PurpleLABS - Detection Infrastructure as Service + Offensive Labs

"Learn how to use "Detection as code" strategy for finding blind spots in your SOC environment."

DEFENSIVE SECURITY

Lab overview

PurpleLABS is a dedicated virtual infrastructure for conducting detection and analysis of attackers' behavior in terms of used techniques, tactics, procedures and offensive tools. The environment is to serve the constant improvement of competences in the field of threat hunting (threat hunting) and learning about current trends of offensive actions (red teaming) in direct detection (blue teaming).

PurpleLABS provides analytical interfaces for all relevant data sources from individual systems and network services available in the virtual infrastructure (sysmon, windows events, fw, bro, suricata, osquery, auth, powershell, waf, proxy, audit).

We are aware that offensive workshops available on the market are considered more "sexy" because of the challenges they pose to the participants, where individual exercise scenarios require focus, commitment and an open mind. In PurpleLABS, offensive actions serve only as an intermediate stage to achieve the actual goal of the training.

Goal

The primary goal of PurpleLABS is to generate offensive attack events / symptoms within systems and networks that later should be detected by Open Source SOC stack including Sigma - the open standard event description rule set and the rest of dedicated, open source security solutions in use.

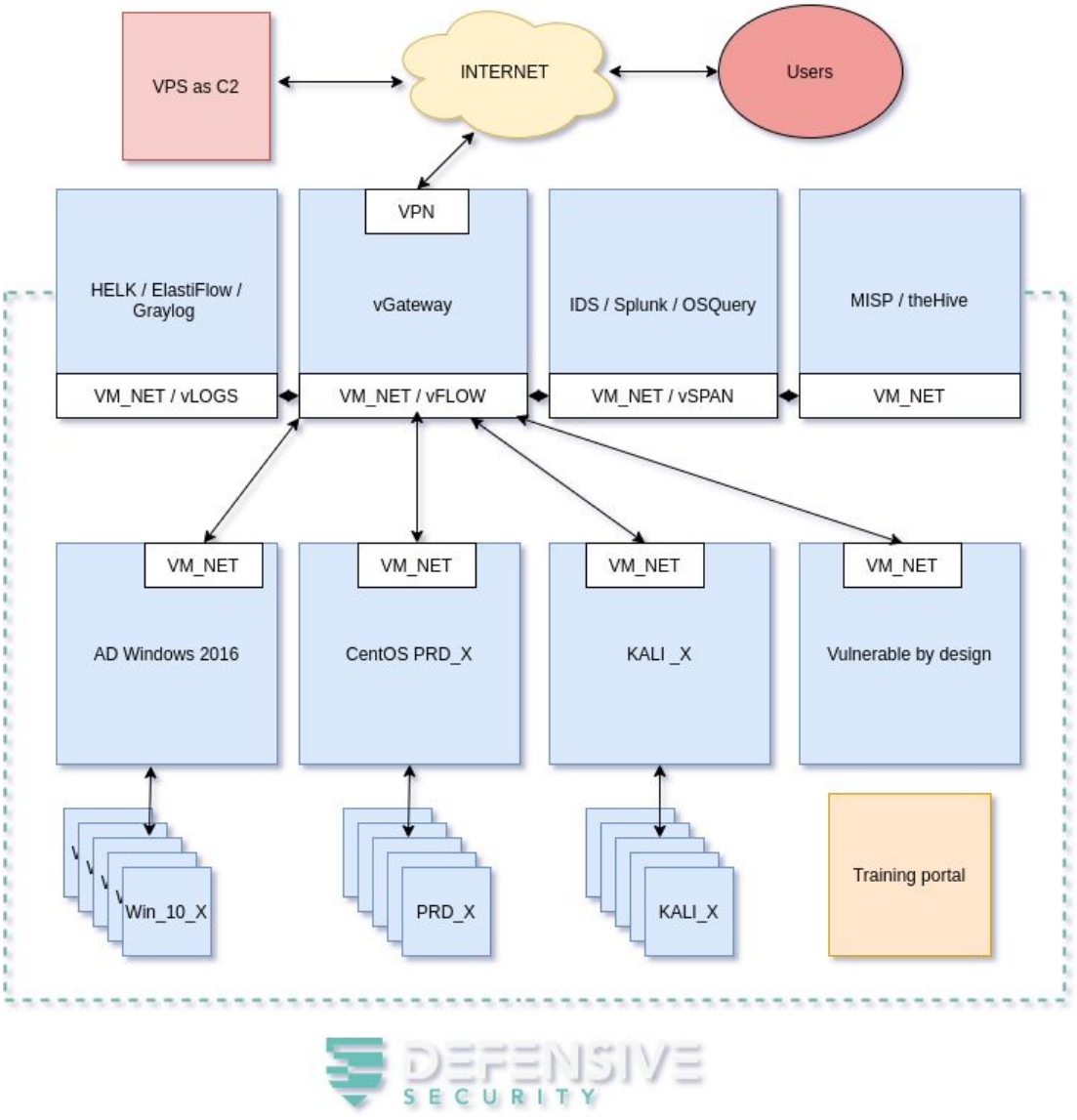
In this way, participants will thoroughly familiarize themselves with the content of the available detection rules and their structure, better understand the essence of offensive actions, learn the low-level relationships between data sources, and thus achieve knowledge in creating their own detection rules and bypassing them. We called this approach 'flip mode', i.e. learn protection through attack in an attractive, standardized form driven by the Open Source community. In addition, participants will use a whole range of open-source (and commercial) solutions dedicated to SOC environments.

We believe that the unique approach of 'Detection as Code vs Adversary Simulations' in a condensed format will allow to increase the level of knowledge in the field of RED / BLUE / PURPLE to both experienced specialists and beginners while maintaining the attractiveness and pleasure of performed tasks - detection does not have to be boring and tedious!

Mission statement

Our mission is to provide knowledge and skills in the field of "Purple Teaming" in the most attractive and affordable way by providing high quality training materials and laboratory environments in a scalable online format.
We want to enable business to improve the detection capability of their SOC teams and achieve better visibility and resistance to attacks. We strongly believe that only combination of deep, low level defensive and offensive security skills guarantee secure and successful deployments.

Network Architecture



- Build on top of powerful dedicated servers:
    - Intel® Xeon® W-2145 Octa-Core Skylake W
    - 64GB / 128GB RAM
    - 2x SSD
    - 1 GBit/s port
- Lab environment includes:
    - AD Windows Domain Controller 2016
    - Windows 10 workstations
    - CentOS / Ubuntu Linux servers
    - Kali Linux desktops
    - vSPAN / vNetflow
    - IDS / IPS
    - Log aggregators and collectors
    - Security event analytics solutions
    - WAF / Proxy server
    - SSH Jump host
    - Vulnerable by design hosts

Software in use

- Defensive tools:
    - OSQuery, Kolide Fleet, Graylog, Elastiflow, Wazuh / OSSEC, ELK, HELK, Splunk, Sigma, Sysmon, BRO/Zeek IDS, Suricata IDS, eBPF, auditd / go-audit, Sysdig, Wireshark, tcpdump, syslogd, Filebeat, Winlogbeat, Rita, MISP, theHive, Cortex, iptables, ngrep, LMD, rkhunter, Volatility Framework, GRR Rapid Response, nsjail, mod_security, LKRG, Yara, Squid Proxy, Wireguard and many more.

- Offensive tools:
    - PowerSploit, Bloodhound, goDoH, dnscat2, nmap, Empire Framework, Metasploit Framework, WMImplant, Invoke-PipeShell, Sharpshooter, PIngCastle, RTA, Atomic Red Team, kerbrute, CME, Salsa tools, Octopus, mimikatz, PSAttack, Weasel, impacket, pyexfil, scapy, Shellter, proxychains, Singularity, poshC2, dns2tcp, Pupy, sg1, DET, xfltreat, fruityC2, tuna, RATTE, nishang, corkscrew, Egress-assess, pivoter, hydra, wondjina, Trevor C2, C3, Koadic, Apfell, sharpSocks, Silent Trinity, WSC2, google_socks, sqlmap, BeeF Framework, twittor, torify, TheFatRat, cloakify, WMIsploit, certreq, Faction C2, Merlin, ThunderShell, udp2raw, PowerLessShell, reGeorg, rpivot, WSC2, thc-flood, yersinia, DNSexfiltrator, SMBmap, testssl, firebolt, Sliver, dumpster fire, APT simulator, icmptunnel, ChunkyTuna, Invoke-DOSfuscation and more

What is included in the package

- VPN access to PurpleLABS cloud Infrastructure
- Dedicated Windows 10 and Kali Linux per student
- Pre-configured remote VPS per student
- Online training materials
- Slack channel access and private forum as a support services
- New lab instructions every single month including attack and detection phases
- Mapping APT group techniques to specific workshop scenarios, Sigma rules and MITRE ATT&CK Framework
- An arsenal of configured simulation tools and C2 frameworks available by default

---

What you will learn

- Learn ways to improve your detection and event correlations skills across many different data sources by using a Sigma - an open standard for rules that allow you to describe searches on log data in generic form
- Find and understand malicious activities and identify threats details in the Windows and Linux network
- Prepare your SOC team for fast filtering out network noise and allow for better incident response handling
- Profile your critical OS and network segments in terms of ‘normal vs suspicious’ behaviour
- Find out how Open Source Software can support your SOC infrastructure from red and blue perspective
- Learn current trends, techniques, and tools for network exfiltration, lateral movement and post-exploitation attack phases
- Understand the value of DLP / IDS / IPS / FW / WAF / Memory Forensics against real adversary lab scenarios
- Understand values from an automated approach to simulating attackers and generating network and system anomalies
- Identify blind spots in your network security posture
- Do your own research within the environment regardless of the lab instructions

---

Contents (as of March 2020)

1. Kerbrute_detection.
2. Sysmon_lsass_memory_dump_spraycatz.
3. Win_hack_bloodhound.
4. Win_powersploit_empire_schtasks.

5. Win_application_shimming.
6. Sysmon_psattack.
7. Backdooring_Winlogon.
8. Win_susp_vssadmin_ntds_activity.
9. Ip_whitelisting.
10. Sysmon_ads_executable.
11. Detecting_wce_editor.
12. Win_powershell_suspicious_parameter_variation.
13. Bro_Meterpreter_network_detection.
14. Linux_fileless_detection.
15. Icmp_anyone?
16. Dns_tunneling_noise.
17. Hiding_behind_ja3
18. LDAP_as_hidden_storage.
19. Fighting_with_AD_as_C2.
20. Rebinding_the_dns_anomalies.
21. Payload_in_TLS.
22. Webshells_vs_yara.
23. Shadow_copy_over_WMI
24. AAAA_C2.
25. Stop_disabling_SELinux.
26. Detecting_linux_injections.
27. Slack_vs_SlackC2.
28. Netflow_for_help!
29. C2_likes_pipes.
30. Rootkits_vs_LKRG.

About us

At Defensive Security we focus on teaching you best practices in securing your Network Infrastructures. Almost 15 years of experience, best ever training flow and high passion level guarantee you one of best in the market IT Security Education & Open Source Security Solution Services. We strongly believe that only combination of deep level defensive and offensive security skills can guarantee secure and safe deployments. With more than 1k trained students we delivered training, workshops and talks globally during:

- BruCON Belgium
- Black Hat USA
- 44CON UK
- Hack in The Box Amsterdam / Singapore / Dubai
- HITB + Cyberweek Abu Dhabi
- OWASP Appsec USA
- FloCON USA
- Confidence PL

- Cyber Hagen Denmark

Contact

- Phone: (0048) 791 611 309
- Email: training@defensive-security.com
- WWW: https://defensive-security.com