Study guide

Monday, June 11, 2018 1:25 PM

Performing heartbleed poodle shellshock?
Blackberry cracking tools?
Pen testing approaches, procedures, risk analytics?
Trojan ports?

Memorize:
Bounds checking prevents buffer overflows
Http-methods script will help you
Splint detects buffer overflows
Gets, sprintf, strcpy are all vulnerable to buffer overflows
Screened subnet used to implement dmz
Tcp allows you to guess sequence number for mitm
Java is not suspectable to stack based buffer overflows
Stateful firewalls inspect packet info dynamically
Spatial domain steg - pixels
Transform domain steg- everything else
Tcptrace can take inputs from Wireshark, tcpdump, etc
Bastion host is separation of duties
Esp transport ensures security with same lan. tunnel is outside.
Os nmap scan -O requires root priv
Passive sniffing is sniffing through a hub
Hypervisor is for vm

Goals	PCI DSS Requirements
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

Scanning & Enumeration
ICMP Message Types
0: Echo Reply: Answer to Type 8 Echo Request
3: Destination Unreachable: No host/ network
Codes

0 – Destination network unreachable
1 – Destination host unreachable
6 – Network unknown
7 – Host unknown
9 – Network administratively prohibited
10 – Host administratively prohibited
13 – Communication administratively prohibited
4: Source Quench: Congestion control message
5: Redirect: 2+ gateways for sender to use or the best route not the configured default gateway
Codes
0 – Redirect datagram for the network
1 – Redirect datagram for the host
8: Echo Request: Ping message requesting echo
11: Time Exceeded: Packet took too long to be routed