Defensible Security Architecture

SANS 530

Ivan S 2022

# #

100G Intrusion Detection with Zeek (NSM) *[b3/p42]* Very scalable, Berkeley cyber lab has run a 100G-capable network monitoring system with Zeek

4over6 *[b2/p107]* IPv6 Tunneling Options

6in4 *[b2/p107]* IPv6 Tunneling Options

6over4 *[b2/p107]* IPv6 Tunneling Options

6rd *[b2/p107]* IPv6 Tunneling Options

6to4 *[b2/p107]* IPv6 Tunneling Options

802.11 Wireless Standards: 802.11n, 802.11ac, 802.11w *[b1/p95]* 802.11 is a group of wireless standards: Wireless N, Wireless AC, Protected Mgmt Frames

Aa

Access Control Monitoring (Data Protection) *[b4/p58]* monitor gained permissions, powershell or python script automation is helpful - locate excessive permissions

Access Control Review *[b4/p59]* limit priveleges, monitor insecure permission usage, verify permissions and enforce least priv, do more than prevent access - detect and respond to unauthorized access

Access-Denied Assistance (Data Control) *[b4/p108]* Windows built-in, visually notifies user of policy violation

Account Management (audit policies) *[b5/p124]* used to track changes to groups, users, and computers - powerful when combined with change control system

Active Directory Rights Mgmt (ADRM) *[b4/p85]*

Active Flow *[b1/p151]*

Administrative Workstations (Remote Access) *[b3/p129]* admin workstations are locked down, use admin workstation design - only standard user access, no productivity apps

Advanced Access Example (Data Control) *[b4/p110]* Access flow chart

African Network Info Center (AFRINIC) *[b2/p73]*

Agentless Log Collection *[b5/p114]* involves central server to collect logs, main benefit is no additional software - Justin prefers agents

Alert Investigation (NIDS) *[b3/p81]* IDS/IPS should have investigation workflows, Sec Onion uses Sguil, Squert, and Kibana

Alert-Driven Workflows vs Data-driven workflows (NSM) *[b3/p26]* most secops live in alert driven world, alerts provide only initial point for investigation | NSM provides additional data needed to pull a thread (go hunt, explore) vs reactively waiting for an alert

Alerts (mitre) *[b5/p140]* some logs represent alerts, others are alerts after creating new search logic

Alerts Problem: volume (mitre) *[b5/p141]* too many alerts to keep up, alert tuning must be done

All-Prevent Defense: failed mindset *[b1/p32]* Only rely on preventative controls, detection is afterthought

Alternate Data Stream (File Classification) *[b4/p80]* Metadata, file that points to another file in NTFS volume

Alternative Submission Methods (malware detonation) *[b3/p95]* systems support manual and automated submissions, usually via web interface or scripting API

Always on VPN (Remote Access) *[b3/p121]* full-tunnel mode with Always On, requires strong pass or certificate

Anomalies vs Signatures diagram (mitre) *[b5/p143]* anomalies has more FPs

Anomaly Identification vs Real Time Alert *[b5/p162]* represent with anomaly scores, not everything works with real time

Antivmdetection (malware detonation) *[b3/p103]* Antivmdetection and VMCloak hide virtual status, modify sandbox images to mask they are VMs

Apache Guacamole (Remote Access) *[b3/p116]* AG is an open source clientless RDP, SSH, and VNC platform through web browser, has guacamole server and client

API Hooking *[b5/p95]*

App Any Run (malware detonation) *[b3/p98]* provides FREE malware detonation box

Apple iOS *[b2/p35]*

Application Attacks (DDoS) *[b3/p147]* e.g. DNS amplification attack, attacks send spoofed SND to open DNS resolver servers

Application Awareness *[b4/p46]* Key offering of DAM/DBF, audit logs include app, allows for situation awareness, allows controls based on app

Application container (MDM) *[b4/p133]* better/more seamless for end user experience

Application Control (NGFW) *[b3/p8]* Identifies application by characteristics: DNS queries, Ports or IP addresses, filenames, TLS field, app signatures, URLs

Application DDoS Mitigation *[b3/p148]* Patch, turn off DNS recursion, disable NTP monlist command

Application Layer Security *[b2/p136]* L7, balance network and host protection

Application Problem (Data Security) *[b4/p8]* custom apps/websites are problematic, there is a need for custom security integrations

Application Proxies *[b2/p137]* Proxy = system that brokers traffic between systems, goal = funnel traffic so it can control data flow, analyze traffic, cache content

Application Rules (NGFW) *[b3/p19]* Move port rules to include applications, goal = restrict all outbound access to ports and apps

Approach to SA&E *[b1/p10]* Focus on implementation, blue team approach | Risk-driven, practical, hands-on approach - mapped to best practices and standards

APT41- Double Dragon *[b2/p6]* Chinese APT observed by Fireeye

Architecture *[b1/p6]* Meant to communicate a future state | Focus on designing and building security in: networks &

infra, apps, endpoints, and cloud | Built from network up | Must be built around business processes

Argus *[b2/p66]*

ARP Attacks: L2 *[b1/p116]* ARP spoofing, poisoning, MitM

ARP Cache Poisoning *[b1/p118]* Diagram

ARP Spoofing Tools and Mitigation *[b1/p119]* Common tools include Ettercap and Cain and Abel

ARP: A Trusting Protocol *[b1/p117]* Dynamic ARP uses no authentication or encryption - trusts whatever answer is provided

ARPANET *[b1/p19]* First TCP/IP network created by US military - precursor infra for internet, massive growth of IP adoption led to birth of NAT, which led to perimeter defense

ASEPs (Log Collection) *[b5/p116]* auto start extensibility points

Attack Surface Analysis *[b1/p68]* Describes all vectors for exploitation, orgs should conduct formal attack surface analysis & document results

Audit Object *[b4/p54]*

Audit Policies *[b5/p120]* log collection is dependent on proper audit policies

Audit Policies Review *[b5/p138]* policies and config files control log generation, log agents and drivers allow the creation of specialty logs - sysmon for windows, auditd for linux ---- sysmon coming to linux

Audit Policies Windows *[b5/p121]* Audit policy - basic log setting, advanced audit policy - granular control of logs

Audit Policy Advanced *[b5/p122]* for advanced, enable audit: force audit policy subcategory settings

audit.rules example *[b5/p136]* rules listed on slide

auditd (audit policies) *[b5/p134]* provides customizable Linux audit system, granular monitoring allows advanced use cases

auditd example (audit policies) *[b5/p135]* linux auditd on slide

Auditing & Logging (containers) *[b4/p179]* Containers are short-lived, making auditing more important. Docker diff shows container changes from its image, docker commit can make snapshot for IR

Auditing Attacker Reconnaissance (red herring) *[b5/p181]* certain insider threat activities are common

Auditing Tool Pro Tip: L3 *[b2/p41]* audit switches and routers before beginning remediation

Auditing Tools: L3 *[b2/p38]* CIS Router Audit Tool (RAT) = old, CIS-CAT Pro = new - 80+ benchmarks, requires $$ | Nipper can be used free

auditpol.exe *[b5/p123]* configure non-domain joined systems, can list and set policies

Authenticated internet Access (NGFW) *[b3/p18]* Restrict internet access to servers and critical assets, allow authenticated access and block everything else

Authenticated vs Unauthenticated Proxy *[b2/p151]* Explicit proxy + authentication = most secure

Authenticating Network Access (ZT) *[b5/p46]* when mutual auth and encryption not possible, alternative is to authenticate network access - with NAC or single packet authorization (SPA)

Automatic Classification Rules (File Classification) *[b4/p81]* multiple methods to set properties on files: manual, location-based, content-based

Automatic Credential Rotation (ZT) *[b5/p26]* high risk accounts need rotation frequently, local admin accounts (if enabled), service accounts

Automatic Enrollment (PKI) (ZT) *[b5/p41]* Windows PKI supports auto enrollment of device and user certificates, integrations with 802.1x, TLS, and IPSec

Autopwn *[b5/p173]* delivers exploit based on user-agent

AutoSecure (Cisco): Layer 2 & 3 *[b2/p30]* automatically configs a switch or router for a variety of best practices, shows config

AutoSecure Mitigations (Cisco): Layer 2 & 3 *[b2/p31]* shows automatic hardening

Azure Info Protection Classify and Protect Example (File Classification) *[b4/p87]*

Azure Information Protection (AIP) *[b4/p86]* support better method to protect files and docs, each doc is encrypted with new AES key, users private key used to sign doc

Azure Information Protection (File Classification) *[b4/p85]* The evolution of Win FCI (file classification infrastructure) - Msoft is pushing Azure Information Protection (AIP) 0 info protection classifies data similar to FCI

Azure Privileged Identity Mgmt (PIM) *[b2/p132]* Just-in-time access, time restrictions, enforced MFA, required approval workflows

Azure Rights Mgmt Connecter (ARMC) *[b4/p89]*

Azure Rights Management Connector (File Classification) *[b4/p89]* Right mgmt connector: syncs and applies AIP policies with auto file classification

Bb

Banners *[b2/p25]* Cisco switches & routers support banners: login, exec, MotD - login is most critical

Bayesian Analysis *[b2/p162]* ongoing statistical analysis that produces probability score, works well with spam but not phishing

Bcrypt *[b2/p24]*

Behavioral-Based NSM with Zeek IDS *[b3/p35]* More than just an IDS, its a network programming language, power of Zeek is that it can help you answer questions

Benchmarks: Layer 2 & 3 *[b2/p28]* Cisco best practices, autosecure, DISA STIGs (defense info systems agency, security technical implementation guide), CIS, Nipper-ng

BitLocker *[b4/p68]* Included in Win10 Pro and Enterprise, supports FDE, can encrypt USB drives, requires TPM for automatic boot handling

BitLocker Network Unlock *[b4/p70]* allows TPM + PIN without user intervention

Blackholes & Darknets *[b2/p63]* Blackhole = anything that gets routed, but there's not a route for - goes into a blackhole | Darknet = request subnet not using but we provide ability to see the request, so we are aware of it

Block Remote Access Programs *[b3/p111]* block all unauthorized remote access programs, use application control, FQDN blocking, or sinkholing

BloodHound (Remote Access) *[b3/p126]* remote access is more than external access - use BloodHound tool to help threat model

Blue/Red Asymmetries *[b1/p46]* Always seek to deploy defensive controls that are easy for blue team but make red team's job harder

Bogon and Fullbogons Filtering *[b2/p58]* IP space that should not be routed on the internet, fullbogons change daily - ideally block both, aim for bogons

Bogon Filter: where to configure *[b2/p60]* block bogons from the ingress start to save resources, i.e. external firewall rule

Bogon: Cisco IOS Filter Config *[b2/p61]* create access list config

Bootkit - Kon-Boot *[b4/p66]* hacking tool used by booting to a USB or CD, can log in to any local or domain cached account - prevent with FDE or locking down BIOS

Bring Your Own Device (BYOD) (MDM) *[b4/p127]* industry is pushing for BYOD, potential for significant org cost savings

Broken Windows Theory *[b1/p79]*

BYOAP - Bring Your Own Access Point *[b1/p93]* prevent with port-level security, detect: look for odd user agent string, look for NAT traffic

BYOD Revisited (MDM) *[b4/p137]* use MDM for policies, but MDM security fails in comparison to traditional system

Cc

Cain *[b1/p119]*

CAM Overflow *[b1/p112]* Content Addressable Memory (CAM) maintains map of MAC/Port pairs. Once CAM table is full, switches back to HUB mode (BAD) - tools like macof (part of dsniff) can flood

CanaryTokens.org (red herring) *[b5/p182]*

CAPTCHA *[b4/p23]*

Captive Portal (NAC) *[b5/p68]* passes initial authentication methods

Carrier-Grade NAT (CGN) *[b2/p73]*

CDP - Cisco Discovery Protocol *[b1/p72]*

CDP: Hardening Against Layer 2 Attacks *[b1/p109]* turn off with no cdp run, no cdp enable

Central Access Policies (Data Control) *[b4/p118]* CAP = central access policy, enforce logic across file servers - enforces business reqs at a global level

Central Intelligence Agency (CIA) *[b1/p84]*

Central Mgmt lockdown (Private Cloud) *[b4/p153]* user access needs to be strictly controlled, SSL communication should not be self-signed

Central Web Server Protection (Data Security) *[b4/p23]* Key advantage for WAF, possible to apply security policies across web servers

Centralized logging: Switches *[b2/p19]* config: Router(config) # logging 10.5.30.5

Centralized Protection (segmentation gateway) *[b5/p84]* internal firewalls provide centralized access controls, helps push filtering as close to source as possible

Centralized Security Approach (MDM) *[b4/p129]* enforce MFA, data should ONLY be accessed by corp resources

Certificate Authorities (CA) (ZT) *[b5/p39]* PKI composed of one or more certificate authorities - Root, Intermediate, Subordinate

Certificate Authority Authorization (CAA) (Network Encryption) *[b3/p163]* CAA requires a simple DNS record to operate - domain validation authorizes specific CAs for domain

Certificate Authority Types (ZT) *[b5/p40]* Standalone and Enterprise

Certificate Transparency Monitoring *[b3/p162]*

Certificate Transparency Monitoring (Network Encryption) *[b3/p162]* CAs are expected to generate public logs, provides near real-time notification of new certificates

CertSpotter *[b3/p162]*

CIS Cisco IOS Benchmark: L3 *[b2/p36]* categorized as Level 1 or Level 2, broken up into mgmt plane, control plane, data plane

CIS Control 1 (NAC) *[b5/p59]* NAC provides real-time enforcement of network access - performs both steps in CIS control 1, inventory of authorized and unauthorized devices

CIS Level 1 and Level 2 Benchmarks: L3 *[b2/p37]* Level 2 = need to evaluate, level 1 = good - implement level 1 and prove level 2

Cisco Best Practices: Layer 2 & 3 *[b2/p29]* summary: monitor, AAA, centralize logs, use secure protocols, netflow, config mgmt

Cisco Catalyst *[b2/p38]*

Claims (Data Control) *[b4/p112]* stored and configured within AD, AD admin center > DAC

ClamAV *[b2/p154]*

Classification is not Protection *[b4/p88]* classification = labels a file to help set limits on use, protection = uses encryption to protect data and clafficiations

Classless inter-domain routing (CIDR) *[b2/p73]*

Clean Source Principle (CSP) and AD Mgmt *[b3/p127]* states that a system can be dependent on a higher trust system but not a lower one - trust levels should talk to same trust levels or higher

Client Certificates (ZT) *[b5/p37]* requires clients to have certificates and a CA

Clifford Stoll *[b1/p21]*

Cloud access security brokers (CASB) *[b4/p167]* enforces security policies to cloud - enforcement through cloud connection points, integration with APIs

Cloud Based DLP *[b4/p100]* e.g. Office 365, Exchange, SharePoint, Macie

Cloud Encryption *[b4/p71]* verify encryption, protect data with access controls too

Cloud Flows *[b1/p145]* IaaS may support exporting flow data, AWS VPC Flow logging - can combine with netflow logging to see whole picture

Cloud Time Restrictions (Data Control) *[b4/p120]* requires on-prem AD synchronization to limit login times

Cloud vs On-Premise (malware detonation) *[b3/p93]* Cloud - integrates with NGFWs, on-prem - dedicated box or VM | best for both is to use a malware detonation appliance

Combating Open-Source Intelligence *[b2/p171]* Threat intelligence is taking the adversary by surprise

Communications Intelligence (COMINT) *[b1/p140]*

Compliance-Driven Security: Failed Mindset *[b1/p35]* Meeting compliance reqs becomes the goal, assessing without remediating

Compression & WAN Optimization (Remote Access) *[b3/p122]* a well-tuned SSL VPN can improve or stay equal to the performance of direct internet access even when tunneling traffic

Computer Emergency Response Team (CERT) *[b1/p26]*

Conditional Access (Data Control) *[b4/p115]* Dynamic access control - DAC enables logical operators

Conficker *[b1/p29]*

Configure NetFlow Exporters *[b1/p143]* config for Cisco NetFlow exporter

Configure Private VLANs *[b1/p135]* config for PVLANs

Container Escapse/Priv Escalation *[b4/p174]* risk of priv esc is greater with containers, container shares host kernel, possible to escape out of container into host

Container Impact *[b4/p173]* Pros vs Cons

Container Security Review *[b4/p180]* protect against container escape, limit container resources to prevent DOS, consider extra kernel security protection

Content Discovery Script example (DB Monitoring & Controls) *[b4/p40]* slide has script, loops through each db, table, and column and checks all values

Content Discovery: (DB Monitoring & Controls) *[b4/p39]* securing data requires knowing where data resides, you MUST perform content discovery on a regular basis

Content Service Switches (CSS) *[b2/p38]*

Control Groups (CGroups) (containers) *[b4/p176]* containers can consume entire host resources, limit resources on per container basis

Controlled Authentication (Remote Access) *[b3/p132]* purpose built remote access allows prevention and detection, e.g. domain admins must come from the jump box

Controlled Network Authentication (Remote Access) *[b3/p126]* remote access is more than external access - use BloodHound tool to help threat model

Corporate Workspaces (MDM) *[b4/p132]* policies typically require password or PIN, personal workspace = no security, corp workspace = policy enforced, limited apps

Course Goals *[b1/p5]* Secure design for infra, apps, and zero trust strategies. Become an All-Around Defender

Credential Rotation (ZT) *[b5/p22]* rotation is beneficial but requires proper password policies

Credential Rotation Review *[b5/p30]* rotating passwords helps to remove access, strong password enforcement necessary to limit risks of password rotation, consider password auditing, MFA highly recommended

Critical Assets *[b1/p47]* Identify and Prioritize critical assets

Crypto Suite Support (Network Encryption) *[b3/p164]* cipher suites are the encryption algorithms supported, tune for your systems

Cuckoo Sandbox (malware detonation) *[b3/p99]* open-source malware analysis platform, Henderson preferred

Cuckoo's Egg *[b1/p21]*

Cyber Kill Chain / Intrusion Kill Chain *[b1/p57]* RWDEICA | Recon, Weaponization, Delivery, Exploitation, Installation, C&C, Actions on Objectives

Cyber Kill Chain Countermeasures *[b1/p58]* Detect, Deny, Disrupt, Degrade, Deceive - (Table)

Dd

DA-R-I-OM Model *[b1/p65]*

DA-R-I-OM summary: Discover and Assess L1 & 2 *[b1/p156]* DA = physical inspection, rogue discovery, protocols, unused services, p2p traffic

DA-R-I-OM summary: Discover and Assess L3, 4 & 7 *[b2/p177]* IPv6 & network devices

DA-R-I-OM summary: Implement L1 & 2 *[b1/p158]* I = robust physical sec, color-coding cables, disable unused ports, MAC filtering, NAC, wireless isolation an PVLANs, VLAN ACLs, disable unused services, enable netflow on-prem and cloud

DA-R-I-OM summary: Operate & Monitor L1 & 2 *[b1/p159]* Track, don't set and forget - must detect for visibility

DA-R-I-OM summary: Operate & Monitor L3, 4 & 7 *[b2/p179]* manage routers over secure protocols, monitor L3, L4 attacks

DA-R-I-OM summary: Redesign & Implement L3, 4 & 7 *[b2/p178]* harden network devices

DA-R-I-OM summary: Redesign L1 & 2 *[b1/p157]* R = l2 prevention & detection controls, wireless protocols, l2 segmentation and authentication according to flow analysis, networking monitoring through span ports or taps

DAAS (segmentation gateway) *[b5/p80]* data, assets, applications, and services

Darknet Architecture *[b2/p66]* route all darknet traffic to a dedicated darknet router, monitor via SNMP

Darknet: what kind of traffic is sent? *[b2/p65]* all traffic sent to darknet is bogus - either misconfigured or malicious

Darknet: Why monitor? *[b2/p64]* Every request to a darknet is a misconfigured asset or malicious access

Data Access over the Network (Data Control) *[b4/p121]* Internal NGFWs can help enforce data access

Data diode *[b5/p107]*

Data Egress Analysis *[b1/p66]*

Data Encryption *[b4/p61]* encryption at rest protects data from disclosure

Data Encryption Review *[b4/p72]* significantly reduces risk of physical theft or accidental disclosure, multiple at rest strategies: DB, file, FDE, disk encryption tech also protects against bootkits: BigLocker, FileVault (Mac), VeraCrypt

Data Expiration (File Classification) *[b4/p83]* File mgmt tasks integrate with FCI (file classification infrastructure) - data expires based on conditions

Data Governance (File Classification) *[b4/p75]* impacted by file classification, DLP, info policy enforcement

Data Governance Review *[b4/p138]* requires multiple solutions, need a combo of data classification, DLP, policy enforcement, auditing, access controls

Data Loss Prevention *[b4/p95]* combination of content inspection and file context, such as file classifications: network, data at rest, endpoint

Data Loss Prevention Review *[b4/p104]* Most orgs own some level of DLP, tune what you have or explore commercial offerings

Data Masking (DB Monitoring & Controls) *[b4/p41]* xxx-xx-1242, allows certain business processes to continue - partial or full mask

Data Policies *[b4/p107]* control who, when, and where data is used - should include how data must be protected

Data Policy Review *[b4/p125]* data policies should enforce audit: who can access data, from what device, when data can be accessed, where data can be placed or be recieved from

Data Protection *[b4/p51]* Access control, encryption

Data Protection Policies (Data Control) *[b4/p124]* use policy enforcement around key data

Data Remanence (Public Cloud) *[b4/p164]* improper data deletion can allow recovery by another tenant, use data encryption, pay for cloud isolation, keep sensitive data on-prem

Data Security *[b4/p5]* Prior focus was just network security, architecture needs to focus on what matters most - our data

Database Activity Monitor (DAM)/Database Firewall (DBF) *[b4/p42]* DB monitoring fills gaps in DB security, adds prevention capabilities, apply controls based on requesting app

Database Encryption *[b4/p63]* DB level - use HSM/EKM (extensible key mgmt), table-level - encryption per table, cell level -encrypts data per specific columns

Database Logging *[b4/p36]* enable change tracking, common compliance criteria, trigger logs, query logs - consider performance issues

Database Monitoring & Controls *[b4/p35]* control who can access data, apply limits to data access, identify sensitive data locations, heavy detection focus

Database Monitoring & Controls Review *[b4/p48]* Expensive - so apply to crown jewels. Limit access, perform data discovery, log and monitor, alert and respond to abnormal data pulls

Database Security *[b4/p37]* built-in security is decent, restrict access, use custom views (saved queries)

Database Security Issues *[b4/p38]* DBs are commonly paired with web servers, creates a key security issue - either requires pass-thru or custom mode

DB Behavior Monitoring *[b4/p44]* DB security solutions use dynamic learning/behavior monitoring - combine with detections. Remember that an anomaly is not an alert, but high amount of anomalies can be an alert

DB Record Limits *[b4/p47]* DAM tracks record counts and can integrate with SIEM - alert on records pulled by source or app that exceeds threshold

DB User Context Awareness *[b4/p45]* DAM/DBF to identify actual user requesting data

DDoS *[b3/p137]* DDoS can target any org, attacks range from a few mins to hours or more - pay up or we'll take you out

DDoS Attack Types *[b3/p139]* Volumetric, Protocol, Application Layer - 70% of attacks use combination of the 3

DDoS Mitigation On-Prem *[b3/p150]* DDoS vendor or ISP is required for bandwidth attacks, use firewalls, reverse proxies, load balancers

DDoS Review *[b3/p151]* DDoS needs to be assessed in your org's risk strategy, on-prem solutions need to be tuned for DDoS protection

DDoS Scrubbing *[b3/p149]* cloud service for preprocessing data, e.g. cloudflare - acts as reverse proxy

De-Perimeterization *[b1/p31]* Rise of cloud, IoT makes this less effective (old = castle analogy) - newer = micro-perimeterization

Deep Packet Inspection (NGFW) *[b3/p7]* Looking at more than IP header info, intrusion prevention (requires payload analysis), URL filtering and web proxy inspection (dive into http/https headers)

Defaced/DoS-ed Cisco Switch with replaced startup config *[b2/p27]* 800 unique scanners looking for port 4768 and aounr 18k internet-exposed devices

Defensible Network Architecture *[b1/p22]*

Defensible Security Architecture *[b1/p21]* Coined by Richard Bejtlich, networks can be watched, limit an intruder's freedom to maneuver, offer a minimum number of services, be kept current

Defensible Security Architecture 2.0 *[b1/p22]* MICCMAC Model: Monitored, Inventoried, Controlled, Claimed, Minimized, Assessed, Current

Defensible Security Architecture Life Cycle DA-R-I-OM *[b1/p65]* DARIOM Model: Discover & Assess, Redesign, Implement, Operate & Monitor

Deficiencies (Traditional) *[b1/p25]* Emphasis on perimeter, most controls emphasize exploitation prevention, IoT, network-centric, compliance-driven security, resistance to change, new tech without analysis

Delegate DNS - Explicit Proxy *[b2/p150]* DNS query is performed by the proxy

Deployment Modes (DB Monitoring & Controls) *[b4/p43]* Local software installed on db server, reverse proxy in front of server, passive monitor out of band

DeT&CT *[b1/p45]* open-source framework for visibility on data sources, detection, and threat actors. Python tool, YAML files. Helps to prioritize where to be investigating more on

Detailed Tracking (audit policies) *[b5/p126]* generate vast amount of logs, proceed with caution

Detection Capabilities (red herring) *[b5/p172]* meaning of detection is based on attack source and dest, external or internal

Device and User Claim (Data Control) *[b4/p111]* user attributes = user claim, device attributes = device claim

DHCP Attacks Mitigation *[b1/p123]* enable dhcp snooping, ip dhcp snooping

DHCP Fingerprinting (NAC) *[b5/p63]* uses combination of MAC address and option 55, still spoofable but much harder than MAC

DHCP Starvation *[b1/p120]* attacker attempts to request all available DHCP addresses

Direct Memory Access (DMA) *[b4/p69]*

DISA - Zero Trust Pillars & Capabilities *[b5/p10]* user, device, network, application & workload, data, visibility, automation

DISA - Zero Trust Reference *[b5/p9]* ZT incorporates several areas that need to be smartly integrated

DISA STIG High severity 1, Layer 2 Benchmark *[b2/p33]* STIG steps severity 1

DISA STIG High severity 2, Layer 2 Benchmark *[b2/p34]* STIG steps severity 2

DISA STIGs *[b2/p32]* Freely available, guidance on switches and routers is legit

Discover & Assess: DSA Lifecycle DA-R-I-OM *[b1/p66]* Identify Reqs, assets in scope, business risk appetite, resources available, and practical threat modeling & risk analysis - i.e. Red Teaming emulating adversary, blue teaming collecting telemetry looking at detections and identifying where gap is

DLP Agent Bypass *[b4/p103]* admin access disable, uninstall, or bypass agent, defent with DLP is still better

DLP Agents *[b4/p102]* Agents provide a lot of capabilities for protecting data, requires agent deployed and running on all systems - consider performance impact

DLP Limitations *[b4/p99]* network DLP protects against basic data leakage, content inspection depends on cleartext visibility, does not mean network DLP is useless - it's proper hygeine

DLP with IDS *[b4/p97]* rules can look for specific content, IDS usually include sensitive data preprocessors

DLP with NGFW *[b4/p98]* positioned well for network inspection, IPS engine can be used just like IDS

DMZ Design *[b2/p123]* if multi servers break up into individual zones, PVLANs may also be used

DMZ: segmentation is more than 2 zones *[b2/p124]* security zones should consider: business and reg reqs, asset criticality, threats, risk appetite

DNS Zone file *[b2/p163]* sender policy framework

DNS Amplification Attack *[b3/p147]*

dnstwist *[b2/p169]* calculates permutations against a given domain, SMTP proxy can protect against cousin domains

Docker (containers) *[b4/p170]* uses Linux container (LXC) to run an app - abstracts software to run on minimal OS, one of the more common container solutions

Docker Content Trust *[b4/p177]*

Docker commit, Docker diff *[b4/p179]*

Docker Example *[b4/p172]* slide shows deploying docker container

Docker Hub *[b4/p177]*

Docker prevent unsigned images *[b4/p177]*

Domain-based message authentication, reporting, and compliance (DMARC) *[b2/p167]* verifies domain authentication via SPF or DKIM, will fail or pass message based on policy defined

DomainKeys Identified Mail (DKIM) *[b2/p165]* uses digital sigs to validate email, assym keys + hashing

Dridex (NSM) *[b3/p60]* Suricata can also use JA3, example shows Dridex match

dsniff *[b1/p112]* flood network with randomly generated MAC addresses, filling CAM table

Due Diligence (Public Cloud) *[b4/p165]* does the CSP provide SOC report, who has access to your corp data within the provider, do you have the right to audit or pentest your tenant

Duplicate Address Detection (DAD) *[b2/p90]*

Dynamic Access Control (DAC) (Data Control) *[b4/p109]* Microsoft uses DAC - uses groups + attributes to calculate level of access at request time

Dynamic ARP Inspection (DAI) *[b1/p119]* checks db before forwarding ARP responses

Dynamic Authorization (segmentation gateway) *[b5/p85]* abnormal conditions should be monitored and reacted to: temporal, geographical, behavioral, frequency

Ee

Effective Access (Data Control) *[b4/p117]* tests user and group access, view effective access to show permissions

Egress Analysis *[b1/p70]* Need to do in addition to Ingress analysis, aka Exfiltration Analysis or Extrusion Analysis

Electric Fence (NAC) *[b5/p72]* dynamic access = electric fence, electric shock results in an automated digital response

Email Data Control (Data Control) *[b4/p123]* Use policy to enforce, orgs often allow personal devices for email

Encapsulating security payload (ESP) *[b5/p44]*

Encrypted Data *[b4/p62]* most encryption solutions do not protect mounted data

Encrypted File System (EFS) *[b4/p64]* can be used to encrypt a user's files or folders, contents encrypted with symmetric key, symmetric key protected by asymmetric key

Encryption Issues (Network Encryption) *[b3/p156]* Malware uses encryption, encryption breaks current security investments

EveBox (NIDS) *[b3/p83]* Designed for Su ricata - provides web based alert and event mgmt tool

Evil Foca: IPv6 *[b2/p72]* tool used for IPv6 MITM

Explicit Proxy Advantages *[b2/p149]* malware is often not proxy aware, under an explicit proxy - this means no internet access, transparent proxy will have access | explicit proxy forces internet flow

Explicit Proxy Advantages - delegated DNS *[b2/p150]* DNS query is performed by the proxy

Extensible Key Mgmt (EKM) *[b4/p63]*

Exterior Gateway Protocol (EGP) *[b2/p9]*

Ff

Failed Mindset: All-Prevent Defense *[b1/p32]* Only rely on preventative controls, detection is afterthought

Failed Mindset: Compliance-Driven Security *[b1/p35]* Meeting compliance reqs becomes the goal, assessing without remediating

Failed Mindset: Introducing Tech Without Analysis *[b1/p36]* Shiny object syndrome, without considering alignment to business strategy

Failed Mindset: LAN or WAN is Secure *[b1/p30]* Thought is inside = trusted, outside = untrusted. Most layer 2, 3, 4 protocols have little or no built-in security. Weak - does not think attacker is already in

FAST (Data Control) *[b4/p113]* Flexible authentication secure tunneling

ffo2:: *[b2/p94]*

File Classification *[b4/p77]* identify key data and where it is expected, identify where it will end up, file classification adds tags to identify and control files

File Classification Acceptance *[b4/p76]* identify key data and where it is expected, identify where it will end up

File Classification Overview *[b4/p90]* Crucial to discover and classify data appropriately, more data = more risk

File Relocation (DLP) *[b4/p101]* files end up in unauthorized locations, DLP agents can find and handle exceptions: exception handling - move file to authorized location, notify user of policy violation and request cleanup

FileVault *[b4/p72]*

Filtering Flows *[b1/p148]* lower chance of duplicates and eliminate storing duplicates

Fingerbank (NAC) *[b5/p64]* online DHCP fingerprint database, contains thousands of DHCP fingerprints

Firefox *[b2/p35]*

Firewall Architecture *[b2/p122]* legs stem from firewall | 2 legged design - LAN + internet/WAN, 3 legged design - adding a DMZ port

Firewall Logging (Host Based Firewalls) *[b5/p57]* monitoring provides the capabilities to implement granular rules

Firewalls: Why they were created *[b1/p26]* ARPANET was globally flat, firewalls invented after Morris Worm

Flare (NSM) *[b3/p61]* Flare can analyze Zeek or Suricata flows to identify C2 beacons | RITA = real intelligence threat analytics

Flat Networks Fail *[b1/p27]* No segmentation in layer 3 or 4 at minimum. Allows intruder to reach large number of other systems, need segmentation to address this risk

Flexible Authentication Secure Tunneling (FAST) *[b4/p113]*

Flowbits (NIDS) *[b3/p76]* rules with flowbits cannot be disabled by disablesid.conf

Frameworks: Security Architecture *[b1/p53]* TOGAR, SABSA, O-ESA, and OSA - most of these focus on the WHAT vs the HOW

Full Disk Encryption (FDE) *[b4/p65]* FDE can protect against bootkit atacks

Full Stack Security (Data Security) *[b4/p7]* apps rarely involve a single component, securing the app means securing the stack: app, web server, db

Gg

Geolocation Blocking (NGFW) *[b3/p16]* block specific countries, add FQDN or IP exceptions as necessary

Global Unicast Addresses: IPv6 *[b2/p83]* Diagram for global unicast and ULA

Goal: Identifying the Unknown Unknowns *[b1/p67]* Donald Rumsfeld addressing NATO in 2002, e.g. IPv6 and QUIC (Google HTTPs over UDP) on network

Good Security Architect *[b1/p8]* Think Red, act Blue | Proj Mgmt Skills | Understand business reqs, reg landscape, threat landscape, IT landscape | Legit Comms | Zoom in and out of big picture (strategic) and individual (tactical) pieces

Google Auth *[b3/p116]*

Google Auth (Remote Access) *[b3/p119]* free MFA tool

gMSA - Group-Managed Service Accounts (ZT) *[b5/p29]* allows service account to work on multiple systems

Granular Auditing (Data Control) *[b4/p116]* Conditional access supports conditional auditing, use for rule staging

Group-Managed Service Accounts (gMSA) (ZT) *[b5/p29]* gMSA allows service account to work on multiple systems

Guest Management: Wireless *[b1/p97]* Disable management services on guest interfaces!

Hh

HALO (honeytokens against leveraging OSINT) (red herring) *[b5/p183]* fake users can be created publicly to combat recon

Hard-Coded MAC Addressess *[b1/p114]* simple, but high-maintenance

Harden Hypervisor (Private Cloud) *[b4/p152]* Turn off unused services and ports, enforce current TLS, remote logging, strong passwords, replace self-signed certificates

Hashing passowrds *[b2/p23]* config for Type 8 and Type 9 passwords

Hierarchy of Needs: IR *[b1/p61]* Inventory, Telemetry, Detection, Triage, Threats, Behaviors, Hunt, Track, Act

High Availability (HA) *[b3/p121]*

HMAC based and Time based one-time passwords (HOTP & TOTP) *[b3/p118]* HOTP uses secret key and counter to generate an HMAC, TOTP involves generating a pass that rotates based on time

HMAC SHA 256 *[b2/p10]*

Honeypots (red herring) *[b5/p175]* system designed only to be attacked and monitored, high interaction (real services) and low interaction (emulation

Honeypots Low Interaction (red herring) *[b5/p176]* justin recommends - easy to set up, two modern frameworks include Modern Honey Network MHN and T-pot

Honeypots Redirecting (red herring) *[b5/p177]* internal-only honeypot should see more than scans, can do redirects

Honeytokens (red herring) *[b5/p178]* fake objects or content is helpful for identifying unauthorized activity, sometimes called canarytokens

Honeytokens Against Leveraging OSINT (HALO) *[b5/p183]*

Honeytokens file auditing (red herring) *[b5/p179]* enable file auditing using windows GPO or Linux auditd

Honeytokens Security Access Token (SAT) *[b5/p180]* lateral movement usually from cred compromise, mimikatz, DCEPT

Host Based Firewalls *[b5/p53]* provide granular controls, Windows comes with Windows Defender Firewall, Linux includes iptables and wrapper like ufw

Host Based Firewalls Capabilities *[b5/p54]* endpoint firewalls include prevention & auditing, outbound defaults to allow and inbound to deny

HOTP *[b3/p118]*

hping - wormhole *[b2/p13]* hping -s -p80 sensitive.sec530.com

HSTS (Network Encryption) *[b3/p159]* HSTS requires setting HTTP header, upgrades HTTP links to HTTPS automatically

HSTS Preloading (Network Encryption) *[b3/p161]* header must include subdomains, age over 1 year, and preload - slide shows config

HTTP DDoS Mitigation *[b3/p146]* Tune web server settings, implement Varnish, reverse proxy

HTTP Strict Transport Security (HSTS) (Network Encryption) *[b3/p159]* HSTS requires setting HTTP header, upgrades HTTP links to HTTPS automatically

Hyper-converged storage (Private Cloud) *[b4/p154]* Limit SSH to only other controllers

Hypervisor Migration (Private Cloud) *[b4/p144]* hypervisors are capable of migrating live VMs from one hypervisor to another, separate physical NICs ideal or dedicate VLAN

Hypervisor Networking (Private Cloud) *[b4/p142]* networking breaks down into high-level functions: VM networking, storage network, migration network, mgmt network

Hypervisor Security (Private Cloud) *[b4/p148]* use hypervisor firewall and authentication restrictions, add network-based firewalls

Hypervisor-Based Endpoint Protection *[b4/p157]* endpoint security solution installed as VM; capabilities fail in comparison to agent within VMs

Hypponen's Law *[b1/p33]* Whenever an appliance is described as being smart, it's vulnerable

Ii

IaaS Network Visibility (Public Cloud) *[b4/p162]* AWS and Azure released VPC traffic mirroring and Azure vTAP in 2019

IBM AIX *[b2/p35]*

ICAP Diagram *[b2/p156]* performs web AV checks, malware detonation, content filtering

Identify Access Management (IAM) (Remote Access) *[b3/p133]* often used for federation and single sign-on (SSO)

Identify Mismatches Between Adversary & Organizations Strategy *[b1/p44]* Use MITRE ATT&CK Navigator, overlay TTPs with org capabilities for visibility, identify gaps in coverage > help to prio defense strategy based on threat intel data

Identifying Adversary: Think Red *[b1/p43]* MITRE ATT&CK provides public repo of threat groups including intent and capabilities

IDS Default Config (NIDS) *[b3/p77]* expect tons of FPs by default, true power = customizing to your environment

IDS Rule Priorities (NIDS) *[b3/p78]* default to classtype, alert defaults to low priority, changing this for all IDS rules = painful

Implement: DSA Lifecycle DA-R-I-OM *[b1/p74]* harden at each layer, enable logging, determine baseline, validate implementation

Improper Sharing (Public Cloud) *[b4/p166]* most breaches in cloud come from poor security practices, auditing of data and policies is a MUST

Inbound Access (Host Based Firewalls) *[b5/p55]* Orgs should only allow connections to authorized services, log inspection can provide list of executables and ports

Inbound Rules (NGFW) *[b3/p20]* Lock down all inbound service requests, apply to one system or application group at a time

Incident Response - The IR Hierarchy of Needs *[b1/p61]* Inventory, Telemetry, Detection, Triage, Threats, Behaviors, Hunt, Track, Act

Inline Malware Detonation *[b3/p94]* sandbox can sit inline on network, protection is not real-time, setting delay for analysis is configurable

Integration with Other Systems (malware detonation) *[b3/p104]* use findings to enhance other solutions - NGFW AV, Endpoint AV, Allow Lists, NGFW URL Filtering

Intentional Email Modification *[b2/p170]* SMTP proxies and email systems can add to a message

Intermediate system-to-intermediate system (IS-IS) *[b2/p9]*

Internet Content Adaptation Protocol (ICAP) *[b2/p155]* used to extend the capabilities of a proxy, provides AV

Internet of Things (IoT) *[b1/p33]* Low-cost internet-enabled devices, if it's described as smart - it's vulnerable

Intra-site automatic tunnel addressing protocol (ISATAP) *[b2/p107]*

Introducing Tech Without Analysis: Failed Mindset *[b1/p36]* Shiny object syndrome, without considering alignment to business strategy

Inventory Automation (segmentation gateway) *[b5/p82]* key tp MCAP grouping is device and user integration

IP Fragmentation *[b1/p23]*

IPSec revisited *[b5/p42]* IPSec is Layer 3, network layer protocol - allows transparent encryption and authentication

iptables *[b2/p99]* input filter example

Iptables Simple Rulset *[b2/p129]* Ruleset for two-legged firewall

IPv4 Multicast Addresses *[b2/p94]* ipv6 does not support broadcast and uses multicast, uses ff00::/8 for multicast

IPv4 vs IPv6 *[b2/p75]* addresses are 32bits vs 128bits long, ipv6 offer massively larger address space

IPv4: Nearly Exhausted *[b2/p73]* Must pay for address IPv4 blocks, all major blocks have been issued - so IPv6 is growing quickly

IPv5 *[b2/p75]* used for research, never adopted

IPv6 & Evil Foca - threats and red team scenario *[b2/p72]* neighbor advertisement spoofing, SLAAC attack, fake DHCPv6, tunneling - for MITM

IPv6 - Discover & Assess *[b2/p71]* can generate IPv6 traffic unless explicitly disabled, needs to be examined and assessed in networks

IPv6 ::1, fc00::/7 *[b2/p93]* ::1 = Ipv4 local 170.0.0.1, fc00::/7 = reserved for unique local addresses (ULA)

IPv6 address format *[b2/p83]* Diagram for global unicast and ULA

IPv6 Address Types *[b2/p82]* Link-local, unique local addresses (ULA), global unicast

IPv6 Addresses *[b2/p80]* uses colon-separated hexadecimal valules, repeated zeroes = " :: "

IPv6 Asset Inventory with Rumble Network Discovery *[b2/p104]* new infosec tool used for network mapping

IPv6 Assigning Addresses *[b2/p95]* Methods: static, SLAAC (stateless), DHCPv6 (stateful & stateless) - DHCPv6 does not assign default gateway, come from the router itself

IPv6 Discovery Tools *[b2/p105]* Zeek, Firewall loge, netflow data, IDS rules, ACls, SNMP MIBs

IPv6 Discovery Tools, Native OS *[b2/p102]* Windows ping, linux ping6, maxOS ping6 , slide has commands table

IPv6 Effect of Temporary Addresses *[b2/p92]* addresses change over time, most orgs use DHCP, slide has commands to check local default lifetimes

IPv6 Extension Headers 1 *[b2/p78]* First header always 40 bytes long, max chain size is unlimited - can lead to attacks

IPv6 Extension Headers 2 *[b2/p79]* Diagram of headers

IPv6 Firewall Support *[b2/p99]* Some firewalls cant support IPv6, i.e. Linux iptables firewall does not - but ip6tables does | firewalls that support IPv6 are often laxer than IPv4 firewalls

IPv6 Header *[b2/p76]* larger (and simpler) than IPv4 header (shown in notes), IPv6 omits checksums, always a fixed legnth - 40bytes

IPv6 Header Fields *[b2/p77]* Version, traffic class, flow label, payload length, next header, hop limit, src and dst IP addresses

IPv6 Hurricane Electric *[b2/p114]* ipv6 training and hands on

IPv6 Network Allocations *[b2/p84]* allocated to orgs by Regional Internet Registries, ULAs generated randomly

IPv6 Privacy Extension and Temporary Addresses *[b2/p88]* used by most orgs, ubuntu config in slide

IPv6 Privacy-Enhance address Generation *[b2/p90]* Duplicate Address Detection (DAD), RFC 4941

IPv6 Redesign & Implement *[b2/p115]* follow NIST SP 800-119, know capabilities of prevention and detection tools, conifugre devices to block/alert on protocol 41, log protocol 41 and UDP 3544, use RA guard

IPv6 Rogue Router Attack *[b2/p112]* Diagram, rogue ipv6 router attack

IPv6 Scanning *[b2/p101]* different than ipv4, would take forever to scan each host, does not use ARP

IPv6 Securing *[b2/p97]* NIST 800-119

IPv6 Security Issues *[b2/p98]* Windows uses IPv6, may not be able to ignore, scanning is challenging, robust tunneling options

IPv6 SLAAC example *[b2/p86]* Diagram, uses MAC address to determine IPv6 address - can result in privacy issues

IPv6 Stateless Address Auto Config (SLAAC) *[b2/p85]* system can independently determine its IPv6 address, can create privacy concerns

IPv6 Subnet Size *[b2/p81]* default subnet size is a /64, 18+ quintillion addresses

IPv6 Temporary Address Lifetime *[b2/p91]* ipv6 have preferred lifetime and a valid lifetime, slide has commands to view lifetimes

IPv6 Tunneling Options *[b2/p107]* Many types, can be used to bypass or evade - slide has list

IPv6 Tunneling Prevent and Detect - protocol 41 *[b2/p108]* identify protocol 41, configure to block and alert on protocol 41 - slide has snort rule

IPv6 Ubee Firewall *[b2/p100]* Cannot block inbound ICMPv6 - more lax than IPv4 firewall, any protocols can be used for tunneling

IPv6 Ubuntu Privacy Extension before and after *[b2/p89]* Shows global and ULA added with extension

IPv6 Unauthorized Router Advertisements (RA) *[b2/p111]* use RA (router advertisements) Guard to mitigate this risk

IPv6: 1 system, 6 IP addreses *[b2/p87]* macOS High Sierra Diagram

IPv6: Growing Fast *[b2/p74]* 33% global adoption, microsoft uses it a lot

IPv6: prevent & detect via IPv4 tunnels with cisco *[b2/p110]* Cisco IOS ACL will allow and log procotol 41 and UDP port 3544 traffic, deny 41

IPV6: Teredo Tunneling *[b2/p109]* Developed by Msoft, uses UDP 3544, detect and block/alert teredo

ISP DDoS Protection *[b3/p141]* ISP can help mitigate attack, may be included in contract, possible to purchase dynamic bandwidth capabilities

Jj

JA3 (NSM) *[b3/p58]* JA3 = technique for creating SSL client fingerprints from the pre-encryption handshakes of the SSL protocol

Journey to Zero Trust *[b1/p13]* 1: Models and Principles, 2: Network Hardening Ingress/Egress Control, 3: Apps Network Centric, 4: Apps Data Centric, 5: Zero Trust

Jump Box Connection Options (Remote Access) *[b3/p130]* RDP, Virtual Desktop Infrastructure (VDI)

Kk

Kerberos Armoring (Data Control) *[b4/p113]* Kerberos vulnerable to MITM and brute force attacks, use FAST

Key chains [b2/p10] given lifetime to auto rotate keys

Kibana SIEM Integration (NIDS) *[b3/p82]* Central location for storing and searching log data, integrate with Kibana for dashboards

Kill Chain *[b1/p54]*

Kon-Boot (bootkit) *[b4/p66]* hacking tool used by booting to a USB or CD, can log in to any local or domain cached account - prevent with FDE or locking down BIOS

Ll

LAN/WAN is "Secure" *[b1/p30]* Thought is inside = trusted, outside = untrusted. Most layer 2, 3, 4 protocols have little or no built-in security. Weak - does not think attacker is already in

Lateral Movement Attacks (Remote Access) *[b3/p128]* main issue with remote access is credential theft and reuse, cleartext password retrieval, hash dumping/token smuggling

Layer 1 Mitigations *[b1/p88]* have physical security, Turn off ports not in use, use MAC filtering, 802.1X, or NAC

Layer 1: Physical Access *[b1/p85]* secure physical access to the network, systems, and facilities

Layer 2 and 3 Benchmarks and Auditing Tools *[b2/p28]* Cisco best practices, autosecure, DISA STIGs (defense info systems agency, security technical implementation guide), CIS, Nipper-ng

Layer 2 Attacks: ARP *[b1/p116]* ARP spoofing, poisoning, MitM

Layer 3 Attacks & Mitigation *[b2/p8]* Attacks: MitM, unauthorized routing updates, Wormhole attacks (unauthorized tunneling)

Layer 3 Auditing Tools *[b2/p38]* CIS Router Audit Tool (RAT) = old, CIS-CAT Pro = new - 80+ benchmarks, requires $$ | Nipper can be used free

Layer 3 Benchmarks *[b2/p35]* CIS, STIGS

Legacy Services: Switches *[b2/p18]* Disable legacy service list and config

Less Rules May be More (NGFW) *[b3/p17]* Allow authorized connections, rules should balance between security and usability

Let's Encrypt (Network Encryption) *[b3/p158]* Free, automated, and open CA - malware can have trusted certifiacte

Leveraging Encryption (Network Encryption) *[b3/p157]* encrypt everything = increase risk, encryption should be deliberate and calculated

Lifecycle: Discover & Assess DA-R-I-OM *[b1/p66]* Identify Reqs, assets in scope, business risk appetite, resources available, and practical threat modeling & risk

analysis - i.e. Red Teaming emulating adversary, blue teaming collecting telemetry looking at detections and identifying where gap is

Lifecycle: DSA Overview DA-R-I-OM *[b1/p65]* DARIOM Model: Discover & Assess, Redesign, Implement, Operate & Monitor

Lifecycle: Implement DA-R-I-OM *[b1/p74]* harden at each layer, enable logging, determine baseline, validate implementation

Lifecycle: Operate & Monitor *[b1/p75]* Continuous security monitoring: data at rest and motion, continuous awareness, maintain threat-focused ops, and augment visibility based on threat intel and IR lessons learned

Lifecycle: Redesign DA-R-I-OM *[b1/p73]* Identify desired state, determine gap, roadmap - documentation | architect decisions are threat focused covering protection, detection, and reaction (P > D + R)

Link Local Multicast Name Resolution (LLMN) *[b2/p94]*

Linux Containers (LXC) *[b4/p170]*

Linux iptables *[b2/p128]* support per-interface input, output, and forward filter chains

Linux Logs (audit policies) *[b5/p130]* syslog is primary method of logging for linux/unix - default log location is /var/log/

Linux Permissions (Data Protection) *[b4/p56]* support basic permission sets (r, w, x) | r = 4, w = 2, x = 1, 6 = r+w | 741 = owner has read, write, and execute; group has read; and everyone has execute

Linux Special Permissions (Data Protection) *[b4/p57]* be careful with SUID (set user ID), attackers use for priv esc

LLDP - Link Layer Discovery Protocol *[b1/p72]*

Local Admin Password Solution (LAPS) (ZT) *[b5/p27]* Free Microsoft tool, automatically rotate local admin password, LAPS is centrally controlled via AD

Local Jump Box (Remote Access) *[b3/p131]* can localize jump box with virtualization, physical host needs to be the secured OS, host OS has full access to VM disks and full memory visibility

Lock Down Basic Ports (NGFW) *[b3/p15]* restrict simple ports to their corresponding apps: 25, 53, 123, 465, 993, 995 - slide has list

Lockdown Mode (Private Cloud) *[b4/p151]* prevents root-level remote access, console access always has full admin rights

Log Agents (Log Collection) *[b5/p107]* provide additional functionality: auto-parsing, log rotation, log buffering, prioritization, filtering - slide has full list

Log Collection *[b5/p97]* typically done with log agents or agentless, network devices often use syslog

Log Collection Summary *[b5/p118]* multiple ways to send or receive logs: agentless, SIEM, 3p agents, system built-in agents, scripts - a strong design likely involves a combo

Log Enrichment (SIEM) *[b5/p92]* adds more context for better analysis, alerting

Log Inspection (SIEM) *[b5/p91]* all systems and network access needs to be verified, SIEM collection and analysis is recommended

Loopback Interface *[b2/p20]* used as a dedicated management IP address, shows config

LXC (containers) *[b4/p171]* the middle between a chroot and a full-fledged vm, uses Linux kernel capabilities to contain processes

Mm

MAC authentication (NAC) *[b5/p62]* not authentication, easy to spoof - should/can be combined with 802.1x

MAC Limiting and Sticky MAC Addressess *[b1/p115]* Limits how many MAC addresses may be associated with one port, stick = switch will learn MAC address of each connected system

MAC Spoofing *[b1/p111]* Diagram

macof *[b1/p112]* flood network with randomly generated MAC addresses, filling CAM table

macOS High Sierra IPv6 *[b2/p87]* macOS High Sierra Diagram

Maintenance Operation Protocol (MOP) *[b2/p18]*

Malicious Images (containers) *[b4/p177]* use docker Content Trust, only allows signed docker containers to run - alternative to signing is using Automated Build images

Malware Behavior Analysis *[b3/p92]* Registry key monitoring, dropping files, persistence mechanisms, network access, memory analysis, process analysis

Malware Detonation *[b3/p90]* Passing malware to dedicated sandbox to analyze and monitor for behaviors, provides scoring

Malware Detonation Network Access Considerations *[b3/p101]* reacts differently based on the network design, slide contains table

Malware Detonation Review *[b3/p105]* Behavioral analysis + signature based detections, detection in depth, prevention in depth

Malware Detonation Workflow *[b3/p91]* file/url submitted > AV and reputation DBs run checks > run file or access URL using a sandbox

malwr.com *[b3/p99]*

Managed Security Service Provider (MSSP) *[b1/p32]*

Managed Service Account (MSA) (ZT) *[b5/p28]* special service account dedicated to one system, password rotated same way computer accounts are, MSA set per computer with PowerShell

MANGLE *[b2/p128]*

MCAP and Network Agent (segmentation gateway) *[b5/p81]* MCAP and access should be based on network agent

MDM Example Policy, WIP *[b4/p135]* Windows Information Protection for Android Device

MDM Example, WIP *[b4/p136]* Results of WIP on Android

Meraki Air Marshall *[b1/p94]* Commercial WIPS

Methods of Securing Transmission (ZT) *[b5/p34]* TLS, IPsec, 802.1x, single packet authorization (SPA) --- TLS and IPsec provide authentication and encryption

MICCMAC Model *[b1/p22]* MICCMAC Model: Monitored, Inventoried, Controlled, Claimed, Minimized, Assessed, Current

Micro core and Perimeter (MCAP) (segmentation gateway) *[b5/p79]* creates logical zones of trust and functionality - full design should include intra-zone connections

Mindset of DSA *[b1/p23]* Build it once, build it right. Bake security in at the beginning, rather than retrofitting later

Mirai (DDoS) *[b3/p138]* Brian Krebs was victim of one of the largest DDoS attacks ever, came from Mirai botnet. Mirai scanned internet for IoT devices with default creds

Mitigations DHCP Attacks *[b1/p123]* enable dhcp snooping, ip dhcp snooping

MITRE ATT&CK Matrix *[b1/p42]* Wikipedia of attacker's behaviors, describes tactics, techniques, procedures (TTPs)

MITRE ATT&CK Matrix *[b5/p145]* actionable framework that described adversary techniques in detail

MITRE ATT&CK Repo *[b1/p43]* MITRE ATT&CK provides public repo of threat groups including intent and capabilities

MITRE Cyber Prep 2.0 *[b1/p41]* Threat Model, Purple Teaming

MITRE Engage and Att&CK MAppings (red herring) *[b5/p167]* shows how red herring techniques can be adopted

Mobile Device Management (MDM) *[b4/p131]* abstracts corp resources from personal use and access - uses either corp workspace approach or app containerization

Mobile Centralized Approach (MDM) *[b4/p128]* treat all BYOD untrusted, data never leaves corp data center, data is accessed using corp controlled access methods

Mobile Issues (MDM) *[b4/p130]* BYOD does not have enforced local security, mobile malware - keyloggers, screen scarping, SSL spoofing

Models Focused on Security Threats *[b1/p54]* Time-Based Security, Intrusion Kill Chain and MITRE ATT&CK, IR and Hierarchy of Needs, Zero Trust Model (Forrester)

Models, Standards, Frameworks, and Best Practices *[b1/p52]* help minimize possibility of missing or forgetting a component in a security architecture

Modern Alternatives to VPN - ZTNA and SDP *[b3/p125]* ZTNA or SDP (software defined perimeter) provides access to an application or resource - not an entire network

Modern Honey Network (MHN) *[b5/p176]*

Modifying User Agents (red herring) *[b5/p173]* proxy modification can be used to protect clients

ModSecurity - WAF (Data Security) *[b4/p16]* open source WAF, slide has rule syntax

MongoDB *[b2/p35]*

Monlist DoS (NTP) *[b2/p56]* commands

Morris Worm *[b1/p26]*

Moving Files (File Classification) *[b4/p84]* restrictions can be applied to documents using properties

MS08-067 *[b1/p29]*

Multicast Listener Discovery (MLD) *[b2/p103]*

Multifactor Authentication (Remote Access) *[b3/p117]* Something you know, have, are

Multitenancy (Public Cloud) *[b4/p163]* most breaches occur from bad customer implementations - accessing hypervisor is game over, meltdown and spectre (cpu vulnerabilities)

Mutual TLS (mTLS) (ZT) *[b5/p36]* slide has steps

Nn

NAC core capabilities *[b5/p61]* authenticate devices various ways: 802.1x port auth, MAC address OUI (org unique identifier), DHCP fingerprint

NAC Deployment *[b5/p60]* initial connect -> authentication via RADIUS -> enter Prod VLAN or unauth VLAN -> DHCP request to NAC -> DHCP response -> client gets captive portal

NAC deployment considerations *[b5/p67]* Inline & Out-of-band pros and cons -- OoB is better

NAC Example *[b5/p65]* Authorized vs Unauthorized

NAC Inline vs out-of-band *[b5/p66]* diagram - better to have NAC out of band

NAC Problems *[b5/p73]* orgs are restricted by time and money, even if deployed - likely to not be deployed everywhere - other means of device discovery are needed

Navigator: MITRE ATT&CK *[b1/p44]* Use MITRE ATT&CK Navigator, overlay TTPs with org capabilities for visibility, identify gaps in coverage > help to prio defense strategy based on threat intel data

Neighbor Authentication: Routers *[b2/p11]* Config of EIGRP

Neighbor Control Protocol (NCP) *[b2/p102]*

NetFlow *[b1/p142]* summarizes network traffic, based on frame and packet headers

NetFlow Cloud *[b1/p145]* IaaS may support exporting flow data, AWS VPC Flow logging - can combine with netflow logging to see whole picture

NetFlow Components *[b1/p149]* Requires exporter, collector, analyzer

NetFlow Data Sources *[b1/p139]* obtained from network equipment and network monitoring

NetFlow Design *[b1/p152]* where to implement exporters to obtain full environment coverage - need to use combination of different flows

NetFlow Exporters Configure *[b1/p143]* config for Cisco NetFlow exporter

NetFlow Intro *[b1/p141]* open standard created by Cisco,

NetFlow Planning *[b1/p144]* Diagram, plan to stop duplicates

Network Access Control (NAC) *[b5/p59]* NAC provides real-time enforcement of network access - performs both steps in CIS control 1, inventory of authorized and unauthorized devices

Network Access Control Review *[b5/p74]*

Network Agent (segmentation gateway) *[b5/p76]* in ZT, identity is the new perimeter - a network agent is a user and device combined -- used to determine authorization

Network Attack Surface Analysis *[b1/p69]* Internet connections, Mobile, IoT, Cloud, VPN, remote access, Modems, Wireless, ICS

Network Closets: Physical *[b1/p84]* Paramount to secure, beyond authentication - accountability should be enforced and auditable, shared demarcs can be problematic

Network Encryption *[b3/p154]* Good = it secures traffic, Bad = malware goes undetected or trusted

Network Encryption Review *[b3/p171]* Bolster with HSTS, CAA, cipher suites, TLS config, visibility is critical for security devices - SSL inspection and SSL decrypt mirroring

Network Flow Data *[b1/p140]* help achieve the goal of Know Thy Network

Network Flows *[b1/p138]* log of connections between systems, flow data easily identifies the connection | high level info of what's occurring on the network

Network Intrusion Detection (NIDS) *[b3/p65]* find evil device, 3 methods: signature, anomaly, protocol analysis | sig and protocol analysis have fewer FPs

Network Metadata (NSM) *[b3/p37]* Allows for learning the environment and identifying abnormal events, unauthorized assets, vulnerable or misconfigured assets

Network Monitoring Visibility (NSM) *[b3/p27]* Out of Band (option 1): purpose is detection, Inline (Option 2): purpose is detection and prevention

Network Policy Server (NPS) *[b5/p70]*

Network Security Monitoring (NSM) *[b3/p25]* not a product, its a mindset - asset discovery and identification, vulnerability identification, NIDS, network metadata capture and analysis, packet captures

Network Security Monitoring Review *[b3/p84]* Many capabilities: identify C2, passive network log generation, packet capturing, alert investigation interfaces | NSM requires investment in people and time

Network Storage (Private Cloud) *[b4/p143]* SAN and NAS require network access, unauthorized access to storage = fail, dedicated network is recommended

Network Taps 1 (NSM) *[b3/p30]* offer more robust sniffing option, will send all frames to the monitoring port(s), including malformed frames

Network Taps 2 (NSM) *[b3/p31]* slide shows multi-aggregation tap picture

Network Traffic Analysis (NTA) Architecture (NSM) *[b3/p39]* Key interest is the metadata aggregator

Network Visibility Analysis *[b1/p71]* Identifying network blind spots for our NIDS, NIPS, full packet capture, NetFlow, etc. | Can malware pivot from one system to another without being seen by any of the controls?

Network Visibility Analysis *[b1/p66]*

Network vs Access Segmentation *[b2/p120]* network vs access controls, micro segmentation - within the system itself

Network-Based DLP *[b4/p96]* Be careful of encryption blindness - network systems with DLP capabilities: NGFW, WAF, DBF, NSM, IDS

Network-Centric Architecture *[b1/p34]* Security Architect often applied narrowly to network architecture, recent attacks have moved to host via Layer 7 - need to take broader view of architecture

Next Gen Firewall (NGFW) *[b5/p3]* Layer 7 firewall, can make decisions based on application level inspection

Next Gen Firewall Capabilities *[b3/p6]* Deep packet inspection, user-based rulesets, SSL/SSH inspection, Reporting, strong logging, geolocation, SDK support

Next Gen Firewall Quick Wins *[b3/p14]* Network antivirus, block subnets/user accounts that ado not need internet access: service accounts, privileged users, servers/key workstations or devices

Next Gen Firewall Review *[b3/p22]* L7 controls greatly increase security, heave emphasis placed on outbound rules

Next Gen Firewall Rule Counters *[b3/p12]* A rule counter increments each time a firewall rule has a match. Use report to identify all outbound ports, if default deny rule is hit - you are missing something

Next Gen Firewall Rule Implementation Suggestions *[b3/p11]* 1 - Port-based, 2 - Quick wins, 3 - Long-term goal

Next Gen Firewall Rulesets *[b3/p10]* show allow all authorized connections

NFdump *[b1/p150]*

NFdump collector *[b1/p150]* netflow collector

NFsen *[b1/p150]*

NfSen NetFlow Analyzer *[b1/p150]* relies on RRDTool to generate graphs

NIDS/NIPS Rules *[b3/p74]* too many rules, maintaining rules on an IDS or IPS is a major task - need to architect with segmentation in mind and classification of users, assets, zones

Nipper-ng *[b2/p39]* parse local text file (router config saved locally), outputs to HTML high quality report

Nipper-ng Report *[b2/p40]* Provides specific syntax advice

NIST 800-207 *[b5/p28]* Zero Trust Architecture Reference

NIST 800-119 *[b2/p97]* Securing IPv6

NIST 800-141: firewalls *[b2/p122]* guidelines to firewalls and firewall policies

NIST 800-63B (ZT) *[b5/p21]* states password rotation not recommended, should force change if there is evidence of compromise of the authenticator

Nortel *[b2/p38]*

NotPetya Case Study *[b1/p29]* Part of NSA malware leaked tools, including ETERNALBLUE. Targeted SMB

nprobe *[b1/p149]*

ntopng *[b1/p151]* Like Splunk, ELK (elastic stack), ntopng contains dashboards

NTP Amplification Attacks *[b2/p55]* udp-based services can be used for spoofed DoS attacks, cloudflare description on slide | turn off monlist

NTP Authentication *[b2/p54]* prefer Stratum server, NTP is sent over UDP, supports authentication

NTP Design *[b2/p53]* diagram and minimal ntpd config

NTP Monlist DoS *[b2/p56]* commands

NTP, securing *[b2/p52]* Implement time correctly, alert on time changes, set max tolerance for computer clock sync to 5mins

NTP Stratum *[b2p54]* level indicates proximity

ntpdc *[b2/p55]*

Number Resource Organization (NRO) *[b2/p60]*

Oo

Object Access (audit policies) *[b5/p125]* one of the most misunderstood settings, audit file system does not log all file access

OneDrive *[b4/p68]*

Open Source Log Agent Capabilities (Log Collection) *[b5/p113]* multi platform, lots of features, open source

OpenVPN *[b3/p109]* Modern VPNs use TLS, usually supports post-authentication checks - e.g. OpenVPN

OpenVPN *[b2/p107]*

Operate & Monitor: DSA Lifecycle DA-R-I-OM *[b1/p75]* Continuous security monitoring: data at rest and motion, continuous awareness, maintain threat-focused ops, and augment visibility based on threat intel and IR lessons learned

Operationalizing Network Logs (NSM) *[b3/p40]* Decentralized vis Scripts, Centralized via SIEM

Optical Character Recognition (OCR) *[b4/p82]*

Optical Character Recognition (OCR) Integration *[b4/p82]* File classification supports OCR of TIFF (faxes and scans), can be integrated into automatic classification with powershell

Organizational Awareness (Data Security) *[b4/p6]* know your assets, network security build a security moat, data security secures the treasure in the caslte

OSPFv2 *[b2/p10]*

Outbound Access (Host Based Firewalls) *[b5/p56]* Win & Linux have thousands of binaries per system, only authorized binaries should make connections - should limit authorized apps to their expected use cases

OWASP *[b4/p11]*

OWASP Top 10 (Data Security) *[b4/p12]* WAF has strong focus on mitigating OWASP Top 10, IPS of NGFW mitigate basic versions of the top 10 attacks but are not designed to handle HTTP as deeply

Pp

PaaS *[b4/p71]*

Packet Captures (NSM) *[b3/p34]* network sensors listen promiscuously to network traffic, "pcaps or it didnt happen"

PAD *[b1/p79]* Packet Assembler/Deassembler - service used by X.25 links

Pafish (malware detonation) *[b3/p102]* poc on how malware detects VM status

Palo Alto *[b2/p35]*

Password Auditing (ZT) *[b5/p25]* should be evaluated for weaknesses, possible to intentionally dump hashes and test them - linux hashes in /etc/passwd and /etc/shadow

Password Fails (Remote Access) *[b3/p114]* Dictionary attack, password spraying, botnet tunneling

Password Hashes: Type 5, 8, 9 *[b2/p22]* 5 = salted MD5, 8 = PBKDF2 - SHA256, 9 = SCRYPT

Password Policies (ZT) *[b5/p23]* rotation increases chance of user picking weak passwords, windows supports fine-grained password policies

Passwords Types *[b2/p21]* use strong passwords - use Type 5, 8, or 9

Path MTU discovery (PMTUD) *[b1/p23]*

Payload Inspection Issues *[b3/p89]* L7 payload inspection works for AV, IDS/IPS, URL Filtering

PBKDF2 *[b2/p21]*

PCI DSS *[b1/p35]*

Perfect Forward Secrecy (PFS) (Network Encryption) *[b3/p167]* negotiates an encryption key using Diffie-hellman, symm key changes per client/server session, even if private key is compromised prior sessions are unlikely to be decrypted

Perimeter Defense *[b1/p20]* Good in 1990, crunchy shell around a soft, chewy center. Hard on the outside, soft on inside. Flat networks with little or no segmentation. Hardened perimeter, but weak/unpatched internals

Perimeter Security & Need for Zero Trust *[b5/p5]* perimeter security was not built with "assume breach in mind"

pfSense Console *[b2/p127]* console commercial quality with GUI

Physical - Discover & Assess *[b1/p80]* Physical inspection, can someone come over the wall

Physical - Network Closets *[b1/p84]* Paramount to secure, beyond authentication - accountability should be enforced and auditable, shared demarcs can be problematic

Physical - Redesign & Implement *[b1/p89]* Robust physical security, color code cables, track all people with access to equipment, secure doors, background checks, SANS paper - Physical Security and Why It Is Important

Physical - Threats *[b1/p83]* Physical access violation

Physical Access: Layer 1 *[b1/p85]* secure physical access to the network, systems, and facilities

Physical Security: Layer 1 *[b1/p79]* Design from the ground up

Physical Separation (Private Cloud) *[b4/p150]* separate hypervisor deployments should be considered based on data sensitivity, compliance reqs, risk of VM compromise

Pivot, Catching them (NIDS) *[b3/p80]* network sensor may be positioned to see pivoting

Planes of Authorization *[b5/p77]*

Planes of Authorization (segmentation gateway) *[b5/p77]* control plane is core of ZT - handled authentication and global policy, data plane handles connections

PMTUD *[b1/p23]*

Point to point tunneling protocol (PPTP) *[b3/p112]*

poison PDF *[b1/p34]*

Port Security: L2 *[b1/p113]* Layer 2 port security can be used to mitigate risk of MAC spoofing and CAM overflow

Ports Lock Down: NGFW *[b3/p15]* restrict simple ports to their corresponding apps: 25, 53, 123, 465, 993, 995 - slide has list

Post-authentication checks (NAC) *[b5/p71]* key to dynamic access, statement of health (SoH) is one form, other checks can be custom or built-in integrations

Post-Authentication Checks (Remote Access) *[b3/p124]* checks can be used to verify system has AV is installed, firewall is on, and other reqs. Can do auto remediation and place clients in various subnets based on results/risk

Presumption of Compromise *[b1/p40]* always operate under the presumption that the network is already compromised, conduct threat hunting

Primary & Secondary VLANs Diagram *[b1/p133]* Private VLANs support this, everyone is part of primary - secondary marks what type part of VLAN port you are

Priority routing *[b5/p107]*

Private Cloud *[b4/p141]* hypervisor abstracts hardware and shares among virtual OS's, orgs using private cloud in data centers

Private Cloud Security Review *[b4/p158]* Harden systems, limit attack surfaces with segmentation, least priv, use VM network visibility to ones advantage, physical hypervisor separation of key VM usage

Private VLAN FUD *[b1/p134]* FUD = fear, uncertainty, doubt - some resist private VLANs claiming they require a lot of work | PVLANs can be trunked with VTP 3

Private VLAN Port Types *[b1/p132]* Diagram

Private VLAN Ports *[b1/p131]* promiscuous, isolated (we want this), community

Private VLANs (PVLANs) *[b1/p127]* wired equivalent to wireless station isolation - makes pivoting more difficult to an attacker

Private VLANs Potential Issues *[b1/p129]* poorly designed networks, p2p client traffic, Win10 has p2p patching mode

Private VLANs: Configure *[b1/p135]* config for PVLANs

privilege attribute certificate (PAC) *[b4/p111]*

Protected Management Frames (PMFs): Wireless *[b1/p96]* Turn it on: Adds cryptography support after association to an AP, blocks spoofing attacks

Protecting against container escape *[b4/p175]* patch kernel, dont run microservices as root

Protocol Attacks (DDoS) *[b3/p142]* Possible to take advantage of everyday protocols like TCP, attacker spoofs multiple SYN packets

Protocol Translation (Data Control) *[b4/p114]* used to support user claims, allows user claims to work for older OSs

Protocol Visibility Analysis *[b1/p72]* Aware of all protocols being used on network and describe the business purpose, process: capture traffic at various network locations

Proxy *[b2/p137]* Proxy = system that brokers traffic between systems, goal = funnel traffic so it can control data flow, analyze traffic, cache content

Proxy Placement *[b2/p152]* ideally, everything would go through explicit proxy | segmentation for dumb devices

ProxyCannon (Remote Access) *[b3/p115]* Emulates a private botnet using Amazon EC2, automation script to deploy EC2s - can help identify detection/prevention/response abilities

Proxy Types (Web) *[b2/p138]* Forward Proxy (e.g. web proxy) vs Reverse Proxy (e.g. ELB)

Public Cloud Security Review *[b4/p168]* cloud = outsourced hardware, platforms, or services. Due diligence and research is required

Public Cloud, Securing *[b4/p161]* Same way you secure on-prem solutions, limited to the capabilities the cloud provider allows

Public Key Infrastructure (PKI) (ZT) *[b5/p38]* private PKI allows automation of certificate deployment, Windows Server capable of significant PKI capabilities

Pulledpork (NIDS) *[b3/p75]* scripted rule management, can help reduce rule mgmt

Purple Teaming: Threat Model *[b1/p41]* MITRE Cyber Prep 2.0

Putting it all Together: TBS + Kill Chain + MITRE ATT&CK *[b1/p59]* Shift left (Detect & Respond earlier), constant race, goal is to detect and minimize impact

Qq

Qualys SSL Labs (Network Encryption) *[b3/p165]* scans and grades SSL/TLS settings - recommendations provided to improve the score

Quarantine (NAC) *[b5/p69]* authorization should not be static, NAC can dynamically control access

QUIC *[b1/p67]* QUIC (Google HTTPs over UDP) on network

Rr

RA Guard: IPv6 *[b2/p111]* Rogue Advertisement Guard

RADIUS: WPA3 *[b1/p102]*

Rate Limiting: SMTP Proxies *[b2/p172]* Protects by slowing down mass email

Real-time device delivery (segmentation gateway) *[b5/p83]* NAC & VPN solutions require authentication before providing network access

Recursive DNS server (RDNSS) *[b2/p95]*

Red Herring *[b5/p166]* a deliberate diversion, red herring defenses

Red Herring and Tripwires Review *[b5/p184]* well-placed diversion aids in: early detection, gaining time to catch and deal with adversaries

Redesign & Implement - Switches & Routers *[b2/p67]* Best Practices

Redesign: DSA Lifecycle DA-R-I-OM *[b1/p73]* Identify desired state, determine gap, roadmap - documentation | architect decisions are threat focused covering protection, detection, and reaction (P > D + R)

Reject MAC, Forged Transmits *[b4/p145]* virtual switch

Remote Access *[b3/p108]* VPN, terminal/virtual desktops, SSH, RDP-SSH, remote access applications

Remote Access Applications *[b3/p110]* apps or services common for remote access, e.g. RDP

Remote Access Review *[b3/p134]* remote access should include: limit admin priv, directional flow of authentication, enforce MFA

Remote Access Risk Tolerance *[b3/p112]* High, Med, or Low risk tolerance - aim for Low risk tolerance, need MFA

Remote Access Risks *[b3/p113]* remote access servers are targets for server-side attacks, remote authentication MUST move past passwords

Remote Desktop on HTML5 with Apache Guacamole *[b3/p116]* AG is an open-source clientless RDP, SSH, and VNC platform through web browser, has guacamole server and client

Removable Media (Data Control) *[b4/p122]* Deny write access to removable drives not protected by BitLocker

Reverse Proxcies, ZTNA and SASE *[b2/p139]* RPs are central to the new strategies: ZTNA and SASE

Reverse Proxy (Data Security) *[b4/p13]* WAF, handles incoming requests - can be on-prem or cloud solution, cloud usually combines DDOS and WAF protection

RFC 3164 *[b5/p98]*

RFC 4193 *[b2/p84]* Describes locally assigned global IDs

RFC 4941 *[b2/p90]* Duplicate Address Detection (DAD), RFC 4941

RFC 4941 *[b2/p90]*

RFC 6106 *[b2/p95]*

RFC 791 *[b2/p77]*

RFID Badges: Wireless *[b1/p105]* Purchase the right card with rolling codes or challenge-response, can use a protective sleeve

RIPv1 , v2 *[b2/p9]*

Risk-Driven & Business Outcome-Focused Architecture *[b1/p38]* Measure risk, costs, and benefits | NIST CSF = Identify, Protect, Detect, Respond, Recover (IPDRR)

RITA (NSM) *[b3/p61]* Flare can analyze Zeek or Suricata flows to identify C2 beacons | RITA = real intelligence threat analytics

robots.txt (Data Security) *[b4/p28]* PHP app that infinitely creates web pages, to confuse or break automated scanners - WAF can integrate WebLabyrinth into every web server. Works best with robots.txt

Rogue DHCP Server *[b1/p121]* often follows DHCP starvation attack, once DHCP is out of leases rogue server takes over

Rogue DHCP Server *[b1/p122]* Diagram

Rogue Pi - Red team scenario *[b1/p82]*

Rogue RA, how to defend *[b2/p113]* have all routers send RA messaged with High-Priority, best solution is to enable RA guard

round robin db tool (RRDtool) *[b1/p150]*

Router ACLs *[b2/p126]* modern routers provide L3/L4 firewall capabilities, slide has config

Routers - Discover & Assess *[b2/p5]* Common issues: secure administration, services offered, vulns, ACLs, banners, logging, AAA

Routers - Threats and Red Team Scenario *[b2/p6]* Scanning, fingerprinting, DOS, IP spoofing, ICMP flood, smurf attacks, route table poisoning | e.g. APT41

Routing Protocols *[b2/p9]* Two basic types: Interior gateway protocols (IGPs_ and exterior gateway protocols (EGPs) | IGP = OSPF, EIGRP, IS-IS | EGP: BGP

Routing Updates Unauthorized *[b2/p10]* BGP and EIGRP only support hashes, OSPF and IS-IS support hash and plaintext authentication

RRDTool *[b1/p150]* Round Robin Database Tool

Rule Counter *[b3/p12]*

Rule creation, what would it take? (mitre) *[b5/p147]* MITRE is hard to operationalize because each product functions differently

Rumble Network Discovery: IPv6 *[b2/p104]* new infosec tool used for network mapping

Ss

S4U2Self *[b4/p114]*

SaaS *[b4/p71]*

Sandbox VMs (malware detonation) *[b3/p100]* customization of VM allows for better use cases

SASE - Reverse Proxy *[b2/p139]* Secure Access Service Edge

ScreenOS *[b2/p38]*

Script collection (Log Collection) *[b5/p115]* sometimes scripts are the only method to obtain logs, especially true for cloud systems and software, 3p apps - scripts can use APIs

Script Use (Log Collection) *[b5/p116]* helpful for collecting custom logs

Scripting & APIs (NGFW) *[b3/p21]* Everything is code today, automation is an architecture decision - majority of NGFWs support automation

SCRYPT *[b2/p21]*

SDP (Remote Access) *[b3/p125]* ZTNA or SDP (software defined perimeter) provides access to an application or resource - not an entire network

Search Criteria (mitre) *[b5/p144]* start with automated alerts the move into threat hunting, anomaly detection

Secrets (containers) *[b4/p178]* Docker swarm, K8s support secrets - sensitive data is stored by mgmt services, data is encrypted during transit to container and at rest

Secure Transmission (Network Encryption) *[b3/p155]* network encryption is designed to secure communication, uses established hierarchical trust

Securing the Detonation (malware detonation) *[b3/p96]* detonation box needs to be secured, place firewall between system and network, risk of malware attacking other orgs

Securing Traffic (ZT) *[b5/p32]* all traffic must be authenticated and encrypted

Securing Traffic Review *[b5/p48]* Authentication & encryption are mandated under ZT, if above is not possible - use alternatives

Security Architect: What do they do? *[b1/p7]* Design, build, and oversee implementation of network and computer security for an org

Security Architecture *[b1/p6]* Meant to communicate a future state | Focus on designing and building security in: networks & infra, apps, endpoints, and cloud | Built from network up | Must be built around business processes

Security Onion (NSM) *[b3/p33]* Contains hundreds of tools to enable network security monitoring

Security Onion FlowData *[b1/p144]* filter out data in /etc/nsm/bpf.conf

Security Onion Network and Endpoint Visibility (NSM) *[b3/p41]* ELK dashboards allow for easy pivoting between network and host data (analytical pivoting)

Security Operations Fundamentals *[b1/p22]*

Security Operations Monitoring in Mind *[b1/p48]* Architect with SecOps in mind, use concept of Zones to defend org

Segmentation *[b2/p119]* segmentation does not stop at the network, needs to include authentication and access

Segmentation gateway *[b5/p78]* NGFW or SDN at the core rather than tiering firewalls, focuses on users and endpoints, heavy allow list approach

Segmentation gateway are just NGFWs *[b5/p80]*

Segmentation Gateway Review *[b5/p86]* provides centralized: network agent access controls, time constraints and limitations, data-centric port and app controls, MCAP trust zoning | NGFW can be deployed as a segmentation gateway

Segmentation Issue (network) *[b2/p130]* example of dangerous design, also need segmentation for access control - 445 (SMB) is open

Segmentation Login *[b2/p131]* use principle of least privilege

Segmentation Principles *[b2/p121]* facilitate prevention and detection, classification levels/tiers must reside in different zones, use gates to inspect traffic and enforce access control, balance security with usability

Segmentation Summary *[b2/p133]* form of risk reduction, apply to network and access - login segmentation | goal = lower damage by limiting overall access

Self-Defeating Network *[b1/p22]*

Sender Authentication *[b2/p168]* only helps with company owned domains

Sender Policy Framework (SPF) *[b2/p163]* DNS record validates email sent from an authorized source

Sensor Placement (NSM) *[b3/p32]* Deploy sensors on inside of network, use Focused sensors: specific rules to address segment/zone. Classify assets, systems, zones, and tiers of users

Service Banners (red herring) *[b5/p169]* apps identify their software and version number upon connection

Service Banners Changing (red herring) *[b5/p171]* alternative is to rewrite or modify service banner, can be done with local software or reverse proxy

Service Banners Minimizing (red herring) *[b5/p170]* hide or limit service information

SIEM *[b5/p89]* Central Brain, SIEM != log collection - it can do so much more --- analytics, alerting, ML, automation, etc

SIEM components *[b5/p90]* consists of multiple pieces: log collectors, log aggregator, log broker, storage, search/report, alert engine

Sigma - how it works (mitre) *[b5/p149]* sigma format -> sigma converter -> elastic search queries, splunk searches, etc

Sigma Detection & Conditions *[b5/p155]* condition: logice for rule matching, detection: object containing items of interest

Sigma Elastisearch rule conversion *[b5/p159]*

Sigma Example rule *[b5/p156]* inbound_ssh.yaml example

Sigma Generic Signatures (mitre) *[b5/p148]* high level generic language for analytics, enables analytics reuse and sharing - works accross SIEM and non-siem tools

Sigma Log source section (mitre) *[b5/p154]* optional classifiers: category, product, service, description

Sigma outputs supported *[b5/p151]* splunk, qradar, arcsight, windows defender, powershell, grep

Sigma rule conversion of signatures to alert queries *[b5/p150]* flow diagram on slide

Sigma Rule format (mitre) *[b5/p152]* get rules to sigma format, plaintext YAML files - metadata, log source, detection, condition

Sigma Rules: Title, Metadata, log source (mitre) *[b5/p153]* written in YAML, example in slide

Sigma Splunk Results *[b5/p158]*

Sigma Splunk Rule Conversion *[b5/p157]* inbound_ssh.yaml example

Sigma2attack (mitre) *[b5/p161]* CLI tool to generate MITRE heatmap from Sigma, useful to compare with threat models

Sigma: what was done *[b5/p160]* one generic rule, two formatted and customized search queries come out

sigmac *[b5/p157]* performs conversion

Signals Intelligence (SIGINT) *[b1/p140]*

Signature Anomalies by Tool (mitre) *[b5/p142]* signature centric, anomaly centric, SIEM falls into both

Signature-Based Detection (NIDS) *[b3/p66]* Known bad stuff

Signed Certificate Timestamp (SCT) *[b3/p162]*

Silk Road *[b2/p63]*

Simple Network Time Protocol (SNTP) *[b2/p52]*

Simple Service Discovery Protocol (SSDP) *[b2/p94]*

Single Packet Authorization (SPA) *[b5/p47]* blocking connections by default, connecting system must first send auth packet, uses asymmetric encryption and HMAC

Site Categories *[b2/p144]* web proxy associated with site category filtering, not a replacement for allow lists

Site Categories: Bypassing *[b2/p145]* domains go up for auction, adversaries buy and can use for phishing

SLAAC - Stateless Address Auto Config: IPv6 *[b2/p85]* system can independently determine its IPv6 address, can create privacy concerns

SLAAC Example *[b2/p86]* Diagram, uses MAC address to determine IPv6 address - can result in privacy issues

Slowloris (DDoS) *[b3/p145]* another resource exhaustion attack, works on web servers like Apache

Smart Install, Cisco *[b2/p26]* plug-and-play config and image mgmt feature that provides zero-touch deployment for new switches, does not require authentication

SMTP Prevention & Detection *[b2/p161]* focus on spam = prevention, but more serious emails need prevention and detection

SMTP Proxy *[b2/p160]* an effective means to control email

SMTP Proxy Review *[b2/p173]* mature technology to deal with spam

Smurf Attack *[b2/p6]*

SNMP Attack (cisco): download the cisco IOS config *[b2/p47]* nmap config

SNMP Attack passwords exposed *[b2/p48]* Type 5 cracked and exposed

SNMP Attack: Guess the community Strings *[b2/p46]* metasploit and nmap launching attack config

SNMP Community String *[b2/p45] passwords*

SNMP Hardening *[b2/p49]* Disable if not required | disable write access, use complex community strings, version 3

SNMP, securing *[b2/p45]* check for SNMPv2c, need to use v3 | read and write strings - if you can figure them out you can pull a config

SNMPv3 config *[b2/p50]* 3 ways to imlpement: no auth, auth, and priv (auth and encryption - use this)

Snort (NIDS) *[b3/p67]* Most common IDS, slide has example signature rule

Snort gid (NIDS) *[b3/p71]* gid number specifies what generates as an event, details in slide

Snort Rule Options (NIDS) *[b3/p70]* rule options are withtin the parentheses, slide contains details

Snort Rules Header (NIDS) *[b3/p68]* alert ip any any -> any any (slide contains details)

Snort Variables (NIDS) *[b3/p69]* most common IP var are HOME_NET and EXTERNAL_NET, slide contains ipvar and portvar details

Solarwinds Breach (ZT) *[b5/p8]* US fed gov making major push to promote ZT adoption, guidelines include DISA ZT reference, NIST SP 800-207

Solid Detection Required (SIEM) *[b5/p88]* all data available in a central location for proper analysis and actioning, use SIEM

SonicWALL *[b2/p38]*

Source Port *[b3/p68]*

Split Tunneling vs Full Tunneling (Remote Access) *[b3/p120]* Split - only specific subnets are routed over VPN, Full - all traffic must traverse VPN

Squid - web proxy *[b2/p154]* open source, supports explicit and transparent configs

SSL Decrypt Example (Network Encryption) *[b3/p170]* wireshark capture of ssl decrypt

SSL Decrypt Mirror Port (Network Encryption) *[b3/p169]* decrypted packets are mirrored out an interface, decrypted traffic shows up with the original port such as 443

SSL Inspection (Network Encryption) *[b3/p168]* SSL Inspection on NGFW, will decrypt, analyze, and re-encrypt -- may not be authorized to do this

SSL Interception *[b2/p143]* encryption blinds a proxy by default, SSL interception allows analysis of encrypted sites

SSL Offloading (Data Security) *[b4/p14]* Reverse Proxy design includes SSL offloading, proxy inspection has full access to every request and response

SSL/SSH Inspection (NGFW) *[b3/p13]* encryption breaks deep packet inspection so ENABLE SSL/SSH inspection

SSL/TLS Passive Decryption (Network Encryption) *[b3/p166]* tools like viewssld can decrypt data on the fly, perfect forward secrecy (PFS) breaks passive decryption

sslstrip (Network Encryption) *[b3/p160]* tool performs downgrade attacks on https, one of the reasons why HSTS was born

Statement of Health (SoH) *[b5/p70]* NAC agents required for real-time health monitoring, monitors for key changes to sysm

Station Isolation: Wireless *[b1/p99]* Diagram

Station Isolation, Potential Issues: Wireless *[b1/p100]* at home, a wireless laptop would not be able to connect to other wireless devices

Station Isolation: Wireless *[b1/p98]* Turn it on: client on a wireless AP may speak to the AP only - can't talk to other clients on the same AP

Sticky MAC Addressess *[b1/p115]* automates process of manually adding addresses, likes config: switchport security max-mac-count 1

Strict-Transport-Security (HSTS) (Network Encryption) *[b3/p159]* HSTS requires setting HTTP header, upgrades HTTP links to HTTPS automatically

Stubbing – DLP *[b4/p101] used in file relocation*

Suricata & TLS Magic with JA3 (NSM) *[b3/p60]* Suricata can also use JA3, example shows Dridex match

Suricata (NIDS) *[b3/p72]* Modern open-source IDS/NSM - prefer it to snort, can do application layer identification - snort can't

Suricata BPF Filtering *[b1/p147]* allows eliminating duplicates

Suricata Flow *[b1/p146]* IDS capable of network security monitoring (NSM), can be unidirectional or bidirectional

Suricata Metadata Logging (NIDS) *[b3/p73]* creates network logs: DNS, http, smtp, TLS and more - give you IDS alerts + context

Switch & Router Security *[b2/p15]* Layer 3 switch contain both switching and routing modules

Switch Mirror Port Overload (NSM) *[b3/p29]* occurs when multiple ports overwhelm the monitoring port

Switch SPAN/Mirror Ports (NSM) *[b3/p28]* offer orgs inexpensive way to gain network visibility - mirror ports can sniff traffic

Switches - Discover & Assess Layer 2 *[b1/p107]* Basic issues: secure administration, services offered, vulnerabilities, ACLs, banners, logging, AAA

Switches - Threats Layer 2 *[b1/p108]* MAC flood, ISL tagging, ARP attacks, etc

Switches Hardening: Physical Access, Ports, and SSHd *[b2/p16]* Force SSHv2, never use telnet. Use 2048 or 4096 bit key, set 'ssh authentication-retires' to 3 (drops after 3 failed logins)

Switches: Disable Unused Services and Legacy Protocols *[b2/p18]* disable bootp, fingerd, httpd, mop, pad, CDP, SNMP (if not being used)

Switches: enable centralized logging *[b2/p19]* enable on all relevant network devices, send logs to syslog server or SIEM

SYN Cookies (DDoS) *[b3/p144]* issued when connection table fills, 5+3+24=32-bit SYN sequence number

SYN Flood Protection (DDoS) *[b3/p143]* Tuning systems can help address SYN floods, slide example of linux /etc/sysctl.conf

Syslog (Log Collection) *[b5/p98]* most common network protocol for sending logs on the network, default is UDP on 514

Syslog Agents & Windows *[b5/p109]* Win events may not fit within constraints of syslog, syslog-based agents may separate logs into smaller pieces -- putting pieces back together add overhead, not good

syslog config examples (ubuntu 16.04 system) (audit policies) *[b5/p132]* examples and details in slide

Syslog Configuration (audit policies) *[b5/p131]* Linux and mac come with built-in syslog agents

Syslog Devices (Log Collection) *[b5/p99]* List

Syslog Field Parsing *[b5/p103]* Regex pattern, fields require pre-meditated parsing

Syslog Message Limitations *[b5/p102]* inconsistent, systems are limited in message size, UDP = 1024 bytes

Syslog traditional logging fields *[b5/p100]* Example in slide, PRI and facility code numbers

Sysmon (audit policies) *[b5/p127]* free from Windows Sysinternals, good for monitoring, provides process hashes and parent processes for analysis

Sysmon Config (audit policies) *[b5/p129]* Granular logging available

Sysmon Example (audit policies) *[b5/p128]* example on slide

Tt

T-Pot *[b5/p176]*

Teensy Attack *[b1/p86]*

Teredo Tunneling: IPv6 *[b2/p109]* Developed by Msoft, uses UDP 3544, detect and block/alert teredo

Terms & Conditions *[b2/p147]* prevent C2 channel

The Onion Router (TOR) *[b2/p63]*

Third Party Agents (Log Collection) *[b5/p112]* more feature rich than built-in agents, focus on transport methods, filtering capabilities, special features, support

Third-party password policy management (ZT) *[b5/p24]* Alternative to use for granular password policy requirements

Threat Modeling with DeT&CT *[b1/p45]* open-source framework for visibility on data sources, detection, and threat actors. Python tool, YAML files. Helps to prioritize where to be investigating more on

Threat Modeling: Purple Teaming *[b1/p41]* MITRE Cyber Prep 2.0

threshold.conf (NIDS) *[b3/p76]* rules with flowbits cannot be disabled by disablesid.conf

thresholds.conf *[b3/p76]*

Tiers: based on criticality and business impact *[b2/p125]* Tier 1 > Tier 2 > Tier 3

Time Restrictions (Data Control) *[b4/p119]* employee access should be limited to working hours, can force logoff when logon hours expire (recommended)

Time-Based Security Model *[b1/p55]* Method to understand how much security a product of tech provides | P > D + R | P - how long protection works, D - how long to detect, R - how long to react - design for parallel P D+R

Time-Based Security: Architecting for PDR *[b1/p56]* Protection buys you time, needs D + R early to help mitigate impact | P < D+R = effective security is impossible to achieve in this system

TLS & IPSEC *[b5/p34]* provide both encryption & auth

TLS-based VPN (Remote Access) *[b3/p109]* Modern VPNs use TLS, usually supports post-authentication checks - e.g. OpenVPN

Traditional Communication (ZT) *[b5/p33]* encryption over internet, used in DMZ services - internal comms is cleartext

Traditional vs Network Extraction (Log Collection) *[b5/p117]* traditional: multiple collection points, network extraction: single collection point

Trust Model Change (ZT) *[b5/p35]* configure systems to use mutual authentication, supported by SSL/TLS

Trust Over Times (ZT) *[b5/p14]* risk to systems increase over time, systems need to be reloaded, creds need to be rotated, certificates need to be replaced

Trusted Platform Module (TPM) *[b4/p69]* like a smart card built into a motherboard, TPM protects volume master key (which unlocks symmetric key)

Tyrell Corp vs Replicants - Red team scenario, Book 1 *[b1/p81]*

Tyrell Corporation Case Study Book 2:1 *[b2/p134]* Diagram

Tyrell Corporation Case Study Book 3:1 *[b3/p3]* Book 3 Diagram

Tyrell Corporation Case Study: Book 1:1 *[b1/p28]* 3 leg architecture - flat network, Tyrell Corp diagram

Tyrell Corporation Case Study: Book 1:2 *[b1/p136]* PVLANs stop from talking on same vlan but not from talking to other vlan devices

Tyrell Corporation Case Study: Book 2:2 *[b2/p158]* Diagram - added web proxy

Tyrell Corporation Case Study: Book 3 Beginning *[b3/p176]* Diagram

Tyrell Corporation Case Study: Book 3 End *[b3/p175]* Diagram

Tyrell Corporation Case Study: Book 3:2 *[b3/p23]* Diagram - added NGFW

Tyrell Corporation Case Study: Book 3:3 *[b3/p62]* Diagram: Included NSM sensors

Tyrell Corporation Case Study: Book 3:4 *[b3/p85]* Diagram, adding Zeek & Suricata sensors

Tyrell Corporation Case Study: Book 3:5 *[b3/p106]* Diagram, added malware detonation - integrate bad signature findings to other security appliances

Tyrell Corporation Case Study: Book 3:6 *[b3/p135]* Diagram, added jumpbox to control remote access flow and authentication

Tyrell Corporation Case Study: Book 3:7 *[b3/p152]* Diagram, added DDos Protection

Tyrell Corporation Case Study: Book 3:8 *[b3/p172]* Diagram, added SSL inspection to NGFW and ssl decrypt mirroring to the NSM

Tyrell Corporation Case Study: Book 4 Beginning *[b4/p183]*

Tyrell Corporation Case Study: Book 4 End *[b4/p184]* data-centric design

Tyrell Corporation Case Study: Book 4:1 *[b4/p9]* Diagram, Webapp

Tyrell Corporation Case Study: Book 4:2 *[b4/p31]* Diagram, added WAF - only in front of PCI since its most important, don't have all the time in the world

Tyrell Corporation Case Study: Book 4:3 *[b4/p49]* Diagram, added DAM - db activity monitor to PCI

Tyrell Corporation Case Study: Book 4:4 *[b4/p73]* Diagram, added whole disk encryption

Tyrell Corporation Case Study: Book 4:5 *[b4/p91]* Diagram, added data classification and encryption requirements

Tyrell Corporation Case Study: Book 4:6 *[b4/p105]* Diagram, added DLP for intellectual property and credit cards

Tyrell Corporation Case Study: Book 4:7 *[b4/p139]* Diagram, added block for accessing IP on mobile assets, MDM

Tyrell Corporation Case Study: Book 4:8 *[b4/p159]* Diagram, separated hypervisors for sensitive and nonsensitive

Tyrell Corporation Case Study: Book 5:1 *[b5/p18]* Diagram, What connections are trusted? Are/should they always be trusted?

Tyrell Corporation Case Study: Book 5:2 *[b5/p49]* Diagram, what visibility do unauthorized machines have?

Tyrell Corporation Case Study: Book 5:3 *[b5/p93]* Diagram, implemented SIEM

Tyrell Corporation Intro *[b1/p11]* Used to illustrate and visualize contents covered in SEC530 - from Bladerunner

Uu

Unique Local Address (ULA): Ipv6 *[b2/p83]* Diagram for global unicast and ULA

US Government - embracing a zero trust security model *[b5/p8]* US fed gov making major push to promote ZT adoption, guidelines include DISA ZT reference, NIST SP 800-207

USB Keyboard Mitigation is Limited *[b1/p87]* USBs have Product IDs (PIDs) and Vendor IDs (VIDs), some USB have unique serial number, mitigations can include facility security and physically blocking USB devices

USB Keyboards Weaponized *[b1/p86]* Loaded with payloads that are able to type command on a logged-in computer

User-agents *[b5/p173]*

Vv

Variable Trust (ZT) *[b5/p13]* access controlled by variable trust - its adaptive, similar to real-life credit scores --- trust must be earned

Varnish (DDoS) *[b3/p146]* Tune web server settings, implement Varnish, reverse proxy

VeraCrypt *[b4/p67]* open-source disk encryption solution, supports FDE with passwords or key files, can also create encrypted containers

Virtual Machine Identification (malware detonation) *[b3/p102]* malware attemps to hide from malware detonation, Pafish is a poc on how malware detects VM status

Virtual Machine Masking (malware detonation) *[b3/p103]* Antivmdetection and VMCloak hide virtual status, modify sandbox images to mask they are VMs

Virtual Machine Tools *[b4/p156]* guest tools add convenience but also add additional risks, can be channels to VM escape

Virtual Network Visibility (Private Cloud) *[b4/p146]* VM in promiscuous mode can see all host traffic, same host VM traffic does not access physical switches

Virtual Patching (Data Security) *[b4/p25]* uses WAF to mitigate the risk without recoding the application

Virtual Switch Security (Private Cloud) *[b4/p145]* Common switch security capabilities: reject MAC address changes, reject forged transmits, traffic mirroring support

VirtualBox *[b3/p131]*

Visibility & Detection - Different Needs *[b1/p60]* Hunt solutions rely on visibility, should be optimized for low FNs - so we need to design for visibility and detection

VLAN hopping *[b1/p108]*

VM Escape (Private Cloud) *[b4/p149]* fix by establish a routine for continuous patching

VM Interaction *[b4/p155]* Limit: copy and paste, clone, DVD/USB, snapshots, view console

VM Masking *[b3/p103]*

VM to VM Traffic (Private Cloud) *[b4/p147]* deploy virtual capture devices on each physical host

VMCloack (malware detonation) *[b3/p103]* Antivmdetection and VMCloak hide virtual status, modify sandbox images to mask they are VMs

Volume Shadow Copy Service (VSS) *[b4/p55]*

Volume Shadow Copy Service (VSS) (Data Protection) *[b4/p55]* Win VSS Keeps record of changes on disk, intended for rollback purpose - files can be exluded

Volumetric Attack *[b3/p139]*

Volumetric Attacks (DDoS) *[b3/p140]* goal = saturate victim's pipe, attack is a matter of brute strength

VTP Transparent Mode *[b1/p134]*

Ww

WAF Allow Listing (Data Security) *[b4/p22]* more secure to only allow what is expected, slide has parameters

WAF Capabilities (Data Security) *[b4/p15]* SSL offloading, content decoding, automatic learning, mitigation of common HTTP attack vector, virtual patching, rate limiting

WAF Challenges (Data Security) *[b4/p17]* not foolproof, need to design to environment - techniques exist to bypass WAF - goal is never to be foolproof, it's to have proper layers setup

WAF Content Routing (Data Security) *[b4/p27]* WAF can dynamically route traffic among web servers, also capable of modifying requests/responses

WAF Deployment (Data Security) *[b4/p21]* Automatic learning - dynamic policy building - WAF learns: methods, entry points and variables, content types, statistics and heuristics, Manual - settings manually tuned

WAF Detection *[b4/p29]* strong preventative tech, best detection capabilities are for internal servers - WAF prevention will fail, so detection is a must

WAF Evasion Example (Data Security) *[b4/p18]* slide has syntax, rule looks for request to /admin.php with invalid user parameter

WAF moving past Allow/Deny (Data Security) *[b4/p26]* WAF can do more than allow/deny - can utilize dynamic actions based on risk identified

WAF Normalization (Data Security) *[b4/p19]* better rule implementation would be to normalize the request before doing a rule check

WAF Review *[b4/p30]* A reverse proxy to secure web servers, implementation should include normalization of data, patch vulns, centralized protection & detection, move past allow/deny mentality, bolster detection

WarBerryPi *[b1/p85]* hardware implant for red teaming to obtain info quietly/stealth

Ways to ATT&CK (mitre) *[b5/p146]* identify before rule engineering SIEM and EDRs

WDS - Windows Deployment Services *[b4/p70]*

Web App Firewalls (WAF) (Data Security) *[b4/p11]* An app firewall for HTTP applications, reverse proxy or local module on a web server

Web Proxy (FWD Proxy) *[b2/p141]* acts as intermediary for web access, primarily used to protect internal assets

Web Proxy Access Options *[b2/p153]* Diagram

Web Proxy Alternatives *[b2/p147]* require Terms and Conditions and authentication, can use splash screen before internet access works

Web Proxy Capabilities *[b2/p142]* Inspection of web traffic, can filter on categories

Web Proxy deployment *[b2/p148]* Transparent - traffic goes through proxy regardless of endpoint config | explicit - endpoints must be configured to use the proxy

Web Proxy Review *[b2/p157]* Need one! Full explicit, full allow lists, apply authentication and terms and conditions

Web Proxy Types *[b2/p138]* Forward Proxy (e.g. web proxy) vs Reverse Proxy (e.g. ELB)

Web Vuln Scanner Integration (Data Security) *[b4/p24]* vuln reports can be imported into WAF solutions, provides virtual patching

WebLabyrinth (Data Security) *[b4/p28]* PHP app that infinitely creates web pages, to confuse or break automated scanners - WAF can integrate WebLabyrinth into every web server. Works best with robots.txt

Website Allow Lists *[b2/p146]* most secure approach, involves more work and maintenance

Websockets (Data Security) *[b4/p20]* HTTP 2.0/websockets represent bidirectional real time comms over HTTP - WAF should include all capabilities your custom apps use

Whitecap Rules (NIDS) *[b3/p79]* use of Snort rules to allow list ICMP traffic

Windows 10 P2P Patching *[b1/p130]* Designed for informal networks such as homes, p2p method to deliver software between client PCs

Windows Always on VPN and DirectAccess (Remote Access) *[b3/p123]* Win has built-in VPN capabilities pre-installed | Win7 has DirectAcces | Win10 has Always On

Windows Auditing (Data Protection) *[b4/p54]* Requires Audit Object Access to be enabled, design for detection

Windows Deployment Services (WDS) *[b4/p70]*

Windows Domain Isolation (IPsec) (ZT) *[b5/p43]* Windows natively supports IPSec for domain isolation, authenticates all traffic, optionally encrypts traffic

Windows Event Collector (Log Collection) *[b5/p111]* push/pull is set up via subscriptions in group policy, can be used with agentless collection or replaced by agents

Windows Event Forwarding (Log Collection) *[b5/p110]* centrally managed via GPO, allows pushing or pulling logs to/from central event collector, encryption and compression

Windows Events (Log Collection) *[b5/p104]* requires Win Event viewer or special agent to read, events are broken up by channels, event IDs, stores as XML

Windows File Classification Infrastructure (FCI) *[b4/p78]* Allows assigning properties to files - clearance required, level of PII, date, impact of disclosure, etc.

Windows File Properties (File Classification) *[b4/p79]* properties can be added in AD Admin Center, can be managed with powershell

Windows Information Protection (WIP) and MDM *[b4/p134]* creates separation between personal and corporate assets

Windows IPSec (ZT) *[b5/p44]* IPSec integration is part of the Windows Firewall, change IPSec default options - granular control via firewall rules

Windows Mgmt Instrumentation Command (WMIC) *[b1/p29]*

Windows Permissions *[b4/p52]*

Windows Permissions (Data Protection) *[b4/p52]* file & folder permissions set per user or group, Explicit permissions win over inherited

Windows Ping Example (IPSec) *[b5/p45]* Without and With IPSec comparison o nslide

Windows Rights (Data Protection) *[b4/p53]* Rights outrank access controls: take ownership, backup files and directories, restore files and directories

Windows Server Update Services (WSUS) *[b1/p130]*

Windows Update Example (NGFW) *[b3/p9]* Many ways to identify Windows update: DNS, HTTP, HTTPS

Wireless *[b1/p91]* 802.11 (what we'll focus on), Bluetooth, Zigbee, Z-wave, cellular, infrared, RFID

Wireless Intrusion Prevention System (WIPS) *[b1/p94]* Can detect and protect against rogue access points, report and alert on rogue devices

Wireless Risk *[b1/p92]* Logic: must be physically present, Truth: physical access is not required

Wormhole Attack Illustrated *[b2/p13]* Diagram, shows hping command

Wormhole Attack: Routers *[b2/p12]* an unauthorized tunnel, configured to and from an internal router

WPA2 Personal vs WPA2 Enterprise *[b1/p101]* WPA2 Personal = home/personal use with PSK. WPA2 Enterprise = business, uses 802.1X and RADIUS

WPA3 Enterprise: WPA2 + PMFs + Stronger Ciphers *[b1/p102]* Announced in 2018, better authentication, increased crypto strength, use of Projected Mgmt Frames (PMFs) to increase network security

Xx

X-forwarded-for (XFF) *[b2/p141]*

XML Logs (Log Collection) *[b5/p105]* XML is structured, requires agent support - traditional agent, modern agent

Zz

Zeek & Network Visibility in the Enterprise (NSM) *[b3/p38]* Zeek = networks Sysmom, add a layer in the overall visibility stack

Zeek (NSM) *[b3/p36]* both an IDS and NSM in that it creates logs -> Next Gen IDS

Zeek Architecture 1 (NSM) *[b3/p43]* not multithreaded, possible to scale by spreading workload across many hosts using a cluster: worker + manager + proxy

Zeek Architecture 2 (NSM) *[b3/p45]* Network > libpcap / PF_Ring > event engine > policy script interpreter

Zeek as command line utility (NSM) *[b3/p49]* analysis can be done from CLI using the Bro binary, slide has config

Zeek Cluster Config: node.cfg (NSM) *[b3/p47]* slide has config

Zeek File Extraction (malware detonation) *[b3/p97]* capable of doing auto file extraction, detonation devices keep a record of each analysis

Zeek IDS, formerly BRO (NSM) *[b3/p35]* More than just an IDS, its a network programming language, power of Zeek is that it can help you answer questions

Zeek inside a Docker Container (NSM) *[b3/p55]* possible, slide contains details

Zeek Minimal Starting Configuration (NSM) *[b3/p46]* slide has config

Zeek Scripts loading, a peek at analysis.bro (NSM) *[b3/p50]* slide has analysis.bro contents

Zeek Use Caes: TLS Magic with JA3 (2) (NSM) *[b3/p59]* slide has config of Zeek to use JA3

Zeek Use Case: Detect Beaconing with Flare and RITA *[b3/p61]* Flare can analyze Zeek or Suricata flows to identify C2 beacons | RITA = real intelligence threat analytics

Zeek Use Case: Spotting the C2 (NSM) *[b3/p56]* "Pulling a thread" with x.509 certificates, slide contains commands

Zeek Use Cases: TLS Magic with JA3 (NSM) *[b3/p58]* JA3 = technique for creating SSL client fingerprints from the pre-encryption handshakes of the SSL protocol

Zeek: IPv6 Discovery Tool *[b2/p105]* slide has command

Zero Trust 3 Concepts *[b1/p63]* All resources are accessed securely regardless of location, least priv strategy and strict access control, inspect and log all traffic | implement less trust with existing tech, layer by layer, to start journey towards Zero Trust

Zero Trust Architecture *[b5/p6]* Data-centric focus, network is always hostile - assume breach, internal and external threat always present, internal network does not equal trusted, everything must be proven, log and inspect all traffic

Zero Trust Credentials *[b5/p20]* creds should be rotated; assumption is creds are compromised

Zero Trust Journey over Time *[b5/p16]* Discovery > assessment > baseline > intermediate > advanced

Zero Trust Mandates *[b5/p12]* 1 - all traffic must be secured, 2 - least priv, 3 - all data flows must be known and controlled, 4 - all assets must be scanned, hardened, and rotated. TRUST NOTHING, VERIFY EVERYTHING

Zero Trust Model *[b1/p62]* Removes concept of "internal is trusted, external is not" - redesign networks from inside out, assume all is untrusted. Officially published in NIST SP 800-207 in 2020

Zero Trust Networks *[b5/p7]* Zero trust concept is modal and strategy, recommended book: zero trust networks

Zero Trust Review *[b5/p17]* least priv, all access authenticated and verified, trust should be earned and dynamically adapt, know thy network

Zero Trust Scenario - Remote Exploitation or Insider Threat *[b5/p15]* malicious cyber actor compromises a user's device through an internet-based mobile code exploit

Zigbee: Wireless *[b1/p104]* Operates in 1 of 3 modes: unsecured, ACL, Secured mode. The more you enable, the less life the battery lasts - must last 2 yrs to pass certification

Zones: Architecting with SecOps in Mind *[b1/p48]* Architect with SecOps in mind, use concept of Zones to defend org

ZTNA - Reverse Proxy *[b2/p139]* Zero Trust Network Architecture