covers the communication from one node to next on the path to destination
• Message remains plain in hosts
• Router or intermediate devices will decrypt the data so that they know where to send it</td><td> 
</td></tr>
<tr><td>End-to-End Encryption
• Encryption is applied between two users - only users can see data - preventing eavesdropping
• Encryption is performed at highest level of network layers
• Data confidentiality is maintained even if a lower layer fails or communication goes through unsecure node</td><td>  </td></tr>
</table>
</td></tr>
<tr><td>Browser Encryption</td><td>• Browsers can encrypt data during transmission - negotiating with server on the algorithm
• SSH
• Authentication (Public keys, Kerberos) and encryption service (DES, AES) - to Shell or OS commands
• Replaces telnet, rlogin, rsh for remote access
• Protects against spoofing & data modification during transmission
• SSL/TLS
• 3 version 1.0, 2.0. 3.0. Version 3.1 is known as TLS
• Implemented at layer 4 (transport layer)
• SSL operates at application level
• Provides server authentication, optionally client authentication and encrypted communication channel between client and server
• SSL encrypts data that is transmitted across the web
• Anyone intercepting data will see only encrypted data - difficult to decrypt
• SSL initiates an authentication process called a handshake between two communicating devices
• ensure that both devices are really who they claim to be
• SSL also digitally signs data in order to provide data integrity</td></tr>
<tr><td>Cypher Suite</td><td>• client & server negotiated encryption algorithm for authentication, session encryption and hashing
• Server sends a set of records listing cypher suite identifiers it can use -</td></tr>
</table>

	• Client responds with the preferred choices
IP Sec	• The IP security (IPSec) is an Internet Engineering Task Force (IETF) standard suite of protocols • • between 2 communication points across the IP network that provide data authentication, integrity, and confidentiality • **IPSec provides confidentiality, integrity, authenticity, and replay protection through two new protocols.** **1. Authentication Header (AH)** a. provides authentication, integrity, and replay protection (but not confidentiality) b. Its main difference with ESP is that AH also secures parts of the IP header of the packet (such as the source/destination addresses). **2. Encapsulated Security Payload (ESP)** **a.** ESP provides authentication, integrity, replay protection, and confidentiality of the data **b.** it secures everything in the packet that follows the header **c.** Replay protection requires authentication and integrity **d.** Confidentiality (encryption) is used with or without authentication/integrity **e.** Similarly, authentication/integrity is possible with or without confidentiality. An example of a tunnel mode AH packet: IPhdr | AH | IPhdr2 | TCPhdr | data An example of a transport mode AH packet: IPhdr | AH | TCPhdr | data ○ Because an ESP header cannot authenticate the outer IP header, it is useful to combine an AH and an ESP header to get this: IPhdr | AH | ESP | TCPhdr | data This is called Transport Adjacency. The tunneling version looks like: IPhdr | AH | ESP | IPhdr2 | TCPhdr | data • IPSec implemented at OSI layer 2 (data layer) • Security Association (SA): a set of security parameter for a secured communication channel • Encryption algorithm, key and mode • Encryption parameters like initialization vector • Authentication protocol and key • Life span of the SA • Address of opposite end of association • Sensitivity level of protected data (used for classified information)
The Onion Routing	• TOR • Link & End to end encryption data is encrypted but client & server address remain exposed • TOR prevents an eavesdropper from learning source, destination, or content of data in transit • transferring communication around a network of computer before delivery to receiver • A encrypts the packet with **B's public key** and appends a header from **Z to B** • Then A encrypts the result with **Z's public key** and appends a header **from Y to Z** • Then A encrypts the result with **Y's public key** and appends a header from **X to Y** • Then A encrypts the result with **X's public key** and appends a header from **A to X** • Upon receipt of the packet, intermediate nodes only know the previous and next nodes for the packet and not the whole path • Browsers: TOR, Orfox, Epic, Comodo Ics Dragon **How it works ?** • The client with access to all the encryption keys i.e. key 1, key 2 & key 3 encrypts the message (get request) **thrice** • wrapping it under 3 layers like an onion which have to be peeled one at a time. • This triple encrypted message is then sent to the first server i.e. Node 1(Input Node). • Node 1 • has the address of Node 2 and Key 1. • it decrypts the message using Key 1 and realizes that it doesn't make any sense because of 2 layers of encryption • so it passes it on to Node 2 • Node 2 • Has key 2 and address of Exit Node • decrypts the message using Key 2 realizes that it's still encrypted and passes it onto the exit node • Node 3 (Exit Node) • peels of the last layer of encryption and finds a GET request • It can view the request (i.e. youtube.com) and passes it on to the actual server • Server will respond back with Webpage. • The response passes through the same nodes in the reverse direction where each node puts on a layer of encryption using their specific key • finally reaches the client in the form of a triple encrypted response • client has access to all the keys  

Firewall

28 April 2021 12:34

Firewall

- Firewalls are network security devices which protect a subnet (mainly internal) from harm by another subnet (mainly external)
- It can also be used to separate the sensitive segments of a network i.e. R&D
- Firewalls run on dedicated systems for performance and security reasons
- Firewall system typically doesn't have compilers, linkers, loaders, text editors, debuggers, programming libraries or other tools which an attacker can take advantage of
- CISCO runs its own OS on its firewalls

How it works?

- Filters traffic between a protected (inside) network and less trustworthy (outside) network
- Firewall is a traffic cop that permits or block data flow between two parts of a network architecture
- Firewalls enforce pre-determined rules (security policies) to govern traffic flow
- Two rules commonly used
  - default permit
  - default deny

Rule	Type	Source Address	Destination Address	Destination Port	Action
1	TCP	*	192.168.1.*	25	Permit
2	UDP	*	192.168.1.*	69	Permit
3	TCP	192.168.1.*	*	80	Permit
4	TCP	*	192.168.1.18	80	Permit
5	TCP	*	192.168.1.*	*	Deny
6	UDP	*	192.168.1.*	*	Deny

- **Security Policy:** Set of rules that define what traffic can or can not pass thru the firewall
- Firewalls enforce pre-determined rules (security policies) to govern traffic flow

- **Rule 1:** Allow traffic from any outside host to 192.168.1 subnet on port 25 (mail transfer)
- **Rule 2:** Allow traffic from any outside host to 192.168.1 subnet on port 69 (file transfer)
- **Rule 3:** Allow traffic from 192.168.1 subnet to any outside host on port 80 (web pages)
- **Rule 4:** Allow traffic from any outside host to 192.168.1.18 on port 80 (web server)
- **Rule 5 & Rule 6:** Deny all other traffic (inbound or outbound)

Rules

Firewalls can enforce pre-determined rules for:

- IP Address
- Domain name
- Protocols
- Programs
- Ports
- Key words

Limitations

Limitations <See PDF>

- Firewall can protect an environment only if the firewall controls entire perimeter
- Firewalls do not protect data outside perimeter
- Firewalls are most visible part of an installation to outsiders and hence most attractive target for attack
- Firewalls must be configured correctly - configuration must be updated
- Firewalls are targets for intruders, check firewall logs periodically for evidence of attempted or successful intrusions
- Firewalls exercise only limited control over the content inside packet - hence may not be able to stop malicious code or inaccurate data completely

Categories

Packet Filtering Firewall

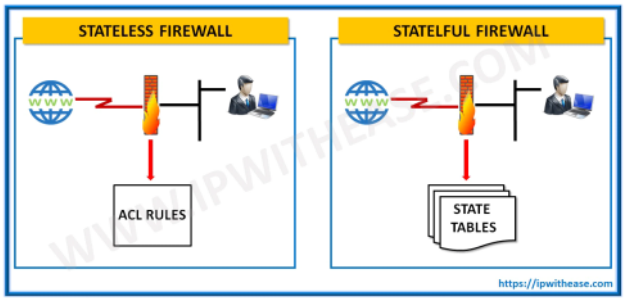
- Simplest form of firewalls
- Controls access based on packet IP address (source or destination) or specific transport protocol type (HTTP, Telnet)
- Doesn't inspect data inside packet
- treats each packet in isolation.
- It has no ability to judge whether a packet is part of an existing stream of traffic.
- Can detect outside traffic with a forged source header
- Usage separate interface cards for inside and outside traffic
- Cannot implement complex rules

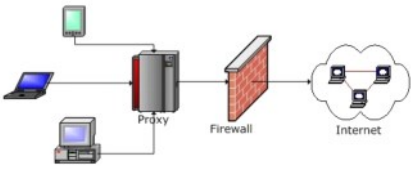
	Source IP	Dest. IP	Source Port	Dest. Port	Action
1	192.168.21.0	--	--	--	deny
2	--	--	--	23	deny
3	--	192.168.21.3	--	--	deny
4	--	192.168.21.0	--	>1023	Allow

1. Incoming packets from network 192.168.21.0 are blocked.
2. Incoming packets destined for internal TELNET server (port 23) are blocked.
3. Incoming packets destined for host 192.168.21.3 are blocked.
4. All well-known services to the network 192.168.21.0 are allowed.

Stateful Inspection

- **performs Stateful Packet Inspection**
- are able to determine the **connection state of packet** which makes it more efficient
- It keeps track of the state of networks connection travelling across it, such as TCP streams.
- Filtering decisions would not only be based on defined rules, but also on packet's history in the state table.
- judge traffic based on information from multiple packets
- If someone is trying to **scan ports in a short time, firewall will block that host**



Application Proxy	• Application proxy firewall simulates the behavior of a protected application on the inside network, **allowing in only safe data** • Application proxy intrudes in the middle of protocol between sender and receiver, similar to man in the middle • Proxy interprets the protocol stream as an application would and takes control action based on things visible inside the protocol • Can filter traffic at application level. • Proxy firewalls monitor traffic for layer 7 protocols (HTTP, FTP etc) and use both **stateful and deep packet inspection** to detect malicious traffic. 
Circuit Level Gateway	• functions as a virtual gateway between two networks • This firewall allows one network to be extension of another network • Firewall verifies the circuit at time of creation after which data transfer is normal • VPN • <see PDF>
Guard Firewall	• proxy type firewall • implements programmable set of conditions, even if the program conditions become very sophisticated • Ex. Great firewall of China (Golden Shield Program) - It filters content based on government restrictions/ rules.

Personal firewall	• program that runs on a single host to monitor and control traffic to that host
	• works in conjunction with support from operating system
	• It does
	  • List of safe/unsafe sites
	  • Policy to download code/files
	  • Unrestricted data sharing
	  • Management access from corporate but not from outside
	  • Combine action with anti-virus software
	• Ex. SaaS Endpoint Protection (McAfee), F-Secure Internet Security, Microsoft Windows Firewall, Zone Alarm, Checkpoint

NAT firewalls	• Network Address Translation :
	  • process in which one or more local IP address is translated into one or more Global IP address and vice versa in order to provide Internet access to the local hosts
	  • The idea of NAT is to allow multiple devices to access the Internet through a single public address
	• attackers scanning a network for IP addresses can't capture specific details,
	• NAT firewalls are similar to **proxy firewalls** in that they act as an intermediary between a group of computers and outside traffic.

NGFW	• Next Generation Firewalls
	• traditional firewall technology with additional functionality, such as encrypted traffic inspection, intrusion prevention systems, anti-virus etc.
	• capability to deep packet inspection (DPI)
	  • While basic firewalls only look at packet headers, deep packet inspection examines the data within the packet itself, enabling users to more effectively identify, categorize, or stop packets with malicious traffic
	• TCP handshake checks
	• Surface level packet inspection
	• Intrusion prevention systems (IPSs) that work to automatically stop attacks against network
	• next-generation firewall must include:
	  • Standard firewall capabilities like stateful inspection
	  • Integrated intrusion prevention
	  • Application awareness and control to see and block risky apps
	  • Upgrade paths to include future information feeds
	  • Techniques to address evolving security threats
	• Ex : FortiGate (Fortinet), Cisco ASA, Cisco Meraki MX, Sophos XG,SonicWall TZ, CheckPoint, Palo Alto, Juniper etc
	
	Features <See PDF for details >
	  • Breach prevention and advanced security
	  • Comprehensive network visibility
	  • Flexible management and deployment options
	  • Fastest time to detection
	  • Automation and product integrations

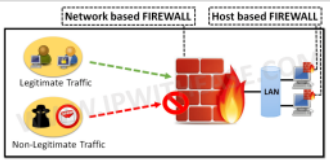
Threat Focused NGFW	• include all the capabilities of a traditional NGFW and also provide advanced threat detection and remediation.
	• We can
	  • Know which assets are most at risk with complete context awareness
	  • Quickly react to attacks with intelligent security automation that sets policies and hardens your defenses dynamically
	  • Better detect evasive or suspicious activity with network and endpoint event correlation
	  • Greatly decrease the time from detection to clean-up with retrospective
	  • security that continuously monitors for suspicious activity and behaviour even after initial inspection
	  • Ease administration and reduce complexity with unified policies that protect across the entire attack continuum

DMZ	• DMZ Network (De-Militarized Zone) functions as a subnetwork • Containing an organization's exposed, outward facing services. • The goal of a DMZ is to add an extra layer of security • end goal of a DMZ is to allow an organization to access untrusted networks, such as the internet, while ensuring its private network or LAN remains secure • Organizations typically store external-facing services and resources, as well as servers for the Domain Name System (DNS), File Transfer Protocol (FTP), mail, proxy, Voice over Internet Protocol (VoIP), and web servers, in the DMZ. • These servers and resources are isolated and given limited access to the LAN to ensure they can be accessed via the internet but the internal LAN cannot • DMZ approach makes it more difficult for a hacker to gain direct access to an organization’s data and internal servers via the internet

Comparing the pros and cons of the different types of firewalls

FIREWALL TYPE	ADVANTAGES	DISADVANTAGES
Packet filtering firewall	■ A single device can filter traffic for the entire network ■ Efficient and fast at processing packets ■ Enables complex security policies through filtering on protocol headers ■ Inexpensive ■ Minimal impact on other resources, network performance, end-user experience	■ Incapable of filtering at the application layer ■ Lacks broad context of other firewall options ■ Can be difficult to securely configure ■ Lacks features like user authentication, logging ■ Vulnerable to spoofing attacks ■ Access controls lists can be difficult to set up and manage
Circuit-level gateway	■ Provides privacy for data passing in/out of private network ■ More efficient processing traffic than application-level gateways ■ Relatively inexpensive ■ Easier to set up and manage ■ Minimal impact on end-user experience	■ Protects circuits (network sessions) rather than individual packets ■ Requires modification to network protocol stack ■ Incapable of content filtering ■ Should be used in conjunction with other firewall technologies ■ Does not offer application-layer monitoring
Application-level gateway	■ Capable of detecting and blocking attacks not visible at the OSI model network or transport layers ■ Obscures private network details ■ Protects user anonymity ■ Enables more fine-grained security controls	■ Complex to configure and maintain ■ High processing overhead ■ Requires a proxy be set up for every network application in use ■ Can affect network performance
Stateful inspection firewall	■ Capable of blocking types of attacks that exploit protocol vulnerabilities ■ Can operate with fewer open ports, reducing attack surface ■ Capable of blocking many types of denial-of-service attacks	■ Can require high degree of skill to securely configure ■ Does not support authenticated connections ■ Not effective against exploits of stateless protocols ■ High processing overhead
Next-generation firewall	■ Provides traditional firewall functionality combined with other security functions, including intrusion detection/prevention systems (IDS/IPS), advanced threat intelligence, malware scanning and others ■ Capable of monitoring network protocols from the data link layer (Layer 2 of the OSI model) through the application layer (Layer 7 of the OSI model) ■ Offers substantive logging capabilities ■ Can be more efficient at processing network traffic than combination of firewall plus IDS/IPS and malware scanning	■ Consolidation of security functions makes the NGFW a single point of failure ■ Requires high front-end investment of resources to acquire, configure and deploy these complex systems ■ Depending on architecture, may be processing-intensive ■ Not all organizations will require all the functionality of an NGFW ■ Can hinder network performance ■ More expensive than other firewall options

Types



Host Based	• Software Firewall - Windows Firewall • Host based Firewall will be the best bet to provide security to the OS and end System • The major benefit of using host based Firewall is that since the protection system is installed in the host itself, it is very easy to point out whether the actual attack was successful or not.
Network based	• Hardware + software Firewalls • is a device which controls access to secured LAN network to protect it from unauthorized access • Firewall acts as a filter which blocks incoming non-legitimate traffic from entering the LAN network and cause attacks.

PARAMETER	NETWORK BASED FIREWALL	HOST BASED FIREWALL
Terminology	Firewall filters traffic going from Internet to secured LAN and vice versa.	A host firewall is a software application or suite of applications installed on a singular computer
Placement	At the Perimeter or border of the network like Internet handoff point to address the unauthorized access from the entry/exit point.	Placed at end Host systems and will be in a way, 2nd line of defence if unauthorized traffic has not been blocked by Network based firewall.
Hardware/Software based	Hardware based	Software based
Functions at	Network Level	Host level
Mobility	Cannot be moved until all the assets of LAN have been migrated to new location	Since Host based Firewall is installed on end machine (Laptop/desktop) , hence Host based firewall is mobility friendly
Internal Protection (same VLAN/Zone)	For end host to end host communication in same VLAN , Network Firewall does not provide security	For end host to end host communication in same VLAN, Host based Firewall provides security control and protection.
Network Protection	Strong defence barrier compared with host-based. Infact Network Firewalls are hardened enough leaving very less space for attacker to play.	Limited defence barrier compared to Network firewalls
Scalability	Easy to scale since increase in number of users in LAN triggers more bandwidth requirement and rightly sized Firewall considering future growth does not require much of effort to accommodate high bandwidth.	More effort required to scale in terms of more installations & maintenance on each device when number of hosts increase
Maintenance	Manpower may be shared and limited since only 1 or 2 sets of Network Firewall need to be managed	Dedicated IT team required to monitor and maintain and update Host based Firewall on each end device
Skillset	Setup requires highly skilled resources with good understanding of Security devices	Skillset of basic Hardware/software understanding and program installation
Cost	Lower when comes to large enterprise	Higher when it comes to large enterprises

https://ipwithease.com

DLP

30 April 2021 17:26

<table>
<tr><td>What?</td><td>• Data Loss Prevention
• data leak incidents in cases where media containing sensitive information is lost and subsequently acquired by an unauthorized party.
• Data loss prevention software detects potential data breaches/data ex-filtration transmissions and prevents them
• by monitoring,[1]
• detecting and blocking sensitive data while in use (endpoint actions),
• in motion (network traffic),
• at rest (data storage)
• DLP looks for indicators:
• Keywords: set of identified words in the data
• Traffic patterns: bulk file transfer, file sharing, connection to outside email etc.
• Encoding/encryption: block outgoing files that they can’t decode/decrypt</td></tr>
<tr><td>Two Implementation</td><td><table><tr><td>Agent Based</td><td>• Installed as a rootkit to monitor user behavior like network connections, file access, applications run etc.</td></tr><tr><td>Application Based</td><td>• Software agents to monitor email, file transfer etc</td></tr></table></td></tr>
<tr><td>Categories</td><td><table><tr><td>Standard Measure</td><td>• such as firewalls, intrusion detection systems (IDSs) and antivirus software, are commonly available products that guard computers against outsider and insider attacks
• The use of a firewall, for example, prevents the access of outsiders to the internal network and an intrusion detection system detects intrusion attempts by outsiders.
• Inside attacks can be averted through antivirus scans that detect Trojan horses that send confidential information, and by the use of thin clients that operate in a client-server architecture with no personal or sensitive data stored on a client device</td></tr><tr><td>Advance Measure</td><td>• employ machine learning and temporal reasoning algorithms to detect abnormal access to data (e.g., databases or information retrieval systems) or abnormal email exchange
• honeypots for detecting authorized personnel with malicious intentions and activity-based verification (e.g., recognition of keystroke dynamics)
• user activity monitoring for detecting abnormal data access.</td></tr><tr><td>Designated Systems</td><td>• detect and prevent unauthorized attempts to copy or send sensitive data, intentionally or unintentionally, mainly by personnel who are authorized to access the sensitive information
• In order to classify certain information as sensitive system uses mechanisms, such as :
• exact data matching
• structured data fingerprinting
• statistical methods, rule and regular expression matching,
• published lexicons,
• conceptual definitions,
• keywords and contextual information such as the source of the data</td></tr></table></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
</table>

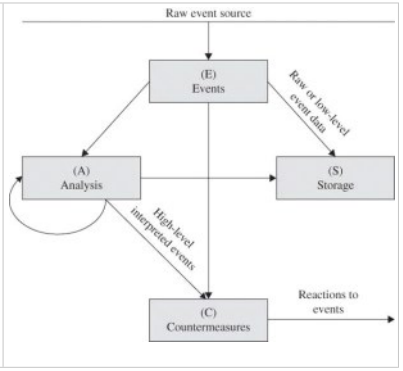
Honeypots

28 April 2021 19:04

<table>
<tr><td>What ?</td><td>• cyber honeypot is a baiting trap for hackers.
• It's a sacrificial computer system to attract cyberattacks, like a decoy.
• Honeypots are filled with fabricated information
• Any access to honeypots triggers monitoring and logging actions
• It mimics a target for hackers, and uses their intrusion attempts to gain information about cybercriminals and the way they are operating or to distract them from other targets.
• Defense through Deception</td></tr>
<tr><td>How it works ?</td><td>• The honeypot looks like a real computer system, with applications and data, fooling cybercriminals into thinking it's a legitimate target
• Once the hackers are in, they can be tracked
• their behavior assessed for clues on how to make the real network more secure.
• Honeypots are made attractive to attackers by building in deliberate security vulnerabilities.
• Vulnerable ports might be left open to entice attackers into the honeypot environment, rather than the more secure live network
• A honeypot isn't set up to address a specific problem, like a firewall or antivirus
• it's an information tool that can help you understand existing threats to your business and spot the emergence of new threats
• With the intelligence obtained from a honeypot, security efforts can be prioritized and focused.</td></tr>
<tr><td>Interaction level</td><td>
<table>
<tr><th>Low Interaction</th><th>Mid Interaction</th><th>High Interaction</th></tr>
<tr><td>• Simple to install
• Only provides few fake services – port emulation
• No real operating system</td><td>• Provides more interaction
• Services are still emulated
• Scripts used to provide more interaction
• Requires higher skills to deploy</td><td>• Actual operating system in place for interacting with attacker
• Potential to gather more information
• Higher risk</td></tr>
<tr><td>• Honeyd
• Back Office Friendly (BOF)</td><td>• MwCollected
• Multipot</td><td>• KFSensor
• Argos
• Minos
• Man Trap</td></tr>
</table>
</td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
</table>

IDS /IPS /Firewall

30 April 2021 17:43

<table>
<tr><td>What ?</td><td>• Intrusion Detection System (IDS) is a system that monitors network traffic for suspicious activity and issues alerts when suc h
activity is discovered
• Like Smoke detector
• IDS response
• Manual : Alarm for someone to take action
• Automate : get into protection mode to isolate the intruder (IPS)</td></tr>
<tr><td>How it works ?</td><td>• Raw inputs from sensors
• Data storage of raw inputs
• Analysis of events
• Intrusion identification
• Countermeasure plan
• Response to events
 
</td></tr>
<tr><td>Functions</td><td>• Monitor the operation of routers, firewalls, key management servers and files
• Help administrators to tune, organize and understand operating system audit trails and other logs to highlight policy violation
• Assess integrity of critical system files for vulnerabilities and misconfiguration
• Provide a user-friendly interface so non-expert staff members can assist with managing system security
• Build and maintain an extensive attack signature database
• Recognize and report when data files have been altered
• Correct system configuration errors
• Install and operate traps to record information about intruders
• Generate an alarm and notify when security has been breached
• React to intruders by blocking them or blocking the server</td></tr>
<tr><td>Components</td><td>
<table>
<tr><td>Network Sensor</td><td>• Electronic eye
• Hardware or software that monitors traffic in network and triggers alerts
• Single session attacks
• Multiple session attacks
• Types
• Host Based
○ Server specific agents
○ Provide both packet and system level monitoring
○ Distributed Agent residing on each server to be protected
○ Tied with underlying OS
○ analysis of data encrypted for transport
○ Monitors kernel-level application behavior, to mitigate attacks such as buffer-overflow and privilege escalation
• Network Based
• Specialized software and/or hardware used to collect and analyses network traffic
• Applications, modules embedded in network infrastructure</td></tr>
<tr><td>Alert Systems</td><td>• Triggers : Circumstances that cause an alert to be sent
• Types
• Detection of an anomaly
○ Requires use of profiles for each authorized user of group of users
○ Describe services and resources normally used by users
○ Accuracy issues
▪ False negative
▪ False positive
• Detection of misuse
○ signature-based detection that uses recognized patterns
○ These patterns describe suspect, collection of sequences of activities or operations that can be possibly be harmful and stor ed in database.
• Matching of a signature
○ Triggers alarm based on characteristics signature of known attacks
○ IDS comes equipped with a database of signatures
▪ can start protecting the network immediately
○ Needs to maintain state information
○ restriction of these signature-based approaches is that they can only detect the intrusions whose attack patterns are already stored in the database
Other detection mechanisms
• Traffic rate monitoring
• Protocol state tracking
• IP packet re-assembly</td></tr>
<tr><td>Command Console</td><td>• Provides a graphical user interface to an IDS - Enables administrators to receive and analyze alert messages and message log files
• should run on a computer dedicated solely to an IDS
• Maximize the speed of response
• Isolate the IDS from attacks</td></tr>
<tr><td>Response System</td><td>• IDS can be setup to take some countermeasures
• Response systems do not substitute administrators
• Administrators can use their judgement to detect a false positive or false negative</td></tr>
<tr><td>Database of Attack Signature and Behaviors</td><td>• IDS don’t have the capability to use judgement

• Signature or rule based
• Reference a database of known attack signatures
• If traffic matches a signature, it sends an alert
• Keep database updated
• Passive detection mode</td></tr>
</table>
</td></tr>
</table>

	• Anomaly based IDS • Store information about users in database
Architecture	<< See PDF >>

IDS Implementation

Install the IDS database	• IDS uses the database to compare traffic detected by sensors • Anomaly based systems • Requires a training period (normally one week) • IDS observes traffic and compiles a network baseline • Signature based system • Can use database immediately • Database can be sourced from third party suppliers
Gather Data	• Network sensors gather data by reading packets • Sensors need to be positioned where they can capture all packets • Host : capture information that enters and leaves a host • Network : read packets as they pass through the network segment
Send Alert Messages	• Sensor captures a packets • IDS software compares captured packet with information in its database • IDS sends alert message • If captured packet matches an attack signature • Deviates from normal network behavior
IDS responds	• Command console receives alert messages - notifies Admins • IDS can be configured to take action when a suspicious packet is received, such as • Send an alarm message • Drop packet • Stop and restart network
Admin assess the damage/risk	• Administrator monitors alerts • Administrator needs to fine tune the database - To avoid false negative
Follow escalation process	• Set of actions to be followed is IDS detects a true positive • spelled out in organization's security policy • Incident levels • Level 1: can be managed quickly • Level 2: represents a more serious threat • Level 3: represents the highest degree of threat
Log & Review event	• IDS events are stored in log files or database • Administrator should review logs • IDS should also provide accountability

Types

NIDS : Network Based IDS
HIDS : Host Based IDS

HIDS	NIDS
• HIDS only notices anything wrong once a file or a setting on a device has already changed • The activity of HIDS is not as aggressive as that of NIDS and can be fulfilled by a lightweight daemon on the computer with very small load on host CPU • Neither NIDS nor HIDS generate extra network traffic	A NIDS gives a lot more monitoring power than a HIDS as it can intercept attacks as they happen • NIDS is usually installed on a stand-alone piece of equipment and doesn't drag down the server processors • Neither NIDS nor HIDS generate extra network traffic •

Table 1: Evaluation of HIDS and NIDS.

NIDS	HIDS
Well for sensing attacks from outside	Well for sensing attacks from inside that NIDS cannot examine
Examines packet headers & entire packet	Does not understand packet headers
Host independent	Host dependent
Bandwidth in need of	Bandwidth free
Slow down the networks that have IDS clients installed	Slow down the hosts that have IDS clients installed
Senses network attacks, as payload is analyzed	Senses local attacks before they hit the network
Not reasonable for encoded and switches arrange	Well-suited for scrambled and switches organize
Does not perform ordinarily discovery of complex attacks	Powerful for examining a conceivable attack in view of pertinent data in database
High false positive rate	Low false positive rate
Examples: Snort [16], Cisco Guard XT [15]	OSSEC[19], Samhain [20], Osiris[21],&eEyeRetina[22]

IDS	Advantages	Disadvantages
HIDS	▪ HIDS can analyze encrypted data and communications activity. ▪ HIDS telling us if an attack is successful or no. ▪ Easy to deploy because it does not require additional hardware, therefore, it does not affect the current architecture.	▪ HIDS breakdown if the OS break down by the attack. ▪ HIDS are not able to detect network scans or DOS attack. ▪ HIDS tend to be resource intensive.
NIDS	▪ Operating Environment Independent, therefore NIDS will not affect the performances of hosts.	▪ Does not indicate whether the attack was successful or no. ▪ Cannot Analyze Encrypted Traffic

IDS	Advantages	Disadvantages
HIDS	▪ HIDS can analyze encrypted data and communications activity. ▪ HIDS telling us if an attack is successful or no. ▪ Easy to deploy because it does not require additional hardware, therefore, it does not affect the current architecture.	▪ HIDS breakdown if the OS break down by the attack. ▪ HIDS are not able to detect network scans or DOS attack. ▪ HIDS tend to be resource intensive.
NIDS	▪ Operating Environment Independent, therefore NIDS will not affect the performances of hosts.	▪ Does not indicate whether the attack was successful or no. ▪ Cannot Analyze Encrypted Traffic. ▪ NIDS is has very limited visibility inside the host machine.
MIDS	▪ More flexible. ▪ More Efficient. ▪ MIDS take advantage of the strengths of the combined type.	▪ High overhead load on the monitored system depending on the combined methodologies. ▪ Processor utilization of the hybrid agent is much great.
WIDS	▪ More accurate. ▪ It can manage wireless protocol activity.	▪ Sensors has limited computational resource and limited energy [16].

Strengths:
- Can detect ever growing number of attacks
- New signatures can be configured
- Have become cheaper and easy to operate
- Can operate in stealth mode to avoid attackers

Limitations:
- Requires strong defense else attacker can render an IDS ineffective
- Attackers tend to gain insight into IDS working over a period of time
- Poor sensitivity could limit accuracy
- Someone needs to monitor IDS reports for actions

PARAMETER	FIREWALL	IPS	IDS
Abbreviation for	-	Intrusion Prevention System	Intrusion Detection System
Philosophy	Firewall is a network security device that filters incoming and outgoing network traffic based on predetermined rules	IPS is a device that inspects traffic, detects it, classifies and then proactively stops malicious traffic from attack.	An intrusion detection system (IDS) is a device or software application that monitors a traffic for malicious activity or policy violations and sends alert on detection.
Principle of working	Filters traffic based on IP address and port numbers	inspects real time traffic and looks for traffic patterns or signatures of attack and then prevents the attacks on detection	Detects real time traffic and looks for traffic patterns or signatures of attack and them generates alerts
Configuration mode	Layer 3 mode or transparent mode	Inline mode , generally being in layer 2	Inline or as end host (via span) for monitoring and detection
Placement	Inline at the Perimeter of Network	Inline generally after Firewall	Non-Inline through port span (or via tap)
Traffic patterns	Not analyzed	Analyzed	Analyzed
Placement wrt each other	Should be 1st Line of defense	Should be placed after the Firewall device in network	Should be placed after firewall
Action on unauthorized traffic detection	Block the traffic	Preventing the traffic on Detection of anomaly	Alerts/alarms on detection of anomaly
Related terminologies	• Stateful packet filtering • permits and blocks traffic by port/protocol rules	• Anomaly based detection • Signature detection • Zero day attacks • Blocking the attack	• Anomaly based detection • Signature detection • Zero day attacks • Monitoring • Alarm
			https://ipwithease.com

Wannacry

01 May 2021 06:45

How to protect against WannaCry Ransomware:

- Install the Windows security update for MS17-010 on all systems on the network. Microsoft made the same available for systems that are no longer supported, such as Windows XP.
- Disable version 1 of SMB (SMBv1) in the Windows domain or on all Windows systems on the network.
- Do not block the domain www[.]luqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com. Unlike normal, this domain prevents the worm from being activated and the malware expects to receive a valid response from it so that it does not propagate to other systems on the local network or on the Internet.
- Because the domain is now operated by researchers and not by criminals, you can let traffic from infected systems to it pass through your network.
- If this is not an option, create a DNS zone for this domain and point it to an internal webserver that can return a valid HTTP response. This option should also be followed by those who have a non-transparent proxy on the network, since the malware does not work well through proxies and as such will never receive a valid response.
- If you have systems already infected, do not pay the ransom, do not be part of the 0.0001% that is paying the criminals.