TRAINING NAME: Blue teamer

DURATION: 10 days

TRAINING OVERVIEW:

Training starts with the introduction to cyber security types and terminology covering wide range of topics like attack types and frameworks as well as key defense concepts, followed by the international cyber related laws and regulations. Networking protocols and devices are covered next, explaining the TCP/IP suite of protocols and various networking devices. Network cabling and physical devices will be explained too. Participants will also learn about the equipment, technologies and techniques used to protect network traffic and network integrity. Windows and Linux protocols and applications used to protect OS and network communication will be reviewed and explained. Training covers the OS and application virtualization technologies, including type 1 and type 2 hypervisors. Participants will learn about Wi-Fi and attack types and possible protections for WEP, WPA, WPA2 and WPA3 protocols.

Everything is in the cloud today, so understanding the big three (Amazon AWS, Microsoft Azure, and Google Cloud) and their differences is a must have knowledge. Participants will learn about the client and cloud provider responsibilities in the cloud environment and some of the options the big three are offering for the data and communication protection. Also, the migration paths and tools provided by CSPs (Cloud Service Providers) to move the data to and from the cloud will be reviewed.

Participants will learn about the network traffic and log analysis, and how to become the productive member of the SOC (Security Operations Center) or NOC (Network Operations Centers) teams by understanding not only the network traffic and log analysis, but by understanding SIEM (Security Information and Event Management) systems, threat intelligence and other log collection and analysis tools. DFIR (Digital Forensics and Incident response) is also an important topic that will prepare the participants to be a productive team member during incident handling process and computer forensic investigations.

Self-study modules (Risk management, Backup and BCDR, and policies and procedures) will help the participants to additionally protect their infrastructure and make it more resilient to both hacking and accidental data destruction.

In the practical part of this training, participants will have the opportunity to start from scratch by installing and configuring the virtualization platform, preparing, configuring, and installing the OSs and networking devices in the virtual environment that will be used throughout the training. Participants will configure both Windows and Linux servers as a router, firewall and VPN server, while Mikrotik router and pfSense firewall will be configured during the networking section of the training. Participants will also configure the Snort IDS/IPS. In Windows section, participants will install and configure AD, configure the group policies, implement the patch management, implement security controls based on JIT (just-in-time) and JEA (Just-enough administration) concepts, perform Windows hardening, implement IIS, implement OS and application virtualization, etc. In Linux section, participants will harden the Linux OS by using the AppArmor and SELinux, automate the Linux configuration and installation with Ansible, implement OS and application virtualization, etc. Wi-Fi will be configured in a secure way by utilizing the client isolation for public networks and RADIUS with certificates for secure enterprise authentication. For cloud LABs we will use the vendors LABs, as the cloud landscape is changing rapidly and best way to practice it is to use vendor official and free LABs. While this part is executed as a self-study, participants will be provided with all required instructions to execute those vendor labsto . For network traffic and log analysis we will use

Wireshark, Splunk, Zeek (formerly known as Bro) and centralized log collection systems like syslog. SIEM and threat intelligence module will cover the Wazuh and OSSIM + OTX. In the DFIR section participants will analyze the network traffic in the .pcap files to recognize the network and malware attacks. Participants will also analyze the memory and bitstream disk image, recover the deleted data from disk image, analyze the EXIF metadata, etc.

This training includes large number of labs and total time for their execution exceeds overall duration of this training., Participants are encouraged to continue to practice the labs on their own pace after the training, as they will create the lab machines during the training, and will have an option to continue to use them afterwards.

KEY LEARNING OUTCOMES:

- Understand the cyber attack types and terminology.
- Understand the international cyber laws and compliance.
- Understand networking basics, including the protocols, cabling, and devices.
- Understand the tools one can use to protect the networks.
- Know how to securely configure Windows and Linux servers as a router, VPN server, web server and the firewall.
- Know how to configure open-source firewall and IDS devices like pfSense and Snort.
- Understand Dos/DDoS concepts and the options one must mitigate the issue.
- Understand Windows tools one can use to deploy secure and hardened systems.
- Know how to use Windows built-in tools for secure deployment and usage.
- Understand Linux tools one can use to deploy secure and hardened systems.
- Know how to use Linux built-in tools for secure deployment and usage.
- Understand Wi-Fi protocols and protection options.
- Understand cloud security issues and some of the tools the big three offer.
- Understand the network logs and traffic analysis.
- Know how to use free and paid tools for centralized log collection and analysis.
- Understand the incident handling and computer forensics as an asset in the enterprise environment.
- Know how to use the tools to conduct the internal digital forensics as part of incident handling process.
- Understand the importance of risk management in information and computer security.
- Understanding the concepts behind the BCDR.

THIS TRAINING IS IDEAL FOR:

- Anyone interested in becoming a part of the blue team.
- Participants looking for a training that will cover the 360 views of the topics needed to become a good blue teamer.
- Participants that do not have the experience as a network and system administrators (the first 5 days of the training).
- Participants that want to learn more about monitoring and incident handling (days 6-10), like system and network administrators, and junior NOC and SOC members.

PREREQUISITES:

- Advanced usage of operating systems (Windows and Linux)
- Understand the IT infrastructure and how the parts fit into it is a bonus.

- During the first five days of the training participants will get an overall picture and there are no specific prerequisites. Days 6-10 do require the full understanding of the first five days topics though.

TRAINING AGENDA:

Cyber attack types and terminology is the introductory module that explains the essential terminology used in cyber security, including the data states and the protections that can be used in each of them. Concepts of Blue/Red/Purple and Yellow/Orange/Green teams will be explained. Participants will also learn about Lockheed's Martin Cyber Kill chain, zero trust model and Software defined perimeter. There are some generic attacks being explained and some of them will be demonstrated here, such as MitM and RP spoofing, and with help of it sniffing of the clear text passwords, HTTPS MitM and SSL strip from the Network attacks, few Web application attacks from OWASP top 10 list, such as SQLi, OS command injection, XSS and Log4Shell vulnerability. Then the device attacks will be covered, such as attack on the Mikrotik router. In the OS and services attacks section we will demonstrate Attack on Windows by using a Print Nightmare vulnerability and attacking the Linux with misconfigured sudo privileges. Lastly, in the Client-side attacks section, attack on a client through vulnerable office and malicious office document will be demonstrated.

Law & compliance module will cover UK laws and some laws from US, Australia and Russia including the problematic CLOUD act from US. NIS directive and GDPR will be covered too

Networking basics module will cover TCP/IP suites of protocols, including the OSI and TCP/IP models, IPv4 and IPv4, and various protocols that exist on the TCP/IP stack, such as ARP, DNS, DHCP, SNMP, SMTP, FTP, TFTP, SSH, VoIP, etc. Participants will learn about the networking types, network topologies and network technologies. Additionally, cabling used to establish the interconnections between the network nodes, such as twisted pair, optical and coaxial, will be covered. This module concludes with networking devices, such as switches, routers, firewalls, IDS/IPS, etc., and software defined networking.

Securing networks module will emphasize the devices used to protect the network traffic and network itself, providing the participants with opportunity to acquire knowledge for configuring some of these components, such as routers and VLANS, Firewalls and Proxy servers, VPNs, IDS/IPS devices. In this module, the Dos/DDoS attacks will be discussed too, and participants will have the opportunity to try some of the DoS attacks against the infrastructure they will create during the lab part of the lectures.

Securing Windows OS and services module will first cover the basics of Windows command prompt, terminal, and PowerShell, and then the Windows powerful security features will be reviewed, such as core strategies for administrative privileges, like PAM/JEA/JIT (Privileged Access Management/Just Enough Administration/Just in Time Administration), Windows Defender credential guard, LAPS, AppLocker, BitLocker, etc. Participants will also learn about password policies, account lockout policies, baselines and OS hardening by using CIS benchmarks, Windows patch management, Windows file permission basics, passwords and password protection and attacks, MFA and SSO, biometrics, AD basics, AD attacks, and Kerberos. OS and application virtualization on Windows will be covered as well, such as Hyper-V and docker/docker for desktop and remote access RDP. This module concludes by focusing on how to secure the boot process with trusted boot, ELAM (Early Launch Anti-Malware), Measured boot and TPM 2.0 which is the prerequisite for the Windows 11. Labs will cover many of the above-mentioned technologies.

Securing Linux OS and services module covers the Bash basics, Linux boot process, Linux troubleshooting tools and Linux file permission basics including Linux ACLs. After this introduction,

participants will learn about the Linux passwords, and Linux security features, such as AppArmor, SELinux, seccomp, cgroups and chroot. Next, Linux kernel firewall iptables will be reviewed, with some examples on how to use it during various troubleshooting steps. Participants will also learn about the Linux patching techniques, and how to harden Linux OS. Besides that, Linux OS and application virtualization will be reviewed, such as KVM, XEN, Citrix hypervisor, QEMU, and VMware ESXi (ESXi is NOT a Linux distribution as per VMware, even though it is using some of the same core commands). Within this module, docker will be further discussed. This module concludes by providing the introduction into the auditing and centralized logging like rsyslog, auditd, and 3rd party tools like ELK and Splunk, since these tools will be reviewed in more details during the 2nd week of the training.

Wi-Fi security module reviews the Wi-Fi protocols and security issues of each of the protocol. Additionally, participants will learn about mostly used attacks on Wi-Fi networks, and available security protections and tools. This module concludes by reviewing the enterprise Wi-Fi supported by RADIUS (Remote Access Dial-in User Service).

Cloud security module discusses the cloud basics. IT is important to understand that the cloud is evolving at the pace that cannot be followed by a normal computer user. Therefore, some "basic" cloud protection tools and services will be covered during this module, followed by the overview of the cloud basics and client/cloud service provider responsibilities. The big three (Amazon AWS, Microsoft Azure, and Google cloud) will be covered from the perspective of available tools and datacenter design, datacenter security, datacenter, and services compliance, on-prem to cloud migration security considerations and migration process itself for VMs, data, databases, and applications. Participants will also learn which tools exist to connect to the cloud securely, tools available to secure access to publicly facing resources, monitoring the cloud security, and additional security services. Theoretical part of this module concludes with the CSA (Cloud Security Alliance) and the options one has on hand to audit CSPs.

Labs are not provided directly in the class lab environment. Participants will use free and publicly available vendor labs during the training.

Network traffic and log analysis module introduces the tools one can use to capture and analyze the network traffic, such as Wireshark, tcpdump, network miner and zeek. It also introduces the various log types and defines the logs and their applicability in various processes including troubleshooting, system monitoring, incident handling, compliance and forensic analysis. Once, differentiation between local and centralized logging types is discussed, Windows, Linux, network devices and web server logs and tools will be covered.

SIEM and threat intelligence module will define the SIEM solutions and market leaders including paid versions like Splunk Enterprise, IBM QRadar, and Rapid7 InsightDR, and open source SIEM tools like OSSIM, ELK, SIEMonster, etc. Threat intelligence lifecycle and use cases and types will be defined in this module, including the IoC (Indicators of Compromise) and IoA (Indicators of Attack).

DFIR module will define both the Digital forensics and incident response, as the name suggests. Participants will have the opportunity to familiarize themselves with the NIST incident handling, ENISA incident management and MITRE ATT&CK frameworks. Participants will learn about the incident handling process, and about adversary TTPs (Tactics, Techniques and Procedures). Computer forensics lesson will cover computer forensics concepts such as the value of the digital evidence, how to create a bit-stream copy, how to approach the digital evidence during the incident and/or investigation, etc., data storage systems and concept, file systems, memory forensics, steganography, and malware forensics.

Self-study modules cover **risk management** and **backup and BCDR.** These modules will help participants to complete the 360-view into the world of cyber security and help them understand why it is so important to secure the systems and which systems to secure, how much money it makes sense to invest in the protections, etc. from the risk management point of view, while the backup and BCDR module will define the importance of creating disaster resilient system in order to support the business.

ABOUT THE TRAINER:



Robert Petrunić works as a senior information security consultant in Eduron IS, the company dedicated to IT security education, penetration testing and computer forensics.

Robert is Microsoft certified trainer since 2002, EC-Council certified trainer since 2008 and $(ISC)^2$ certified trainer since 2014. Today, he lectures mostly hacking and security related courses for red teams and DFIR (Digital Forensics and Incident Response) related courses for blue team members. Since 2004, he worked primarily in the security field, and Microsoft acknowledged this in 2008, by assigning him the most valuable Microsoft's professional recognition for nine years in a row.

For the last eighteen years Robert is working on programs related to ethical hacking and IT security awareness for systems administrators, developers, and IT security consultants. He is also often a lecturer at regional IT conferences.

Robert holds many industry certifications, such as $(ISC)^2$ CISSP and CCSP, Offensive Security OSCP, OSCE and OSWP, EC-Council CPENT, CEH, CHFI, CND, ECIH to name the few.