Review

IT443 – Network Security Administration
Network Basics

• Network Layers
  – Application layer
  – Transport layer
  – IP layer
  – Data link layer

  – TCP, UDP, IP, SSH, HTTP
  – IP address, MAC address, TCP address?
  – Port number
Network Basics

• Headers
  – [ether net header [IP header [TCP header [Payload]]]]

• TCP / UDP
  – TCP is reliable
    • Acknowledgement, retransmission, discard duplicates, …
  – TCP 3-way handshake
    • SYN, ACK, FIN
Network Basics

• IP layer
  – Routing (different paths)
  – IP prefix, e.g., 12.34.158.0/24
  – Classful Addressing (Class A, B, C)
  – Classless Inter-Domain Routing (CIDR)
  – Private networks
    • 10.0.0.0/8 (255.0.0.0)
    • 172.16.0.0/12 (255.240.0.0)
    • 192.168.0.0/16 (255.255.0.0)
Network Basics

• DNS
  – Hierarchical name space
  – Local DNS server / caching
  – dig / dig -x

• Data link layer
  – MAC address
  – ARP messages / ARP table
Network Basics

• Questions
  – true/false
    192.168.x.x is not globally accessible.
  – multiple choice
    Which of the following header may contain port numbers:
    A. TCP header    B. IP header
    C. Ethernet header   D. All of above
  – Compare TCP and UDP, and briefly describe their difference.
Crypto Basics

• Encryption/Decryption
  – Plaintext, ciphertext, key
  – Secret key/symmetric key crypto
  – Public key/asymmetric key crypto
  – Hash function
Crypto Basics

• Secret key crypto
  – Block cipher (with padding)
  – File size
Crypto Basics

- Public key crypto
  - Public/private key pair
  - Encryption/decryption (different keys)
  - Sign/verify (digital signature)
  - Much slower than secret key operations
Crypto Basics

• Hash function
  – One way transformation
  – Collision resistance
  – Applications
    • Message digest/checksum
    • File integrity
    • Password
    • …
Crypto Basics

Questions

- True or false
  In block encryption, the encrypted file’s size may be larger than the original file.

- Which of the following gives the desired properties of hash functions?
  - a. One-way property, that is, it’s easy to reverse the hash computation, but computationally infeasible to compute the hash function itself.
  - b. Collision free, that is, it’s computationally infeasible to find two messages that have the same hash value.
  - c. Only authorized parties can perform hash functions.
Crypto Basics

• What’s wrong with this picture? Fix it
Authentication

• What’s authentication
  – User authentication
    • Allow a user to prove his/her identity to another entity (e.g., a system, a device).
  – Message authentication
    • Verify that a message has not been altered without proper authorization.
Authentication

• Certificate
  – How do you know the public key of a node?
  – Certification Authorities (CA)
  – Everybody needs to know the CA public key
  – The CA generates certificates: Signed(A, public-key, validity information)

[Alice’s public key is 876234]_{carol}
[Carol’s public key is 676554]_{Ted} & [Alice’s public key is 876234]_{carol}
Authentication

• Password guessing
  – Online vs. offline
  – Dictionary attack
  – Password salt
SSL

• Which layer

• Why we need it
  – Think about https

• Main processes
  – Negotiate cipher suites
  – Authenticate servers
  – Verify certificates
Firewall / IDS

• What are their roles
  – Prevent vs. detect

• Firewall
  – Packet filtering (stateless) vs. session filtering (stateful)
  – iptables
Firewall / IDS

• IDS

  – Misuse detection (signatures)
  – Anomaly detection

  – Host-based (e.g., aide)
  – Network-based (e.g., snort)
Firewall

• Questions

– True or false
   A stateless firewall on a server cannot limit the number of TCP connections per client.

– Describe the goal of the following firewall rule:
  `iptables -A INPUT -p icmp -j DROP`
IDS

• Questions

– Explain the following snort rule and describe how to trigger the alert:

  alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS 80
  (msg:"Test attack"; content:"test_attack"; ... ... )

– Compare host-based and network-based IDS, and briefly describe the difference.