Deception Techniques!! My World Of HoneyNets

Shomiron Das Gupta

Agenda

- Bearings – Honeypots and Honeynets
- HOWTO
- Decoy Planning
- Deception and Fish-bowling

Bearings

- HoneyPots
- Routing and Reverse Walling
- Bait and Switch (HoneyWall)
- Intrusion Alert
- Protected Logging Systems
- HoneyNets!!

HOWTO

- HoneyPots
- Routing and Reverse Walling
- Bait and Switch (HoneyWall)
- Intrusion Alert
- Protected Logging Systems
- HoneyNets!!

HoneyPots

- Tarpitting – Labrea
- Service Decoys – Honeyd
- Live Decoys
- War Decoys

Routing and Reverse Walling

- Open routers – No ACLS!!
- Out of band management
- Secured SNMP Stats – Stats Server
- TFTP – DISABLED!!
- IP Killers
- Limited Reverse Traffic
- Static MAC Addressing – No Poisoning
- No STP or Trunk’ing

Bait and Switch (HoneyWall)

- Inline Intrusion Detection System – Snort-Inline
- Firewall – IPTables
- NAT v/s Bridge
- Connection Control – Egress
- DROP, SDROP, Reject Rules
- REPLACE Functions

Intrusion Alert

- Log alerts – manual ☹
- Log repository software ☹
- String Search Utilities and log management software ☺
- #> last /var/log/alerts | grep xxxx ☺

Protected Logging Systems

- S-Syslog – Symmetric Key Encryption
- Stunnel – One of the alternatives
- SABEK2 – The best known
- Our own – Scripted tcpdump –w xxx.log
- On alert logging systems (Home Grown)

Decoy Planning

- Decoy planning guide – SDG
- HoneyD – Revisited
- Labrea – Revisited
- Live Decoy Systems
- Architecture study
- Parallel networks
- Random data generators
- Event recording systems – Our own Syslog!!

Deception and Fish - bowling

- Deception = Planned Decoys
- Strategy = Risk Mitigation
- IPtraf, IPlog, TCP hunt etc.
- Fish - bowling = Central Alert Management System
- Log monitoring system