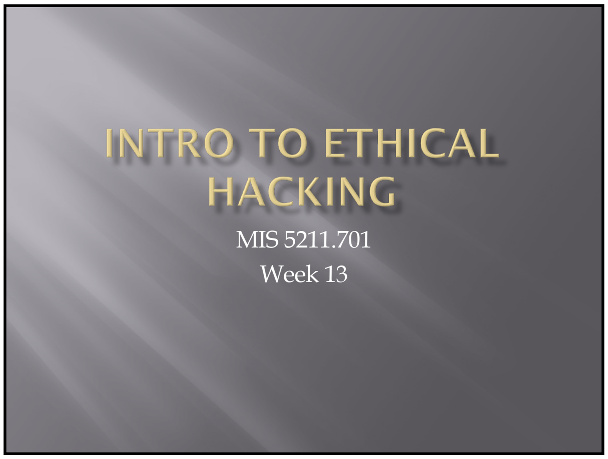
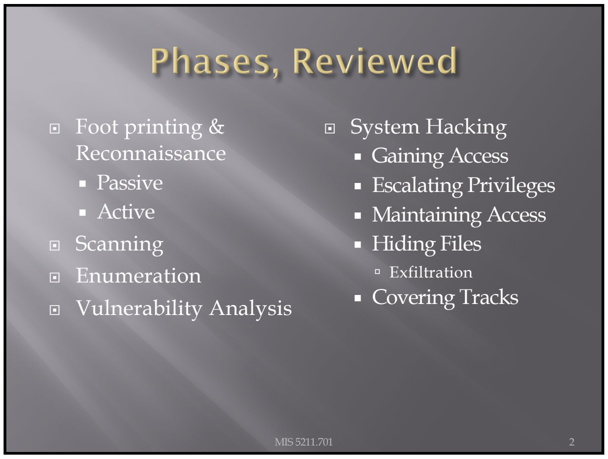


INTRO TO ETHICAL HACKING

MIS 5211.701

Week 13

1

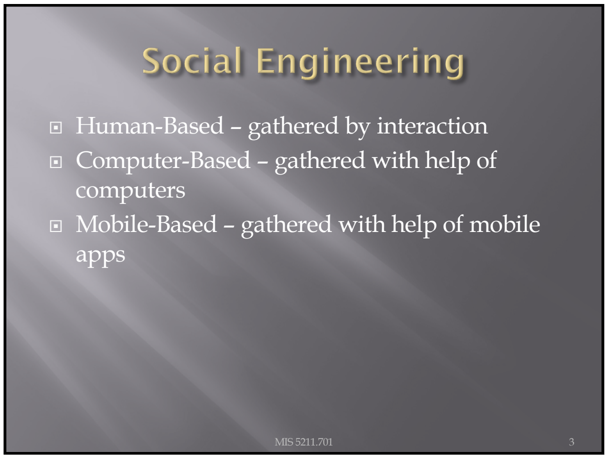


Phases, Reviewed

- Foot printing & Reconnaissance
  - Passive
  - Active
- Scanning
- Enumeration
- Vulnerability Analysis
- System Hacking
  - Gaining Access
  - Escalating Privileges
  - Maintaining Access
  - Hiding Files
    - Exfiltration
  - Covering Tracks

MIS 5211.701 2

2

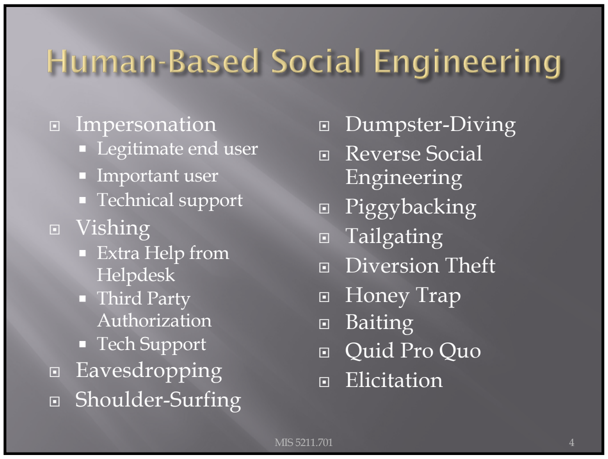


Social Engineering

- Human-Based – gathered by interaction
- Computer-Based – gathered with help of computers
- Mobile-Based – gathered with help of mobile apps

MIS 5211.701 3

3

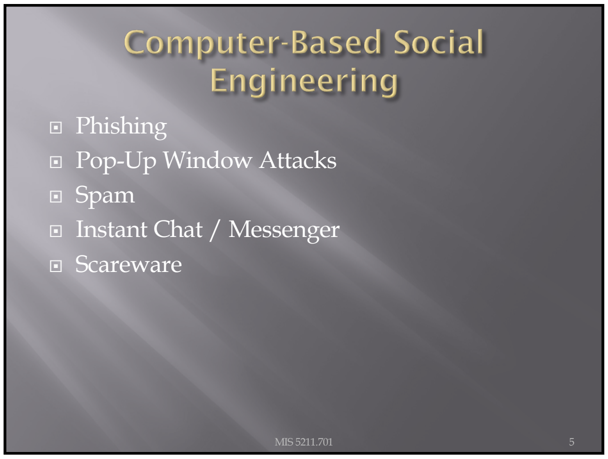


Human-Based Social Engineering

- Impersonation
  - Legitimate end user
  - Important user
  - Technical support
- Vishing
  - Extra Help from Helpdesk
  - Third Party Authorization
  - Tech Support
- Eavesdropping
- Shoulder-Surfing
- Dumpster-Diving
- Reverse Social Engineering
- Piggybacking
- Tailgating
- Diversion Theft
- Honey Trap
- Baiting
- Quid Pro Quo
- Elicitation

MIS 5211.701 4

4

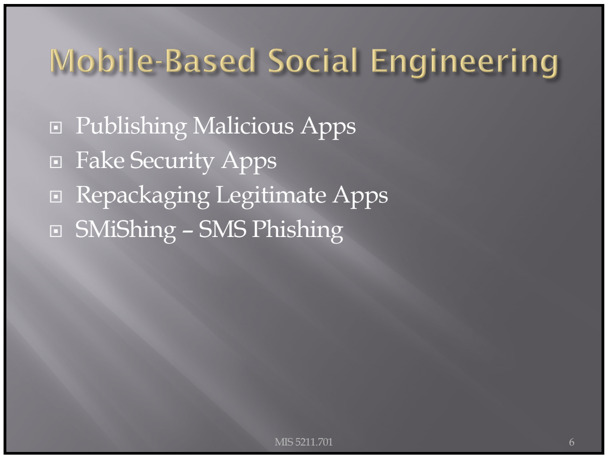


Computer-Based Social Engineering

- Phishing
- Pop-Up Window Attacks
- Spam
- Instant Chat / Messenger
- Scareware

MIS 5211.701 5

5

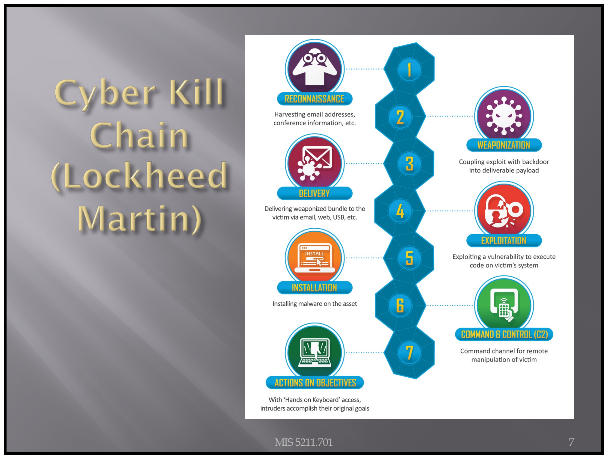


Mobile-Based Social Engineering

- Publishing Malicious Apps
- Fake Security Apps
- Repackaging Legitimate Apps
- SMiShing – SMS Phishing

MIS 5211.701 6

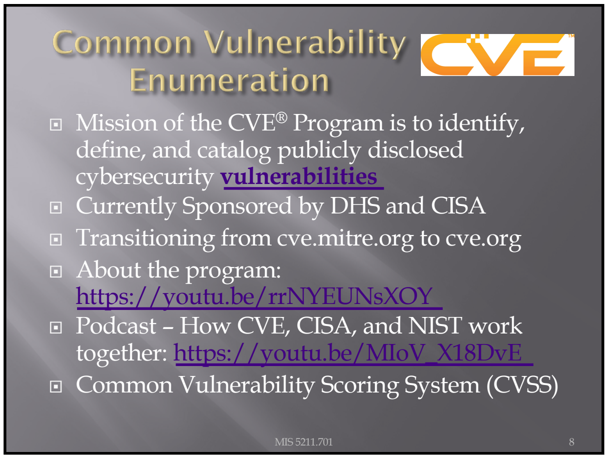
6



Cyber Kill Chain (Lockheed Martin)

1
RECONNAISSANCE
Harvesting email addresses, conference information, etc.
2
WEAPONIZATION
Coupling exploit with backdoor into deliverable payload
3
DELIVERY
Delivering weaponized bundle to the victim via email, web, USB, etc.
4
EXPLOITATION
Exploiting a vulnerability to execute code on victim's system
5
INSTALLATION
Installing malware on the asset
6
COMMAND & CONTROL (C2)
Command channel for remote manipulation of victim
7
ACTIONS ON OBJECTIVES
With 'Hands on Keyboard' access, intruders accomplish their original goals

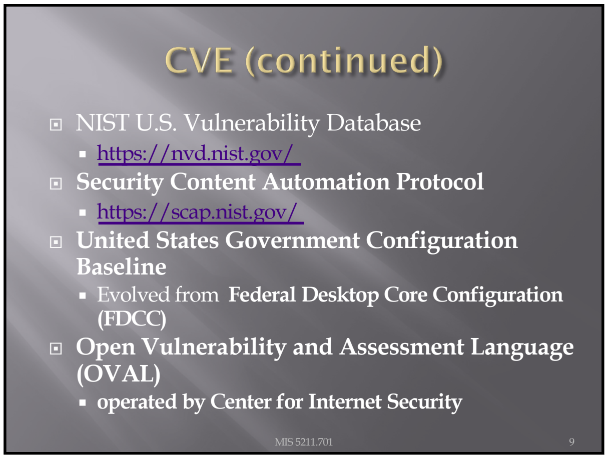
7



Common Vulnerability Enumeration

- Mission of the CVE® Program is to identify, define, and catalog publicly disclosed cybersecurity **vulnerabilities**
- Currently Sponsored by DHS and CISA
- Transitioning from cve.mitre.org to cve.org
- About the program: https://youtu.be/rrNYEUNsXOY
- Podcast – How CVE, CISA, and NIST work together: https://youtu.be/MIoV_X18DvE
- Common Vulnerability Scoring System (CVSS)

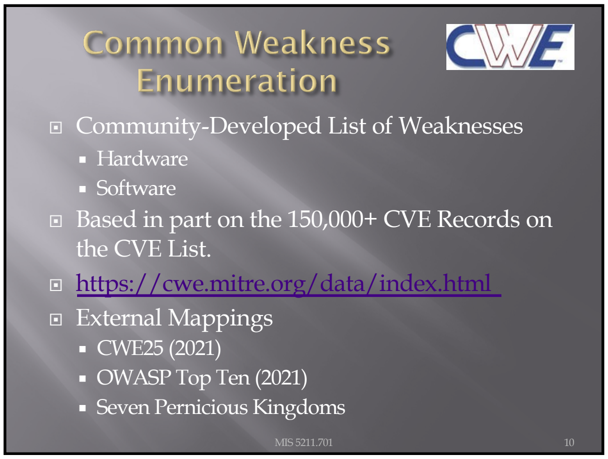
8



CVE (continued)

- NIST U.S. Vulnerability Database
  - https://nvd.nist.gov/
- **Security Content Automation Protocol**
  - https://scap.nist.gov/
- **United States Government Configuration Baseline**
  - Evolved from **Federal Desktop Core Configuration (FDCC)**
- **Open Vulnerability and Assessment Language (OVAL)**
  - **operated by Center for Internet Security**

9

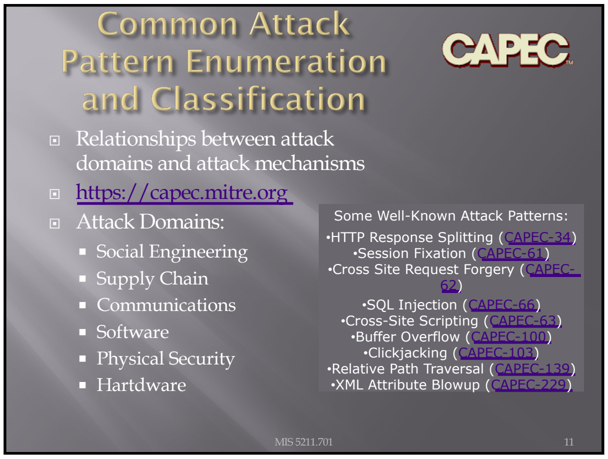


Common Weakness Enumeration

- Community-Developed List of Weaknesses
  - Hardware
  - Software
- Based in part on the 150,000+ CVE Records on the CVE List.
- https://cwe.mitre.org/data/index.html
- External Mappings
  - CWE25 (2021)
  - OWASP Top Ten (2021)
  - Seven Pernicious Kingdoms

MIS 5211.701 10

10



Common Attack Pattern Enumeration and Classification

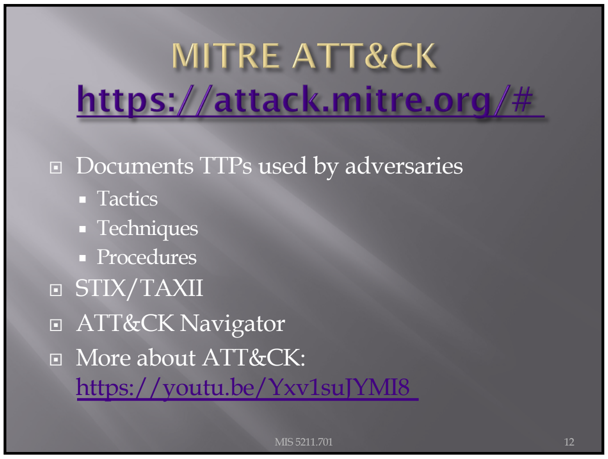
- Relationships between attack domains and attack mechanisms
- https://capec.mitre.org
- Attack Domains:
  - Social Engineering
  - Supply Chain
  - Communications
  - Software
  - Physical Security
  - Hartdware

Some Well-Known Attack Patterns:

•HTTP Response Splitting (CAPEC-34)
•Session Fixation (CAPEC-61)
•Cross Site Request Forgery (CAPEC-62)
•SQL Injection (CAPEC-66)
•Cross-Site Scripting (CAPEC-63)
•Buffer Overflow (CAPEC-100)
•Clickjacking (CAPEC-103)
•Relative Path Traversal (CAPEC-139)
•XML Attribute Blowup (CAPEC-229)

MIS 5211.701 11

11



MITRE ATT&CK https://attack.mitre.org/#

- Documents TTPs used by adversaries
  - Tactics
  - Techniques
  - Procedures
- STIX/TAXII
- ATT&CK Navigator
- More about ATT&CK: https://youtu.be/Yxv1suJYMI8

MIS 5211.701 12

12

MITRE ATT&CK Categories

- Initial access
- Execution
- Persistence
- Privilege escalation
- Defense evasion
- Credentialed access
- Discovery
- Lateral movement
- Collection
- Exfiltration
- Command and Control

13

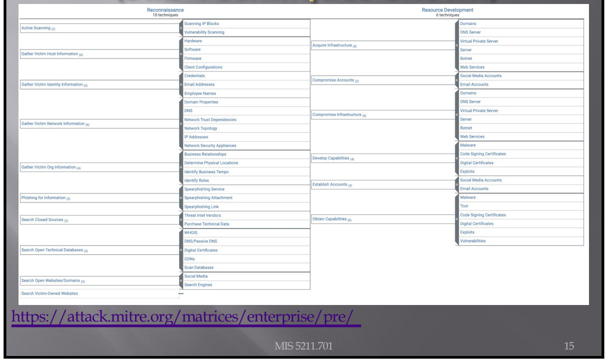
MITRE ATT&CK Matrices

- Enterprise
  - PRE (Preparatory)
  - Windows
  - MacOS
  - Linux
  - Cloud
  - Network
- Mobile
- ICS

Matrix - Enterprise | MITRE ATT&CK®

14

MITRE ATT&CK - PRE (Sub-Techniques Shown)



Reconnaissance
10 techniques

Active Scanning (2)	Scanning IP Blocks Vulnerability Scanning
Gather Victim Host Information (4)	Hardware Software Firmware Client Configurations
Gather Victim Identity Information (3)	Credentials Email Addresses Employee Names
Gather Victim Network Information (6)	Domain Properties DNS Network Trust Dependencies Network Topology IP Addresses Network Security Appliances
Gather Victim Org Information (4)	Business Relationships Determine Physical Locations Identify Business Tempo Identify Roles
Phishing for Information (3)	Spearphishing Service Spearphishing Attachment Spearphishing Link
Search Closed Sources (2)	Threat Intel Vendors Purchase Technical Data
Search Open Technical Databases (5)	WHOIS DNS/Passive DNS Digital Certificates CDNs Scan Databases
Search Open Websites/Domains (2)	Social Media Search Engines
Search Victim-Owned Websites	

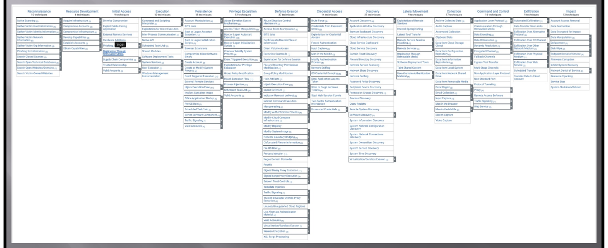
Resource Development
6 techniques

Acquire Infrastructure (6)	Domains DNS Server Virtual Private Server Server Botnet Web Services
Compromise Accounts (2)	Social Media Accounts Email Accounts
Compromise Infrastructure (6)	Domains DNS Server Virtual Private Server Server Botnet Web Services
Develop Capabilities (4)	Malware Code Signing Certificates Digital Certificates Exploits
Establish Accounts (2)	Social Media Accounts Email Accounts
Obtain Capabilities (6)	Malware Tool Code Signing Certificates Digital Certificates Exploits Vulnerabilities

https://attack.mitre.org/matrices/enterprise/pre/

15

MITRE ATT&CK - Enterprise

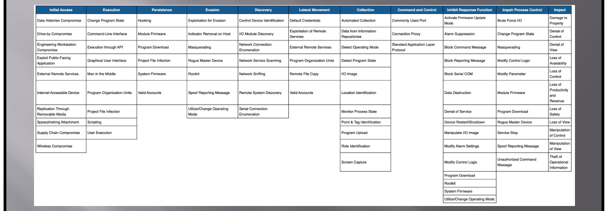


Reconnaissance 10 techniques	Resource Development 6 techniques	Initial Access 9 techniques	Execution 10 techniques	Persistence 18 techniques	Privilege Escalation 12 techniques	Defense Evasion 37 techniques
Active Scanning (2)	Acquire Infrastructure (6)	Drive-by Compromise	Command and Scripting Interpreter (8)	Account Manipulation (4)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)
Gather Victim Host Information (4)	Compromise Accounts (2)	Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)
Gather Victim Identity Information (3)	Compromise Infrastructure (6)	External Remote Services	Inter-Process Communication (2)	Boot or Logon Autostart Execution (12)	Boot or Logon Autostart Execution (12)	BITS Jobs
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions	Native API	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Deobfuscate/Decode Files or Information
Gather Victim Org Information (4)	Establish Accounts (2)	Phishing T1091	Scheduled Task/Job (6)	Browser Extensions	Create or Modify System Process (4)	Direct Volume Access
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Shared Modules	Compromise Client Software Binary	Event Triggered Execution (15)	Execution Guardrails (1)
Search Closed Sources (2)		Supply Chain Compromise (3)	Software Deployment Tools	Create Account (3)	Exploitation for Privilege Escalation	Exploitation for Defense Evasion
Search Open Technical Databases (5)		Trusted Relationship	System Services (2)	Create or Modify System Process (4)	Group Policy Modification	File and Directory Permissions Modification (2)
Search Open Websites/Domains (2)		Valid Accounts (4)	User Execution (2)	Event Triggered Execution (15)	Hijack Execution Flow (11)	Group Policy Modification
Search Victim-Owned Websites			Windows Management Instrumentation	External Remote Services	Process Injection (11)	Hide Artifacts (7)
				Hijack Execution Flow (11)	Scheduled Task/Job (6)	Hijack Execution Flow (11)
				Implant Container Image	Valid Accounts (4)	Impair Defenses (7)
				Office Application Startup (6)		Indicator Removal on Host (6)
				Pre-OS Boot (5)		Indirect Command Execution
				Scheduled Task/Job (6)		Masquerading (6)
				Server Software Component (3)		Modify Authentication Process (4)
				Traffic Signaling (1)		Modify Cloud Compute Infrastructure (4)
				Valid Accounts (4)		Modify Registry
						Modify System Image (2)
						Network Boundary Bridging (1)
						Obfuscated Files or Information (5)
						Pre-OS Boot (5)
						Process Injection (11)
						Rogue Domain Controller
						Rootkit
						Signed Binary Proxy Execution (11)
						Signed Script Proxy Execution (1)
						Subvert Trust Controls (4)
						Template Injection
						Traffic Signaling (1)
						Trusted Developer Utilities Proxy Execution (1)
						Unused/Unsupported Cloud Regions
						Use Alternate Authentication Material (4)
						Valid Accounts (4)
						Virtualization/Sandbox Evasion (3)
						Weaken Encryption (2)
						XSL Script Processing

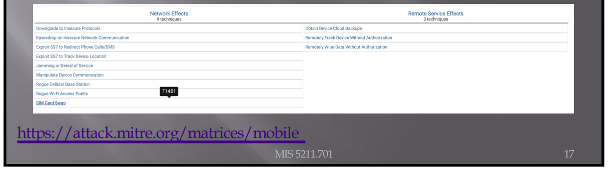
Credential Access 14 techniques	Discovery 25 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Brute Force (4)	Account Discovery (4)	Exploitation of Remote Services	Archive Collected Data (3)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Credentials from Password Stores (3)	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding (2)	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Forced Authentication	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Clipboard Data	Data Obfuscation (3)	Exfiltration Over C2 Channel	Data Manipulation (3)
Input Capture (4)	Cloud Service Dashboard	Remote Services (6)	Data from Cloud Storage Object	Dynamic Resolution (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Man-in-the-Middle (2)	Cloud Service Discovery	Replication Through Removable Media	Data from Configuration Repository (2)	Encrypted Channel (2)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Modify Authentication Process (4)	Domain Trust Discovery	Software Deployment Tools	Data from Information Repositories (2)	Fallback Channels	Exfiltration Over Web Service (2)	Endpoint Denial of Service (4)
Network Sniffing	File and Directory Discovery	Taint Shared Content	Data from Local System	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
OS Credential Dumping (8)	Network Service Scanning	Use Alternate Authentication Material (4)	Data from Network Shared Drive	Multi-Stage Channels	Transfer Data to Cloud Account	Inhibit System Recovery
Steal Application Access Token	Network Share Discovery		Data from Removable Media	Non-Application Layer Protocol		Network Denial of Service (2)
Steal or Forge Kerberos Tickets (4)	Network Sniffing		Data Staged (2)	Non-Standard Port		Resource Hijacking
Steal Web Session Cookie	Password Policy Discovery		Email Collection (3)	Protocol Tunneling		Service Stop
Two-Factor Authentication Interception	Peripheral Device Discovery		Input Capture (4)	Proxy (4)		System Shutdown/Reboot
Unsecured Credentials (6)	Permission Groups Discovery (3)		Man in the Browser	Remote Access Software		
	Process Discovery		Man-in-the-Middle (2)	Traffic Signaling (1)		
	Query Registry		Screen Capture	Web Service (3)		
	Remote System Discovery		Video Capture			
	Software Discovery (1)					
	System Information Discovery					
	System Network Configuration Discovery					
	System Network Connections Discovery					
	System Owner/User Discovery					
	System Service Discovery					
	System Time Discovery					
	Virtualization/Sandbox Evasion (3)					

https://attack.mitre.org/matrices/enterprise

MITRE ATT&CK – Mobile



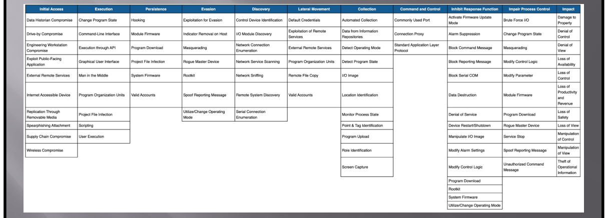
Initial Access	Execution	Persistence	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
Data Historian Compromise	Change Program State	Hooking	Exploitation for Evasion	Control Device Identification	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Drive-by Compromise	Command-Line Interface	Module Firmware	Indicator Removal on Host	I/O Module Discovery	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Change Program State	Denial of Control
Engineering Workstation Compromise	Execution through API	Program Download	Masquerading	Network Connection Enumeration	External Remote Services	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Masquerading	Denial of View
Exploit Public-Facing Application	Graphical User Interface	Project File Infection	Rogue Master Device	Network Service Scanning	Program Organization Units	Detect Program State		Block Reporting Message	Modify Control Logic	Loss of Availability
External Remote Services	Man in the Middle	System Firmware	Rootkit	Network Sniffing	Remote File Copy	I/O Image		Block Serial COM	Modify Parameter	Loss of Control
Internet Accessible Device	Program Organization Units	Valid Accounts	Spoof Reporting Message	Remote System Discovery	Valid Accounts	Location Identification		Data Destruction	Module Firmware	Loss of Productivity and Revenue
Replication Through Removable Media	Project File Infection		Utilize/Change Operating Mode	Serial Connection Enumeration		Monitor Process State		Denial of Service	Program Download	Loss of Safety
Spearphishing Attachment	Scripting					Point & Tag Identification		Device Restart/Shutdown	Rogue Master Device	Loss of View
Supply Chain Compromise	User Execution					Program Upload		Manipulate I/O Image	Service Stop	Manipulation of Control
Wireless Compromise						Role Identification		Modify Alarm Settings	Spoof Reporting Message	Manipulation of View
						Screen Capture		Modify Control Logic	Unauthorized Command Message	Theft of Operational Information
								Program Download		
								Rootkit		
								System Firmware		
								Utilize/Change Operating Mode		



Network Effects 9 techniques	Remote Service Effects 3 techniques
Downgrade to Insecure Protocols	Obtain Device Cloud Backups
Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization
Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization
Exploit SS7 to Track Device Location	
Jamming or Denial of Service	
Manipulate Device Communication	
Rogue Cellular Base Station	
Rogue Wi-Fi Access Points T1451	
SIM Card Swap	

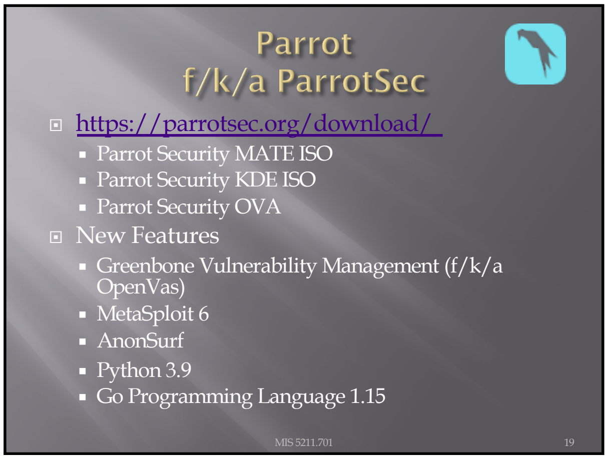
https://attack.mitre.org/matrices/mobile

MITRE ATT&CK for ICS



Initial Access	Execution	Persistence	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
Data Historian Compromise	Change Program State	Hooking	Exploitation for Evasion	Control Device Identification	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Drive-by Compromise	Command-Line Interface	Module Firmware	Indicator Removal on Host	I/O Module Discovery	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Change Program State	Denial of Control
Engineering Workstation Compromise	Execution through API	Program Download	Masquerading	Network Connection Enumeration	External Remote Services	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Masquerading	Denial of View
Exploit Public-Facing Application	Graphical User Interface	Project File Infection	Rogue Master Device	Network Service Scanning	Program Organization Units	Detect Program State		Block Reporting Message	Modify Control Logic	Loss of Availability
External Remote Services	Man in the Middle	System Firmware	Rootkit	Network Sniffing	Remote File Copy	I/O Image		Block Serial COM	Modify Parameter	Loss of Control
Internet Accessible Device	Program Organization Units	Valid Accounts	Spoof Reporting Message	Remote System Discovery	Valid Accounts	Location Identification		Data Destruction	Module Firmware	Loss of Productivity and Revenue
Replication Through Removable Media	Project File Infection		Utilize/Change Operating Mode	Serial Connection Enumeration		Monitor Process State		Denial of Service	Program Download	Loss of Safety
Spearphishing Attachment	Scripting					Point & Tag Identification		Device Restart/Shutdown	Rogue Master Device	Loss of View
Supply Chain Compromise	User Execution					Program Upload		Manipulate I/O Image	Service Stop	Manipulation of Control
Wireless Compromise						Role Identification		Modify Alarm Settings	Spoof Reporting Message	Manipulation of View
						Screen Capture		Modify Control Logic	Unauthorized Command Message	Theft of Operational Information
								Program Download		
								Rootkit		
								System Firmware		
								Utilize/Change Operating Mode		

https://collaborate.mitre.org/attackics/index.php/Main_Page

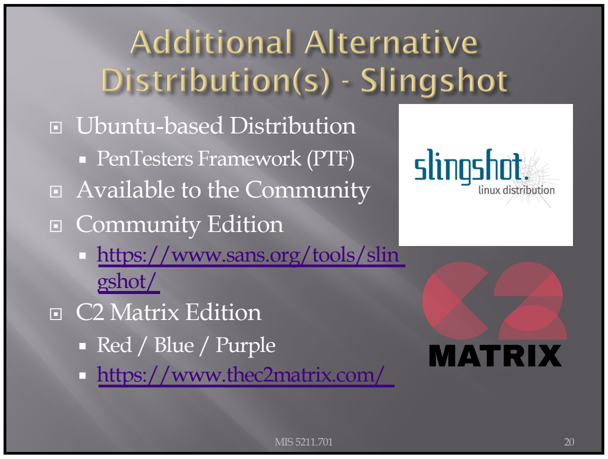


Parrot f/k/a ParrotSec

- https://parrotsec.org/download/
  - Parrot Security MATE ISO
  - Parrot Security KDE ISO
  - Parrot Security OVA
- New Features
  - Greenbone Vulnerability Management (f/k/a OpenVas)
  - MetaSploit 6
  - AnonSurf
  - Python 3.9
  - Go Programming Language 1.15

MIS 5211.701 19

19



Additional Alternative Distribution(s) - Slingshot

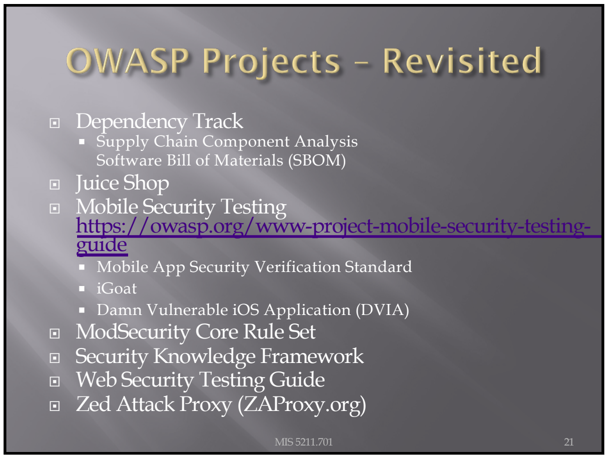
- Ubuntu-based Distribution
  - PenTesters Framework (PTF)
- Available to the Community
- Community Edition
  - https://www.sans.org/tools/slingshot/
- C2 Matrix Edition
  - Red / Blue / Purple
  - https://www.thec2matrix.com/

slingshot linux distribution

MATRIX

MIS 5211.701 20

20

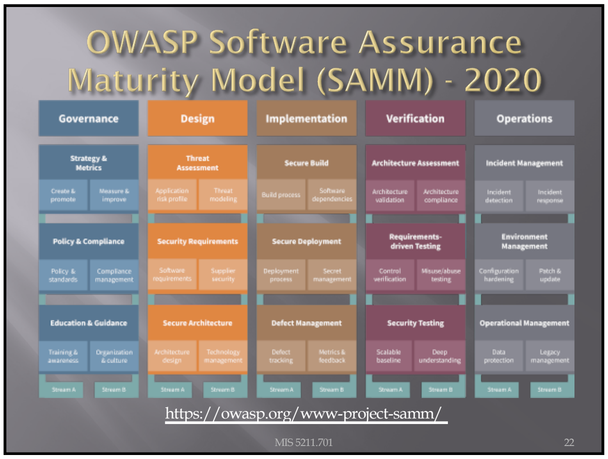


OWASP Projects – Revisited

- Dependency Track
  - Supply Chain Component Analysis
    Software Bill of Materials (SBOM)
- Juice Shop
- Mobile Security Testing
  https://owasp.org/www-project-mobile-security-testing-guide
  - Mobile App Security Verification Standard
  - iGoat
  - Damn Vulnerable iOS Application (DVIA)
- ModSecurity Core Rule Set
- Security Knowledge Framework
- Web Security Testing Guide
- Zed Attack Proxy (ZAProxy.org)

MIS 5211.701 21

21



OWASP Software Assurance Maturity Model (SAMM) - 2020

Governance	Design	Implementation	Verification	Operations
Strategy & Metrics	Threat Assessment	Secure Build	Architecture Assessment	Incident Management
Create & promote Measure & improve	Application risk profile Threat modeling	Build process Software dependencies	Architecture validation Architecture compliance	Incident detection Incident response
Policy & Compliance	Security Requirements	Secure Deployment	Requirements-driven Testing	Environment Management
Policy & standards Compliance management	Software requirements Supplier security	Deployment process Secret management	Control verification Misuse/abuse testing	Configuration hardening Patch & update
Education & Guidance	Secure Architecture	Defect Management	Security Testing	Operational Management
Training & awareness Organization & culture	Architecture design Technology management	Defect tracking Metrics & feedback	Scalable baseline Deep understanding	Data protection Legacy management
Stream A Stream B	Stream A Stream B	Stream A Stream B	Stream A Stream B	Stream A Stream B

https://owasp.org/www-project-samm/

MIS 5211.701 22

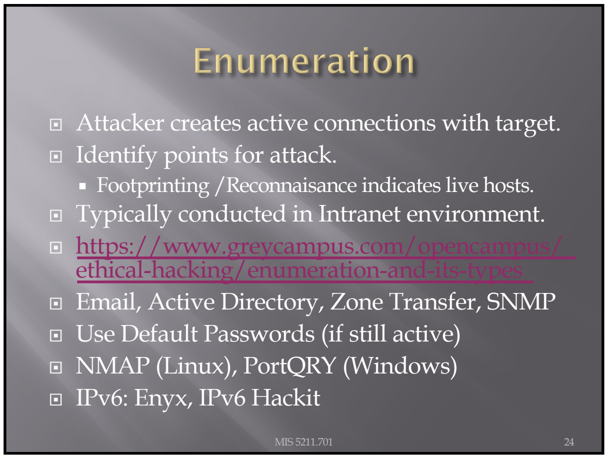
22

Soft Skills & Job Search BsidesDE Video

- Security BSides Delaware 2020 - TheBlindHacker – YouTube
- The Blindhacker on Soft skills and the job search

MIS 5211.701 23

23

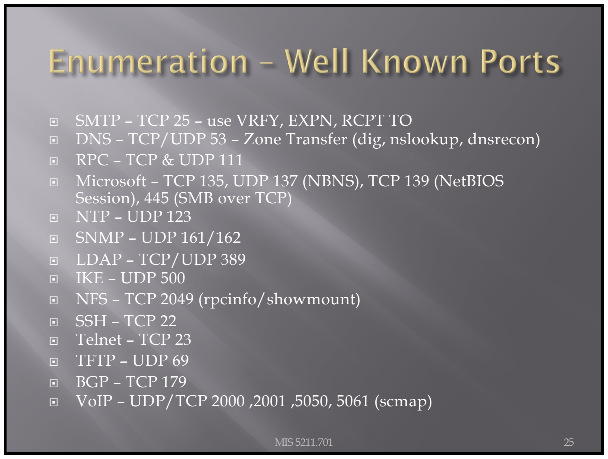


Enumeration

- Attacker creates active connections with target.
- Identify points for attack.
  - Footprinting /Reconnaisance indicates live hosts.
- Typically conducted in Intranet environment.
- https://www.greycampus.com/opencampus/ethical-hacking/enumeration-and-its-types
- Email, Active Directory, Zone Transfer, SNMP
- Use Default Passwords (if still active)
- NMAP (Linux), PortQRY (Windows)
- IPv6: Enyx, IPv6 Hackit

MIS 5211.701 24

24

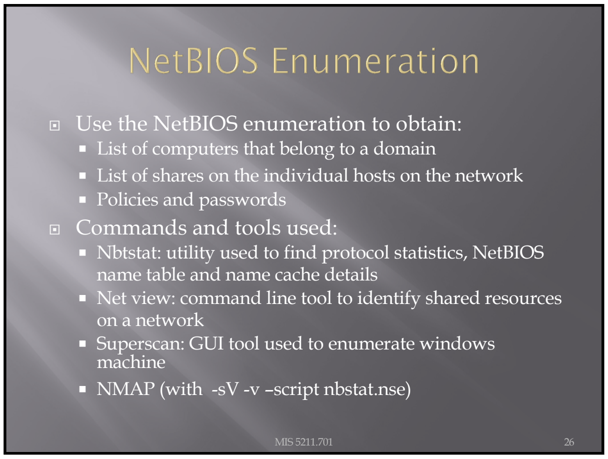


Enumeration – Well Known Ports

- SMTP – TCP 25 – use VRFY, EXPN, RCPT TO
- DNS – TCP/UDP 53 – Zone Transfer (dig, nslookup, dnsrecon)
- RPC – TCP & UDP 111
- Microsoft – TCP 135, UDP 137 (NBNS), TCP 139 (NetBIOS Session), 445 (SMB over TCP)
- NTP – UDP 123
- SNMP – UDP 161/162
- LDAP – TCP/UDP 389
- IKE – UDP 500
- NFS – TCP 2049 (rpcinfo/showmount)
- SSH – TCP 22
- Telnet – TCP 23
- TFTP – UDP 69
- BGP – TCP 179
- VoIP – UDP/TCP 2000 ,2001 ,5050, 5061 (scmap)

MIS 5211.701 25

25

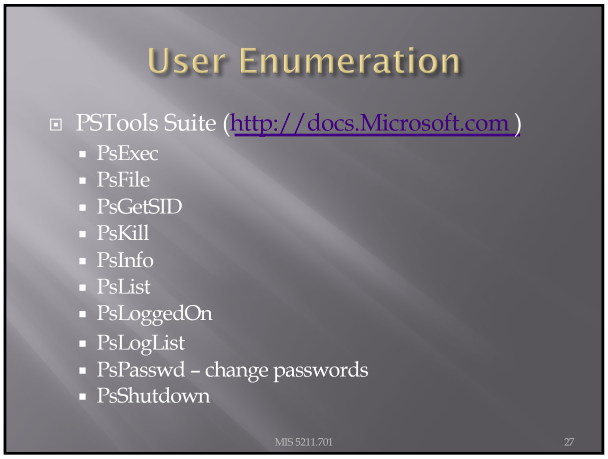


NetBIOS Enumeration

- Use the NetBIOS enumeration to obtain:
  - List of computers that belong to a domain
  - List of shares on the individual hosts on the network
  - Policies and passwords
- Commands and tools used:
  - Nbtstat: utility used to find protocol statistics, NetBIOS name table and name cache details
  - Net view: command line tool to identify shared resources on a network
  - Superscan: GUI tool used to enumerate windows machine
  - NMAP (with -sV -v –script nbstat.nse)

MIS 5211.701 26

26

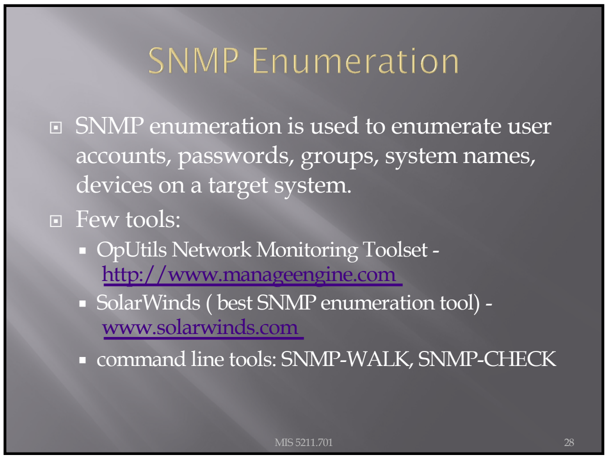


User Enumeration

- PSTools Suite (http://docs.Microsoft.com)
  - PsExec
  - PsFile
  - PsGetSID
  - PsKill
  - PsInfo
  - PsList
  - PsLoggedOn
  - PsLogList
  - PsPasswd – change passwords
  - PsShutdown

MIS 5211.701 27

27

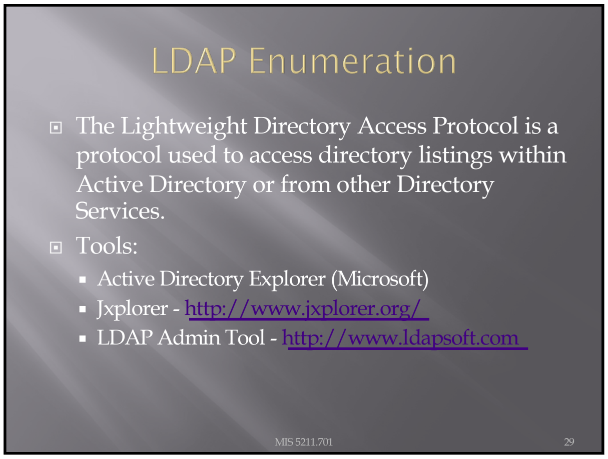


SNMP Enumeration

- SNMP enumeration is used to enumerate user accounts, passwords, groups, system names, devices on a target system.
- Few tools:
  - OpUtils Network Monitoring Toolset - http://www.manageengine.com
  - SolarWinds (best SNMP enumeration tool) - www.solarwinds.com
  - command line tools: SNMP-WALK, SNMP-CHECK

MIS 5211.701 28

28

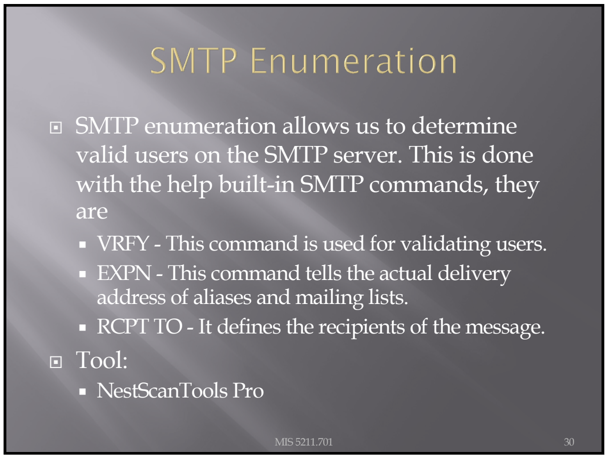


LDAP Enumeration

- The Lightweight Directory Access Protocol is a protocol used to access directory listings within Active Directory or from other Directory Services.
- Tools:
  - Active Directory Explorer (Microsoft)
  - Jxplorer - http://www.jxplorer.org/
  - LDAP Admin Tool - http://www.ldapsoft.com

MIS 5211.701 29

29

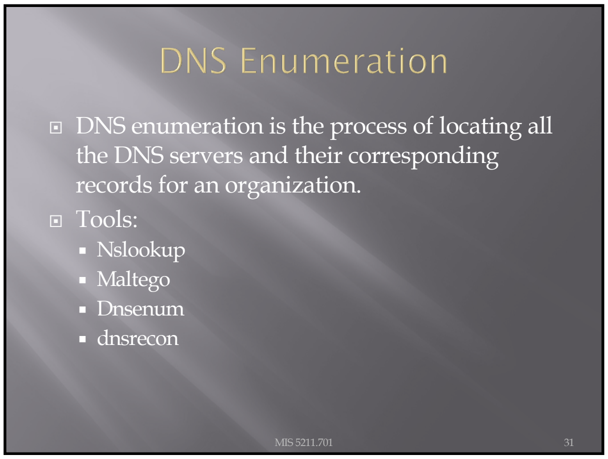


SMTP Enumeration

- SMTP enumeration allows us to determine valid users on the SMTP server. This is done with the help built-in SMTP commands, they are
  - VRFY - This command is used for validating users.
  - EXPN - This command tells the actual delivery address of aliases and mailing lists.
  - RCPT TO - It defines the recipients of the message.
- Tool:
  - NestScanTools Pro

MIS 5211.701 30

30

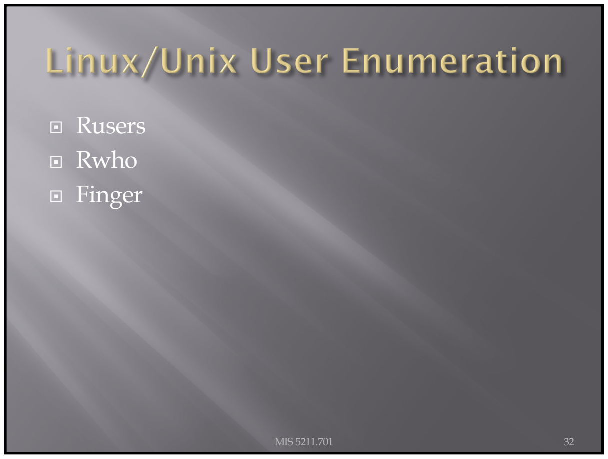


DNS Enumeration

- DNS enumeration is the process of locating all the DNS servers and their corresponding records for an organization.
- Tools:
  - Nslookup
  - Maltego
  - Dnsenum
  - dnsrecon

MIS 5211.701 31

31

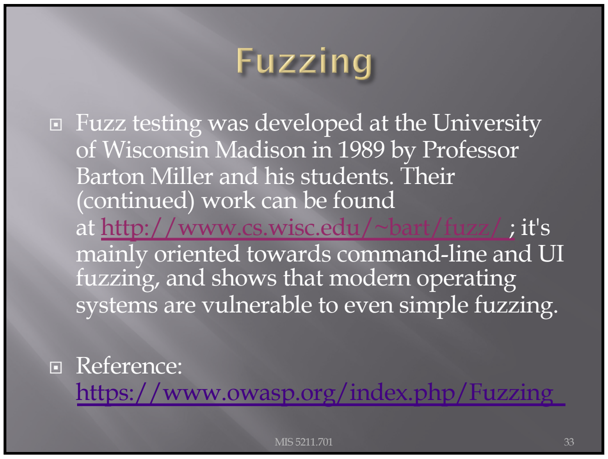


Linux/Unix User Enumeration

- Rusers
- Rwho
- Finger

MIS 5211.701 32

32

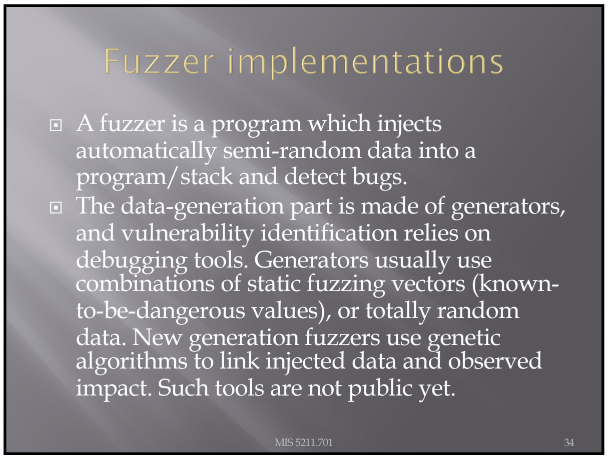


Fuzzing

- Fuzz testing was developed at the University of Wisconsin Madison in 1989 by Professor Barton Miller and his students. Their (continued) work can be found at http://www.cs.wisc.edu/~bart/fuzz/ ; it's mainly oriented towards command-line and UI fuzzing, and shows that modern operating systems are vulnerable to even simple fuzzing.
- Reference: https://www.owasp.org/index.php/Fuzzing

MIS 5211.701 33

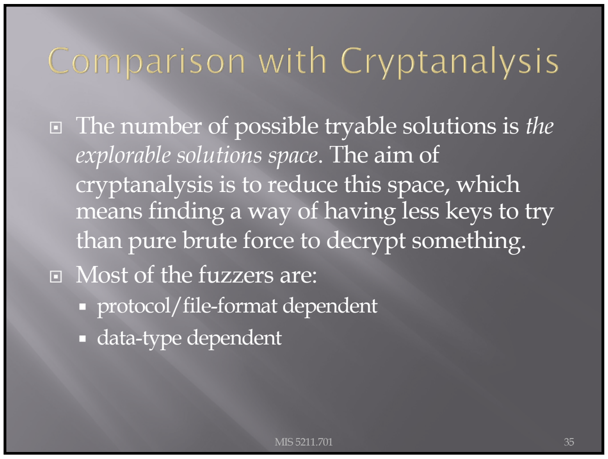
33



Fuzzer implementations

- A fuzzer is a program which injects automatically semi-random data into a program/stack and detect bugs.
- The data-generation part is made of generators, and vulnerability identification relies on debugging tools. Generators usually use combinations of static fuzzing vectors (known-to-be-dangerous values), or totally random data. New generation fuzzers use genetic algorithms to link injected data and observed impact. Such tools are not public yet.

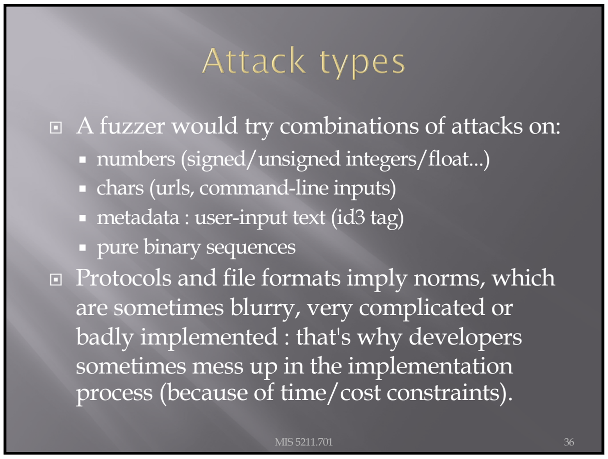
34



Comparison with Cryptanalysis

- The number of possible tryable solutions is *the explorable solutions space*. The aim of cryptanalysis is to reduce this space, which means finding a way of having less keys to try than pure brute force to decrypt something.
- Most of the fuzzers are:
  - protocol/file-format dependent
  - data-type dependent

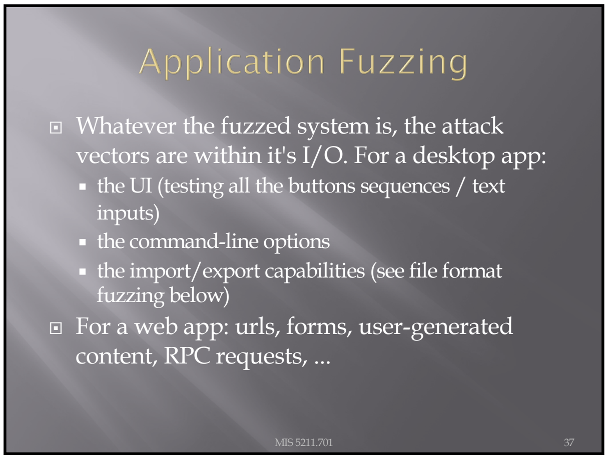
35



Attack types

- A fuzzer would try combinations of attacks on:
  - numbers (signed/unsigned integers/float...)
  - chars (urls, command-line inputs)
  - metadata : user-input text (id3 tag)
  - pure binary sequences
- Protocols and file formats imply norms, which are sometimes blurry, very complicated or badly implemented : that's why developers sometimes mess up in the implementation process (because of time/cost constraints).

36

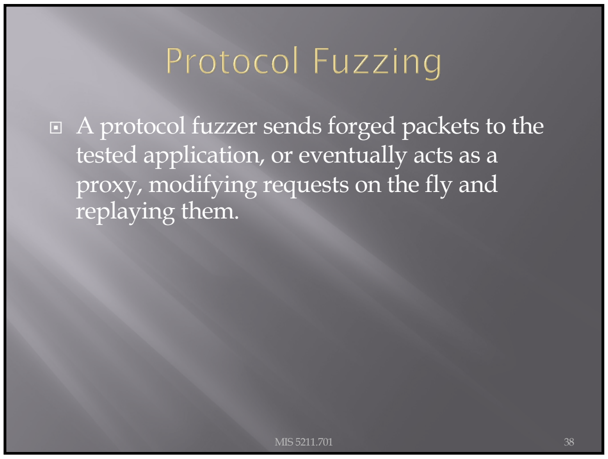


Application Fuzzing

- Whatever the fuzzed system is, the attack vectors are within it's I/O. For a desktop app:
  - the UI (testing all the buttons sequences / text inputs)
  - the command-line options
  - the import/export capabilities (see file format fuzzing below)
- For a web app: urls, forms, user-generated content, RPC requests, ...

MIS 5211.701 37

37

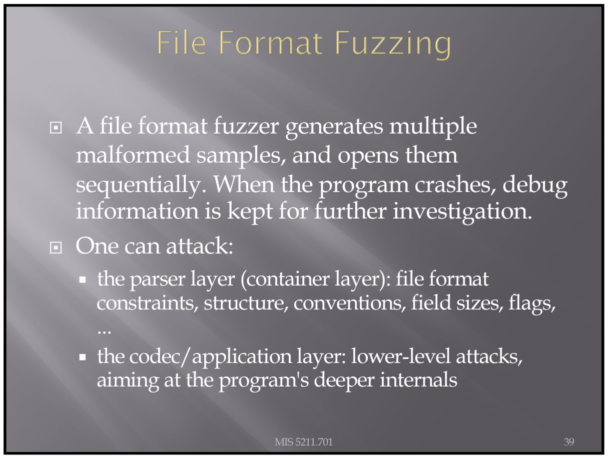


Protocol Fuzzing

- A protocol fuzzer sends forged packets to the tested application, or eventually acts as a proxy, modifying requests on the fly and replaying them.

MIS 5211.701 38

38

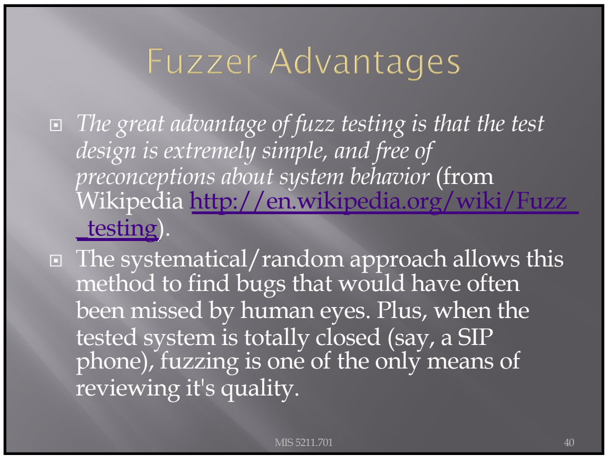


File Format Fuzzing

- A file format fuzzer generates multiple malformed samples, and opens them sequentially. When the program crashes, debug information is kept for further investigation.
- One can attack:
  - the parser layer (container layer): file format constraints, structure, conventions, field sizes, flags, ...
  - the codec/application layer: lower-level attacks, aiming at the program's deeper internals

MIS 5211.701 39

39

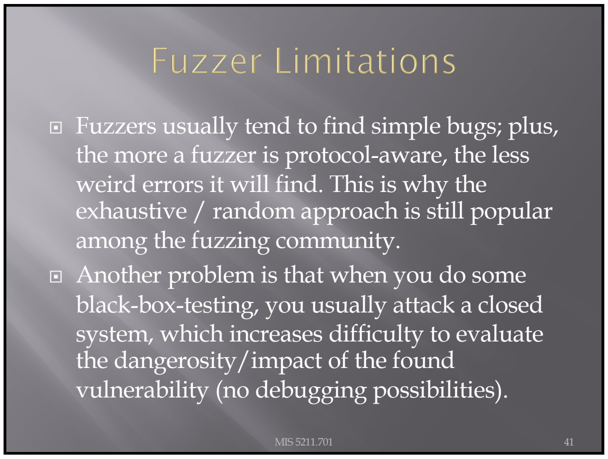


Fuzzer Advantages

- *The great advantage of fuzz testing is that the test design is extremely simple, and free of preconceptions about system behavior* (from Wikipedia http://en.wikipedia.org/wiki/Fuzz_testing).
- The systematical/random approach allows this method to find bugs that would have often been missed by human eyes. Plus, when the tested system is totally closed (say, a SIP phone), fuzzing is one of the only means of reviewing it's quality.

MIS 5211.701 40

40

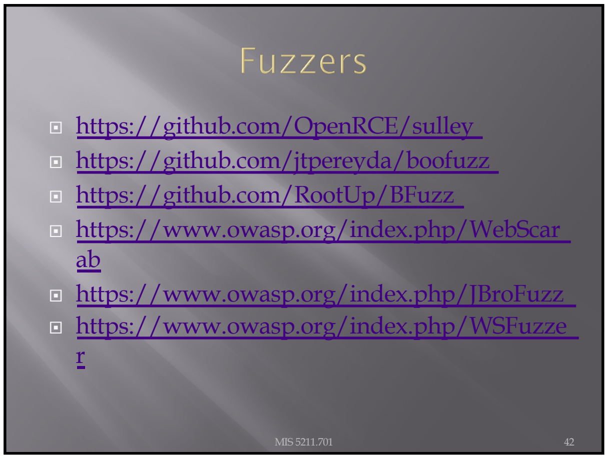


Fuzzer Limitations

- Fuzzers usually tend to find simple bugs; plus, the more a fuzzer is protocol-aware, the less weird errors it will find. This is why the exhaustive / random approach is still popular among the fuzzing community.
- Another problem is that when you do some black-box-testing, you usually attack a closed system, which increases difficulty to evaluate the dangerosity/impact of the found vulnerability (no debugging possibilities).

MIS 5211.701 41

41

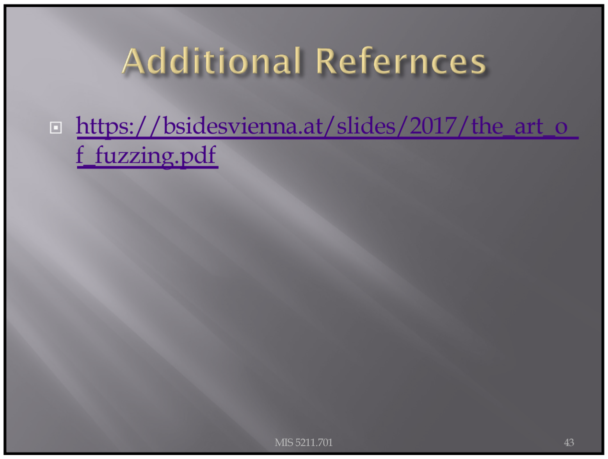


Fuzzers

- https://github.com/OpenRCE/sulley
- https://github.com/jtpereyda/boofuzz
- https://github.com/RootUp/BFuzz
- https://www.owasp.org/index.php/WebScarab
- https://www.owasp.org/index.php/JBroFuzz
- https://www.owasp.org/index.php/WSFuzzer

MIS 5211.701 42

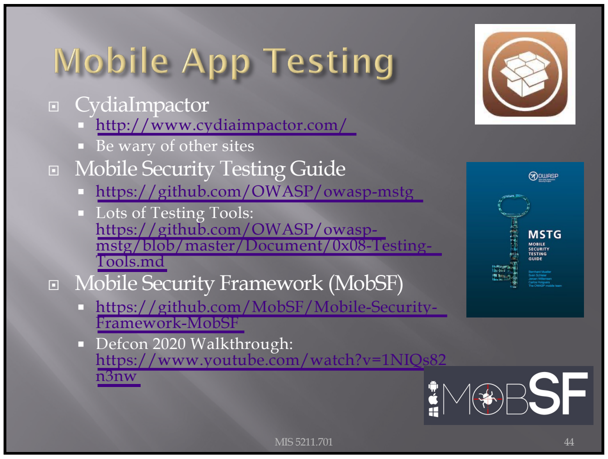
42



Additional Refernces

- https://bsidesvienna.at/slides/2017/the_art_of_fuzzing.pdf

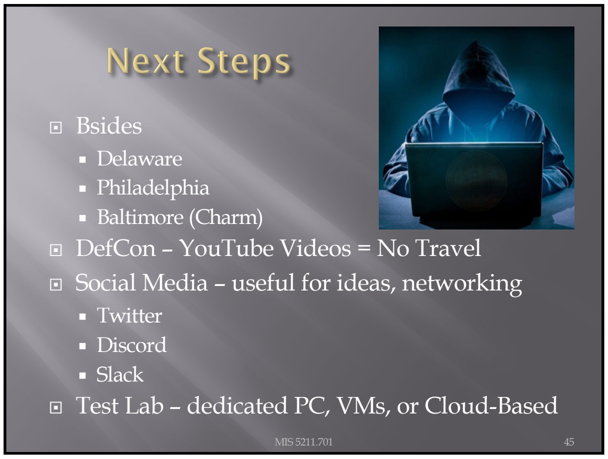
43



Mobile App Testing

- CydiaImpactor
  - http://www.cydiaimpactor.com/
  - Be wary of other sites
- Mobile Security Testing Guide
  - https://github.com/OWASP/owasp-mstg
  - Lots of Testing Tools: https://github.com/OWASP/owasp-mstg/blob/master/Document/0x08-Testing-Tools.md
- Mobile Security Framework (MobSF)
  - https://github.com/MobSF/Mobile-Security-Framework-MobSF
  - Defcon 2020 Walkthrough: https://www.youtube.com/watch?v=1NIQs82n3nw

44



Next Steps

- Bsides
  - Delaware
  - Philadelphia
  - Baltimore (Charm)
- DefCon – YouTube Videos = No Travel
- Social Media – useful for ideas, networking
  - Twitter
  - Discord
  - Slack
- Test Lab – dedicated PC, VMs, or Cloud-Based

45