QUIZ

How do we evade Firewalls?

- By making our network traffic look legitimate. ✓

👏 Good job! We can evade Firewalls by making our network traffic look legitimate.

- By dousing ourselves in water.
- By conducting careful reconnaissance before we act.
- By not creating known indicators of compromise.

What is the defining characteristic of Ephemeral Keys?

- They are discarded after use. ✓

👏 Good job!

- They are used by hackers to remain undetected.
- They are used by ghost sessions.
- They aren't stored in RAM.

What digitally signed documents are used by Public-Key Infrastructure to verify the authenticity of public keys?

- Pedigrees
- Passports
- Certificates ✓

👏 Good job!

- Certifications

How do we evade honeypots?

By making your network traffic look like regular network traffic.

By not creating obvious evidence of your presence.

By disguising yourself as a bee.

By conducting good reconnaissance before acting, and taking your time.

Good job! The best way to deal with honeypots is to not fall in in the first place.

What is a piece of hardware or software that filters network traffic according to a set of rules?

An IDS

A Honeypot

A Watchdog

A Firewall

Good job! Firewalls are a piece of hardware or software that filters network traffic according to a set of rules.

What is a piece of hardware or software that monitors activity within a network and look for evidence of malicious or prohibited activities?

An Intrusion Detection System (IDS)

Good job! An Intrusion Detection System is a piece of hardware or software that monitors activity within a network and look for evidence of malicious or prohibited activities.

A Sentinel

A Firewall

A Honeypot

What is the basic purpose of Public-Key Infrastructure?

To prevent public keys from being stolen.

To generate public keys.

To verify the authenticity of public keys.

 Good job!

To transmit public keys.

How do we evade Intrusion Detection Systems (IDS)?

By conducting lots of reconnaissance before acting.

By making our traffic look as innocuous as possible.

By being so obvious that the system marks you as a false-positive.

By not creating known indicators of compromise.

 Good job! We can evade Intrusion Detection Systems by not creating known indicators of compromise.

What do you call a decoy computer or network to entice intruders and keep them distracted?

A Firewall

An IDS

A Honeypot

 Good job! Decoy networks are also sometimes called Honeynets.

A Mousetrap