Locked Shields 2017

Michal Kostěnec, CESNET z. s. p. o.

Locked Shields

- NATO CCDCOE
  - Cooperative Cyber Defence Centrum of Excelence
  - Tallinn, Estonsko
- BLUE/RED cvičení
- Každoročně od 2010
- Letos 20 účastníků
- Předpřipravené virtuální prostředí + příběh, interakce v reálném čase

Scénář cvičení (Berylie a Crimsonie)

- Berylie
  - Ostrovní stát v Atlantickém oceánu o velikosti Španělska
  - Beryliáni jsou většina, menšina Crimsoniánů usiluje o větší vliv
  - Moderní, rychle rostoucí ekonomika
  - Ozbrojené síly velice investují do Dronů, výzkum/vývoj
    - Důležitá složka jejich vzdušné výzbroje
    - Hlavní letecká základna ve městě Buka
  - Podzim 2016 – rozsáhlá špionáž a sabotáž v oblasti vývoje dronů
    - Crimsoniáni ~ velké politické napětí

Scénář cvičení (Kyberútok na základnu Buka)

- 0430Z – Základna Buka pod trvalým kyberútokem
- 0600Z – Národní bezpečnostní tým nechal zřídit tým rychlé reakce
  - (RRT ~ Rapid Reaction Team = tzv. BLUE týmy)
- 0700Z – je právě teď, jsme členy RRT a dorazili jsme na základnu!

Různobarevné týmy a jejich role

- RED- útok na infrastrukturu BLUE týmů
- BLUE- obrana infrastruktury
- GREEN- příprava herního prostředí
- WHITE- řízení jednotlivých fází, předávání informací RED týmu
- YELLOW- sledování průběhu, předávání informací z reportů WHITE týmu

„BLUE“ tým

- Zabezpečení proti útokům RED týmů
- Správa systémů pro zaručení dostupnosti a správné funkcionality
- Reakce na reportované uživatelské problémy
- Reportování problémů WHITE týmu
- Řešení forenzního úkolu
- Právní úkoly
- Komunikace s médii

“BLUE” tým – požadavky

- Doporučeno 14 členů
  - 10 + 2 + 2 (10 infrastruktura/systémy, 2 forenzní úkol, 2 právní a komunikace)
- Znalost síťových protolů
  - TCP/IP DNS, NTP, DHCP, HTTP, HTTPS, SMTP, POP3, IMAP, SSH, FTP, VoIP, …
- Znalost webových technologií
- Znalost OS
  - Windows, Linux, MacOS, FW (pfSense), Vmware

“BLUE” tým – požadavky

- Síťové prvky
  - Cisco IOS, NX-OS
- ICS
  - PLC, HMI, SCADA software
- Forenzní analýza koncových zařízení a počítačových sítí
  - Obrazy HDD, operační paměti a záznam síťového provozu (pcap)
- Právní úkony
- Monitorování, detekce, analýza, reportování a řešení incidentů
- Strategické plánování

Náš "BLUE" tým

- Společně v sídle NCKB
  - Národní Centrum Kybernetické Bezpečnosti, BRNO
- 30+ členů
  - doporučeno 14? ☺
- Složení
  - Převážně NBU
  - CESNET, CZ.NIC
  - MUNI,VZ, …

Infrastruktura

- Kompletně virtualizovaná
  - VMware
- Identická pro všechny BLUE týmy
  - 20x cca 120 zařízení
  - + stroje RED, GREEN, WHITE týmů
- Přístup do „GAMENETU“ přes VPN
  - + management

Infrastruktura

- 3x FW (Mikrotik, pfSense, Vyatta)
- 2x CSR (Cisco Cloud Service Router) 1000V
- Podsítě
  - DMZ, OPS, LAB, GDT, SEC, ICS, PWR,HQ, DRONE

Pravidla hry

- RED
  - Útočí rovnoměrně na všechny BLUE týmy
  - Neútočí na management, základní infrastrukturu GREEN, nemění účty pro skórování
- BLUE
  - Dle tabulky seznam uživatelských kont
  - Nemění nastavení DNS serverů
  - Nevyužívá VPN pro stahování logů, odklonu komunikace či testování zranitelností
  - Systémy dostupné dle „tabulky dostupnosti“

Bodování

- Dostupnost
  - Automatické testování („scoring bot“)
- Použitelnost
  - Simulace uživatelů
- Úspěšný útok
  - Srážka bodů, lze získat za kvalitní report
- Situační reporty - SITREPS
  - 2x denně globální report
- Sdílení informací
- Právní, mediální, forenzní úkoly
- Požadavek na GREEN tým

Přípravná fáze – “Familiarization period”

- Týden před hlavní fází
  - 2 dny
  - Seznámení s prostředím
- Odpovědnost
  - R1 a R2
  - FW3 – Vyatta (VyOS)
  - GDT – Win7, Win10, Win2012 R2

Hlavní fáze

- Úterý
  - Možnost testování navrhovaných řešení
  - Testování infrastruktury, komunikace (RED, GREEN, WHITE)
- Středa
  - 8:00 – začátek, 30 minut „hájení“
  - 17:00 – konec prvního dne, zamezení přístupu do GAMETNETu
- Čtvrtek
  - 8:00 – začátek
  - 17:00 – konec cvičení

Windows

- Vzdálený přístup do příkazové řádky
- Sběr základních informací
  - systeminfo; net user; net localgroup administrators; net localgroup "Remote Desktop Users"; net share; …
- Uživatelská konta
  - Změna hesel, odebrání nepotřebných
- Antivir
  - Windows defender, následně Kaspersky
- Aktualizace
  - Možné instalovat aktualizace z wsus.ex

Windows

- Nastavení systému
  - Vypnutí LM a NTLMv1, vypnutí SMBv1, SMB signing
- Vypnutí cache uživatelských kredencí
- Security logy
- Firewall
- AppLocker???
- Vlastní skript
  - Výpis procesů + síťová komunikace

Vyatta (VyOS)

- Debian-based
- Záloha
  - tar czf /tmp/fw3-base.tgz /bin /boot /config /etc /home /lib /lib64 /opt /root /sbin /usr /var
- Změna hesel, odebrání nepotřebných účtů
- Vypnout nepotřebné démony
- Změnit FW
  - Vlastní iptables

Vyatta (VyOS) – sshd backdoor

- Hledání napadených binárek
  - find /var/lib/dpkg/info/ -name "*md5sums" -exec md5sum -c {} \; | grep -v OK

usr/bin/scp: **FAILED**

usr/bin/sftp: **FAILED**

usr/bin/ssh: **FAILED**

md5sum: WARNING: **3 of 39 computed checksums did NOT match**

R1 a R2 (Cisco IOS)

- Zrušení nadbytečné konfigurace
  - no enable password
  - username kostenec privilege 15 secret SuperHesloXXXXXX.2017
  - no username admin
  - no snmp-server community public RO
  - no snmp-server community private RW
  - no ip http server
  - no ip http secure-server
  - transport input ssh
- Tuning BGP

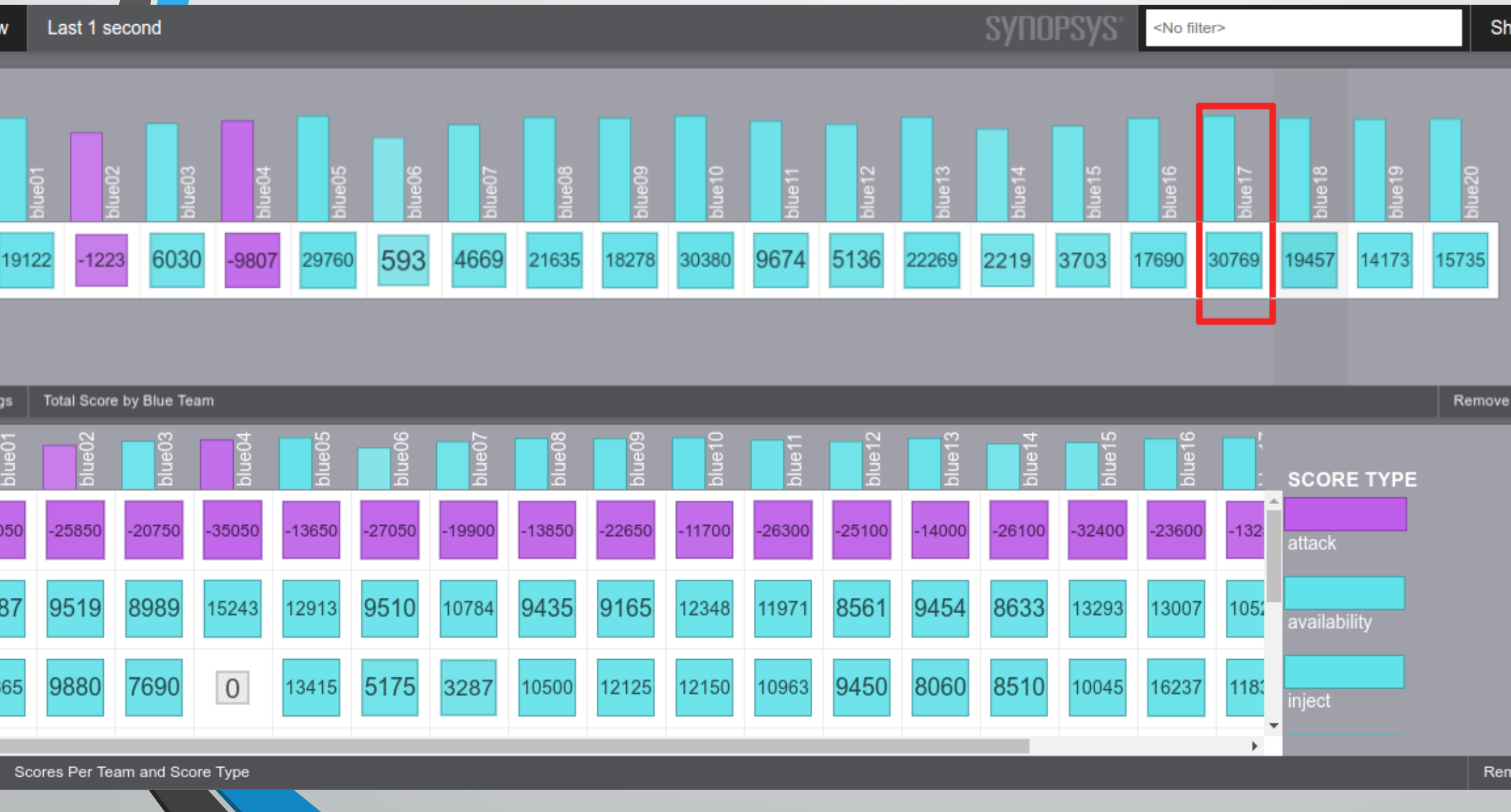
Cíle cvičení

- Síťové prostředí
- Správa OS a prevence útoků
- Monitoring sítě, detekce a řešení problémů
- Řešení incidentů
- Forenzní úkoly
- Týmová práce

Cíle cvičení

- Kooperace, sdílení informací
- Schopnost globálního vyhodnocení situace
- Reporting
- Krizové scénáře
- Časový management a prioritizace úkolů/činností


LOCKED
SHIELDS
BT01
BT02
BT03
BT04
BT05
BT06
BT07
BT08
BT09
BT10
BT11
BT12
BT13
BT14
BT16
BT17
BT18
BT19
BT20


Last 1 second
SYNOPSYS
<No filter>
blue01 blue02 blue03 blue04 blue05 blue06 blue07 blue08 blue09 blue10 blue11 blue12 blue13 blue14 blue15 blue16 blue17 blue18 blue19 blue20
19122 -1223 6030 -9807 29760 593 4669 21635 18278 30380 9674 5136 22269 2219 3703 17690 30769 19457 14173 15735
Total Score by Blue Team
Remove
blue01 blue02 blue03 blue04 blue05 blue06 blue07 blue08 blue09 blue10 blue11 blue12 blue13 blue14 blue15 blue16
-25850 -20750 -35050 -13650 -27050 -19900 -13850 -22650 -11700 -26300 -25100 -14000 -26100 -32400 -23600
9519 8989 15243 12913 9510 10784 9435 9165 12348 11971 8561 9454 8633 13293 13007
9880 7690 0 13415 5175 3287 10500 12125 12150 10963 9450 8060 8510 10045 16237
SCORE TYPE
attack
availability
inject
Scores Per Team and Score Type

Dotazy?


BT06
BT07
BT08
BT09
BT11
BT12
BT13
BT14
BT16
BT17
BT18
SIEMENS
LOCKED
2017
LOCKED SHIELDS