PENTEST IOT/OT - OVERVIEW

JOAS ANTONIO

DETAILS

- This is a pdf about pentest in IoT and OT, hope it's useful!
- https://www.linkedin.com/in/joas-antonio-dos-santos/

WHAT IS IOT/OT?

- https://www.nozominetworks.com/?gclid=CjwKCAjwhuCKBhADEiwA1HegOenrCu-qZkLLfb8neAeuv7fSKPzfvah9v6LvDgbUTNuE1JZf_xBR_BoC4RUQAvD_BwE
- https://securityboulevard.com/2020/09/iot-security-fundamentals-iot-vs-ot-operational-technology/
- https://www.aloxy.io/publications/introduction-to-industrial-iot
- https://www.i-scoop.eu/internet-of-things-iot/industrial-internet-things-it-ot/
- https://searchitoperations.techtarget.com/definition/IT-OT-convergence
- https://www.tripwire.com/state-of-security/featured/the-iot-convergence-how-it-and-ot-can-work-together-to-secure-the-internet-of-things/
- https://en.wikipedia.org/wiki/Operational_technology
- https://www.coolfiresolutions.com/blog/difference-between-it-ot/
- https://www.forcepoint.com/cyber-edu/ot-operational-technology-security

WHAT IS IOT/OT?

- https://www.gartner.com/en/information-technology/glossary/operational-technology-ot
- https://www.cisco.com/c/en/us/solutions/internet-of-things/what-is-ot-vs-it.html
- https://atos.net/wp-content/uploads/2020/12/Q1_2021_CyberSecurity_Magazine_Future_of_IoT_and-OT-security.pdf
- https://www.fortinet.com/solutions/industries/scada-industrial-control-systems/what-is-ot-security
- https://www.sierrawireless.com/iot-blog/it-ot-convergence/
- https://medium.com/@prashunjaveri/the-seven-layers-of-iot-it-vs-ot-debate-and-the-role-of-iot-c5303066f615
- https://www.csoonline.com/article/3279545/it-ot-and-iot-existential-technology-lifecycle-management.html

WHAT IS IOT/OT?

- https://www.sas.com/en_us/insights/articles/big-data/it-ot-convergence-the-dilemma-of-the-iot-perception-gap.html
- http://trustcentral.com/use-cases/operational-technology-ot-and-iiot/
- https://cementanswers.com/what-is-ot-in-iot/
- https://www.b-sec.net/en/assessment/
- https://tulip.co/blog/it-ot-convergence-tips-for-gaining-visibility-in-your-connected-factory/

OPERATION TECHNOLOGY SECURITY

- https://www.fortinet.com/content/dam/fortinet/assets/analyst-reports/report-state-of-operational-technology.pdf
- https://www.pwc.com.au/industry/energy-utilities-mining/mining/assets/cyber-savvy-top-10-ot-issues-feb18.pdf
- https://media.defense.gov/2021/Apr/29/2002630479/-1/-1/1/CSA_STOP-MCA-AGAINST-OT_UOO13672321.PDF
- https://cpb-eu-w2.wpmucdn.com/blogs.bristol.ac.uk/dist/0/610/files/2020/08/SOC-UC-developments-for-OT.pdf
- https://www.cisa.gov/sites/default/files/publications/CISA_Fact_Sheet-Rising_Ransomware_Threat_to_OT_Assets_508C.pdf
- https://www.forescout.com/resources/ics-solution-brief/
- https://www.checkpoint.com/downloads/products/top-10-cybersecurity-vulnerabilities-threat-for-critical-infrastructure-scada-ics.pdf
- https://www.cisco.com/c/dam/en_us/solutions/industries/manufacturing/ITOT-convergence-whitepaper.pdf
- https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-82r2.pdf
- https://www2.deloitte.com/content/dam/Deloitte/us/Documents/about-deloitte/us-deloitte-google-cloud-alliance-future-of-the-SOC-whitepaper.pdf

OPERATION TECHNOLOGY SECURITY

- https://www2.deloitte.com/content/dam/Deloitte/us/Documents/about-deloitte/us-deloitte-google-cloud-alliance-future-of-the-SOC-whitepaper.pdf
- https://www.sgs.com/-/media/global/documents/flyers-and-leaflets/sgs-tuev-br8-it-sicherheit-en-a4.pdf
- https://assets.siemens-energy.com/siemens/assets/api/uuid:b3b1da61-d4d3-46fa-a43d-bff249b75835/pipelinetechjournal-key-cyber-security-controls-pipelines-articl.pdf
- https://www.secureops.com/wp-content/uploads/2021/06/Critical-Elements-of-Improving-Effectiveness-of-SOC-v2.pdf
- https://www.hse.gov.uk/foi/internalops/og/og-0086.pdf
- https://www.mckinsey.com/~/media/McKinsey/McKinsey%20Solutions/Cyber%20Solutions/Perspectives%20on%20transforming%20cybersecurity/Transforming%20cybersecurity_March2019.ashx
- https://www.infradata.com/resources/what-is-ot-security/
- https://www.forescout.com/solutions/ot-security/

OPERATION TECHNOLOGY SECURITY

- https://www.otorio.com/blog/it-security-vs-ot-security-the-operational-technology-cybersecurity-guide-for-industry-professionals/
- https://www.ibm.com/br-pt/security/operational-technology
- https://www.checkpoint.com/cyber-hub/network-security/what-is-operational-technology-ot-security/
- https://verveindustrial.com/resources/blog/the-ultimate-guide-to-understanding-ot-security/
- https://csrc.nist.gov/projects/operational-technology-security
- https://www.zscaler.com/resources/security-terms-glossary/what-is-ot-security

INTERNET OF THINGS SECURITY

- https://www.otorio.com/blog/it-security-vs-ot-security-the-operational-technology-cybersecurity-guide-for-industry-professionals/
- https://www.ibm.com/br-pt/security/operational-technology
- https://www.checkpoint.com/cyber-hub/network-security/what-is-operational-technology-ot-security/
- https://verveindustrial.com/resources/blog/the-ultimate-guide-to-understanding-ot-security/
- https://csrc.nist.gov/projects/operational-technology-security
- https://www.zscaler.com/resources/security-terms-glossary/what-is-ot-security
- https://www.thalesgroup.com/en/markets/digital-identity-and-security/iot/iot-security#:~:text=IoT%20security%20is%20the%20practice,confidentiality%20of%20your%20IoT%20solution.
- https://www.iotsecurityfoundation.org/
- https://www.fortinet.com/resources/cyberglossary/iot-security
- https://internetofthingsagenda.techtarget.com/definition/IoT-security-Internet-of-Things-security
- https://www.kaspersky.com/resource-center/definitions/what-is-iot
- https://www.arm.com/glossary/iot-security

INTERNET OF THINGS SECURITY

- https://www.forescout.com/resources/internet-things-solution-brief/
- https://www.icao.int/Meetings/MIDCyberSec/PublishingImages/Pages/Presentations/4_1_Cyber%20Security.pdf
- https://www.meti.go.jp/policy/netsecurity/wg1/IoT-SSF_ver1.0_eng.pdf
- https://i.blackhat.com/eu-19/Thursday/eu-19-Lin-Understanding-The-IoT-Threat-Landscape-And-A-Home-Appliance-Manufactures-Approach-To-Counter-Threats-To-IoT-2.pdf
- https://www.blackhat.com/docs/asia-16/materials/asia-16-Zillner-Lets-See-Whats-Out-There-Mapping-The-Wireless-IOT.pdf
- https://i.blackhat.com/us-18/Thu-August-9/us-18-Palansky-Legal-Liability-For-IoT-Vulnerabilities.pdf
- https://www.blackhat.com/docs/us-17/wednesday/us-17-Rios-When-IoT-Attacks-Understanding-The-Safety-Risks-Associated-With-Connected-Devices-wp.pdf
- https://i.blackhat.com/USA-19/Thursday/us-19-Ray-Moving-From-Hacking-IoT-Gadgets-To-Breaking-Into-One-Of-Europes-Highest-Hotel-Suites.pdf
- https://i.blackhat.com/briefings/asia/2018/asia-18-Yang-UbootKit-A-Worm-Attack-for-the-Bootloader-of-IoT-Devices.pdf
- https://www.blackhat.com/docs/us-17/thursday/us-17-Luo-Iotcandyjar-Towards-An-Intelligent-Interaction-Honeypot-For-IoT-Devices.pdf

PENTEST OT/IOT

WIRESHARK

- https://wiki.wireshark.org/DisplayFilters
- https://www.wireshark.org/docs/man-pages/wireshark-filter.html
- https://www.wireshark.org/docs/wsug_html_chunked/ChWorkBuildDisplayFilterSection.html
- https://www.wireshark.org/docs/wsug_html_chunked/ChWorkDisplayFilterSection.html
- https://www.networkdatapedia.com/post/2019/01/29/top-10-wireshark-filters
- https://medium.com/hacker-toolbelt/wireshark-filters-list-983c49468a45
- https://networkproguide.com/epic-list-top-searched-wireshark-display-filters/
- https://insights.profitap.com/14-powerful-wireshark-filters-to-use
- https://www.comparitech.com/net-admin/wireshark-cheat-sheet/
- https://www.stationx.net/wireshark-cheat-sheet/
- https://medium.com/hacker-toolbelt/wireshark-filters-cheat-sheet-eacdc438969c

WIRESHARK

- https://www.youtube.com/watch?v=Mgpv5aF7U9Q&ab_channel=TheTechnologyFirm
- https://www.youtube.com/watch?v=wwMMoWTBwcY&ab_channel=Cisco
- https://www.alibabacloud.com/blog/how-to-analyze-the-network-behaviors-of-iot-enabled-devices-using-wireshark_595848
- https://ask.wireshark.org/question/9492/how-can-we-use-wireshark-to-sniff-data-from-wifi-based-iot-device-to-aws-s3/
- https://medium.com/@alexharasic/hijacking-your-home-iot-appliance-part-1-8c2aabdf950d
- https://github.com/arlotito/iot-device-wireshark
- https://www.garlandtechnology.com/blog/bridging-the-it-ot-iot-divide
- https://stackoverflow.com/questions/68889803/capturing-packets-using-wireshark-of-an-iot-device
- https://alibaba-cloud.medium.com/how-to-analyze-the-network-behaviors-of-iot-enabled-devices-using-wireshark-1c5fc914e869
- https://www.youtube.com/watch?v=P-aO2lLmmcI&ab_channel=akibafreaks
- https://www.youtube.com/watch?v=ltfWjpNcn20&ab_channel=Hak5
- https://www.youtube.com/watch?v=P-aO2lLmmcI&ab_channel=akibafreaks

NMAP

- https://github.com/ifding/iot/blob/master/rasp-pi/using-nmap-scan-network.md
- https://www.cyberciti.biz/security/nmap-command-examples-tutorials/
- https://insinuator.net/2016/04/discover-the-unknown-analyzing-an-iot-device/
- https://iotsecure.io/2021/05/beyond-nmap-port-scanner-better-detail-without-device-interference/
- https://www.lume.ufrgs.br/bitstream/handle/10183/222479/001126492.pdf?sequence=1
- https://nmap.org/book/osdetect-device-types.html
- https://mediakiosque.univ-pau.fr/video/9691-lab-4225-port-scanning-an-iot-device/
- https://www.diva-portal.org/smash/get/diva2:1464454/FULLTEXT01.pdf
- https://www.redhat.com/sysadmin/finding-rogue-devices

DISCOVERING

- https://www.netsparker.com/blog/web-security/discovering-hacking-iot-devices-using-web-based-attacks/
- http://ceur-ws.org/Vol-2597/paper-17.pdf
- https://www.cs.bham.ac.uk/~tpc/Papers/pentestingIoT.pdf
- https://securityboulevard.com/2021/08/why-penetration-testing-needs-to-be-part-of-your-iot-security/
- https://www.researchgate.net/publication/324813472_Penetration_Testing_in_the_IoT_Age
- https://medium.com/brandlitic/top-iot-hacking-tools-f9355e384db0
- https://github.com/Telefonica/HomePWN
- https://nostarch.com/practical-iot-hacking

DISCOVERING

- https://www.netsparker.com/blog/web-security/discovering-hacking-iot-devices-using-web-based-attacks/
- http://ceur-ws.org/Vol-2597/paper-17.pdf
- https://www.cs.bham.ac.uk/~tpc/Papers/pentestingIoT.pdf
- https://securityboulevard.com/2021/08/why-penetration-testing-needs-to-be-part-of-your-iot-security/
- https://www.researchgate.net/publication/324813472_Penetration_Testing_in_the_IoT_Age
- https://medium.com/brandlitic/top-iot-hacking-tools-f9355e384db0
- https://github.com/Telefonica/HomePWN
- https://nostarch.com/practical-iot-hacking

FCC DISCOVERY

- https://www.pentestpartners.com/security-blog/keep-your-iot-schematics-private/
- ftp://ftp.registro.br/pub/gts/gts34/04-IotHackingMethod.pdf
- https://www.fcc.gov/oet/ea/fccid
- https://www.youtube.com/watch?v=iFQy19CPNmM&ab_channel=CWNPTV

UART HACKING

- https://www.youtube.com/watch?v=6_Q663YkyXE&ab_channel=MakeMeHack
- https://www.youtube.com/watch?v=ZFM_F3eAw3k&ab_channel=rwg42985
- https://resources.infosecinstitute.com/topic/gaining-shell-access-via-uart-interface-part-1/
- https://medium.com/analytics-vidhya/uart-communication-4cef0840be2e
- https://payatu.com/blog/asmita-jha/hardware-attack-surface-uart
- https://nse.digital/pages/guides/hardware/uart.html
- https://ebookreading.net/view/book/EB9781484243008_6.html
- https://www.riverloopsecurity.com/blog/2020/01/hw-101-uart/
- https://labs.f-secure.com/archive/hacking-embedded-devices-uart-consoles/

I²C AND SPI

- https://www.riverloopsecurity.com/blog/2020/02/hw-101-spi/
- https://hackaday.com/tag/spi/
- https://sergioprado.org/bus-pirate-o-pirata-dos-barramentos/
- https://payatu.com/blog/asmita-jha/hardware-attack-surface-i2c
- https://nse.digital/pages/guides/hardware/i2c.html
- https://abrictosecurity.com/blog/introduction-to-hardware-hacking-part-1/
- https://elinux.org/images/d/d8/Stoppa.pdf
- https://news.ycombinator.com/item?id=26790862
- https://www.rapid7.com/blog/post/2019/02/20/iot-security-introduction-to-embedded-hardware-hacking/
- https://www.youtube.com/watch?v=H8Rkk8McYCw&ab_channel=Hugatry%27sHackVlog

EEPROM

- https://www.eevblog.com/forum/projects/hacking-a-test-equipment-best-way-to-read-and-modify-an-eeprom/
- https://www.tarlogic.com/blog/hardware-hacking-chip-off-for-beginners/
- https://labdegaragem.com/forum/topics/eeprom-24c01
- https://www.youtube.com/watch?v=LdhJD1EcsSc&ab_channel=SecuritySociety
- https://www.youtube.com/watch?v=Y31GoCOBMDI&ab_channel=antonanchev
- https://www.youtube.com/watch?v=MLnXEyarf4I&ab_channel=FlorianUhlemann
- https://www.youtube.com/watch?v=eUgadvawA1I&ab_channel=Electricks
- https://www.youtube.com/watch?v=OW95vw2_BxQ

JTAG DEBUGGING AND EXPLOITATION

- https://elinux.org/images/5/56/DebuggingWithJtagCelf2009.pdf
- https://www.xjtag.com/about-jtag/what-is-jtag/
- https://www.youtube.com/watch?v=3EVRL1CGMEo&ab_channel=hupstream
- https://www.youtube.com/watch?v=R0vLLndKQxA&ab_channel=ArduPilot
- https://www.youtube.com/watch?v=3xKB72SBOp4&ab_channel=IntelFPGA
- https://www.youtube.com/watch?v=EpA25bCHHtk&ab_channel=LiveOverflow
- https://sergioprado.org/linux-kernel-debugging-com-jtag/
- https://people.ece.cornell.edu/land/courses/ece4760/FinalProjects/s2009/jgs33_rrw32/Final%20Paper/index.html
- https://software-dl.ti.com/ccs/esd/documents/ccs_debugging_jtag_connectivity_issues.html
- https://www.youtube.com/watch?v=LcRMFXBuAh0&ab_channel=MattPratt
- https://www.embedded.com/debugging-the-linux-kernel-with-jtag/
- https://docs.espressif.com/projects/esp-idf/en/latest/esp32/api-guides/jtag-debugging/
- https://www.riverloopsecurity.com/blog/2021/07/hw-101-jtag-part3/

FIRMWARE REVERSE ENGINEERING AND EXPLOITATION

- https://embeddedbits.org/reverse-engineering-router-firmware-with-binwalk/
- https://www.youtube.com/watch?v=oqk3cU7ekag&ab_channel=EngineerMan
- https://www.youtube.com/watch?v=fkPSlBxh7Nw&ab_channel=hardwear.io
- https://www.youtube.com/watch?v=GIU4yJn2-2A&ab_channel=TonyGambacorta
- https://www.youtube.com/watch?v=ccgB3UuCxjE&ab_channel=HACKADAY
- https://resources.infosecinstitute.com/topic/iot-security-fundamentals-reverse-engineering-firmware/
- https://payatu.com/blog/munawwar/iot-security---part-7-reverse-engineering-an-iot-firmware
- https://hackaday.com/2011/05/30/reverse-engineering-embedded-device-firmware/
- https://blog.securelayer7.net/how-to-start-iot-device-firmware-reverse-engineering/
- https://medium.com/geekculture/reverse-engineering-bare-metal-firmware-part-3-analyzing-arm-assembly-and-exploiting-3b2dbe219f19
- https://linuxsecurityblog.com/2019/10/03/reverse-engineering-router-firmware/
- https://owasp.org/www-chapter-coimbatore/assets/files/Router%20Reversing%20by%20Adithyan%20AK.pdf
- https://hakin9.org/uefi_retool-a-tool-for-uefi-firmware-reverse-engineering/

FIRMWARE REVERSE ENGINEERING AND EXPLOITATION

- http://solidsystemsllc.com/firmware-security/#:~:text=Firmware%20malware%20will%20exploit%20this,be%20used%20for%20several%20purposes.
- https://cromwell-intl.com/cybersecurity/hardware.html
- https://www.csoonline.com/article/3410046/hardware-and-firmware-vulnerabilities-a-guide-to-the-threats.html
- https://www.manageengine.com/network-configuration-manager/firmware-vulnerability.html
- https://www.tanaza.com/tanazaclassic/blog/hackers-exploit-firmware-vulnerabilities-on-ubiquity-network-devices/
- https://www.darkreading.com/risk/unsecured-iot-8-ways-hackers-exploit-firmware-vulnerabilities
- https://digitalguardian.com/blog/router-firmware-vulnerability-bypasses-authentication
- https://resources.infosecinstitute.com/topic/how-to-identify-and-prevent-firmware-vulnerabilities/
- https://medium.datadriveninvestor.com/iot-security-firmware-exploitation-8160028d8a2d

EXPLOIT NETWORK IOT

- https://www.esecurityplanet.com/cloud/attackers-exploit-flaw-in-millions-of-routers-iot-devices/
- https://i.blackhat.com/USA-19/Wednesday/us-19-Shaik-New-Vulnerabilities-In-5G-Networks-wp.pdf
- https://www.blackhat.com/docs/us-15/materials/us-15-Zillner-ZigBee-Exploited-The-Good-The-Bad-And-The-Ugly-wp.pdf
- https://i.blackhat.com/asia-21/Thursday-Handouts/as-21-dosSantos-The-Cost-of-Complexity-Different-Vulnerabilities-While-Implementing-the-Same-RFC-wp.pdf
- https://i.blackhat.com/USA21/Wednesday-Handouts/us-21-Over-The-Air-Baseband-Exploit-Gaining-Remote-Code-Execution-On-5G-Smartphones-wp.pdf
- https://i.blackhat.com/eu-20/Wednesday/eu-20-dosSantos-How-Embedded-TCPIP-Stacks-Breed-Critical-Vulnerabilities-wp.pdf
- https://www.blackhat.com/docs/us-15/materials/us-15-Zillner-ZigBee-Exploited-The-Good-The-Bad-And-The-Ugly.pdf
- https://www.blackhat.com/docs/us-16/materials/us-16-Sabanal-Into-The-Core-In-Depth-Exploration-Of-Windows-10-IoT-Core-wp.pdf
- https://www.blackhat.com/docs/us-17/thursday/us-17-Luo-Iotcandyjar-Towards-An-Intelligent-Interaction-Honeypot-For-IoT-Devices-wp.pdf

EXPLOIT NETWORK IOT

- https://i.blackhat.com/USA-20/Thursday/us-20-Seri-EtherOops-Exploring-Practical-Methods-To-Exploit-Ethernet-Packet-In-Packet-Attacks-wp.pdf
- https://i.blackhat.com/USA-20/Wednesday/us-20-Maggi-OTRazor-Static-Code-Analysis-For-Vulnerability-Discovery-In-Industrial-Automation-Scripts-wp.pdf
- https://i.blackhat.com/eu-20/Wednesday/eu-20-dosSantos-How-Embedded-TCPIP-Stacks-Breed-Critical-Vulnerabilities.pdf
- https://i.blackhat.com/USA-20/Wednesday/us-20-Balduzzi-Industrial-Protocol-Gateways-Under-Analysis-wp.pdf