OSI Model

- OSI = Open System interconnect
- 7 layers

• Application	7 Service protocols
• Presentation	6 Data formats
• Session	5 Authentication/crypto
• Transport	4 ports, logical service 2 service, TCP
• Data	3 Network to Network (PPTP)
• Network	2 Host to Host links
• physical	1 Media

CIA

- Confidentiality, integrated, Availability
- Confidentiality:-
  Keeping data from being exposed to those that should not have access to it
- Integrity:-
  Keeping data from being modified tampered with or deleted by those whom should not have access to it
- Availability:-
  Keeping data available for those system or people that should have access to it
- SLA – Service Level Agreement

Permission

- Sign a formal contract and NDA - Non-disclosure agreement.
- Information gathering
- (which hosts are in play and which are not purpose of test, etc...)
- perform the assessment
- participate in remediation requests
- Turn over deliverable
- Store and or destroy data.

Angry IP

- very fast IP address port scanner
- cross platform
- lightweight

IKE Scan

- IKE-Scan is a command-line tool that uses the IKE protocol to discover, fingerprint and test IPsec VPN Server.

ARP Scan

- arp-scan Sends ARP packets to hosts on the local network and displays any responses that are received.

Traceroute (OT)

- Diagnostic tool for displaying the route (path) and measuring transit delays of packets.
- Sends a sequence of User datagram protocol (UDP) packet addressed to a destination host. The time-to-live (TTL) value, also known as hop limit, is used in determining intermediate routers being traversed towards destination.

Routers decrement TTL values of packets by one when routing and discard packets whose TTL value has reached zero, returning ICMP error message ICMP time exceeded.

The exam has questions about types and codes in ICMP

What is the code for a 'Destination Network Unreachable' ICMP message?

Spoofing

- In the context of network security, spoofing is a situation in which one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage.
- e.g. I pretend to be another person and send an email with their email address, trying to get them to open an attachment.
- e.g. I send packacts on a network using another computer network address, instead of my own.
- e.g. I use a VPN tunnel to present my IP address as 74.32.25.33 (A US Based IP) versus my real Combodian IP address of 204.21.33.56
- Spoofing does not necessarily constitute attack.

1-1 Jacking

- To take control of a system, device (IoT) that someone else is controlling.
- can be done to computer, application, drone TV thermostat, accounts, domain name, webmail account, SaaS accounts, etc ---

DNS (domain Name Service) (1)

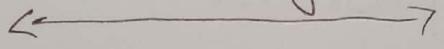
- Translate somedomain.com to an IPv4 or v6
- Typically interrogated early on in a security assessment when enumerating.
- large attack surface / highly sought after
- Attack surface : domain Transfer, zone - transfer, zone poisoning, cache poisoning, reflection Dos, Dos, information leak (internal DNS info).

DNS (Domain Name Service) (2)

- Domain Transfers hijacking of domain
- Zone Transfers process of copying from primary DNS server to secondary DNS server. If a hacker is able to successfull do this they may result in an information leak. DNS record often contain sensitive information

```
nslookup; ls -d example.com
dig @ns1.exam.dom AXFR
host -t AXFR exp.dom ns1.exam.dom
```

- Zone poisoning — Breach primary server and alter the zone file to corrupt the domain
- cache poisoning — send false answer to cache server until store them. If the records are pointed to a server under your control, this is called DNS pharming.



DNS (domain Name Servie) (3)

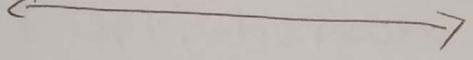
- Reflection DoS — Involves spoofing source address to that of the target from multiple other server. In case of reflected DoS, sourcing machine do not need to be compromised.

DNS (Domain Name Service) (4)

- DoS - classic attack, consume available connections on the server (Rinse, wash, Repeat)
- Information leak (internal DNS info) -

In the event the DNS record contain internal server name and IP addresses, the attacker may be able to obtain knowledge of LAN network without ever touching network. longer you can drag out time hacker is on the network the more likely they will be discovered -

- Attacking SOA record results in DoS
- A common SOA vulnerability is XML DoS
- SOA = Service Oriented Architecture -



DNS (Domain Name Service) (5)

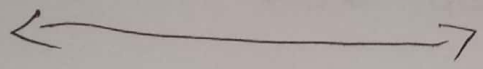
- Fields in the SOA record: (Time in seconds)
- 1882919 7200 3600 14400 2400
- serial, refresh, retry, expiry - TTL
- Zone files contain: SOA, NS, A and MX record

@ In SOA nameserver.place.dom - postmaster.p.dom

```
1
3600    ;  serial number
600     ;  refresh   [1h]
86400   ;  retry     [10m]
3600    ;  expire    [1d]
        ;  min TTL   [1h]
```

DNS (Domain Name Service) (6)

"A" Records IPv4 mapping of hostname to IP addresses of hosts - also used for DNSBL "AAAA" Records IPv6 mapping of hostnames to IP addresses of hosts



Split Horizon

- A route advertisement method of preventing routing loop in distance-vector routing protocols by prohibiting a route from advertising a route back onto the interface from which it was learned.
- Split-horizon routing with poison reverse is a variant of split-horizon route advertising in which a router actively advertises routes as unreachable over interface over which they were learned by setting route metric to infinite (16 for RIP)

CIDR Notation

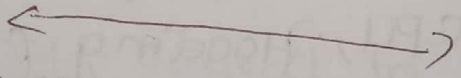
- Classless inter-domain Routing
- class A subnet: 4,294,967,296 addresses
- class B subnet: 16,777,216 addresses
- class C subnet: 256 addresses

- A.B.C/32 = 1 IP Add of 256
- A.B.C.D/31 = 2 IP Add of 256
- A.B.C.0/24 = 256 IP Add
- A.B.0.0/16 = 65,536 IP Add
- A.0.0.0/8 = 16,777,216 IP Add

- http://en.wikipedia.org/wiki/classless_inter-domain_routing
- Subnet calculators can help with understanding this notation -

Regional Internet Registries & Terminology

- Regional internet Registries (RIRs)
- local internet Registries (LIRs)
- Asia-pacific Network information centre (APNIC)
- Roseau IP Europeans Network coodination center (RIPE NCC)
- Latin America and caribbean N/w information centre (LACNIC
- American Registry for internet numbers (ARIN)
- African Network information center (AFRINIC)



ARP (address Resolution protocol)

- Translate an IP address into a MAC address and vice versa.
- Switches and routers use Mac (media access control) addresses
- Stateless protocol, Therefore subjectable to MiTM attac

MAC Address (Media Access Controller)

- Example: 00:00:0C:01:25:21 (7 octets)
- How can manufacturer be determined?
  the first six character (octets) describe the manufacture.
- Vendor lookup sites are plentiful:
  http://www.macvendorlookup.com/
- A flood of MAC addresses sent to a smart switch will turn it into a hub when memory buffer are overrun.

MAC Address (media Access Controller)

CISCO set of MAC address, examples.

IPv4 Addressing:

- IPv4 exhausting occured in Aug 2015
- IVP4 address looks like: 204.35.22.A5
- Non routable addressing (private networks):

IPv6 Addressing

- Theoritically speaking, can never be exhausted
- many security issues are being discovered
- NOOb network engineers will see IPv6 first day on job.
- Be sure to understand its strenght and weaknesses.
- Non routable IVPs addresses (private Network):

prefix/L	Global ID	Subnet ID	N. interface add subnet
Fd	XX:XXXX:XXXX	YYYY	18,446,744,073,709,551,616
48 bit		16 bits	64 bits

- Stateless Address Auto Configuration (SLAAC) - auto address config via neigbhor discovery protocol
- zero may be omitted in address notation

24:42:55:55 ::::02 == 24:42:55:55:00:00:00:02

Social Engineering

- Tricking someone into providing information they would never otherwise provide.
- Fake emails that appear to be from your supervisor / boss / manager
- "Hi I am from your bank - I need your a/c info"
- 'Hi, I am from SEC - I need access to your computer immediately" (position of authority)
- Simple getting someone to do something they would otherwise not do.
- useful in determining which user need end-user training
- Spam mitigation: stop email from reaching end user.

Dumpster Diving

- when someone literally dives into a dumpster of a target and start digging in trash.
- mitigation technique — crosscut shredders shredding service, recurring security awareness training.

Interrupts :

- System interrupts are access request for process or time-

- The processor will respond to IRQs (Interrupt Request) before processing anything else.

- These are utilized by rogue code and things key loggers to perform their work-

DHCP (Dynamic host control protocal)

- Answer request for devices requiring and IP address on the LAN
- Configured to use specific address ranges
- Can be configured to give same MAC address same IP address every time-
- Can be configured to rotate IP Addresses at specific rates
- Ie: roll IP every hour day/ week, etc —

Wireshark

- Formerly called : Ethereal
- protocol Analyzer _ Not a packet sniffer
- limitation : dependent on what protocols it 'knowns' and what packet sniffer, that are packaged with it, feed it
- Insufficient for analyzing anything other than what it know about remember its protocol analyzer.
- Filter to display packets with TCP SYN, PSH and RST flags set:

(tcp.flags.syn == 1) || (tcp.push == 1) || (tcp.flags.reset == 1)

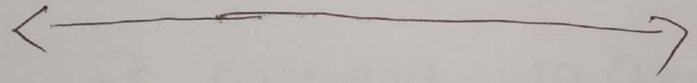
- How to capture all TCP traffic going to or from ~~to~~ 192.168.0.125 on port 25?

tcp.port == 25 and ip.host == 192.168.0.125

- ESSID (extend service set identifier)

Smurf Attack

- DDOS (distributed denial of service) Attack
- Large number so ICMP packets with the intended victims spoofed source address are broadcast to a network using an IP broadcast address. Most devices will respond by sending a reply to the source IP address. if enough machine respond a DDOS is the result.
- Old attack, many basic security devices will protect against this attack.
- may still work on IoT and industrial environment.
- In 1999 routers and switches are pre configured NOT to forward those types of packets.
- Smurf amplification networks exists today.
- mitigated by disallowing ping on a router.



Fraggle Attack

- DoS attack that sends a large amount of spoofed UDP traffic to a routers broadcast address within a network
- Mitigated by disabling 'broadcast' on switches and routers.
- Results in amplication of responses and thus DoS as the machine will slow to a crawl for anyone trying to use it.
- old attack, many basic security devices will protect against this attack.
- may still work on IoT and industrial environment.

Teardrop Attack

- Sending of mangled IP fragments with overlapping, oversized payloads to the target device.
- can crash older stack implementation
- Affects: win 95, 3.1, NT, linux 2.0, 2.1 kernal, older devices that are connected to the internet.

Ping of Death Attack

- Comprised of sending a malformed ping to host.
- Any IPv4 packet may be as large 56,535 Bytes.
- A malformed POD packet is larger than 56,535 bytes
- cause a buffer overflow than reassembled on other end of the connection.
- may facilitate injection of malicious code
- old attack, many basic security devices will protect against this attack
- may still work on IoT and industrial environment
- To protect against this attack, sum of 'segment offset' and 'Total lenght' field in the IP header of each IP fragment is smaller than 65,535. If sum is larger, packet is invalid.
- many fire walls will perform this check.

PING Commands

- what ping command lets a tester enumerate live system in a class c network via ICMP using native windows tools?

```
for /L %V in (1 1 254) do PING -n 1 192.168.2.%V
| FIND /I "Reply"
```

- How can ping be used to fingerprint a web server?

```
telnet webserver Address 80 HEAD / HTTP/1.0
```

BURP proxy

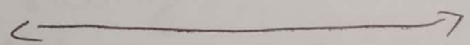
- https://portswigger.net/burp/proxy.html
- Security Assessment Tool (software testing as well)
- Great Free version
  - proxy (intercept and passive at press of button)
  - spider (scour site for hidden file/directories
  - Repeater
  - Sequencer (evaluate a sites ability to handle subtle sequencing attacks)
  - Decoder (attempt to decode what it can various decod
  - comparer (compare result with previous result)

HPING

- hping is a command-line oriented TCP/IP packet assembler/analyzer. hping isnt only able to send ICMP echo requests. it support TCP, UDP, ICMP and RAW-IP protocols has a traceroute mode, the ability to send files between a covered channel and many other features
- Can be used for rule validation as well as attacking,
- Works on windows and *nix

Hping 2

- Same as hping but has more option associated with it.
- hping tools are used to scan:
  - Firewall Testing
  - Advanced port scanning
  - Network testing, using different protocols, TOS, fragmentation
  - manual path MTU discovery
  - Advanced traceroute, under all the supported protocols.
  - Remote OS fingerprint.
  - Remote uptime guessing.
  - TCP/IP stack auditing.
  - hping can be also useful student that are learning TCP/IP



Hping 3

- Even more options associated with this version
- Adds ability for CLI (command line inter
  scripting via TCL, and other switched options.

Cross Site Scripting 1

- A type of vulnerability typically found in web applications.
- Requires HttpOnly flag be set (for test only)
- Abbreviated XSS
- Enables attackers to inject client-side script into web pages viewed by other users.
- may be used by attacker to bypass access control such as same-origin policy.
- In its most basic form

IMG SRC = vbscript:msgbox("vulnerable"); > originalAttribute = "SRC" originalPath = "vbscript:msgbox("vulnerable");>"

CSRF (Cross Site Request Forgery) 1

- Also known as:
  - A one-click attack
  - Session riding
  - Abbrevicated as CSRF (sometimes pronounced sea-surf) or XSRF
- An attack that forces an end user to execute unwanted action on a web application in which they are currently authenticated
- Targets state-changing request, not theft or data, Since the attacker has no way to see response to forget request.

Cross site Request Forgery

- With little help of social engineering (such as - sending links via email or chat), an attaker may trick users of a web application into executing action of attackers choosing. If victim is normal user.
- If victim is an administrative account, CSRF can compromise entire web application.

Cross site Request Forgery 2

- mitigated with special libraries
- OWASP has a CSRF protector project consisting of 2 parts: Apache module, PHP library.
- mitigation is test. howev Real life.

Netcat 1

- Considered malware by most AV vendors
- often abbreviated by nc
- facilitated reading and writing to network connection using TCP or UDP
- was not created to be a 'hacking' tool but is used one quite often.
- can perform port scanning, transferring and port listening and can be used as a backdoor.

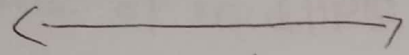
Netcat 2

- open a raw connection on port 25
  nc. mail.server.net 25
- listen on 2222 and output anything rxed to a remote connection on 10.1.0.43 port 1234
  nc-l-p 2222 | nc 10.1.0.43 <1234
- very powerful, hence its use as hacking tool
- https://nmap.org/ncat/
- Scan UDP 0-1024 with:

  Netcat -u -v -w2 <host> 1.1024

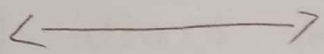
Firesheep

- Firefox extension that uses a packet Sniffer to intercept unencrypted cookie from websites, such as FB, Twitter.
- Facilitates discovery of identities and displays them in Sidebar.
- Allows attacker to take over identity of those persons in Sidebar.



N-Tier Architecture

- A term describing multi-level architecture systems
- include security in depth architecture for example, FW on perimeter (WAN/Egress point) and restrictive FW in font of database inside of LAN, etc.—
- Group of server each with a unique role



Certificate and public key pinning

- public key pinning involves one extra step over the normal x509 process
- The extra step is to take a hash of the certificate and compare it against a list of known hashes of certificates.
- prevent being duped by forged, stolen certificates, etc—
- used in hardened environments.

Nikto Web Scanner

- Open Source (GPL) web server vulnerability Scanner,
- looks for over 6700 potentially dangerous files
- Checks for outdated version of over 1250 Server.
- version specific problems
- it also checks for server configuration item such as presence of multiple index files, HTTP Server option, and will attempt to identify installed web Server and software.
- Scan item and plugins are frequently updated and can be automatically updated

BT Crack

- Blue tooth pass phrase (PIN) brute force
- The link-key allows remote connection without victim noticing.
- Link-key allow and attacker to connect to device in non-pairing mode non discoverable mode.
- The link-key allows decryption of data.

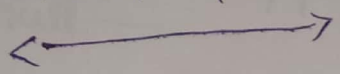
Havij

- SQL injection tool (Automatic)

LAN Attack mitigation

- Know your architectures (vectors of attack)
- How to stop inside attacker (rogue)
  - NAC (Network Admission control)
  - 802.1x port based Authentication
  - port security

These mitigations protect against an outsider physically connecting to network from inside.



Nslookup

- Tool used to query DNS lookups
- Stand for Name service lookups
- READ the main page for this one!
- Nslookup set type=ns pk.com

SQL Injection

- method of manipulating a database into leaking information
- Valid Query:
  - SELECT * FROM products WHERE id_product='25';
  - Delete from products;
  - Drop tables from products;
- Attack Example, URL:
  http://www.example.com/product.php?id=10 UNION SELECT 1, null, null —
- Attack Example, un-sanitized inputs:
  anyusername or 1=1' anypassword
- Injection string start with an apostrophe

MS SQL

- Microsoft SQL
- XP_cmdshell feature, allows issuing commands from SQL server to OS.

SQL (structured Query language):

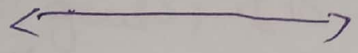
- Many Flavors of SQL
  - MS SQL
  - MySQL
  - postgresql
  - Transact-SQL
  - Oracle (PL-SQL)
  - persistent stored modulus (PL-PSM)
  - SPL (stored procedural language)
  - SQL/PSM (ANSI/ISO standard)
- Special programming language designed for managind data held in RDMS (Relational database management system)

SQL (structured Query language) :

- Attacked with SQL injection
  - Normal SQL injections: Throwing (firing queries at a server and looking for errors immediately returned
  - Blind SQL injections: Throwing queries into a field and looking for observed behavior elsewhere (like attempting to login it query created account).
- Automation Tools
  - SQL injectors (like MOLE
  - SQL injector (automates SQL injection)

Wardialing

- A technique of using a modem to automatically scan a list of telephone numbers.
- could include dialing EVERY number in an area code
- Toneloc (Tool)
- This is product to do when conducting a security assessment because many companies have dial up modems and may be unaware they are still connected to internet.

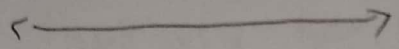


Windows

- XP is totally obsolete and riddled with vulnerabilities
- Exploit DB exploits need to be compiled, but ones for xp with metasploit.
- it is imperative to know a modern windows OS when learning security.
- The skills are required for labs.
- http://www.oldversion.com/ Repository of old version of All kinds of software. this can be useful in finding vulnerable target for practice.

Linux

- it is imperative to know a modern linux OS
- The skills are required for performing labs
- know different flavors or distribution (distros)



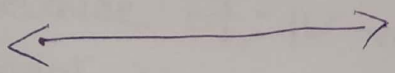
OS X

- OS X is built on BSD Linux
- OSX is not imperative to know, but if skills with malware, vulnerabilities and security assessment are goals, it is imperative to know them all. OS X can be downloaded free and run as a VM.
- When performing assessment know your weakness. it is better to call in an expert with OS X skills if you do not posses them.

Access Control List (ACLs)

- List of permission attached to an object.
- Specify which users or system process are granted access to object as well as what operation are allowed on given objects.
- each rule typically specifies a ~~bo~~ subject and an operation.
- e.g/ permit 217.77.88.12.11.12.13.50 RDP 3389
  e.g/ permit 217.77.88.12.11.12.13.0/24 RDP 3389

This would allow RDP (remote desktop protocol) connection from the first IP to the second IP using specified protocol

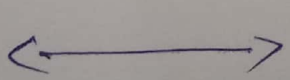


Kismet

- 802.11 layer2 wireless network dectector, sniffer and intrusion detection system.
- perform RAW wireless packet sniffing (rfmon, radio frequency monitoring)
- Can detect wireless network that do not beacon (broadcast their (SSID) by passing listening for traffic going to/from them. this is called 'decloaking'.
- WEP cracking within 60 seconds (require : mac of AP and ESSID to perform false authentication)
- Distributed remote sniffing with Kismet Drones.
- WEP is weak because of; IV range is too small no key management, flaws in implementation

WebGoat

- Created by OWASP
- A deliberately vulnerable web application maintained by OWASP designed to teach web application security lessons.



WebScarab

- WebScarab is a framework for analyzing application that communicate using HTTP and HTTPS protocols.

Binary Operations

- OR - OR operation. if you have a 1 or 1 then the result is a 1
- XOR - Exclusive OR. if you have a 1 xor 1 the the answer is 0. this operation results in a 1 only if one or the is a 1, not both, used in encryption.
- AND - if you have a 1 and 1 then result is a 1 else its 0.

Signs A system is Hacked

- increased amont of failed logon events
- pattern in time gaps in system and/or event logs.
- New user accounts created -

Wireless Network security 1

- 802.1x port Based Authentication (PNAC) - important EAP over LAN
- MAC Authentication bypass is not safe to implement. MAC addresses may be snifted off of the wire and reused, thus bypassing authentication.
- NAC (Network Access Control) - Security approach that attempts to combine user or system authentication, network security enforcemet and endpoint security (like AV, HIP, vulnerability assessment, disk encryption.

Wireless Network security 2

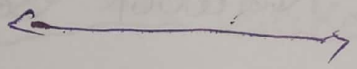
- 802.1x authentication involve three points -
  - Supplicat
  - Authenticator
  - Authentication server.

Wireless Network Security 3

- WPA2 uses AES 128 CCMP for encryption.

Wireless Network Security 4

- Packet structure:
  - Management – packets used to establish connectivity between hosts at layer two. Subtypes include: authentication, association and beacon packets.
  - Control – control packet allow for delivery of management and data packets and are concerned with congestion management. Subtype include: RTS and CTS
  - Data – These packets obtain actual data and are only packet type that can be forwarded from wireless network to wired network (sniffing concern here)



Wireless Network Security 5

- OFDM is a frequency-division multiplexing (FDM) scheme used as a digital multi-carrier modulation method. A large number of closely spaced orthogonal sub-carrier signals are used to carry data on several parallel data streams or channel.

1-Hardening

- Hardening is the process of methodically reducing the attack surface of an app. System, device, Thing, etc.
- Example /
  - Shutting down unused ports
  - Removing banners
  - Mitigating vulnerabilities
  - Etc —

IDS (Intrusion Detection System) :

- System that looks at network traffic (the wire) instead of host for malware signatures.
- SNORT is a popular OS IDS
- When a rule is matched, further evaluation until ALL rules are checked.
- Can be configured as:
  - Sniffer
  - packet logger
  - NIDS (Network intrusion detection system)

Metrics

- Taking and organizing data in such a way to show trending in event reporting.
- Trends go up, trends go down
- Can indicate:
  - problems are growing or shrinking
  - Effectiveness or ineffectiveness of tools

Responsible Reporting

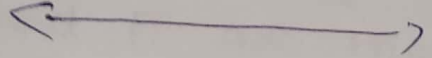
- when security assessors (pen testers) find issue on other sites or via research, they attempt- to report them to responsible party and give them time to remedy problem before publicly reporting issue-

SID Strategies (security in depth)

- ~~Secori~~ 'separation of Duties — it would not be prudent to give someone access to RFID card access, access to server room and access to logs on server-
- Assume network hacked and plan-accordingly-
- Dont solely depend egress point protection-

Firewalk

- **Firewalking**: is a technique that employs traceroute-like techniques to analyze IP packet response to determine gateway ACL filters and map networks.
- **Firewalk**: The tool employs technique to determine filters rules in place on packet forwarding device- (utilize tool for test)
- If a packet passes through the FW, A 'TTL — exceeded' will be returned versus 'no response'



Firewall

- Types:
  - packet Filtering — 1st Generation, look at network addresses and ports of packets and determine if that packet should be allowed or blocked
  - Application-layer — works on the application level of TCP/IP stack (OSI model)
  - Circuit-level gateway firewall / stateful — 2nd generation, perform 1st Gen work up to layer 4 (transport layer) of OSI model. records all connection passing through it and determine whether a packet is start, of new connection, part of an existing connection or not part of any connection (monitor TCP handshakes)

Ciphers 1

- Can be attacked by frequency ale analysis, pattern, words, chosen ciphertext attacks-
- If attacker is able to decrypt 'some' parts of a message, chosen ciphertext attacks are now possible
- Frequency Analysis – in English language, E, T, A and O are most common while Z, Q and X are rare.

likewise, Th, ER, ON and AN are most common pairs of letters (termed: bigrams or digraphs) and SS, EE, TT and FF are most common repeating letters. this is where it all starts-

Ciphers 2

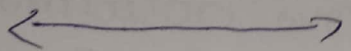
- Vigenere – using a series of Caesars Cipher, simple form of polyalphabetic substitution. See vigenere square. (key plaintext, ciphertext)
- Caesars Cipher – known as shift cipher, substitution cipher in which each letter in plaintext is replaced by a letter some fixed number of position down alphabet. e.g/ with left shift of 3 would mean 'D' would replaced by 'A'. if you rotate 26 letters, you end up with original message (OT)

plaintext: The Quick brown fox jumps over the

ciphertext: QEB NRF ZH YOLTK

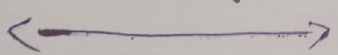
Data Center Humidity

- If the humidity gets above 45-50% RH the electronics can short out or corrodo.
- If humidity gets below 45-50% RH static electricity can destroy components.



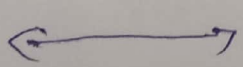
Binary To Text Encoding

- Represent binary data in ASCII format
- Base64 is most popular today in malware.
- most rogue emails are base64 encoded.
- online decoders/encoders.
  https://www.base64decode.org/
- MIME encoding, used for email attachments
- common use is to fool security analysis tools and for sending data over wide sec-



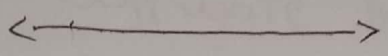
Substitution

- Encryption method where one character is replaced with another.



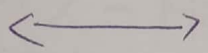
Encryption DPI (deep packet inspection)

- Formerly known as SSL inspection, SSL, DPI, etc
- Can be utilized as a covert channel, A covert channel is method used to defeat multi-level security solution to leak data.
- Transfers information over, within a computer system, or network that is outside of the security policy.



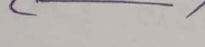
SOAP (simple object Access protocol)

- A messaging protocol that allows program that run on disparate operating system (such as windows and linux) to communicate using Hypertext Transfer protocol (HTTP) and its extensible markup language (XML)



Telephone Knowledge

- POTS (plain Old Telephone Service)- Basic wire line telecommunication connection.
- PBX (private branch Exchange)- switches calls between enterprise users on local lines while allowing others to share the certain number of external phone lines.
- Asterisk: A software implementation of a PBX
- PSTN (public Switched Telephone Network)- is worlds collection of interconnect voice-oriented public telephone networks, both commercial and government owned, also referred to POTS.
- VoIP (voice Over IP) - Allows calls to be complete using broadband instead of PSTN (100% of calls today are turned into VoIP at Switch-



Policies

- Acceptable-use policy (AUP)- set of rules that describe ways in which network, site or System may be used and sets guides as to how it should be used
- Remote-Access policy - a document which outlines and defines acceptable method of remotely connecting internal network-
  - Dial-in
  - SLIP/PPP (serial Line IP, point to point protocol)
  - ISDN
  - Telnet access from internet
  - cable modem
- permissive policy - A policy in which majority of internet traffic is accepted, versus restrictive.
- CM (configuration management) ensures that policies are made in controlled and documented fashion.
- Employers protect assets with security policies pertaining to employee surveillance activities by providing clear boundaries of monitoring activities and consequences.

SSL is History

- SSL = Secure Socket layer
- SSL version: SSLv2.0, SSLv3.0
- SSL is insecure and should not be used on ANY ports. most engineer will catch it use on port 443, but they almost always miss it on mail ports. (pops, SMTP, etc) and other ports using encryption protocols (database, industrial system, IoTs devices, etc)
- SSL replaced by TLS (transport layer sec)
- PCI (payment card industry) requires SSL not be used for securing transfers or system processing PCI data-
- CA (certificate Authorities)

TLS Encryption

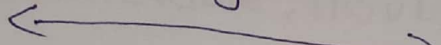
- TLS = Transport layer security
- version: TLSv1.0, TLSv1.1, 1.2, 1.3 (Draft)
- only allowable version in PCIv3.6 and hardened environments in TLSv1.2
- TLS is a cipher suite or a suite of cipher modes
- preventative control

Attack against TLS

- Renegotiation
- version rollback
- Beast
- crime
- POODLE
- RC4
- Truncation
- FREAK and logjam bug
- Heartbleed
- lucky13

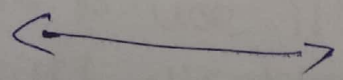
Renegotiation Attack

- Requires access to the HTTPS connection (MiTM)
- Attacker splice in own request into the beginning of conversation client has with server
- Allows decrypting of client-server communicatio
- mitigation
  - disable renegotiation



Version Rollback Attack

- Allowed modification to cipher suite list sent by client to server (an attacker may succeed in influencing cipher suite selection in an attempt to downgrade cipher suite strength, to use either weaker Symmetric encryption algorithm or a weaker key exchange
- Allow attack to recover encryption keys offline and to access encrypted data -
- mitigation
  - remove weak cipher suites from server configuration
  - periodically revisit cipher suit supported by server.



BEAST Attack

- BEAST = Browser Exploit Against SSL/TLS
- MiTM attacks
- Attacker must be able to snoop on the traffic and capture at least two consecutive cipher text blocks.
- Exploit weak ciphereos.
- TLSv1.0 is vulnerable, TLSv1.1, 1.2 and 1.3 are not yet
- As distributed computing power becomes more and more affordable encryption standards will be periodically revisited.
- RC4 is immune BUT RC4 has other issues, thus using RC4 for mitigating choosing lesser of two evils.

Crime/Breach ⟷ Attack

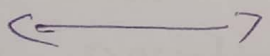
- Can allow an attacker to recover content of web cookies when data compression is used along with TLS via session hijacking.
- Allow attacker to perform session hijacking on an authenticated web session
- MiTM attacker
- mitigation is to use TLSv1.1, 2, 3 and disabling v1.0 be aware! disabling TLSv1.0 will likely cause outage to customer if a company server devices a wide audience and array of

POODLE Attack

- padding oracle on downgraded legacy encryption
- CVE-2014-3566
- SSLv2.0, 3.0, TLS 1.0 are all susceptible
- If successful, all of traffic could be decrypted
- MiTM
- mitigation is done by using TLS 1.1, TLSv1.2, TLS v1.3 and disabling TLSv1.0

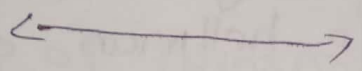
RC4 Attack

- RC4 is susceptible to many different attacks and is known for being weak to even basic cryptanalysis.
- used is SSLv2.0, 3.0 and TLSv1.0
- mitigation is done by using TLSv1.1, 1.2, 1.3 and disabling TLSv1.0



Truncation Attack

- A TLS truncation attack blocks a victims account logout requests so that user unknowingly remains logged into a web service.
- when request to sign out is sent, attacker injects an unencrypted TCP FIN message to close connection.
- The server therefore doesn't receive logout request and is unaware abnormal termination
- Browser user thinks communication has stopped
- Session on server remains open
- MITM



FREAK and logjam Attack

- Downgrade Attack can force servers and clients to negotiate a connection using cryptographically weak keys.
- MiTM
- FREAK tricks server into negotiating a TLS connection using cryptographically weak 512 bit encryption keys.

Heartbleed Bug Attack

- This vulnerability facilitates theft of private keys from server that should normally be protected, Allows anyone on internet to read memory of systems protected by vulnerable version of OpenSSL software -
- OpenSSL version 1.0.1 to 1.0.1f are affected
- Caused by a buffer over-read bug in OpenSSL rather than detect in SSL or TLS
- Not a MiTM attack, but stolen information can be used to perform MiTM attack -

Lucky13 Attack

- A cryptographic timing attack against implementation of Transport layer security (TLS) protocol
- MiTM
- Not a danger to ordinary user of TLS
- Attempt access against Cookies protected by TLS (Security in depth strategy here would prevent a breach from one layer protection)
- extremely complex timing attack against protocols.
- leverage BEAST and Same origin policy
- mitigation is incorporation of GCM cipher.

Cryptographic MAC

In cryptography a message authentication code (MAC) is a short piece of information used to authenticate a message, in other words, to provide integrity and authenticity assurance on message, integrity assurance detect accidental and intentional message changes. while authenticity assurance - affirm message origin

~~integrity assurance detect~~

Also called - keyed hash function -

Encryption Analysis

- https://www.ssllabs.com (Free)

Encryption 1

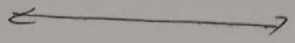
- performed by xoring bytes repeatedly
- XOR = Exclusive OR
- output is 1 only if both input to system are same
- XOR operation is primary algorithms used in stream ciphers
- weaknesses in xoring - if key is smaller than data, successful cryptanalysis via frequency attack is possible,

Encryption 2

- symmetric - FAST! same key used to encrypt that is used to decrept,
  DES (Data Encryption Standard), AES (- Advanced Encryption Standard)
- RC = Rivest cipher
- RC4 = stream cipher (40-2048 Bit key size) Can it's way out!)
- RC5 = Block cipher (Block size support 32, 64 / 128 bit
- RC6 = Block cipher (Block size support of 128, 192 256 bits.
- Asymmetric - Requires large encryption keys, different keys can be used to encrypt and to decrypt,
  PKI (public key infrastructure) DH (Diffie-hellman), DSA

Steam versus block Encryption

- Steam Encryption - encrypts byte by byte
- Block Encryption - encrypts blocks of byte at a time.



Example Question

- For message sent through an insecure channel, properly implemented digital signature gives receiver reason to believe message was sent by claimed sender.

while using digital signature, message digest is encrypted with which key?

- Sender's private key

Symmetric Ciphers

- AES
- Blowfish
- DES
- 3DES (Triple DES)
- Serpent
- Twofish
- Camellia
- CAST-128
- IDEA

- RC2
- RC5
- SEED
- ARIA
- Skipjack
- TEA
- xTEA

Assymmetric ciphers

- DH
- DSA (digital Signature Algorithm)
- ECDH
- ECDSA
- EdDSA
- EKE

Features

- Used in Public Key Cryptography
- used to build Key infrastructure (PKI)
- Based on elliptic Curve cryptography

DH-1

- DH Group 1: 768-bits group
- DH Group 2: 1024-bit group
- DH Group 5: 1536-bit group
- DH Group 14: 2048-bit group
- DH Group 15: 3072-bit group
- DH Group 19: 256-bit elliptic curve group
- DH Group 20: 384-bit elliptic curve group-

Backups

- verification!
- The only way to know for sure data is valid is to perform an entire restore -

Encryption (3)

- PGP - pretty Good privacy (windows, *nix)
- GPG - GNU privacy Guard (OSX, *nix)
- Enigmail plugin (Thunderbird)
  - support every OS
  - very popular
  - has been around a long time
- http://www.mailvelope.com/
  - Support FF and Chrome.
- PGP and GPG use Asymmetric cryptography

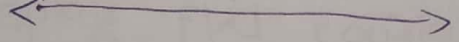
PKI (public key infrastructure) 1

- A set of hardware, software, people, policies and procedure needed to create, manage, distribute, use, revoke and store digital certificates and manage public key encryption.

Requires:

- Generating key pairs (public key / private key)
- Initial key exchange (sending other pub key)
- Encryption of a message with receiver public key
- Receiver uses private key he has and decrypt msg.

- Key Escrow – used to securely store private keys.
- key management Server – Facilites revoking keys and storing them.
- public key server – used to store publicly available keys, search by email address.
- utilizes port 500
- IKE – initial key exchange
- used in IPSEC

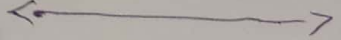


PKI (public key Infrastructure) 2

- RA – Registration Authority, responsible for verifying applicant.
- CA – Certificate Authority, responsible for managing unique IDs (issuing and revocation and answering verification requests.
- pKI uses RSA 1024 bit keys (Not IRL)
- IRL key lengths are configurable.

IRC (Internet Relay Chat):

- An application layer protocol that facilites communication in form of text.
- Chat process works on a client/server networking model.
- Can also be used in P2P fashion via direct messaging.
- May act als a control interface for botnets.
- IRC usage
- Investigate IRC usage on your network.



Netsh

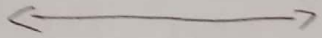
- Network shell
- Windows (95, vista, 98, NT)
- Command line utility for older version of windows, allow local or remote configuration of network devices.
- May display FW config.
- netsh firewall show config.

Power Shell

- Task automation and configuration management framework for windows (modern)
- Several test questions on power shell in q
- Be sure to do a lab or tutorial on power shell.
- Command to display running services: sc query.

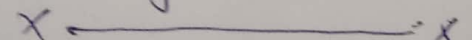
Localhost

- IP address of: 127.0.0.1 (home, myself)



Dual homed

- A term describing network device that has two network cards.
- Common on IDS/IPS
- For Test: Required for proper function on IPS/IDS
- optional
  - configured in such a way that traffic traverses one interface to other.
  - The traffic may be modified or analyzed during flight.



Back Door

- method of bypassing normal authentication
- Back orifice - Tool for providing back doors. uses port 31337 (hacker spelling of elite)
- Trap Door - Sometime used instead of back door, back door proper term.

VIRI 1

- Polymorphic – Mutates over time or after every execution, changing code used to deliver its payload and enabling to hide from signature matching (marburg, tuareg, satan bug)
- Multipartite – May spread multiple ways, take different actions on infected computer depending on variables such as operating system installed or existence of certain files (flip, invader, tequila)
- Macro – Alters or replaces a macro, which is set of commands used by program to perform common option, target MS products.
  (melissa.A, Relax, Bablas 97M/Y2K)
- Stealth – complex malware that hides itself after infecting a computer, once hidden, it copies information from uninfected data onto itself and relays this to antivirus software during a scan. This makes it a difficult type of virus to detect and delete –

VIRI 2

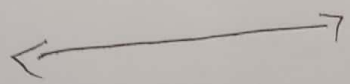
- Memory Resident = Fix themselves in device memory, are activated every time OS runs and end up infecting other opened files (cmj, meve, randex)
- Overwrite – overwrite part of existing data in files, effectively destroying data in them. (Trj.reboot, way, trivial.88.D)
- Direct Action – must be directly launched, when certain conditions are met they will act - infecting autoexec.bat, found in root directory. (vienna)
- Directory - Infect computers directory by changing path indicating file location. usually usually located in disk but affect entire directory (dir-2 virus)
- Web scripting - code embedded in web browser causing undesirable behavior. (js. fortnight)

VIRIS

- FAT – lazy viri that attack file allocation table (FAT) which is the disc part used to store information about available space, location of files, unusable space, etc – (linF)
- Companion – infect files like and has ability to self-replicate leading to negative effects on device (Jovgate.F, Sobig.D, Trile.C, PSW Bugbear.B – map scan)
- Trojan – Attack banking and other credential
- Email – Spread via email, hide in an email and detonate when the recipient open mail-
- Boot infectors – include boot sector plus MBR (master boot Records), viral code may lie in different areas (brain virus – first ever to be created and found in wild)

Malware Types 1

- APTs - Advanced persistent threats; sometimes hide in bios and 'self heal' if removed.
- Adware - Adds victim to spamming network.
- Bots - Adds victim to its network for DoSing or CPU/bandwidth rentals.
- Bugs - May mimic malware and corrupt data or block communication.
- Rootkits - Slave victims, self healing, difficult to remove, parts usually discovered are what rootkits have installed, not rootkit itself.
  - Rootkits come in 3 variables. hypervisor, kernel and application.
  - For test there are 3 varieties of rootkits in reality there are others that infect BIOS and other component as well.
  - can bypass windows 7 code signing by infecting Bootsector.



Malware Types 2

- Spyware :- Facilitates utilizing victims camera, microphones, files, etc (google, cassidy wolf)
- Toojan :- May appear as normal software or masquerade as a real application; while giving access via a backdoor to attacker.
- Viruses :- Attempt to consume computer resources (memory, storage, etc) they replicate over and over until all resources are consumed and system halts or crashes.
- Ransomware :- Encrypt storage, require payment in exchange for key.

Common malware

- Zeus Family (2.8 leaked, gameover, dyre wolf (current) many variant since leaked)
- Coyptolocker
- Andriod / Tedlss
- Stagefright.N
- Fobus.A (Andriod)

Obfuscating malware

- Break Trojan into multiple smaller files and zip individual pieaces, impractile to rebuild on host w/out a rootkit installed-
- change content of trojan using hex editor and thus checksum will be different-
- Encrypt/encode trojan using multiple hashing algorithms (MD5/SHA-1, etc—)

Reamining current

- Shmoocon
- RSA (c-level)
- blackhat (government)
- DEFCON (everyone)
- Derbycon

Cons

- PUMPCon
- Bsides (all world)
- Many more—

Daily Reading

- packetstormsecurity.org
- darkreading.com
- Blackhatlibrary.net
- databreachtoday.com
- Threatpost.com
- Attackresearch.com

- malwarebytes.org
- cyberpedia.in
- ghettoforensics.com
- secguru.com
- liquidmatrix.org

many more-

Acceptance

*FAR :- False Acceptance rate

Buffer overflow protection (1)

- If inputs to application and program are not sanitized properly, buffer overflows and manipulation may result.
- To stop rampant amount of buffer overflow attacks two different techniques were created ASLR and DEP
- Data Execution prevention (DEP) is a sec feature included in modern OS. it marks areas of memory as either "executable" or "non-executable") and allows only data in an "executable" area to be run by programs service, device drivers etc. It is known to be available in OSX, windows / IOS / OS.
- Address space layout randomization (ASLR) is a memory-protection process for OS (OSes) that guards against buffer-overflow attacks by randomizing location where system executables are loaded into memory.

Buffer Overflow protection (3)

- #1 reason for buffer overflows is failed or non existing input sanitization (OT) ← know this! live it, learn it,
- Sanitize inputs or verify they are sanitized or perish by it!
- IRL = just because a crash may be caused it does not mean bug be exploited.
- IRL = Just because it won't crash, does not mean it may not be exploited.

Paths in Common OSs (OT) ←→

- Windows
  - \windows\system32\drivers\etc\hosts
  - \windows\system32\drivers\
- Linux
  - /etc/hosts
  - /etc/services
- hosts file contains URL and IP address of known hosts eg/. Somedomain.com 192.192.192.1
- Service file contains map of ports to application that are going to use them
  SMTP 25

PCI (Payment Card Industry):

- PCI-DSS (data security standard) is driven by visa, master card, discover, JCB and Amex.
- PCI-DSS v3.1 is current as April 2015 (and is current in december 2015.

PCI -2

Control objectives set forth by PCI-DSS

- Require penetration testing after any major upgrades
- Require a penetration test once per year.

Build Maintain Secure Network & system

1 :- Install and maintain a firewall configuration to protect cardholder data-

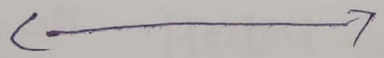
1.1 // Implement CPT so that when FW changes occur, regression tests are performed-

1.2 // FW and Router configuration should restrict all inbound and outbound traffic from 'untrusted' network (including wireless) and hosts and specifically deny all other traffic except for protocol necessary for cardholder environment.

1.3 // prohibit direct public access between internet and any system component in cardholder environment.

1.4 // Install personal firewall software on any mobile and/or employee-owned devices that connect to internet when outside network, and which are also used to access network-

1.5 // Ensure that related security policies and operational procedure are documented, in use, and known to all affected parties.



Build maintain Secure Network and System

2. Do not use vendor-supplied defaults for system passwords an other security parameters.

2.1 // Always change All vendor-supplied default and remove or disable unnecessary default account before installing a system on network. this includes wireless devices that are connected to cardholder data environment or are used to transmit cardholder data.

2.2 // Develop configuration standards for all system component that address all known security vulnerability and are consistent with industry accepted definition, update system configuration standard are new vulnerability issues are identified.

2.3 // Using strong cryptography, encrypt all non-console administrative access such as browser / web-based management tool.

2.4 // maintain an inventory of system components that are in scope for PCI DSS

2.5 // Ensure that related security policies and operational procedures are documented, in use and known to all affected parties.

2.6 // Shared hosting providers must protect each entity's hosted environment and cardholder data.

x——————x

Protect Cardholder Data

- Cardholder data should not be stored unless it's necessary to meet needs of business
- Sensitive data on mag stripe or chip must never be stored after authorization.
- If for some reason it is stored, it must be rendered unreadable.

protect cardholder Data.

3.1// limit cardholder data storage and retention time to what which is required for business, legal, and/or regulatory purposes stored data at least quarterly.

3.2// Do not store sensitive authentication data after authorization (even if it is encrypted) see Render all sensitive authentication process issuers and related entities may store sensitive ~~information~~ authentication

3.3// Mask PAN when displayed (The first six and last four digits are the maximum number of digits you may display), so that only authorized people with legitimate business need can see full PAN. this does not supersede stricter requirements that may be in place for displays of cardholder data, such as on a point-of-sale receipt.

3.4// Renders PAN unreadable anywhere it is stored - including on portable digital media, backup media, in logs, and data received. from or stored by wireless network. Technology solutions for this requirement may include strong one-way hash function of entire PAN, truncation, index tokens with securely stored pads, or strong cryptography.

Encryption primer :- Cryptography uses a mathematical formula to render plaintext data unreadable to people without special knowledge (called a "key"). Cryptography is applied to stored data as well as data transmitted over a network, encryption changes plaintext into ciphertext. Decryption changes ciphertext back into the plaintext.

Protect Cardholder Data

3.5// Document and implement procedure to protect and keys used for encryption of cardholder data from disclosure and misuse.

3.6// Fully document and implement key mangemt processes and procedures for cryptographic keys used for encryption of cardholder data.

3.7// Ensure that related security policies and operational procedures are documented, in use, and known to all affected parties.

Encrypt transmission Cardholder Data Across open public Network

4.1// use strong cryptography and security protocols such as TLS, SSH or IPSec to safeguard sensitive cardholder data during transmission over open, public network (e.g// internet, wireless Techs cellular technologies, Generall packet Radio service [GPRS], satellite communication) ensure wireless network transmiting cardholder data or connected to cardholder environment use industry best practices (e.g// IEEE 802.11i) to implement strong encryption for authentication and transmission The use of WEP as a security control is prohibited.

4.2// Never send unprotected PANs by end user messaging technologies (for example, e-mail, instant messaging, SMS, chat, etc).

4.3// Ensure that related security policies and operational procedures are documented, in use and known to all affected parties.

Protect All systems Against malware and regularly update Anti-virus software / programs

5.1// Deploy anti-virus software on all system commonly affected by malicious software (particularly personal computer and servers). For system not affected commonly by malicious software, perform periodic evaluations to evaluate evolving malware threats and confirm whether such systems continue to not require anti-virus software.

5.2// Ensures that all anti-virus mechanisms are kept current, perform periodic scans, generate audit logs which are retained per PCI DSS requirement 10.7

5.3// Ensure that anti-virus mechanism are actively running and can't be disabled or altered by users, unless specifically authorized by management on case-by-case basis for a limited time period.

5.4// Ensure that related security policies and operational procedures are documented, in use and known to all affected parties.

Develop and maintain secure system and applications

6.1// Establish a process to identify security vulnerabilities using reputable outside sources, and assign a risk ranking (e.g// "high", "medium" or "low") to newly discovered security vulnerabilities.

6.2// protect all system component and software from known vulnerabilities by installing applicable vendor-supplied security patches, install critical security patches within one month of release.

6.3// Develop internal and external software apps including web-based administrative access to applications in accordance with PCI DSS and based on industry best practices.

- Incorporate information security throughout software development life cycle.
- This applies to all software developed internally as well as custom software developed by a third party.

Develop & maintain secure systems & applications.

6.4// Follow change control processes and procedures for system components.

6.5// prevent common coding vulnerabilities in software development.

- Train developers in secure coding technique -
- Develop applications based on secure coding guideline, including memory data storage.

6.6 Ensure all public-facing web applications are protected against known attacks and applicable vulnerabilities.

- perform application vulnerability assessment at least annually and after any changes -
- or by installing ~~vulnerability~~ automated technical solutions that detects and prevents web-based attack (for example, a web-app firewall) to Continually check all traffic.

6.7// Ensure that related security policies and operational procedures are documented, in use and known to all affected parties (wide distribution)

Restrict access to cardholder data by business need-to-Know

7.1// Limit access to system components and cardholder data to only those individual whose job requires such access. RESTRICTING ACCESS IS CRUCIAL! Restrict access to cardholder data environment by employing access control limit access to specifically allowed to access cardholders data and system, this guide provides supplemental information that does not replace or supersede PCI SSC security standard or their supporting documents -

7.2// Establish an access control system components that restricts access based on a users need to know, and is set to a "deny all" unless specifically allowed.

7.3// Ensure that related security policies and operational procedures are documented in use and known to all affected parties -

Identify & authenticate access to system components

8.1 Define and implement policies and procedures to ensure proper user identification management for user and administrators on all system components. Assign all user a unique user name before allowing them to access system components or Cardholder data.

8.2 Employ at least one of these to authenticate all users: something you know, such as password or passphrase; something you have; such as a token device or smart card; or something you are; such as biometric, use strong authentication method and vendor all passwords unreadable during transmission and storage using strong cryptography

8.3 Implement two-factor authentication for all remote network access that originates from outside network by employees, administrators, and third parties including vendor access for support or maintenance. example of two-factor technologies include remote authentication and dial-in service (RADIUS) with tokens; terminal access controller access control system (TACACS) with tokens; or other technologies that facilitate two-factor authentication. using one factor twice. eg: using two separate passwords) is not considered two-factor authentication.

Identify & Authenticate Access to System Components

8.4// Develop, implement & communicate authentication policies & procedures to all users. this guide provides supplemental information that doesn't replace or supersede PCI SSC security standard or their supporting documents.

8.5// Do not use group, shared or generic IDs or other authentication method. Service provides with access to customers environments must use a unique authentication credential (such as a password/passphrase) for each customer environment (Note: This requirement for service providers is best practice until june 30, 2015, after which it becomes a requirement.)

8.6// Use of other authentication mechanisms such as physical security tokens, smart cards & certificates must be assigned to an individual account.

8.7// All access to any database containing cardholder data must be restricted: all user access must be through programmatic methods; only database administrators can have direct or query access; & application IDs for database applications can only be used by applications (& not by users or non-app processes)

8.8// Ensures that related security policies & operational procedures are documented, in use & known to all affected parties.

Restrict physical access to cardholder data

9.1// use appropriate facility entry controls to limit & monitor physical access to system in the cardholder data environment.

9.2// Develop procedures to easily distinguish b/w onsite personnel & visitors, such as assigning ID badges.

9.3// Control physical access for onsite personnel to sensitive areas. Access must be authorized and based on individual job function; access must be revoked immediately upon termination & all physical access mechanism, such as keys, access cards etc, returned or disabled.

9.4// Ensure all visitors are authorized before entering areas where cardholder data is processed or maintained; given a physical token that expires and that identifies visitors as not onsite personnel; and are asked to surrender physical token before leaving facility or at date of expiration.

- use a visitor log to maintain a physical audit trail of visitor information & activity, including visitor name, company & onsite personnel authorizing physical access.
- Retain log for at least three months unless otherwise restricted by law.

Restrict Physical Access to cardholder data

9.5// physically secure all media; store media back-ups in a secure location, preferably off site.

9.6// Maintain strict control over internal or external distribution of any kind of media.

9.7// Maintain strict control over storage & accessibility of media.

9.8// Destroy media when it is no longer needed for business or legal reasons.

9.9// protect devices that captures payment card data via direct physical interaction with card from tampering & training personnel to be aware of suspicious activity.

9.10// Ensures related security policies & operational procedures are documented, in use & known to all affected parties.

Track & monitor all access to network resources & cardholder data

10.1 / Implement audit trails to link all access to system components to each individual user.

10.2 // Implement automated audit trails for system component for reconstructing these events:

- all individual user accesses to cardholder data.
- all actions taken by any individual with root or administrative privileges
- access to all audit trails.
- invalid logical access attempts.
- use of and changes to identification & authentication mechanism (including creation of new accounts, elevation of privileges) & all changes, additions, deletions to accounts with root or administrative privileges.
- initialization, stopping or pausing of audit logs.
- creation and deletion of system-level objects.

Track & monitor all access to network resources & cardholder data

10.3// Record audit trail entries for all system components for each events, including at a minimum user identification, type of event, date & time, success or failure indication, origination of events & identity or name of affected data, system component or resources.

10.4// using time synchronization technology, synchronize all critical system clocks & times & implement controls for acquiring, distributing & storing time.

10.5// Secure audit trails so they can't be altered

10.6// Review logs & security events for all system components to identify anomalies or suspicious activity. perform critical log reviews at least daily.

10.7// ~~Review~~ Retain audit trail history for at least one year; at least three months of history must be immediately available for analysis.

10.8// Ensures that related security policies & operational procedure are documented, in use & known to all affected parties.

Regularly test security & processes

11.1// Implement processes to test for presence of wireless access points (802.11) & detect & identify all authorized & unauthorized wirless access point & implement incident response procedures in event unauthorized wireless access points are detected.

11.2// Run internal & external network vulnerability scans at least quarterly & after any significant change in network. perform rescans as needed, until passing scans are achéived. after passing scan initial PCI DSS compliance, an entity must, in subsequent years, pass four consecutive quartely scans as a requirement for compliance. Quarterly external scans must be performed by an approved scanning vendor (ASV). scan conducted after network changes & internal scans may be performed by internal staff.

11.3// Develop & implement a methodology for penetration testing that includes external & internal penetration testing at least annually & after any upgrade or modification, if segmentation is used to reduce PCI DSS scope, perform penetration tests to verify segmentation. methods are operational & effective.

Regularly test security System & processes

11.4// use network intrusion detection &/or intrusion prevention technique to detect and/or prevent intrusion into network.

- monitor all traffic at perimeter of the cardholder data environment as well as at critical points inside of cardholder data environment, & alert personnel to suspected compromises.
- IDS/IPS engines, baselines & signatures must be kept up to date.

11.5// Deploy a change detection mechanism (for example, file integrity monitoring tools) to alert personnel to unauthorized modification (including changes, additions, & deletions) of critical system files, configuration files or content files. Configure software to perform critical file comparison at least weekly. implement a process to respond to any alert generated by change-detection solution.

11.6// Ensured that related security policies and operational procedures are documented, in use & known to all affected parties.

EAP

- EAP is used in:
  - hardening wireless networks
  - Transfering certificates in a secure manner for smart cards in point to point networks.

Kali Linux

Steganography

- Hiding data inside of images
- Ideas is to avoid attention
- most steganography images are all black the black images are result of trying to put too much data inside of images
- use the LSBs of the target images

nLSB

0000 0000 0000 0000 0000 00000 0000 0000

- Data hiding analysis can be useful LSB in detecting & recovering data the may indicate knowledge, ownership or intent.

Defacement

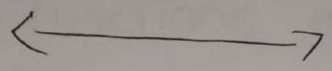
- Act of changing a website presentation in any way.
- can be done via DNS hijacking, poisoning
- can be done via hacking into webserver

nitigation

dont use wordpress!

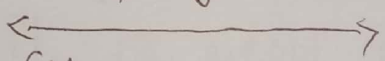
Miscellance Tools

- http://www.qualys.com/forms/freescan/patch-tuesday/
- https://www.qualys.com/forms/freescan/owasp
- https://www.qualys.com/forms/freescan/scap
- https://www.qualys.com/forms/freescan
- https://www.qualys.com/~~forms/~~free-tools-trials/browsercheck/



virusshare.com

- Why on earth would I want live malware?
  - practicing dynamic analysis (you know what this malware does, its been analyzed)
  - The output of this malware (URLs, IPs) is worth tens of thousands of dollars
  - Testing signature analysis (product evaluation)
  - You need to be invited (its free)
  - you must be responsible when handling it.
  - practicing static/dynamic analysis.



File Hashes (1)

- used for verification that file was not modified or corrupted in flight/transport
- MD5 - No longer safe to use due to collision
- Hashes are non-reversible, they are ONE way

File Hashes (2)

MD5 produces 128 bit hashes
SHA-1 produces 160 bit hashes

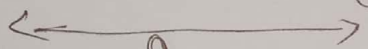
// Remember MD5 is deprecated
// Avoid hash functions that can cause collisions
// A hash collision occurs when two different files are hashes and the output of two hashes files in same-
// SHA-1, SHA-256, SHA-512, SHA-3 are current standard for hashing-
// Hashing can be used to encrypt/disguise a Trojan so that it can bypass security monitoring tools.

File Handling (3)

MD4 - in use today for optimizing confidential communication.
For example, it is used for encoding data in flight - like bidirectional data and voice.

SSDLC

- Secure Software development life cycle
- Highlights - make sure inputs are sanitized!
  - If expecting text less than 10 characters, validate & verify that
  - If moving memory, be assertive that source fits in destination before attempting a move
  - DO NOT TRUST DATA: before it takes flight sanitize it; Before it is put to rest, sanitize it.
- perform static analysis - may be expensive & requires properly trained persons to perform them.
  (significantly beneficial in preventing breaches)
- perform dynamic analysis for validation (security assessment / penetration test)



Threat Modeling :

- procedure for optimizing network security by identifying objectives & vulnerabilities & then defining countermeasures or mitigations for them.
- occurs in design phase of development
- viewing a system environment through security glasses.

Threat Modeling 2

- Methodology for threat modeling
  - Assessment Scope
  - System modeling
  - Identify threats
  - Identify vulnerabilities
  - Examining threat history
  - Evaluation of impact on business
  - Developing a security threat response plan.

Threat Modeling 3

- **Assessment Scope** - Identifying tangible assets, like databases of information or sensitive files is usually easy. understanding capabilities provided by the application and valuing them is more difficult.
- **Identify Threat Agent & possible Attacks** - A key part of threat model is a characterization of different groups of people who might be able to attack your application. these groups should include insiders & outsiders, performing both inadvertent mistakes & malicious attacks
- **Understand existing countermeasures** - The model must include existing countermeasures.
- **Identify exploitable vulnerabilities** - once you have an understanding of security in application, you can then analyze for new vulnerabilities. Search is for vulnerabilities that connect possible attack you have identified to negative consequences you have identified.
- **prioritized identified risks** - prioritization is everything in threat modeling - as these are always lots of risks that simply don't rate any attention for each threat, you estimate a number of likehood & impact factors to determine an overall risk or security level.
- **Identify Countermeasure to reduce threat** The last step is to identify countermeasures to reduce risk to acceptable levels.

Repudiation

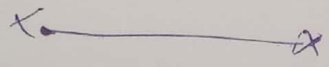
- Users may dispute transactions if there is insufficient auditing or recordkeeping of their activities.
- In this space, as white/gray hats, we are interested in non-repudiation.

Kali Linux

- http://www.kali.org
- Created by offensive security
- Spin off from backtrack Linux (now defunct)
- it's a toolkit
- most hacker tools are tool kits of many smaller one off tools.

Honeypots

- System configured to look like (mimic) other system (ports, traffic, etc...)



Network Telescope

- A network of computers used to watch trending of large scale events taking place on internet.
- Accomplish by observing traffic on dark (unadvertised) IP address space
- All traffic to these sensors (systems) is suspicious
- Example of one is: CAIDA network telescope
- E.g.
  - DDOS Attack
  - Random scanning worms

Network Canary

- Several Definitions
  - A detection method or program that can alert something when it has been trigged.
- E.g.
  - A document, with an embedded canary in it, is stolen & opened - it will notify a listening server it was programmed to notify.
- network stacks can be embedded with canaries so that if a smash or overflow occurs specific actions may be undertaken

Three phases of Security testing

- preparation
- Conducting
- Conclusion

wget

- Free tool for *nix & windows that retrieves HTTP, HTTPS & FTP data
- Can clone an entire site offline inspection (minus database)

Form Scalpel

- Tool for automatically extracting form from a given web page & splits up all fields for editing & manipulation