NSRC
Network Startup Resource Center

Security Workshop Topic Mindmap
April, 2015

Security Workshop Topics

- **E-Mail**
  - Theory
    - Blacklists
  - Toolkit
    - ClamAV
    - Spam Assassin
  - Exercises
- **Network Security**
  - Firewalls
    - Architectures
      - Border firewalls vs. firewall close to asset
      - Transparent vs. Routed
    - Best Practices
      - Rule validation
      - Configuration management
      - Logging NAT translations, or 1-1 NAT
    - Why?
      - Blocking Bogons
      - Spam Mitigation (control port 25)
      - C&C Blackholes
    - Why not?
      - Bandwidth
      - Increased network complexity
      - Maintenance overhead
  - Theory
    - DDOS
    - Spoofing
      - BCP38
    - Routing Protocols
      - Authentication
        - RPKI
      - P2P Links
    - Wireless
      - Encryption / authentication best practices
        - WPA2
        - DOT1X
      - Rogue APs
        - Detection, mitigation
    - NAC
    - Segregating management interfaces
    - Layer 2
      - Vlan Hopping (https://www.cisco.com/web/ME/exposaudi2009/assets/docs/layer2_attacks_and_mitigation_t.pdf)
      - Mac Flooding
      - Rogue DHCP
      - Arp Poisoning
    - VOIP
  - Toolkit
    - nmap
    - packet fence
    - netcat
    - tcpdump
    - traceroute
    - scapy
    - Cisco
      - PVLAN
      - VRF
      - dhcp-snooping
      - port-security
      - bpdu guard
  - Exercises
    - Discovering services on your network (nmap diffs)
    - Auditing firewall rules
    - Automatically filtering Bogons, peering with Team Cymru (http://www.team-cymru.org/Services/Bogons/bgp.html)
    - Implementing RPKI
- **Layer 8, Community engagement**
  - News and Discussion
    - Blogs
      - https://www.schneier.com/
      - http://krebsonsecurity.com/
      - https://securityblog.verizonenterprise.com/
      - http://contagiodump.blogspot.com/
    - Mailing Lists
      - DailyDave
      - NANOG
      - Emerging Threats
  - Vulnerability information
    - http://cwe.mitre.org/
    - http://cve.mitre.org/
    - https://nvd.nist.gov/
    - http://www.redhat.com/mailman/listinfo/rhsa-announce
    - https://lists.ubuntu.com/mailman/listinfo/ubuntu-security-announce
  - Abuse Handling
    - ShadowServer
    - maintaining abuse@yourdomain.tld
    - Leveraging breaches for political capital
  - Phishing / spear phishing
    - Training sessions for user base
- **Encoding, Encryption, Hashing**
  - Theory
    - Asymmetric vs. Symmetric
      - Lockbox tutorial
    - Encryption vs Hashing vs Encoding
    - Web of trust
      - SSL
        - Self signed certificates
        - Certificate Authorities
        - Wildcard certs
        - GPG Key Signing
      - Algorithms
        - Which algorithms must be avoided? Where to find this information?
  - Toolkit
    - SSH
      - XForwarding
      - Tunneling
      - SOCKS Proxy (ssh -D)
      - Local code execution on remote server (ssh x.x.x.x "bash -s" < ./myscript.sh)
      - Protection against MITM -- "WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!"
      - Generating, storing, distributing keys
      - Generating, storing, distributing keys
    - GPG
      - Revoking a key
      - Encrypting/decrypting a message / file
    - stunnel
    - OpenSSL
    - OpenVPN
  - Exercises
    - Tunnelling unencrypted traffic
    - Encrypting E-mail
      - Methods
        - GPG
        - S-MIME
    - Signing E-mail
    - Encrypting Web Services
      - Certificates
        - Certificate formats (DER, PEM) ...
        - Matching against certificates
        - Certificate expiration, renewal
- **Authentication**
  - Theory
    - Passwords
      - Strong passwords, generating, storing
      - Password expiration
      - Password storage
    - Federation
      - How, what, why?
      - Communities
    - Two-factor
      - How, what, why?
    - Public / Private Key Authentication
      - (See Encryption)
  - Toolkit
    - RADIUS
    - LDAP
    - PAM
    - SAML
      - Gluu (http://www.gluu.org)
  - Exercises
    - Authenticating Linux box off LDAP server
    - Authenticating non-root users against auth DB with PAM
    - Configuring RADIUS servers for eduroam
    - Using SSH Keys for authentication
    - Configuring and admin for Google two-factor
- **Policy, Planning, Compliance**
  - Theory
    - Data Retention
      - What to retain?
      - Why retain?
      - Laws?
    - Acceptable Use
    - Incident Reponse Plan
  - Toolkit
  - Exercises
    - Limiting the number of days you retain a log with logrotate
- **System Hardening**
  - Theory
    - Permissions
      - File permissions
        - Windows file permissions
        - Linux File Permissions
        - chrooting untrusted users
      - User permissions
        - sudoers
        - POSIX capabilities
        - restricted shells
    - Remote Access
      - VPN
      - Bastion hosts
        - (see authentication)
    - Patching
      - Automatic updates
      - Reducing barriers to updates
      - Unpatchables?
      - Authenticating packages. Why?
    - Service segregation
    - Logging
      - (See monitoring, visibility)
  - Toolkit
    - Ansible
    - Puppet
    - iptables
    - chkconfig
    - jailkit
    - capsudo
  - Exercises
    - Creating/maintaining local RPM, DEB repos
    - Limiting use of 'root' user with sudo, posix capabilities, and service users
    - Configuration management for critical servers
    - Bastion hosts with SSH Agent forwarding for simple, secure remote access
    - Giving a process limited superuser privileges with capabilities
    - Configuring ntp servers, deploying ntp clients
- **Web Applications**
  - Theory
    - Authentication
      - (See authentication theory)
    - Permissions
      - File system
      - Web Application Firewall
      - Database
    - Encryption
      - Certificates
        - (See encryption)
    - Monitoring
      - Access logs
      - Authentication logs
    - Common Web Application vulnerabilities
  - Toolkit
    - modsecurity
    - wget / curl
    - burpsuite
    - (See authentication tools)
  - Exercises
    - Monitoring service availablity/reliablity
    - Writing a 'robots.txt'
    - Auditing what is internet accessible on your web app
    - Mirroring a CMS to Static pages
    - Detecting scrapers
- **Pentesting**
  - Theory
    - Ethics
    - Why pentest?
    - What pentest?
  - Toolkit
    - OpenVAS
    - BurpSuite
    - Nessus
    - Metasploit
    - NMAP, NSE
    - ZMAP
    - SIP Vicious
  - Exercises
    - Vulnerability scanning
    - Basic SQL injection
    - Escaping restricted shell (http://pen-testing.sans.org/blog/2012/06/06/escaping-restricted-linux-shells/comment-page-1/)
    - Open HTTP, SOCKS proxy discovery with nmap NSE -- (http://nmap.org/nsedoc/scripts/http-open-proxy.html, http://nmap.org/nsedoc/scripts/socks-open-proxy.html)
    - Open redirect discovery with nmap NSE -- (http://cwe.mitre.org/data/definitions/601.html, http://nmap.org/nsedoc/scripts/http-open-redirect.html)
- **Incident response**
  - Theory
    - Forensics
      - Disk
        - Filesystems
          - Permissions
          - timestamps
        - Common services and logs
          - Bash history
          - audit log
        - Signs of lurking evil
          - processes running out of home directories
          - services running on high ports
          - strange outbound connections
      - Memory
      - Network
        - Network metadata
    - Incident response cycle (http://digital-forensics.sans.org/blog/2010/09/27/digital-forensics-security-incident-cycle/)
    - DDOS
      - Know your upstream!
  - Toolkit
    - pstree
    - ps
    - BART PE
    - netstat
    - dd
    - lsof
    - grr
    - volatility
    - FTK
    - hashdeep
    - find
    - top
    - CAINE (http://www.caine-live.net)
  - Exercises
    - Responding to a DOS
    - Making a clone of a drive
    - IP, MAC to identity mapping
    - How did process x get spawned? What is it doing? (Exercise in lsof, pstree, ps)
    - File integrity checking
    - Recovering deleted files
- **Intrusion Prevention**
  - Theory
    - DNS Blackholing
      - http://www.malwaredomains.com/bhdns.html
    - Active defense
      - Blacklisting bruteforcers
  - Toolkit
    - Fail2ban
    - DNSBL
    - Snort
  - Exercises
    - Using fail2ban to block SSH bruteforcers
    - Implementing DNSBH with Malware domains
- **Service, System, Network Monitoring / Visibility**
  - Theory
    - Benefits of centralized SYSYLOG
  - Toolkit
    - Packet capture
      - L2+
        - Bro
        - ntop
      - L3 - L4
        - Argus
    - Logs
      - RSYSLOG
      - Logrotate
      - collectd https://collectd.org/
    - SNMP
      - observium
  - Exercises
    - Detecting scanners
    - Exporting Windows events to SYSLOG with SNARE (http://sourceforge.net/projects/snare/)
    - Implementing NDPI and NTOP for web application visibility
    - Realtime flow visibility with Argus and ratop
    - Detecting Bruteforcing (SSH)
    - Logging executed commands with Snoopy (https://github.com/a2o/snoopy)
    - Reliably and securely sending and receiving SYSLOG
    - Configuring and receiving MAC notification traps for mapping MACs to switchports
- **Malware**
  - Theory
    - Examples
      - C&C's
        - DNS
          - Fast flux DNS
          - DynDns
      - Malware families
        - OnionDuke -- https://www.f-secure.com/weblog/archives/00002764.html
    - Incentives
      - Confidentiality
        - Financial
        - PII
        - Intellectual property
      - Availability
        - DOS
      - Integrity
        - Code injection
    - Common infection vectors
      - Drive-by-download
      - E-mail Attachments
  - Toolkit
    - Automated Sandboxes
      - Anubis
      - Cuckoo Sandbox
    - Yara (http://plusvic.github.io/yara/)
    - Anti-virus
      - VirusTotal
      - Team Cymru MHR
      - ClamAV
  - Exercises
    - Examining suspicious documents
    - Using intuition to spot the malware domains
- **Threat Intelligence**
  - Theory
    - Turning attacks into intelligence
  - Toolkit
    - Splunk
    - Elastic Search
    - grep
    - sed/awk
    - gnu parallel
  - Exercises
    - Elastic Search, Logstash, Kibana
      - Searching, correlating logs with Kibana
      - Ingesting logs with LogStash
    - Installing a Splunk search head
    - Creating threat intelligence
      - Mining SSH logs for bruteforcers
      - Mining darknets for scanners
- **Intrusion detection**
  - Theory
    - "Cyber Kill Chain Analysis" http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf
    - Where to tap? Why?
    - (See malware)
  - Toolkit
    - Host
      - Linux
        - OSSEC (Advanced)
        - AIDE (Basic)
        - logwatch (very basic)
      - Windows
    - Network
      - Signature Based
        - Snort
        - Suricata
      - Data acquisition
        - Tapping
          - VACLs + RSPAN for granular traffic capture (http://www.cisco.com/en/US/products/hw/switches/ps708/products_white_paper09186a008017b753.shtml)
          - SPAN
          - RSPAN
        - PF_RING
      - Non-signature Based
        - Bro
        - SNMP
      - Distros
        - Security Onion
    - Visualization, Correlation
      - Snorby
      - Splunk
      - ELK Stack
  - Exercises
    - Integrating intelligence / sig feeds into Bro, Suricata
      - Malware Domains
      - ET
    - Hunting for evil in network metadata
      - Finding weird UA Strings
      - Vulnerable version detection
      - Malware dropper detection
    - Installing, exploring, getting the most out of Snort / Bro Dashboards in Splunk
    - Installing, caretaking for Snorby
    - Snort / Suricata
      - Analyzing alerts
      - Updating signatures with PulledPork
      - Writing / Analyzing Snort Sigs
    - Investigating Intel Matches / Sig alerts
      - Gathering info with PDNS, WHOIS, etc.
      - Sniffing out false positives